

**Integrated Dell Remote Access Controller 7 (iDRAC7)
Version 1.00.00 User's Guide**



Notes, Cautions, and Warnings



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



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



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

Information in this publication is subject to change without notice.

© 2012 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, Dell Precision™, OptiPlex™, Latitude™, PowerEdge™, PowerVault™, PowerConnect™, OpenManage™, EqualLogic™, Compellent™, KACE™, FlexAddress™, Force10™ and Vostro™ are trademarks of Dell Inc. Intel®, Pentium®, Xeon®, Core® and Celeron® are registered trademarks of Intel Corporation in the U.S. and other countries. AMD® is a registered trademark and AMD Opteron™, AMD Phenom™ and AMD Sempron™ are trademarks of Advanced Micro Devices, Inc. Microsoft®, Windows®, Windows Server®, Internet Explorer®, MS-DOS®, Windows Vista® 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/or other countries. Novell® and SUSE® are registered trademarks of Novell Inc. in the United States and other countries. Oracle® is a registered trademark of Oracle Corporation and/or its affiliates. Citrix®, Xen®, XenServer® and XenMotion® are either registered trademarks or trademarks of Citrix Systems, Inc. in the United States and/or other countries. VMware®, Virtual SMP®, vMotion®, vCenter® and vSphere® are registered trademarks or trademarks of VMware, Inc. in the United States or other countries. IBM® is a registered trademark of International Business Machines Corporation.

Other trademarks and trade names may be used in this publication 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.

2012 - 03

Rev. A00

Contents

| | |
|---|-----------|
| Notes, Cautions, and Warnings..... | 2 |
| 1 Overview..... | 13 |
| Benefits of Using iDRAC7 with Lifecycle Controller..... | 13 |
| Key Features..... | 14 |
| Managing Licenses | 15 |
| Types of Licenses..... | 15 |
| Acquiring Licenses..... | 15 |
| License Operations..... | 15 |
| Licensable Features In iDRAC7..... | 17 |
| Interfaces and Protocols to Access iDRAC7..... | 19 |
| iDRAC7 Port Information..... | 21 |
| Other Documents You May Need..... | 21 |
| Contacting Dell..... | 22 |
| 2 Logging In to iDRAC7..... | 23 |
| Logging Into iDRAC7 as Local User, Active Directory User, or LDAP User..... | 23 |
| Logging Into iDRAC7 Using Smart Card..... | 24 |
| Logging Into iDRAC7 as a Local User Using Smart Card..... | 24 |
| Logging Into iDRAC7 as an Active Directory User Using Smart Card..... | 25 |
| Logging Into iDRAC7 Using Single Sign-on | 25 |
| Logging into iDRAC7 SSO Using iDRAC7 Web Interface..... | 25 |
| Logging In to iDRAC7 SSO Using iDRAC7 Web Interface..... | 26 |
| Accessing iDRAC7 Using Remote RACADM..... | 26 |
| Validating CA Certificate To Use Remote RACADM on Linux..... | 26 |
| Accessing iDRAC7 Using Local RACADM..... | 26 |
| Accessing iDRAC7 Using Firmware RACADM..... | 27 |
| Accessing iDRAC7 Using SMCLP..... | 27 |
| Logging in to iDRAC7 Using Public Key Authentication..... | 27 |
| Multiple iDRAC7 Sessions..... | 27 |
| 3 Setting Up Managed System and Management Station..... | 29 |
| Setting Up iDRAC7 IP Address..... | 29 |
| Setting Up iDRAC IP Using iDRAC Settings Utility..... | 30 |
| Setting Up iDRAC7 IP Using CMC Web Interface..... | 32 |
| Enabling Auto-discovery..... | 33 |
| Setting Up Management Station..... | 34 |

| | |
|---|----|
| Accessing iDRAC7 Remotely..... | 34 |
| Setting Up Managed System..... | 34 |
| Modifying Local Administrator Account Settings..... | 35 |
| Setting Up Managed System Location..... | 35 |
| Configuring Supported Web Browsers..... | 36 |
| Adding iDRAC7 to the List of Trusted Domains..... | 38 |
| Disabling Whitelist Feature in Firefox..... | 38 |
| Viewing Localized Versions of Web Interface..... | 38 |
| Updating iDRAC7 Firmware..... | 39 |
| Downloading iDRAC7 Firmware..... | 39 |
| Updating Firmware Using iDRAC7 Web Interface..... | 40 |
| Updating Firmware Using CMC Web Interface..... | 41 |
| Updating Firmware Using DUP..... | 41 |
| Updating Firmware Using Remote RACADM..... | 41 |
| Updating Firmware Using Lifecycle Controller Remote Services..... | 42 |
| Rolling Back iDRAC7 Firmware..... | 42 |
| Rollback Firmware Using iDRAC7 Web Interface..... | 42 |
| Rollback Firmware Using CMC Web Interface..... | 43 |
| Rollback Firmware Using RACADM..... | 43 |
| Rollback Firmware Using Lifecycle Controller..... | 43 |
| Rollback Firmware Using Lifecycle Controller-Remote Services..... | 43 |
| Recovering iDRAC7..... | 43 |
| Using TFTP Server..... | 44 |
| Monitoring iDRAC7 Using Other Systems Management Tools..... | 44 |

4 Configuring iDRAC7.....45

| | |
|---|----|
| Viewing iDRAC7 Information..... | 46 |
| Viewing iDRAC7 Information Using Web Interface..... | 46 |
| Viewing iDRAC7 Information Using RACADM..... | 46 |
| Modifying Network Settings..... | 46 |
| Modifying Network Settings Using Web Interface..... | 47 |
| Modifying Network Settings Using Local RACADM..... | 47 |
| Configuring IP Filtering and IP blocking..... | 47 |
| Configuring Services..... | 49 |
| Configuring Services Using Web Interface..... | 49 |
| Configuring Services Using RACADM..... | 49 |
| Configuring Front Panel Display..... | 50 |
| Configuring LCD Setting..... | 50 |
| Configuring System ID LED Setting..... | 51 |
| Setting First Boot Device..... | 52 |
| Setting First Boot Device Using Web Interface..... | 52 |
| Setting First Boot Device Using RACADM..... | 52 |

| | |
|--|-----------|
| Enabling Internal Systems Management Communication..... | 52 |
| Enabling Last Crash Screen..... | 53 |
| Obtaining Certificates..... | 53 |
| SSL Server Certificates..... | 54 |
| Generating a New Certificate Signing Request..... | 55 |
| Uploading Server Certificate..... | 55 |
| Viewing Server Certificate..... | 56 |
| Configuring Multiple iDRAC7s Using RACADM..... | 56 |
| Creating an iDRAC7 Configuration File..... | 57 |
| Parsing Rules..... | 57 |
| Modifying the iDRAC7 IP Address..... | 58 |
| Disabling Access to Modify iDRAC7 Configuration Settings on Host System..... | 59 |
| 5 Viewing iDRAC7 and Managed System Information..... | 61 |
| Viewing Managed System Health and Properties..... | 61 |
| Viewing System Inventory..... | 61 |
| Viewing Sensor Information..... | 61 |
| Inventory and Monitoring Storage Devices..... | 63 |
| Monitoring Storage Device Using Web Interface..... | 63 |
| Monitoring Storage Device Using RACADM..... | 64 |
| Inventory and Monitoring Network Devices..... | 64 |
| Monitoring Network Devices Using Web Interface..... | 64 |
| Monitoring Network Devices Using RACADM..... | 64 |
| Viewing FlexAddress Mezzanine Card Fabric Connections..... | 64 |
| Viewing or Terminating iDRAC7 Sessions..... | 65 |
| Terminating iDRAC7 Sessions Using Web Interface..... | 65 |
| Terminating iDRAC7 Sessions Using RACADM..... | 65 |
| 6 Setting Up iDRAC7 Communication..... | 67 |
| Communicating With iDRAC7 Through Serial Connection Using DB9 Cable..... | 68 |
| Configuring BIOS For Serial Connection..... | 68 |
| Enabling RAC Serial Connection..... | 69 |
| Enabling IPMI Serial Connection Basic and Terminal Modes..... | 69 |
| Switching Between RAC Serial and Serial Console While Using DB9 Cable..... | 71 |
| Switching From Serial Console to RAC Serial..... | 71 |
| Switching From RAC Serial to Serial Console..... | 71 |
| Communicating With iDRAC7 Using IPMI SOL..... | 71 |
| Configuring BIOS For Serial Connection..... | 72 |
| Configuring iDRAC7 to Use SOL..... | 72 |
| Enabling Supported Protocol..... | 73 |
| Communicating With iDRAC7 Using IPMI Over LAN..... | 76 |
| Configuring IPMI Over LAN Using Web Interface..... | 76 |

| | |
|--|----|
| Configuring IPMI Over LAN Using iDRAC Settings Utility..... | 77 |
| Configuring IPMI Over LAN Using RACADM..... | 77 |
| Enabling or Disabling Remote RACADM..... | 77 |
| Enabling or Disabling Remote RACADM Using Web Interface..... | 77 |
| Enabling or Disabling Remote RACADM Using RACADM..... | 78 |
| Disabling Local RACADM..... | 78 |
| Enabling IPMI on Managed System..... | 78 |
| Configuring Linux for Serial Console During Boot..... | 78 |
| Enabling Login to the Virtual Console After Boot..... | 79 |
| Supported SSH Cryptography Schemes..... | 80 |
| Using Public Key Authentication For SSH..... | 81 |

7 Configuring User Accounts and Privileges.....85

| | |
|--|-----|
| Configuring Local Users..... | 85 |
| Configuring Local Users Using iDRAC7 Web Interface..... | 85 |
| Configuring Local Users Using RACADM..... | 86 |
| Configuring Active Directory Users..... | 87 |
| Prerequisites for Using Active Directory Authentication for iDRAC7..... | 88 |
| Supported Active Directory Authentication Mechanisms..... | 90 |
| Standard Schema Active Directory Overview..... | 91 |
| Configuring Standard Schema Active Directory..... | 92 |
| Extended Schema Active Directory Overview..... | 94 |
| Configuring Extended Schema Active Directory..... | 96 |
| Testing Active Directory Settings..... | 104 |
| Configuring Generic LDAP Users..... | 104 |
| Configuring Generic LDAP Directory Service Using iDRAC7 Web-Based Interface..... | 105 |
| Configuring Generic LDAP Directory Service Using RACADM..... | 105 |
| Testing LDAP Directory Service Settings..... | 105 |

8 Configuring iDRAC7 for Single Sign-On or Smart Card Login.....107

| | |
|--|-----|
| Prerequisites for Active Directory Single Sign-On or Smart Card Login..... | 107 |
| Registering iDRAC7 as a Computer in Active Directory Root Domain..... | 108 |
| Generating Kerberos Keytab File..... | 108 |
| Creating Active Directory Objects and Providing Privileges..... | 109 |
| Configuring Browser to Enable Active Directory SSO..... | 109 |
| Configuring iDRAC7 SSO Login for Active Directory Users..... | 109 |
| Configuring iDRAC7 SSO Login for Active Directory Users Using Web Interface..... | 110 |
| Configuring iDRAC7 SSO Login for Active Directory Users Using RACADM..... | 110 |
| Configuring iDRAC7 Smart Card Login for Local Users..... | 110 |
| Uploading Smart Card User Certificate..... | 110 |
| Uploading Trusted CA Certificate For Smart Card..... | 111 |
| Configuring iDRAC7 Smart Card Login for Active Directory Users..... | 111 |

| | |
|--|------------|
| Enabling or Disabling Smart Card Login..... | 112 |
| Enabling or Disabling Smart Card Login Using Web Interface..... | 112 |
| Enabling or Disabling Smart Card Login Using RACADM..... | 112 |
| Enabling or Disabling Smart Card Login Using iDRAC Settings Utility..... | 112 |
| 9 Configuring iDRAC7 to Send Alerts..... | 113 |
| Enabling or Disabling Alerts..... | 113 |
| Enabling or Disabling Alerts Using Web Interface..... | 113 |
| Enabling or Disabling Alerts Using RACADM..... | 114 |
| Enabling or Disabling Alerts Using iDRAC Settings Utility..... | 114 |
| Filtering Alerts | 114 |
| Filtering Alerts Using iDRAC7 Web Interface..... | 114 |
| Filtering Alerts Using RACADM..... | 115 |
| Setting Event Alerts..... | 115 |
| Setting Event Alerts Using Web Interface..... | 115 |
| Setting Event Alerts Using RACADM..... | 115 |
| Setting Event Actions..... | 115 |
| Setting Event Actions Using Web Interface..... | 115 |
| Setting Event Actions Using RACADM..... | 116 |
| Configuring E-mail Alert, SNMP Trap, or IPMI Trap Settings..... | 116 |
| Configuring IP Alert Destinations..... | 116 |
| Configuring E-Mail Alert Settings..... | 117 |
| Alerts Message IDs..... | 119 |
| 10 Managing Logs..... | 123 |
| Viewing System Event Log..... | 123 |
| Viewing System Event Log Using Web Interface..... | 123 |
| Viewing System Event Log Using RACADM..... | 123 |
| Viewing Lifecycle Log | 124 |
| Viewing Lifecycle Log Using Web Interface..... | 124 |
| Viewing Lifecycle Log Using RACADM..... | 125 |
| Adding Work Notes..... | 125 |
| Configuring Remote System Logging..... | 125 |
| Configuring Remote System Logging Using Web Interface..... | 125 |
| Configuring Remote System Logging Using RACADM..... | 125 |
| 11 Monitoring and Managing Power..... | 127 |
| Monitoring Power..... | 127 |
| Monitoring Power Using Web Interface..... | 127 |
| Monitoring Power Using RACADM..... | 127 |
| Executing Power Control Operations..... | 128 |
| Executing Power Control Operations Using Web Interface..... | 128 |

| | |
|---|------------|
| Executing Power Control Operations Using RACADM..... | 128 |
| Power Capping..... | 128 |
| Power Capping in Blade Servers..... | 128 |
| Viewing and Configuring Power Cap Policy..... | 129 |
| Configuring Power Supply Options..... | 130 |
| Configuring Power Supply Options Using Web Interface..... | 130 |
| Configuring Power Supply Options Using RACADM..... | 130 |
| Configuring Power Supply Options Using iDRAC Setting Utility..... | 131 |
| Enabling or Disabling Power Button..... | 131 |
| 12 Configuring and Using Virtual Console..... | 133 |
| Supported Screen Resolutions and Refresh Rates..... | 133 |
| Configuring Web Browsers to Use Virtual Console..... | 134 |
| Configuring Web Browser to Use Java Plug-in..... | 134 |
| Configuring IE to Use ActiveX Plug-in..... | 134 |
| Importing CA Certificates to Management Station..... | 136 |
| Configuring Virtual Console..... | 137 |
| Configuring Virtual Console Using Web Interface..... | 137 |
| Configuring Virtual Console Using RACADM..... | 137 |
| Previewing Virtual Console..... | 137 |
| Launching Virtual Console..... | 138 |
| Launching Virtual Console Using Web Interface..... | 138 |
| Launching Virtual Console Using URL..... | 139 |
| Using Virtual Console Viewer..... | 139 |
| Synchronizing Mouse Pointers..... | 139 |
| Passing All Keystrokes Through Virtual Console..... | 140 |
| 13 Managing Virtual Media..... | 143 |
| Supported Drives and Devices..... | 144 |
| Configuring Virtual Media..... | 144 |
| Configuring Virtual Media Using iDRAC7 Web Interface..... | 144 |
| Configuring Virtual Media Using RACADM..... | 144 |
| Configuring Virtual Media Using iDRAC Settings Utility..... | 144 |
| Attached Media State and System Response..... | 145 |
| Accessing Virtual Media..... | 145 |
| Launching Virtual Media Using Virtual Console..... | 145 |
| Launching Virtual Media Without Using Virtual Console..... | 146 |
| Adding Virtual Media Images..... | 146 |
| Removing Virtual Media Images..... | 146 |
| Viewing Virtual Device Details..... | 147 |
| Resetting USB..... | 147 |
| Mapping Virtual Drive..... | 147 |

| | |
|---|------------|
| Unmapping Virtual Drive..... | 148 |
| Setting Boot Order Through BIOS..... | 148 |
| Enabling Boot Once for Virtual Media..... | 148 |
| 14 Installing and Using VMCLI Utility..... | 151 |
| Installing VMCLI..... | 151 |
| Running VMCLI Utility..... | 151 |
| VMCLI Syntax..... | 151 |
| VMCLI Commands to Access Virtual Media | 152 |
| VMCLI Operating System Shell Options | 153 |
| 15 Managing vFlash SD Card..... | 155 |
| Configuring vFlash SD Card..... | 155 |
| Viewing vFlash SD Card Properties..... | 155 |
| Enabling or Disabling vFlash Functionality..... | 156 |
| Initializing vFlash SD Card..... | 157 |
| Getting the Last Status Using RACADM..... | 157 |
| Managing vFlash Partitions..... | 158 |
| Creating an Empty Partition..... | 158 |
| Creating a Partition Using an Image File..... | 159 |
| Formatting a Partition..... | 160 |
| Viewing Available Partitions..... | 160 |
| Modifying a Partition..... | 161 |
| Attaching or Detaching Partitions..... | 162 |
| Deleting Existing Partitions..... | 163 |
| Downloading Partition Contents..... | 163 |
| Booting to a Partition..... | 164 |
| 16 Using SMCLP..... | 165 |
| System Management Capabilities Using SMCLP..... | 165 |
| Running SMCLP Commands..... | 165 |
| iDRAC7 SMCLP Syntax..... | 166 |
| Navigating the MAP Address Space..... | 168 |
| Using Show Verb..... | 169 |
| Using the -display Option..... | 169 |
| Using the -level Option..... | 169 |
| Using the -output Option..... | 169 |
| Usage Examples..... | 169 |
| Server Power Management..... | 169 |
| SEL Management..... | 170 |
| MAP Target Navigation..... | 171 |

| | |
|--|------------|
| 17 Deploying Operating Systems..... | 173 |
| Deploying Operating System Using VMCLI | 173 |
| Deploying Operating System Using Remote File Share..... | 174 |
| Managing Remote File Share..... | 175 |
| Configuring Remote File Share Using Web Interface..... | 175 |
| Configuring Remote File Share Using RACADM..... | 176 |
| Deploying Operating System Using Virtual Media..... | 176 |
| Installing Operating System From Multiple Disks..... | 177 |
| Deploying Embedded Operating System On SD Card..... | 177 |
| Enabling SD Module and Redundancy in BIOS..... | 177 |
| | |
| 18 Troubleshooting Managed System Using iDRAC7..... | 179 |
| Using Diagnostic Console..... | 179 |
| Viewing Post Codes..... | 179 |
| Viewing Boot and Crash Capture Videos..... | 180 |
| Viewing Logs..... | 180 |
| Viewing Last System Crash Screen..... | 180 |
| Viewing Front Panel Status..... | 180 |
| Viewing System Front Panel LCD Status..... | 181 |
| Viewing System Front Panel LED Status..... | 181 |
| Hardware Trouble Indicators..... | 181 |
| Viewing System Health..... | 182 |
| Checking Server Status Screen for Error Messages..... | 182 |
| Restarting iDRAC7..... | 182 |
| Resetting iDRAC7 Using iDRAC7 Web Interface..... | 183 |
| Resetting iDRAC7 Using RACADM..... | 183 |
| Resetting iDRAC7 to Factory Default Settings..... | 183 |
| | |
| 19 Frequently Asked Questions..... | 185 |
| System Event Log..... | 185 |
| Network Security..... | 185 |
| Active Directory..... | 186 |
| Single Sign-On..... | 188 |
| Smart Card Login..... | 189 |
| Virtual Console..... | 189 |
| Virtual Media..... | 192 |
| vFlash SD Card..... | 194 |
| SNMP Authentication..... | 194 |
| Storage Devices..... | 195 |
| RACADM..... | 195 |
| Miscellaneous..... | 196 |

| | |
|--|------------|
| 20 Use Case Scenarios..... | 199 |
| Troubleshooting An Inaccessible Managed System..... | 199 |
| Obtaining System Information and Assess system Health..... | 199 |
| Setting Up Alerts and Configuring E-mail Alerts..... | 199 |
| Viewing and Exporting Lifecycle Log and System Event Log..... | 200 |
| Interfaces to Update iDRAC Firmware..... | 200 |
| Performing Graceful Shutdown..... | 200 |
| Creating New Administrator User Account..... | 200 |
| Launching Server's Remote Console and Mounting a USB Drive..... | 201 |
| Installing Bare Metal OS Using Attached Virtual Media and Remote File Share..... | 201 |
| Managing Rack Density..... | 201 |
| Installing New Electronic License..... | 201 |

Overview

The Integrated Dell Remote Access Controller 7 (iDRAC7) is designed to make server administrators more productive and improve the overall availability of Dell servers. iDRAC7 alerts administrators to server issues, helps them perform remote server management, and reduces the need for physical access to the server.

iDRAC7 with Lifecycle controller technology is part of a larger datacenter solution that helps keep business critical applications and workloads available at all times. The technology allows administrators to deploy, monitor, manage, configure, update, troubleshoot and remediate Dell servers from any location, and without the use of agents. It accomplishes this regardless of operating system or hypervisor presence or state.

Several products work in conjunction with the iDRAC7 and Lifecycle controller to simplify and streamline IT operations, such as:

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

The iDRAC7 is available in the following variants:

- Basic Management with IPMI
- iDRAC7 Express
- iDRAC7 Express for Blades
- iDRAC7 Enterprise

For more information, see the *iDRAC7 Overview and Feature Guide* available at support.dell.com.

Benefits of Using iDRAC7 with Lifecycle Controller

The benefits include:

- **Increased Availability** — Early notification of potential or actual failures that help prevent a server failure or reduce recovery time after failure.
- **Improved Productivity and Lower Total Cost of Ownership (TCO)** — Extending the reach of administrators to larger numbers of distant servers can make IT staff more productive while driving down operational costs such as travel.
- **Secure Environment** — By providing secure access to remote servers, administrators can perform critical management functions while maintaining server and network security.
- **Enhanced Embedded Management through Lifecycle Controller** – Lifecycle Controller provides deployment and simplified serviceability through Lifecycle Controller GUI for local deployment and Remote Services (WS-Management) interfaces for remote deployment integrated with Dell OpenManage Essentials and partner consoles.

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

Key Features

The key features in iDRAC7 include:

Inventory and Monitoring

- View managed server health.
- Inventory and monitor network adapters and storage subsystem without any operating system agents.
- View system inventory.
- View sensor information.
- Monitor and control power usage.
- For blade servers: launch Chassis Management Controller (CMC) Web interface, view CMC information, and WWN/MAC addresses.



NOTE: CMC provides access to iDRAC7 through the M1000E Chassis LCD panel and local console connections. For more information, see *Chassis Management Controller User's Guide* available at support.dell.com/manuals.

Deployment

- Manage vFlash SD card partitions.
- Configure front panel display settings.
- Launch Lifecycle Controller, which allows you to configure and update BIOS and supported network and storage adapters.
- Manage iDRAC7 network settings.
- Configure and use virtual console and virtual media.
- Deploy operating systems using remote file share, virtual media, and VMCLI.
- Enable auto-discovery.

Update

- Manage iDRAC7 licenses.
- Update or rollback iDRAC7 firmware.

Maintenance and Troubleshooting


- Perform power related operations and monitor power consumption.
- No dependency on Server Administrator for generation of alerts.
- Log event data: Lifecycle Log and RAC logs.
- Set e-mail, IPMI, or SNMP alerts for events and improved e-mail alert notification.
- Capture last system crash image.
- View boot and crash capture videos.

Secure Connectivity

Securing access to critical network resources is a priority. iDRAC7 implements a range of security features that includes:

- Secure Sockets Layer (SSL).
- Signed firmware updates.
- User authentication through Microsoft Active Directory, generic LDAP Directory Service, or locally administered user IDs and passwords.

- Two-factor authentication using the Smart-Card logon feature. The two-factor authentication is based on the physical smart card and the smart card PIN.
- Single Sign-on and Public Key Authentication.
- Role-based authorization, to configure specific privileges for each user.
- User ID and password configuration.
- SMCLP and Web interfaces that support 128-bit and 40-bit encryption (for countries where 128 bit is not acceptable), using the SSL 3.0 standard.
- Session time-out configuration (in seconds).
- Configurable IP ports (for HTTP, HTTPS, SSH, Telnet, Virtual Console and Virtual Media).

 **NOTE:** Telnet does not support SSL encryption and is disabled by default.

- Secure Shell (SSH) that uses an encrypted transport layer for higher security.
- Login failure limits per IP address, with login blocking from that IP address when the limit is exceeded.
- Limited IP address range for clients connecting to iDRAC7.
- Dedicated Gigabit Ethernet adapter on rack and tower servers with Enterprise license.

Managing Licenses

iDRAC7 features are available based on the license (Basic Management, iDRAC7 Express, iDRAC7 Express for Blades, or iDRAC7 Enterprise) purchased. Only licensed features are available in the interfaces that allow you to configure or use iDRAC7. For example, iDRAC7 Web interface, RACADM, WS-MAN, OpenManage Server Administrator, and so on. Some features, such as dedicated NIC or vFlash requires iDRAC ports card, which is optional on 200-500 server series.

iDRAC7 license management and firmware update functionality is always available through iDRAC7 Web interface and RACADM.

Types of Licenses

The types of licenses offered are:

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


Acquiring Licenses

Use any of the following methods to acquire the licenses:

- E-mail — License is attached to an e-mail that is sent after requesting it from the technical support center.
- Self-service portal — A link to the Self-Service Portal is available from iDRAC7. Click this link to open the licensing Self-Service Portal on the internet from where you can purchase licenses. For more information, see the online help for the self-service portal page.
- Point-of-sale — License is acquired while placing the order for a system.


License Operations

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


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

You can perform the following licensing operations using iDRAC7, RACADM, WS-MAN, and Lifecycle Controller-Remote Services for one-to-one license management, and Dell License Manager for one-to-many license management:

- View — View the current license information.
- Import — After acquiring the license, store the license in a local storage and import it into iDRAC7 using one of the supported interfaces. The license is imported if it passes the validation checks.

 **NOTE:** For a few features, a system restart is required to enable the features.

- Export — Export the installed license into an external storage device for backup or to reinstall it again after a part or motherboard replacement. The file name and format of the exported license is **<EntitlementID>.xml**.
- Delete — Delete the license that is assigned to a component if the component is missing. After the license is deleted, it is not stored in iDRAC7 and the base product functions are enabled.
- Replace — Replace the license to extend an evaluation license, change a license type such as an evaluation license with a purchased license, or extend an expired license.
 - An evaluation license may be replaced with an upgraded evaluation license or with a purchased license.
 - A purchased license may be replaced with an updated license or with an upgraded license.
- Learn More — Learn more about an installed license, or the licenses available for a component installed in the server.

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

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

License Component State or Condition and Available Operations

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

Table 1. License Operations Based on State and Condition

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

Managing Licenses Using iDRAC7 Web Interface

To manage the licenses using the iDRAC7 Web interface, go to **Overview Server Licenses**.

The **Licensing** page displays the licenses that are associated to devices, or the licenses that are installed but the device is not present in the system. For more information on importing, exporting, deleting, or replacing a license, see the *iDRAC7 Online Help*.

Managing Licenses Using RACADM

To manage licenses using RACADM, use the **license** subcommand. For more information, see the *RACADM Command Line Reference Guide for iDRAC7 and CMC* available at support.dell.com/manuals.

See also:

- Managing Licenses
- Types of Licenses
- Acquiring Licenses
- Licensable Features In iDRAC7

Licensable Features In iDRAC7

The following table provides the iDRAC7 features that are enabled based on the license purchased.

Table 2. iDRAC7 Licensable Features

| Feature | Base Management with IPMI | iDRAC7 Express | iDRAC7 Express for Blades | iDRAC7 Enterprise |
|--|---------------------------|----------------|---------------------------|-------------------|
| Interface and Standards Support | | | | |
| IPMI 2.0 | Yes | Yes | Yes | Yes |
| Web-based interface [1] | No | Yes | Yes | Yes |
| SNMP | No | Yes | Yes | Yes |
| WS-MAN | Yes | Yes | Yes | Yes |
| SMASH-CLP (SSH) | No | Yes | Yes | Yes |
| RACADM (SSH, Local, and Remote) [1] | No | Yes | Yes | Yes |
| Telnet | No | Yes | Yes | Yes |
| Connectivity | | | | |
| Shared or Failover Network Modes (rack and tower servers only) | Yes | Yes | No | Yes |
| Dedicated NIC | No | No | Yes [2] | Yes [2,6] |
| DNS | Yes | Yes | Yes | Yes |
| VLAN Tagging | Yes | Yes | Yes | Yes |
| IPv4 | Yes | Yes | Yes | Yes |
| IPv6 | No | Yes | Yes | Yes |
| Dynamic DNS | No | Yes | Yes | Yes |
| Security and Authentication | | | | |
| Role-based authority | Yes | Yes | Yes | Yes |
| Local Users | Yes | Yes | Yes | Yes |
| Directory Services (Active Directory and Generic LDAP) | No | No | No | Yes |
| SSL Encryption | Yes | Yes | Yes | Yes |
| Two-factor Authentication [3] | No | No | No | Yes |
| Single Sign-On (SSO) | No | No | No | Yes |
| PK Authentication (for SSH) | No | No | No | Yes |

| Feature | Base Management with IPMI | iDRAC7 Express | iDRAC7 Express for Blades | iDRAC7 Enterprise |
|--|---------------------------|----------------|---------------------------|-------------------|
| Security Lockout | No | Yes | Yes | Yes |
| Remote Management and Remediation | | | | |
| Embedded Diagnostic | Yes | Yes | Yes | Yes |
| Serial Over LAN (with proxy) | Yes | Yes | Yes | Yes |
| Serial Over LAN (no proxy) | No | Yes | Yes | Yes |
| Crash Screen capture | No | Yes | Yes | Yes |
| Crash Video Capture | No | No | No | Yes |
| Boot Capture | No | No | No | Yes |
| Virtual Media [4] | No | No | Yes | Yes |
| Virtual Console [4] | No | No | Yes [5] | Yes |
| Console Collaboration [4] | No | No | No | Yes |
| Virtual Folder | No | No | No | Yes |
| Virtual Console chat | No | No | No | Yes |
| Remote File Share | No | No | No | Yes |
| vFlash [6] | No | No | No | Yes |
| vFlash Partitions [6] | No | No | No | Yes |
| Auto-discovery | No | Yes | Yes | Yes |
| Monitoring and Power | | | | |
| Sensor monitoring and alerting | Yes | Yes | Yes | Yes |
| Device Monitoring | No | Yes | Yes | Yes |
| Storage Monitoring | No | Yes | Yes | Yes |
| E-mail Alerts | No | Yes | Yes | Yes |
| Historical Power counters | Yes | Yes | Yes | Yes |
| Power capping | No | No | No | Yes |
| Real-time power monitoring | Yes | Yes | Yes | Yes |
| Real-time power graphing | No | Yes | Yes | Yes |
| Logging | | | | |
| System Event Log | Yes | Yes | Yes | Yes |
| RAC Log [7] | No | Yes | Yes | Yes |
| Trace Log [7] | No | Yes | Yes | Yes |
| Remote Syslog | No | No | No | Yes |

[1] iDRAC7 license management and firmware update functionality is always available through iDRAC7 Web interface and RACADM.

[2] All blade servers use dedicated NIC for iDRAC7 at all times, but the speed is limited to 100 Mbps. GIGABYTE Ethernet card does not work on blade servers due to limitations of the chassis, but works on rack and tower servers with Enterprise license. Shared LOM is not enabled for blade servers.

[3] Two-factor authentication is available through Active-X and therefore only supports Internet Explorer.

[4] Virtual Console and Virtual Media are available through both Java and Active-X plug-ins.

[5] Single user Virtual Console with remote launch.

[6] On some systems the optional iDRAC7 ports card is required.

[7] RAC and trace logs are available in Base version through WS-MAN.

Interfaces and Protocols to Access iDRAC7

The following table lists the interfaces to access iDRAC7.




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

Table 3. Interfaces and Protocols to Access iDRAC7

| Interface or Protocol | Description |
|--|---|
| iDRAC Settings Utility | <p>Use the iDRAC Settings utility to perform pre-OS operations. It has a subset of the features that are available in iDRAC7 Web interface along with other features.</p> <p>To access iDRAC Settings utility, press <F2> during boot and then click iDRAC Settings on the System Setup Main Menu page.</p> |
| iDRAC7 Web Interface | <p>Use the iDRAC7 Web interface to manage iDRAC7 and monitor the managed system. The browser connects to the Web server through the HTTPS port. Data streams are encrypted using 128-bit SSL to provide privacy and integrity. Any connection to the HTTP port is redirected to HTTPS. Administrators can upload their own SSL certificate through an SSL CSR generation process to secure the Web server. The default HTTP and HTTPS ports can be changed. The user access is based on user privileges.</p> |
| RACADM | <p>Use this command line utility to perform iDRAC7 and server management. You can use RACADM locally and remotely.</p> <ul style="list-style-type: none">• Local RACADM command line interface runs on the managed systems that have Server Administrator installed. Local RACADM communicates with iDRAC7 through its in-band IPMI host interface. Since it is installed on the local managed system, users are required to log in to the operating system to run this utility. A user must have a full administrator privilege or be a root user to use this utility.• Remote RACADM is a client utility that runs on a management station. It uses the out-of-band network interface to run RACADM commands on the managed system and uses the HTTPs channel. The <code>-r</code> option runs the RACADM command over a network.• Firmware RACADM is accessible by logging in to iDRAC7 using SSH or telnet. You can run the firmware RACADM commands without specifying the iDRAC7 IP, user name, or password.• You do not have to specify the iDRAC7 IP, user name, or password to run the firmware RACADM commands. After you enter the RACADM prompt, you can directly run the commands without the <code>racadm</code> prefix. |
| Server LCD Panel/ Chassis LCD Panel | <p>Use the LCD on the server front panel to:</p> <ul style="list-style-type: none">• View alerts, iDRAC7 IP or MAC address, user programmable strings.• Set DHCP• Configure iDRAC7 static IP settings. <p>For blade servers, the LCD is on the chassis front panel and is shared between all the blades.</p> <p>To reset iDRAC without rebooting the server, press and hold the System Identification  button for 16 seconds.</p> |
| CMC Web Interface | <p>In addition to monitoring and managing the chassis, use the CMC Web interface to:</p> <ul style="list-style-type: none">• View the status of a managed system |

| Interface or Protocol | Description |
|-----------------------|--|
| | <ul style="list-style-type: none"> • Update iDRAC7 firmware • Configure iDRAC7 network settings • Log in to iDRAC7 Web interface • Start, stop, or reset the managed system • Update BIOS, PERC, and supported network adapters |
| Lifecycle Controller | Use Lifecycle Controller to perform iDRAC7 configurations. To access Lifecycle Controller, press <F10> during boot and go to System Setup → Advanced Hardware Configuration → iDRAC Settings . For more information, see <i>Lifecycle Controller User's Guide</i> available at support.dell.com/manuals . |
| Telnet | Use Telnet to access iDRAC7 where you can run RACADM and SMCLP commands. For details about RACADM, see <i>RACADM Command Line Reference Guide for iDRAC7 and CMC</i> available at support.dell.com/manuals . For details about SMCLP, see Using SMCLP .  NOTE: Telnet is not a secure protocol and is disabled by default. Telnet transmits all data, including passwords in plain text. When transmitting sensitive information, use the SSH interface. |
| SSH | Use SSH to run RACADM and SMCLP commands. It provides the same capabilities as the Telnet console using an encrypted transport layer for higher security. The SSH service is enabled by default on iDRAC7. The SSH service can be disabled in iDRAC7. iDRAC7 only supports SSH version 2 with DSA and the RSA host key algorithm. A unique 1024-bit DSA and 1024-bit RSA host key is generated when you power-up iDRAC7 for the first time. |
| IPMITool | Use the IPMITool to access the remote system's basic management features through iDRAC7. The interface includes local IPMI, IPMI over LAN, IPMI over Serial, and Serial over LAN. For more information on IPMITool, see the <i>Dell OpenManage Baseboard Management Controller Utilities User's Guide</i> at support.dell.com/manuals . |
| VMCLI | Use the Virtual Media Command Line Interface (VMCLI) to access a remote media through the management station and deploy operating systems on multiple managed systems. |
| SMCLP | Use Server Management Workgroup Server Management-Command Line Protocol (SMCLP) to perform systems management tasks. This is available through SSH or Telnet. For more information about SMCLP, see Using SMCLP . |
| WS-MAN | The LC-Remote Services is based on the WS-Management protocol to do one-to-many systems management tasks. You must use WS-MAN client such as WinRM client (Windows) or the OpenWSMAN client (Linux) to use the LC-Remote Services functionality. You can also use Power Shell and Python to script to the WS-MAN interface. Web Services for Management (WS-Management) is a Simple Object Access Protocol (SOAP)-based protocol used for systems management. iDRAC7 uses WS-Management to convey Distributed Management Task Force (DMTF) Common Information Model (CIM)-based management information. The CIM information defines the semantics and information types that can be modified in a managed system. The data available through WS-Management is provided by iDRAC7 instrumentation interface mapped to the DMTF profiles and extension profiles. For more information, see the following: <ul style="list-style-type: none"> • Lifecycle Controller-Remote Services User's Guide available at support.dell.com/manuals. • Lifecycle Controller Integration Best Practices Guide available at support.dell.com/manuals. • Lifecycle Controller page on Dell TechCenter — delltechcenter.com/page/Lifecycle+Controller • Lifecycle Controller WS-Management Script Center — delltechcenter.com/page/Scripting+the+Dell+Lifecycle+Controller |

- MOFs and Profiles — delltechcenter.com/page/DCIM.Library
- DTMF Web site — dmtf.org/standards/profiles/

iDRAC7 Port Information

The following information ports are required to remotely access iDRAC7 through firewalls. These are the ports iDRAC7 listens to for connections.

Table 4. Ports iDRAC7 Listens for Connections

| Port Number | Function |
|-------------|---|
| 22* | SSH |
| 23* | Telnet |
| 80* | HTTP |
| 443* | HTTPS |
| 623 | RMCP/RMCP+ |
| 5900* | Virtual Console keyboard and mouse redirection, Virtual Media, Virtual Folders, and Remote File Share |

* Configurable port

The following table lists the ports that iDRAC7 uses as a client.

Table 5. Ports iDRAC7 Uses as Client

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

Other Documents You May Need

In addition to this guide, the following documents available on the Dell Support website at support.dell.com/manuals provides additional information about the setup and operation of iDRAC7 in your system. On the **Manuals** page, click **Software** → **Systems Management**. Click on the appropriate product link on the right-side to access the documents.

- The *iDRAC7 Online Help* provides detailed information about the fields available on the iDRAC7 Web interface and the descriptions for the same. You can access the online help after you install iDRAC7.
- The *RACADM Command Line Reference Guide for iDRAC7 and CMC* provides information about the RACADM sub-commands, supported interfaces, and iDRAC7 property database groups and object definitions.

- The *Systems Management Overview Guide* provides brief information about the various software available to perform systems management tasks.
- The *Dell Lifecycle Controller User's Guide and Remote Services User Guide* provide information on using Lifecycle Controller and Remote Services, respectively.
- The Dell Remote Access Configuration Tool User's Guide provides information on how to use the tool to discover iDRAC IP addresses in your network and perform one-to-many firmware updates and active directory configurations for the discovered IP addresses.
- The *Dell Systems Software Support Matrix* provides information about the various Dell systems, the operating systems supported by these systems, and the Dell OpenManage components that can be installed on these systems.
- The *Dell OpenManage Server Administrator Installation Guide* contains instructions to help you install Dell OpenManage Server Administrator.
- The *Dell OpenManage Management Station Software Installation Guide* contains instructions to help you install Dell OpenManage management station software that includes Baseboard Management Utility, DRAC Tools, and Active Directory Snap-In.
- The *Dell OpenManage Baseboard Management Controller Management Utilities User's Guide* has information about the IPMI interface.
- Readme files may be included to provide last-minute updates to the system or documentation or advanced technical reference material intended for experienced users or technicians.
- The *Glossary* provides information about the terms used in this document.

The following system documents are available to provide more information:

- The *iDRAC7 Overview and Feature Guide* provides information about iDRAC7, its licensable features, and license upgrade options.
- The safety instructions that came with your system provide important safety and regulatory information. For additional regulatory information, see the Regulatory Compliance home page at dell.com/regulatory_compliance. Warranty information may be included within this document or as a separate document.
- The *Rack Installation Instructions* included with your rack solution describe how to install your system into a rack.
- The *Getting Started Guide* provides an overview of system features, setting up your system, and technical specifications.
- The *Owner's Manual* provides information about system features and describes how to troubleshoot the system and install or replace system components.

Contacting Dell




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

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

1. Visit support.dell.com.
2. Select your support category.
3. If you are not a U.S. customer, select your country code at the bottom of the support.dell.com page, or select **All** to see more choices.
4. Select the appropriate service or support link based on your need.

Logging In to iDRAC7

You can log in to iDRAC7 as an iDRAC7 user, as a Microsoft Active Directory user, or as an LDAP user. The default user name and password is root and calvin, respectively. You can also log in using Single Sign-On or Smart Card.

 **NOTE:** You must have Login to iDRAC privilege to log in to iDRAC7.

Related Links


[Logging Into iDRAC7 as Local User, Active Directory User, or LDAP User](#)


[Logging Into iDRAC7 Using Smart Card](#)

[Logging Into iDRAC7 Using Single Sign-on](#)

Logging Into iDRAC7 as Local User, Active Directory User, or LDAP User


Before you log in to iDRAC7 using the Web interface, make sure that you have configured a supported Web browser (Internet Explorer or Firefox) is configured and the user account is created with the required privileges.

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

 **NOTE:** In addition to Active Directory, openLDAP, openDS, Novell eDir, and Fedora based directory services are supported. "<" and ">" characters are not allowed in the user name.

To log into iDRAC7 as local user, Active Directory user, or LDAP user:

1. Open a supported Web browser.
2. In the **Address** field, type `https://[iDRAC7-IP-address]` and press **Enter**.

 **NOTE:** If the default HTTPS port number (port 443) was changed, enter: `https://[iDRAC7-IP-address]:[port-number]` where, `[iDRAC7-IP-address]` is the iDRAC7 IPv4 or IPv6 address and `[port-number]` is the HTTPS port number.

The **Login** page is displayed.

3. For a local user:
 - In the **Username** and **Password** fields, enter your iDRAC7 user name and password.
 - From the **Domain** drop-down menu, select **This iDRAC**.
4. For an Active Directory user, in the **Username** and **Password** fields, enter the Active Directory user name and password. If you have specified the domain name as a part of the username, select **This iDRAC** from the drop-down menu. The format of the user name can be: `<domain>\<username>`, `<domain>/<username>`, or `<user>@<domain>`. For example, `dell.com\john_doe`, or `JOHN_DOE@DELL.COM`.
If the domain is not specified in the user name, select the Active Directory domain from the **Domain** drop-down menu.
5. For an LDAP user, in the **Username** and **Password** fields, enter your LDAP user name and password. Domain name is not required for LDAP login. By default, **This iDRAC** is selected in the drop-down menu.
6. Click **Submit**. You are logged into iDRAC7 with the required user privileges.

Related Links

- [Configuring User Accounts and Privileges](#)
- [Configuring Supported Web Browsers](#)

Logging Into iDRAC7 Using Smart Card

You can log in to iDRAC7 using a smart card. Smart cards provide Two Factor Authentication (TFA) that provide two-layers of security:

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

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

Related Links


- [Logging Into iDRAC7 as a Local User Using Smart Card](#)
- [Logging Into iDRAC7 as an Active Directory User Using Smart Card](#)

Logging Into iDRAC7 as a Local User Using Smart Card

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


- Upload user smart card certificate and the trusted Certificate Authority (CA) certificate to iDRAC7
- Enable smart card logon.

The iDRAC7 Web interface displays the smart card logon page for users who are configured to use the smart card.


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

To log in to iDRAC7 as a local user using smart card:

1. Access the iDRAC7 Web interface using the link `https://[IP address]`.
The **iDRAC7 Login** page is displayed prompting you to insert the smart card.

 **NOTE:** If the default HTTPS port number (port 443) has been changed, type: `https://[IP address]:[port number]` where, `[IP address]` is the IP address for the iDRAC7 and `[port number]` is the HTTPS port number.

2. Insert the Smart Card into the reader and click **Login**.
A prompt is displayed for the Smart Card's PIN. A password is not required.
3. Enter the Smart Card PIN for local Smart Card users.
You are logged into the iDRAC7.

 **NOTE:** If you are a local user for whom **Enable CRL check for Smart Card Logon** is enabled, iDRAC7 attempts to download the CRL and checks the CRL for the user's certificate. The login fails if the certificate is listed as revoked in the CRL or if the CRL cannot be downloaded for some reason.

Related Links

- [Enabling or Disabling Smart Card Login](#)
- [Configuring iDRAC7 Smart Card Login for Local Users](#)


Logging Into iDRAC7 as an Active Directory User Using Smart Card

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

- Upload a Trusted Certificate Authority (CA) certificate (CA-signed Active Directory certificate) to iDRAC7.
- Configure the DNS server.
- Enable Active Directory login.
- Enable Smart Card login.

To log in to iDRAC7 as an Active Directory user using smart card:

1. Log in to iDRAC7 using the link `https://[IP address]`.
The **iDRAC7 Login** page is displayed prompting you to insert the Smart Card.

 **NOTE:** If the default HTTPS port number (port 443) is changed, type: `https://[IP address]:[port number]` where, `[IP address]` is the iDRAC7 IP address and `[port number]` is the HTTPS port number.

2. Insert the Smart Card and click **Login**.
The **PIN** pop-up is displayed.
3. Enter the PIN and click **Submit**.
You are logged in to iDRAC7 with your Active Directory credentials.

 **NOTE:**

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

Related Links

- [Enabling or Disabling Smart Card Login](#)
- [Configuring iDRAC7 Smart Card Login for Active Directory Users](#)

Logging Into iDRAC7 Using Single Sign-on

When Single Sign-On (SSO) is enabled, you can log in to iDRAC7 without entering your domain user authentication credentials, such as user name and password.

Related Links

- [Configuring iDRAC7 SSO Login for Active Directory Users](#)


Logging into iDRAC7 SSO Using iDRAC7 Web Interface


Before logging into iDRAC7 using Single Sign-on, make sure that:

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

To login to iDRAC7 using Web interface:

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

 **NOTE:** If the default HTTPS port number (port 443) has been changed, type: `https://[FQDN address]:[port number]` where, `[FQDN address]` is the iDRAC7 FQDN (iDRAC7dnsname.domain.name) and `[port number]` is the HTTPS port number.

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

iDRAC7 logs you in with appropriate Microsoft Active Directory privileges, using your credentials that were cached in the operating system when you logged in using a valid Active Directory account.

Logging In to iDRAC7 SSO Using iDRAC7 Web Interface

Using the SSO feature, you can launch iDRAC7 Web interface from CMC Web interface. A CMC user has the CMC user privileges when launching iDRAC7 from CMC. If the user account is present in CMC and not in iDRAC, the user can still launch iDRAC7 from CMC.

If iDRAC7 network LAN is disabled (LAN Enabled = No), SSO is not available.

If the server is removed from the chassis, iDRAC7 IP address is changed, or there is a problem in iDRAC7 network connection, the option to Launch iDRAC7 is grayed-out in the CMC Web interface.


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

Accessing iDRAC7 Using Remote RACADM

You can use remote RACADM to access iDRAC7 using RACADM utility.

For more information, see the *RACADM Reference Guide for iDRAC7 and CMC* available at support.dell.com/manuals.

If the management station has not stored the iDRAC7's SSL certificate in its default certificate storage, a warning message is displayed when you run the RACADM command. However, the command is executed successfully.

 **NOTE:** The iDRAC7 certificate is the certificate iDRAC7 sends to the RACADM client to establish the secure session. This certificate is either issued by a CA or self-signed. In either case, if the management station does not recognize the CA or signing authority, a warning is displayed.

Related Links

[Validating CA Certificate To Use Remote RACADM on Linux](#)

Validating CA Certificate To Use Remote RACADM on Linux

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

To validate the certificate for using remote RACADM:

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

```
openssl x509 -inform pem -in [yourdownloadedderformatcert.crt] -outform pem -out [outcertfileinpemformat.pem] -text
```
2. Find the location of the default CA certificate bundle on the management station. For example, for RHEL5 64-bit, it is **/etc/pki/tls/cert.pem**.
3. Append the PEM formatted CA certificate to the management station CA certificate.
For example, use the `cat` command: `- cat testcacert.pem >> cert.pem`
4. Generate and upload the server certificate to iDRAC7.

Accessing iDRAC7 Using Local RACADM

For information to access iDRAC7 using local RACADM, see the *RACADM Command Line Reference Guide for iDRAC7 and CMC* available at support.dell.com/manuals.

Accessing iDRAC7 Using Firmware RACADM

You can use SSH or Telnet interfaces to access iDRAC7 and run firmware RACADM commands. For more information, see the *RACADM Command Line Reference Guide for iDRAC7 and CMC* available at support.dell.com/manuals.

Accessing iDRAC7 Using SMCLP

SMCLP is the default command line prompt when you log in to iDRAC7 using Telnet or SSH. For more information, see [Using SMCLP](#).

Logging in to iDRAC7 Using Public Key Authentication

You can log into the iDRAC7 over SSH without entering a password. You can also send a single RACADM command as a command line argument to the SSH application. The command line options behave similar to remote RACADM since the session ends after the command is completed.

For example:

Logging in:

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

or

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

where `IP_address` is the IP address of the iDRAC7.

Sending RACADM commands:

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

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

Related Links

[Using Public Key Authentication For SSH](#)

Multiple iDRAC7 Sessions


The following table provides the list of multiple iDRAC7 sessions that are possible using the various interfaces.

Table 6. Multiple iDRAC7 Sessions

| Interface | Number of Sessions |
|-------------------------|-------------------------------------|
| iDRAC7 Web Interface | 4 |
| Remote RACADM | 4 |
| Firmware RACADM / SMCLP | SSH - 2 Telnet - 2 Serial - 1 |

Setting Up Managed System and Management Station

To perform out-of-band systems management using iDRAC7, you must configure iDRAC7 for remote accessibility, set up the management station and managed system, and configure the supported Web browsers.

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


Related Links

- [Setting Up iDRAC7 IP Address](#)
- [Setting Up Managed System](#)
- [Updating iDRAC7 Firmware](#)
- [Rolling Back iDRAC7 Firmware](#)
- [Setting Up Management Station](#)
- [Configuring Supported Web Browsers](#)

Setting Up iDRAC7 IP Address

You must configure the initial network settings based on your network infrastructure to enable the communication to and from iDRAC7. You can set up the IP address using one of the following interfaces:

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

 **NOTE:** In case of blade servers, you can configure the network setting using the Chassis LCD panel only during initial configuration of CMC. After the chassis is deployed, you cannot reconfigure iDRAC7 using the Chassis LCD panel.

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

In case of rack and tower servers, you can set up the IP address or use the default iDRAC7 IP address 192.168.0.120 to configure initial network settings, including setting up DHCP or the static IP for iDRAC7.

In case of blade servers, the iDRAC7 network interface is disabled by default.

After you configure iDRAC7 IP address:

- Make sure to *change the default user name and password after setting up the iDRAC7 IP address.*
- Access it through any of the following interfaces:
 - iDRAC7 Web interface using a supported browser (Internet Explorer or Firefox)
 - Secure Shell (SSH) — Requires a client such as PuTTY on Windows. SSH is available by default in most of the Linux systems and hence does not require a client.
 - Telnet (must be enabled, since it is disabled by default)
 - IPMITool (uses IPMI command) or shell prompt (requires Dell customized installer in Windows or Linux, available from *Systems Management Documentation and Tools DVD* or support.dell.com)

Related Links

- [Setting Up iDRAC IP Using iDRAC Settings Utility](#)
- [Setting Up iDRAC7 IP Using CMC Web Interface](#)
- [Enabling Auto-discovery](#)

Setting Up iDRAC IP Using iDRAC Settings Utility

To set up the iDRAC7 IP address:

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

Related Links

- [Network Settings](#)
- [Common Settings](#)
- [IPv4 Settings](#)
- [IPv6 Settings](#)
- [IPMI Settings](#)
- [VLAN Settings](#)


Network Settings

To configure the Network Settings:




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

1. Under **Enable NIC**, select the **Enabled** option.
2. From the **NIC Selection** drop-down menu, select one of the following ports based on the network requirement:
 - **Dedicated** — Enables the remote access device to use the dedicated network interface available on the Remote Access Controller (RAC). This interface is not shared with the host operating system and routes the management traffic to a separate physical network, enabling it to be separated from the application traffic. This option implies that iDRAC's dedicated network port routes its traffic separately from the Server's LOM or NIC ports. With respect to managing network traffic, the Dedicated option allows iDRAC to be assigned an IP address from the same subnet or different subnet in comparison to the IP addresses assigned to the Host LOM or NICs.

 **NOTE:** The option is available only on rack or tower systems with iDRAC7 Enterprise licence. For blades, it is available by default.

- LOM1
- LOM2
- LOM3
- LOM4

 **NOTE:** In the case of rack and tower servers, two LOM options (LOM1 and LOM2) or all four LOM options are available depending on the server model. Blade servers do not use LOM for iDRAC7 communication.


3. From the **Failover Network** drop-down menu, select one of the remaining LOMs. If a network fails, the traffic is routed through the failover network.

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

For example, to route the iDRAC7 network traffic through LOM2 when LOM1 is down, select **LOM1** for **NIC Selection** and **LOM2** for **Failover Network**.

4. Under **Auto Negotiation**, select **On** if iDRAC7 must automatically set the duplex mode and network speed. This option is available only for dedicated mode. If enabled, iDRAC7 sets the network speed to 10, 100, or 1000 Mbps based on the network speed.

5. Under **Network Speed**, select either 10 Mbps or 100 Mbps.

 **NOTE:** You cannot manually set the Network Speed to 1000 Mbps. This option is available only if **Auto Negotiation** option is enabled.

6. Under **Duplex Mode**, select **Half Duplex** or **Full Duplex** option.

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

Common Settings

If network infrastructure has DNS server, register iDRAC7 on the DNS. These are the initial settings requirements for advanced features such as Directory services—Active Directory or LDAP, Single Sign On, and smart card.

To register iDRAC7:

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

IPv4 Settings

To configure the IPv4 settings:

1. Select **Enabled** option under **Enable IPv4**.
2. Select **Enabled** option under **Enable DHCP**, so that DHCP can automatically assign the IP address, gateway, and subnet mask to iDRAC7. Else, select **Disabled** and enter the values for:
 - IP Address
 - Gateway
 - Subnet Mask
3. Optionally, enable **Use DHCP to obtain DNS server address**, so that the DHCP server can assign the **Preferred DNS Server** and **Alternate DNS Server**. Else, enter the IP addresses for **Preferred DNS Server** and **Alternate DNS Server**.

IPv6 Settings

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

To configure the IPv6 settings:

1. Select **Enabled** option under **Enable IPv6**.
2. For the DHCPv6 server to automatically assign the IP address, gateway, and subnet mask to iDRAC7, select **Enabled** option under **Enable Autoconfiguration**. If enabled, the static values are disabled. Else, proceed to the next step to configure using the static IP address.
3. In the **IP Address 1** box, enter the static IPv6 address.
4. In the **Prefix Length** box, enter a value between 0 and 128.
5. In the **Gateway** box, enter the gateway address.
6. If you are using DHCP, enable **DHCPv6 to obtain DNS Server addresses** to obtain Primary and Secondary DNS server addresses from DHCPv6 server.
7. Optionally, enable **Use DHCP to obtain DNS server address**, so that the DHCPv6 server can assign the **Preferred DNS Server** and **Alternate DNS Server**. Else, enter the IP addresses in the **Preferred DNS Server** and **Alternate DNS Server** boxes. Else:
 - In the **Preferred DNS Server** box, enter the static DNS server IPv6 address.
 - In the **Alternate DNS Server** box, enter the static alternate DNS server.

IPMI Settings

To enable the IPMI Settings:

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

VLAN Settings

You can configure iDRAC7 into the VLAN infrastructure. To configure VLAN Settings:

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

Setting Up iDRAC7 IP Using CMC Web Interface

To set up the iDRAC7 IP address using CMC Web interface:


 **NOTE:** You must have Chassis Configuration Administrator privilege to set up iDRAC7 network settings from CMC.

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

5. Click **Launch iDRAC** and go to **Overview** → **iDRAC Settings** → **Network**.

6. In the **Network** page, specify the following settings:

- Network Settings
- Common Settings
- IPV4 Settings
- IPV6 Settings
- IPMI Settings
- VLAN Settings

 **NOTE:** For more information, see iDRAC7 Online Help.

7. To save the network information, click **Apply**.

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

Enabling Auto-discovery

The auto-discovery feature allows newly installed servers to automatically discover the remote management console that hosts the provisioning server. The *provisioning server* provides custom administrative user credentials to iDRAC7, so that the unprovisioned server can be discovered and managed from the management console. For more information about auto-discovery, see the *Lifecycle Controller Remote Services User's Guide* available at support.dell.com/manuals.


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

If auto-discovery feature is not enabled on the factory-shipped system, the default administrator account (user name as root and password as calvin) is enabled. Before enabling auto-discovery, make sure to disable this administrator account.

You can enable auto-discovery using iDRAC7 Settings Utility or using Lifecycle Controller. For information on using Lifecycle Controller, see *Lifecycle Controller User's Guide* available at support.dell.com/manuals.

To enable auto-discovery using iDRAC Settings utility:

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

 **NOTE:** Specifying the provisioning server IP is optional. If it is not set, it is discovered using DHCP or DNS settings (step 7).


4. Click **Network**.
The **iDRAC Settings Network** page is displayed.

5. Enable NIC.

6. Enable IPv4.

 **NOTE:** IPv6 is not supported for auto-discovery.

7. Enable DHCP and get the domain name, DNS server address, and DNS domain name from DHCP.

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

Setting Up Management Station

A management station is a computer used for accessing iDRAC7 interfaces to remotely monitor and manage the PowerEdge server(s).

To set up the management station:

1. Install a supported operating system. For more information, see the readme.
2. Install and configure a supported Web browser (Internet Explorer or Firefox.)
3. Install the latest Java Runtime Environment (JRE) (required if Java plug-in type is used to access iDRAC7 using a Web browser).
4. From the *Dell Systems Management Tools and Documentation* DVD, install Remote RACADM and VMCLI from the SYSMGMT folder. Else, run **Setup** on the DVD to install Remote RACADM by default and other OpenManage software. For more information about RACADM, see *RACADM Command Line Reference Guide for iDRAC7 and CMC* available at support.dell.com/manuals.
5. Install the following based on the requirement:
 - Telnet
 - SSH client
 - TFTP
 - Dell OpenManage Essentials

Related Links

- [Installing and Using VMCLI Utility](#)
- [Configuring Supported Web Browsers](#)

Accessing iDRAC7 Remotely

To remotely access iDRAC7 Web interface from a management station, make sure that the management station is in the same network as iDRAC7. For example:

- Blade servers — The management station must be on the same network as CMC. For more information on isolating CMC network from the managed system's network, see *Chassis Management Controller User's Guide* available at support.dell.com/manuals.
- Rack and tower servers — Set the iDRAC7 NIC to LOM1 and make sure that the management station is on the same network as iDRAC7.

 **NOTE:** If the system is upgraded to iDRAC7 Enterprise, you can set the iDRAC7 NIC to **Dedicated**.

To access the managed system's console from a management station, use Virtual Console through iDRAC7 Web interface.

Related Links

- [Launching Virtual Console](#)
- [Network Settings](#)

Setting Up Managed System

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

- Local RACADM

- Server Administrator

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

Related Links

[Modifying Local Administrator Account Settings](#)

Modifying Local Administrator Account Settings

After setting the iDRAC7 IP address, you can modify the local administrator account settings (that is, user 2) using the iDRAC Settings utility. To do this:

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

Setting Up Managed System Location

You can specify the location details of the managed system in the data center using the iDRAC7 Web interface or iDRAC Settings utility.

Setting Up Managed System Location Using Web Interface

To specify the system location details:

1. In the iDRAC7 Web interface, go to **Overview** → **Server** → **Properties** → **Details**.
The **System Details** page is displayed.
2. Under **System Location**, enter the location details of the managed system in the data center.
For information about the options, see the *iDRAC7 Online Help*.
3. Click **Apply**. The system location details is saved in iDRAC7.

Setting Up Managed System Location Using RACADM

To specify the system location details, use the `System.Location` group objects. For more information, see the *RACADM Command Line Reference Guide for iDRAC7 and CMC* available at support.dell.com/manuals.

Setting Up Managed System Location Using iDRAC Settings Utility

To specify the system location details:

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

Optimizing System Performance and Power Consumption

You can optimize the performance, set the maximum air exhaust temperature, and fan speed of the managed system using the iDRAC Settings utility. To do this:


1. In the iDRAC Settings utility, go to **Thermal**.
The **iDRAC Settings Thermal** page is displayed.
2. Specify the thermal, user option, and fan settings.
For more information see *iDRAC Settings Online Help*.
3. Click **Back**, click **Finish**, and click **Yes**.
The thermal settings are configured.

Configuring Supported Web Browsers

If you are connecting to iDRAC7 Web interface from a management station that connects to the Internet through a proxy server, you must configure the Web browser to access the Internet from through this server.

To configure the Internet Explorer Web browser:

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

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

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

Under **Downloads**:

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

Under **Miscellaneous**:

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

Under **Scripting**:

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

Under **HTTP 1.1 settings**:

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

Under **Java (Sun)**:


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

Under **Multimedia**:

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

Under **Security**:

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

 **NOTE:** To modify the settings, it is recommended that you learn and understand the consequences. For example, if you block pop-ups, parts of iDRAC7 Web interface may not function properly.

6. Click **Apply**, and then click **OK**.
7. Click the **Connections** tab.
8. Under **Local Area Network (LAN) settings**, click **LAN Settings**.
9. If the **Use a proxy server** box is selected, select the **Bypass proxy server for local addresses** box.
10. Click **OK** twice.

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

Related Links

[Viewing Localized Versions of Web Interface](#)


[Adding iDRAC7 to the List of Trusted Domains](#)

[Disabling Whitelist Feature in Firefox](#)

Adding iDRAC7 to the List of Trusted Domains

When you access iDRAC7 Web interface, you are prompted to add iDRAC7 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 iDRAC7 Web interface.

On some operating systems, Internet Explorer (IE) 8 may not prompt you to add iDRAC7 IP address to the list of trusted domains if the IP address is missing from the list.

 **NOTE:** When connecting to the iDRAC7 Web interface with a certificate the browser does not trust, the browser's certificate error warning may display a second time after you acknowledge the first warning. This is the expected behavior to for security.

To add iDRAC7 IP address to the list of trusted domains in IE8, do the following:

1. Select **Tools** → **Internet Options** → **Security** → **Trusted sites** → **Sites**.
2. Enter iDRAC7 IP address to the **Add this website to the zone**.
3. Click **Add**, click **OK**, and then click **Close**.
4. Click **OK** and then refresh your browser.

Disabling Whitelist Feature in Firefox

Firefox has a "whitelist" security feature that requires user permission to install plug-ins for each distinct site that hosts a plug-in. If enabled, the whitelist feature requires you to install a Virtual Console viewer for each iDRAC7 you visit, even though the viewer versions are identical.

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

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

Viewing Localized Versions of Web Interface


iDRAC7 Web interface is supported in the following languages:

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

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

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

iDRAC7 Web interface is designed to work with localized keyboards for the supported language variants. Some features of iDRAC7 Web interface, such as Virtual Console, may require additional steps to access certain functions or letters. Other keyboards are not supported and may cause unexpected problems.

 **NOTE:** See the browser documentation on how to configure or setup different languages and view localized versions of iDRAC7 Web interface.


Updating iDRAC7 Firmware

You can update the firmware using any of the following methods:

- iDRAC7 Web interface
- RACADM CLI (iDRAC7 and CMC)
- Dell Update Package (DUP)
- CMC Web interface
- Lifecycle Controller–Remote Services
- Lifecycle Controller

During firmware update:

- After firmware update is complete, iDRAC7 is reset. This disconnects all connections and sessions.
- The fans in the rack and tower servers protect the system from overheating. After the update is complete, normal fan speed regulation resumes.
- iDRAC7 generates new SHA1 and MD5 keys for the SSL certificate if the configuration is not preserved.

 **NOTE:** Close all the browser windows that are connected to iDRAC7 after the firmware update is complete. Else, an Invalid Certificate error message is displayed as the keys are different from those in the browser session before update.

- If there is an interruption for any reason, firmware update feature is not enabled up to 30 minutes.

Related Links

[Downloading iDRAC7 Firmware](#)

[Updating Firmware Using iDRAC7 Web Interface](#)

[Updating Firmware Using CMC Web Interface](#)

[Updating Firmware Using DUP](#)


[Updating Firmware Using Remote RACADM](#)

[Updating Firmware Using Lifecycle Controller Remote Services](#)

Downloading iDRAC7 Firmware

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

- iDRAC7 Web interface — Download the binary image packaged as a self-extracting archive. The default firmware image file is **firmimg.d7**.

 **NOTE:** The same file format is used to recover iDRAC7 using CMC Web interface.

- Managed System — Download the operating system-specific Dell Update Package (DUP). The file extensions are **.bin** for Linux Operating systems and **.exe** for Windows operating systems.

- Lifecycle Controller — Download the latest catalog file and DUPs and use the *Platform Update* feature in Lifecycle Controller to update the iDRAC7 firmware. For more information about Platform Update, see *Lifecycle Controller User's Guide* available at support.dell.com/manuals.


Updating Firmware Using iDRAC7 Web Interface

To update using iDRAC7 Web interface:


1. Download the latest iDRAC7 firmware image.
2. In the iDRAC7 Web interface, go to **Overview** → **iDRAC Settings** → **iDRAC Firmware Update**.
The **Firmware Update** page is displayed.
3. Under **File Path**, click **Browse** to select the firmware image that is downloaded and click **Upload**.
The **Status (Step 2 of 3)** page is displayed. After the upload is complete, the current and the new firmware versions are displayed.

If the image does not upload and passes all verification checks, an error message is displayed and the update returns to the Firmware Update page. However, you can retry updating iDRAC7 or click **Cancel** to reset iDRAC7 to normal operating mode.

During firmware upgrade, if the image does not upload due to network issues, it continues to display firmware update is in-progress. After 30 minutes, it returns to the **Firmware Update** page.

 **NOTE:** During these 30 minutes, you cannot perform any firmware upgrade operations.

4. By default, the **Preserve Configuration** option is selected that saves the existing iDRAC7 configuration settings after a firmware update. If this option is cleared, all iDRAC7 configurations are reset to default values.

 **NOTE:** If iDRAC7 configuration is reset to default values, the iDRAC7 IP address is reset to 192.168.0.120. You can access iDRAC7 using this IP, or reconfigure the iDRAC7 IP address using local RACADM, front panel (LCD), or press F2 (remote RACADM requires network access).

To save the current settings, use the local RACADM or remote RACADM to export the iDRAC7 settings to a file and import the settings back in to iDRAC7 after the firmware is updated and the configurations are reset to default values. This is not required if you preserve configuration during firmware update.

For exporting iDRAC7 configuration settings from iDRAC7 to a file through RACADM interface:


- Local RACADM command is: `racadm getconfig -f iDRAC-config.txt`
- Remote RACADM command is: `racadm -r <iDRAC IP Address> -u <idrac-username> -p <password> getconfig -f iDRAC-config.txt`, where **iDRAC-config.txt** is the file that has the settings.

For importing iDRAC configuration settings from the file to iDRAC7 through RACADM:

- Local RACADM command is: `racadm config -f iDRAC-config.txt`
- Remote RACADM command is: `racadm -r <iDRAC IP Address> -u <idrac-username> -p <password> config -f iDRAC-config.txt`, where **iDRAC-config.txt** is the file that has the settings.

5. Click **Next**.

The **Updating (Step 3 of 3)** page is displayed and the progress of the update (in percentage) appears in the **Progress** column.

 **NOTE:** While in update mode, the update process continues in the background even if you navigate away from this page.

6. After the update is complete, to use iDRAC7, close the current browser window and reconnect using a new browser window.
7. To view the iDRAC7 firmware version in any of the following pages:

- Go to **Overview** → **Server** → **Properties** → **Summary** and view the firmware version under **Server Information** section.
- Go to **Overview** → **iDRAC Settings** → **Properties** and view the firmware version under **Integrated Dell Remote Access Controller 7** section.

Related Links

- [Updating iDRAC7 Firmware](#)
- [Downloading iDRAC7 Firmware](#)

Updating Firmware Using CMC Web Interface

You can update iDRAC7 firmware for blade servers using the CMC Web interface.

To update iDRAC7 firmware using the CMC Web interface:

1. Log in to CMC Web interface.
2. Go to **Server Overview** → **<server name>** .
The **Server Status** page is displayed.
3. Click **Launch iDRAC Web interface** and perform **iDRAC Firmware Update**.

Related Links

- [Updating iDRAC7 Firmware](#)
- [Downloading iDRAC7 Firmware](#)
- [Updating Firmware Using iDRAC7 Web Interface](#)

Updating Firmware Using DUP

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

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

 **NOTE:** While updating the iDRAC7 firmware using the DUP utility in Linux, if you see error messages such as `usb 5-2: device descriptor read/64, error -71` displayed on the console, ignore them.

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

To update iDRAC7 using DUP:

1. Download the DUP based on the installed operating system and run it on the managed system.
2. Run the DUP.
The firmware is updated. A system restart is not required after firmware update is complete.

Updating Firmware Using Remote RACADM

To update using remote RACADM:

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

```
racadm -r <iDRAC7 IP address> -u <username> -p <password> fwupdate -g -u -a <path>
```

where *path* is the location on the TFTP server where **firmimg.d7** is stored.

FTP server:

```
racadm -r <iDRAC7 IP address> -u <username> -p <password> fwupdate -f <ftpserver IP> <ftpserver username> <ftpserver password> -d <path>
```

where *path* is the location on the FTP server where **firmimg.d7** is stored.

For more information, see `fwupdate` command in the *RACADM Command Line Reference Guide for iDRAC7 and CMC Guide* available at support.dell.com/manuals.

Updating Firmware Using Lifecycle Controller Remote Services

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

Rolling Back iDRAC7 Firmware

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

- iDRAC7 Web interface
- CMC Web interface
- RACADM CLI (iDRAC7 and CMC)
- Lifecycle Controller
- Lifecycle Controller-Remote Services

Related Links

[Rollback Firmware Using iDRAC7 Web Interface](#)

[Rollback Firmware Using CMC Web Interface](#)

[Rollback Firmware Using RACADM](#)


[Rollback Firmware Using Lifecycle Controller](#)

[Rollback Firmware Using Lifecycle Controller-Remote Services](#)


Rollback Firmware Using iDRAC7 Web Interface

To roll back using iDRAC7 Web interface:

1. In the iDRAC7 Web interface, go to **Overview** → **iDRAC Settings** → **iDRAC Firmware Update**. The **Firmware - Upload / Rollback (Step 1 of 3)** page is displayed.
2. Click **Rollback**. The **Status (Step 2 of 3)** page displays the current and the rollback firmware versions.
3. By default, the **Preserve Configuration** check box is selected that saves the existing iDRAC7 configuration settings after a firmware rollback. To reset iDRAC7 to its default settings, clear the check box.

 **NOTE:** If iDRAC7 configuration is reset to default values, the iDRAC7 IP address is reset to 192.168.0.120. You can access iDRAC7 using this IP, or reconfigure the iDRAC7 address using local RACADM or F2 (remote RACADM requires network access).

4. Click **Next**. The **Updating (Step 3 of 3)** page is displayed.

 **NOTE:** While in rollback mode, the rollback process continues in the background even if you navigate away from this page.

5. After the rollback is complete, iDRAC7 is reset. To use iDRAC7, you must close the current browser window and reconnect using a new browser window.
6. To view the iDRAC7 firmware version, go to any of the following pages:
 - Go to **Overview** → **Server** → **Properties** → **Summary** and view the firmware version under **Server Information** section.
 - Go to **Overview** → **iDRAC Settings** → **Properties** and view the firmware version under **Integrated Dell Remote Access Controller 7** section.

Rollback Firmware Using CMC Web Interface

To roll back using the CMC Web interface:

1. Log in to CMC Web interface.
2. Go to **Server Overview** → **<server name>**.
The **Server Status** page is displayed.
3. Click **Launch iDRAC** Web interface and perform iDRAC7 firmware rollback.

Rollback Firmware Using RACADM

To rollback to a previous firmware version, use **fwupdate** command. For more information, see *RACADM Command Line Reference Guide for iDRAC7 and CMC* available at support.dell.com/manuals.

Rollback Firmware Using Lifecycle Controller

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

Rollback Firmware Using Lifecycle Controller-Remote Services

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


Recovering iDRAC7

iDRAC7 supports two operating system images to make sure a bootable iDRAC7. In the event of an unforeseen catastrophic error and you lose both boot paths:

- iDRAC7 bootloader detects that there is no bootable image.
- System Health and Identify LED is flashed at ~1/2 second rate. (LED is located on the back of a rack and tower servers and on the front of a blade server.)
- Bootloader is now polling the SD card slot.
- Format an SD card with FAT using a Windows operating system, or EXT3 using a Linux operating system.
- Copy **firmimg.d7** to the SD card.
- Insert the SD card into the server.
- Bootloader detects the SD card, turns the flashing LED to solid amber, reads the firmimg.d7, reprograms iDRAC7, and then reboots iDRAC7.

Using TFTP Server

You can use Trivial File Transfer Protocol (TFTP) server to upgrade or downgrade iDRAC7 firmware or install certificates. It is used in SM-CLP and RACADM command line interfaces to transfer files to and from iDRAC7. The TFTP server must be accessible using an iDRAC7 IP address or DNS name.

 **NOTE:** If you use iDRAC7 Web interface to transfer certificates and update firmware, TFTP server is not required.

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

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

Monitoring iDRAC7 Using Other Systems Management Tools

You can discover and monitor iDRAC7 using IT Assistant, Dell Management Console, and Dell OpenManage Essentials. You can also use Dell Remote Access Configuration Tool (DRACT) to discover iDRACs, update firmware, and set up Active Directory. For more information, see the respective user's guides.

Configuring iDRAC7


iDRAC7 enables you to configure iDRAC7 properties, set up users, and set up alerts to perform remote management tasks.

Before you configure iDRAC7, make sure that the iDRAC7 network settings and a supported browser is configured, and the required licenses are updated. For more information about the licensable feature in iDRAC7, see [Managing Licenses](#).

You can configure iDRAC7 using:

- iDRAC7 Web Interface
- RACADM
- Remote Services (see *Lifecycle Controller Remote Services User's Guide*)
- IPMITool (see *Baseboard Management Controller Management Utilities User's Guide*)

To configure iDRAC7:

1. Log in to iDRAC7.
2. Modify the network settings if required.
-  **NOTE:** If you have configured iDRAC7 network settings, using iDRAC Settings utility during iDRAC7 IP address setup, then ignore this step.
3. Configure interfaces to access iDRAC7.
4. Configure front panel display.
5. Configure System Location if required.
6. Establish any of the following alternate communication methods to iDRAC7:
 - IPMI or RAC serial
 - IPMI serial over LAN
 - IPMI over LAN
 - SSH or Telnet client
7. Obtain the required certificates.
8. Add and configure iDRAC7 users with privileges.
9. Configure and enable e-mail alerts, SNMP traps, or IPMI alerts.
10. Set the power cap policy if required.
11. Enable the Last Crash Screen.
12. Configure virtual console and virtual media if required.
13. Configure vFlash SD card if required.
14. Set the first boot device if required.
15. Set the internal management communication if required.

Related Links

[Logging In to iDRAC7](#)

[Modifying Network Settings](#)

- [Configuring Services](#)
- [Configuring Front Panel Display](#)
- [Setting Up Managed System Location](#)
- [Setting Up iDRAC7 Communication](#)
- [Configuring User Accounts and Privileges](#)
- [Monitoring and Managing Power](#)
- [Enabling Last Crash Screen](#)
- [Configuring and Using Virtual Console](#)
- [Managing Virtual Media](#)
- [Managing vFlash SD Card](#)
- [Setting First Boot Device](#)
- [Enabling Internal Systems Management Communication](#)
- [Configuring iDRAC7 to Send Alerts](#)

Viewing iDRAC7 Information

You can view the basic properties of iDRAC7.

Viewing iDRAC7 Information Using Web Interface

In the iDRAC7 Web interface, go to **Overview** → **iDRAC Settings** → **Properties** to view the following information related to iDRAC7. For information about the properties, see *iDRAC7 Online Help*.

- Device type
- Hardware and firmware version
- Last firmware update
- RAC time
- Number of possible active sessions
- Number of current sessions
- LAN is enabled or disabled
- IPMI version
- User interface title bar information
- Network settings
- IPv4 Settings
- IPv6 Settings


Viewing iDRAC7 Information Using RACADM

To view iDRAC7 information using RACADM, see `getsysinfo` or `get` subcommand details provided in the *RACADM Command Line Reference Guide for iDRAC7 and CMC* available at support.dell.com/manuals.

Modifying Network Settings

After configuring the iDRAC7 network settings using the iDRAC Settings utility, you can also modify the settings through the iDRAC7 Web interface, RACADM, Lifecycle Controller, Dell Deployment Toolkit, and Server Administrator (after booting to the operating system). For more information on the tools and privilege settings, see the respective user's guides.

To modify the network settings using iDRAC7 Web interface or RACADM, you must have **Configure iDRAC** privileges.

 **NOTE:** Changing the network settings may terminate the current network connections to iDRAC7.

Modifying Network Settings Using Web Interface

To modify the iDRAC7 network settings:

1. In the iDRAC7 Web interface, go to **Overview** → **iDRAC Settings** → **Network**.
The **Network** page is displayed.
2. Specify the required information and click **Apply**.
For information about the various settings, see the *iDRAC7 Online Help*.

Modifying Network Settings Using Local RACADM

To generate a list of available network properties, type 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 following is an example of how the command may be used to configure the required 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**, the iDRAC7 LAN is disabled even if DHCP is enabled.


Configuring IP Filtering and IP blocking


In addition to user authentication, use the following options to provide additional security while accessing iDRAC7:

- IP filtering limits the IP address range of the clients accessing iDRAC7. It compares the IP address of an incoming login to the specified range and allows iDRAC7 access only from a management station whose IP address is within the range. All other login requests are denied.
- IP blocking dynamically determines when excessive login failures occur from a particular IP address and blocks (or prevents) the address from logging in to iDRAC7 for a preselected time span. It includes:
 - The number of allowed login failures.
 - The time frame in seconds during which these failures must occur.

- The time frame in seconds that the blocked IP address is prevented from establishing a session after the allowed number of failures have exceeded.

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

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

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

Configure IP Filtering and IP Blocking Using iDRAC7 Web Interface

You must have Configure iDRAC7 privilege to perform these steps.

To configure IP filtering and blocking:

1. In iDRAC7 Web interface, go to **Overview** → **iDRAC Settings** → **Network** → **Network**.
The **Network** page is displayed.
2. Click **Advanced Settings**.
The **Network Security** page is displayed.
3. Specify the IP filtering and blocking settings.
For more information about the options, see *iDRAC7 Online Help*.
4. Click **Apply** to save the settings.

Configuring IP Filtering and IP Blocking Using RACADM

You must have configure iDRAC7 privilege to perform these steps.

To configure IP filtering and IP blocking, use the following RACADM objects:

- `cfgRacTuneIpRangeEnable`
- `cfgRacTuneIpRangeAddr`
- `cfgRacTuneIpRangeMask`
- `cfgRacTuneIpBlkEnable`
- `cfgRacTuneIpBlkFailCount`
- `cfgRacTuneIpBlkFailWindow`

The `cfgRacTuneIpRangeMask` property is applied to both the incoming IP address and to the `cfgRacTuneIpRangeAddr` property. If the results are identical, the incoming login request is allowed to access iDRAC7. Logging in from IP addresses outside this range results in 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.

Examples for IP Filtering

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


```
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.

Examples for IP blocking

- The following example prevents a management station IP address from establishing a session for five minutes if it has failed five login attempts within a minute.

```
racadm config -g cfgRacTuning -o cfgRacTuneIpRangeEnable 1
racadm config -g cfgRacTuning -o cfgRacTuneIpBlkFailCount 5
racadm config -g cfgRacTuning -o cfgRacTuneIpBlkFailWindow 60
```

- The following example prevents more than three failed attempts within a 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
```

For more information, see the *RACADM Command Line Reference Guide for iDRAC7 and CMC* available at support.dell.com/manuals.

Configuring Services

You can configure and enable the following services on iDRAC7:

- Local Configuration — Disable access to iDRAC7 configuration (from the host system) using Local RACADM and iDRAC Settings utility.
- Web Server — Enable access to iDRAC7 Web interface. If you disable the option, you can enable it using RACADM.
- SSH — Access iDRAC7 through firmware RACADM.
- Telnet — Access iDRAC7 through firmware RACADM
- Remote RACADM — Remotely access iDRAC7.
- SNMP Agent — Enable iDRAC7 to send SNMP traps for events.
- Automated System Recovery Agent — Enable Last System Crash Screen.

Configuring Services Using Web Interface

To configure the services using iDRAC7 Web interface:

1. In the iDRAC7 Web interface, go to **Overview** → **iDRAC Settings** → **Network** → **Services**. The **Services** page is displayed.
2. Specify the required information and click **Apply**.
For information about the various settings, see the *iDRAC7 Online Help*.

Configuring Services Using RACADM

To enable and configure the various services, use the following RACADM objects:

- `cfgRacTuneLocalConfigDisable`
- `cfgRacTuneCtrlEConfigDisable`
- `cfgSerialSshEnable`
- `cfgRacTuneSshPort`
- `cfgSsnMgtSshIdleTimeout`
- `cfgSerialTelnetEnable`
- `cfgRacTuneTelnetPort`
- `cfgSsnMgtTelnetIdleTimeout`
- `cfgRacTuneWebserverEnable`
- `cfgSsnMgtWebserverTimeout`
- `cfgRacTuneHttpPort`
- `cfgRacTuneHttpsPort`
- `cfgRacTuneRemoteRacadmEnable`
- `cfgSsnMgtRacadmTimeout`
- `cfgOobSnmpAgentEnable`
- `cfgOobSnmpAgentCommunity`

For more information about these objects, see *RACADM Command Line Reference Guide for iDRAC7 and CMC* available at support.dell.com/manuals.

Configuring Front Panel Display

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

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

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

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

Related Links

[Configuring LCD Setting](#)

[Configuring System ID LED Setting](#)

Configuring LCD Setting

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

Configuring LCD Setting Using Web Interface

To configure the server LCD front panel display:

1. In iDRAC7 Web interface, go to **Overview** → **Hardware** → **Front Panel**.
2. In **LCD Settings** section, from the **Set Home Message** drop-down menu, select any of the following:
 - Service Tag (default)
 - Asset Tag
 - DRAC MAC Address
 - DRAC IPv4 Address

- DRAC IPv6 Address
- System Power
- Ambient Temperature
- System Model
- Host Name
- User Defined
- None

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

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

3. Click **Apply.**

The server LCD front panel displays the configured home message.

Configuring LCD Setting Using RACADM

To configure the server LCD front panel display, use the objects in the `System.LCD` group. For more information, see the *RACADM Command Line Reference Guide for iDRAC7 and CMC* available at support.dell.com/manuals.

Configuring LCD Setting Using iDRAC Settings Utility

To configure the server LCD front panel display:

1. In the iDRAC Settings utility, go to **LCD**.
The **iDRAC Settings LCD** page is displayed.
2. Specify the required options.
For more information, see the *iDRAC Settings Utility Online Help*.
3. Click **Back**, click **Finish**, and then click **Yes**.
The settings are saved.

Configuring System ID LED Setting

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

Configuring System ID LED Setting Using Web Interface

To configure the System ID LED display:

1. In iDRAC7 Web interface, go to **Overview** → **Hardware** → **Front Panel**. The **Front Panel** page is displayed.
2. In **System ID LED Settings** section, select any of the following options to enable or disable LED blinking:
 - Blink Off
 - Blink On
 - Blink On 1 Day Timeout
 - Blink On 1 Week Timeout
 - Blink On 1 Month Timeout

3. Click **Apply.**


The LED blinking on the front panel is configured.

Configuring System ID LED Setting Using RACADM

To configure system ID LED, use the **setled** command. For more information, see the *RACADM Command Line Reference Guide for iDRAC7 and CMC* available at support.dell.com/manuals.

Setting First Boot Device

You can set the first boot device for the next boot only or for all subsequent reboots. Based on this selection, you can set the first boot device for the system. The system boots from the selected device on the next and subsequent reboots and remains as the first boot device in the BIOS boot order, until it is changed again either from the iDRAC7 Web interface or from the BIOS boot sequence.

 **NOTE:** The first boot device setting in iDRAC7 Web Interface overrides the System BIOS boot settings.

Setting First Boot Device Using Web Interface

To set the first boot device using iDRAC7 Web interface:

1. Go to **Overview** → **Server** → **Setup** → **First Boot Device**.
The **First Boot Device** page is displayed.
2. Select the required first boot device from the drop-down list, and click **Apply**.
The system boots from the selected device for subsequent reboots.
3. To boot from the selected device only once on the next boot, select **Boot Once**. Thereafter, the system boots from the first boot device in the BIOS boot order.
For more information about the options, see the *iDRAC7 Online Help*.

Setting First Boot Device Using RACADM

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

For more information about these objects, see the *RACADM Command Line Reference Guide for iDRAC7 and CMC* available at support.dell.com/manuals.

Enabling Internal Systems Management Communication

In rack or tower systems that have Network Daughter Card (NDC) or LAN On Motherboard (LOM) devices, you can enable the Internal Systems Management Communication channel that provides a high-speed bi-directional in-band communication between iDRAC7 and the host operating system through a shared LOM. You can enable this channel using:

- iDRAC Settings utility (pre-operating system environment),
- RACADM or WS-MAN (post operating system environment)
- iDRAC7 is in shared mode (that is, NIC selection is assigned to one of the LOMs)
- Host operating system and iDRAC7 are in the same subnet and same VLAN.

IMC supports IPv4 and IPv6 addresses.

Before enabling the internal systems management communication, make sure that:

- iDRAC7 is in shared mode (that is, NIC selection is assigned to one of the LOMs).
- Host operating system and iDRAC7 are in the same subnet and same VLAN.

Enabling IMC Using iDRAC Settings Utility

To enable IMC using iDRAC Settings utility:

1. In the iDRAC Settings utility, go to **Communication Pass-Through**.
The **Communication Pass-Through** page is displayed.
2. Select **Enabled**.
For information about the options, see the *iDRAC Settings Utility Online Help*.
3. Click **Back**, click **Finish**, and then click **Yes**.
The details are saved.

Enabling IMC Using RACADM

To set iDRAC7 in shared mode (example LOM1):

```
racadm config -g cfglannetworking -o cfgnicselection 2
```

To enable IMC:

```
racadm set idrac.imc.AdministrativeState Enabled
```

Enabling Last Crash Screen

To troubleshoot the cause of managed system crash, you can capture the system crash image using iDRAC7.

To enable the last crash screen:

1. From the *Dell Systems Management Tools and Documentation* DVD, install Server Administrator on the managed system.
For more information, see the *Dell OpenManage Server Administrator Installation Guide* at support.dell.com/manuals.
2. In the **Windows** startup and recovery window, make sure that the automatic reboot option is not selected.
For more information, see Windows documentation.
3. Use Server Administrator to enable the **Auto Recovery** timer, set the Auto Recovery action to **Reset, Power Off**, or **Power Cycle**, and set the timer in seconds (a value between 60 - 480).
For more information, see the *Dell OpenManage Server Administrator Installation Guide* at support.dell.com/manuals.
4. Enable the **Auto Shutdown and Recovery (ASR)** option using one of the following:
 - Server Administrator — See *Dell OpenManage Server Administrator User's Guide* at support.dell.com/manuals.
 - Local RACADM — Use the command:


```
racadm config -g cfgRacTuning -o cfgRacTuneAsrEnable 1
```
5. Enable **Automated System Recovery Agent**. To do this, go to **Overview** → **iDRAC Settings** → **Network** → **Services**, select **Enabled** and click **Apply**.

Obtaining Certificates

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

Table 7. Types of Certificate Based on Login Type

| Login Type | Certificate Type | How to Obtain |
|--|--|--|
| Single Sign-on using Active Directory | Trusted CA certificate | Generate a CSR and get it signed from a Certificate Authority |
| Smart Card login as a local or Active Directory user | <ul style="list-style-type: none"> • User certificate • Trusted CA certificate | <ul style="list-style-type: none"> • User Certificate — Export the smart card user certificate as Base64-encoded file using the card management software provided by the smart card vendor. • Trusted CA certificate — This certificate is issued by a CA. |
| Active Directory user login | Trusted CA certificate | This certificate is issued by a CA. |
| Local User login | SSL Certificate | Generate a CSR and get it signed from a trusted CA |

 **NOTE:** iDRAC7 ships with a default self-signed SSL server certificate. The iDRAC7 Web server, Virtual Media, and Virtual Console use this certificate.

Related Links

- [SSL Server Certificates](#)
- [Generating a New Certificate Signing Request](#)

SSL Server Certificates

iDRAC7 includes a Web server that is configured to use the industry-standard SSL security protocol to transfer encrypted data over a network. Built upon asymmetric encryption technology, SSL is widely accepted for providing authenticated and encrypted communication between clients and servers to prevent eavesdropping across a network.

An SSL-enabled system can perform the following tasks:

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

The encryption process provides a high level of data protection. iDRAC7 employs the 128-bit SSL encryption standard, the most secure form of encryption generally available for Internet browsers in North America.

iDRAC7 Web server has a Dell self-signed SSL digital certificate by default. To make sure iDRAC7 sessions are authentic and prevent administrators from revealing iDRAC7 credentials to unauthorized users, replace the SSL server 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, use either iDRAC7 Web interface or RACADM interface to generate a Certificate Signing Request (CSR) with your company’s information. Then, submit the generated CSR to a CA such as VeriSign or Thawte.

Related Links

- [Generating a New Certificate Signing Request](#)
- [Uploading Server Certificate](#)
- [Viewing Server Certificate](#)

Generating a New Certificate Signing Request

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

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


After the CA approves the CSR and issues the SSL server certificate, it can be uploaded to iDRAC7. The information used to generate the CSR, stored on the iDRAC7 firmware, must match the information contained in the SSL server certificate, that is, the certificate must have been generated using the CSR created by iDRAC7.

Related Links

[SSL Server Certificates](#)

Generating CSR Using Web Interface

To generate a new CSR:

 **NOTE:** Each new CSR overwrites any previous CSR data stored in the firmware. The information in the CSR must match the information in the SSL server certificate. Else, iDRAC7 does not accept the certificate.

1. In the iDRAC7 Web interface, go to **Overview** → **iDRAC Settings** → **Network** → **SSL**, select **Generate a New Certificate Signing Request (CSR)** and click **Next**.

The **Generate a New Certificate Signing Request** page is displayed.

2. Enter a value for each CSR attribute.
For more information, see *iDRAC7 Online Help*.
3. Click **Generate**.
A new CSR is generated.
4. Click **Download** to save the CSR file to the management station.

Generating CSR Using RACADM

To generate a CSR, use the objects in `cfgRacSecurityData` group to specify the values and the use the `sslcsrgen` command to generate the CSR. For more information, see the *RACADM Command Line Reference Guide for iDRAC7 and CMC* available at support.dell.com/manuals.

Uploading Server Certificate

After generating a CSR, you can upload the signed SSL server certificate to the iDRAC7 firmware. iDRAC7 resets after the certificate is uploaded. iDRAC7 accepts only X509, Base 64 encoded Web server certificates.

 **CAUTION:** During the certificate upload process, iDRAC7 is not available.

Related Links

[SSL Server Certificates](#)

Uploading Server Certificate Using Web Interface

To upload the SSL server certificate:

1. In the iDRAC7 Web interface, go to **Overview** → **iDRAC Settings** → **Network** → **SSL**, select **Upload Server Certificate** and click **Next**.

The **Certificate Upload** page is displayed.

2. Under **File Path**, click **Browse** and select the certificate on the management station.
3. Click **Apply**.

The SSL server certificate is uploaded to iDRAC7 firmware, and replaces the existing certificate.

Uploading Server Certificate Using RACADM

To upload the SSL server certificate, use the `sslcertupload` command. For more information, see the *RACADM Command Line Reference Guide for iDRAC7 and CMC* available at support.dell.com/manuals.

Viewing Server Certificate

You can view the SSL server certificate that is currently being used in iDRAC7.

Related Links

[SSL Server Certificates](#)

Viewing Server Certificate Using Web Interface


In the iDRAC7 Web interface, go to **Overview** → **iDRAC Settings** → **Network** → **SSL**, select **View Server Certificate** and click **Next**. The **View Server Certificate** page displays the SSL server certificate currently in use.

Viewing Server Certificate Using RACADM

To view the SSL server certificate, use the `sslcertview` command. For more information, see the *RACADM Command Line Reference Guide for iDRAC7 and CMC* available at support.dell.com/manuals.

Configuring Multiple iDRAC7s Using RACADM


You can configure one or more iDRAC7s with identical properties using RACADM. When you query a specific iDRAC7 using its group ID and object ID, RACADM creates the `.cfg` configuration file from the retrieved information. File name is user specified. Import the file to other iDRAC7s to identically configure them.


 **NOTE:** Few configuration files contain unique iDRAC7 information (such as the static IP address) that you must modify before you export the file to other iDRAC7s.

To configure multiple iDRAC7s:

1. Query the target iDRAC7 that contains the required configuration using the command: `racadm getconfig -f myfile.cfg`.


The command requests the iDRAC7 configuration and generates the `myfile.cfg` file. If required, you can configure the file with another name.

 **NOTE:** Redirecting the iDRAC7 configuration to a file using `getconfig -f` is only supported with the local and remote RACADM interfaces.

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

The `getconfig` command displays all configuration properties in a group (specified by group name and index) and all configuration properties for a user by user name.

2. Modify the configuration file using a simple text editor (optional).

 **NOTE:** It is recommended that you edit this file with a simple text editor. The RACADM utility uses an ASCII text parser. Any formatting confuses the parser, which may corrupt the RACADM database.

3. Use the new configuration file to modify the target iDRAC7 using the command: `racadm config -f myfile.cfg`
This loads the information into the other iDRAC7. You can use `config` subcommand to synchronize the user and password database with Server Administrator.
4. Reset the target iDRAC7 using the command: `racadm racreset`

Creating an iDRAC7 Configuration File

The configuration file `.cfg` can be:


- Created
 - Obtained from a `racadm getconfig -f <filename>.cfg` command
 - Obtained from a `racadm getconfig -f <filename>.cfg` command, and then edited
- For information about the `getconfig` command, see `getconfig` command in the *RACADM Command Line Reference Guide for iDRAC7 and CMC* available at support.dell.com/manuals .

The `.cfg` file is first parsed to verify that valid group and object names are present and the basic syntax rules are being followed. Errors are flagged with the line number that detected the error, and a message explains the problem. The entire file is parsed for correctness, and all errors are displayed. Write commands are not transmitted to iDRAC7 if an error is found in the `.cfg` file. The user must correct all errors before using the file to configure iDRAC7. Use the `-c` option in the `config` subcommand, which verifies the syntax and does not perform a write operation to iDRAC7.

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

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


```
[cfgUserAdmin]
# cfgUserAdminIndex=11
cfgUserAdminUserName=
# cfgUserAdminPassword=***** (Write-Only)
cfgUserAdminEnable=0
cfgUserAdminPrivilege=0x00000000
cfgUserAdminIpmlanPrivilege=15
cfgUserAdminIpmlSerialPrivilege=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 iDRAC7 and CMC* available at support.dell.com/manuals .
- Use the `racresetcfg` subcommand to reset the iDRAC7 to original defaults, and then run the `racadm config -f <filename>.cfg` command. Make sure that the `.cfg` file includes all required objects, users, indexes, and other parameters.

 **CAUTION: Use the `racresetcfg` subcommand to reset the database and the iDRAC7 NIC settings to the original default settings and remove all users and user configurations. While the root user is available, other user settings are also reset to the default settings.**

Parsing Rules

- All lines that start with '#' are treated as comments. A comment line must start in column one. A '#' character in any other column is treated as a '#' character. Some modem parameters may include # characters in its string.

An escape character is not required. You may want to generate a **.cfg** from a `racadm getconfig -f <filename> .cfg` command, and then perform a `racadm config -f <filename> .cfg` command to a different iDRAC7, without adding escape characters. Example:

```
#
# This is a comment
[cfgUserAdmin]
cfgUserAdminPageModemInitString=<Modem init # not a comment>
```

- All group entries must be surrounded by "[" and "]" characters. The starting "[" character denoting a group name *must* start in column one. This group name *must* be specified before any of the objects in that group. Objects that do not include an associated group name generate an error. The configuration data is organized into groups as defined in the *RACADM Command Line Reference Guide for iDRAC7 and CMC* available at support.dell.com/manuals. The following example displays a group name, object, and the object's property value.

```
[cfgLanNetworking] -{group name}
cfgNicIpAddress=143.154.133.121 {object name}
```

- All parameters are specified as "object=value" pairs with no white space between the object, =, or value. White spaces that are included after the value are ignored. A white space inside a value string remains unmodified. Any character to the right of the '=' is taken as is (for example, a second '=', or a '#', '[', ']', and so forth). These characters are valid modem chat script characters.

See the example in the previous bullet.

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

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

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

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

```
[cfgUserAdmin]
cfgUserAdminIndex=11
```

If you type `racadm getconfig -f <myexample> .cfg`, the command builds a **.cfg** file for the current iDRAC7 configuration. This configuration file can be used as an example and as a starting point for your unique **.cfg** file.

Modifying the iDRAC7 IP Address

When you modify the iDRAC7 IP address in the configuration file, remove all unnecessary `<variable>=value` entries. Only the actual variable group's label with "[" and "]" remains, including the two `<variable>=value` entries pertaining to the IP address change.

For example:

```
#
# Object Group "cfgLanNetworking"
#
[cfgLanNetworking]
cfgNicIpAddress=10.35.10.110
cfgNicGateway=10.35.10.1
```


This file is updated as follows:

```
#
# Object Group "cfgLanNetworking"
```

```
#  
[cfgLanNetworking]  
cfgNicIpAddress=10.35.9.143  
# comment, the rest of this line is ignored  
cfgNicGateway=10.35.9.1
```

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


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

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

Disabling Access to Modify iDRAC7 Configuration Settings on Host System

You can disable access to modify the iDRAC7 configuration settings through Local RACADM or iDRAC Settings utility. However, you can view these configuration settings. To do this:

1. In iDRAC7 Web interface, go to **Overview** → **iDRAC Settings** → **Network** → **Services**.
2. Select one or both of the following:
 - **Disable the iDRAC Local Configuration using iDRAC Settings** — Disables access to modify the configuration settings in iDRAC Settings utility.
 - **Disable the iDRAC Local Configuration using RACADM** — Disables access to modify the configuration settings in Local RACADM.
3. Click **Apply**.

 **NOTE:** If access is disabled, you cannot use Server Administrator or IPMITool to perform iDRAC7 configurations. However, you can use IPMI Over LAN.

Viewing iDRAC7 and Managed System Information

You can view iDRAC7 and managed system's health and properties, hardware and firmware inventory, sensor health, storage devices, network devices, and view and terminate user sessions. For blade servers, you can also view the flex address information.

Related Links

- [Viewing Managed System Health and Properties](#)
- [Viewing System Inventory](#)
- [Viewing Sensor Information](#)
- [Inventory and Monitoring Storage Devices](#)
- [Inventory and Monitoring Network Devices](#)
- [Viewing FlexAddress Mezzanine Card Fabric Connections](#)
- [Viewing or Terminating iDRAC7 Sessions](#)

Viewing Managed System Health and Properties

When you log in to iDRAC7 Web interface, the **System Summary** page allows you to view the managed system's health, basic iDRAC7 information, preview the virtual console, add and view work notes, and quickly launch tasks such as power on or off, power cycle, view logs, update firmware, and reset iDRAC7.


To access the **System Summary** page, go to **Overview** → **Server** → **Properties** → **Summary**. The **System Summary** page is displayed. For more information, see the *iDRAC7 Online Help*.

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

Viewing System Inventory

You can view information about the hardware and firmware components installed on the managed system. To do this, in iDRAC7 Web interface, go to **Overview** → **Server** → **Properties** → **System Inventory**. For information about the displayed properties, see the *iDRAC7 Online Help*.


When you replace any hardware component or update the firmware versions, make sure to enable and run the **Collect System Inventory on Reboot** (CSIOR) option to collect the system inventory on reboot. After a few minutes, log in to iDRAC7, and navigate to the **System Inventory** page to view the details. It may take up to five minutes for the information to be available depending on the hardware installed on the server.

 **NOTE:** CSIOR option is enabled by default.


Viewing Sensor Information

The following sensors help to monitor the health of the managed system:

- **Battery Sensor** — Provides information about the batteries on the system board CMOS and storage RAID On Motherboard (ROMB).

 **NOTE:** The Storage ROMB battery settings are available only if the system has a ROMB with a battery.

- **Fan Sensor** (available only for rack and tower servers) — Provides information about the system fans —fan redundancy and fans list that display fan speed and threshold values.
- **CPU Sensor** — Indicates the health and state of the CPUs in the managed system.
- **Intrusion Sensor** — Provides information about the chassis.
- **Power Supplies Sensor** (available only for rack and tower servers) — Provides information about the power supplies and the power supply redundancy status.

 **NOTE:** If there is only one power supply in the system, the power supply redundancy is set to **Disabled**.

- **Removable Flash Media Sensor** — Provides information about the Internal SD Modules—vFlash and Internal Dual SD Module (IDSDM).
 - When IDSDM redundancy is enabled, the following IDSDM sensor status is displayed—IDSDM Redundancy Status, IDSDM SD1, IDSDM SD2. When redundancy is disabled, only IDSDM SD1 is displayed.
 - If IDSDM redundancy is initially disabled when the system is powered on or after an iDRAC reset, the IDSDM SD1 sensor status is displayed only after a card is inserted.
 - If IDSDM redundancy is enabled with two SD cards present in the IDSDM, and the status of one SD card is *online* while the status of the other card is *offline*. A system reboot is required to restore redundancy between the two SD cards in the IDSDM. After the redundancy is restored, the status of both the SD cards in the IDSDM is *online*.
 - During the rebuilding operation to restore redundancy between two SD cards present in the IDSDM, the IDSDM status is not displayed since the IDSDM sensors are powered off.
 - System Event Logs (SEL) for a write-protected or corrupt SD card in the IDSDM module are not repeated until they are cleared by replacing the SD card with a writable or good SD card, respectively.
- **Temperature Sensor** — Provides information about the system board inlet temperature and exhaust temperature (only applies to racks and towers). The temperature probe indicates whether the status of the probe is within the pre-set warning and critical threshold value.
- **Voltage Sensor** — Indicates the status and reading of the voltage sensors on various system components.

The following table provides how to view the sensor information using iDRAC7 Web interface and RACADM. For information about the properties that are displayed on the Web interface, see the *iDRAC7 Online Help* for the respective pages.

Table 8. Sensor Information Using Web Interface and RACADM

| View Sensor Information For | Using Web Interface | Using RACADM |
|-----------------------------|---|---|
| Battery | Overview → Hardware → Batteries | Use the getsensorinfo command. For power supplies, you can also use the System.Power.Supply command with the get subcommand. For more information, see the <i>RACADM Command Line Reference Guide for iDRAC7 and CMC</i> available at support.dell.com/manuals . |
| Fan | Overview → Hardware → Fans | |
| CPU | Overview → Hardware → CPU | |
| Intrusion | Overview → Server → Intrusion | |
| Power Supplies | Overview → Hardware → Power Supplies | |

| View Sensor Information For | Using Web Interface | Using RACADM |
|-----------------------------|--|--------------|
| Removable Flash Media | Overview → Hardware → Removable Flash Media | |
| Temperature | Overview → Server → Power/Thermal → Temperatures | |
| Voltage | Overview → Server → Power/Thermal → Voltages | |

Inventory and Monitoring Storage Devices

You can remotely monitor the health and view the inventory of the following Comprehensive Embedded Management (CEM) enabled storage devices in the managed system using iDRAC7 Web interface or RACADM:

- RAID controllers that include battery.
- Enclosures that includes Enclosure Management Modules (EMMs), power supply, fan probe, and temperature probe
- Physical disks
- Virtual disks

However, WS-MAN displays information for most of the storage devices in the system.

iDRAC7 inventories and monitors the PERC 8 series of RAID controllers that include H310, H710, H710P, and H810. The controllers that do not support Comprehensive Embedded Management are Internal Tape Adapters (ITAs) and SAS 6Gbps HBA.

The recent storage events and topology of storage devices are also displayed.

Alerts and SNMP traps are generated for storage events. The events are logged in the Lifecycle Log.

For the conceptual information, see *OpenManage Storage Management User's Guide* available at support.dell.com/manuals.

Monitoring Storage Device Using Web Interface

To view the storage device information using Web interface:

- Go to **Overview** → **Storage** → **Summary** to view the summary of the storage components and the recently logged events. This page is automatically refreshed every 30 seconds.
- Go to **Overview** → **Storage** → **Topology** to view the hierarchical physical containment view of the key storage components.
- Go to **Overview** → **Storage** → **Physical Disks** to view physical disk information. The **Physical Disks** page is displayed.
- Go to **Overview** → **Storage** → **Virtual Disks** to view virtual disks information. The **Virtual Disks** page is displayed.
- Go to **Overview** → **Storage** → **Controllers** to view the RAID controller information. The **Controllers** page is displayed.
- Go to **Overview** → **Storage** → **Enclosures** to view the enclosure information. The **Enclosures** page is displayed.

You can also use filters to view specific device information.

For more information on the displayed properties and to use the filter options, see *iDRAC7 Online Help*.

Monitoring Storage Device Using RACADM

To view the storage device information, use the **raid** command. For more information, see the *RACADM Command Line Reference Guide for iDRAC7 and CMC* available at support.dell.com/manuals.

Inventory and Monitoring Network Devices

You can remotely monitor the health and view the inventory of the following network devices in the managed system:


- Network Interface Cards (NICs)
- Converged Network Adapters (CNAs)
- LAN On Motherboards (LOMs)
- Network Daughter Cards (NDCs)
- Mezzanine cards (only for blade servers)

For each device, you can view the following information of the ports and supported partitions:

- Link Status
- Properties
- Settings and Capabilities
- Receive and Transmit Statistics

Monitoring Network Devices Using Web Interface

To view the network device information using Web interface, go to **Overview** → **Hardware** → **Network Devices**. The **Network Devices** page is displayed. For more information about the displayed properties, see *iDRAC7 Online Help*.

 **NOTE:** If the **OS Driver State** displays the state as Operational, it indicates the operating system driver state or the UEFI driver state.

Monitoring Network Devices Using RACADM

To view the network device information, use the **hwinventory** and **nicstatistics** commands. For more information, see the *RACADM Command Line Reference Guide for iDRAC7 and CMC* available at support.dell.com/manuals.

Additional properties may be displayed when using RACADM or WS-MAN in addition to the properties displayed in the iDRAC7 Web interface.

Viewing FlexAddress Mezzanine Card Fabric Connections


In blade servers, FlexAddress allows the use of persistent, chassis-assigned World Wide Names and MAC addresses (WWN/MAC) for each managed server port connection.

You can view the following information for each installed embedded Ethernet and optional mezzanine card port:

- Fabrics to which the cards are connected.
- Type of fabric.
- Server-assigned, chassis-assigned, or remotely assigned MAC addresses.

To view the Flex Address information in iDRAC7, configure and enable the Flex Address feature in Chassis Management Controller (CMC). For more information, see the *Dell Chassis Management Controller User Guide* available at

support.dell.com/manuals. Any existing Virtual Console or Virtual Media session terminates if the FlexAddress setting is enabled or disabled.

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

The FlexAddress feature replaces the server–assigned MAC addresses with chassis–assigned MAC addresses and is implemented for iDRAC7 along with blade LOMs, mezzanine cards and I/O modules. The iDRAC7 FlexAddress feature supports preservation of slot specific MAC address for iDRAC7s in a chassis. The chassis–assigned MAC address is stored in CMC non–volatile memory and is sent to iDRAC7 during an iDRAC7 boot or when CMC FlexAddress is enabled. If CMC enables chassis–assigned MAC addresses, iDRAC7 displays the **MAC address** on any of the following pages:

- **Overview** → **Server** → **Properties Details** → **iDRAC Information**.
- **Overview** → **Server** → **Properties WWN/MAC**.
- **Overview** → **iDRAC Settings** → **Properties iDRAC Information** → **Current Network Settings**.
- **Overview** → **iDRAC Settings** → **Network Network** → **Network Settings**.

 **CAUTION:** With FlexAddress enabled, if you switch from a server–assigned MAC address to a chassis–assigned MAC address and vice–versa, iDRAC7 IP address also changes.

Viewing or Terminating iDRAC7 Sessions

You can view the number of users currently logged in to iDRAC7 and terminate the user sessions.

Terminating iDRAC7 Sessions Using Web Interface

The users who do not have administrative privileges must have Configure iDRAC7 privilege to terminate iDRAC7 sessions using iDRAC7 Web interface.

To view and terminate the iDRAC7 sessions:

1. In the iDRAC7 Web interface, go to **Overview** → **iDRAC Settings** → **Sessions**.
The **Sessions** page displays the session ID, username, IP address, and session type. For more information about these properties, see the *iDRAC7 Online Help*.
2. To terminate the session, under the **Terminate** column, click the Trashcan icon for a session.

Terminating iDRAC7 Sessions Using RACADM

You must have administrator privileges to terminate iDRAC7 sessions using RACADM.

To view the current user sessions, use the **getssninfo** command.

To terminate a user session, use the **closeasn** command.

For more information about these commands, see the *RACADM Command Line Reference Guide for iDRAC7 and CMC* available at support.dell.com/manuals.

Setting Up iDRAC7 Communication

You can communicate with iDRAC7 using any of the following modes:

- iDRAC7 Web Interface
- Serial connection using DB9 cable (RAC serial or IPMI serial) - For rack and tower servers only
- IPMI Serial Over LAN
- IPMI Over LAN
- Remote RACADM
- Local RACADM
- Remote Services

For an overview of the supported protocols, supported commands, and pre-requisites, see the following table.

Table 9. Communication Modes—Summary

| Mode of Communication | Supported Protocol | Supported Commands | Prerequisite |
|--|---|--------------------------------------|--|
| iDRAC7 Web Interface | Internet Protocol (https) | NA | Web Server |
| Serial using Null modem DB9 cable | Serial Protocol | RACADM SMCLP IPMI | Part of iDRAC7 firmware RAC Serial or IPMI Serial is enabled. |
| IPMI Serial Over LAN | Intelligent Platform Management Bus protocol SSH Telnet | IPMI | IPMITool is installed and IPMI Serial Over LAN is enabled. |
| IPMI over LAN | Intelligent Platform Management Bus protocol | IPMI | IPMITool is installed and IPMI Settings is enabled. |
| SMCLP | SSH Telnet | SMCLP | SSH or Telnet on iDRAC7 is enabled. |
| Remote RACADM | https | Remote RACADM | Remote RACADM is installed and enabled. |
| Firmware RACADM | SSH Telnet | Firmware RACADM | Firmware RACADM is installed and enabled |
| Local RACADM | IPMI | Local RACADM | Local RACADM is installed. |
| Remote Services [1] | WS-MAN | WinRM (Windows) OpenWSMAN (Linux) | WinRM is installed (Windows) or OpenWSMAN is installed (Linux). |

[1] For more information, see the *Lifecycle Controller Remote Services User's Guide* available at support.dell.com/manuals.

Related Links


[Communicating With iDRAC7 Through Serial Connection Using DB9 Cable](#)
[Switching Between RAC Serial and Serial Console While Using DB9 Cable](#)

- [Communicating With iDRAC7 Using IPMI SOL](#)
- [Communicating With iDRAC7 Using IPMI Over LAN](#)
- [Enabling or Disabling Remote RACADM](#)
- [Disabling Local RACADM](#)
- [Enabling IPMI on Managed System](#)
- [Configuring Linux for Serial Console During Boot](#)
- [Supported SSH Cryptography Schemes](#)

Communicating With iDRAC7 Through Serial Connection Using DB9 Cable

You can use any of the following communication methods to perform systems management tasks through serial connection to rack and tower servers:

- RAC Serial
- IPMI Serial — Direct Connect Basic mode and Direct Connect Terminal mode

 **NOTE:** In case of blade servers, the serial connection is established through the chassis. For more information, see the *Chassis Management Controller User's Guide* available at support.dell.com/manuals.

To establish the serial connection:

1. Configure the BIOS to enable serial connection:
2. Connect the Null Modem DB9 cable from the management station's serial port to the managed system's external serial connector.
3. Make sure that the management station's terminal emulation software is configured for serial connection using any of the following:
 - Linux Minicom in an Xterm
 - Hilgraeve's HyperTerminal Private Edition (version 6.3)

Based on where the managed system is in its boot process, you can see either the POST screen or the operating system screen. This is based on the configuration: SAC for Windows and Linux text mode screens for Linux.


4. Enable RAC serial or IPMI serial connections in iDRAC7.

Related Links

- [Configuring BIOS For Serial Connection](#)
- [Enabling RAC Serial Connection](#)
- [Enabling IPMI Serial Connection Basic and Terminal Modes](#)

Configuring BIOS For Serial Connection

To configure BIOS for Serial Connection:


 **NOTE:** This is applicable only for iDRAC7 on rack and tower servers.

1. Turn on or restart the system.
2. Press <F2>.
3. Go to **System BIOS Settings** → **Serial Communication**.
4. Select **External Serial Connector** to **Remote Access device**.
5. Click **Back**, click **Finish**, and then click **Yes**.

6. Press <Esc> to exit **System Setup**.

Enabling RAC Serial Connection

After configuring serial connection in BIOS, enable RAC serial in iDRAC7.

 **NOTE:** This is applicable only for iDRAC7 on rack and tower servers.

Enabling RAC Serial Connection Using Web Interface

To enable RAC serial connection:

1. In the iDRAC7 Web interface, go to **Overview** → **iDRAC Settings** → **Network** → **Serial**.
The **Serial** page is displayed.
2. Under **RAC Serial**, select **Enabled** and specify the values for the attributes.
3. Click **Apply**.
The IPMI serial settings are configured.


Enabling RAC Serial Connection Using RACADM

To enable RAC serial connection:

```
racadm config -g cfgSerial -o cfgSerialConsoleEnable 1
```

Enabling IPMI Serial Connection Basic and Terminal Modes

To enable IPMI serial routing of BIOS to iDRAC7, configure IPMI Serial in any of the following modes in iDRAC7:

 **NOTE:** This is applicable only for iDRAC7 on rack and tower servers.

- IPMI basic mode — Supports a binary interface for program access, such as the IPMI shell (ipmish) that is included with the Baseboard Management Utility (BMU). For example, to print the System Event Log using ipmish via IPMI Basic mode, run the following command:

```
ipmish -com 1 -baud 57600 -flow cts -u root -p calvin sel get
```
- IPMI terminal mode — Supports ASCII commands that are sent from a serial terminal. This mode supports limited number of commands (including power control) and raw IPMI commands that are typed as hexadecimal ASCII characters. It allows you to view the operating system boot sequences up to BIOS, when you login to iDRAC7 through SSH or Telnet.

Related Links

[Configuring BIOS For Serial Connection](#)

[Additional Settings For IPMI Serial Terminal Mode](#)

Enabling Serial Connection Using Web Interface

Make sure to disable the RAC serial interface to enable IPMI Serial.

To configure IPMI Serial settings:

1. In the iDRAC7 Web interface, go to **Overview** → **iDRAC Settings** → **Network** → **Serial**.
2. Under **IPMI Serial**, specify the values for the attributes. For information about the options, see the *iDRAC7 Online Help*.
3. Click **Apply**.

Enabling Serial Connection IPMI Mode Using RACADM

To configure the IPMI mode:

1. Disable the RAC serial interface:

```
racadm config -g cfgSerial -o cfgSerialConsoleEnable 0
```
2. Enable the appropriate IPMI mode.

```
racadm config -g cfgIpmiSerial -o cfgIpmiSerialConnectionMode <0 or 1>
```

where, *0* indicates Terminal mode and *1* indicates Basic mode.

Enabling Serial Connection IPMI Serial Settings Using RACADM

To configure IPMI Serial settings:

1. Change the IPMI serial connection mode to the appropriate setting using the command:

```
racadm config -g cfgSerial -o cfgSerialConsoleEnable 0
```
2. Set the IPMI Serial baud rate using the command: `racadm config -g cfgIpmiSerial -o cfgIpmiSerialBaudRate <baud_rate>` where `<baud_rate>` is 9600, 19200, 57600, or 115200 bps.
3. Enable the IPMI serial hardware flow control using the command: `racadm config -g cfgIpmiSerial -o cfgIpmiSerialFlowControl 1`
4. Set the IPMI serial channel minimum privilege level using the command: `racadm config -g cfgIpmiSerial -o cfgIpmiSerialChanPrivLimit <level>`, where `<level>` is 2 (User), 3 (Operator), or 4 (Administrator).
5. Make sure that the serial MUX (external serial connector) is set correctly to the remote access device in the BIOS Setup program to configure BIOS for serial connection.

For more information about these properties, see the IPMI 2.0 specification.

Additional Settings For IPMI Serial Terminal Mode

This section provides additional configuration settings for IPMI serial terminal mode.

Configuring Additional Settings for IPMI Serial Terminal Mode Using Web Interface

To set the Terminal Mode settings:

1. In the iDRAC7 Web interface, go to **Overview** → **iDRAC Settings** → **Network** → **Serial**

The **Serial** page is displayed.
2. Enable IPMI serial.
3. Click **Terminal Mode Settings**.

The **Terminal Mode Settings** page is displayed.
4. Specify the following values:
 - Line editing
 - Delete control
 - Echo Control
 - Handshaking control
 - New line sequence
 - Input new line sequences

For information about the options, see the *iDRAC7 Online Help*.

5. Click **Apply**.

The terminal mode settings are configured.
6. Make sure that the serial MUX (external serial connector) is set correctly to the remote access device in the BIOS Setup program to configure BIOS for serial connection.

Configuring Additional Settings for IPMI Serial Terminal Mode Using RACADM

To configure the Terminal Mode settings, run the following command:`racadm config cfgIpmiSerial`

Switching Between RAC Serial and Serial Console While Using DB9 Cable

iDRAC7 supports Escape key sequences that allow switching between RAC Serial Interface communication and Serial Console on rack and tower servers.

Switching From Serial Console to RAC Serial

To switch to RAC Serial Interface communication mode when in Serial Console Mode, use the following key sequence:

`<Esc> +<Shift> <9>`

The key sequence directs you to the "iDRAC Login" prompt (if the iDRAC is set to RAC Serial mode) or to the Serial Connection mode where terminal commands can be issued if iDRAC is set to IPMI Serial Direct Connect Terminal Mode.

Switching From RAC Serial to Serial Console

To switch to Serial Console Mode when in RAC Serial Interface Communication Mode, use the following key sequence:

`<Esc> +<Shift> <q>`

When in terminal mode, to switch the connection to the Serial Console mode use:

`<Esc> +<Shift> <q>`

To go back to the terminal mode use, when connected in Serial Console mode:

`<Esc> +<Shift> <9>`

Communicating With iDRAC7 Using IPMI SOL

IPMI Serial Over LAN (SOL) allows a managed system's text-based console serial data to be redirected over iDRAC7's dedicated or shared out-of-band ethernet management network. Using SOL you can:

- Remotely access operating systems with no time-out.
- Diagnose host systems on Emergency Management Services (EMS) or Special Administrator Console (SAC) for Windows or Linux shell.
- View the progress of a servers during POST and reconfigure the BIOS setup program.

To setup the SOL communication mode:

1. Configure BIOS for serial connection.
2. Configure iDRAC7 to Use SOL.
3. Enable a supported protocol (SSH, Telnet, IPMItool).

Related Links


[Configuring BIOS For Serial Connection](#)

[Configuring iDRAC7 to Use SOL](#)

[Enabling Supported Protocol](#)

Configuring BIOS For Serial Connection

To configure BIOS for Serial Connection:

 **NOTE:** This is applicable only for iDRAC7 on rack and tower servers.

1. Turn on or restart the system.
2. Press <F2>.
3. Go to **System BIOS Settings** → **Serial Communication**.
4. Specify the following values:
 - Serial Communication — On With Console Redirection
 - Serial Port Address — COM2.

 **NOTE:** You can set the **serial communication** field to **On with serial redirection via com1** if **serial device2** in the **serial port address** field is also set to com1.

- External serial connector — Serial device 2
 - Failsafe Baud Rate — 115200
 - Remote Terminal Type — VT100/VT220
 - Redirection After Boot — Enabled
5. Click **Back** and then click **Finish**.
 6. Click **Yes** to save the changes.
 7. Press <Esc> to exit **System Setup**.

Configuring iDRAC7 to Use SOL

You can specify the SOL settings in iDRAC7 using Web interface, RACADM, or iDRAC Settings utility.

Configuring iDRAC7 to Use SOL Using iDRAC7 Web Interface


To configure IPMI Serial over LAN (SOL):

1. In the iDRAC7 Web interface, go to **Overview** → **iDRAC Settings** → **Network** → **Serial Over LAN**.
The **Serial over LAN** page is displayed.
2. Enable SOL, specify the values, and click **Apply**.
The IPMI SOL settings are configured.
3. To set the character accumulate interval and the character send threshold, select **Advanced Settings**.
The **Serial Over LAN Advanced Settings** page is displayed.
4. Specify the values for the attributes and click **Apply**.
The IPMI SOL advanced settings are configured. These values help to improve the performance.
For information about the options, see the *iDRAC7 Online Help*.


Configuring iDRAC7 to Use SOL Using RACADM

To configure IPMI Serial over LAN (SOL):

1. To enable IPMI Serial over Lan, run the command: `racadm config -g cfgIpmiSol -o cfgIpmiSolEnable 1`
2. Update the IPMI SOL minimum privilege level using the command: `racadm config -g cfgIpmiSol o cfgIpmiSolMinPrivilege <level>`, where <level> is 2 (User), 3 (Operator), 4 (Administrator).

 **NOTE:** The IPMI SOL minimum privilege level determines the minimum privilege to activate IPMI SOL. For more information, see the IPMI 2.0 specification.

3. Update the IPMI SOL baud rate using the command: `racadm config -g cfgIpmiSol -o cfgIpmiSolBaudRate <baud_rate>` where `<baud_rate>` is 9600, 19200, 57600, or 115200 bps.

 **NOTE:** To redirect the serial console over LAN, make sure that the SOL baud rate is identical to the managed system's baud rate.

4. Enable SOL for each user using the command: `racadm config -g cfgUserAdmin -o cfgUserAdminSolEnable -i <id> 2` where, `<id>` is the user's unique ID.

Enabling Supported Protocol

The supported protocols are IPMI, SSH, and Telnet.

Enabling Supported Protocol Using Web Interface


To enable SSH or Telnet, go to **Overview** → **iDRAC Settings** → **Network** → **Services** and select **Enabled** for SSH or Telnet, respectively.

To enable IPMI, go to **Overview** → **iDRAC Settings** → **Network** and select **Enable IPMI Over LAN**. Make sure that the **Encryption Key** value is all zeroes or press the backspace key to clear and change the value to NULL characters.

Enabling Supported Protocol Using RACADM

To enable the SSH or Telnet, run the command:

- Telnet- `racadm config -g cfgSerial -o cfgSerialTelnetEnable 1`
- SSH- `racadm config -g cfgSerial -o cfgSerialSshEnable 1`

 **NOTE:** To change the SSH port, run the command `racadm config -g cfgRacTuning -o cfgRacTuneSshPort <port number>`

You can use tools such as:

- IPMItool for using IPMI protocol
- Putty/OpenSSH for using SSH or Telnet protocol

Related Links

[SOL Using IPMI Protocol](#)

[SOL Using SSH or Telnet Protocol](#)

SOL Using IPMI Protocol


IPMItool <--> LAN/WAN connection <--> iDRAC7

The IPMI-based SOL utility and IPMItool uses RMCP+ delivered using UDP datagrams to port 623. The RMCP+ provides improved authentication, data integrity checks, encryption, and the ability to carry multiple types of payloads while using IPMI 2.0. For more information, see <http://ipmitool.sourceforge.net/manpage.html>.


The RMCP+ uses an 40-character hexadecimal string (characters 0-9, a-f, and A-F) encryption key for authentication. The default value is a string of 40 zeros.

An RMCP+ connection to iDRAC7 must be encrypted using the encryption Key (Key Generator (KG)Key). You can configure the encryption key using the iDRAC7 Web interface or iDRAC Settings utility.

To start SOL session using IPMItool from a management station:

 **NOTE:** If required, you can change the default SOL time-out at **Overview** → **iDRAC Settings** → **Network** → **Services**.

1. Install IPMITool from the *Dell Systems Management Tools and Documentation DVD*.
For installation instructions, see the *Software Quick Installation Guide*.
2. At the command prompt (Windows or Linux), run the command to start SOL from iDRAC7: `ipmitool -H <iDRAC7-ip-address> -I lanplus -U <login name> -P <login password> sol activate`
This connects the management station to the managed system's serial port.
3. To quit a SOL session from IPMITool, press <-> and <.> one after the other. The SOL session closes.


 **NOTE:** If a SOL session does not terminate, reset iDRAC7 and allow up to two minutes to complete booting.

SOL Using SSH or Telnet Protocol

Secure Shell (SSH) and Telnet are network protocols used to perform command line communications to iDRAC7. You can parse remote RACADM and SMCLP commands through either of these interfaces.

SSH has improved security over Telnet. iDRAC7 only supports SSH version 2 with password authentication, and is enabled by default. iDRAC7 supports up to two SSH sessions and two Telnet sessions at a time. It is recommended to use SSH as Telnet is not a secure protocol. You must use Telnet only if you cannot install an SSH client or if your network infrastructure is secure.

Use opensource programs such as PuTTY or OpenSSH that support SSH and Telnet network protocols on a management station to connect to iDRAC7.

 **NOTE:** Run OpenSSH from a VT100 or ANSI terminal emulator on Windows. Running OpenSSH at the Windows command prompt does not result in full functionality (that is, some keys do not respond and no graphics are displayed).

Before using SSH or Telnet to communicate with iDRAC7, make sure to:

1. Configure BIOS to enable Serial Console.
2. Configure SOL in iDRAC7.
3. Enable SSH or Telnet using iDRAC7 Web interface or RACADM.
Telnet (port 23)/ SSH (port 22) client <--> WAN connection <--> iDRAC7


The IPMI-based SOL that uses SSH or Telnet protocol eliminates the need for an additional utility because the serial to network translation happens within iDRAC7. The SSH or Telnet console that you use must be able to interpret and respond to the data arriving from the managed systems's serial port. The serial port usually attaches to a shell that emulates an ANSI- or VT100/VT220-terminal. The serial console is automatically redirected to the SSH or Telnet console.

Related Links


- [Using SOL From Putty On Windows](#)
- [Using SOL From OpenSSH or Telnet On Linux](#)

Using SOL From Putty On Windows

To start IPMI SOL from PuTTY on a Windows management station:

 **NOTE:** If required, you can change the default SSH or Telnet time-out at **Overview** → **iDRAC Settings** → **Network** → **Services**.

1. Run the command to connect to iDRAC7: `putty.exe [-ssh | -telnet] <login name>@<iDRAC7-ip-address> <port number>`

 **NOTE:** The port number is optional. It is required only when the port number is reassigned.

2. Run the command `console com2` or `connect` to start SOL and boot the managed system.

A SOL session from the management station to the managed system using the SSH or Telnet protocol is opened. To access the iDRAC7 command line console, follow the ESC key sequence. Putty and SOL connection behavior:


- While accessing the managed system through putty during POST, if the The Function keys and keypad option on putty is set to:
 - * VT100+ — F2 passes, but F12 cannot pass.
 - * ESC[n~ — F12 passes, but F2 cannot pass.
- In Windows, if the Emergency Management System (EMS) console is opened immediately after a host reboot, the Special Admin Console (SAC) terminal may get corrupted. Quit the SOL session, close the terminal, open another terminal, and start the SOL session using the same command.

Related Links

[Disconnecting SOL Session in iDRAC7 Command Line Console](#)

Using SOL From OpenSSH or Telnet On Linux

To start SOL from OpenSSH or Telnet on a Linux management station:

 **NOTE:** If required, you can change the default SSH or Telnet session time-out at **Overview** → **iDRAC Settings** → **Network** → **Services**.

1. Start a shell.
2. Connect to iDRAC7 using the following command:
 - For SSH: `ssh <iDRAC7-ip-address> -l <login name>`
 - For Telnet: `telnet <iDRAC7-ip-address>`

 **NOTE:** If you have changed the port number for the Telnet service from the default (port 23), add the port number to the end of the Telnet command.

3. Enter one of the following commands at the command prompt to start SOL:

- `connect`
- `console com2`

This connects iDRAC7 to the managed system's SOL port. Once a SOL session is established, iDRAC7 command line console is not available. Follow the escape sequence correctly to open the iDRAC7 command line console. The escape sequence is also printed on the screen as soon as a SOL session is connected. When the managed system is off, it takes sometime to establish the SOL session.

The `console -h com2` command displays the contents of the serial history buffer before waiting for input from the keyboard or new characters from the serial port.

The default (and maximum) size of the history buffer is 8192 characters. You can set this number to a smaller value using the command:

```
racadm config -g cfgSerial -o cfgSerialHistorySize <number>
```

4. Quit the SOL session to close an active SOL session.

Related Links

[Using Telnet Virtual Console](#)

[Configuring Backspace Key For Your Telnet Session](#)

[Disconnecting SOL Session in iDRAC7 Command Line Console](#)

Using Telnet Virtual Console

Some Telnet clients on the Microsoft operating systems may not display the BIOS setup screen correctly when BIOS Virtual Console is set for VT100/VT220 emulation. If this issue occurs, change the BIOS console to ANSI mode to update

the display. To perform this procedure in the BIOS setup menu, select **Virtual Console** → **Remote Terminal Type** → **ANSI**.

When you configure the client VT100 emulation window, set the window or application that is displaying the redirected Virtual Console to 25 rows x 80 columns to make sure correct text display. Else, some text screens may be garbled.

To use Telnet virtual console:

1. Enable **Telnet** in **Windows Component Services**.
2. Connect to the iDRAC7 using the command: `telnet <IP address>:<port number>`, where `IP address` is the IP address for the iDRAC7 and `port number` is the Telnet port number (if you are using a new port).

Configuring Backspace Key For Your Telnet Session

Depending on the Telnet client, using the <Backspace> key may produce unexpected results. For example, the session may echo ^h. However, most Microsoft and Linux Telnet clients can be configured to use the <Backspace> key.

To configure a Linux Telnet session to use the <Backspace> key, open a command prompt and type `stty erase ^h`. At the prompt, type `telnet`.

To configure Microsoft Telnet clients to use the <Backspace> key:

1. Open a command prompt window (if required).
2. If you are not running a Telnet session, type `telnet`. If you are running a Telnet session, press <Ctrl><]>.
3. At the prompt, type `set bsasdel`.

The message `Backspace will be sent as delete` is displayed.

Disconnecting SOL Session in iDRAC7 Command Line Console

The commands to disconnect a SOL session are based on the utility. You can exit the utility only when a SOL session is completely terminated.

To disconnect a SOL session, terminate the SOL session from the iDRAC7 command line console:

- To quit SOL redirection, press <Enter>, <Esc>, and then <␣>. The SOL session closes.
- To quit a SOL session from Telnet on Linux, press and hold <Ctrl>+]. A Telnet prompt is displayed. Enter `quit` to exit Telnet.
- If a SOL session is not terminated completely in the utility, other SOL sessions may not be available. To resolve this, terminate the command line console in the Web interface under **Overview** → **iDRAC Settings** → **Sessions**.

Communicating With iDRAC7 Using IPMI Over LAN

You must configure IPMI over LAN for iDRAC7 to enable or disable IPMI commands over LAN channels to any external systems. If it is not configuration is not done, then external systems cannot communicate with the iDRAC7 server using IPMI commands.

Configuring IPMI Over LAN Using Web Interface

To configure IPMI over LAN:

1. In the iDRAC7 Web interface, go to **Overview** → **iDRAC Settings** → **Network**.
The **Network** page is displayed.
2. Under **IPMI Settings**, specify the values for the attributes and click **Apply**.
For information about the options, see the *iDRAC7 Online Help*.
The IPMI over LAN settings are configured.

Configuring IPMI Over LAN Using iDRAC Settings Utility

To configure IPMI over LAN:

1. In the **iDRAC Settings Utility**, go to **Network**.
The **iDRAC Settings Network** page is displayed.
2. For **IPMI Settings**, specify the values.
For information about the options, see the *iDRAC Settings Utility Online Help*.
3. Click **Back**, click **Finish**, and then click **Yes**.
The IPMI over LAN settings are configured.


Configuring IPMI Over LAN Using RACADM

To configure IPMI over LAN:

1. Enable IPMI over LAN using the command: `racadm config -g cfgIpmiLan -o cfgIpmiLanEnable 1`

 **NOTE:** This setting determines the IPMI commands that are executed using IPMI over LAN interface. For more information, see the IPMI 2.0 specifications at intel.com.

2. Update the IPMI channel privileges using the command: `racadm config -g cfgIpmiLan -o cfgIpmiLanPrivilegeLimit <level>` where, where <level> is one of the following: 2 (User), 3 (Operator) or 4 (Administrator)
3. Set the IPMI LAN channel encryption key (if required) using the command: `racadm config -g cfgIpmiLan -o cfgIpmiEncryptionKey <key>` where <key> is a 20-character encryption key in a valid hexadecimal format.

 **NOTE:** The iDRAC7 IPMI supports the RMCP+ protocol. For more information, see the IPMI 2.0 specifications at intel.com.

Enabling or Disabling Remote RACADM

You can enable or disable remote RACADM using the iDRAC7 Web interface or RACADM. You can run up to five remote RACADM sessions in parallel.


Enabling or Disabling Remote RACADM Using Web Interface

To enable or disable remote RACADM:

1. In iDRAC7 Web interface, go to **Overview** → **iDRAC Settings** → **Network** → **Services**.
The **Services** page is displayed.
2. Under **Remote RACADM**, select **Enabled**. Else, select **Disabled**.
3. Click **Apply**.
The remote RACADM is enabled or disabled based on the selection.

Enabling or Disabling Remote RACADM Using RACADM

The RACADM remote capability is enabled by default. If disabled, type the command: `racadm config -g cfgRacTuning -o cfgRacTuneRemoteRacadmEnable 1` to enable. To disable the remote capability, type the command: `racadm config -g cfgRacTuning -o cfgRacTuneRemoteRacadmEnable 0`

 **NOTE:** It is recommended to run these commands on the local system.

Disabling Local RACADM


The local RACADM is enabled by default. To disable, see [Disabling Access to Modify iDRAC7 Configuration Settings on Host System](#).

Enabling IPMI on Managed System

On a managed system, use the Dell Open Manage Server Administrator to enable or disable IPMI. For more information, see the *Dell Open Manage Server Administrator's User Guide* at support.dell.com/manuals.

Configuring Linux for Serial Console During Boot

The following steps are specific to the Linux GRand Unified Bootloader (GRUB). Similar changes are required if a different boot loader is used.

 **NOTE:** When you configure the client VT100 emulation window, set the window or application that is displaying the redirected Virtual Console to 25 rows x 80 columns to make sure the correct text displays. Else, some text screens may be garbled.

Edit the `/etc/grub.conf` file as follows:

1. Locate the General Setting sections in the file and add the following:
`serial --unit=1 --speed=57600 terminal --timeout=10 serial`
2. Append two options to the kernel line:
`kernel console=ttyS1,115200n8r console=tty1`
3. Disable GRUB's graphical interface and use the text-based interface. Else, the GRUB screen is not displayed in RAC Virtual Console. To disable the graphical interface, comment-out the line starting with `splashimage`.

The following example provides a sample `/etc/grub.conf` file that shows the changes described in this procedure.

```
# grub.conf generated by anaconda
# Note that you do not have to rerun grub after making changes to this file
# NOTICE: You do not have a /boot partition. This means that all
# kernel and initrd paths are relative to /, e.g.
# root (hd0,0)
# kernel /boot/vmlinuz-version ro root=/dev/sda1
# initrd /boot/initrd-version.img
#boot=/dev/sda
default=0
timeout=10
#splashimage=(hd0,2)/grub/splash.xpm.gz

serial --unit=1 --speed=57600
terminal --timeout=10 serial

title Red Hat Linux Advanced Server (2.4.9-e.3smp) root (hd0,0)
```

```
kernel /boot/vmlinuz-2.4.9-e.3smp ro root=/dev/sda1 hda=ide-scsi
console=ttyS0
console=ttyS1,115200n8r
initrd /boot/initrd-2.4.9-e.3smp.img
title Red Hat Linux Advanced Server-up (2.4.9-e.3) root (hd0,00)
kernel /boot/vmlinuz-2.4.9-e.3 ro root=/dev/sda1 s
initrd /boot/initrd-2.4.9-e.3.im
```

4. To enable multiple GRUB options to start Virtual Console sessions through the RAC serial connection, add the following line to all options:

```
console=ttyS1,115200n8r console=tty1
```

The example shows `console=ttyS1,57600` added to the first option.

Enabling Login to the Virtual Console After Boot

In the file `/etc/inittab`, add a new line to configure `agetty` on the COM2 serial port:

```
co:2345:respawn:/sbin/agetty -h -L 57600 ttyS1 ansi
```

The following example shows a sample file with the new line.

```
#inittab This file describes how the INIT process should set up
#the system in a certain run-level.
#Author:Miquel van Smoorenburg
#Modified for RHS Linux by Marc Ewing and Donnie Barnes
#Default runlevel. The runlevels used by RHS are:
#0 - halt (Do NOT set initdefault to this)
#1 - Single user mode
#2 - Multiuser, without NFS (The same as 3, if you do not have #networking)
#3 - Full multiuser mode
#4 - unused
#5 - X11
#6 - reboot (Do NOT set initdefault to this)
id:3:initdefault:
#System initialization.
si::sysinit:/etc/rc.d/rc.sysinit
l0:0:wait:/etc/rc.d/rc 0
l1:1:wait:/etc/rc.d/rc 1
l2:2:wait:/etc/rc.d/rc 2
l3:3:wait:/etc/rc.d/rc 3
l4:4:wait:/etc/rc.d/rc 4
l5:5:wait:/etc/rc.d/rc 5
l6:6:wait:/etc/rc.d/rc 6
#Things to run in every runlevel.
ud::once:/sbin/update
ud::once:/sbin/update
#Trap CTRL-ALT-DELETE
ca::ctrlaltdel:/sbin/shutdown -t3 -r now
#When our UPS tells us power has failed, assume we have a few
#minutes of power left. Schedule a shutdown for 2 minutes from now.
#This does, of course, assume you have power installed and your
#UPS is connected and working correctly.
pf::powerfail:/sbin/shutdown -f -h +2 "Power Failure; System Shutting Down"
#If power was restored before the shutdown kicked in, cancel it.
pr:12345:powerokwait:/sbin/shutdown -c "Power Restored; Shutdown Cancelled"

#Run gettys in standard runlevels
co:2345:respawn:/sbin/agetty -h -L 57600 ttyS1 ansi
1:2345:respawn:/sbin/mingetty tty1
2:2345:respawn:/sbin/mingetty tty2
3:2345:respawn:/sbin/mingetty tty3
4:2345:respawn:/sbin/mingetty tty4
5:2345:respawn:/sbin/mingetty tty5
```


```
6:2345:respawn:/sbin/mingetty tty6

#Run xdm in runlevel 5
#xdm is now a separate service
x:5:respawn:/etc/X11/prefdm -nodaemon
```

In the file **/etc/securetty** add a new line with the name of the serial tty for COM2:

```
ttyS1
```

The following example shows a sample file with the new line.

 **NOTE:** Use the Break Key Sequence (~B) to execute the Linux **Magic SysRq** key commands on serial console using IPMI Tool.

```
vc/1
vc/2
vc/3
vc/4
vc/5
vc/6
vc/7
vc/8
vc/9
vc/10
vc/11
tty1
tty2
tty3
tty4
tty5
tty6
tty7
tty8
tty9
tty10
tty11
ttyS1
```

Supported SSH Cryptography Schemes

To communicate with iDRAC7 using SSH protocol, it supports multiple cryptography schemes listed in the following table.

Table 10. SSH Cryptography Schemes

| Scheme Type | Scheme |
|-------------------------|--|
| Asymmetric Cryptography | Diffie-Hellman DSA/DSS 512-1024 (random) bits per NIST specification |
| Symmetric Cryptography | <ul style="list-style-type: none">• AES256-CBC• RIJNDAEL256-CBC• AES192-CBC• RIJNDAEL192-CBC• AES128-CBC• RIJNDAEL128-CBC• BLOWFISH-128-CBC• 3DES-192-CBC |

| Scheme Type | Scheme |
|--------------------|--|
| | <ul style="list-style-type: none"> • ARCFOUR-128 |
| Message Integrity | <ul style="list-style-type: none"> • HMAC-SHA1-160 • HMAC-SHA1-96 • HMAC-MD5-128 • HMAC-MD5-96 |
| Authentication | Password |
| PKA Authentication | Public-private key pairs |


Using Public Key Authentication For SSH

iDRAC7 supports the Public Key Authentication (PKA) over SSH. This is a licensed feature. When the PKA over SSH is set up and used correctly, you need not enter the user name or password while logging into iDRAC7. This is useful for setting up automated scripts that perform various functions. The uploaded keys must be in RFC 4716 or openssh format. Else, you must convert the keys into that format.

In any scenario, a pair of private and public key must be generated on the management station. The public key is uploaded to iDRAC7 local user and private key is used by the SSH client to establish the trust relationship between the management station and iDRAC7.

You can generate the public or private key pair using:

- *PuTTY Key Generator* application for clients running Windows
- *ssh-keygen* CLI for clients running Linux.

 **CAUTION:** This privilege is normally reserved for users who are members of the Administrator user group on iDRAC7. However, users in the 'Custom' user group can be assigned this privilege. A user with this privilege can modify any user's configuration. This includes creation or deletion of any user, SSH Key management for users, and so on. For these reasons, assign this privilege carefully.

 **CAUTION:** The capability to upload, view, and/ or delete SSH keys is based on the 'Configure Users' user privilege. This privilege allows user(s) to configure another user's SSH key. You should grant this privilege carefully.

Generating Public Keys for Windows

To use the *PuTTY Key Generator* application to create the basic key:


1. Start the application and select either SSH-2 RSA or SSH-2 DSA for the type of key to generate. (SSH-1 is not supported). The supported key generation algorithms are RSA and DSA only.
2. Enter the number of bits for the key. For RSA, it is between 768 and 4096 bits and for DSA, it 1024 bits.
3. Click **Generate** and move the mouse in the window as directed.
The keys are generated.
4. You can modify the key comment field.
5. Enter a passphrase to secure the key.
6. Save the public and private key.

Generating Public Keys for Linux


To use the *ssh-keygen* application to create the basic key, open a terminal window and at the shell prompt, enter `ssh-keygen -t rsa -b 1024 -C testing`


where:

- `-t` is either *dsa* or *rsa*.
- `-b` specifies the bit encryption size between 768 and 4096.
- `-C` allows modifying the public key comment and is optional.

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

Follow the instructions. After the command executes, upload the public file.

 **CAUTION:** Keys generated from the Linux management station using `ssh-keygen` are in non-4716 format. Convert the keys into the 4716 format using `ssh-keygen -e -f /root/.ssh/id_rsa.pub > std_rsa.pub`. Do not change the permissions of the key file. The conversion must be done using default permissions.

 **NOTE:** iDRAC7 does not support ssh-agent forward of keys.

Uploading SSH Keys

You can upload up to four public keys *per user* to use over an SSH interface. Before adding the public keys, make sure that you view the keys if they are set up, so that a key is not accidentally overwritten.

When adding new public keys, make sure that the existing keys are not at the index where the new key is added. iDRAC7 does not perform checks to make sure previous key(s) are deleted before a new key(s) are added. When a new key is added, it is usable if the SSH interface is enabled.

Uploading SSH Keys Using Web Interface

To upload the SSH keys:


1. In the iDRAC7 Web interface, go to **Overview** → **iDRAC Settings** → **Network** → **User Authentication** → **Local Users**.
The **Users** page is displayed.
2. In the **User ID** column, click a user ID number.
The **Users Main Menu** page is displayed.
3. Under **SSH Key Configurations**, select **Upload SSH Key(s)** and click **Next**.
The **Upload SSH Key(s)** page is displayed.
4. Upload the SSH keys in one of the following ways:
 - Upload the key file.
 - Copy the contents of the key file into the text box

For more information, see iDRAC7 Online Help.

5. Click **Apply**.

Uploading SSH Keys Using RACADM


To upload the SSH keys, run the following command:

 **NOTE:** You cannot upload and copy a key at the same time.

- For local RACADM: `racadm sshpkauth -i <2 to 16> -k <1 to 4> -f <filename>`
- From remote RACADM using Telnet or SSH: `racadm sshpkauth -i <2 to 16> -k <1 to 4> -t <key-text>`

For example, to upload a valid key to iDRAC7 User ID 2 in the first key space using a file, run the following command:

```
$ racadm sshpkauth -i 2 -k 1 -f pkkey.key
```

 **NOTE:** The `-f` option is not supported on telnet/ssh/serial RACADM.

Viewing SSH Keys

You can view the keys that are uploaded to iDRAC7.

Viewing SSH Keys Using Web Interface

To view the SSH keys:

1. In Web interface, go to **Overview** → **iDRAC Settings** → **Network** → **User Authentication** → **Local Users** .
The **Users** page is displayed.
2. In the **User ID** column, click a user ID number.
The **Users Main Menu** page is displayed.
3. Under **SSH Key Configurations**, select **View/Remove SSH Key(s)** and click **Next**.
The **View/Remove SSH Key(s)** page is displayed with the key details.

Viewing SSH Keys Using RACADM

To view the SSH keys, run the following command:

- Specific key — `racadm sshpkauth -i <2 to 16> -v -k <1 to 4>`
- All keys — `racadm sshpkauth -i <2 to 16> -v -k all`

Deleting SSH Keys

Before deleting the public keys, make sure that you view the keys if they are set up, so that a key is not accidentally deleted.

Deleting SSH Keys Using Web Interface

To delete the SSH key(s):

1. In Web interface, go to **Overview** → **iDRAC Settings** → **Network** → **User Authentication** → **Local Users** .
The **Users** page is displayed.
2. In the **User ID** column, click a user ID number.
The **Users Main Menu** page is displayed.
3. Under **SSH Key Configurations**, select **View/Remove SSH Key(s)** and click **Next**.
The **View/Remove SSH Key(s)** page displays the key details.
4. Select **Remove for the key(s) you want to delete, and click Apply**.
The selected key(s) is deleted.

Deleting SSH Keys Using RACADM

To delete the SSH key(s), run the following commands:

- Specific key — `racadm sshpkauth -i <2 to 16> -d -k <1 to 4>`
- All keys — `racadm sshpkauth -i <2 to 16> -d -k all`

Configuring User Accounts and Privileges

You can setup user accounts with specific privileges (*role-based authority*) to manage your system using iDRAC7 and maintain system security. By default iDRAC7 is configured with a local administrator account. This default user name is *root* and the password is *calvin*. As an administrator, you can setup user accounts to allow other users to access iDRAC7.

You can setup local users or use directory services such as Microsoft Active Directory or LDAP to setup user accounts. Using a directory service provides a central location for managing authorized user accounts.

iDRAC7 supports role-based access to users with a set of associated privileges. The roles are administrator, operator, read only, or none. The role defines the maximum privileges available.

Related Links

[Configuring Local Users](#)

[Configuring Active Directory Users](#)

[Configuring Generic LDAP Users](#)

Configuring Local Users

You can configure up to 16 local users in iDRAC7 with specific access permissions. Before you create an iDRAC7 user, verify if any current users exist. You can set user names, passwords, and roles with the privileges for these users. The user names and passwords can be changed using any of the iDRAC7 secured interfaces (that is, Web interface, RACADM or WS-MAN).

Configuring Local Users Using iDRAC7 Web Interface

To add and configure local iDRAC7 users:



NOTE: You must have Configure Users permission to create an iDRAC7 user.


1. In the iDRAC7 Web interface, go to **Overview** → **iDRAC Settings** → **User Authentication** → **Local Users** .
The **Users** page is displayed.
2. In the **User ID** column, click a user ID number.



NOTE: User 1 is reserved for the IPMI anonymous user and you cannot change this configuration.

- The **User Main Menu** page is displayed.
3. Select **Configure User** and click **Next**.
The **User Configuration** page is displayed.
4. Enable the user ID and specify the user name, password, and access privileges for the user. For more information about the options, see the *iDRAC7 Online Help*.
5. Click **Apply**. The user is created with the required privileges.

Configuring Local Users Using RACADM


 **NOTE:** You must be logged in as user **root** to execute RACADM commands on a remote Linux system.

You can configure single or multiple iDRAC7 users using RACADM.

To configure multiple iDRAC7 users with identical configuration settings, perform one of the following procedures:

- Use the RACADM examples in this section as a guide to create a batch file of RACADM commands and then execute the batch file on each managed system.
- Create the iDRAC7 configuration file and execute the **racadm config** subcommand on each managed system using the same configuration file.

If you are configuring a new iDRAC7 or if you have used the **racadm racresetcfg** command, the only current user is **root** with the password **calvin**. The **racresetcfg** subcommand resets the iDRAC7 to the default values.

 **NOTE:** Users can be enabled and disabled over time. As a result, a user may have a different index number on each iDRAC7.

To verify if a user exists, type the following command at the command prompt:

```
racadm getconfig -u <username >
```

OR

Type the following command once for each index (1–16):

```
racadm getconfig -g cfgUserAdmin -i <index>
```

 **NOTE:** You can also type **racadm getconfig -f <myfile.cfg>** and view or edit the **myfile.cfg** file, which includes all iDRAC7 configuration parameters.

Several parameters and object IDs are displayed with their current values. Two objects of importance are:

```
# cfgUserAdminIndex=XX
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 taken by that user name.

When you manually enable or disable a user with the **racadm config** subcommand, you *must* specify the index with the **-i** option.

Observe that the **cfgUserAdminIndex** object displayed in the previous example contains a '#' character. It indicates that it is a read-only object. Also, if you use the **racadm config -f racadm.cfg** command to specify any number of groups/objects to write, the index cannot be specified. A new user is added to the first available index. This behavior allows more flexibility in configuring multiple iDRAC7 with the same settings.

Adding iDRAC7 User Using RACADM

To add a new user to the RAC configuration, perform the following:

1. Set the user name.
2. Set the password.
3. Set the following user privileges:
 - iDRAC7
 - LAN
 - Serial Port
 - Serial Over LAN

4. Enable the user.

Example:

The following example describes how to add a new user named "John" with a "123456" password and LOGIN privileges to the RAC.

```
racadm config -g cfgUserAdmin -o cfgUserAdminUserName -i 3 john
racadm config -g cfgUserAdmin -o cfgUserAdminPassword -i 3 123456
racadm config -g cfgUserAdmin -i 3 -o cfgUserAdminPrivilege 0x00000001
racadm config -g cfgUserAdmin -i 3 -o cfgUserAdminIpmiLanPrivilege 2
racadm config -g cfgUserAdmin -i 3 -o cfgUserAdminIpmiSerialPrivilege 2
racadm config -g cfgUserAdmin -i 3 -o cfgUserAdminSolEnable 1
racadm config -g cfgUserAdmin -i 3 -o cfgUserAdminEnable 1
```

To verify, use one of the following commands:

```
racadm getconfig -u john
racadm getconfig -g cfgUserAdmin -i 3
```

For more information on the RACADM commands, see the *RACADM Command Line Reference Guide for iDRAC7 and CMC* available at support.dell.com/manuals.

Removing iDRAC7 User

When using RACADM, users must be disabled manually and on an individual basis. Users cannot be deleted using a configuration file.

To delete an iDRAC7 user, the command syntax is:

```
racadm config -g cfgUserAdmin -o cfgUserAdminUserName
-i <index> ""
```

A null string of double quote characters ("") instructs iDRAC7 to remove the user configuration at the specified index and reset the user configuration to the original factory defaults.

Enabling iDRAC7 User With Permissions

To enable a user with specific administrative permissions (role-based authority):

1. Locate an available user index using the command syntax:

```
racadm getconfig -g cfgUserAdmin -i <index>
```
2. Type the following commands with the new user name and password.

```
racadm config -g cfgUserAdmin -o cfgUserAdminPrivilege -i <index> <user
privilege bitmask value>
```

 **NOTE:** For a list of valid bit mask values for specific user privileges, see the *RACADM Command Line Reference Guide for iDRAC7 and CMC* available at support.dell.com/manuals. The default privilege value is 0, which indicates the user has no privileges enabled.

Configuring Active Directory Users

If your company uses the Microsoft Active Directory software, you can configure the software to provide access to iDRAC7, allowing you to add and control iDRAC7 user privileges to your existing users in your directory service. This is a licensed feature.



NOTE: Using Active Directory to recognize iDRAC7 users is supported on the Microsoft Windows 2000, Windows Server 2003, and Windows Server 2008 operating systems.

You can configure user authentication through Active Directory to log in to the iDRAC7. You can also provide role-based authority, which enables an administrator to configure specific privileges for each user.

The iDRAC7 role and privilege names have changed from earlier generation of servers. The role names are:

Table 11. iDRAC7 Roles

| Prior Generation | Current Generation | Privileges |
|------------------|--------------------|---|
| Administrator | Administrator | Login, Configure, Configure Users, Logs, System Control, Access Virtual Console, Access Virtual Media, System Operations, Debug |
| Power User | Operator | Login, Configure, System Control, Access Virtual Console, Access Virtual Media, System Operations, Debug |
| Guest User | Read Only | Login |
| None | None | None |

Table 12. iDRAC7 User Privileges

| Prior Generation | Current Generation | Description |
|--|------------------------|--|
| Login to iDRAC | Login | Enables the user to log in to iDRAC. |
| Configure iDRAC | Configure | Enables the user to configure iDRAC. |
| Configure Users | Configure Users | Enables the user to allow specific users to access the system. |
| Clear Logs | Logs | Enables the user to only clear the System Event Log (SEL). |
| Execute Server Control Commands | System Control | Enables the user to execute RACADM commands. |
| Access Virtual Console Redirection (for blade servers) | Access Virtual Console | Enables the user to run Virtual Console. |
| Access Virtual Console (for rack and tower servers) | | |
| Access Virtual Media | Access Virtual Media | Enables the user to run and use Virtual Media. |
| Test Alerts | System Operations | Enables the user to send test alerts to a specific user. |
| Execute Diagnostic Commands | Debug | Enables the user to run diagnostic commands. |

Related Links

- [Prerequisites for Using Active Directory Authentication for iDRAC7](#)
- [Supported Active Directory Authentication Mechanisms](#)

Prerequisites for Using Active Directory Authentication for iDRAC7

To use the Active Directory authentication feature of iDRAC7, make sure that you have:

- Deployed an Active Directory infrastructure. See the Microsoft website for more information.
- Integrated PKI into the Active Directory infrastructure. iDRAC7 uses the standard Public Key Infrastructure (PKI) mechanism to authenticate securely into the Active Directory. See the Microsoft website for more information.
- Enabled the Secure Socket Layer (SSL) on all domain controllers that iDRAC7 connects to for authenticating to all the domain controllers.

Related Links

[Enabling SSL on Domain Controller](#)

Enabling SSL on Domain Controller

When iDRAC7 authenticates users with an Active Directory domain controller, it starts an SSL session with the domain controller. At this time, the domain controller must publish a certificate signed by the Certificate Authority (CA)—the root certificate of which is also uploaded into iDRAC7. For iDRAC7 to authenticate to *any* domain controller—whether it is the root or the child domain controller—that domain controller must have an SSL-enabled certificate signed by the domain's CA.

If you are using Microsoft Enterprise Root CA to *automatically* assign all your domain controllers to an SSL certificate, you must:

1. Install the SSL certificate on each domain controller.
2. Export the Domain Controller Root CA Certificate to iDRAC7.
3. Import iDRAC7 Firmware SSL Certificate.

Related Links

[Installing SSL Certificate For Each Domain Controller](#)

[Exporting Domain Controller Root CA Certificate to iDRAC7](#)


[Importing iDRAC7 Firmware SSL Certificate](#)

Installing SSL Certificate For Each Domain Controller

To install the SSL certificate for each controller:

1. Click **Start** → **Administrative Tools** → **Domain Security Policy**.
2. Expand the **Public Key Policies** folder, right-click **Automatic Certificate Request Settings** and click **Automatic Certificate Request**.
The **Automatic Certificate Request Setup Wizard** is displayed.
3. Click **Next** and select **Domain Controller**.
4. Click **Next** and click **Finish**. The SSL certificate is installed.

Exporting Domain Controller Root CA Certificate to iDRAC7

 **NOTE:** If your system is running Windows 2000 or if you are using standalone CA, the following steps may vary.

To export the domain controller root CA certificate to iDRAC7:

1. Locate the domain controller that is running the Microsoft Enterprise CA service.
2. Click **Start** → **Run**.
3. Enter `mmc` and click **OK**.
4. In the **Console 1** (MMC) window, click **File** (or **Console** on Windows 2000 systems) and select **Add/Remove Snap-in**.
5. In the **Add/Remove Snap-In** window, click **Add**.
6. In the **Standalone Snap-In** window, select **Certificates** and click **Add**.
7. Select **Computer** and click **Next**.
8. Select **Local Computer**, click **Finish**, and click **OK**.


9. In the **Console 1** window, go to **Certificates Personal Certificates** folder.
10. Locate and right-click the root CA certificate, select **All Tasks**, and click **Export...**
11. In the **Certificate Export Wizard**, click **Next**, and select **No do not export the private key**.
12. Click **Next** and select **Base-64 encoded X.509 (.cer)** as the format.
13. Click **Next** and save the certificate to a directory on your system.
14. Upload the certificate you saved in step 13 to iDRAC7.

Importing iDRAC7 Firmware SSL Certificate

iDRAC7 SSL certificate is the identical certificate used for iDRAC7 Web server. All iDRAC7 controllers are shipped with a default self-signed certificate.

If the Active Directory Server is set to authenticate the client during an SSL session initialization phase, you need to upload iDRAC7 Server certificate to the Active Directory Domain controller. This additional step is not required if the Active Directory does not perform a client authentication during an SSL session's initialization phase.

 **NOTE:** If your system is running Windows 2000, the following steps may vary.

 **NOTE:** If iDRAC7 firmware SSL certificate is CA-signed and the certificate of that CA is already in the domain controller's Trusted Root Certificate Authority list, do not perform the steps in this section.

To import iDRAC7 firmware SSL certificate to all domain controller trusted certificate lists:

1. Download iDRAC7 SSL certificate using the following RACADM command:

```
racadm sslcertdownload -t 0x1 -f <RAC SSL certificate>
```
2. On the domain controller, open an **MMC Console** window and select **Certificates** → **Trusted Root Certification Authorities**.
3. Right-click **Certificates**, select **All Tasks** and click **Import**.
4. Click **Next** and browse to the SSL certificate file.
5. Install iDRAC7 SSL Certificate in each domain controller's **Trusted Root Certification Authority**.
 If you have installed your own certificate, make sure that the CA signing your certificate is in the **Trusted Root Certification Authority** list. If the Authority is not in the list, you must install it on all your domain controllers.
6. Click **Next** and select whether you want Windows to automatically select the certificate store based on the type of certificate, or browse to a store of your choice.
7. Click **Finish** and click **OK**. The iDRAC7 firmware SSL certificate is imported to all domain controller trusted certificate lists.

Supported Active Directory Authentication Mechanisms

You can use Active Directory to define iDRAC7 user access using two methods:

- *Standard schema* solution, which uses Microsoft's default Active Directory group objects only.
- *Extended schema* solution, which has customized Active Directory objects. All the access control objects are maintained in Active Directory. It provides maximum flexibility to configure user access on different iDRAC7s with varying privilege levels.

Related Links

[Standard Schema Active Directory Overview](#)

[Extended Schema Active Directory Overview](#)

Standard Schema Active Directory Overview

As shown in the following figure, using standard schema for Active Directory integration requires configuration on both Active Directory and iDRAC7.

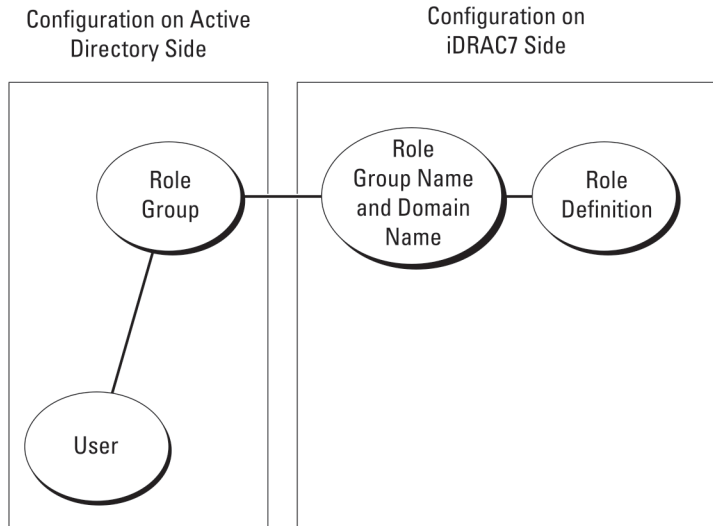



Figure 1. Configuration of iDRAC7 with Active Directory Standard Schema

In Active Directory, a standard group object is used as a role group. A user who has iDRAC7 access is a member of the role group. To give this user access to a specific iDRAC7, the role group name and its domain name need to be configured on the specific iDRAC7. The role and the privilege level is defined on each iDRAC7 and not in the Active Directory. You can configure up to five role groups in each iDRAC7. Table reference no shows the default role group privileges.

Table 13. Default Role Group Privileges

| Role Groups | Default Privilege Level | Permissions Granted | Bit Mask |
|--------------|-------------------------|---|------------|
| Role Group 1 | None | Login to iDRAC, Configure iDRAC, Configure Users, Clear Logs, Execute Server Control Commands, Access Virtual Console, Access Virtual Media, Test Alerts, Execute Diagnostic Commands | 0x000001ff |
| Role Group 2 | None | Login to iDRAC, Configure iDRAC, Execute Server Control Commands, Access Virtual Console, Access Virtual Media, Test Alerts, Execute Diagnostic Commands | 0x000000f9 |
| Role Group 3 | None | Login to iDRAC | 0x00000001 |
| Role Group 4 | None | No assigned permissions | 0x00000000 |
| Role Group 5 | None | No assigned permissions | 0x00000000 |

 **NOTE:** The Bit Mask values are used only when setting Standard Schema with the RACADM.

Single Domain Versus Multiple Domain Scenarios

If all the login users and role groups, including the nested groups, are in the same domain, then only the domain controllers' addresses must be configured on iDRAC7. In this single domain scenario, any group type is supported.

If all the login users and role groups, or any of the nested groups, are from multiple domains, then Global Catalog server addresses must be configured on iDRAC7. In this multiple domain scenario, all the role groups and nested groups, if any, must be a Universal Group type.

Configuring Standard Schema Active Directory

To configure iDRAC7 for a Active Directory login access:


1. On an Active Directory server (domain controller), open the Active Directory Users and Computers Snap-in.
2. Create a group or select an existing group. Add the Active Directory user as a member of the Active Directory group to access iDRAC7.
3. Configure the group name, domain name, and the role privileges on iDRAC7 using the iDRAC7 Web interface or RACADM.

Related Links

[Configuring Active Directory With Standard Schema Using iDRAC7 Web Interface](#)

[Configuring Active Directory With Standard Schema Using RACADM](#)

Configuring Active Directory With Standard Schema Using iDRAC7 Web Interface

 **NOTE:** For information about the various fields, see the *iDRAC7 Online Help*.

1. In the iDRAC7 Web interface, go to **Overview** → **iDRAC Settings** → **User Authentication** → **Directory Services** → **Microsoft Active Directory**.

The **Active Directory summary** page is displayed.

2. Click **Configure Active Directory**.


The **Active Directory Configuration and Management Step 1 of 4** page is displayed.

3. Optionally, enable certificate validation and upload the CA-signed digital certificate used during initiation of SSL connections when communicating with the Active Directory (AD) server. For this, the Domain Controllers and Global Catalog FQDN must be specified. This is done in the next steps. And hence the DNS should be configured properly in the network settings.

4. Click **Next**.

The **Active Directory Configuration and Management Step 2 of 4** page is displayed.

5. Enable Active Directory and specify the location information about Active Directory servers and user accounts. Also, specify the time iDRAC7 must wait for responses from Active Directory during iDRAC7 login.

 **NOTE:** If certificate validation is enabled, specify the Domain Controller Server addresses and the Global Catalog FQDN. Make sure that DNS is configured correctly under **Overview** → **iDRAC Settings** → **Network**.

6. Click **Next**. The **Active Directory Configuration and Management Step 3 of 4** page is displayed.

7. Select **Standard Schema** and click **Next**.

The **Active Directory Configuration and Management Step 4a of 4** page is displayed.

8. Enter the location of Active Directory global catalog server(s) and specify privilege groups used to authorize users.

9. Click a **Role Group** to configure the control authorization policy for users under the standard schema mode.

The **Active Directory Configuration and Management Step 4b of 4** page is displayed.

10. Specify the privileges and click **Apply**.

The settings are applied and the **Active Directory Configuration and Management Step 4a of 4** page is displayed.

11. Click **Finish**. The Active Directory settings for standard schema is configured.

Configuring Active Directory With Standard Schema Using RACADM


To configure iDRAC7 Active Directory with Standard Schema using the RACADM:


1. At the racadm command prompt, run the following 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 [Default Role Group Privileges](#).


```
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 three addresses is required to be configured. iDRAC7 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. In 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.

To enforce the certificate validation during SSL handshake (optional):

```
racadm config -g cfgActiveDirectory -o cfgADCertValidationEnable 1
```

In this case, you must upload the CA certificate using the following RACADM command:

```
racadm sslcertupload -t 0x2 -f <ADS root CA certificate>
```

 **NOTE:** If certificate validation is enabled, specify the Domain Controller Server addresses and the Global Catalog FQDN. Make sure that DNS is configured correctly under **Overview** → **iDRAC Settings** → **Network**.

Using the following RACADM command may be optional.

```
racadm sslcertdownload -t 0x1 -f <RAC SSL certificate>
```

2. If DHCP is enabled on iDRAC7 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 iDRAC7 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.

Extended Schema Active Directory Overview

Using the extended schema solution requires the Active Directory schema extension.

Active Directory Schema Extensions

The Active Directory data is a distributed database of *attributes* and *classes*. The Active Directory schema includes the rules that determine the type of data that can be added or included in the database. The user class is one example of a *class* that is stored in the database. Some example user class attributes can include the user's first name, last name, phone number, and so on. You can extend the Active Directory database by adding your own unique *attributes* and *classes* for specific requirements. Dell has extended the schema to include the necessary changes to support remote management authentication and authorization using Active Directory.

Each *attribute* or *class* that is added to an existing Active Directory Schema must be defined with a unique ID. To maintain unique IDs across the industry, Microsoft maintains a database of Active Directory Object Identifiers (OIDs) so that when companies add extensions to the schema, they can be guaranteed to be unique and not to conflict with each other. To extend the schema in Microsoft's Active Directory, Dell received unique OIDs, unique name extensions, and uniquely linked attribute IDs for the attributes and classes that are added into the directory service:

- Extension is: dell
- Base OID is: 1.2.840.113556.1.8000.1280
- RAC LinkID range is: 12070 to 12079

Overview of iDRAC7 Schema Extensions

Dell has extended the schema to include an *Association*, *Device*, and *Privilege* property. The *Association* property is used to link together the users or groups with a specific set of privileges to one or more iDRAC7 devices. This model provides an administrator maximum flexibility over the different combinations of users, iDRAC7 privileges, and iDRAC7 devices on the network without much complexity.

For each physical iDRAC7 device on the network that you want to integrate with Active Directory for authentication and authorization, create at least one association object and one iDRAC7 device object. You can create multiple association objects, and each association object can be linked to as many users, groups of users, or iDRAC7 device objects as required. The users and iDRAC7 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 iDRAC7 device objects) to only one privilege object. This example allows an administrator to control each user's privileges on specific iDRAC7 devices. iDRAC7 device object is the link to iDRAC7 firmware for querying Active Directory for authentication and authorization. When iDRAC7 is added to the network, the administrator must configure iDRAC7 and its device object with its Active Directory name so that users can perform authentication and authorization with Active Directory. Additionally, the administrator must add iDRAC7 to at least one association object for users to authenticate.

The following figure shows that the association object provides the connection that is needed for the authentication and authorization.

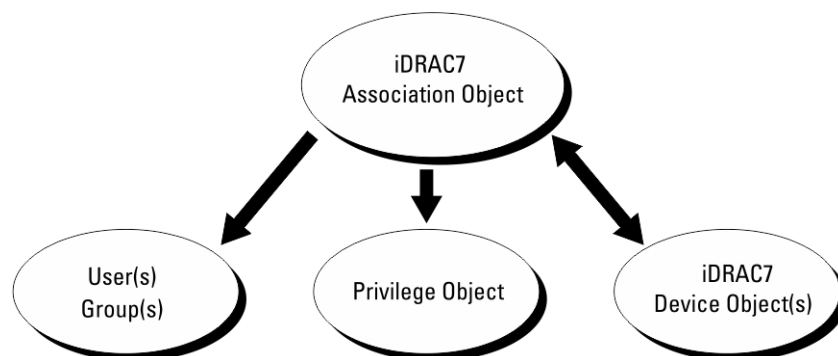


Figure 2. Typical Setup for Active Directory Objects

You can create as many or as few association objects as required. However, you must create at least one Association Object, and you must have one iDRAC7 Device Object for each iDRAC7 device on the network that you want to integrate with Active Directory for Authentication and Authorization with iDRAC7.

The Association Object allows for as many or as few users and/or groups as well as iDRAC7 Device Objects. However, the Association Object only includes one Privilege Object per Association Object. The Association Object connects the Users who have Privileges on iDRAC7 devices.

The Dell extension to the ADUC MMC Snap-in only allows associating the Privilege Object and iDRAC7 Objects from the same domain with the Association Object. The Dell extension does not allow a group or an iDRAC7 object from other domains to be added as a product member of the Association Object.

When adding Universal Groups from separate domains, create an Association Object with Universal Scope. The Default Association objects created by the Dell Schema Extender Utility are Domain Local Groups and does not work with Universal Groups from other domains.

Users, user groups, or nested user groups from any domain can be added into the Association Object. Extended Schema solutions support any user group type and any user group nesting across multiple domains allowed by Microsoft Active Directory.

Accumulating Privileges Using Extended Schema

The Extended Schema Authentication mechanism supports Privilege Accumulation from different privilege objects associated with the same user through different Association Objects. In other words, Extended Schema Authentication accumulates privileges to allow the user the super set of all assigned privileges corresponding to the different privilege objects associated with the same user.

The following figure provides an example of accumulating privileges using Extended Schema.

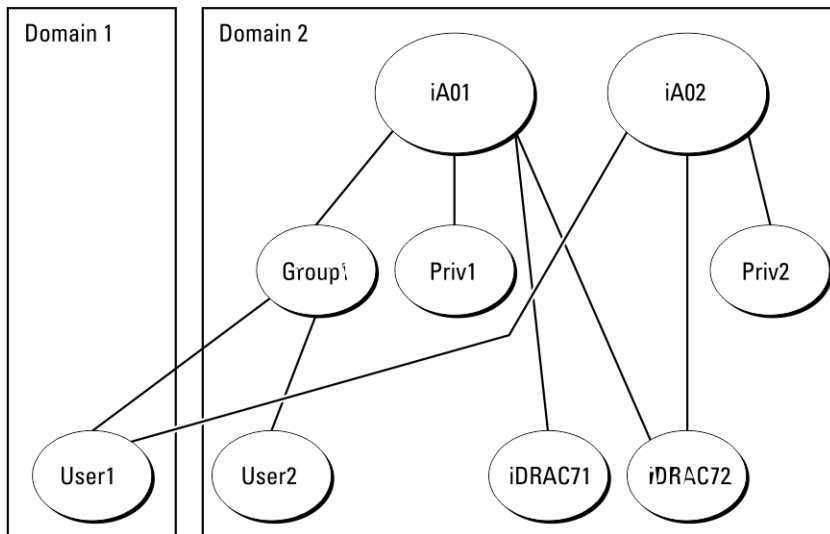


Figure 3. Privilege Accumulation for a User

The figure shows two Association Objects—A01 and A02. User1 is associated to iDRAC72 through both association objects.

Extended Schema Authentication accumulates privileges to allow the user the maximum set of privileges possible considering the assigned privileges of the different privilege objects associated to the same user.

In this example, User1 has both Priv1 and Priv2 privileges on iDRAC72. User1 has Priv1 privileges on iDRAC71 only. User2 has Priv1 privileges on both iDRAC71 and iDRAC72. In addition, this figure shows that User1 can be in a different domain and can be a member of a group.

Configuring Extended Schema Active Directory

To configure Active Directory to access iDRAC7:

1. Extend the Active Directory schema.
2. Extend the Active Directory Users and Computers Snap-in.
3. Add iDRAC7 users and their privileges to Active Directory.
4. Configure iDRAC7 Active Directory properties using iDRAC7 Web interface or RACADM.

Related Links

[Extended Schema Active Directory Overview](#)

[Installing Dell Extension to the Active Directory Users and Computers Snap-In](#)


[Adding iDRAC7 Users and Privileges to Active Directory](#)


[Configuring Active Directory With Extended Schema Using iDRAC7 Web Interface](#)

[Configuring Active Directory With Extended Schema Using RACADM](#)

Extending Active Directory Schema

Extending your Active Directory schema adds a Dell organizational unit, schema classes and attributes, and example privileges and association objects to the Active Directory schema. Before you extend the schema, make sure that you have Schema Admin privileges on the Schema Master Flexible Single Master Operation (FSMO) Role Owner of the domain forest.

 **NOTE:** Make sure to use the schema extension for this product is different from the previous generations of RAC products. The earlier schema does not work with this product.

 **NOTE:** Extending the new schema has no impact on previous versions of the product.

You can extend your schema using one of the following methods:

- Dell Schema Extender utility
- LDIF script file

If you use the LDIF script file, the Dell organizational unit is not added to the schema.


The LDIF files and Dell Schema Extender are located on your *Dell Systems Management Tools and Documentation* DVD in the following respective directories:

- DVDdrive:\SYSMGMT\ManagementStation\support\OMActiveDirectory_Tools\Remote_Management_Advanced\LDIF_Files
- <DVDdrive>:\SYSMGMT\ManagementStation\support\OMActiveDirectory_Tools\Remote_Management_Advanced\Schema Extender

To use the LDIF files, see the instructions in the readme included in the **LDIF_Files** directory.

You can copy and run the Schema Extender or LDIF files from any location.

Using Dell Schema Extender

 **CAUTION:** The Dell Schema Extender uses the SchemaExtenderOem.ini file. To make sure that the Dell Schema Extender utility functions properly, do not modify the name of this file.

1. In the **Welcome** screen, click **Next**.
2. Read and understand the warning and click **Next**.
3. Select **Use Current Log In Credentials** or enter a user name and password with schema administrator rights.
4. Click **Next** to run the Dell Schema Extender.
5. Click **Finish**.

The schema is extended. To verify the schema extension, use the MMC and the Active Directory Schema Snap-in to verify that the classes and attributes [Classes and Attributes](#) exist. See the Microsoft documentation for details about using the MMC and the Active Directory Schema Snap-in.

Classes and Attributes

Table 14. 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 15. dellRacDevice Class

| | |
|-------------|--|
| OID | 1.2.840.113556.1.8000.1280.1.7.1.1 |
| Description | Represents the Dell iDRAC7 device. iDRAC7 must be configured as dellIDRACDevice in Active Directory. |

| | |
|--------------|--|
| OID | 1.2.840.113556.1.8000.1280.1.7.1.1 |
| Description | This configuration enables iDRAC to send Lightweight Directory Access Protocol (LDAP) queries to Active Directory. |
| Class Type | Structural Class |
| SuperClasses | dellProduct |
| Attributes | dellSchemaVersion dellRacType |

Table 16. dellIDRACAssociationObject Class

| | |
|--------------|---|
| OID | 1.2.840.113556.1.8000.1280.1.7.1.2 |
| Description | Represents the Dell Association Object. The Association Object provides the connection between the users and the devices. |
| Class Type | Structural Class |
| SuperClasses | Group |
| Attributes | dellProductMembers dellPrivilegeMember |

Table 17. dellRAC4Privileges Class

| | |
|--------------|--|
| OID | 1.2.840.113556.1.8000.1280.1.1.1.3 |
| Description | Defines the privileges (Authorization Rights) for iDRAC7 |
| Class Type | Auxiliary Class |
| SuperClasses | None |
| Attributes | dellIsLoginUser dellIsCardConfigAdmin dellIsUserConfigAdmin dellIsLogClearAdmin dellIsServerResetUser dellIsConsoleRedirectUser dellIsVirtualMediaUser dellIsTestAlertUser dellIsDebugCommandAdmin |

Table 18. 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 19. 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 20. List of Attributes Added to the Active Directory Schema

| Attribute Name/Description | Assigned OID/Syntax Object Identifier | Single Valued |
|--|---|---------------|
| dellPrivilegeMember List of dellPrivilege Objects that belong to this Attribute. | 1.2.840.113556.1.8000.1280.1.1.2.1 Distinguished Name (LDAPTYPE_DN 1.3.6.1.4.1.1466.115.121.1.12) | FALSE |
| dellProductMembers List of dellRacDevice and DelliDRACDevice Objects that belong to this role. This attribute is the forward link to the dellAssociationMembers backward link. Link ID: 12070 | 1.2.840.113556.1.8000.1280.1.1.2.2 Distinguished Name (LDAPTYPE_DN 1.3.6.1.4.1.1466.115.121.1.12) | FALSE |
| dellsLoginUser TRUE if the user has Login rights on the device. | 1.2.840.113556.1.8000.1280.1.1.2.3 Boolean (LDAPTYPE_BOOLEAN 1.3.6.1.4.1.1466.115.121.1.7) | TRUE |
| dellsCardConfigAdmin TRUE if the user has Card Configuration rights on the device. | 1.2.840.113556.1.8000.1280.1.1.2.4 Boolean (LDAPTYPE_BOOLEAN 1.3.6.1.4.1.1466.115.121.1.7) | TRUE |
| dellsUserConfigAdmin TRUE if the user has User Configuration rights on the device. | 1.2.840.113556.1.8000.1280.1.1.2.5 Boolean (LDAPTYPE_BOOLEAN 1.3.6.1.4.1.1466.115.121.1.7) | TRUE |
| dellsLogClearAdmin TRUE if the user has Log Clearing rights on the device. | 1.2.840.113556.1.8000.1280.1.1.2.6 Boolean (LDAPTYPE_BOOLEAN 1.3.6.1.4.1.1466.115.121.1.7) | TRUE |
| dellsServerResetUser TRUE if the user has Server Reset rights on the device. | 1.2.840.113556.1.8000.1280.1.1.2.7 Boolean (LDAPTYPE_BOOLEAN 1.3.6.1.4.1.1466.115.121.1.7) | TRUE |
| dellsConsoleRedirectUser TRUE if the user has Virtual Console rights on the device. | 1.2.840.113556.1.8000.1280.1.1.2.8 Boolean (LDAPTYPE_BOOLEAN 1.3.6.1.4.1.1466.115.121.1.7) | TRUE |
| dellsVirtualMediaUser TRUE if the user has Virtual Media rights on the device. | 1.2.840.113556.1.8000.1280.1.1.2.9 Boolean (LDAPTYPE_BOOLEAN 1.3.6.1.4.1.1466.115.121.1.7) | TRUE |
| dellsTestAlertUser TRUE if the user has Test Alert User rights on the device. | 1.2.840.113556.1.8000.1280.1.1.2.10 Boolean (LDAPTYPE_BOOLEAN 1.3.6.1.4.1.1466.115.121.1.7) | TRUE |
| dellsDebugCommandAdmin | 1.2.840.113556.1.8000.1280.1.1.2.11 | TRUE |

| Attribute Name/Description | Assigned OID/Syntax Object Identifier | Single Valued |
|--|--|---------------|
| TRUE if the user has Debug Command Admin rights on the device. | Boolean (LDAPTYPE_BOOLEAN 1.3.6.1.4.1.1466.115.121.1.7) | |
| dellSchemaVersion The Current Schema Version is used to update the schema. | 1.2.840.113556.1.8000.1280.1.1.2.12 Case Ignore String (LDAPTYPE_CASEIGNORESTRING 1.2.840.113556.1.4.905) | TRUE |
| dellRacType This attribute is the Current RAC Type for the dellIDRACDevice object and the backward link to the dellAssociationObjectMembers forward link. | 1.2.840.113556.1.8000.1280.1.1.2.13 Case Ignore String (LDAPTYPE_CASEIGNORESTRING 1.2.840.113556.1.4.905) | TRUE |
| dellAssociationMembers List of dellAssociationObjectMembers that belong to this Product. This attribute is the backward link to the dellProductMembers linked attribute. Link ID: 12071 | 1.2.840.113556.1.8000.1280.1.1.2.14 Distinguished Name (LDAPTYPE_DN 1.3.6.1.4.1.1466.115.121.1.12) | FALSE |

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

When you extend the schema in Active Directory, you must also extend the Active Directory Users and Computers Snap-in so the administrator can manage iDRAC7 devices, users and user groups, iDRAC7 associations, and iDRAC7 privileges.

When you install your systems management software using the *Dell Systems Management Tools and Documentation* DVD, you can extend the Snap-in by selecting the **Active Directory Users and Computers Snap-in** option during the installation procedure. See the Dell OpenManage Software Quick Installation Guide for additional instructions about installing systems management software. For 64-bit Windows Operating Systems, the Snap-in installer is located under:

<DVDdrive>\<SYSMGMT\ManagementStation\support\OMActiveDirectory_SnapIn64

For more information about the Active Directory Users and Computers Snap-in, see Microsoft documentation.

Adding iDRAC7 Users and Privileges to Active Directory

Using the Dell-extended Active Directory Users and Computers Snap-in, you can add iDRAC7 users and privileges by creating device, association, and privilege objects. To add each object, perform the following:

- Create an iDRAC7 device Object
- Create a Privilege Object
- Create an Association Object
- Add objects to an Association Object

Related Links

[Adding Objects to Association Object](#)

[Creating iDRAC7 Device Object](#)

[Creating Privilege Object](#)

[Creating Association Object](#)

Creating iDRAC7 Device Object

To create iDRAC7 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 iDRAC7 name that you enter while configuring Active Directory properties using iDRAC7 Web interface.
4. Select **iDRAC Device Object** and click OK.

Creating Privilege Object

To create privilege object:



NOTE: You must create a privilege object in the same domain as the related association object.

1. In the **Console Root** (MMC) window, right-click a container.
2. Select **New** → **Dell Remote Management Object Advanced**.
The **New Object** window is displayed.
3. Enter a name for the new object.
4. Select **Privilege Object** and click OK.
5. Right-click the privilege object that you created, and select **Properties**.
6. Click the **Remote Management Privileges** tab and assign the privileges for the user or group.

Creating Association Object

To create association object:



NOTE: iDRAC7 association object is derived from the group and its scope is set to Domain Local.

1. In the **Console Root** (MMC) window, right-click a container.
2. Select **New** → **Dell Remote Management Object Advanced**.
This **New Object** window is displayed.
3. Enter a name for the new object and select **Association Object**.
4. Select the scope for the **Association Object** and click OK.
5. Provide access privileges to the authenticated users for accessing the created association objects.

Related Links

[Providing User Access Privileges For Association Objects](#)

Providing User Access Privileges For Association Objects

To provide access privileges to the authenticated users for accessing the created association objects:

1. Go to **Administrative Tools** → **ADSI Edit**. The **ADSI Edit** window is displayed.
2. In the right-pane, navigate to the created association object, right-click and select **Properties**.
3. In the **Security** tab, click **Add**.
4. Type `Authenticated Users`, click **Check Names**, and click **OK**. The authenticated users is added to the list of **Groups and user names**.
5. Click **OK**.

Adding Objects to Association Object

Using the **Association Object Properties** window, you can associate users or user groups, privilege objects, and iDRAC7 devices or iDRAC7 device groups.

You can add groups of users and iDRAC7 devices.

Related Links

[Adding Users or User Groups](#)

[Adding Privileges](#)

[Adding iDRAC7 Devices or iDRAC7 Device Groups](#)

Adding Users or User Groups

To add users or user groups:

1. Right-click the **Association Object** and select **Properties**.
2. Select the **Users** tab and click **Add**.
3. Enter the user or user group name and click **OK**.

Adding Privileges

To add privileges:

Click the **Privilege Object** tab to add the privilege object to the association that defines the user's or user group's privileges when authenticating to an iDRAC7 device. Only one privilege object can be added to an Association Object.

1. Select the **Privileges Object** tab and click **Add**.
2. Enter the privilege object name and click **OK**.
3. Click the **Privilege Object** tab to add the privilege object to the association that defines the user's or user group's privileges when authenticating to an iDRAC7 device. Only one privilege object can be added to an Association Object.

Adding iDRAC7 Devices or iDRAC7 Device Groups

To add iDRAC7 devices or iDRAC7 device groups:

1. Select the **Products** tab and click **Add**.
2. Enter iDRAC7 devices or iDRAC7 device group name and click **OK**.
3. In the **Properties** window, click **Apply** and click **OK**.
4. Click the **Products** tab to add one iDRAC7 device connected to the network that is available for the defined users or user groups. You can add multiple iDRAC7 devices to an Association Object.

Configuring Active Directory With Extended Schema Using iDRAC7 Web Interface

To configure Active Directory with extended schema using Web interface:



NOTE: For information about the various fields, see the *iDRAC7 Online Help*.

1. In the iDRAC7 Web interface, go to **Overview** → **iDRAC Settings** → **User Authentication** → **Directory Services** → **Microsoft Active Directory**.
The **Active Directory** summary page is displayed.
2. Click **Configure Active Directory**.
The **Active Directory Configuration and Management Step 1 of 4** page is displayed.
3. Optionally, enable certificate validation and upload the CA-signed digital certificate used during initiation of SSL connections when communicating with the Active Directory (AD) server.
4. Click **Next**.

The **Active Directory Configuration and Management Step 2 of 4** page is displayed.

5. Specify the location information about Active Directory (AD) servers and user accounts. Also, specify the time iDRAC7 must wait for responses from AD during login process.

 **NOTE:** If certificate validation is enabled, specify the Domain Controller Server addresses and the FQDN. Make sure that DNS is configured correctly under **Overview** → **iDRAC Settings** → **Network**.

6. Click **Next**. The **Active Directory Configuration and Management Step 3 of 4** page is displayed.

7. Select **Extended Schema** and click **Next**.

The **Active Directory Configuration and Management Step 4 of 4** page is displayed.

8. Enter the name and location of the iDRAC7 device object in Active Directory (AD) and click **Finish**.


The Active Directory settings for extended schema mode is configured.

Configuring Active Directory With Extended Schema Using RACADM

To configure Active Directory with Extended Schema using the RACADM:


1. Open a command prompt and enter the following RACADM commands:

```
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. iDRAC7 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 iDRAC7 device is located.

To disable the certificate validation during SSL handshake (optional):

```
racadm config -g cfgActiveDirectory -o cfgADCertValidationEnable 0
```

 **NOTE:** In this case, you do not have to upload a CA certificate.

To enforce the certificate validation during SSL handshake (optional):

```
racadm config -g cfgActiveDirectory -o cfgADCertValidationEnable 1
```

In this case, you must upload a CA certificate:

```
racadm sslcertupload -t 0x2 -f <ADS root CA certificate >
```

 **NOTE:** If certificate validation is enabled, specify the Domain Controller Server addresses and the FQDN. Make sure that DNS is configured correctly under **Overview** → **iDRAC Settings** → **Network**.

Using the following RACADM command may be optional:

```
racadm sslcertdownload -t 0x1 -f <RAC SSL certificate >
```

2. If DHCP is enabled on iDRAC7 and you want to use the DNS provided by the DHCP server, enter the following RACADM command:
3. If DHCP is disabled in iDRAC7 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 iDRAC7 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.

5. Press **Enter** to complete the Active Directory configuration with Extended Schema.

Testing Active Directory Settings

You can test the Active Directory settings to verify whether your configuration is correct, or to diagnose the problem with a failed Active Directory log in.

Testing Active Directory Settings Using iDRAC7 Web Interface


To test the Active Directory settings:

1. In iDRAC7 Web Interface, go to **Overview** → **iDRAC Settings** → **User Authentication** → **Directory Services** → **Microsoft Active Directory**.

The **Active Directory** summary page is displayed.

2. Click **Test Settings**.
3. Enter a test user's name (for example, **username@domain.com**) and password and click **Start Test**. A detailed test results and the test log displays.

If there is a failure in any step, examine the details in the test log to identify the problem and a possible solution.

 **NOTE:** When testing Active Directory settings with Enable Certificate Validation checked, iDRAC7 requires that the Active Directory server be identified by the FQDN and not an IP address. If the Active Directory server is identified by an IP address, certificate validation fails because iDRAC7 is not able to communicate with the Active Directory server.


Testing Active Directory Settings Using RACADM

To test the Active Directory settings, use the `testfeature` command. For more information, see the *RACADM Command Line Reference Guide for iDRAC7 and CMC* available at support.dell.com/manuals.

Configuring Generic LDAP Users

iDRAC7 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 iDRAC7 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 iDRAC7.


 **NOTE:** The Smart Card based Two Factor Authentication (TFA) and the Single Sign-On (SSO) logins are not supported for generic LDAP Directory Service.

Related Links

[Configuring Generic LDAP Directory Service Using iDRAC7 Web-Based Interface](#)

Configuring Generic LDAP Directory Service Using iDRAC7 Web-Based Interface


To configure the generic LDAP directory service using Web interface:

 **NOTE:** For information about the various fields, see the *iDRAC7 Online Help*.

1. In the iDRAC7 Web interface, go to **Overview** → **iDRAC Settings** → **User Authentication** → **Directory Services** → **Generic LDAP Directory Service**.

The **Generic LDAP Configuration and Management** page displays the current generic LDAP settings.

2. Click **Configure Generic LDAP**.
3. Optionally, enable certificate validation and upload the digital certificate used during initiation of SSL connections when communicating with a generic LDAP server.


 **NOTE:** In this release, non-SSL port based LDAP bind is not supported. Only LDAP over SSL is supported.

4. Click **Next**.

The **Generic LDAP Configuration and Management Step 2 of 3** page is displayed.

5. Enable generic LDAP authentication and specify the location information about generic LDAP servers and user accounts.

 **NOTE:** If certificate validation is enabled, specify the LDAP Server's FQDN and make sure that DNS is configured correctly under **Overview** → **iDRAC Settings** → **Network**.

 **NOTE:** In this release, nested group is not supported. The firmware searches for the direct member of the group to match the user DN. Also, only single domain is supported. Cross domain is not supported.


6. Click **Next**.

The **Generic LDAP Configuration and Management Step 3a of 3** page is displayed.

7. Click **Role Group**.

The **Generic LDAP Configuration and Management Step 3b of 3** page is displayed.

8. Specify the group distinguished name, the privileges associated with the group, and click **Apply**.

 **NOTE:** If you are using Novell eDirectory and if you have used these characters—#(hash), "(double quotes), ;(semi colon), > (greater than), , (comma), or <(lesser than)—for the Group DN name, they must be escaped.

The role group settings are saved. The **Generic LDAP Configuration and Management Step 3a of 3** page displays the role group settings.

9. If you want to configure additional role groups, repeat steps 7 and 8.

10. Click **Finish**. The generic LDAP directory service is configured.

Configuring Generic LDAP Directory Service Using RACADM

To configure the LDAP directory service, use the objects in **cfgLdap** and **cfgLdapRoleGroup** RACADM groups. For more information, see the *RACADM Command Line Reference Guide for iDRAC7 and CMC* available at support.dell.com/manuals.

Testing LDAP Directory Service Settings

You can test the LDAP directory service settings to verify whether your configuration is correct, or to diagnose the problem with a failed LDAP log in.

Testing LDAP Directory Service Settings Using iDRAC7 Web Interface


To test the LDAP directory service settings:


1. In iDRAC7 Web Interface, go to **Overview** → **iDRAC Settings** → **User Authentication** → **Directory Services** → **Generic LDAP Directory Service**.

The **Generic LDAP Configuration and Management** page displays the current generic LDAP settings.

2. Click **Test Settings**.

3. Enter the user name and password of a directory user that is chosen to test the LDAP settings. The format depends on the *Attribute of User Login* is used and the user name entered must match the value of the chosen attribute.

 **NOTE:** When testing LDAP settings with **Enable Certificate Validation** checked, iDRAC7 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 iDRAC7 is not able to communicate with the LDAP server.

 **NOTE:** When generic LDAP is enabled, iDRAC7 first tries to login the user as a directory user. If it fails, local user lookup is enabled.

The test results and the test log are displayed.

Testing LDAP Directory Service Settings Using RACADM

To test the LDAP directory service settings, use the `testfeature` command. For more information, see the *RACADM Command Line Reference Guide for iDRAC7 and CMC* available at support.dell.com/manuals.

Configuring iDRAC7 for Single Sign-On or Smart Card Login

This section provides information to configure iDRAC7 for Smart Card login (for local users and Active Directory users), and Single Sign-On (SSO) login (for Active Directory users.) SSO and smart card login are licensed features.

iDRAC7 supports Kerberos based Active Directory authentication to support Smart Card and SSO logins. For information on Kerberos, see the Microsoft website.

Related Links

- [Configuring iDRAC7 SSO Login for Active Directory Users](#)
- [Configuring iDRAC7 Smart Card Login for Local Users](#)
- [Configuring iDRAC7 Smart Card Login for Active Directory Users](#)

Prerequisites for Active Directory Single Sign-On or Smart Card Login

The pre-requisites to Active Directory based SSO or Smart Card logins are:

- Synchronize iDRAC7 time with the Active Directory domain controller time. If not, kerberos authentication on iDRAC7 fails. The offset value is in minutes from iDRAC time (UTC) to the Domain Controller's time (for example, -360 for Central Time zone). A maximum time difference of five minutes is allowed. After synchronizing the server time with the domain controller time, **reset (reboot)** iDRAC7.

You can also use the following RACADM time zone offset command to synchronize the time:


```
racadm config -g cfgRacTuning -o
cfgRacTuneTimeZoneOffset <offset value>
```

If daylight savings time is in effect, use the following command:

```
cfgRacTuneDaylightOffset <offset value>
```

For more information, see the *RACADM Command Line Reference Guide for iDRAC7 and CMC* available at support.dell.com/manuals.

- Register iDRAC7 as a computer in the Active Directory root domain.
- Generate a keytab file using the ktpass tool.
- To enable single sign-on for Extended schema, make sure that the **Trust this user for delegation to any service (Kerberos only)** option is selected on the **Delegation** tab for the keytab user. This tab is available only after creating the keytab file using ktpass utility.
- Configure the browser to enable SSO login.
- Create the Active Directory objects and provide the required privileges.
- For SSO, configure the reverse lookup zone on the DNS servers for the subnet where iDRAC7 resides.

 **NOTE:** If the host name does not match the reverse DNS lookup, Kerberos authentication fails.

Related Links

- [Configuring Browser to Enable Active Directory SSO](#)
- [Registering iDRAC7 as a Computer in Active Directory Root Domain](#)
- [Generating Kerberos Keytab File](#)

Registering iDRAC7 as a Computer in Active Directory Root Domain

To register iDRAC7 in Active Directory root domain:

1. Click **Overview** → **iDRAC Settings** → **Network** → **Network**.
The **Network** page is displayed.
2. Provide a valid **Preferred/Alternate DNS Server** IP address. This value is a valid DNS server IP address that is part of the root domain.
3. Select **Register iDRAC on DNS**.
4. Provide a valid **DNS Domain Name**.
5. Verify that network DNS configuration matches with the Active Directory DNS information.
For more information about the options, see the *iDRAC7 Online Help*.

Generating Kerberos Keytab File

To support the SSO and smart card login authentication, iDRAC7 supports the configuration to enable itself as a kerberized service on a Windows Kerberos network. The Kerberos configuration on iDRAC7 involves the same steps as configuring a non-Windows Server Kerberos service as a security principal in Windows Server Active Directory.

The *ktpass* tool (available from Microsoft as part of the server installation CD/DVD) is used to create the Service Principal Name (SPN) bindings to a user account and export the trust information into a MIT-style Kerberos *keytab* file, which enables a trust relation between an external user or system and the Key Distribution Centre (KDC). The keytab file contains a cryptographic key, which is used to encrypt the information between the server and the KDC. The *ktpass* tool allows UNIX-based services that support Kerberos authentication to use the interoperability features provided by a Windows Server Kerberos KDC service. For more information on the *ktpass* utility, see the Microsoft website at: [technet.microsoft.com/en-us/library/cc779157\(Ws.10\).aspx](http://technet.microsoft.com/en-us/library/cc779157(Ws.10).aspx)


Before generating a keytab file, you must create an Active Directory user account for use with the **-mapuser** option of the *ktpass* command. Also, you must have the same name as iDRAC7 DNS name to which you upload the generated keytab file.

To generate a keytab file using the *ktpass* tool:

1. Run the *ktpass* utility on the domain controller (Active Directory server) where you want to map iDRAC7 to a user account in Active Directory.
2. Use the following *ktpass* command to create the Kerberos keytab file:

```
C:\> ktpass.exe -princ HTTP/idrac7name.domainname.com@DOMAINNAME.COM -  
mapuser DOMAINNAME\username -mapOp set -crypto DES-CBC-MD5 -ptype  
KRB5_NT_PRINCIPAL -pass [password] +DesOnly -out c:\krbkeytab
```


The encryption type 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:** Use lowercase letters for the **iDRAC7name** and **Service Principal Name**. Use uppercase letters for the domain name as shown in the example.

3. Run the following command:

```
C:\>setspn -a HTTP/idrac7name.domainname.com username
```

A keytab file is generated.

 **NOTE:** If you find any issues with iDRAC7 user for which the keytab file is created, create a new user and a new keytab file. If the same keytab file which was initially created is again executed, it does not configure correctly.

Creating Active Directory Objects and Providing Privileges

Perform the following steps for Active Directory Extended schema based SSO login:

1. Create the device object, privilege object, and association object in the Active Directory server.
2. Set access privileges to the created privilege object. It is recommended not to provide administrator privileges as this could bypass some security checks.
3. Associate the device object and privilege object using the association object.
4. Add the preceding SSO user (login user) to the device object.
5. Provide access privilege to *Authenticated Users* for accessing the created association object.

Related Links

[Adding iDRAC7 Users and Privileges to Active Directory](#)

Configuring Browser to Enable Active Directory SSO

This section provides the browser settings for Internet Explorer and Firefox to enable Active Directory SSO.

Configuring Internet Explorer to Enable Active Directory SSO

To configure the browser settings for Internet Explorer:

1. In Internet Explorer, navigate to **Local Intranet** and click **Sites**.
2. Select the following options only:
 - Include all local (intranet) sites not listed on other zones.
 - Include all sites that bypass the proxy server.
3. Click **Advanced**.
4. Add all relative domain names that will be used for iDRAC7 instances that is part of the SSO configuration (for example, **myhost.example.com**.)
5. Click **Close** and click **OK** twice.

Configuring Firefox to Enable Active Directory SSO

To configure the browser settings for Firefox:

1. In Firefox address bar, enter `about:config`.
2. In **Filter**, enter `network.negotiate`.
3. Add the iDRAC7 name to `network.negotiate-auth.trusted-uris` (using comma separated list.)
4. Add the iDRAC7 name to `network.negotiate-auth.delegation-uris` (using comma separated list.)

Configuring iDRAC7 SSO Login for Active Directory Users

Before configuring iDRAC7 for Active Directory SSO login, make sure that you have completed all the prerequisites.

You can configure iDRAC7 for Active Directory SSO when you setup an user account based on Active Directory.


Related Links

[Prerequisites for Active Directory Single Sign-On or Smart Card Login](#)

[Configuring Active Directory With Standard Schema Using iDRAC7 Web Interface](#)
[Configuring Active Directory With Standard Schema Using RACADM](#)
[Configuring Active Directory With Extended Schema Using iDRAC7 Web Interface](#)
[Configuring Active Directory With Extended Schema Using RACADM](#)

Configuring iDRAC7 SSO Login for Active Directory Users Using Web Interface

To configure iDRAC7 for Active Directory SSO login:

 **NOTE:** For information about the options, see the *iDRAC7 Online Help*.

1. Verify whether the iDRAC7 DNS name matches the iDRAC7 Fully Qualified Domain Name. To do this, in iDRAC7 Web interface, go to **Overview** → **iDRAC Settings** → **Network** → **Network** and see the **DNS Domain Name** property.
2. While configuring Active Directory to setup a user account based on standard schema or extended schema, perform the following two additional steps to configure SSO:
 - Upload the keytab file on the **Active Directory Configuration and Management Step 1 of 4** page.
 - Select **Enable Single Sign-On** option on the **Active Directory Configuration and Management Step 2 of 4** page.

Configuring iDRAC7 SSO Login for Active Directory Users Using RACADM

In addition to the steps performed while configuring Active Directory, to enable SSO, run the following command:

```
racadm -g cfgActiveDirectory -o cfgADSSOEnable 1
```

Configuring iDRAC7 Smart Card Login for Local Users

To configure iDRAC7 local user for smart card login:

1. Upload the smart card user certificate and trusted CA certificate to iDRAC7.
2. Enable smart card login.

Related Links

[Obtaining Certificates](#)
[Uploading Smart Card User Certificate](#)
[Enabling or Disabling Smart Card Login](#)

Uploading Smart Card User Certificate

Before you upload the user certificate, make sure that the user certificate from the smart card vendor is exported in Base64 format.

Related Links

[Obtaining Certificates](#)

Uploading Smart Card User Certificate Using Web Interface

To upload smart card user certificate:

1. In iDRAC7 Web interface, go to **Overview** → **iDRAC Settings** → **Network** → **User Authentication** → **Local Users**. The **Users** page is displayed.
2. In the **User ID** column, click a user ID number.

The **Users Main Menu** page is displayed.

3. Under **Smart Card Configurations**, select **Upload User Certificate** and click **Next**.
The **User Certificate Upload** page is displayed.
4. Browse and select the Base64 user certificate, and click **Apply**.

Uploading Smart Card User Certificate Using RACADM

To upload smart card user certificate, use the **usercertupload** object. For more information, see the *RACADM Command Line Reference Guide for iDRAC7 and CMC* available at support.dell.com/manuals.

Uploading Trusted CA Certificate For Smart Card

Before you upload the CA certificate, make sure that you have a CA-signed certificate.

Related Links

[Obtaining Certificates](#)

Uploading Trusted CA Certificate For Smart Card Using Web Interface

To upload trusted CA certificate for smart card login:

1. In iDRAC7 Web interface, go to **Overview** → **iDRAC Settings** → **Network** → **User Authentication** → **Local Users**.
The **Users** page is displayed.
2. In the **User ID** column, click a user ID number.
The **Users Main Menu** page is displayed.
3. Under **Smart Card Configurations**, select **Upload Trusted CA Certificate** and click **Next**.
The **Trusted CA Certificate Upload** page is displayed.
4. Browse and select the trusted CA certificate, and click **Apply**.

Uploading Trusted CA Certificate For Smart Card Using RACADM

To upload trusted CA certificate for smart card login, use the **usercertupload** object. For more information, see the *RACADM Command Line Reference Guide for iDRAC7 and CMC* available at support.dell.com/manuals.

Configuring iDRAC7 Smart Card Login for Active Directory Users

Before configuring iDRAC7 Smart Card login for Active Directory users, make sure that you have completed the required prerequisites.

To configure iDRAC7 for smart card login:

1. In iDRAC7 Web interface, while configuring Active Directory to set up an user account based on standard schema or extended schema, on the **Active Directory Configuration and Management Step 1 of 4** page:
 - Enable certificate validation.
 - Upload a trusted CA-signed certificate.
 - Upload the keytab file.
2. Enable smart card login. For information about the options, see the *iDRAC7 Online Help*.

Related Links

[Enabling or Disabling Smart Card Login](#)

[Obtaining Certificates](#)


[Generating Kerberos Keytab File](#)

[Configuring Active Directory With Standard Schema Using iDRAC7 Web Interface](#)
[Configuring Active Directory With Standard Schema Using RACADM](#)
[Configuring Active Directory With Extended Schema Using iDRAC7 Web Interface](#)
[Configuring Active Directory With Extended Schema Using RACADM](#)

Enabling or Disabling Smart Card Login

Before enabling or disabling smart card login for iDRAC7, make sure that:

- You have configured iDRAC7 permissions.
- iDRAC7 local user configuration or Active Directory user configuration with the appropriate certificates is complete.

 **NOTE:** If smart card login is enabled, then SSH, Telnet, IPMI Over LAN, Serial Over LAN, and remote RACADM are disabled. Again, if you disable smart card login, the interfaces are not enabled automatically.

Related Links

[Obtaining Certificates](#)
[Configuring iDRAC7 Smart Card Login for Active Directory Users](#)
[Configuring iDRAC7 Smart Card Login for Local Users](#)

Enabling or Disabling Smart Card Login Using Web Interface

To enable or disable the Smart Card logon feature:

1. In the iDRAC7 Web interface, go to **Overview** → **iDRAC Settings** → **User Authentication** → **Smart Card** .
The **Smart Card** page is displayed.
2. From the **Configure Smart Card Logon** drop-down menu, select **Enabled** to enable smart card logon or select **Enabled With Remote RACADM**. Else, select **Disabled**.
For more information about the options, see the *iDRAC7 Online Help*.
3. Click **Apply** to apply the settings.
You are prompted for a Smart Card login during any subsequent logon attempts using the iDRAC7 Web interface.

Enabling or Disabling Smart Card Login Using RACADM

To enable smart card login, use the **cfgSmartCardLogonEnable** and **cfgSmartCardCRLEnable** objects. For more information, see the *RACADM Command Line Reference Guide for iDRAC7 and CMC* available at support.dell.com/manuals.

Enabling or Disabling Smart Card Login Using iDRAC Settings Utility

To enable or disable the Smart Card logon feature:

1. In the iDRAC Settings utility, go to **Smart Card**.
The **iDRAC Settings Smart Card** page is displayed.
2. Select **Enabled** to enable smart card logon. Else, select **Disabled**. For more information about the options, see *iDRAC Settings Utility Online Help*.
3. Click **Back**, click **Finish**, and then click **Yes**.
The smart card logon feature is enabled or disabled based on the selection.

Configuring iDRAC7 to Send Alerts

You can set alerts and actions for certain events that occur on the managed system. An event occurs when the status of a system component is greater than the pre-defined condition. If an event matches an event filter and you have configured this filter to generate an alert (e-mail, SNMP trap, or IPMI alert), then an alert is sent to one or more configured destinations. If the same event filter is also configured to perform an action (such as reboot, power cycle, or power off the system), the action is performed. You can set only one action for each event.

To configure iDRAC7 to send alerts:

1. Enable alerts.
2. Optionally, you can filter the alerts based on category or severity.
3. Configure the e-mail alert, IPMI alert, or SNMP trap settings.
4. Enable event alerts and actions such as:
 - Send an email alert, IPMI alert, or SNMP traps to configured destinations.
 - Perform a reboot, power off, or power cycle the managed system.

Related Links

[Enabling or Disabling Alerts](#)

[Filtering Alerts](#)

[Setting Event Alerts](#)

[Configuring E-mail Alert, SNMP Trap, or IPMI Trap Settings](#)

[Alerts Message IDs](#)

Enabling or Disabling Alerts

For sending an alert to configured destinations or to perform an event action, you must enable the global alerting option. This property overrides individual alerting or event actions that is set.

Related Links

[Filtering Alerts](#)

[Configuring E-mail Alert, SNMP Trap, or IPMI Trap Settings](#)

Enabling or Disabling Alerts Using Web Interface

To enable or disable generating alerts:

1. In iDRAC7 Web interface, go to **Overview** → **Server** → **Alerts**. The **Alerts** page is displayed.
2. Under **Alerts** section:
 - Select **Enable** to enable alert generation or perform an event action.
 - Select **Disable** to disable alert generation or disable an event action.
3. Click **Apply** to save the setting.

Enabling or Disabling Alerts Using RACADM

To enable or disable generating alerts or event actions:

```
racadm config -g cfgIpmiLan -o cfgIpmiLanAlertEnable 1
```

Enabling or Disabling Alerts Using iDRAC Settings Utility

To enable or disable generating alerts or event actions:

1. In the iDRAC Settings utility, go to **Alerts**.
The **iDRAC Settings Alerts** page is displayed.
2. Under **Platform Events**, select **Enabled** to enable alert generation or event action. Else, select **Disabled**. For more information about the options, see *iDRAC Settings Utility Online Help*.
3. Click **Back**, click **Finish**, and then click **Yes**.
The alert settings are configured.

Filtering Alerts

You can filter alerts based on category and severity.


Related Links

[Enabling or Disabling Alerts](#)

[Configuring E-mail Alert, SNMP Trap, or IPMI Trap Settings](#)

Filtering Alerts Using iDRAC7 Web Interface

To filter the alerts based on category and severity:

 **NOTE:** Even if you are a user with read-only privileges, you can filter the alerts.

1. In iDRAC7 Web interface, go to **Overview** → **Server** → **Alerts** . The **Alerts** page is displayed.
2. Under **Alerts Filter** section, select one or more of the following categories:
 - System Health
 - Storage
 - Configuration
 - Audit
 - Updates
 - Work Notes
3. Select one or more of the following severity levels:
 - Informational
 - Warning
 - Critical
4. Click **Apply**.
The **Alert Results** section displays the results based on the selected category and severity.

Filtering Alerts Using RACADM

To filter the alerts, use the **eventfilters** command. For more information, see the *RACADM Command Line Reference Guide for iDRAC7 and CMC* available at support.dell.com/manuals.

Setting Event Alerts

You can set event alerts such as e-mail alerts, IPMI alerts, and SNMP traps to be sent to configured destinations.

Related Links

[Enabling or Disabling Alerts](#)

[Configuring E-mail Alert, SNMP Trap, or IPMI Trap Settings](#)

[Filtering Alerts](#)

Setting Event Alerts Using Web Interface

To set an event alert using the Web interface:

1. Make sure that you have configured the e-mail alert, IPMI alert, and SNMP trap settings.
2. Go to **Overview** → **Server** → **Alerts**.
The **Alerts** page is displayed.
3. Under **Alerts Results**, select one or all of the following alerts for the required events:
 - Email Alert
 - SNMP Trap
 - IPMI Alert
4. Click **Apply**.
The setting is saved.
5. Under **Alerts** section, select the **Enable** option to send alerts to configured destinations.

Setting Event Alerts Using RACADM

To set an event alert, use the **eventfilters** command. For more information, see the *RACADM Command Line Reference Guide for iDRAC7 and CMC* available at support.dell.com/manuals.

Setting Event Actions

You can set event actions such as perform a reboot, power cycle, power off, or perform no action on the system.

Related Links

[Filtering Alerts](#)

[Enabling or Disabling Alerts](#)

Setting Event Actions Using Web Interface

To set an event action:

1. In iDRAC7 Web interface, go to **Overview** → **Server** → **Alerts**. The **Alerts** page is displayed.
2. Under **Alerts Results**, from the **Actions** drop-down menu, for each event select an action:

- Reboot
- Power Cycle
- Power Off
- No Action

3. Click **Apply.**

The setting is saved.

Setting Event Actions Using RACADM

To configure an event action use **cfgIpmiPefAction** object or **eventfilters** command. For more information, see the *RACADM Command Line Reference Guide for iDRAC7 and CMC* available at support.dell.com/manuals.

Configuring E-mail Alert, SNMP Trap, or IPMI Trap Settings

The management station uses Simple Network Management Protocol (SNMP) and Intelligent Platform Management Interface (IPMI) traps to receive data from iDRAC7. For systems with large number of nodes, it may not be efficient for a management station to poll each iDRAC7 for every condition that may occur. For example, event traps can help a management station with load balancing between nodes or by issuing an alert if an authentication failure occurs.

You can configure the IPv4 and IPv6 alert destinations, e-mail settings, and SMTP server settings, and test these settings.

Before configuring the e-mail, SNMP, or IPMI trap settings, make sure that:

- You have Configure RAC permission.
- You have configured the event filters.

Related Links

[Configuring IP Alert Destinations](#)

[Configuring E-Mail Alert Settings](#)


Configuring IP Alert Destinations

You can configure the IPv6 or IPv4 addresses to receive the IPMI alerts or SNMP traps.

Configuring IP Alert Destinations Using Web Interface

To configure IPv4 or IPv6 alert destination settings using Web interface:

1. Go to **Overview** → **Server** → **Alerts** → **SNMP and E-mail Settings**.
2. Select the **State** option to enable the IP address to receive the traps and enter the IP address(es) for IPv4 and IPv6. You can specify up to four IPv4 and four IPv6 destination addresses. For more information about the options, see the *iDRAC7 Online Help*.
3. Enter the iDRAC7 SNMP community string. For more information about the options, see the *iDRAC7 Online Help*.

 **NOTE:** The Community String value indicates the community string to use in a Simple Network Management Protocol (SNMP) alert trap sent from iDRAC7. Make sure that the destination community string is the same as the iDRAC7 community string. The default value is Public.

4. To test whether the IP address is receiving the IPMI or SNMP traps, click **Send** under **Test IPMI Trap** and **Test SNMP Trap** respectively.
5. Click **Apply**. The alert destinations are configured.

Configuring IP Alert Destinations Using RACADM

To configure the trap alert settings:

1. To enable traps:

- For IPv4 address:

```
racadm config -g cfgIpmiPet -o cfgIpmiPetAlertEnable -i (index) (0|1)
```

- For IPv6 address:

```
racadm config -g cfgIpmiPetIpv6 -o cfgIpmiPetIpv6AlertEnable -i  
(index) (0|1)
```

where, (index) is the destination index and 0 or 1 disables or enables the trap, respectively.

For example, to enable trap with index 4, enter the following command:

```
racadm config -g cfgIpmiPet -o cfgIpmiPetAlertEnable -i 4 1
```

2. To configure the trap destination address:

```
racadm config -g cfgIpmiPetIpv6 -o cfgIpmiPetIpv6AlertDestIPAddr -i  
[index] [IP-address]
```

where [index] is the trap destination index and [IP-address] is the destination IP address of the system that receives the platform event alerts.

3. Configure the SNMP community name string:

```
racadm config -g cfgIpmiLan -o cfgIpmiPetCommunityName [name]
```

where [name] is the SNMP Community Name.

4. To test the trap, if required:

```
racadm testtrap -i [index]
```

where [index] is the trap destination index to test.

For more information, see the *RACADM Command Line Reference Guide for iDRAC7 and CMC* available at support.dell.com/manuals.

Configuring IP Alert Destinations Using iDRAC Settings Utility

You can configure only IPv4 alert destinations using the iDRAC Settings utility. To do this:

1. In the **iDRAC Settings utility**, go to **Alerts**.

The **iDRAC Settings Alerts** page is displayed.

2. Under **Trap Settings**, enable the IP address(es) to receive the traps and enter the IPv4 destination address(es). You can specify up to four IPv4 addresses.

3. Enter the community string name.

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

4. Click Back, click Finish, and then click Yes.

The IPv4 alert destinations are configured.

Configuring E-Mail Alert Settings

You can configure the e-mail address to receive the e-mail alerts. Also, configure the SMTP server address settings.



NOTE: If your mail server is Microsoft Exchange Server 2007, make sure that iDRAC7 domain name is configured for the mail server to receive the email alerts from iDRAC7.



NOTE: E-mail alerts support both IPv4 and IPv6 addresses. The DRAC DNS Domain Name must be specified when using IPv6.

Related Links

[Configuring SMTP E-mail Server Address Settings](#)

Configuring E-Mail Alert Settings Using Web Interface

To configure the e-mail alert settings using Web interface:

1. Go to **Overview** → **Server** → **Alerts** → **SNMP and E-mail Settings**.
2. Select the **State** option to enable the email address to receive the alerts and type a valid e-mail address. For more information about the options, see the *iDRAC7 Online Help*.
3. Click **Send** under **Test E-mail** to test the configured e-mail alert settings.
4. Click **Apply**.

Configuring E-Mail Alert Settings Using RACADM

To configure the e-mail alert settings:

1. To enable e-mail alert:

```
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
```

2. To configure e-mail settings:

```
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.

3. To configure a custom message:

```
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.

4. To test the configured e-mail alert, if required:

```
racadm testemail -i [index]
```

where [index] is the e-mail destination index to test.

For more information, see the *RACADM Command Line Reference Guide for iDRAC7 and CMC* available at support.dell.com/manuals.

Configuring SMTP E-mail Server Address Settings

You must configure the SMTP server address for e-mail alerts to be sent to specified destinations.

Configuring SMTP Email Server Address Settings Using iDRAC7 Web Interface

To configure the SMTP server address:

1. In iDRAC7 Web interface, go to **Overview** → **Server** → **Alerts** → **SNMP and E-mail Settings**.
2. Select the **Enable Authentication** option, specify the user name and password (user who has access to SMTP server), and enter a valid IP address or fully qualified domain name (FQDN) of the SMTP server to be used in the configuration.

For more information about the options, see the *iDRAC7 Online Help*.

3. Click Apply.

The SMTP settings are configured.

Configuring SMTP Email Server Address Settings Using RACADM

To configure the SMTP e-mail server, run the following command:

```
racadm config -g cfgRemoteHosts -o cfgRhostsSmtServerIpAddr <SMTP E-mail  
Server IP Address>
```

Alerts Message IDs

The following table provides the list of message IDs that are displayed for the alerts.

Table 21. Alert Message IDs

| Message ID | Description |
|------------|-----------------|
| AMP | Amperage |
| ASR | Auto Sys Reset |
| BAR | Backup/Restore |
| BAT | Battery Event |
| BIOS | BIOS Management |
| BOOT | BOOT Control |
| CBL | Cable |
| CPU | Processor |
| CPUA | Proc Absent |
| CTL | Storage Contr |
| DH | Cert Mgmt |
| DIS | Auto-Discovery |
| ENC | Storage Enclosr |
| FAN | Fan Event |
| FSD | Debug |
| HWC | Hardware Config |
| IPA | DRAC IP Change |
| ITR | Intrusion |
| JCP | Job Control |
| LC | Lifecycle Contr |
| LIC | Licensing |
| LNK | Link Status |
| LOG | Log event |
| MEM | Memory |
| NDR | NIC OS Driver |
| NIC | NIC Config |

| Message ID | Description |
|------------|------------------|
| OSD | OS Deployment |
| OSE | OS Event |
| PCI | PCI Device |
| PDR | Physical Disk |
| PR | Part Exchange |
| PST | BIOS POST |
| PSU | Power Supply |
| PSUA | PSU Absent |
| PWR | Power Usage |
| RAC | RAC Event |
| RDU | Redundancy |
| RED | FW Download |
| RFL | IDSDM Media |
| RFLA | IDSDM Absent |
| RFM | FlexAddress SD |
| RRDU | IDSDM Redundancy |
| RSI | Remote Service |
| SEC | Security Event |
| SEL | Sys Event Log |
| SRD | Software RAID |
| SSD | PCIe SSD |
| STOR | Storage |
| SUP | FW Update Job |
| SWC | Software Config |
| SWU | Software Change |
| SYS | System Info |
| TMP | Temperature |
| TST | Test Alert |
| UEFI | UEFI Event |
| USR | User Tracking |
| VDR | Virtual Disk |
| VF | vFlash SD card |
| VFL | vFlash Event |
| VFLA | vFlash Absent |
| VLT | Voltage |
| VME | Virtual Media |
| VRM | Virtual Console |

Message ID

Description

WRK

Work Note

Managing Logs

iDRAC7 provides Lifecycle log that contains events related to system, storage devices, network devices, firmware updates, configuration changes, license messages, and so on. However, the system events are also available as a separate log called System Event Log (SEL). The lifecycle log is accessible through iDRAC7 Web interface, RACADM, and WS-MAN interface.

When the size of the lifecycle log reaches 800 KB, the logs are compressed and archived. You can only view the non-archived log entries, and apply filters and comments to non-archived logs. To view the archived logs, you must export the entire lifecycle log to a location on your system.

Related Links

[Viewing System Event Log](#)

[Viewing Lifecycle Log](#)

[Adding Work Notes](#)

[Configuring Remote System Logging](#)

Viewing System Event Log

When a system event occurs on a managed system, it is recorded in the System Event Log (SEL). The same SEL entry is also available in the LC log.

Viewing System Event Log Using Web Interface

To view the SEL, in iDRAC7 Web interface, go to **Overview** → **Server** → **Logs** tab.

The **System Event Log** page displays a system health indicator, a time stamp, and a description for each event logged. For more information, see the *iDRAC7 Online Help*.

Click **Save As** to save the **SEL** to a location of your choice.



NOTE: If you are using Internet Explorer and encounter a problem when saving, make sure to download the Cumulative Security Update for Internet Explorer, located on the Microsoft Support website at support.microsoft.com.

Viewing System Event Log Using RACADM

To view the SEL:

```
racadm getsel <options>
```

If no arguments are specified, the entire log is displayed.

To display the number of SEL entries:

```
racadm getsel -i
```

For more information, see *RACADM Command Line Reference Guide for iDRAC7 and CMC* available at support.dell.com/manuals.

Viewing Lifecycle Log

Lifecycle Controller logs provide the history of changes related to components installed on a managed system. It provides logs about events related to:

- Storage Devices
- System events
- Network Devices
- Configuration
- Audit
- Updates
- Work notes

You can filter logs based on the category and severity level, view, export, and add a work note to a log event.

Related Links

[Filtering Lifecycle Logs](#)

[Exporting Lifecycle Log Results](#)

[Adding Comments to Lifecycle Logs](#)

Viewing Lifecycle Log Using Web Interface

To view the Lifecycle Logs, click **Overview** → **Server** → **Logs** → **Lifecycle Log**. The **Lifecycle Log** page is displayed. For more information about the options, see the *iDRAC7 Online Help*.

Filtering Lifecycle Logs

You can filter logs based on category, severity, keyword, or date range.

To filter the lifecycle logs:

1. In the **Lifecycle Log** page, under the **Log Filter** section, do any or all of the following:
 - Select the **Log Type** from the drop-down list.
 - Select the severity level from the **Status Level** drop-down list.
 - Enter a keyword.
 - Specify the date range.

2. Click **Apply**.

The filtered log entries are displayed in **Log Results**.

Exporting Lifecycle Log Results

To export the lifecycle log results, in the **Lifecycle Log** page, in the **Log Results** section, click **Export**. A dialog box is displayed that allows you to save the log entries in an XML format to a location of your choice.

Adding Comments to Lifecycle Logs

To add comments to the lifecycle logs:

1. In the **Lifecycle Log** page, click the + icon for the required log entry.
The Message ID details are displayed.
2. Enter the comments for the log entry in the **Comment** box.


The comments are displayed in the **Comment** box.

Viewing Lifecycle Log Using RACADM

To view Lifecycle logs, use the `lcllog` command. For more information, see the *RACADM Command Line Reference Guide for iDRAC7 and CMC* available at support.dell.com/manuals.


Adding Work Notes

Each user who logs in to iDRAC7 can add work notes and this is stored in the lifecycle log as an event. You must have iDRAC7 logs privilege to add work notes. A maximum of 255 characters are supported for each new work note.

 **NOTE:** You cannot delete a work note.

To add a work note:

1. In the iDRAC7 Web interface, go to **Overview** → **Server** → **Properties** → **Summary**.
The **System Summary** page is displayed.
2. Under **Work Notes**, enter the text in the blank text box.

 **NOTE:** It is recommended not to use too many special characters.

3. Click **Add**.
The work note is added to the log. For more information, see the *iDRAC7 Online Help*.

Configuring Remote System Logging

You can send lifecycle logs to a remote system. Before doing this, make sure that:

- There is network connectivity between iDRAC7 and the remote system.
- The remote system and iDRAC7 is on the same network.

Configuring Remote System Logging Using Web Interface

To configure the remote syslog server settings:

1. In the iDRAC7 Web interface, go to **Overview** → **Server** → **Logs** → **Settings**.
The **Remote Syslog Settings** page is displayed
2. Enable remote syslog, specify the server address, and the port number. For information about the options, see the *iDRAC7 Online Help*.
3. Click **Apply**.
The settings are saved. All logs written to the lifecycle log are also simultaneously written to configured remote server(s).

Configuring Remote System Logging Using RACADM

To configure the remote syslog server settings, use the following RACADM objects:

- `cfgRhostsSyslogEnable`
- `cfgRhostsSyslogPort`
- `cfgRhostsSyslogServer1`

- `cfgRhostsSyslogServer2`
- `cfgRhostsSyslogServer3`

For more information, see the *RACADM Command Line Reference Guide for iDRAC7 and CMC* available at support.dell.com/manuals.

Monitoring and Managing Power

You can use iDRAC7 to monitor and manage the power requirements of the managed system. This helps to protect the system from power outages by appropriately distributing and regulating the power consumption on the system.

The key features are:

- **Power Monitoring** — View the power status, history of power measurements, the current averages, peaks, and so on for the managed system.
- **Power Capping** — View and set the power cap for the managed system, including displaying the minimum and maximum potential power consumption. This is a licensed feature.
- **Power Control** — Enables you to remotely perform power control operations (such as, power on, power off, system reset, power cycle, and graceful shutdown) on the managed system.
- **Power Supply Options** — Configure the power supply options such as redundancy policy, hot spare, and power factor correction.

Related Links

- [Monitoring Power](#)
- [Executing Power Control Operations](#)
- [Power Capping](#)
- [Configuring Power Supply Options](#)
- [Enabling or Disabling Power Button](#)

Monitoring Power

iDRAC7 monitors the power consumption in the system continuously and displays the following power values:

- Power consumption warning and critical thresholds.
- Cumulative power, peak power, and peak amperage values.
- Power consumption over the last hour, last day or last week.
- Average, minimum, and maximum power consumption.
- Historical peak values and peak timestamps.
- Peak headroom and instantaneous headroom values (for rack and tower servers).

Monitoring Power Using Web Interface

To view the power monitoring information, in iDRAC7 Web interface, go to **Overview** → **Server** → **Power/Thermal** → **Power Monitoring**. The **Power Monitoring** page is displayed. For more information, see the *iDRAC7 Online Help*.

Monitoring Power Using RACADM

To view the power monitoring information, use the **System.Power** group objects with the **get** command or the **cfgServerPower** object with the **getconfig** command. For more information, see the *RACADM Command Line Reference Guide for iDRAC7 and CMC* available at support.dell.com/manuals.

Executing Power Control Operations

iDRAC7 enables you to remotely perform a power-on, power off, reset, graceful shutdown, Non-Masking Interrupt (NMI), or power cycle using the Web interface or RACADM.

You can also perform these operations using Lifecycle Controller Remote Services or WS-Management. For more information, see the *Lifecycle Controller Remote Services User's Guide* available at support.dell.com/manuals and the *Dell Power State Management* profile document available at delltechcenter.com.

Executing Power Control Operations Using Web Interface

To perform power control operations:

1. In iDRAC7 Web interface, go to **Overview** → **Server** → **Power/Thermal** → **Power Configuration** → **Power Control**. The **Power Control** page is displayed.
2. Select the required power operation:
 - Power On System
 - Power Off System
 - NMI (Non-Masking Interrupt)
 - Graceful Shutdown
 - Reset System (warm boot)
 - Power Cycle System (cold boot)
3. Click **Apply**. For more information, see the *iDRAC7 Online Help*.

Executing Power Control Operations Using RACADM

To perform power actions, use the **serveraction** command. For more information, see the *RACADM Command Line Reference Guide for iDRAC7 and CMC* available at support.dell.com/manuals.

Power Capping

You can view the power threshold limits that covers the range of AC and DC power consumption that a system under heavy workload presents to the datacenter. This is a licensed feature.

Power Capping in Blade Servers

Before a blade server powers up, iDRAC7 provides CMC with its power requirements. It is higher than the actual power that the blade can consume and is calculated based on limited hardware inventory information. It may request a smaller power range after the server is powered up based on the actual power consumed by the server. If the power consumption increases over time and if the server is consuming power near its maximum allocation, iDRAC7 may request an increase of the maximum potential power consumption thus increasing the power envelope. iDRAC7 only increases its maximum potential power consumption request to CMC. It does not request for a lesser minimum potential power if the consumption decreases. iDRAC7 continues to request for more power if the power consumption exceeds the power allocated by CMC.

After, the system is powered on and initialized, iDRAC7 calculates a new power requirement based on the actual blade configuration. The blade stays powered on even if the CMC fails to allocate new power request.

CMC reclaims any unused power from lower priority servers and subsequently allocates the reclaimed power to a higher priority infrastructure module or a server.

If there is not enough power allocated, the blade server does not power on. If the blade has been allocated enough power, the iDRAC7 turns on the system power.

Viewing and Configuring Power Cap Policy

When power cap policy is enabled, it enforces user-defined power limits for the system. If not, it uses the hardware power protection policy that is implemented by default. This power protection policy is independent of the user defined policy. The system performance is dynamically adjusted to maintain power consumption close to the specified threshold.

Actual power consumption may be less for light workloads and momentarily may exceed the threshold until performance adjustments are completed. For example, for a given system configuration, the Maximum Potential Power Consumption is 700W and the Minimum Potential Power Consumption is 500W. You can specify and enable a Power Budget Threshold to reduce consumption from its current 650W to 525W. From that point onwards, the system's performance is dynamically adjusted to maintain power consumption so as to not exceed the user-specified threshold of 525W.

If the power cap value is set to be lower than the minimum recommended threshold, iDRAC7 may not be able maintain the requested power cap.

You can specify the value in Watts, BTU/hr, or as a percentage (%) of the recommended maximum power limit.

When setting the power cap threshold in BTU/hr, the conversion to Watts is rounded to the nearest integer. When reading the power cap threshold back, the Watts to BTU/hr conversion is again rounded in this manner. As a result, the value written could be nominally different than the value read; for example, a threshold set to 600 BTU/hr will be read back as 601 BTU/hr.

Configuring Power Cap Policy Using Web Interface

To view and configure the power policies:

1. In iDRAC7 Web interface, go to **Overview** → **Server** → **Power/Thermal** → **Power Configuration** → **Power Configuration**. The **Power Configuration** page is displayed.
The **Power Configuration** page is displayed. The current power policy limit is displayed under the **Currently Active Power Cap Policy** section.
2. Select **Enable** under **iDRAC Power Cap Policy**.
3. Under **User-Defined Limits** section, enter the maximum power limit in Watts and BTU/hr or the maximum % of recommended system limit.
4. Click **Apply** to apply the values.

Configuring Power Cap Policy Using RACADM

To view and configure the current power cap values:

- Use the following objects with the **config** subcommand:
 - `cfgServerPowerCapWatts`
 - `cfgServerPowerCapBTUhr`
 - `cfgServerPowerCapPercent`
 - `cfgServerPowerCapEnable`
- Using the following objects with the **set** subcommand:
 - `System.Power.Cap.Enable`

- System.Power.Cap.Watts
- System.Power.Cap.Btuhr
- System.Power.Cap.Percent

For more information, see the *RACADM Command Line Reference Guide for iDRAC7 and CMC* available at support.dell.com/manuals.

Configuring Power Cap Policy Using iDRAC Settings Utility

To view and configure power policies:

1. In iDRAC Settings utility, go to **Power Configuration**.
The **iDRAC Settings Power Configuration** page is displayed.
2. Select **Enabled** to enable the **iDRAC Power Limit Policy**. Else, select **Disabled**.
3. Use the recommended settings, or under **User Defined Limits**, enter the required limits.
For more information about the options, see the *iDRAC Settings Utility Online Help*.
4. Click **Back**, click **Finish**, and then click **Yes**.
The power cap values are configured.

Configuring Power Supply Options

You can configure the power supply options such as redundancy policy, hot spare, and power factor correction.

Hot spare is a power supply feature that configures redundant Power Supply Units (PSUs) to turn off depending on the server load. This allows the remaining PSUs to operate at a higher load and efficiency. This requires PSUs that support this feature, so that it quickly powers ON when needed.

In a two PSU system, you must set the primary PSU (that must be ON.) In a four PSU system, you must set the pair of PSUs (1+1 or 2+2) that must be ON.

After Hot Spare is enabled, PSUs can become active or go to sleep mode based on load.

Power factor is the ratio of real power consumed to the apparent power. If power factor correction is disabled, power consumption is reduced when the server is powered off. By default, power factor correction is enabled when the system is turned on.

Configuring Power Supply Options Using Web Interface

To configure the power supply options:

1. In iDRAC7 Web interface, go to **Overview** → **Server** → **Power/Thermal** → **Power Configuration** → **Power Configuration**. The **Power Configuration** page is displayed.
2. Under **Power Supply Options**, select the required options. For more information, see *iDRAC7 Online Help*.
3. Click **Apply**. The power supply options are configured.

Configuring Power Supply Options Using RACADM

To configure the power supply options, use the following objects with the **set** subcommand:

- System.Power.RedundancyPolicy
- System.Power.Hotspare.Enable
- System.Power.Hotspare.PrimaryPSU
- System.Power.PFC.Enable

For more information, see the *RACADM Command Line Reference Guide for iDRAC7 and CMC* available at support.dell.com/manuals.

Configuring Power Supply Options Using iDRAC Setting Utility

To configure the power supply options:

1. In iDRAC Settings utility, go to **Power Configuration**.
The **iDRAC Settings Power Configuration** page is displayed.
2. Under Power Supply Options:
 - Enable or disable power supply redundancy.
 - Enable or disable hot spare.
 - Set the primary power supply unit.
 - Enable or disable power factor correction. For more information about the options, see the *iDRAC Settings Utility Online Help*.
3. Click **Back**, click **Finish**, and then click **Yes**.
The power supply options are configured.

Enabling or Disabling Power Button

To enable or disable the power button on the managed system:

1. In iDRAC Settings utility, go to **Security Configuration**.
The **iDRAC Settings Security Configuration** page is displayed.
2. Select **Enabled** to enable the power button. Else, select **Disabled**.
3. Click **Back**, click **Finish**, and then click **Yes**. The settings are saved.

Configuring and Using Virtual Console

You can use the virtual console to manage a remote system using the keyboard, video, and mouse on your management station to control the corresponding devices on a managed server. This is a licensed feature for rack and tower servers. It is available by default in blade servers.

The key features are:

- A maximum of four simultaneous Virtual Console sessions are supported. All the sessions view the same managed server console simultaneously.
- You can launch virtual console in a supported Web browser using Java or ActiveX plug-in. You must use the Java viewer if the management station runs on an operating system other than Windows.
- When you open a Virtual Console session, the managed server does not indicate that the console has been redirected.
- You can open multiple Virtual Console sessions from a single management station to one or more managed systems simultaneously.
- You cannot open two virtual console sessions from the management station to the managed server using the same plug-in.
- If a second user requests a Virtual Console session, the first user is notified and is given the option to refuse access, allow read-only access, or allow full shared access. The second user is notified that another user has control. The first user must respond within thirty seconds, or else access is granted to the second user based on the default setting. When two sessions are concurrently active, the first user sees a message in the upper-right corner of the screen that the second user has an active session. If neither the first or second user has administrator privileges, terminating the first user's session automatically terminates the second user's session.

Related Links

[Configuring Web Browsers to Use Virtual Console](#)

[Configuring Virtual Console](#)

[Launching Virtual Console](#)


Supported Screen Resolutions and Refresh Rates

The following table lists the supported screen resolutions and corresponding refresh rates for a Virtual Console session running on the managed server.

Table 22. 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 |


It is recommended that you configure your monitor display resolution to 1280x1024 pixels or higher.

 **NOTE:** If you have an active Virtual Console session and a lower resolution monitor is connected to the Virtual Console, the server console resolution may reset if the server is selected on the local console. If the system is running a Linux operating system, an X11 console may not be viewable on the local monitor. Press <Ctrl><Alt><F1> at the iDRAC7 Virtual Console to switch Linux to a text console.


Configuring Web Browsers to Use Virtual Console

To use Virtual Console on your management station:

1. Make sure that a supported version of Internet Explorer (Windows) or Mozilla Firefox (Windows or Linux) is installed.
For more information about the supported browser versions for Windows and Linux operating systems, see the readme.
2. Configure the Web browser to use ActiveX or Java plug-in.
ActiveX viewer is supported only with Internet Explorer. A Java viewer is supported on any browser.
3. If Virtual Console and Virtual Media are configured to use Java plug-in, then you must disable *Enhanced Security Mode* in Internet Explorer. If this is not possible, then in iDRAC7, configure Virtual Console to use ActiveX plug-in. You must enable ActiveX control in IE, add the iDRAC7 Web URL to the Intranet security zone, and set the security level for this zone as *Medium-Low* for Virtual Console and Virtual Media to work properly.

 **NOTE:** For Windows Server operating systems, you can access the IE Enhanced Security Configuration settings in the **Control Panel** → **Administrative Tools Server Manager** → **Internet Explorer Enhanced Security Configuration** window. You can also set the required privileges in this window.

4. Import the root certificates on the managed system to avoid the pop-ups that prompt you to verify the certificates.
5. Install the **compat-libstdc++-33-3.2.3-61** related package.


 **NOTE:** On Windows, the "compat-libstdc++-33-3.2.3-61" related package may be included in the .NET framework package or the operating system package.

Related Links

- [Configuring Web Browser to Use Java Plug-in](#)
- [Configuring IE to Use ActiveX Plug-in](#)
- [Importing CA Certificates to Management Station](#)

Configuring Web Browser to Use Java Plug-in

Install a Java Runtime Environment (JRE) if you are using Firefox or IE and want to use the Java Viewer.

 **NOTE:** Install a 32-bit or 64-bit JRE version on a 64-bit operating system or a 32-bit JRE version on a 32-bit operating system.

To configure IE to use Java plug-in:

- Disable automatic prompting for file downloads in Internet Explorer.
- Disable *Enhanced Security Mode* in Internet Explorer.

Related Links


- [Configuring Virtual Console](#)

Configuring IE to Use ActiveX Plug-in


You can use ActiveX plug-in only with Internet Explorer.

To configure IE to use ActiveX plug-in:

1. Clear the browser's cache.
2. Add iDRAC7 IP or hostname to the **Trusted Sites** list.
3. Reset the custom settings to **Medium-low** or change the settings to allow installation of signed ActiveX plug-ins.
4. Enable the browser to download encrypted content and to enable third-party browser extensions. To do this, go to **Tools** → **Internet Options** → **Advanced**, clear the **Do not save encrypted pages to disk** option, and select the **Enable third-party browser extensions** option.

 **NOTE:** Restart Internet Explorer for the Enable third-party browser extension setting to take effect.

5. Go to **Tools** → **Internet Options** → **Security** and select the zone you want to run the application.
6. Click **Custom level**. In the **Security Settings** window, do the following:
 - Select **Enable** for **Automatic prompting for ActiveX controls**.
 - Select **Prompt** for **Download signed ActiveX controls**.
 - Select **Enable** or **Prompt** for **Run ActiveX controls and plug-ins**.
 - Select **Enable** or **Prompt** for **Script ActiveX controls marked safe for scripting**.
7. Click **OK** to close the **Security Settings** window.
8. Click **OK** to close the **Internet Options** window.

 **NOTE:** Before installing the ActiveX control, Internet Explorer may display a security warning. To complete the ActiveX control installation procedure, accept the ActiveX control when Internet Explorer prompts you with a security warning.

Related Links

[Clearing Browser Cache](#)

[Additional Settings for Windows Vista or Newer Microsoft Operating Systems](#)

Additional Settings for Windows Vista or Newer Microsoft Operating Systems


The Internet Explorer browsers in Windows Vista or newer operating systems have an additional security feature called *Protected Mode*.

To launch and run ActiveX applications in Internet Explorer browsers with *Protected Mode*:

1. Run IE as an administrator.
2. Go to **Tools** → **Internet Options** → **Security** → **Trusted Sites**.
3. Make sure that the **Enable Protected Mode** option is not selected for Trusted Sites zone. Alternatively, you can add the iDRAC7 address to sites in the Intranet zone. By default, protected mode is turned off for sites in Intranet Zone and Trusted Sites zone.
4. Click **Sites**.
5. In the **Add this website to the zone** field, add the address of your iDRAC7 and click **Add**.
6. Click **Close** and then click **OK**.
7. Close and restart the browser for the settings to take effect.

Clearing Browser Cache

If you have issues when operating the Virtual Console, (out of range errors, synchronization issues, and so on) clear the browser's cache to remove or delete any old versions of the viewer that may be stored on the system and try again.

 **NOTE:** You must have administrator privilege to clear the browser's cache.

Clearing Earlier ActiveX Versions in IE7

To clear earlier versions of Active-X viewer for IE7, do the following:

1. Close the Video Viewer and Internet Explorer browser.
2. Open the Internet Explorer browser again and go to **Internet Explorer** → **Tools** → **Manage Add-ons** and click **Enable or Disable Add-ons**. The **Manage Add-ons** window is displayed.
3. Select **Add-ons that have been used by Internet Explorer** from the **Show** drop-down menu.
4. Delete the *Video Viewer* add-on.

Clearing Earlier ActiveX Versions in IE8

To clear earlier versions of Active-X viewer for IE8, do the following:

1. Close the Video Viewer and Internet Explorer browser.
2. Open the Internet Explorer browser again and go to **Internet Explorer** → **Tools** → **Manage Add-ons** and click **Enable or Disable Add-ons**. The **Manage Add-ons** window is displayed.
3. Select **All Add-ons** from the **Show** drop-down menu.
4. Select the *Video Viewer* add-on and click the **More Information** link.
5. Select **Remove** from the **More Information** window.
6. Close the **More Information** and the **Manage Add-ons** windows.

Clearing Earlier Java Versions

To clear older versions of Java viewer in Windows or Linux, do the following:

1. At the command prompt, run `javaws-viewer` or `javaws-uninstall`.
The **Java Cache** viewer is displayed.
2. Delete the items titled *iDRAC7 Virtual Console Client*.

Importing CA Certificates to Management Station

When you launch Virtual Console or Virtual Media, prompts are displayed to verify the certificates. If you have custom Web server certificates, you can avoid these prompts by importing the CA certificates to the Java or ActiveX trusted certificate store.

Related Links

- [Importing CA certificate to Java Trusted Certificate Store](#)
- [Importing CA Certificate to ActiveX Trusted Certificate Store](#)

Importing CA certificate to Java Trusted Certificate Store

To import the CA certificate to the Java trusted certificate store:

1. Launch the **Java Control Panel**.
2. Click **Security** tab and then click **Certificates**.
The **Certificates** dialog box is displayed.
3. From the Certificate type drop-down menu, select **Trusted Certificates**.
4. Click **Import**, browse, select the CA certificate (in Base64 encoded format), and click **Open**.
The selected certificate is imported to the Web start trusted certificate store.
5. Click **Close** and then click **OK**. The **Java Control Panel** window closes.

Importing CA Certificate to ActiveX Trusted Certificate Store

You must use the OpenSSL command line tool to create the certificate Hash using Secure Hash Algorithm (SHA). It is recommended to use OpenSSL tool 1.0.x and later since it uses SHA by default. The CA certificate must be in Base64 encoded PEM format. This is one-time process to import each CA certificate.

To import the CA certificate to the ActiveX trusted certificate store:

1. Open the OpenSSL command prompt.
2. Run a 8 byte hash on the CA certificate that is currently in-use on the management station using the command:
`openssl x509 -in (name of CA cert) -noout -hash`
An output file is generated. For example, if the CA certificate file name is **cacert.pem**, the command is:
`openssl x509 -in cacert.pem -noout -hash`
The output similar to "431db322" is generated.
3. Rename the CA file to the output file name and include a ".0" extension. For example, 431db322.0.
4. Copy the renamed CA certificate to your home directory. For example, **C:\Documents and Settings\<user> directory**.

Configuring Virtual Console

Before configuring the Virtual Console, make sure that the management station is configured.

You can configure the virtual console using iDRAC7 Web interface or RACADM command line interface.

Related Links

[Configuring Web Browsers to Use Virtual Console](#)

[Launching Virtual Console](#)

Configuring Virtual Console Using Web Interface

To configure Virtual Console using iDRAC7 Web interface:

1. Go to **Overview** → **Server** → **Console**. The **Virtual Console** page is displayed.
2. Enable virtual console and specify the required values. For information about the options, see the *iDRAC7 Online Help*.
3. Click **Apply**. The virtual console is configured.

Configuring Virtual Console Using RACADM

To configure the Virtual Console, use the following objects:

- `cfgRACTuneConRedirEnable`
- `cfgRACTuneConRedirPort`
- `cfgRACTuneConRedirEncryptEnable`
- `cfgRacTunePluginType`
- `cfgRacTuneVirtualConsoleAuthorizeMultipleSessions`

For more information on these objects, see the *RACADM Command Line Reference Guide for iDRAC7 and CMC* available at support.dell.com/manuals.

Previewing Virtual Console


Before launching the Virtual Console, you can preview the state of the Virtual Console on the **System** → **Properties** → **System Summary** page. The **Virtual Console Preview** section displays an image showing the state of the Virtual Console. The image is refreshed every 30 seconds. This is a licensed feature.



NOTE: The Virtual Console image is available only if you have enabled Virtual Console.

Launching Virtual Console

You can launch the virtual console using the iDRAC7 Web Interface or a URL.

 **NOTE:** Do not launch a Virtual Console session from a Web browser on the managed system.

Before launching the Virtual Console, make sure that:

- You have administrator privileges.
- Web browser is configured to use Java or ActiveX plug-ins.
- Minimum network bandwidth of one MB/sec is available.

While launching Virtual Console using 32-bit or 64-bit IE browsers, the required plug-in (Java or ActiveX) is available in the respective browser. The Internet Options settings are common for both the browsers.

While launching the Virtual Console using Java plug-in, occasionally you may see a Java compilation error. To resolve this, go to **Java control panel** → **General** → **Network Settings** and select **Direct Connection**.

If the Virtual Console is configured to use ActiveX plug-in, it may not launch the first time. This is because of the slow network connection and the temporary credentials (that Virtual Console uses to connect) timeout is two minutes. The ActiveX client plug-in download time may exceed this time. After the plug-in is successfully downloaded, you can launch the Virtual Console normally.

When you launch Virtual Console for the first time using IE8 with ActiveX plug-in, a "Certificate Error: Navigation Blocked" message may be displayed. Click **Continue to this website** and then click **Install** to install ActiveX controls on the **Security Warning** window. The Virtual Console session is launched.

Related Links

- [Launching Virtual Console Using URL](#)
- [Configuring Web Browser to Use Java Plug-in](#)
- [Configuring IE to Use ActiveX Plug-in](#)
- [Launching Virtual Console Using Web Interface](#)
- [Synchronizing Mouse Pointers](#)

Launching Virtual Console Using Web Interface

You can launch the virtual console in the following ways:

- Go to **Overview** → **Server** → **Console**. The **Virtual Console** page is displayed. Click **Launch Virtual Console**. The **Virtual Console Viewer** is launched.
- Go to **Overview** → **Server** → **Properties**. The **System Summary** page is displayed. Under **Virtual Console Preview** section, click **Launch**. The **Virtual Console Viewer** is launched.

The **Virtual Console Viewer** displays the remote system's desktop. Using this viewer, you can control the remote system's mouse and keyboard functions from your management station.

Multiple message boxes may appear after you launch the application. To prevent unauthorized access to the application, navigate through these message boxes within three minutes. Otherwise, you are prompted to relaunch the application.

If one or more Security Alert windows appear while launching the viewer, click Yes to continue.

Two mouse pointers may appear in the viewer window: one for the managed server and another for your management station. If the cursors do not synchronize, select **Single Cursor** from the **Tools** menu in the Virtual Console Viewer.


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>**
- **Control Panel** → **Power Options** → **High-Performance** → **Advanced Settings** → **Hard Disk** → **Turnoff Hard Disk After <time_out>**

Launching Virtual Console Using URL

To launch the Virtual Console using the URL:


1. Open a supported Web browser and in the address box, type the following URL in lower case: **https://iDRAC7_ip/console**
2. Based on the login configuration, the corresponding **Login** page is displayed:
 - If Single Sign On is disabled and Local, Active Directory, LDAP, or Smart Card login is enabled, the corresponding **Login** page is displayed.
 - If Single-Sign On is enabled, the **Virtual Console Viewer** is launched and the **Virtual Console** page is displayed in the background.

 **NOTE:** Internet Explorer supports Local, Active Directory, LDAP, Smart Card (SC) and Single Sign-On (SSO) logins. Firefox supports Local, AD, and SSO logins on Windows-based operating system and Local, Active Directory, and LDAP logins on Linux-based operating systems.

 **NOTE:** If you do not have Access Virtual Console privilege but have Access Virtual Media privilege, then using this URL launches the Virtual Media instead of the Virtual Console.

Using Virtual Console Viewer

The Virtual Console Viewer provides various controls such as mouse synchronization, chat options, keyboard macros, power actions, and access to Virtual Media. For more information, see the *iDRAC7 Online Help*.

 **NOTE:** If the remote server is powered off, the message 'No Signal' is displayed.

The Virtual Console Viewer title bar displays the DNS name or the IP address of the iDRAC7 you are connected to from the management station. If iDRAC7 does not have a DNS name, then the IP address is displayed. The format is:

- For rack and tower servers:
`<DNS name / IPv6 address / IPv4 address>, <Model>, User: <username>, <fps>`
- For blade servers:
`<DNS name / IPv6 address / IPv4 address>, <Model>, <Slot number>, User: <username>, <fps>`

Sometimes the Virtual Console Viewer may display low quality video. This is due to slow network connectivity that leads to loss of one or two video frames when you start the Virtual Console session. To transmit all the video frames and improve the subsequent video quality, do any of the following:


- In the **System Summary** page, under **Virtual Console Preview** section, click **Refresh**.
- In the **Virtual Console Viewer**, under **Performance** tab, set the slider to **Maximum Video Quality**.

Synchronizing Mouse Pointers

When you connect to a managed system through the Virtual Console, the mouse acceleration speed on the managed system may not synchronize with the mouse pointer on the management station and displays two mouse pointers in the Viewer window.

When using Red Hat Enterprise Linux or Novell SUSE Linux, configure the mouse mode for Linux before you launch the Virtual Console viewer. The operating system's default mouse settings are used to control the mouse arrow in the Virtual Console viewer.

When two mouse cursors are seen on the client Virtual Console viewer, it indicates that the server's operating system supports Relative Positioning. This is typical for Linux operating systems or Lifecycle Controller and causes two mouse cursors if the server's mouse acceleration settings are different from the mouse acceleration settings on the Virtual Console client. To resolve this, switch to single cursor by selecting **Single Cursor** from the **Tools** menu (in the Virtual Console Viewer) or try to match the mouse acceleration on the managed system and the management station. To exit single cursor mode, press <F9>.

 **NOTE:** This is not applicable for managed systems running Windows operating system since they support Absolute Positioning.

When using the Virtual Console to connect to a managed system with a recent Linux distribution operating system installed, you may experience mouse synchronization problems. This may be due to the Predictable Pointer Acceleration feature of the GNOME desktop. For correct mouse synchronization in the iDRAC7 Virtual Console, this feature must be disabled. To disable Predictable Pointer Acceleration, in the mouse section of the `/etc/X11/xorg.conf` file, add:

```
Option "AccelerationScheme" "lightweight".
```

If synchronization problems continue, do the following additional change in the `<user_home>/.gconf/desktop/gnome/peripherals/mouse/%gconf.xml` file:

Change the values for `motion_threshold` and `motion_acceleration` to `-1`.

If you turn off mouse acceleration in GNOME desktop, in the Virtual Console viewer, go to **Tools** → **Session Options** → **Mouse**. Under **Mouse Acceleration** tab, select **None**.

For exclusive access to the managed server console, you must disable the local console and reconfigure the **Max Sessions** to `1` on the **Virtual Console page**.

Passing All Keystrokes Through Virtual Console

You can enable Pass All Keystrokes to Server option and send all keystrokes and key combinations from the management station to the managed system through the Virtual Console Viewer. If it is disabled, it directs all the key combinations to the management station where the Virtual Console session is running.

The behavior of the Pass All Keystrokes to Server feature depends on the:

- Plug-in type (Java or ActiveX) based on which Virtual Console session is launched.
- Operating system running on the management station and managed system. The key combinations that are meaningful to the operating system on the management station are not passed to the managed system.
- Virtual Console Viewer mode—Windowed or Full Screen.
 - In Full Screen mode, Pass all keystrokes to server is enabled by default.
 - In windowed mode, the keys passed only when the Virtual Console Viewer is visible and is active.
 - When changed from Full Screen mode to Windowed mode, the previous state of Pass all keys is resumed.

Related Links

[Java-based Virtual Console Session running on Windows Operating System](#)

[Java Based Virtual Console Session Running on Linux Operating System](#)

[ActiveX Based Virtual Console Session Running on Windows Operating System](#)

Java-based Virtual Console Session running on Windows Operating System

- Ctrl+Alt+Del key is not sent to the managed system, but always interpreted by the management station.
- When Pass All Keystrokes to Server is enabled, the following keys are not sent to the managed system:

- Browser Back Key
 - Browser Forward Key
 - Browser Refresh key
 - Browser Stop Key
 - Browser Search Key
 - Browser Favorites key
 - Browser Start and Home key
 - Volume mute key
 - Volume down key
 - Volume up key
 - Next track key
 - Previous track key
 - Stop Media key
 - Play/Pause media key
 - Start mail key
 - Select media key
 - Start Application 1 key
 - Start Application 2 key
- All the individual keys (not a combination of different keys, but a single key stroke) are always sent to the managed system. This includes all the Function keys, Shift, Alt, Ctrl key and Menu keys. Some of these keys affect both management station and managed system.
For example, if the management station and the managed system is running Windows operating system, and Pass All Keys is disabled, when you press the Windows key to open the **Start** Menu, the **Start** menu opens on both management station and managed system. However, if Pass All Keys is enabled, then the **Start** menu is opened only on the managed system and not on the management station.
 - When Pass All Keys is disabled, the behavior depends on the key combinations pressed and the special combinations interpreted by the operating system on the management station.

Java Based Virtual Console Session Running on Linux Operating System

The behavior mentioned for Windows operating system is also applicable for Linux operating system with the following exceptions:

- When Pass all keystrokes to server is enabled, <Ctrl+Alt+Del> is passed to the operating system on the managed system.
- Magic SysRq keys are key combinations interpreted by the Linux Kernel. It is useful if the operating system on the management station or the managed system freezes and you need to recover the system. You can enable the magic SysRq keys on the Linux operating system using one of the following methods:
 - Add an entry to **/etc/sysctl.conf**
 - echo "1" > /proc/sys/kernel/sysrq
- When Pass all keystrokes to server is enabled, the magic SysRq keys are sent to the operating system on the managed system. The key sequence behavior to reset the operating system, that is reboot without un-mounting or sync, depends on whether the magic SysRq is enabled or disabled on the management station:
 - If SysRq is enabled on the management station, then <Ctrl+Alt+SysRq+b> or <Alt+SysRq+b> resets the management station irrespective of the system's state.
 - If SysRq is disabled on the management station, then the <Ctrl+Alt+SysRq+b> or <Alt+SysRq+b> keys resets the operating system on the managed system.
 - Other SysRq key combinations (example, <Alt+SysRq+k>, <Ctrl+Alt+SysRq+m>, and so on) are passed to the managed system irrespective of the SysRq keys enabled or not on the management station.

ActiveX Based Virtual Console Session Running on Windows Operating System

The behavior of the pass all keystrokes to server feature in ActiveX based Virtual Console session running on Windows operating system is similar to the behavior explained for Java based Virtual Console session running on the Windows management station with the following exceptions:

- When Pass All Keys is disabled, pressing F1 launches the application Help on both management station and managed system, and the following message is displayed:
`Click Help on the Virtual Console page to view the online Help`
- The media keys may not be blocked explicitly.
- <Alt + Space>, <Ctrl + Alt + +>, <Ctrl + Alt + -> are not sent to the managed system and is interpreted by the operating system on the management station.

Managing Virtual Media

Virtual media allows the managed server to access media devices on the management station or ISO CD/DVD images on a network share as if they were devices on the managed server.

Using the Virtual Media feature, you can:

- Remotely access media connected to a remote system over the network
- Install applications
- Update drivers
- Install an operating system on the managed system

This is a licensed feature for rack and tower servers. It is available by default for blade servers.

The key features are:

- Virtual Media supports virtual optical drives (CD/DVD), floppy drives (including USB-based drives), and USB flash drives.
- You can attach only one floppy, USB flash drive, image, or key and one optical drive on the management station to a managed system. Supported floppy drives include a floppy image or one available floppy drive. Supported optical drives include a maximum of one available optical drive or one ISO image file.

The following figure shows a typical Virtual Media setup.

- Virtual floppy media of iDRAC7 is not accessible from virtual machines.
- Any connected Virtual Media emulates a physical device on the managed system.
- On Windows-based managed systems, the Virtual Media drives are auto-mounted if they are attached and configured with a drive letter.
- On Linux-based managed systems with some configurations, the Virtual Media drives are not auto-mounted. To manually mount the drives, use the mount command.
- All the virtual drive access requests from the managed system are directed to the management station across the network.
- Virtual devices appear as two drives on the managed system without the media being installed in the drives.
- You can share the management station CD/DVD drive (read only), but not a USB media, between two managed systems.
- Virtual media requires a minimum available network bandwidth of 128 Kbps.
- If LOM or NIC failover occurs, then the Virtual Media session may be disconnected.

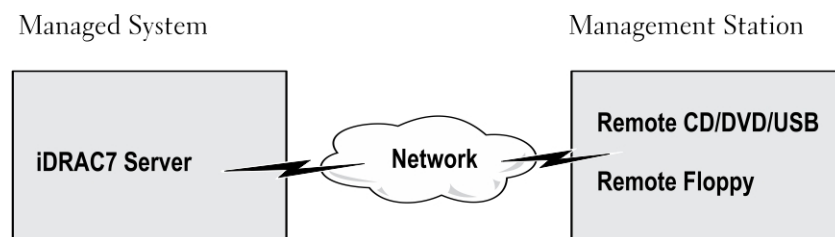


Figure 4. Virtual Media Setup

Supported Drives and Devices

The following table lists the drives supported through virtual media.

Table 23. Supported Drives and Devices

| Drive | Supported Storage Media |
|------------------------|---|
| Virtual Optical Drives | <ul style="list-style-type: none">• Legacy 1.44 floppy drive with a 1.44 floppy diskette• CD-ROM• DVD• CD-RW• Combination drive with CD-ROM media |
| Virtual floppy drives | <ul style="list-style-type: none">• CD-ROM/DVD image file in the ISO9660 format• Floppy image file in the ISO9660 format |
| USB flash drives | <ul style="list-style-type: none">• USB CD-ROM drive with CD-ROM media• USB Key image in the ISO9660 format |

Configuring Virtual Media

Before you configure the Virtual Media settings, make sure that you have configured your Web browser to use Java or ActiveX plug-in.

Related Links

[Configuring Web Browsers to Use Virtual Console](#)

Configuring Virtual Media Using iDRAC7 Web Interface

To configure virtual media settings:

 **CAUTION: Do not reset iDRAC7 when running a Virtual Media session. Otherwise, undesirable results may occur, including data loss.**

1. In the iDRAC7 Web interface, go to **Overview** → **Server** → **Attached Media**.
2. Specify the required settings. For more information, see the *iDRAC7 Online Help*.
3. Click **Apply** to save the settings.

Configuring Virtual Media Using RACADM

To configure the virtual media, use the objects in the **cfgRacVirtual** group. For more information, see the *RACADM Command Line Reference Guide for iDRAC7 and CMC* available at support.dell.com/manuals.

Configuring Virtual Media Using iDRAC Settings Utility

You can attach, detach, or auto-attach virtual media using the iDRAC Settings utility. To do this:

1. In the iDRAC Settings utility, go to **Virtual Media**.

The **iDRAC Settings Virtual Media** page is displayed.

2. Select **Detach**, **Attach**, or **Auto attach** based on the requirement. For more information about the options, see *iDRAC Settings Utility Online Help*.
3. Click **Back**, click **Finish**, and then click **Yes**.

The alert settings are configured.

Attached Media State and System Response

The following table describes the system response based on the Attached Media setting.

Table 24. Attached Media State and System Response

| Attached Media State | System Response |
|----------------------|---|
| Detach | Cannot map an image to the system. |
| Attach | Media is mapped even when Client View is closed. |
| Auto-attach | Media is mapped when Client View is opened and unmapped when Client View is closed. |

Accessing Virtual Media

You can access Virtual Media with or without using the Virtual Console. Before you access the Virtual Media, make sure to configure the Web browsers.

Related Links

- [Configuring Web Browsers to Use Virtual Console](#)
- [Configuring Virtual Media](#)


Launching Virtual Media Using Virtual Console

Before you launch Virtual Media through the Virtual Console, make sure that:


- Virtual Console is enabled.
- System is configured to unhide empty drives. To do this, in Windows Explorer, navigate to **Folder Options**, clear the **Hide empty drives in the Computer folder** options and click **OK**.

To access Virtual Media using Virtual Console:

1. In the iDRAC7 Web Interface, go to **Overview** → **Server** → **Console** .
The **Virtual Console** page is displayed.
2. Click **Launch Virtual Console**.
The **Virtual Console Viewer** is launched.

 **NOTE:** On Linux, JAVA is the default plug-in type for accessing the Virtual Console. On Windows, to access the Virtual Console using JAVA, open the **.jnlp** file to launch the Virtual Console. 3Click

3. Click **Virtual Media** → **Launch Virtual Media**.
The Virtual Media **Client View** window is displayed listing the devices available for mapping

 **NOTE:** The **Virtual Console Viewer** window must remain active while you access the Virtual Media.

Related Links

- [Configuring Web Browsers to Use Virtual Console](#)

Launching Virtual Media Without Using Virtual Console

Before you launch Virtual Media when the **Virtual Console** is disabled, make sure that

- Virtual Media is in *Attach* state.
- System is configured to unhide empty drives. To do this, in Windows Explorer, navigate to **Folder Options**, clear the **Hide empty drives in the Computer folder** option, and click **OK**.

To launch Virtual Media when Virtual Console is disabled:

1. In the iDRAC7 Web Interface, go to **Overview** → **Server** → **Console** .
The **Virtual Console** page is displayed.


2. Click **Launch Virtual Console**.


The following message is displayed:

```
Virtual Console has been disabled. Do you want to continue using Virtual Media redirection?
```

3. Click **OK** to connect to the Virtual Media.

The Virtual Media **Client View** window is displayed listing the devices available for mapping.

 **NOTE:** The virtual device drive letters on the managed system do not coincide with the physical drive letters on the management station.

 **NOTE:** The Virtual Media may not function correctly on Windows operating system clients that are configured with Internet Explorer Enhanced Security. To resolve this issue, see the Microsoft operating system documentation or contact the system administrator.

Related Links

[Configuring Virtual Media](#)

Adding Virtual Media Images

To add Virtual Media images, in the Virtual Media **Client View** window:

- To add images, click **Add Image** and then select the image file from the management station or the C: drive of the managed system.
The ISO or floppy image is added to the list of available devices.
- To add a folder as a ISO and floppy image, click **Add Folder as Image**. This feature creates a media image of the remote folder and mounts it as a USB attached device to the server's operating system.
The media is connected and the information is updated in the **Client View** window.
When folder is added as an image, a **.iso** file is created on the Desktop of the management station from where this feature is used. If this **.iso** file is moved or deleted, then the corresponding entry for this folder in the Virtual Media **Client View** window does not work. Therefore, it is recommended not to move or delete the **.iso** file while the *added folder* is being used. However, the **.iso** file can be removed after the relevant entry is first deselected and then removed using the **Remove Image** to remove the entry.

Removing Virtual Media Images

To remove the image, in the Virtual Media **Client View** window, select the required mapped image and click **Remove Image**.

The selected image is removed from the list of devices in the **Client View** window.


Viewing Virtual Device Details

To view the Virtual Devices details, in the Virtual Media **Client View** window, click **Details**. The **Details** section is displayed showing the available virtual devices and the read/write activity for each device.

Resetting USB


To reset the USB device:

1. In the Virtual Media **Client View** window, click **Details** and then click **USB Reset**.
A message is displayed warning the user that resetting the USB connection can affect all the input to the target device including Virtual Media, keyboard, and mouse.
2. Click **Yes**.
The USB is reset.

 **NOTE:** iDRAC7 Virtual Media does not terminate even after you log out of iDRAC7 Web interface session.

Mapping Virtual Drive

To map the virtual drive:

 **NOTE:** While using ActiveX-based Virtual Media, you must have administrative privileges to map an operating system DVD or a USB flash drive (that is connected to the management station.) To map the drives, launch IE as an administrator or add the iDRAC7 IP address to the list of trusted sites.

1. Disconnect any existing mapped drive before mapping it to another media source.
2. In the Virtual Media **Client View** window, add the image or the folder that has the image.
3. Under the **Mapped** column, select the check box related to the drive with the required image. To map writable devices as read-only, select the **Read-only** option for the device before it is mapped.
The device is mapped to the managed system.

Related Links

- [Displaying Correct Virtual Drives For Mapping](#)
- [Adding Virtual Media Images](#)

Displaying Correct Virtual Drives For Mapping

On a Linux-based management station, the Virtual Media **Client** window may display removable disks and floppy disks that are not part of the management station. To make sure that the correct virtual drives are available to map, you must enable the port setting for the connected SATA hard drive. To do this:

1. Reboot the operating system on the management station. During POST, press <F2> or <F12> to enter System Setup.
2. Go to **SATA settings**. The port details are displayed.
3. Enable the ports that are actually present and connected to the hard drive.
4. Access the Virtual Media **Client** window. It displays the correct drives that can be mapped.

Related Links

- [Mapping Virtual Drive](#)

Unmapping Virtual Drive

To unmap the virtual drive:

1. In the Virtual Media **Client View** window, under the **Mapped** column, clear the checkbox of the drive.
The virtual drive is unmapped from the managed system.
2. Click **Exit** to terminate the **Virtual Media** session.
The Virtual Media **Client View** window closes.

Setting Boot Order Through BIOS

Using the System BIOS Settings utility, you can set the managed system to boot from virtual optical drives or virtual floppy drives.

 **NOTE:** Changing Virtual Media while connected may stop the system boot sequence.

To enable the managed system to boot:

1. Boot the managed system.
2. Press <F2> to enter the **System Setup** page.
3. Go to **System BIOS Settings** → **Boot Settings** → **BIOS Boot Settings** → **Boot Sequence**.
In the pop-up window, the virtual optical drives and virtual floppy drives are listed with the standard boot devices.
4. Make sure that the virtual drive is enabled and listed as the first device with bootable media. If required, follow the on-screen instructions to modify the boot order.
5. Click **OK**, navigate back to **System BIOS Settings** page, and click **Finish**.
6. Click **Yes** to save the changes and exit.

The managed system reboots.

The managed system attempts to boot from a bootable device based on the boot order. If the virtual device is connected and a bootable media is present, the system boots to the virtual device. Otherwise, the system overlooks the device—similar to a physical device without bootable media.

Enabling Boot Once for Virtual Media

You can change the boot order only once when you boot after attaching remote Virtual Media device.

Before you enable the boot once option, make sure that:

- You have *Configure User* privilege.
- Map the local or virtual drives (CD/DVD, Floppy, or USB flash device) with the bootable media or image using the Virtual Media options
- Virtual Media is in *Attached* state for the virtual drives to appear in the boot sequence.

To enable the boot once option and boot the managed system from the Virtual Media:

1. In the iDRAC7 Web interface, go to **Overview** → **Server** → **Attached Media**.
2. Under **Virtual Media**, select the **Enable Boot Once** and click **Apply**.
3. Turn on the managed system and press <F2> to enter **iDRAC Settings**.
4. Change the boot sequence to boot from the remote Virtual Media device.
5. Reboot the server.

The managed system boots once from the Virtual Media.


Related Links

[Mapping Virtual Drive](#)

[Configuring Virtual Media](#)


Installing and Using VMCLI Utility

The Virtual Media Command Line Interface (VMCLI) utility is an interface that provides virtual media features from the management station to iDRAC7 on the managed system. Using this utility you can access virtual media features, including image files and physical drives, to deploy an operating system on multiple remote systems in a network.

 **NOTE:** You can run the VMCLI utility only on the management station.

The VMCLI utility supports the following features:

- Manage removable devices or images that are accessible through virtual media.
- Automatically terminate the session when the iDRAC7 firmware **Boot Once** option is enabled.
- Secure communications to iDRAC7 using Secure Sockets Layer (SSL).
- Execute VMCLI commands until:
 - The connections automatically terminate.
 - An operating system terminates the process.

 **NOTE:** To terminate the process in Windows, use the Task Manager.

Installing VMCLI

The VMCLI utility is included in the *Dell Systems Management Tools and Documentation* DVD.

To install the VMCLI utility:

1. Insert the *Dell Systems Management Tools and Documentation* DVD into the management station's DVD drive.
2. Follow the on-screen instructions to install DRAC tools.
3. After successful install, check `install\Dell\SysMgt\trac5` folder to make sure `vmcli.exe` exists. Similarly, check the respective path for UNIX.

The VMCLI utility is installed on the system.

Running VMCLI Utility

- If the operating system requires specific privileges or group membership, you require similar privileges to run the VMCLI commands.
- On Windows systems, non-administrators must have **Power User** privileges to run the VMCLI utility.
- On Linux systems, to access iDRAC7, run VMCLI utility, and log user commands, non-administrators must prefix `sudo` to the VMCLI commands. However, to add or edit users in the VMCLI administrators group, use the `visudo` command.


VMCLI Syntax

The VMCLI interface is identical on both Windows and Linux systems. The VMCLI syntax is:

```
VMCLI [parameter] [operating_system_shell_options]
```

For example, `vmcli -r iDRAC7-IP-address:iDRAC7-SSL-port`

The *parameter* enables VMCLI to connect to the specified server, access iDRAC7, and map to the specified virtual media.

 **NOTE:** VMCLI syntax is case-sensitive.

To ensure security, it is recommended to use the following VMCLI parameters:

- `vmcli -i` — Enables an interactive method of starting VMCLI. It ensures that the user name and password are not visible when processes are examined by other users.
- `vmcli -r <iDRAC7-IP-address[:iDRAC7-SSL-port]> -S -u <iDRAC7-user-name> -p <iDRAC7-user-password> -c {<device-name> | <image-file>}` — Indicates whether the iDRAC7 CA certificate is valid. If the certificate is not valid, a warning message is displayed when you run this command. However, the command is executed successfully and a VMCLI session is established. For more information on VMCLI parameters, see the *VMCLI Help* or the *VMCLI Man pages*.

Related Links

[VMCLI Commands to Access Virtual Media](#)

[VMCLI Operating System Shell Options](#)

VMCLI Commands to Access Virtual Media

The following table provides the VMCLI commands required for accessing different virtual media.

Table 25. VMCLI Commands

| Virtual Media | Command |
|----------------------------------|---|
| Floppy drive | <code>vmcli -r [iDRAC IP or hostname] -u [iDRAC7 user name] -p [iDRAC7 user password] -f [device name]</code> |
| Bootable floppy or USB key image | <code>vmcli -r [iDRAC7 IP address] [iDRAC7 user name] -p [iDRAC7 password] -f [floppy.img]</code> |
| CD drive using -f option | <code>vmcli -r [iDRAC7 IP address] -u [iDRAC7 user name] -p [iDRAC7 password] -f [device name] [image file]-f [cdrom - dev]</code> |
| Bootable CD/DVD image | <code>vmcli -r [iDRAC7 IP address] -u [iDRAC7 user name] -p [iDRAC7 password] -c [DVD.img]</code> |

If the file is not write-protected, Virtual Media may write to the image file. To make sure that Virtual Media does not write to the media:

- Configure the operating system to write-protect a floppy image file that must not be overwritten.
- Use the write-protection feature of the device.

When virtualizing read-only image files, multiple sessions can use the same image media simultaneously.

When virtualizing physical drives, only one session can access a given physical drive at a time.

VMCLI Operating System Shell Options

VMCLI uses shell options to enable the following operating system features:

- **stderr/stdout redirection** — Redirects any printed utility output to a file.
For example, using the greater-than character (>) followed by a filename overwrites the specified file with the printed output of the VMCLI utility.



NOTE: The VMCLI utility does not read from standard input (stdin). Hence, stdin redirection is not required.

- **Background execution** — By default, the VMCLI utility runs in the foreground. Use the operating system's command shell features for the utility to run in the background.
For example, under a Linux operating system, the ampersand character (&) following the command causes the program to be spawned as a new background process. This technique is useful in script programs, as it allows the script to proceed after a new process is started for the VMCLI command (otherwise, the script blocks until the VMCLI program is terminated).


When multiple VMCLI sessions are started, use the operating system-specific facilities for listing and terminating processes.

Managing vFlash SD Card

The vFlash SD card is a Secure Digital (SD) card that plugs into the vFlash SD card slot in the system. You can use a card with a maximum of 16 GB capacity. After you insert the card, you must enable vFlash functionality to create and manage partitions. vFlash is a licensed feature.


If the card is not available in the system's vFlash SD card slot, the following error message is displayed in the iDRAC7 Web interface at **Overview** → **Server** → **vFlash**:

SD card not detected. Please insert an SD card of size 256MB or greater.

 **NOTE:** Make sure that you only insert a vFlash compatible SD card in the iDRAC7 vFlash card slot. If you insert a non-compatible SD card, the following error message is displayed when you initialize the card: *An error has occurred while initializing SD card.*


The key features are:

- Provides storage space and emulates USB device (s).
- Create up to 16 partitions. These partitions, when attached, are exposed to the system as a Floppy drive, Hard Disk drive, or a CD/DVD drive depending on the selected emulation mode.
- Create partitions from supported file system types. Supports **.img** format for floppy, **.iso** format for CD/DVD, and both **.iso** and **.img** formats for Hard Disk emulation types.
- Create bootable USB device(s).
- Boot once to an emulated USB device.

 **NOTE:** It is possible that a vFlash license may expire during a vFlash operation. If it happens, the on-going vFlash operations complete normally.

Configuring vFlash SD Card

Before configuring vFlash, make sure that the vFlash SD card is installed on the system. For information on how to install and remove the card from your system, see the system's *Hardware Owner's Manual* at support.dell.com/manuals.

 **NOTE:** You must have Configure iDRAC7 permission to enable or disable vFlash functionality, and initialize the card.

Related Links

[Viewing vFlash SD Card Properties](#)

[Enabling or Disabling vFlash Functionality](#)

[Initializing vFlash SD Card](#)

Viewing vFlash SD Card Properties

After vFlash functionality is enabled, you can view the SD card properties using iDRAC7 Web interface or RACADM.

Viewing vFlash SD Card Properties Using Web Interface

To view the vFlash SD card properties, in the iDRAC7 Web interface, go to **Overview** → **Server** → **vFlash**. The **SD Card Properties** page is displayed. For information about the displayed properties, see the *iDRAC7 Online Help*.

Viewing vFlash SD Card Properties Using RACADM

To view the vFlash SD card properties using RACADM:

1. Open a telnet, SSH, or Serial console to the system and log in.
2. Enter the command: `racadm getconfig -g cfgvFlashSD`

The following read-only properties are displayed:

- `cfgVFlashSDSize`
- `cfgVFlashSDLicensed`
- `cfgVFlashSDAvailableSize`
- `cfgVFlashSDHealth`
- `cfgVFlashSDEnable`
- `cfgVFlashSDWriteProtect`
- `cfgVFlashSDInitialized`

Viewing vFlash SD Card Properties Using iDRAC Settings Utility

To view the vFlash SD card properties, in the **iDRAC Settings Utility**, go to **vFlash Media**. The **iDRAC Settings vFlash Media** page displays the properties. For information about the displayed properties, see the *iDRAC Settings Utility Online Help*.


Enabling or Disabling vFlash Functionality

You must enable the vFlash functionality to perform partition management.

Enabling or Disabling vFlash Functionality Using Web Interface

To enable or disable the vFlash functionality:

1. In the iDRAC7 Web interface, go to **Overview** → **Server** → **vFlash** .
The **SD Card Properties** page is displayed.
2. Select or clear the **vFLASH Enabled** option to enable or disable the vFlash functionality. If any vFlash partition is attached, you cannot disable vFlash and an error message is displayed.


 **NOTE:** If vFlash functionality is disabled, SD card properties are not displayed.

3. Click **Apply**. The vFlash functionality is enabled or disabled based on the selection.

Enabling or Disabling vFlash Functionality Using RACADM

To enable or disable the vFlash functionality using RACADM:

1. Open a telnet, SSH, or Serial console to the system and log in.
2. Enter the following commands:
 - To enable vFlash, type:
`racadm config -g cfgvFlashsd -o cfgvflashSDEnable 1`
 - To disable vFlash, type:
`racadm config -g cfgvFlashsd -o cfgvflashSDEnable 0`

 **NOTE:** The RACADM command functions only if a vFlash SD card is present. If a card is not present, the following message is displayed: *ERROR: SD Card not present*.

Enabling or Disabling vFlash Functionality Using iDRAC Settings Utility

To enable or disable the vFlash functionality:

1. In the iDRAC Settings utility, go to **vFlash Media**.
The **iDRAC Settings vFlash Media** page is displayed.
2. Select **Enabled** to enable vFlash functionality or select **Disabled** to disable the vFlash functionality.
3. Click **Back**, click **Finish**, and then click **Yes**.
The vFlash functionality is enabled or disabled based on the selection.

Initializing vFlash SD Card

The initialize operation reformats the SD card and configures the initial vFlash system information on the card.

Initializing vFlash SD Card Using Web Interface

To initialize the vFlash SD card:

1. In the iDRAC7 Web interface, go to **Overview** → **Server** → **vFlash** .
The **SD Card Properties** page is displayed.
2. Enable **vFLASH** and click **Initialize**.
All existing contents are removed and the card is reformatted with the new vFlash system information.
If any vFlash partition is attached, the initialize operation fails and an error message is displayed.

Initializing vFlash SD Card Using RACADM

To initialize the vFlash SD card using RACADM:

1. Open a telnet, SSH, or Serial console to the system and log in.
2. Enter the command: `racadm vflashsd initialize`
All existing partitions are deleted and the card is reformatted.

Initializing vFlash SD Card Using iDRAC Settings Utility

To initialize the vFlash SD card using iDRAC Settings utility:


1. In the iDRAC Settings utility, go to **vFlash Media**.
The **iDRAC Settings vFlash Media** page is displayed.
2. Click **Initialize vFlash**.
3. Click **Yes**. The initialization operation starts.
4. Click **Back** and navigate to the same **iDRAC Settings vFlash Media** page to view the successful message.
All existing contents are removed and the card is reformatted with the new vFlash system information.

Getting the Last Status Using RACADM

To get the status of the last initialize command sent to the vFlash SD card:


1. Open a telnet, SSH, or Serial console to the system and log in.
2. Enter the command: `racadm vFlashsd status`
The status of commands sent to the SD card is displayed.

3. To get the last status of all the vflash partitions, use the command:`racadm vflashpartition status -a`
4. To get the last status of a particular partition, use command:`racadm vflashpartition status -i (index)`


 **NOTE:** If iDRAC7 is reset, the status of the last partition operation is lost.

Managing vFlash Partitions

You can perform the following using the iDRAC7 Web interface or RACADM:

 **NOTE:** An administrator can perform all operations on the vFlash partitions. Else, you must have **Access Virtual Media** privilege to create, delete, format, attach, detach, or copy the contents for the partition.

- [Creating an Empty Partition](#)
- [Creating a Partition Using an Image File](#)
- [Formatting a Partition](#)
- [Viewing Available Partitions](#)
- [Modifying a Partition](#)
- [Attaching or Detaching Partitions](#)
- [Deleting Existing Partitions](#)
- [Downloading Partition Contents](#)
- [Booting to a Partition](#)

 **NOTE:** If you click any option on the vFlash pages when an application such as WS-MAN, iDRAC Settings utility, or RACADM is using vFlash, or if you navigate to some other page in the GUI, iDRAC7 may display the message:
`vFlash is currently in use by another process. Try again after some time.`

vFlash is capable of performing fast partition creation when there is no other on-going vFlash operation such as formatting, attaching partitions, and so on. Therefore, it is recommended to first create all partitions before performing other individual partition operations.

Creating an Empty Partition

An empty partition, when attached to the system, is similar to an empty USB flash drive. You can create empty partitions on a vFlash SD card. You can create partitions of type *Floppy* or *Hard Disk*. The partition type CD is supported only while creating partitions using images.

Before creating an empty partition, make sure that:

- You have **Access Virtual Media** privilege.
- The card is initialized.
- The card is not write-protected.
- An initialize operation is not being performed on the card.

Creating an Empty Partition Using the Web Interface

To create an empty vFlash partition:

1. In iDRAC7 Web interface, go to **Overview** → **Server** → **vFlash** → **Create Empty Partition**.
The **Create Empty Partition** page is displayed.
2. Specify the required information and click **Apply**. For information about the options, see the *iDRAC7 Online Help*.
A new unformatted empty partition is created that is read-only by default. A page indicating the progress percentage is displayed. An error message is displayed if:

- The card is write-protected.
- The label name matches the label of an existing partition.
- A non-integer value is entered for the partition size, the value exceeds the available space on the card, or the partition size is greater than 4 GB.
- An initialize operation is being performed on the card.

Creating an Empty Partition Using RACADM

To create a 20 MB empty partition:


1. Open a telnet, SSH, or Serial console to the system and log in.
2. Enter the command: `racadm vflashpartition create -i 1 -o drive1 -t empty -e HDD -f fat16 -s 20`
A 20 MB empty partition in FAT16 format is created. By default, an empty partition is created as read-write.

Creating a Partition Using an Image File

You can create a new partition on the vFlash SD card using an image file (available in the **.img** or **.iso** format.) The partitions are of emulation types: Floppy (**.img**), Hard Disk (**.img** or **.iso**), or CD (**.iso**). The created partition size is equal to the image file size.

Before creating a partition from an image file, make sure that:

- You have Access Virtual Media privilege.
- The card is initialized.
- The card is not write-protected.
- An initialize operation is not being performed on the card.
- The image type and the emulation type match.

 **NOTE:** The uploaded image and the emulation type must match. There are issues when iDRAC7 emulates a device with incorrect image type. For example, if the partition is created using an ISO image and the emulation type is specified as Hard Disk, then the BIOS cannot boot from this image.

- Image file size is less than or equal to the available space on the card.
- Image file size is less than or equal to 4 GB as the maximum partition size supported is 4 GB. However, while creating a partition using a Web browser, the image file size must be less than 2 GB.

Creating a Partition Using an Image File Using Web Interface

To create a vFlash partition from an image file:


1. In iDRAC7 Web interface, go to **Overview** → **Server** → **vFlash** → **Create From Image**.
The **Create Partition from Image File** page is displayed.
2. Enter the required information and click **Apply**. For information about the options, see the *iDRAC7 Online Help*.
A new partition is created. For CD emulation type, a read-only partition is created. For Floppy or Hard Disk emulation type, a read-write partition is created. An error message is displayed if:
 - The card is write-protected
 - The label name matches the label of an existing partition.
 - The size of the image file is greater than 4GB or exceeds the available space on the card.
 - The image file does not exist or the image file extension is neither **.img** nor **.iso**.
 - An initialize operation is already being performed on the card.


Creating a Partition Using an Image File Using RACADM

To create a partition from an image file using RACADM:

1. Open a telnet, SSH, or Serial console to the system and log in.
2. Enter the command: `racadm vflashpartition create -i 1 -o drive1 -e HDD -t image -l //myserver/sharedfolder/foo.iso -u root -p mypassword`

A new partition is created. By default, the created partition is read-only. This command is case sensitive for the image file name extension. If the file name extension is in upper case, for example FOO.ISO instead of FOO.iso, then the command returns a syntax error.

 **NOTE:** This feature is not supported in local RACADM.

 **NOTE:** Creating vFlash partition from an image file located on the CFS or NFS IPv6 enabled network share is not supported.

Formatting a Partition

You can format an existing partition on the vFlash SD card based on the type of file system. The supported file system types are EXT2, EXT3, FAT16, and FAT32. You can only format partitions of type Hard Disk or Floppy, and not CD. You cannot format read-only partitions.

Before creating an partition from an image file, make sure that:

- You have **Access Virtual Media** privilege.
- The card is initialized.
- The card is not write-protected.
- An initialize operation is not being performed on the card.

To format vFlash partition:

1. In iDRAC7 Web interface, go to **Overview** → **Server** → **vFlash** → **Format**.
The **Format Partition** page is displayed.
2. Enter the required information and click **Apply**.
For information about the options, see the *iDRAC7 Online Help*.
A warning message indicating that all the data on the partition will be erased is displayed.
3. Click **OK**.
The selected partition is formatted to the specified file system type. An error message is displayed if:
 - The card is write-protected.
 - An initialize operation is already being performed on the card.

Viewing Available Partitions

Make sure that the vFlash functionality is enabled to view the list of available partitions.


Viewing Available Partitions Using Web Interface

To view the available vFlash partitions, in the iDRAC7 Web interface, go to **Overview** → **Server** → **vFlash** → **Manage**. The **Manage Partitions** page is displayed listing the available partitions and related information for each partition. For information on the partitions, see the *iDRAC7 Online Help*.

Viewing Available Partitions Using RACADM

To view the available partitions and their properties using RACADM:


1. Open a Telnet, SSH, or Serial console to the system and log in.
2. Enter the following commands:
 - To list all existing partitions and its properties:
`racadm vflashpartition list`
 - To get the status of operation on partition 1:
`racadm vflashpartition status -i 1`
 - To get the status of all existing partitions:
`racadm vflashpartition status -a`

 **NOTE:** The -a option is valid only with the status action.

Modifying a Partition

You can change a read-only partition to read-write or vice-versa. Before modifying the partition, make sure that:


- The vFlash functionality is enabled.
- You have **Access Virtual Media** privileges.

 **NOTE:** By default, a read-only partition is created.

Modifying a Partition Using Web Interface

To modify a partition:

1. In the iDRAC7 Web interface, go to **Overview** → **Server** → **vFlash** → **Manage**.
The **Manage Partitions** page is displayed.
2. In the **Read-Only** column:
 - Select the checkbox for the partition(s) and click **Apply** to change to read-only.
 - Clear the checkbox for the partition(s) and click **Apply** to change to read-write.
The partitions are changed to read-only or read-write, based on the selections.

 **NOTE:** If the partition is of type CD, the state is read-only. You cannot change the state to read-write. If the partition is attached, the check box is grayed-out.

Modifying a Partition Using RACADM

To view the available partitions and their properties on the card:

1. Open a telnet, SSH, or Serial console to the system and log in.
2. Enter the following commands:
 - 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`

Attaching or Detaching Partitions

When you attach one or more partitions, they are visible to the operating system and BIOS as USB mass storage devices. When you attach multiple partitions, based on the assigned index, they are listed in an ascending order in the operating system and the BIOS boot order menu.

If you detach a partition, it is not visible in the operating system and the BIOS boot order menu.

When you attach or detach a partition, the USB bus in the managed system is reset. This affects applications that are using vFlash and disconnects the iDRAC7 Virtual Media sessions.

Before attaching or detaching a partition, make sure that:

- The vFlash functionality is enabled.
- An initialize operation is not already being performed on the card.
- You have **Access Virtual Media** privileges.

Attaching or Detaching Partitions Using Web Interface

To attach or detach partitions:

1. In the iDRAC7 Web interface, go to **Overview** → **Server** → **vFlash** → **Manage**.
The **Manage Partitions** page is displayed.
2. In the **Attached** column:
 - Select the checkbox for the partition(s) and click **Apply** to attach the partition(s).
 - Clear the checkbox for the partition(s) and click **Apply** to detach the partition(s).The partitions are attached or detached, based on the selections.

Attaching or Detaching Partitions Using RACADM

To attach or detach partitions:

1. Open a telnet, SSH, or Serial console to the system and log in.
2. Enter the following commands:
 - 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
```

Operating System Behavior for Attached Partitions

For Windows and Linux operating systems:

- The operating system controls and assigns the drive letters to the attached partitions.
- Read-only partitions are read-only drives in the operating system.
- The operating system must support the file system of an attached partition. Else, you cannot read or modify the contents of the partition from the operating system. For example, in a Windows environment the operating system cannot read the partition type EXT2 which is native to Linux. Also, in a Linux environment the operating system cannot read the partition type NTFS which is native to Windows.
- The vFlash partition label is different from the volume name of the file system on the emulated USB device. You can change the volume name of the emulated USB device from the operating system. However, it does not change the partition label name stored in iDRAC7.

Deleting Existing Partitions

Before deleting existing partition(s), make sure that:

- The vFlash functionality is enabled.
- The card is not write-protected.
- The partition is not attached.
- An initialize operation is not being performed on the card.

Deleting Existing Partitions Using Web Interface

To delete an existing partition:

1. In the iDRAC7 Web interface, go to **Overview** → **Server** → **vFlash** → **Manage**.
The **Manage Partitions** page is displayed.
2. In the **Delete** column, click the delete icon for the partition that you want to delete.
A message is displayed indicating that this action permanently deletes the partition.
3. Click **OK**.
The partition is deleted.

Deleting Existing Partitions Using RACADM

To delete partitions:

1. Open a telnet, SSH, or Serial console to the system and log in.
2. Enter the following commands:
 - To delete a partition:
`racadm vflashpartition delete -i 1`
 - To delete all partitions, re-initialize the vFlash SD card.

Downloading Partition Contents

You can download the contents of a vFlash partition in the **.img** or **.iso** format to the:


- Managed system (where iDRAC7 is operated from)
- Network location mapped to a management station.

Before downloading the partition contents, make sure that:

- You have Access Virtual Media privileges.
- The vFlash functionality is enabled.
- An initialize operation is not being performed on the card.
- For a read-write partition, it must not be attached.


To download the contents of the vFlash partition:

1. In the iDRAC7 Web interface, go to **Overview** → **Server** → **vFlash** → **Download**.
The **Download Partition** page is displayed.
2. From the **Label** drop-down menu, select a partition that you want to download and click **Download**.

 **NOTE:** All existing partitions (except attached partitions) are displayed in the list. The first partition is selected by default.

3. Specify the location to save the file.

The contents of the selected partition are downloaded to the specified location.

 **NOTE:** If only the folder location is specified, then the partition label is used as the file name, along with the extension **.iso** for CD and Hard Disk type partitions, and **.img** for Floppy and Hard Disk type partitions.

Booting to a Partition


You can set an attached vFlash partition as the boot device for the next boot operation.

Before booting a partition, make sure that:

- The vFlash partition contains a bootable image (in the **.img** or **.iso** format) to boot from the device.
- The vFlash functionality is enabled.
- You have Access Virtual Media privileges.


Booting to a Partition Using Web Interface

To set the vFlash partition as a first boot device, see [Setting First Boot Device](#).

 **NOTE:** If the attached vFlash partition(s) are not listed in the **First Boot Device** drop-down menu, make sure that the BIOS is updated to the latest version.


Booting to a Partition Using RACADM

To set a vFlash partition as the first boot device, use `cfgServerInfo`. For more information, see the *RACADM Command Line Reference Guide for iDRAC7 and CMC* available at support.dell.com/manuals.

 **NOTE:** When you run this command, the vFlash partition label is automatically set to boot once—`cfgserverBootOnce` is set to 1. Boot once boots the device to the partition only once and does not keep it persistently first in the boot order.


Using SMCLP

The Server Management Command Line Protocol (SMCLP) specification enables CLI-based systems management. It defines a protocol for management commands transmitted over standard character oriented streams. This protocol accesses a Common Information Model Object Manager (CIMOM) using a human-oriented command set. The SMCLP is a sub-component of the Distributed Management Task Force (DMTF) SMASH initiative to streamline systems management across multiple platforms. The SMCLP specification, along with the Managed Element Addressing Specification and numerous profiles to SMCLP mapping specifications, describes the standard verbs and targets for various management task executions.

 **NOTE:** It is assumed that you are familiar with the Systems Management Architecture for Server Hardware (SMASH) Initiative and the SMWG SMCLP specifications.

The SM-CLP is a subcomponent of the Distributed Management Task Force (DMTF) SMASH initiative to streamline server management across multiple platforms. The SM-CLP specification, along with the Managed Element Addressing Specification and numerous profiles to SM-CLP mapping specifications, describes the standard verbs and targets for various management task executions.

The SMCLP is hosted from the iDRAC7 controller firmware and supports Telnet, SSH, and serial-based interfaces. The iDRAC7 SMCLP interface is based on the SMCLP Specification Version 1.0 provided by the DMTF organization.

 **NOTE:** Information about the profiles, extensions, and MOFs are available at delltechcenter.com and all DMTF information is available at dmtof.org/standards/profiles/.

SM-CLP commands implement a subset of the local RACADM commands. The commands are useful for scripting since you can execute these commands from a management station command line. You can retrieve the output of commands in well-defined formats, including XML, facilitating scripting and integration with existing reporting and management tools.

System Management Capabilities Using SMCLP

iDRAC7 SMCLP enables you to:

- Manage Server Power — Turn on, shut down, or reboot the system
- Manage System Event Log (SEL) — Display or clear the SEL records
- Manage iDRAC7 user account
- View system properties


Running SMCLP Commands

You can run the SMCLP commands using SSH or Telnet interface. Open a SSH or Telnet interface and log in to iDRAC7 as an administrator. The SMCLP prompt (admin ->) is displayed.

SMCLP prompts:

- yx1x blade servers use `-$.`
- yx1x rack and tower servers use `admin->.`
- yx2x blade, rack, and tower servers use `admin->.`

where, y is a alpha-numeric character such as M (for blade servers), R (for rack servers), and T (for tower servers) and x is a number. This indicates the generation of Dell PowerEdge servers.

 **NOTE:** Scripts using `-$` can use these for yx1x systems, but starting with yx2x systems one script with `admin->` can be used for blade, rack, and tower servers.

iDRAC7 SMCLP Syntax

The iDRAC7 SMCLP uses the concept of verbs and targets to provide systems management capabilities through the CLI. The verb indicates the operation to perform, and the target determines the entity (or object) that runs the operation.

The SMCLP command line syntax:

```
<verb> [<options>] [<target>] [<properties>]
```

The following table provides the verbs and its definitions.

Table 26. SMCLP Verbs

| Verb | Definition |
|---------|---|
| cd | Navigates through the MAP using the shell |
| set | Sets a property to a specific value |
| help | Displays help for a specific target |
| reset | Resets the target |
| show | Displays the target properties, verbs, and subtargets |
| start | Turns on a target |
| stop | Shuts down a target |
| exit | Exits from the SMCLP shell session |
| version | Displays the version attributes of a target |
| load | Moves a binary image to a specified target address from a URL |

The following table provides a list of targets.

Table 27. SMCLP Targets

| Target | Definitions |
|--|---|
| admin1 | admin domain |
| admin1/profiles1 | Registered profiles in iDRAC7 |
| admin1/hdwr1 | Hardware |
| admin1/system1 | Managed system target |
| admin1/system1/capabilities1 | Managed system SMASH collection capabilities |
| admin1/system1/capabilities1/pwracap1 | Managed system power utilization capabilities |
| admin1/system1/capabilities1/electcap1 | Managed system target capabilities |
| admin1/system1/logs1 | Record Log collections target |
| admin1/system1/logs1/log1 | System Event Log (SEL) record entry |

| Target | Definitions |
|--|---|
| admin1/system1/logs1/log1/record* | An individual SEL record instance on the managed system |
| admin1/system1/settings1 | Managed system SMASH collection settings |
| admin1/system1/capacities1 | Managed system capacities SMASH collection |
| admin1/system1/consoles1 | Managed system consoles SMASH collection |
| admin1/system1/sp1 | Service Processor |
| admin1/system1/sp1/timesvc1 | Service Processor time service |
| admin1/system1/sp1/capabilities1 | Service processor capabilities SMASH collection |
| admin1/system1/sp1/capabilities1/ clpcap1 | CLP service capabilities |
| admin1/system1/sp1/capabilities1/ pwrmgtcap1 | Power state management service capabilities on the system |
| admin1/system1/sp1/capabilities1/ acctmgtcap* | Account management service capabilities |
| admin1/system1/sp1/capabilities1/ rolemgtcap* | Local Role Based Management capabilities |
| admin1/system1/sp1/capabilities/ PwrutilmgtCap1 | Power utilization management capabilities |
| admin1/system1/sp1/capabilities1/ elecapi | Authentication capabilities |
| admin1/system1/sp1/settings1 | Service Processor settings collection |
| admin1/system1/sp1/settings1/ clpsetting1 | CLP service settings data |
| admin1/system1/sp1/clpsvc1 | CLP service protocol service |
| admin1/system1/sp1/clpsvc1/clpendpt* | CLP service protocol endpoint |
| admin1/system1/sp1/clpsvc1/tcpendpt* | CLP service protocol TCP endpoint |
| admin1/system1/sp1/jobq1 | CLP service protocol job queue |
| admin1/system1/sp1/jobq1/job* | CLP service protocol job |
| admin1/system1/sp1/pwrmgtsvc1 | Power state management service |
| admin1/system1/sp1/account1-16 | Local user account |
| admin1/sysetm1/sp1/account1-16/ identity1 | Local user identity account |
| admin1/sysetm1/sp1/account1-16/ identity2 | IPMI identity (LAN) account |

| Target | Definitions |
|---|---|
| admin1/sysetm1/sp1/account1-16/identity3 | IPMI identity (Serial) account |
| admin1/sysetm1/sp1/account1-16/identity4 | CLP identity account |
| admin1/system1/sp1/acctsvc1 | Local user account management service |
| admin1/system1/sp1/acctsvc2 | IPMI account management service |
| admin1/system1/sp1/acctsvc3 | CLP account management service |
| admin1/system1/sp1/rolesvc1 | Local Role Base Authorization (RBA) service |
| admin1/system1/sp1/rolesvc1/Role1-16 | Local role |
| admin1/system1/sp1/rolesvc1/Role1-16/privilege1 | Local role privilege |
| admin1/system1/sp1/rolesvc2 | IPMI RBA service |
| admin1/system1/sp1/rolesvc2/Role1-3 | IPMI role |
| admin1/system1/sp1/rolesvc2/Role4 | IPMI Serial Over LAN (SOL) role |
| admin1/system1/sp1/rolesvc3 | CLP RBA Service |
| admin1/system1/sp1/rolesvc3/Role1-3 | CLP role |
| admin1/system1/sp1/rolesvc3/Role1-3/privilege1 | CLP role privilege |

Related Links


[Running SMCLP Commands](#)

[Usage Examples](#)

Navigating the MAP Address Space

Objects that can be managed with SM-CLP are represented by targets arranged in a hierarchical space called the Manageability Access Point (MAP) address space. An address path specifies the path from the root of the address space to an object in the address space.

The root target is represented by a slash (/) or a backslash (\). It is the default starting point when you log in to iDRAC7. Navigate down from the root using the `cd` verb.

 **NOTE:** The slash (/) and backslash (\) are interchangeable in SM-CLP address paths. However, a backslash at the end of a command line continues the command on the next line and is ignored when the command is parsed.

For example to navigate to the third record in the System Event Log (SEL), enter the following command:

```
->cd /admin1/system1/logs1/log1/record3
```

Enter the `cd` verb with no target to find your current location in the address space. The `..` and `.` abbreviations work as they do in Windows and Linux: `..` refers to the parent level and `.` refers to the current level.

Using Show Verb

To learn more about a target use the `show` verb. This verb displays the target's properties, sub-targets, associations, and a list of the SM-CLP verbs that are allowed at that location.

Using the `-display` Option

The `show -display` option allows you to limit the output of the command to one or more of properties, targets, associations, and verbs. For example, to display just the properties and targets at the current location, use the following command:

```
show -display properties,targets
```

To list only certain properties, qualify them, as in the following command:

```
show -d properties=(userid,name) /admin1/system1/sp1/account1
```

If you only want to show one property, you can omit the parentheses.

Using the `-level` Option

The `show -level` option executes `show` over additional levels beneath the specified target. To see all targets and properties in the address space, use the `-l all` option.

Using the `-output` Option

The `-output` option specifies one of four formats for the output of SM-CLP verbs: **text**, **clpcsv**, **keyword**, and **clpxml**.

The default format is **text**, and is the most readable output. The **clpcsv** format is a comma-separated values format suitable for loading into a spreadsheet program. The **keyword** format outputs information as a list of keyword=value pairs one per line. The **clpxml** format is an XML document containing a **response** XML element. The DMTF has specified the **clpcsv** and **clpxml** formats and their specifications can be found on the DMTF website at dmtf.org.

The following example shows how to output the contents of the SEL in XML:

```
show -l all -output format=clpxml /admin1/system1/logs1/log1
```

Usage Examples

This section provides use case scenarios for SMCLP:

- [Server Power Management](#)
- [SEL Management](#)
- [MAP Target Navigation](#)

Server Power Management

The following examples show how to use SMCLP to perform power management operations on a managed system.

Type the following commands at the SMCLP command prompt:

- To switch off the server:

```
stop /system1
```

The following message is displayed:

```
system1 has been stopped successfully
```

- **To switch on the server:**

```
start /system1
```

The following message is displayed:

```
system1 has been started successfully
```

- **To reboot the server:**

```
reset /system1
```

The following message is displayed:

```
system1 has been reset successfully
```

SEL Management

The following examples show how to use the SMCLP to perform SEL-related operations on the managed system. Type the following commands at the SMCLP command prompt:

- **To view the SEL:**

```
show/system1/logs1/log1
```

The following output is displayed :

```
/system1/logs1/log1
```

Targets:

Record1

Record2

Record3

Record4

Record5

Properties:

InstanceID = IPMI:BMC1 SEL Log

MaxNumberOfRecords = 512

CurrentNumberOfRecords = 5

Name = IPMI SEL

EnabledState = 2

OperationalState = 2

HealthState = 2

Caption = IPMI SEL

Description = IPMI SEL

ElementName = IPMI SEL

Commands:

cd

show

help

exit

version

- **To view the SEL record:**

```
show/system1/logs1/log1
```

The following output is displayed :

```
/system1/logs1/log1/record4
Properties:
LogCreationClassName= CIM_RecordLog
CreationClassName= CIM_LogRecord
LogName= IPMI SEL
RecordID= 1
MessageTimeStamp= 20050620100512.000000-000
Description= FAN 7 RPM: fan sensor, detected a failure
ElementName= IPMI SEL Record

Commands:
cd
show
help
exit
version
```

- To clear the SEL:
delete /system1/logs1/log1/record*
The following output is displayed:
All records deleted successfully

MAP Target Navigation

The following examples show how to use the cd verb to navigate the MAP. In all examples, the initial default target is assumed to be /.

Type the following commands at the SMCLP command prompt:

- To navigate to the system target and reboot:
cd system1 reset The current default target is /.
- To navigate to the SEL target and display the log records:
cd system1
cd logs1/log1
show
- To display current target:
type cd .
- To move up one level:
type cd ..
- To exit:
exit

Deploying Operating Systems

You can use any of the following utilities to deploy operating systems to managed systems:

- Virtual Media Command Line Interface (CLI)
- Virtual Media Console
- Remote File Share

Related Links

[Deploying Operating System Using VMCLI](#)


[Deploying Operating System Using Remote File Share](#)

[Deploying Operating System Using Virtual Media](#)


Deploying Operating System Using VMCLI

Before you deploy the operating system using the `vmdeploy` script, make sure that:

- VMCLI utility is installed on the management station.
- **Configure User** and **Access Virtual Media** privileges for iDRAC7 are enabled for the user.
- IPMItool is installed on the management station.

 **NOTE:** IPMItool does not work if IPv6 is configured either on the managed system or the management station.

- iDRAC7 is configured on the target remote systems.
- System is able to boot from the image file.
- IPMI Over LAN is enabled in iDRAC7.
- Network share contains drivers and operating system bootable image file, in an industry standard format such as `.img` or `.iso`.

 **NOTE:** While creating the image file, follow standard network-based installation procedures, and mark the deployment image as read-only to make sure that each target system boots and executes the same deployment procedure.


- Virtual Media status is in attach state.
- **vmdeploy** script is installed on the management station. Review this sample `vmdeploy` script included with VMCLI. The script describes how to deploy the operating system to remote systems in the network. It internally uses VMCLI and IPMItool.


 **NOTE:** The **vmdeploy** script is dependent on some support files in the directory during installation. To use the script from another directory, copy all the files with it. If the IPMItool utility is not installed, copy the utility along with the other files.

To deploy the operating system on target remote systems:

1. List the iDRAC7 IPv4 addresses of the target remote systems, in the `ip.txt` text file. List one IPv4 address per line.
2. Insert a bootable operating system, CD or DVD, into the management station drive.
3. Open a command prompt with administrator privileges and run the **vmdeploy** script:

```
vmdeploy.bat -r <iDRAC7-IPAddress or file> -u <iDRAC7-user> -p <iDRAC7-user-  
passwd> [ -f {<floppy-image> | < device-name>} | -c { <device-name>|<image-  
file>} ] [-i <DeviceID>]
```

 **NOTE:** vmdeploy does not support IPv6, since IPv6 does not support the IPMI tool.

 **NOTE:** The vmdeploy script processes the `-r` option slightly differently than the `vmcli -r` option. If the argument to the `-r` option is the name of an existing file, the script reads iDRAC7 IPv4 or IPv6 addresses from the specified file and runs the utility once for each line. If the argument to the `-r` option is not a filename, then it should be a single iDRAC7 address. In this case, the `-r` works as described for the VMCLI utility.

The following table describes the vmdeploy command parameters.

Table 28. vmdeploy Command Parameters

| Parameter | Description |
|--|---|
| <code><iDRAC7-user></code> | iDRAC7 user name. It must have the following attributes: <ul style="list-style-type: none"> Valid user name iDRAC7 Virtual Media User permission If iDRAC7 authentication fails, an error message is displayed and the command is terminated. |
| <code><iDRAC7-ip file></code> | iDRAC7 IP address or the file containing the iDRAC7 IP address. |
| <code><iDRAC7-user-password> or <iDRAC7-passwd></code> | Password for the iDRAC7 user. If iDRAC7 authentication fails, an error message is displayed and the command is terminated. |
| <code>-c {<device-name> <image-file>}</code> | Path to an ISO9660 image of the operating system installation CD or DVD. |
| <code><floppy-device></code> | Path to the device containing the operating system installation CD, DVD, or Floppy. |
| <code><floppy-image></code> | Path to a valid floppy image. |
| <code><Device ID></code> | ID of the device to boot once. |

Related Links


[Configuring Virtual Media](#)

[Configuring iDRAC7](#)

Deploying Operating System Using Remote File Share

Before you deploy the operating system using Remote File Share, make sure that:

- Virtual Media is in **Attached** state for the virtual drives to appear in the boot sequence.
- Configure User** and **Access Virtual Media** privileges for iDRAC7 are enabled for the user.
- Remote File Share is enabled.
- Network share contains drivers and operating system bootable image file, in an industry standard format such as `.img` or `.iso`.

 **NOTE:** While creating the image file, follow standard network-based installation procedures, and mark the deployment image as read-only to make sure that each target system boots and executes the same deployment procedure.

To deploy an operating system using Remote File Share:

1. Mount the ISO or IMG image file to the managed system using NFS or CIFS.
2. Go to **Overview** → **Setup** → **First Boot Device**.
3. Set the boot order in the **First Boot Device** drop-down list to **Remote File Share**.
4. Select the **Boot Once** option to enable the managed system to reboot using the image file for the next instance only.
5. Click **Apply**.
6. Reboot the managed system and follow the on-screen instructions to complete the deployment.

Related Links

- [Configuring Virtual Media](#)
- [Setting First Boot Device](#)
- [Managing Remote File Share](#)


Managing Remote File Share

Using Remote File Share (RFS) feature, you can set an ISO or IMG 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. This is a licensed feature.

 **NOTE:** IPv4 address is supported for both CIFS and NFS. IPv6 address is supported only for CIFS.

Remote file share supports only **.img** and **.iso** image file formats. A **.img** file is redirected as a virtual floppy and a **.iso** file is redirected as a virtual CDROM.

You must have Virtual Media privileges to perform an RFS mounting.

 **NOTE:** If ESXi is running on the managed system and if you mount a floppy image (**.img**) using Remote File Share, the connected floppy image is not available to the ESXi operating system.


The connection status for RFS is available in iDRAC7 log. Once connected, an RFS mounted virtual drive does not disconnect even if you log out from iDRAC7. The RFS connection is closed if iDRAC7 is reset or the network connection is dropped. The Web interface and command line options are also available in CMC and iDRAC7 to close the RFS connection. The RFS connection from CMC always overrides an existing RFS mount in iDRAC7.

 **NOTE:** iDRAC7 vFlash feature and RFS are not related.

Configuring Remote File Share Using Web Interface

To enable remote file sharing:

1. In iDRAC7 Web interface, go to **Overview** → **Server** → **Attached Media**.
The **Attached Media** page is displayed.
2. Under **Remote File Share**, select attach or auto-attach and specify the user name, password, and the image file path. For more information, see the *iDRAC7 Online Help*.
3. Click **Apply** and then click **Connect**.
The connection is established and the **Connection Status** displays connected.

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

For Linux distributions, this feature may require a manual mount command when operating at runlevel init 3. The syntax for the command is:

```
mount /dev/OS_specific_device / user_defined_mount_point
```

where, `user_defined_mount_point` is any directory you choose to use for the mount similar to any mount command.

For RHEL, the CD device (**.iso** virtual device) is `/dev/scd0` and floppy device (**.img** virtual device) is `/dev/sdc`.

For SLES, the CD device is `/dev/sr0` and the floppy device is `/dev/sdc`. To make sure that the correct device is used (for either SLES or RHEL), when you connect the virtual device, on the Linux OS you must immediately run the command:

```
tail /var/log/messages | grep SCSI
```

This displays the text that identifies the device (example, SCSI device `sdc`). This procedure also applies to Virtual Media when you are using Linux distributions in runlevel `init 3`. By default, the virtual media is not auto-mounted in `init 3`.

Configuring Remote File Share Using RACADM

To configure remote file share using RACADM, use:

```
racadm remoteimage  
racadm remoteimage <options>
```

Options are:

- c: connect image
- d: disconnect image
- u <username>: username to access the network share
- p <password>: password to access the network share
- l <image_location>: image location on the network share; use double quotes around the location
- s: display current status



NOTE: All characters including alphanumeric and special characters are allowed as part of user name, password, and `image_location` except the following characters: ' (single quote), "(double quote), ,(comma), < (less than), and > (greater than).

Deploying Operating System Using Virtual Media

Before you deploy the operating system using Virtual Media, make sure that:

- Virtual Media is in *Attached* state for the virtual drives to appear in the boot sequence.
- If Virtual Media is in *Auto Attached* mode, the Virtual Media application must be launched before booting the system.
- Network share contains drivers and operating system bootable image file, in an industry standard format such as **.img** or **.iso**.

To deploy an operating system using Virtual Media:

1. Do one of the following:
 - Insert the operating system installation CD or DVD into the management station CD or DVD drive.
 - Attach the operating system image.
2. Select the drive on the management station with the required image to map it.
3. Use one of the following methods to boot to the required device:
 - Set the boot order to boot once from **Virtual Floppy** or **Virtual CD/DVD/ISO** using the iDRAC7 Web interface.
 - Set the boot order through **System Setup** → **System BIOS Settings** by pressing <F2> during boot.

4. Reboot the managed system and follow the on-screen instructions to complete the deployment.

Related Links

[Configuring Virtual Media](#)

[Setting First Boot Device](#)

[Configuring iDRAC7](#)

Installing Operating System From Multiple Disks

1. Unmap the existing CD/DVD.
2. Insert the next CD/DVD into the remote optical drive.
3. Remap the CD/DVD drive.

Deploying Embedded Operating System On SD Card

To install an embedded hypervisor on an SD card:

1. Insert the two SD cards in the Internal Dual SD Module (IDSMD) slots on the system.
2. Enable SD module and redundancy (if required) in BIOS.
3. Verify if the SD card is available on one of the drives when you <F11> during boot.
4. Deploy the embedded operating system and follow the operating system installation instructions.

Related Links

[About IDSMD](#)

[Enabling SD Module and Redundancy in BIOS](#)

Enabling SD Module and Redundancy in BIOS

To enable SD module and redundancy in BIOS:

1. Press <F2> during boot.
2. Go to **System Setup** → **System BIOS Settings** → **Integrated Devices**.
3. Set the **Internal USB Port** to **On**. If it is set to **Off**, the IDSMD is not available as a boot device.
4. If redundancy is not required (single SD card), set **Internal SD Card Port** to **On** and **Internal SD Card Redundancy** to **Disabled**.
5. If redundancy is required (two SD cards), set **Internal SD Card Port** to **On** and **Internal SD Card Redundancy** to **Mirror**.
6. Click **Back** and click **Finish**.
7. Click **Yes** to save the settings and press <Esc> to exit **System Setup**.

About IDSMD

Internal Dual SD Module (IDSMD) is available only on applicable platforms. IDSMD provides redundancy on the hypervisor SD card by using another SD card that mirrors the first SD card's content.

Either of the two SD cards can be the master. For example, if two new SD cards are installed in the IDSMD, SD1 is active (master) card and SD2 is the standby card. The data is written on both the cards, but the data is read from SD1. At any time if SD1 fails or is removed, SD2 automatically become the active (master) card.

You can view the status, health, and the availability of IDSDM using iDRAC7 Web Interface or RACADM. The SD card redundancy status and failure events are logged to SEL, displayed on the front panel, and PET alerts are generated if alerts are enabled.

Related Links

[Viewing Sensor Information](#)

Troubleshooting Managed System Using iDRAC7

You can diagnose and troubleshoot a remote managed system using:

- Diagnostic console
- Post code
- Boot and crash capture videos
- Last system crash screen
- System event logs
- Lifecycle logs
- Front panel status
- Trouble indicators
- System health

Related Links

[Using Diagnostic Console](#)

[Viewing Post Codes](#)

[Viewing Boot and Crash Capture Videos](#)

[Viewing Logs](#)

[Viewing Last System Crash Screen](#)

[Viewing Front Panel Status](#)

[Hardware Trouble Indicators](#)

[Viewing System Health](#)

Using Diagnostic Console

iDRAC7 provides a standard set of network diagnostic tools that are similar to the tools included with Microsoft Windows or Linux-based systems. Using iDRAC7 Web interface, you can access the network debugging tools.

To access Diagnostics Console:

1. In the iDRAC7 Web interface, go to **Overview** → **Server** → **Troubleshooting** → **Diagnostics**.
2. In the **Command** text box, enter a command and click **Submit**. For information about the commands, see the *iDRAC7 Online Help*.

The results are displayed on the same page.

Viewing Post Codes

Post codes are progress indicators from the system BIOS, indicating various stages of the boot sequence from power-on-reset, and allows you to diagnose any faults related to system boot-up. The **Post Codes** page displays the last system post code prior to booting the operating system.

To view the Post Codes, go to **Overview** → **Server** → **Troubleshooting** → **Post Code**.

The **Post Code** page displays the system health indicator, a hexadecimal code, and a description of the code.


Viewing Boot and Crash Capture Videos

You can view the video recordings of:

- Last three boot cycles — A boot cycle video logs the sequence of events for a boot cycle. The boot cycle videos are arranged in the order of latest to oldest.
- Last crash video — A crash video logs the sequence of events leading to the failure.

This is a licensed feature.

iDRAC7 records fifty frames during boot time. Playback of the boot screens occur at a rate of 1 frame per second. If iDRAC7 is reset, the boot capture video is not available as it is stored in RAM and is deleted.

 **NOTE:** You must have Access Virtual Console or administrator privileges to playback the Boot Capture and Crash Capture videos.

To view the **Boot Capture** screen, click **Overview** → **Server** → **Troubleshooting** → **Video Capture**.

The **Video Capture** screen displays the video recordings. For more information, see the *iDRAC7 Online Help*.

Viewing Logs

You can view System Event Logs (SELs) and Lifecycle logs. For more information, see [Viewing System Event Log](#) and [Viewing Lifecycle Log](#).

Viewing Last System Crash Screen

The last crash screen feature captures a screenshot of the most recent system crash, saves, and displays it in iDRAC7. This is a licensed feature.

To view the last crash screen:

1. Make sure that the last system crash screen feature is enabled.
2. In iDRAC7 Web interface, go to **Overview** → **Server** → **Troubleshooting** → **Last Crash Screen**.
The **Last Crash Screen** page displays the last saved crash screen from the managed system.
Click **Clear** to delete the last crash screen.

Related Links

[Enabling Last Crash Screen](#)

Viewing Front Panel Status

The Front Panel on the managed system summarizes the status of the following components in the system:

- Batteries
- Fans
- Intrusion
- Power Supplies
- Removable Flash Media
- Temperatures
- Voltages

You can view the status of the front panel of the managed system:

- For rack and tower servers: LCD front panel and system ID LED status or LED front panel and system ID LED status.
- For blade servers: Only system ID LEDs.

Viewing System Front Panel LCD Status

To view the LCD front panel status for applicable rack and tower servers, in iDRAC7 Web interface, go to **Overview** → **Hardware** → **Front Panel**. The **Front Panel** page displays.

The **Live Front Panel Feed** section displays the live feed of the messages currently being displayed on the LCD front panel. When the system is operating normally (indicated by Solid Blue color in the LCD front panel), then both **Hide Error** and **UnHide Error** is grayed-out. You can hide or unhide the errors only for rack and tower servers.

To view LCD front panel status using RACADM, use the objects in the `System.LCD` group. For more information, see the *RACADM Command Line Reference Guide for iDRAC7 and CMC* available at support.dell.com/manuals.

Related Links

[Configuring LCD Setting](#)

Viewing System Front Panel LED Status

To view the current system ID LED status, in iDRAC7 Web interface, go to **Overview** → **Hardware** → **Front Panel**. The **Live Front Panel Feed** section displays the current front panel status:

- Solid blue — No errors present on the managed system.
- Blinking blue — Identify mode is enabled (regardless of managed system error presence).
- Solid amber — Managed system is in failsafe mode.
- Blinking amber — Errors present on managed system.

When the system is operating normally (indicated by blue Health icon on the LED front panel), then both **Hide Error** and **UnHide Error** is grayed-out. You can hide or unhide the errors only for rack and tower servers.

To view system ID LED status using RACADM, use the `getled` command. For more information, see the *RACADM Command Line Reference Guide for iDRAC7 and CMC* available at support.dell.com/manuals.

Related Links

[Configuring System ID LED Setting](#)

Hardware Trouble Indicators

The hardware related problems are:


- Failure to power up
- Noisy fans
- Loss of network connectivity
- Hard drive failure
- USB media failure
- Physical damage

Based on the problem, use the following methods to correct the problem:

- Reseat the module or component and restart the system
- In case of a blade server, insert the module into a different bay in the chassis
- Replace hard drives or USB flash drives

- Reconnect or replace the power and network cables

If problem persists, see the *Hardware Owner's Manual* for specific troubleshooting information about the hardware device.

 **CAUTION: You should only perform troubleshooting and simple repairs as authorized in your product documentation, or as directed by online or telephone service and support team. Damage due to servicing that is not authorized by Dell is not covered by your warranty. Read and follow the safety instructions that came with the product.**

Viewing System Health





iDRAC7 and CMC (for blade servers) Web interfaces display the status for the following:

- Batteries
- Fans
- Intrusion
- Power Supplies
- Removable Flash Media
- Temperatures
- Voltages
- CPU

In iDRAC7 Web interface, go to **Overview** → **Server** → **System Summary** → **Server Health** section.

To view CPU health, go to **Overview** → **Hardware** → **CPU**.

The system health indicators are:

-  — Indicates a normal status.
-  — Indicates a warning status.
-  — Indicates a failure status.
-  — Indicates an unknown status.

Click any component name in the **Server Health** section to view details about the component.

Checking Server Status Screen for Error Messages

When a flashing amber LED is blinking, and a particular server has an error, the main Server Status Screen on the LCD highlights the affected server in orange. Use the LCD navigation buttons to highlight the affected server, then click the center button. Error and warning messages will be displayed on the second line. For the list of error messages displayed on the LCD panel, see the server's Owner's Manual.

Restarting iDRAC7

You can perform a hard or soft iDRAC7 restart without turning off the server:

- Hard restart — On the server, press and hold the LED button for 15 seconds.
- Soft restart — Using iDRAC7 Web interface or RACADM.

Resetting iDRAC7 Using iDRAC7 Web Interface

To restart iDRAC7, do one of the following in the iDRAC7 Web interface:

- Go to **Overview** → **Server** → **Summary**. Under **Quick Launch Tasks**, click **Reset iDRAC**.
- Go to **Overview** → **Server** → **Troubleshooting** → **Diagnostics**. Click **Reset iDRAC**.

Resetting iDRAC7 Using RACADM

To restart iDRAC7, use the **racreset** command. For more information, see the *RACADM Reference Guide for iDRAC7 and CMC* available at support.dell.com/manuals.

Resetting iDRAC7 to Factory Default Settings

You can reset iDRAC7 to the factory default settings using the iDRAC Settings utility, or make sure to deselect the **Preserve Configuration** option while performing a firmware update.

To reset iDRAC7 to factory default values using the iDRAC Settings utility:

1. In the iDRAC Settings utility, go to **Reset iDRAC configurations to defaults**.
The **iDRAC Settings Reset iDRAC configurations to defaults** page is displayed.
2. Click **Yes**. iDRAC reset starts.
3. Click **Back** and navigate to the same **Reset iDRAC configurations to defaults** page to view the success message.

Frequently Asked Questions

This section lists the frequently asked questions for the following:


- [System Event Log](#)
- [Network Security](#)
- [Active Directory](#)
- [Single Sign On](#)
- [Smart Card Login](#)
- [Virtual Console](#)
- [Virtual Media](#)
- [vFlash SD Card](#)
- [SNMP Authentication](#)
- [Storage Devices](#)
- [RACADM](#)
- [Miscellaneous](#)

System Event Log

While using iDRAC7 Web interface through Internet Explorer, why does SEL not save using the Save As option?

This is due to a browser setting. To resolve this:

1. In Internet Explorer, go to **Tools** → **Internet Options** → **Security** and select the zone you are attempting to download in.
For example, if the iDRAC7 device is on the local intranet, select **Local Intranet** and click **Custom level...**
2. In the **Security Settings** window, under **Downloads** make sure that the following options are enabled:
 - Automatic prompting for file downloads (if this option is available)
 - File download

 **CAUTION: To make sure that the computer used to access iDRAC7 is safe, under Miscellaneous, do not enable the Launching applications and unsafe files option.**

Network Security

While accessing the iDRAC7 Web interface, a security warning appears stating that the SSL certificate issued by the Certificate Authority (CA) is not trusted.

iDRAC7 includes a default iDRAC7 server certificate to ensure network security while accessing through the Web-based interface and remote RACADM. This certificate is not issued by a trusted CA. To resolve this, upload a iDRAC7 server certificate issued by a trusted CA (for example, Microsoft Certificate Authority, Thawte or Verisign).

Why the DNS server not registering iDRAC7?

Some DNS servers register iDRAC7 names that contain only up to 31 characters.

When accessing the iDRAC7 Web-based interface, a security warning is displayed stating that the SSL certificate host name does not match the iDRAC7 host name.

iDRAC7 includes a default iDRAC7 server certificate to ensure network security while accessing through the Web-based interface and remote RACADM. When this certificate is used, the Web browser displays a security warning because the default certificate that is issued to iDRAC7 does not match the iDRAC7 host name (for example, the IP address).

To resolve this, upload an iDRAC7 server certificate issued to the IP address or the iDRAC7 host name. When generating the CSR (used for issuing the certificate), make sure that the common name (CN) of the CSR matches the iDRAC7 IP address (if certificate issued to IP) or the registered DNS iDRAC7 name (if certificate is issued to iDRAC7 registered name).

To make sure that the CSR matches the registered DNS iDRAC7 name:

1. In iDRAC7 Web interface, go to **Overview** → **iDRAC Settings** → **Network**. The **Network** page is displayed.
2. In the **Common Settings** section:
 - Select the **Register iDRAC on DNS** option.
 - In the **DNS iDRAC Name** field, enter the iDRAC7 name.
3. Click **Apply**.

Active Directory

Active Directory login failed. How to resolve this?

To diagnose the problem, on the **Active Directory Configuration and Management** page, click **Test Settings**. Review the test results and fix the problem. Change the configuration and run the test until the test user passes the authorization step.

In general, check the following:

- While logging in, make sure that you use the correct user domain name and not the NetBIOS name. If you have a local iDRAC7 user account, log into iDRAC7 using the local credentials. After logging in, make sure that:
 - The **Enable Active Directory** option is selected on the **Active Directory Configuration and Management** page.
 - The DNS setting is correct on the **iDRAC7 Networking configuration** page.
 - The correct Active Directory root CA certificate is uploaded to iDRAC7 if certificate validation was enabled.
 - The iDRAC name and iDRAC Domain name matches the Active Directory environment configuration if you are using extended schema.
 - The Group Name and Group Domain Name matches the Active Directory configuration if you are using standard schema.
- Check the domain controller SSL certificates to make sure that the iDRAC7 time is within the valid period of the certificate.

Active Directory login fails even if certificate validation is enabled. The test results display the following error message. Why does this occur and how to resolve this?

```
ERROR: Can't contact LDAP server, error:14090086:SSL
routines:SSL3_GET_SERVER_CERTIFICATE:certificate verify failed: Please check
the correct Certificate Authority (CA) certificate has been uploaded to iDRAC7.
Please also check if the iDRAC7 date is within the valid period of the
certificates and if the Domain Controller Address configured in iDRAC7 matches
the subject of the Directory Server Certificate.
```

If certificate validation is enabled, when iDRAC7 establishes the SSL connection with the directory server, iDRAC7 uses the uploaded CA certificate to verify the directory server certificate. The most common reasons for failing certification validation are:

- iDRAC7 date is not within the validity period of the server certificate or CA certificate. Check the iDRAC7 time and the validity period of your certificate.
- The domain controller addresses configured in iDRAC7 does not match the Subject or Subject Alternative Name of the directory server certificate. If you are using an IP address, read the next question. If you are using FQDN, make sure you are using the FQDN of the domain controller and not the domain. For example, **servername.example.com** instead of **example.com**.

Certificate validation fails even if IP address is used as the domain controller address. How to resolve this?

Check the Subject or Subject Alternative Name field of your domain controller certificate. Normally, Active Directory uses the host name and not the IP address of the domain controller in the Subject or Subject Alternative Name field of the domain controller certificate. To resolve this, do any of the following:

- Configure the host name (FQDN) of the domain controller as the *domain controller address(es)* on iDRAC7 to match the Subject or Subject Alternative Name of the server certificate.
- Reissue the server certificate to use an IP address in the Subject or Subject Alternative Name field, so that it matches the IP address configured in iDRAC7.
- Disable certificate validation if you choose to trust this domain controller without certificate validation during the SSL handshake.

How to configure the domain controller address(es) when using extended schema in a multiple domain environment?

This must be the host name (FQDN) or the IP address of the domain controller(s) that serves the domain in which the iDRAC7 object resides.

When to configure Global Catalog Address(es)?

If you are using standard schema and the users and role groups are from different domains, Global Catalog Address(es) are required. In this case, you can use only Universal Group.

If you are using standard schema and all the users and role groups are in the same domain, Global Catalog Address(es) are not required.

If you are using extended schema, the Global Catalog Address is not used.

How does standard schema query work?

iDRAC7 connects to the configured domain controller address(es) first. If the user and role groups are in that domain, the privileges are saved.

If Global Controller Address(es) is configured, iDRAC7 continues to query the Global Catalog. If additional privileges are retrieved from the Global Catalog, these privileges are accumulated.

Does iDRAC7 always use LDAP over SSL?

Yes. All the transportation is over secure port 636 and/or 3269. During test setting, iDRAC7 does a LDAP CONNECT only to isolate the problem, but it does not do an LDAP BIND on an insecure connection.

Why does iDRAC7 enable certificate validation by default?

iDRAC7 enforces strong security to ensure the identity of the domain controller that iDRAC7 connects to. Without certificate validation, a hacker can spoof a domain controller and hijack the SSL connection. If you choose to trust all the domain controllers in your security boundary without certificate validation, you can disable it through the Web interface or RACADM.

Does iDRAC7 support the NetBIOS name?

Not in this release.

Why does it take up to four minutes to log in to iDRAC7 using Active Directory Single Sign-On or Smart Card Login?

The Active Directory Single Sign-On or Smart Card log in normally takes less than 10 seconds, but it may take up to four minutes to log in if you have specified the preferred DNS server and the alternate DNS server, and the preferred DNS server has failed. DNS time-outs are expected when a DNS server is down. iDRAC7 logs you in using the alternate DNS server.

The Active Directory is configured for a domain present in Windows Server 2008 Active Directory. A child or sub domain is present for the domain, the user and group is present in the same child domain, and the user is a member of that group. When trying to log in to iDRAC7 using the user present in the child domain, Active Directory Single Sign-On login fails.

This may be because of the an incorrect group type. There are two kinds of Group types in the Active Directory server:

- Security — Security groups allow you to manage user and computer access to shared resources and to filter group policy settings.
- Distribution — Distribution groups are intended to be used only as e-mail distribution lists.

Always make sure that the group type is Security. You cannot use distribution groups to assign permission on any object, however use them to filter group policy settings.

Single Sign-On

SSO login fails on Windows Server 2008 R2 x64. What are the settings required to resolve this?

1. Run the [technet.microsoft.com/en-us/library/dd560670\(WS.10\).aspx](http://technet.microsoft.com/en-us/library/dd560670(WS.10).aspx) for the domain controller and domain policy.
2. Configure the computers to use the DES-CBC-MD5 cipher suite.
These settings may affect compatibility with client computers or services and applications in your environment. The Configure encryption types allowed for Kerberos policy setting is located at **Computer Configuration** → **Security Settings** → **Local Policies** → **Security Options**.
3. Make sure that the domain clients have the updated GPO.
4. At the command line, type `gpupdate /force` and delete the old key tab with `klist purge` command.
5. After the GPO is updated, create the new keytab.
6. Upload the keytab to iDRAC7.

You can now log in to iDRAC7 using SSO.

Why does SSO login fail with Active Directory users on Windows 7 and Windows Server 2008 R2?

You must enable the encryption types for Windows 7 and Windows Server 2008 R2. To enable the encryption types:

1. Log in as administrator or as a user with administrative privilege.
2. Go to **Start** and run `gpedit.msc`. The **Local Group Policy Editor** window is displayed.
3. Go to **Local Computer Settings** → **Windows Settings** → **Security Settings** → **Local Policies** → **Security Options**.
4. Right-click **Network Security: Configure encryption types allowed for kerberos** and select **Properties**.
5. Enable all the options.
6. Click **OK**. You can now log in to iDRAC7 using SSO.

Perform the following additional settings for Extended Schema:

1. In the **Local Group Policy Editor** window, navigate to **Local Computer Settings** → **Windows Settings** → **Security Settings** → **Local Policies** → **Security Options**.
2. Right-click **Network Security: Restrict NTLM: Outgoing NTLM traffic to remote server** and select **Properties**.
3. Select **Allow all**, click **OK**, and close the **Local Group Policy Editor** window.
4. Go to **Start** and run `cmd`. The command prompt window is displayed.
5. Run the command `gpupdate /force`. The group policies are updated. Close the command prompt window.
6. Go to **Start** and run `regedit`. The **Registry Editor** window is displayed.
7. Navigate to **HKEY_LOCAL_MACHINE** → **System** → **CurrentControlSet** → **Control** → **LSA**.
8. In the right-pane, right-click and select **New** → **DWORD (32-bit) Value**.

9. Name the new key as **SuppressExtendedProtection**.
10. Right-click **SuppressExtendedProtection** and click **Modify**.
11. In the **Value** data field, type **1** and click **OK**.
12. Close the **Registry Editor** window. You can now log in to iDRAC7 using SSO.

If you have enabled SSO for iDRAC7 and you are using Internet Explorer to log in to iDRAC7, SSO fails and you are prompted to enter your user name and password. How to resolve this?

Make sure that the iDRAC7 IP address is listed in the **Tools** → **Internet Options** → **Security** → **Trusted sites**. If it is not listed, SSO fails and you are prompted to enter your user name and password. Click **Cancel** and proceed.

Smart Card Login

It takes up to four minutes to log into iDRAC7 using Active Directory Smart Card login.

The normal Active Directory Smart Card login normally takes less than 10 seconds, however it may take up to four minutes if you have specified the preferred DNS server and the alternate DNS server in the **Network** page, and the preferred DNS server has failed. DNS time-outs are expected when a DNS server is down. iDRAC7 logs you in using the alternate DNS server.

ActiveX plug-in unable to detect the Smart Card reader.

Make sure that the smart card is supported on the Microsoft Windows operating system. Windows supports a limited number of smart card Cryptographic Service Providers (CSPs).

In general, check if the smart card CSPs are present on a particular client, insert the smart card in the reader at the Windows logon (Ctrl-Alt-Del) screen and check if Windows detects the smart card and displays the PIN dialog-box.

Incorrect Smart Card PIN.

Check if the smart card is locked due to too many attempts with an incorrect PIN. In such cases, contact the smart card issuer in the organization to get a new smart card.

Virtual Console

Virtual Console session is active even if you have logged out of iDRAC7 Web interface. Is this the expected behavior?

Yes. Close the Virtual Console Viewer window to log out of the corresponding session.

Can a new remote console video session be started when the local video on the server is turned off?

Yes.

Why does it take 15 seconds to turn off the local video on the server after requesting to turn off the local video?

It gives a local user an opportunity to take any action before the video is switched off.

Is there a time delay when turning on the local video?

No, after a local video turn ON request is received by iDRAC7, the video is turned on instantly.

Can the local user also turn off or turn on the video?

When the local console is disabled, the local user cannot turn off or turn on the video.

Does switching off the local video also switch off the local keyboard and mouse?

No.

Does turning off the local console turn off the video on the remote console session?

No, turning the local video on or off is independent of the remote console session.

What privileges are required for an iDRAC7 user to turn on or turn off the local server video?

Any user with iDRAC7 configuration privileges can turn on or turn off the local console.

How to get the current status of the local server video?

The status is displayed on the Virtual Console page.

Use the RACADM command `racadm getconfig -g cfgRacTuning` to display the status in the object `cfgRacTuneLocalServerVideo`.

Or, use the following RACADM command from a Telnet, SSH, or a remote session:

```
racadm -r (iDRAC IP) -u -p getconfig -g cfgRacTuning
```

The status is also seen on the Virtual Console OSCAR display. When the local console is enabled, a green status is displayed next to the server name. When disabled, a yellow dot indicates that iDRAC7 has locked the local console.

Why is the bottom of the system screen not seen from the Virtual Console window?

Make sure that the management station's monitor resolution is set to 1280 x 1024.

Why is the Virtual Console Viewer window garbled on Linux operating system?

The console viewer on Linux requires a UTF-8 character set. Check your locale and reset the character set if required.

Why does the mouse not synchronize under the Linux text console in Lifecycle Controller?

Virtual Console requires the USB mouse driver, but the USB mouse driver is available only under the X-Window operating system. In the Virtual Console viewer, do any of the following:

- Go to **Tools** → **Session Options** → **Mouse** tab. Under **Mouse Acceleration**, select **Linux**.
- Under the **Tools** menu, select **Single Cursor** option .

How to synchronize the mouse pointers on the Virtual Console Viewer window?

Before starting a Virtual Console session, make sure that the correct mouse is selected for your operating system.

Make sure that the **Single Cursor** option under **Tools** in the iDRAC7 Virtual Console menu is selected on iDRAC7 Virtual Console client. The default is two cursor mode.

Can a keyboard or mouse be used while installing a Microsoft operating system remotely through the Virtual Console?

No. When you remotely install a supported Microsoft operating system on a system with Virtual Console enabled in the BIOS, an EMS Connection Message is sent that requires that you select **OK** remotely. You must either select **OK** on the local system or restart the remotely managed server, reinstall, and then turn off the Virtual Console in BIOS.

This message is generated by Microsoft to alert the user that Virtual Console is enabled. To make sure that this message does not appear, always turn off Virtual Console in the iDRAC Settings utility before remotely installing an operating system.

Why does the Num Lock indicator on the management station not reflect the status of the Num Lock on the remote server?

When accessed through the iDRAC7, the Num Lock indicator on the management station does not necessarily coincide with the state of the Num Lock on the remote server. The state of the Num Lock is dependent on the setting on the remote server when the remote session is connected, regardless of the state of the Num Lock on the management station.

Why do multiple Session Viewer windows appear when a Virtual Console session is established from the local host?

You are configuring a Virtual Console session from the local system. This is not supported.

If a Virtual Console session is in-progress and a local user accesses the managed server, does the first user receive a warning message?

No. If a local user accesses the system, both have control of the system.

How much bandwidth is required to run a Virtual Console session?

It is recommended to have a 5 MBPS connection for good performance. A 1 MBPS connection is required for minimal performance.

What are the minimum system requirements for the management station to run Virtual Console?

The management station requires an Intel Pentium III 500 MHz processor with at least 256 MB of RAM.

Why does Virtual Console Viewer window sometimes displays No Signal message?

You may see this message because the iDRAC7 Virtual Console plug-in is not receiving the remote server desktop video. Generally, this behavior may occur when the remote server is turned off. Occasionally, the message may be displayed due to a remote server desktop video reception malfunction.

Why does Virtual Console Viewer window sometimes display an Out of Range message?

You may see this message because a parameter necessary to capture video is beyond the range for which the iDRAC7 can capture the video. Parameters such as display resolution or refresh rate too high will cause an out of range condition. Normally, physical limitations such as video memory size or bandwidth sets the maximum range of parameters.

When starting a Virtual Console session from iDRAC7 Web interface, why is an ActiveX security popup displayed?

iDRAC7 may not be in the trusted site list. To prevent the security popup from appearing every time you begin a Virtual Console session, add iDRAC7 to the trusted site list in the client browser:

1. Click **Tools** → **Internet Options** → **Security** → **Trusted sites**.
2. Click **Sites** and enter the IP address or the DNS name of iDRAC7
3. Click **Add**.
4. Click **Custom Level**.
5. In the **Security Settings** window, select **Prompt** under **Download unsigned ActiveX Controls**.

Why is the Virtual Console Viewer window blank?

If you have Virtual Media privilege, but not Virtual Console privilege, you can start the viewer to access the virtual media feature, but the managed server's console is not displayed.

Why doesn't the mouse synchronize in DOS when using Virtual Console?

The Dell BIOS is emulating the mouse driver as a PS/2 mouse. By design, the PS/2 mouse uses relative position for the mouse pointer, which causes the lag in syncing. iDRAC7 has a USB mouse driver, that allows absolute position and closer tracking of the mouse pointer. Even if iDRAC7 passes the USB absolute mouse position to the Dell BIOS, the BIOS emulation converts it back to relative position and the behavior remains. To fix this problem, set the mouse mode to USC/Diags in the Configuration screen.

After launching the Virtual Console, the mouse cursor is active on the Virtual Console, but not on the local system. Why does this occur and how to resolve this?

This occurs if the **Mouse Mode** is set to **USC/Diags**. Press **Alt + M** hot key to use the mouse on the local system. Press **Alt + M** again to use the mouse on the Virtual Console.

When iDRAC7 Web interface is launched from the CMC Web interface soon after Virtual Console is launched, why does GUI session time-out?

When launching the Virtual Console to iDRAC7 from the CMC Web interface a popup is opened to launch the Virtual Console. The popup closes shortly after the Virtual Console opens.

When launching both the GUI and Virtual Console to the same iDRAC7 system on a management station, a session time-out for the iDRAC7 GUI occurs if the GUI is launched before the popup closes. If the iDRAC7 GUI is launched from the CMC Web interface after the popup with the Virtual Console closed, this issue does not appear.


Why does Linux SysRq key not work with Internet Explorer?

The Linux SysRq key behavior is different when using Virtual Console from Internet Explorer. To send the SysRq key, press the **Print Screen** key and release while holding the **Ctrl** and **Alt** keys. To send the SysRq key to a remote Linux server through iDRAC7, while using Internet Explorer:

1. Activate the magic key function on the remote Linux server. You can use the following command to activate it on the Linux terminal:

```
echo 1 > /proc/sys/kernel/sysrq
```

2. Activate the keyboard pass-through mode of Active X Viewer.
3. Press **Ctrl + Alt +Print Screen**.
4. Release only **Print Screen**.
5. Press **Print Screen+Ctrl+Alt**.

 **NOTE:** The SysRq feature is currently not supported with Internet Explorer and Java.

Why is the "Link Interrupted" message displayed at the bottom of the Virtual Console?

When using the shared network port during a server reboot, iDRAC is disconnected while BIOS is resetting the network card. This duration is longer on 10 Gb cards, and is also exceptionally long if the connected network switch has Spanning Tree Protocol (STP) enabled. In this case, it is recommended to enable "portfast" for the switch port connected to the server. In most cases, the Virtual Console restores itself.

Virtual Media

Why does the Virtual Media client connection sometimes drop?

When a network time-out occurs, iDRAC7 firmware drops the connection, disconnecting the link between the server and the virtual drive.

If you change the CD in the client system, the new CD may have an autostart feature. In this case, the firmware can time-out and the connection is lost if the client system takes too long to read the CD. If a connection is lost, reconnect from the GUI and continue the previous operation.

If the Virtual Media configuration settings are changed in the iDRAC7 Web interface or through local RACADM commands, any connected media is disconnected when the configuration change is applied.

To reconnect to the Virtual Drive, use the Virtual Media **Client View** window.

Why does a Windows operating system installation through Virtual Media takes an extended amount of time?

If you are installing the Windows operating system using the *Dell Systems Management Tools and Documentation DVD* and the network connection is slow, the installation procedure may require an extended amount of time to access iDRAC7 Web interface due to network latency. The installation window does not indicate the installation progress.

How to configure the virtual device as a bootable device?

On the managed system, access BIOS Setup and go to the boot menu. Locate the virtual CD, virtual floppy, or vFlash and change the device boot order as required. Also, press the "spacebar" key in the boot sequence in the CMOS setup to make the virtual device bootable. For example, to boot from a CD drive, configure the CD drive as the first device in the boot order.

What are the types of media that can be set as a bootable device?

iDRAC7 allows you to boot from the following bootable media:

- CDROM/DVD Data media
- ISO 9660 image
- 1.44 Floppy disk or floppy image
- A USB key that is recognized by the operating system as a removable disk
- A USB key image

How to make the USB key a bootable device?

Search support.dell.com for the Dell Boot Utility

You can also boot with a Windows 98 startup disk and copy system files from the startup disk to the USB key. For example, from the DOS prompt, type the following command:

```
sys a: x: /s
```

where, x: is the USB key that is required to be set as a bootable device.

The Virtual Media is attached and connected to the remote floppy. But, cannot locate the Virtual Floppy/Virtual CD device on a system running Red Hat Enterprise Linux or the SUSE Linux operating system. How to resolve this?

Some Linux versions do not auto-mount the virtual floppy drive and the virtual CD drive in the same method. To mount the virtual floppy drive, locate the device node that Linux assigns to the virtual floppy drive. To mount the virtual floppy drive:

1. Open a Linux command prompt and run the following command:

```
grep "Virtual Floppy" /var/log/messages
```

2. Locate the last entry to that message and note the time.

3. At the Linux prompt, run the following command:

```
grep "hh:mm:ss" /var/log/messages
```

where, hh:mm:ss is the time stamp of the message returned by grep in step 1.

4. In step 3, read the result of the grep command and locate the device name that is given to the Virtual Floppy.

5. Make sure that you are attached and connected to the virtual floppy drive.

6. At the Linux prompt, run the following command:

```
mount /dev/sdx /mnt/floppy
```

where, /dev/sdx is the device name found in step 4 and /mnt/floppy is the mount point.

To mount the virtual CD drive, locate the device node that Linux assigns to the virtual CD drive. To mount the virtual CD drive:

1. Open a Linux command prompt and run the following command:

```
grep "Virtual CD" /var/log/messages
```

2. Locate the last entry to that message and note the time.

3. At the Linux prompt, run the following command:

```
grep "hh:mm:ss" /var/log/messages
```

where, hh:mm:ss is the timestamp of the message returned by grep in step 1.

4. In step 3, read the result of the grep command and locate the device name that is given to the *Dell Virtual CD*.

5. Make sure that the Virtual CD Drive is attached and connected.

6. At the Linux prompt, run the following command:

```
mount /dev/sdx /mnt/CD
```

where: /dev/sdx is the device name found in step 4 and /mnt/floppy is the mount point.

Why are the virtual drives attached the server removed after performing a remote firmware update using the iDRAC7 Web interface?

Firmware updates cause the iDRAC7 to reset, drop the remote connection, and unmount the virtual drives. The drives reappear when iDRAC7 reset is complete.

Why are all the USB devices detached after connecting a USB device?

Virtual media devices and vFlash devices are connected as a composite USB device to the Host USB BUS, and they share a common USB port. Whenever any virtual media or vFlash USB device is connected to or disconnected from the

host USB bus, all the Virtual Media and vFlash devices are disconnected momentarily from the host USB bus, and then they are re-connected. If the host operating system uses a virtual media device, do not attach or detach one or more virtual media or vFlash devices. It is recommended that you connect all the required USB devices first before using them.


What does the USB Reset do?

It resets the remote and local USB devices connected to the server.

How to maximize Virtual Media performance?

To maximize Virtual Media performance, launch the Virtual Media with the Virtual Console disabled or do one of the following:

- Change the performance slider to Maximum Speed.
- Disable encryption for both Virtual Media and Virtual Console.

 **NOTE:** In this case, the data transfer between managed server and iDRAC7 for Virtual Media and Virtual Console will not be secured.

- If you are using any Windows server operating systems, stop the Windows service named Windows Event Collector. To do this, go to **Start** → **Administrative Tools** → **Services**. Right-click **Windows Event Collector** and click **Stop**.

While viewing the contents of a floppy drive or USB key, a connection failure message is displayed if the same drive is attached through the virtual media?

Simultaneous access to virtual floppy drives are not allowed. Close the application used to view the drive contents before attempting to virtualize the drive.

What file system types are supported on the Virtual Floppy Drive?

The virtual floppy drive supports FAT16 or FAT32 file systems.

Why is an error message displayed when trying to connect a DVD/USB through virtual media even though the virtual media is currently not in use?

The error message is displayed if Remote File Share (RFS) feature is also in use. At a time, you can use RFS or Virtual Media and not both.

vFlash SD Card

When is the vFlash SD card locked?

The vFlash SD card is locked when an operation is in-progress. For example, during an initialize operation.

SNMP Authentication

Why is the message 'Remote Access: SNMP Authentication Failure' displayed?

As part of discovery, IT Assistant attempts to verify the get and set community names of the device. In IT Assistant, you have the get community name = public and the set community name = private. By default, the SNMP agent community name for iDRAC7 agent is public. When IT Assistant sends out a set request, the iDRAC7 agent generates the SNMP authentication error because it accepts requests only from community = public.

To prevent SNMP authentication errors from being generated, you must enter community names that are accepted by the agent. Since the iDRAC7 only allows one community name, you must use the same get and set community name for IT Assistant discovery setup.

Storage Devices

Information for all the storage devices connected to the system are not displayed and OpenManage Storage Management displays more storage devices than iDRAC7. Why?

iDRAC7 displays information for only the Comprehensive Embedded Management (CEM) supported devices.

RACADM

After performing an iDRAC7 reset (using the `racadm racreset` command), if any command is issued, the following message is displayed. What does this indicate?

```
ERROR: Unable to connect to RAC at specified IP address
```

The message indicates that you must wait until the iDRAC7 completes the reset before issuing another command.

When using RACADM commands and subcommands, some errors are not clear.

You may see one or more of the following errors when using the RACADM commands and subcommands:

- Local RACADM error messages — Problems such as syntax, typographical errors, and incorrect names.
- Remote RACADM error messages — Problems such as incorrect IP Address, incorrect user name, or incorrect password.

During a ping test to iDRAC7, if the network mode is switched between Dedicated and Shared modes, there is no ping response.

Clear the ARP table on your system.

Remote RACADM fails to connect to iDRAC7 from SUSE Linux Enterprise Server (SLES) 11 SP1.

Make sure that the official `openssl` and `libopenssl` versions are installed. Run the following command to install the RPM packages:

```
rpm -ivh --force < filename >
```

where, `filename` is the `openssl` or `libopenssl` rpm package file.

For example:

```
rpm -ivh --force openssl-0.9.8h-30.22.21.1.x86_64.rpm
```

```
rpm -ivh --force libopenssl10_9_8-0.9.8h-30.22.21.1.x86_64.rpm
```

Why are the remote RACADM and Web-based services unavailable after a property change?

It may take a while for the remote RACADM services and the Web-based interface to become available after the iDRAC7 Web server resets.

The iDRAC7 Web server is reset when:

- The network configuration or network security properties are changed using the iDRAC7 Web user interface.
- The `cfgRacTuneHttpsPort` property is changed (including when a `config -f (config file)` changes it).
- The `racresetcfg` command is used.
- iDRAC7 is reset.
- A new SSL server certificate is uploaded.

Why is an error message displayed if you try to delete a partition after creating it using local RACADM?

This occurs because the create partition operation is in-progress. However, the partition is deleted after sometime and a message that the partition is deleted is displayed. If not, wait until the create partition operation is completed and then delete the partition.

Miscellaneous

How to find an iDRAC IP address for a blade server?

You can find the iDRAC IP address using any of the following methods:

Using CMC Web interface: Go to **Chassis** → **Servers** → **Setup** → **Deploy**, and in the displayed table, view the IP address for the server.

Using the Virtual Console: Reboot the server to view the iDRAC IP address during POST. Select the "Dell CMC" console in the OSCAR to log in to CMC through a local serial connection. CMC RACADM commands can be sent from this connection. See the *RACADM Command Line Reference Guide for iDRAC7 and CMC* for a complete list of CMC RACADM subcommands.

From local RACADM, Use the command: `racadm getsysinfo` For example:

```
$ racadm getniccfg -m server-1
DHCP Enabled      = 1
IP Address        = 192.168.0.1
Subnet Mask       = 255.255.255.0
Gateway          = 192.168.0.1
```


Using LCD: On the Main Menu, highlight the Server and press the check button and select the required server and press the check button.

How to find the CMC IP address related to the blade server?

From iDRAC7 Web interface: Click **Overview** → **iDRAC Settings** → **CMC**. The **CMC Summary** page displays the CMC IP address.

From the Virtual Console: Select the "Dell CMC" console in the OSCAR to log in to CMC through a local serial connection. CMC RACADM commands can be issued from this connection. See the *RACADM Command Line Reference Guide for iDRAC7 and CMC* for a complete list of CMC RACADM subcommands

```
$ racadm getniccfg -m chassis
NIC Enabled       = 1
DHCP Enabled      = 1
Static IP Address = 192.168.0.120
Static Subnet Mask = 255.255.255.0
Static Gateway    = 192.168.0.1
Current IP Address = 10.35.155.151
Current Subnet Mask = 255.255.255.0
Current Gateway   = 10.35.155.1
Speed             = Autonegotiate
Duplex            = Autonegotiate
```

 **NOTE:** You can also perform this using remote RACADM.

How to find iDRAC IP address for rack and tower server?

From iDRAC7 Web Interface: Go to **Overview** → **Server** → **Properties** → **Summary**. The **System Summary** page displays the iDRAC7 IP address.

From Local RACADM: Use the command `racadm getsysinfo`.

From LCD: On the physical server, use the LCD panel navigation buttons to view the iDRAC7 IP address. Go to **Setup View** → **View** → **iDRAC IP** → **IPv4** or **IPv6** → **IP**.

From OpenManage Server Administrator: In the Server Administrator Web interface, go to **Modular Enclosure** → **System/Server Module** → **Main System Chassis/Main System** → **Remote Access**.

iDRAC7 network connection is not working.

For blade servers:

- Make sure that the LAN cable is connected to CMC.
- Make sure that NIC settings, IPv4 or IPv6 settings, and either Static or DHCP is enabled for your network.

For rack and tower servers:

- In shared mode, make sure the LAN cable is connected to the NIC port where the wrench symbol is present.
- In Dedicated mode, make sure the LAN cable is connected to the iDRAC LAN port.
- Make sure that NIC settings, IPv4 and IPv6 settings and either Static or DHCP is enabled for your network.

Inserted the blade server into the chassis and pressed the power switch, but it did not power on.

- iDRAC7 requires up to two minutes to initialize before the server can power on.
- Check CMC power budget. The chassis power budget may have exceeded.

How to retrieve an iDRAC7 administrative user name and password?

You must restore iDRAC7 to its default settings. For more information, see [Resetting iDRAC7 to Factory Default Settings](#).

How to change the name of the slot for the system in a chassis?

1. Log in to CMC Web interface and go to **Chassis** → **Servers** → **Setup** .
2. Enter the new name for the slot in the row for your server and click **Apply**.

iDRAC7 on blade server is not responding during boot.

Remove and reinsert the server.

Check CMC Web interface to see if iDRAC7 is displayed as an upgradable component. If it does, follow the instructions in [Updating Firmware Using CMC Web Interface](#).

If the problem persists, contact technical support.

When attempting to boot the managed server, the power indicator is green, but there is no POST or no video.

This happens due to any of the following conditions:

- Memory is not installed or is inaccessible.
- CPU is not installed or is inaccessible
- Video riser card is missing or not connected properly.

Also, see error messages in iDRAC7 log using iDRAC7 Web interface or from the server LCD.

Use Case Scenarios

This section helps you in navigating to specific sections in the guide to perform typical use case scenarios.

Troubleshooting An Inaccessible Managed System

After receiving alerts from OpenManage Essentials, Dell Management Console, or a local trap collector, five servers in a data center are not accessible with issues such as hanging operating system or server. Need to identify the cause to troubleshoot and bring up the server using iDRAC7.

Before troubleshooting the inaccessible system, make sure that the following prerequisites are met:

- Enable last crash screen
- Alerts are enabled on iDRAC7

To identify the cause, check the following in the iDRAC Web interface and re-establish the connection to the system:



NOTE: If you are not able access the iDRAC Web interface: go to the sever, access the LCD panel, write down the IP address or the host name, and then perform the following operations using iDRAC Web interface from your management station:

- Server's LED status — Blinking amber or Solid amber.
- Front Panel LCD status or error message — Amber LCD or error message.
- Operating system image is seen in the Virtual Console. If you can see the image, reset the system (warm boot) and log in again. If you are able to log in, the issue is fixed.
- Last crash screen.
- Boot capture video.
- Crash capture video.
- Server Health status — Red *x* icons for the system components with issues.
- Storage array status — Possible array offline or failed
- Lifecycle log for critical events related to system hardware and firmware and the log entries that were logged at the time of system crash.

Obtaining System Information and Assess system Health

To obtain system information and assess system health:

- In iDRAC7 Web interface, go to **Overview** → **Server** → **System Summary** to view the system information and access various links on this page to asses system health. For example, you can check the health of the chassis fan.
- You can also configure the chassis locator LED and based on the color, assess the system health.

Setting Up Alerts and Configuring E-mail Alerts


To set up alerts and configure e-mail alerts:

1. Enable alerts.
2. Configure the e-mail alert and check the ports.
3. Perform a reboot, power off, or power cycle the managed system.
4. Send test alert.

Viewing and Exporting Lifecycle Log and System Event Log

To view and export lifecycle log and system event log (SEL):

1. In iDRAC7 Web interface, go to **Overview** → **Server** → **Logs** to view SEL and **Overview** → **Server** → **Logs** → **Lifecycle Log** to view lifecycle log.

 **NOTE:** The SEL is also recorded in the lifecycle log. Using the filtering options to view the SEL.

2. Export the SEL or lifecycle log in the XML format to an external location (management station, USB, network share, and so on). Alternatively, you can enable remote system logging, so that all the logs written to the lifecycle log are also simultaneously written to the configured remote server(s).

Interfaces to Update iDRAC Firmware

Use the following interfaces to update the iDRAC firmware:

- iDRAC7 Web interface
- RACADM CLI (iDRAC7 and CMC)
- Dell Update Package (DUP)
- CMC Web interface
- Lifecycle Controller–Remote Services
- Lifecycle Controller
- Dell Remote Access Configuration Tool (DRACT)

Performing Graceful Shutdown

To perform graceful shutdown, in iDRAC7 Web interface, go to one of the following locations:

- **Overview** → **Server** → **Power/Thermal** → **Power Configuration** → **Power Control**. The **Power Control** page is displayed. Select **Graceful Shutdown** and click **Apply**.
- **Overview** → **Server** → **Power/Thermal** → **Power Monitoring**. From the **Power Control** drop-down menu, select **Graceful Shutdown** and click **Apply**.

For more information, see the *iDRAC7 Online Help*.

Creating New Administrator User Account

You can modify the default local administrator user account or create a new administrator user account. To modify the local administrator user account, see [Modifying Local Administrator Account Settings](#).

To create a new administrator account, see the following sections:

- [Configuring Local Users](#)
- [Configuring Active Directory Users](#)
- [Configuring Generic LDAP Users](#)

Launching Server's Remote Console and Mounting a USB Drive

To launch the remote console and mount a USB drive:

1. Connect a USB flash drive (with the required image) to the management station.
2. Use one the following methods to launch virtual console through the iDRAC7 Web Interface:
 - Go to **Overview** → **Server** → **Console** and click **Launch Virtual Console**.
 - Go to **Overview** → **Server** → **Properties** and click **Launch** under **Virtual Console Preview**.

The **Virtual Console Viewer** is displayed.

3. From the **File** menu, click **Virtual Media** → **Launch Virtual Media** .
4. Click **Add Image** and select the image that is located on the USB flash drive.
The image is added to the list of available drives.
5. Select the drive to map it. The image on the USB flash drive is mapped to the managed system.

Installing Bare Metal OS Using Attached Virtual Media and Remote File Share


To do this, see [Deploying Operating System Using Remote File Share](#).

Managing Rack Density

Currently, the two servers are installed in a rack. To add two additional servers, need to determine how much capacity is left in the rack.

To assess the capacity of a rack to add additional servers:

1. View the current power consumption data and historical power consumption data for the servers.
2. Based on the data, power infrastructure and cooling system limitations, enable the power cap policy and set the power cap values.

 **NOTE:** It is recommended that you set a cap close to the peak, and then use that capped level to determine how much capacity is remaining in the rack for adding more servers.

Installing New Electronic License

See [License Operations](#) for more information.