# Integrated Dell Remote Access Controller 6 (iDRAC6)

# Administrator Reference Guide

# Notes and Cautions

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

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



**July 2010**

# Contents

# 1

# Introduction

This document provides information about the RACADM subcommands, supported RACADM interfaces, and property database groups and object definitions for the following:

- iDRAC6 Enterprise on Blade Servers
- iDRAC6 Enterprise or Express on Rack and Tower Servers

## Supported RACADM Interfaces

The RACADM command-line utility provides a scriptable interface that allows you to locally or remotely configure your Remote Access Controller (RAC). The utility runs on the management station and the managed system. It is available on the *Dell OpenManage Systems Management and Documentation* DVD or at **support.dell.com**.

The RACADM utility supports the following interfaces:

- Local — Supports executing RACADM commands from the managed server's Operating System. You must install the OpenManage software on the managed server to run local racadm commands.
- SSH or Telnet — Supports executing RACADM commands from a SSH or Telnet session to iDRAC.
- Remote — Supports executing RACADM commands from a remote management station such as a laptop or desktop computer. You must install the OpenManage software on the remote computer to run remote RACADM commands. To execute remote RACADM commands, you must formulate the command like a local or SSH/Telnet RACADM command except that you must also use the –r –i options or the –r –u –p options. For more information on these options, see the "RACADM Subcommand Details" on page 23.

Table 1-1 provides the supported RACADM interfaces for iDRAC6 Enterprise and iDRAC6 Express.

**Table 1-1. Supported RACADM Interfaces**

| iDRAC Type | Local RACADM | SSH/Telnet RACADM | Remote RACADM |
|---|---|---|---|
| iDRAC6 Enterprise | ✓ | ✓ | ✓ |
| iDRAC6 Express | ✓ | ✓ | ✗ |

✓ = Supported; ✗ = Not supported

# Supported RACADM Subcommands

Table 1-2 provides the list of RACADM subcommands and their corresponding interface support. For detailed information of the RACADM subcommands including syntax and valid entries, see "RACADM Subcommand Details" on page 23.

**Table 1-2. RACADM Subcommands**

| Subcommand | iDRAC6 on Blade Servers | iDRAC6 on Rack and Tower Servers | Telnet/SSH/ Serial | Local RACADM | Remote RACADM |
|---|---|---|---|---|---|
| arp | ✓ | ✓ | ✓ | ✗ | ✓ |
| clearasrscreen | ✓ | ✓ | ✓ | ✓ | ✓ |
| closessn | ✓ | ✓ | ✓ | ✓ | ✓ |
| clrraclog | ✓ | ✓ | ✓ | ✓ | ✓ |
| clrsel | ✓ | ✓ | ✓ | ✓ | ✓ |
| config | ✓ | ✓ | ✓ | ✓ | ✓ |
| coredump | ✓ | ✓ | ✓ | ✗ | ✓ |
| coredumpdelete | ✓ | ✓ | ✓ | ✓ | ✓ |
| fwupdate | ✓ | ✓ | ✓ | ✓ | ✓ |

**Table 1-2. RACADM Subcommands *(continued)***

| Subcommand | iDRAC6 on Blade Servers | iDRAC6 on Rack and Tower Servers | Telnet/SSH/ Serial | Local RACADM | Remote RACADM |
|---|---|---|---|---|---|
| getconfig | ✓ | ✓ | ✓ | ✓ | ✓ |
| getniccfg | ✓ | ✓ | ✓ | ✓ | ✓ |
| getraclog | ✓ | ✓ | ✓ | ✓ | ✓ |
| getractime | ✓ | ✓ | ✓ | ✓ | ✓ |
| getsel | ✓ | ✓ | ✓ | ✓ | ✓ |
| getssninfo | ✓ | ✓ | ✓ | ✓ | ✓ |
| getsvctag | ✓ | ✓ | ✓ | ✓ | ✓ |
| getsysinfo | ✓ | ✓ | ✓ | ✓ | ✓ |
| gettracelog | ✓ | ✓ | ✓ | ✓ | ✓ |
| help | ✓ | ✓ | ✓ | ✓ | ✓ |
| ifconfig | ✓ | ✓ | ✓ | ✗ | ✓ |
| krbkeytabupload | ✓ | ✓ | ✗ | ✓ | ✓ |
| localConRedirDisable | ✓ | ✓ | ✗ | ✓ | ✗ |
| netstat | ✓ | ✓ | ✓ | ✗ | ✓ |
| ping | ✓ | ✓ | ✓ | ✗ | ✓ |
| ping6 | ✓ | ✗ | ✓ | ✗ | ✓ |
| racdump | ✓ | ✓ | ✓ | ✗ | ✓ |
| racreset | ✓ | ✓ | ✓ | ✓ | ✓ |
| racresetcfg | ✓ | ✓ | ✓ | ✓ | ✓ |

**Table 1-2. RACADM Subcommands *(continued)***

| Subcommand | iDRAC6 on Blade Servers | iDRAC6 on Rack and Tower Servers | Telnet/SSH/ Serial | Local RACADM | Remote RACADM |
|---|---|---|---|---|---|
| remoteimage | ✓ | ✗ | ✓ | ✗ | ✓ |
| serveraction | ✓ | ✓ | ✓ | ✓ | ✓ |
| setniccfg | ✓ | ✓ | ✓ | ✓ | ✓ |
| sshpkauth | ✓ | ✓ | ✓ | ✓ | ✓ |
| sslcertdownload | ✓ | ✓ | ✗ | ✓ | ✓ |
| sslcertupload | ✓ | ✓ | ✗ | ✓ | ✓ |
| sslcertview | ✓ | ✓ | ✓ | ✓ | ✓ |
| sslcsrgen | ✓ | ✓ | ✗ | ✓ | ✓ |
| sslkeyupload | ✗ | ✓ | ✗ | ✓ | ✓ |
| testemail | ✓ | ✓ | ✓ | ✓ | ✓ |
| testtrap | ✓ | ✓ | ✓ | ✓ | ✓ |
| traceroute | ✓ | ✗ | ✓ | ✗ | ✓ |
| traceroute6 | ✓ | ✗ | ✓ | ✗ | ✓ |
| usercertupload | ✗ | ✓ | ✗ | ✓ | ✓ |
| usercertview | ✗ | ✓ | ✓ | ✓ | ✓ |
| version | ✓ | ✗ | ✗ | ✓ | ✗ |
| vflashsd | ✓ | ✓ | ✓ | ✓ | ✓ |
| vflashpartition | ✓ | ✓ | ✓ | ✓ | ✓ |
| vmdisconnect | ✓ | ✓ | ✓ | ✓ | ✓ |
| vmkey | ✓ | ✓ | ✓ | ✓ | ✓ |

## Other Documents You May Need

In addition to this guide, you can access the following guides available on the Dell Support website at **support.dell.com/manuals**. On the **Manuals** page, click **Software→ Systems Management**. Click on the appropriate product link on the right-side to access the documents.

- The *Integrated Dell Remote Access Controller 6 (iDRAC6) Enterprise for Blade Servers User Guide* provides information about configuring and using an iDRAC6 for blade servers to remotely manage and monitor your system and its shared resources through a network.
- The *Integrated Dell Remote Access Controller 6 (iDRAC6) User Guide* provides complete information about configuring and using an iDRAC6 for rack and tower servers to remotely manage and monitor your system and its shared resources through a network.
- The *Glossary* provides information about the terms used in this document.

# 2

# RACADM Subcommand Details

This section provides detailed descriptions of the RACADM subcommands including the syntax and valid entries.

**CAUTION: The latest iDRAC6 1.5 and 3.0 firmware releases supports only the latest RACADM version. You may encounter errors if you use an older version of RACADM to query iDRAC6 with the latest firmware. Install the RACADM version shipped with the *Dell Systems Management Tools and Documentation* DVD Version 6.3.**

## help

**NOTE:** To use this subcommand, you must have **Login to iDRAC** permission.

| Subcommand | Definition |
|---|---|
| help | Lists all the subcommands available to use with RACADM and provides a short description for each. |

### Synopsis

```
racadm help
racadm help <subcommand>
```

### Description

The **help** subcommand lists all the subcommands that are available when using the **racadm** command along with a one-line description. You may also type a subcommand after **help** to get the syntax for a specific subcommand.

### Output

The **racadm help** command displays a complete list of subcommands.

The **racadm help** <*subcommand*> command displays information for the specified subcommand only.

# arp

**NOTE:** To use this subcommand, you must have **Administrator** and **Execute Diagnostic Commands** permission.

| Subcommand | Definition |
|---|---|
| arp | Displays the contents of the Address Resolution Protocol (ARP) table. ARP table entries cannot be added or deleted. |

## Synopsis

```
racadm arp
```

## Example

| IP Address | HW Type | Flags | HW Address | Mask | Device |
|---|---|---|---|---|---|
| 192.168.1.1 | 0x1 | 0x2 | 00:00:0C:07:AC:0F | * | eth0 |

# clearasrscreen

**NOTE:** To use this subcommand, you must have **Clear Logs** permission.

| Subcommand | Definition |
|---|---|
| clearasrscreen | Clears the last crash (ASR) screen that is in memory. See *Configuring the Managed Server to Capture the Last Crash Screen* and *Disabling the Windows Automatic Reboot Option* sections in the *iDRAC6 Enterprise for Blade Servers User Guide*. |

## Synopsis

```
racadm clearasrscreen
```

# closessn

**NOTE:** To use this subcommand, you must have **Administrator** permission.

| Subcommand | Definition |
|---|---|
| **closessn** | Closes a communication session on the device. Use **getssninfo** to view a list of sessions that can be closed using this command. |

## Synopsis

```
racadm closessn –i <session id>

racadm closessn -a

racadm closessn -u <username>
```

## Options

Table 2-1 describes the **closessn** subcommand options.

**Table 2-1. closessn Subcommand Options and Descriptions**

| Option | Description |
|---|---|
| **-i<session id>** | The session ID of the session to close, which can be retrieved using racadm **getssninfo** subcommand.<br>**NOTE:** Session executing this command cannot be closed. |
| **-a** | Closes all sessions. |
| **-u <user name>** | Close all sessions for a particular user name.<br>**NOTE:** -u option can be used in local RACADM only if the username contains upto 16 characters.<br>If the user name contains more than 16 characters, use one of the following options to close a session:<br>Local RACADM: -i option<br>Remote RACADM: -u option or -i option |

### Examples:

- `racadm closessn -i 1234`
  Closes the session 1234.
- `racadm closessn –u root`
  Closes all the sessions for root user.
- `racadm closessn –a`
  Closes all the sessions.

## clrraclog

**NOTE:** To use this subcommand, you must have **Clear Logs** permission. .

| Subcommand | Definition |
|---|---|
| clrraclog | Removes all existing records from the iDRAC6 log. A new single record is created to record the date and time when the log was cleared. |

### Synopsis

```
racadm clrraclog
```

## clrsel

**NOTE:** To use this subcommand, you must have **Clear Logs** permission.

| Subcommand | Definition |
|---|---|
| clrsel | Removes all existing records from the System Event Log (SEL). |

### Synopsis

```
racadm clrsel
```

# config

**NOTE:** To use this subcommand, you must have **Log In iDRAC** permission.

| Subcommand | Definition |
|---|---|
| config | Configures the iDRAC6. |

## Synopsis

```
racadm config [-c|-p] -f <filename>
```

```
racadm config -g <groupName> -o <objectName> [-i
<index>] <Value>
```

## Description

The **config** subcommand allows you to set iDRAC6 configuration parameters individually or to batch them as part of a configuration file. If the data is different, that iDRAC6 object is written with the new value.

**NOTE:** The configuration file retrieved using remote racadm and local racadm are not interoperable. The configuration file retrieved using remote racadm shows the index property for some of the indexed groups as read-write, for example cfgSSADRoleGroupIndex. For the `config -f <file name>` command, use the configuration file retrieved from the same interface. For example, for local racadm `config -f <file name>`, use the file generated from the local racadm command `getconfig -f <file name>`.

## Input

Table 2-2 describes the **config** subcommand options.

**NOTE:** The **-f** and **-p** options are not supported for the serial/Telnet/ssh console.

**Table 2-2. config Subcommand Options and Descriptions**

| Option | Description |
|---|---|
| -f | The **-f *<filename>*** option causes **config** to read the contents of the file specified by *<filename>* and configure the iDRAC6. The file must contain data in the format specified in the section *Parsing Rules* in the *iDRAC6 User's Guide* available on the Dell Support website at **support.dell.com/manuals**. |

**Table 2-2. config Subcommand Options and Descriptions *(continued)***

| Option | Description |
|---|---|
| -p | The **-p**, or password option, directs **config** to delete the password entries contained in the config file **-f *<filename>*** after the configuration is complete. |
| -g | The **-g *<groupName>***, or group option, must be used with the **-o** option. The <*groupName*> specifies the group containing the object that is to be set. |
| -o | The **-o *<objectName> <Value>***, or object option, must be used with the **-g** option. This option specifies the object name that is written with the string <*value*>. |
| -i | The -i ***<index>***, or index option, is valid only for indexed groups and can be used to specify a unique group. The <*index*> is a decimal integer from 1 through n, where n can vary from 1 to maximum number of indexes a particular group supports. If **-i** <*index*> is not specified, a value of 1 is assumed for groups, which are tables that have multiple entries. The index is specified by the index value, not a *named* value. |
| -c | The **-c**, or check option, is used with the **config** subcommand and allows the user to parse the **.cfg** file to locate syntax errors. If errors are found, the line number and a short description of what is incorrect are displayed. Writes do not occur to the iDRAC6. This option is a check only. |

## Output

This subcommand generates error output for any of the following reasons:

- Invalid syntax, group name, object name, index, or other invalid database members
- RACADM CLI failures

This subcommand returns an indication of the number of configuration objects that were written out of the total objects in the **.cfg** file.

### Examples

- `racadm config -g cfgLanNetworking -o cfgNicIpAddress 10.35.10.100`

  Sets the **cfgNicIpAddress** configuration parameter (object) to the value 10.35.10.110. This IP address object is contained in the group **cfgLanNetworking**.

- `racadm config -f myrac.cfg`

  Configures or reconfigures the iDRAC6. The **myrac.cfg** file may be created from the **getconfig** command. The **myrac.cfg** file may also be edited manually as long as the parsing rules are followed.

  **NOTE:** The **myrac.cfg** file does not contain passwords. To include passwords in the file, you must enter them manually. If you want to remove password information from the **myrac.cfg** file during configuration, use the **-p** option.

# coredump

**NOTE:** To use this subcommand, you must have **Execute Debug Commands** permission.

| Subcommand | Definition |
|---|---|
| **coredump** | Displays the last iDRAC6 core dump. |

### Synopsis

```
racadm coredump
```

### Description

The **coredump** subcommand displays detailed information related to any recent critical issues that have occurred with the RAC. The coredump information can be used to diagnose these critical issues.

If available, the coredump information is persistent across iDRAC6 power cycles and remains available until either of the following conditions occur:

- The coredump information is cleared with the **coredumpdelete** subcommand.
- Another critical condition occurs on the RAC. In this case, the coredump information is relative to the last critical error that occurred.

See the **coredumpdelete** subcommand for more information about clearing the **coredump**.

# coredumpdelete

**NOTE:** To use this subcommand, you must have **Clear Logs** or **Execute Debug Commands** permission.

| Subcommand | Definition |
|---|---|
| **coredumpdelete** | Deletes the core dump stored in the iDRAC6. |

## Synopsis

```
racadm coredumpdelete
```

## Description

The **coredumpdelete** subcommand can be used to clear any currently resident **coredump** data stored in the RAC.

**NOTE:** If a **coredumpdelete** command is issued and a coredump is not currently stored in the RAC, the command displays a success message. This behavior is expected.

See the **coredump** subcommand for more information on viewing a coredump.

# fwupdate

**NOTE:** To use this subcommand, you must have **Configure iDRAC6** permission.

Before you begin your firmware update, see the *Advanced iDRAC6 Configuration* section in the *iDRAC6 User's Guide* available on the Dell Support website at **support.dell.com/manuals**.

| Subcommand | Definition |
|---|---|
| **fwupdate** | Updates the firmware on the iDRAC6 |

## Synopsis

```
racadm fwupdate -s

racadm fwupdate -g -u -a <TFTP_Server_IP_Address> [-d <path>]

racadm fwupdate -r

racadm fwupdate -p -u [-d <path>]
```

## Description

The **fwupdate** subcommand allows users to update the firmware on the iDRAC6. You can:

- Check the firmware update process status
- Update the iDRAC6 firmware from a TFTP server by providing an IP address and optional path
- Update the iDRAC6 firmware from the local file system using local RACADM
- Rollback to the standby firmware

## Input

Table 2-3 describes the **fwupdate** subcommand options.

**NOTE:** The **-p** option is supported on local and remote RACADM and is not supported with the serial/Telnet/ssh console. The **-p** option is also not supported on Linux Operating Systems.

**Table 2-3. fwupdate Subcommand Options**

| Option | Description |
|---|---|
| **-u** | The **update** option performs a checksum of the firmware update file and starts the actual update process. This option may be used along with the **-g** or **-p** options. At the end of the update, the iDRAC6 performs a soft reset. |
| **-s** | The **status** option returns the current status of where you are in the update process. This option is always used by itself. |
| **-g** | The **get** option instructs the firmware to get the firmware update file from the TFTP server. You must also specify the **-a**, **-u**, and **-d** options. In the absence of the **-a** option, the defaults are read from properties contained in the group **cfgRemoteHosts**, using properties **cfgRhostsFwUpdateIpAddr** and **cfgRhostsFwUpdatePath**. |
| **-a** | The **IP Address** option specifies the TFTP server IP address, used with **-g** option. |
| **-d** | The **-d,** or **directory**, option specifies the directory on the TFTP server or on the iDRAC6's host server where the firmware update file resides. |
| **-p** | The **-p**, or **put**, option is used to update the firmware file from the managed system to the iDRAC6. The **-u** option must be used with the **-p** option. |
| **-r** | The **rollback** option is used to rollback to the standby firmware. |

## Output

Displays a message indicating the operation that is being performed.

### Examples

- `racadm fwupdate -g -u - a 143.166.154.143 -d <path>`

  In this example, the **-g** option tells the firmware to download the firmware update file from a location (specified by the **-d** option) on the TFTP server at a specific IP address (specified by the **-a** option). After the image file is downloaded from the TFTP server, the update process begins. When completed, iDRAC6 is reset.

- `racadm fwupdate -s`

  This option reads the current status of the firmware update.

**NOTE:** Remote RACADM firmware update through the local path is not supported on Linux Operating Systems.

# getconfig

| Subcommand | Definition |
|---|---|
| getconfig | Retrieves iDRAC6 configuration parameters individually, or all the iDRAC6 configuration groups may be retrieved and saved to a file. |

### Synopsis

```
racadm getconfig -f <filename>

racadm getconfig -g <groupName> [-i <index>]

racadm getconfig -u <username>

racadm getconfig -h

racadm getconfig -g <groupName> -o <objectName> [-i
index]
```

## Input

Table 2-4 describes the **getconfig** subcommand options.

**Table 2-4. getconfig Subcommand Options**

| Option | Description |
|---|---|
| **-f** | The -f <*filename*> option directs getconfig to write the entire iDRAC6 configuration to a configuration file. This file can be used for batch configuration operations using the **config** subcommand. |
| **-g** | The -g <*groupName*>, or group option, can be used to display the configuration for a single group. The **groupName** is the name for the group used in the **racadm.cfg** files. If the group is an indexed group, use the **-i** option. |
| **-h** | The **-h**, or **help** option, displays a list of all available configuration groups in alphabetical order. This option is useful when you do not remember exact group names. |
| **-i** | The -i <*index*>, or index option, is valid only for indexed groups and can be used to specify a unique group. The <*index*> is a decimal integer from 1 through n, where n can vary from 1 to maximum number of indexes a particular group supports. If **-i** <*index*> is not specified, a value of 1 is assumed for groups, which are tables that have multiple entries. The index is specified by the index value, not a *named* value. |
| **-o** | The -o <*objectname*> or object option specifies the object name that is used in the query. This option is optional and can be used with the -g option. |
| **-u** | The -u <*username*>, or user n**ame** option, can be used to display the configuration for the specified user. The <*username*> option is the login name for the user. |
| **-v** | The **-v** option displays additional details with the display of the properties and is used with the **-g** option. |

## Output

This subcommand generates error output upon encountering either of the following:

- Invalid syntax, group name, object name, index, or other invalid database members
- RACADM CLI transport failures

If errors are not encountered, this subcommand displays the contents of the specified configuration.

### Examples

- `racadm getconfig -g cfgLanNetworking`

  Displays all of the configuration properties (objects) that are contained in the group **cfgLanNetworking**.

- `racadm getconfig -f myrac.cfg`

  Saves all group configuration objects from the iDRAC6 to **myrac.cfg**.

- `racadm getconfig -h`

  Displays a list of the available configuration groups on the iDRAC6 in an alphabetical order.

- `racadm getconfig -u root`

  Displays the configuration properties for the user named root.

- `racadm getconfig -g cfgUserAdmin -i 2 -v`

  Displays the user group instance at index 2 with verbose information for the property values.

## getniccfg

**NOTE:** To use this subcommand, you must have **Login to iDRAC** permission.

| Subcommand | Definition |
|---|---|
| **getniccfg** | Displays the current IP configuration for iDRAC6. |

### Synopsis

`racadm getniccfg`

### Description

The **getniccfg** subcommand displays the current NIC settings.

### Sample Output

The **getniccfg** subcommand displays an appropriate error message if the operation is not successful. Otherwise, on success, the output is displayed in the following format:

```
IPv4 settings:
NIC Enabled     = 1
IPv4 Enabled = 1
DHCP Enabled    = 1
IP Address      = 10.35.0.64
Subnet Mask     = 255.255.255.0
Gateway         = 10.35.0.1
IPv6 settings:
IPv6 Enabled       = 0
DHCP6 Enabled      = 1
IP Address 1       = ::
Gateway            = ::
Link Local Address = ::
IP Address 2       = ::
IP Address 3       = ::
IP Address 4       = ::
IP Address 5       = ::
IP Address 6       = ::
IP Address 7       = ::
IP Address 8       = ::
IP Address 9       = ::
IP Address 10      = ::
IP Address 11      = ::
IP Address 12      = ::
IP Address 13      = ::
IP Address 14      = ::
```

```
IP Address 15      = ::
LOM Status:
NIC Selection   = Dedicated
Link Detected   = Yes
Speed           = 10Mb/s
Duplex Mode     = Half Duplex
```

**NOTE:** IPv6 information is displayed only if IPv6 is enabled in iDRAC6.

**NOTE:** LOM Status is displayed only for iDRAC6 on Rack and Tower servers and is not displayed for iDRAC6 Enterprise on Blade servers.

# getraclog

**NOTE:** To use this subcommand, you must have **Login to iDRAC** permission.

| Command | Definition |
|---|---|
| **getraclog -i** | Displays the number of entries in the iDRAC6 log. |
| **getraclog** | Displays the iDRAC6 log entries. |

## Synopsis

```
racadm getraclog -i
racadm getraclog [-A] [-o] [-c count] [-s start-record] [--more]
```

## Description

The **getraclog -i** command displays the number of entries in the iDRAC6 log.

Table 2-5 lists the options that allow the **getraclog** command to read entries.

**Table 2-5. getraclog Subcommand Options**

| Option | Description |
|---|---|
| **-A** | Displays the output with no headers or labels. |
| **-c** | Provides the maximum count of entries to be returned. |

**Table 2-5. getraclog Subcommand Options *(continued)***

| Option | Description |
|---|---|
| **--more** | Displays one screen at a time and prompts the user to continue (similar to the UNIX **more** command). |
| **-o** | Displays the output in a single line. |
| **-s** | Specifies the starting record used for the display. |

**NOTE:** If no options are provided, the entire log is displayed.

### Output

The default output display shows the record number, time stamp, source, and description. The timestamp begins at midnight, January 1 and increases until the system boots. After the system boots, the system's timestamp is used.

**NOTE:** For iDRAC6 Enterprise on Blade Servers, the iDRAC6 Log entries for *SystemBoot* displayed using the local racadm command `racadm getraclog` may not be correctly formatted. For example, some extra characters may be displayed in the **Description** field, or the **Source** field may be empty.

### Sample Output

```
Record:       1
Date/Time:    Dec  8 08:10:11
Source:       login[433]
Description:  root login from 143.166.157.103
```

## getractime

**NOTE:** To use this subcommand, you must have **Login to iDRAC** permission.

| Subcommand | Definition |
|---|---|
| **getractime** | Displays the current time from the remote access controller. |

### Synopsis

```
racadm getractime [-d]
```

### Description

With no options, the **getractime** subcommand displays the time in a common readable format.

With the **-d** option, **getractime** displays the time in the format, *yyyymmddhhmmss.mmmmmm*, which is the same format returned by the UNIX **date** command.

### Output

The **getractime** subcommand displays the output on one line.

### Sample Output

```
racadm getractime
Thu Dec  8 20:15:26 2005

racadm getractime -d
20051208201542.000000
```

## getsel

**NOTE:** To use this subcommand, you must have **Login to iDRAC** permission.

| Command | Definition |
|---|---|
| **getsel -i** | Displays the number of entries in the System Event Log. |
| **getsel** | Displays all the SEL entries. |

### Synopsis

```
racadm getsel -i[-A]

racadm getsel [-s <start>] [-c <count>] [-A] [-o] [-E]
[-R] [--more]
```

### Description

The **getsel -i** command displays the number of entries in the SEL.

The following **getsel** options (without the **-i** option) are used to read entries.

**NOTE:** If no arguments are specified, the entire log is displayed.

**Table 2-6. getsel Subcommand Options**

| Option | Description |
|---|---|
| **-A** | Specifies output with no display headers or labels. |
| **-c** | Provides the number of records to be displayed. |
| **-o** | Displays each entry in the SEL in a single line. |
| **-s** | Specifies the starting record used for the display. |
| **-E** | Displays RAW SEL data with the other data for each entry. |
| **-R** | Displays only RAW SEL data for each entry. |
| **-i** | Displays the number of entries in the SEL. |
| **--more** | Displays one screen at a time and prompts the user to continue (similar to the UNIX **more** command). |

## Output

The default output display shows the record number, timestamp, severity, and description.

For example:

```
Record:      1
Date/Time:   11/16/2005 22:40:43
Severity:    Ok
Description: System Board SEL: event log sensor for
System Board, log cleared was asserted
```

# getssninfo

**NOTE:** To use this subcommand, you must have **Login to iDRAC** permission.

| Subcommand | Definition |
|---|---|
| **getssninfo** | Retrieves session information for one or more currently active or pending sessions from the Session Manager's session table. |

## Synopsis

```
racadm getssninfo [-A] [-u <username> | *]
```

## Description

The **getssninfo** subcommand returns a list of users that are connected to the iDRAC6. The following information is displayed:

- Session ID
- Username
- IP address (if applicable)
- Session type (for example, serial or Telnet)
- Login date and time in MM/DD/YYYY HH:MM:SS format

Based on the Session ID (SSNID) or the user name (User), the iDRAC administrator can close the respective sessions or all the sessions using the , **closessn** subcommand. See "closessn" on page 25 for more information.

## Input

Table 2-7 describes the **getssninfo** subcommand options.

**Table 2-7. getssninfo Subcommand Options**

| Option | Description |
|---|---|
| **-A** | The **-A** option eliminates the printing of data headers. |
| **-u** | The **-u <***username***>** user name option limits the printed output to only the detail session records for the given user name. If an (*) symbol is given as the user name, all users are listed. Summary information is not printed when this option is specified. |

### Examples

- `racadm getssninfo`

The following table provides an example of output from the **getssninfo** command.

| SSNID | Type | User | IP Address | Login Date/Time |
|---|---|---|---|---|
| 6 | GUI | root | 192.168.0.10 | 04/07/2010 12:00:34 |

- `racadm getssninfo -A`

  `"root" "143.166.174.19" "Telnet" "NONE"`

- `racadm getssninfo -A -u *`

  `"root" "143.166.174.19" "Telnet" "NONE"`

  `"bob" "143.166.174.19" "GUI" "NONE"`

## getsvctag

**NOTE:** To use this subcommand, you must have **Login to iDRAC** permission.

| Subcommand | Definition |
|---|---|
| **getsvctag** | Displays a service tag. |

### Synopsis

`racadm getsvctag`

### Description

The **getsvctag** subcommand displays the service tag of the host system.

### Example

Type `getsvctag` at the command prompt. The output is displayed as follows:

```
Y76TP0G
```

# getsysinfo

**NOTE:** To use this subcommand, you must have **Login to iDRAC** permission.

| Command | Definition |
|---|---|
| **getsysinfo** | Displays iDRAC6 information, system information, and watchdog status information. |

## Synopsis

```
racadm getsysinfo [-d] [-s] [-w] [-A] [-c] [-4] [-6]
```

## Description

The **getsysinfo** subcommand displays information related to the iDRAC, managed system, and watchdog configuration.

**NOTE:** The local racadm *getsysinfo* subcommand on Linux displays the *PrefixLength* on separate lines for IPv6 Address 2 – IPv6 Address 15 and the Link Local Address.

## Input

Table 2-8 describes the **getsysinfo** subcommand options.

**Table 2-8. getsysinfo Subcommand Options**

| Option | Description |
|---|---|
| **-4** | Displays IPv4 settings |
| **-6** | Displays IPv6 settings |
| **-c** | Displays common settings |
| **-d** | Displays iDRAC6 information |
| **-s** | Displays system information |
| **-w** | Displays watchdog information |
| **-A** | Eliminates the printing of headers/labels |

If the **-w** option is not specified, then the other options are used as defaults.

### Output

The **getsysinfo** subcommand displays information related to the RAC, managed system, and watchdog configuration.

### Sample Output

```
RAC Information:
RAC Date/Time           = 10/27/2009 14:38:00
Firmware Version        = 1.30
Firmware Build          = 20
Last Firmware Update    = 10/26/2009 16:55:08
Hardware Version        = 0.01
MAC Address             = 00:24:e8:2e:c5:d3

Common settings:
Register DNS RAC Name   = 1
DNS RAC Name            = eval710-08-r
Current DNS Domain      = blr.amer.dell.com
Domain Name from DHCP   = 1

IPv4 settings:
Enabled                 = 1
Current IP Address      = 10.94.20.134
Current IP Gateway      = 10.94.20.1
Current IP Netmask      = 255.255.254.0
DHCP Enabled            = 1
Current DNS Server 1    = 163.244.180.39
Current DNS Server 2    = 163.244.180.40
DNS Servers from DHCP   = 1

IPv6 settings:
```

```
Enabled                 = 1
Current IP Address 1    = ::
Current IP Gateway      = ::
Autoconfig              = 1
Link Local IP Address   = fe80::224:e8ff:fe2e:c5d3/255
Current IP Address 2    = ::
Current IP Address 3    = ::
Current IP Address 4    = ::
Current IP Address 5    = ::
Current IP Address 6    = ::
Current IP Address 7    = ::
Current IP Address 8    = ::
Current IP Address 9    = ::
Current IP Address 10   = ::
Current IP Address 11   = ::
Current IP Address 12   = ::
Current IP Address 13   = ::
Current IP Address 14   = ::
Current IP Address 15   = ::
DNS Servers from DHCPv6 = 0
Current DNS Server 1    = ::
Current DNS Server 2    = ::

System Information:
System Model            = PowerEdge R710
System BIOS Version     = 1.0.4
Service Tag             = 2X2Q12S
Host Name               = WIN-IHF5D2BF5SN
OS Name                 =
```

```
Power Status            = ON

Embedded NIC MAC Addresses:
NIC1 Ethernet           = 00:24:e8:2e:c5:cb
     iSCSI              = 00:24:e8:2e:c5:cc
NIC2 Ethernet           = 00:24:e8:2e:c5:cd
     iSCSI              = 00:24:e8:2e:c5:ce
NIC3 Ethernet           = 00:24:e8:2e:c5:cf
     iSCSI              = 00:24:e8:2e:c5:d0
NIC4 Ethernet           = 00:24:e8:2e:c5:d1
     iSCSI              = 00:24:e8:2e:c5:d2

Watchdog Information:
Recovery Action         = None
Present countdown value = 15 seconds
Initial countdown value = 15 seconds
```

## Examples

- `racadm getsysinfo -A -s`

  ```
  "System Information:" "PowerEdge 2900" "A08" "1.0"
  "EF23VQ-0023" "Hostname"

  "Microsoft Windows 2000 version 5.0, Build Number
  2195, Service Pack 2" "ON"
  ```

- `racadm getsysinfo -w -s`

  ```
  System Information:
  System Model              = PowerEdge 2900
  System Revision           = I
  System BIOS Version       = 0.2.3
  BMC Firmware Version      = 0.17
  Service Tag               = 48192
  Host Name                 = racdev103
  OS Name                   = Microsoft Windows
  ```

```
Server 2003
Power Status            = OFF

Watchdog Information:
Recovery Action          = None
Present countdown value  = 0 seconds
Initial countdown value = 0 seconds
```

### Limitations

The Hostname and OS Name fields in the **getsysinfo** output display accurate information only if Dell OpenManage Server Administrator is installed on the managed system. If it is not installed, these fields may be blank or inaccurate. An exception to this are VMware operating system names, which are displayed even if Server Administrator is not installed on the managed system.

## gettracelog

**NOTE:** To use this subcommand, you must have **Login to iDRAC** permission.

| Command | Definition |
|---|---|
| **gettracelog -i** | Displays the number of entries in the iDRAC6 trace log. |
| **gettracelog** | Displays the iDRAC6 trace log. |

### Synopsis

```
racadm gettracelog -i[-A]

racadm gettracelog [-s <start>] [-c <count>] [--more]
[-A] [-o]
```

### Description

The **gettracelog** (without the **-i** option) command reads entries.
The following **gettracelog** entries are used to read entries:

**Table 2-9. gettracelog Subcommand options**

| Option | Description |
|---|---|
| **-i** | Displays the number of entries in **iDRAC6 trace log**. |
| **--more** | Displays one screen at a time and prompts the user to continue (similar to the UNIX **more** command). |
| **-o** | Displays each entry in a single line. |
| **-c** | Specifies the number of records to display. |
| **-s** | Specifies the starting record to display. |
| **-A** | Do not display headers or labels. |

### Output

The default output display shows the record number, timestamp, source, and description. The timestamp begins at midnight, January 1 and increases until the system boots. After the system boots, the system's timestamp is used.

For example:

```
Record:      1
Date/Time:   Dec  8 08:21:30
Source:      ssnmgrd[175]
Description: root from 143.166.157.103: session
timeout sid 0be0aef4
```

# ifconfig

**NOTE:** To use this subcommand, you must have **Execute Diagnostic Commands** or **Configure iDRAC** permission.

| Subcommand | Definition |
|---|---|
| ifconfig | Displays the contents of the network interface table. |

### Synopsis

```
racadm ifconfig
```

### Example

```
$ racadm ifconfig

eth0     Link encap:Ethernet  HWaddr 00:1D:09:FF:DA:23

         inet addr:10.35.155.136  Bcast:10.35.155.255
Mask:255.255.255.0

          UP BROADCAST RUNNING MULTICAST  MTU:1500
Metric:1

          RX packets:2550665 errors:0 dropped:0
overruns:0 frame:0

          TX packets:0 errors:0 dropped:0 overruns:0
carrier:0

          collisions:0 txqueuelen:1000

          RX bytes:272532097 (259.9 MiB)  TX bytes:0
(0.0 B)
```

# krbkeytabupload

**NOTE:** To use this subcommand, you must have **Configure iDRAC** permission.

| Subcommand | Description |
|---|---|
| **krbkeytabupload** | Uploads a Kerberos keytab file. |

### Synopsis

```
racadm krbkeytabupload [-f <filename>]
```

<*filename*> is the name of the file including the path.

### Options

Table 2-10 describes the **krbkeytabupload** subcommand options.

**Table 2-10. kerbkeytabupload Subcommand Options**

| Option | Description |
|---|---|
| -f | Specifies the file name of the keytab to be uploaded. If the file is not specified, the keytab file in the current directory is selected. |

The **krbkeytabupload** command returns `0` when successful and returns a non–zero number when unsuccessful.

### Example

```
racadm krbkeytabupload -f c:\keytab\krbkeytab.tab
```

## localConRedirDisable

**NOTE:** Only a local RACADM user can execute this command.

| Subcommand | Description |
|---|---|
| localConRedirDisable | Disables Virtual Console to the management station. |

### Synopsis

```
racadm localConRedirDisable <option>
```

If *<option>* is set to 1, Virtual Console is disabled.

If *<option>* is set to 0, Virtual Console is enabled.

## netstat

**NOTE:** To use this subcommand, you must have **Execute Diagnostic Commands** permission.

| Subcommand | Definition |
|---|---|
| **netstat** | Displays the routing table and the current connections. |

### Synopsis

```
racadm netstat
```

# ping

**NOTE:** To use this subcommand, you must have **Execute Diagnostic Commands** or **Configure iDRAC** permission.

| Subcommand | Definition |
|---|---|
| ping | Verifies that the destination IP address is reachable from the iDRAC6 with the current routing-table contents. A destination IP address is required. An ICMP echo packet is sent to the destination IP address based on the current routing-table contents. |

## Synopsis

```
racadm ping <ipaddress>
```

# ping6

**NOTE:** To use this subcommand, you must have **Execute Diagnostic Commands** or **Configure iDRAC6** permission.

| Subcommand | Definition |
|---|---|
| ping6 | Verifies that the destination IPv6 address is reachable from iDRAC6 with the current routing-table contents. A destination IPv6 address is required. An ICMP echo packet is sent to the destination IPv6 address based on the current routing-table contents. |

## Synopsis

```
racadm ping6 <ipv6address>
```

# racdump

**NOTE:** To use this subcommand, you must have **Debug** permission.

| Subcommand | Definition |
|---|---|
| racdump | Displays status and general iDRAC6 information. |

## Synopsis

```
racadm racdump
```

## Description

The **racdump** subcommand provides a single command to get dump, status, and general iDRAC6 board information.

The following information is displayed when the **racdump** subcommand is processed:

- General system/RAC information
- Coredump
- Session information
- Process information
- Firmware build information

# racreset

**NOTE:** To use this subcommand, you must have **Configure iDRAC** permission.

| Subcommand | Definition |
|---|---|
| racreset | Resets iDRAC6. |

**NOTE:** When you issue a racreset subcommand, iDRAC6 may require up to two minutes to return to a usable state.

## Synopsis

```
racadm racreset [hard | soft]
```

### Description

The **racreset** subcommand issues a reset to the iDRAC6. The reset event is written into the iDRAC6 log.

**NOTE:** You must reboot your system after performing a hard reset of the iDRAC6 as described in Table 2-11.

Table 2-11 describes the **racreset** subcommand options.

**Table 2-11. racreset Subcommand Options**

| Option | Description |
|---|---|
| **hard** | A *hard* reset performs a deep reset operation on the remote access controller. A hard reset should only be used as a last case resort of resetting the iDRAC6 controller for recovery purposes. |
| **soft** | A *soft* reset performs a graceful reboot operation on the RAC. |

### Examples

- `racadm racreset`

  Start the iDRAC6 soft reset sequence.

- `racadm racreset hard`

  Start the iDRAC6 hard reset sequence.

## racresetcfg

**NOTE:** To use this subcommand, you must have **Configure iDRAC** permission.

| Subcommand | Definition |
|---|---|
| racresetcfg | Resets the entire iDRAC6 configuration to factory default values.<br>**NOTE:** The **racresetcfg** subcommand does not reset the **cfgDNSRacName** object. |

### Synopsis

```
racadm racresetcfg
```

### Description

The **racresetcfg** command removes all user-configured database property entries. The database has default properties for all entries that are used to restore iDRAC6 to the default settings. After resetting the database properties, the iDRAC6 resets automatically.

**NOTE:** This command deletes your current iDRAC6 configuration and resets the iDRAC6 and serial configuration to the default settings. After reset, the default name and password is **root** and **calvin**, respectively, and the IP address is 192.168.0.120. Only for iDRAC6 Enterprise on Blade servers, it is IP address plus the number of the slot the server inhabits in the chassis. If you issue **racresetcfg** from a network client (for example, a supported Web browser, Telnet/ssh, or remote RACADM), you must use the default IP address.

**NOTE:** Certain iDRAC6 firmware processes need to be stopped and restarted for reset to defaults to complete. iDRAC6 becomes unresponsive for about 30 seconds while this operation completes.

## remoteimage

**NOTE:** To use this subcommand, you must have **Administrator** permission.

| Subcommand | Definition |
|---|---|
| remoteimage | Connects, disconnects, or deploys a media file on a remote server. |

### Synopsis

```
racadm remoteimage <options>
```

### Description

Connects, disconnects, or deploys a media file on a remote server.

Table 2-12 describes the **remoteimage** subcommand options.

**Table 2-12. remoteimage Subcommand Options and Descriptions**

| Option | Description |
|---|---|
| **-c** | Connect the image. |
| **-d** | Disconnect image. |
| **-u** | Username to access the network share. |
| **-p** | Password to access the network share. |
| **-l** | Image location on the network share; use double quotes around the location. |
| **-s** | Display current status; –a is assumed if not specified |

# serveraction

**NOTE:** To use this subcommand, you must have **Execute Server Control Commands** permission.

| Subcommand | Definition |
|---|---|
| **serveraction** | Executes a managed system reset or power-on/off/cycle. |

## Synopsis

```
racadm serveraction <action>
```

## Description

The serveraction subcommand enables users to perform power management operations on the host system. Table 2-13 describes the **serveraction** power control options.

**Table 2-13. serveraction Subcommand Options**

| String | Definition |
|---|---|
| <*action*> | Specifies the action. The options for the <*action*> string are:<br>• **powerdown** — Powers down the managed system.<br>• **powerup** — Powers up the managed system.<br>• **powercycle** — Issues a power-cycle operation on the managed system. This action is similar to pressing the power button on the system's front panel to power down and then power up the system.<br>• **powerstatus** — Displays the current power status of the server (ON or OFF)<br>• **hardreset** — Performs a reset (reboot) operation on the managed system. |

### Output

The **serveraction** subcommand displays an error message if the requested operation could not be performed, or a success message if the operation completed successfully.

## setniccfg

**NOTE:** To use the **setniccfg** command, you must have **Configure iDRAC** permission.

| Subcommand | Definition |
|---|---|
| setniccfg | Sets the IP configuration for iDRAC6. |

**NOTE:** The terms NIC and Ethernet management port may be used interchangeably.

### Synopsis

```
racadm setniccfg -d

racadm setniccfg -d6

racadm setniccfg -s <IPv4Address> <netmask> <IPv4
gateway>
```

```
racadm setniccfg -s6 <IPv6 Address> <IPv6 Prefix
Length> <IPv6 Gateway>

racadm setniccfg -o
```

### Description

The **setniccfg** subcommand sets the iDRAC6 IP address.

- The **-d** option enables DHCP for the NIC (default is DHCP disabled).
- The **-d6** option enables AutoConfig for the NIC. It is enabled by default.
- The **-s** option enables static IP settings. The IPv4 address, netmask, and gateway can be specified. Otherwise, the existing static settings are used. <*IPv4Address*>, <*netmask*>, and <*gateway*> must be typed as dot-separated strings.

  ```
  racadm setniccfg -s 192.168.0.120 255.255.255.0
  192.168.0.1
  ```

- The **-s6** option enables static IPv6 settings. The IPv6 address, Prefix Length, and the IPv6 Gateway can be specified.
- The **-o** option disables the NIC completely.

### Output

The **setniccfg** subcommand displays an appropriate error message if the operation is not successful. If successful, a message is displayed.

## sshpkauth

| Subcommand | Definition |
|---|---|
| **sshpkauth** | Allows you to upload and manage up to four different SSH public keys per user. You can upload a key file or key text, view keys, or delete keys. |

### Synopsis

```
racadm sshpkauth
```

### Upload

The upload mode allows you to upload a keyfile or to copy the key text on the command line. You cannot upload and copy a key at the same time.

*Local* and *Remote* RACADM:

```
racadm sshpkauth -i <2 to 16> -k <1 to 4> -f
<filename>
racadm sshpkauth -i <2 to 16> -k <1 to 4> -t
<key-text>
```

*Telnet/ssh/serial* RACADM:

```
racadm sshpkauth -i <2 to 16> -k <1 to 4> -t
<key-text>
```

### View

The view mode allows the user to view a key specified by the user or all keys.

```
racadm sshpkauth -i <2 to 16> -v -k <1 to 4>
racadm sshpkauth -i <2 to 16> -v -k all
```

### Delete

The delete mode allows the user to delete a key specified by the user or all keys.

```
racadm sshpkauth -i <2 to 16> -d -k <1 to 4>
racadm sshpkauth -i <2 to 16> -d -k all
```

## Description

Enables you to upload and manage up to 4 different SSH public keys *per user*. You can upload a key file or key text, view keys, or delete keys. This command has three mutually exclusive modes—upload, view, and delete that are determined by the options (see Table 2-14) provided to the command.

## Options

**Table 2-14. sshpkauth Subcommand Options**

| Option | Description |
|---|---|
| **-i <user index>** | Index for the user. <user index> must be between 2 to 16 on iDRAC6. |
| **-k [<key index> \| all]** | Index to assign the PK key being uploaded. **all** only works with the -v or -d options. <key index> must be between 1 to 4 or **all** on iDRAC6. |
| **-t <PK Key Text>** | Key text for the SSH Public key. |
| **-f <filename>** | File containing the key text to upload. The **-f** option is not supported on Telnet/ssh/serial RACADM. |
| **-v** | View the key text for the index provided. |
| **-d** | Delete the key for the index provided. |

## Examples

**Upload an invalid key to iDRAC6 User 2 in the first key space using a string:**

```
$ racadm sshpkauth -i 2 -k 1 -t "This is invalid key
Text"

ERROR: Key text appears to be corrupt
```

**Upload a valid key to iDRAC6 User 2 in the first key space using a file:**

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

Key file successfully uploaded.
```

**Get all keys for User 2 on iDRAC6:**

```
$ racadm sshpkauth -v -i 2 -k all

******************** User ID 2 *****************

Key ID 1:

ssh-rsa
AAAAB3NzaC1yc2EAAAABIwAAAIEAzzy+k2npnKqVEXGXIzo0sbR6J
gA5YNbWs3ekoxXV
fe3yJVpVc/5zrrr7XrwKbJAJTqSw8Dg3iR4n3vUaP+lPHmUv5Mn55
Ea6LHUslAXFqXmOdlThd
```

```
wilU2VLw/iRH1ZymUFnut8ggbPQgqV2L8bsUaMqb5PooIIvV6hy4i
sCNJU= 1024-bit RSA, converted from OpenSSH by
xx_xx@xx.xx
Key ID 2:

Key ID 3:

Key ID 4:
```

# sslcertdownload

**NOTE:** To use this subcommand, you must have **Configure iDRAC** permission.

| Subcommand | Description |
|---|---|
| **sslcertupload** | Downloads an SSL certificate from iDRAC6 to the client's file system. |

## Synopsis

```
racadm sslcertdownload -t <type> [-f <filename>]
```

## Options

Table 2-15 describes the **sslcertdownload** subcommand options.

**Table 2-15. sslcertdownload Subcommand Options**

| Option | Description |
|---|---|
| **-t** | Specifies the type of certificate to download, either the CA certificate for Directory Service or the server certificate.<br>1 = server certificate<br>2 = CA certificate for Directory Service |
| **-f** | Specifies the file name of the certificate to be uploaded. If the **-f** option or the filename is not specified, the **sslcert** file in the current directory is selected. |

The **sslcertdownload** command returns `0` when successful and returns a nonzero number when unsuccessful.

### Example

```
racadm sslcertdownload -t 1 -f c:\cert\cert.txt
```

## sslcertupload

**NOTE:** To use this subcommand, you must have **Configure iDRAC** permission.

| Subcommand | Description |
|---|---|
| **sslcertupload** | Uploads a custom SSL server or CA certificate for Directory Service from the client to the iDRAC6. |

### Synopsis

```
racadm sslcertupload -t <type> [-f <filename>]
```

### Options

Table 2-16 describes the **sslcertupload** subcommand options.

**Table 2-16. sslcertupload Subcommand Options**

| Option | Description |
|---|---|
| **-t** | Specifies the type of certificate to upload, either the CA certificate for Directory Service or the server certificate.<br>1 = server certificate<br>2 = CA certificate for Directory Service |
| **-f** | Specifies the file name of the certificate to be uploaded. If the file is not specified, the **sslcert** file in the current directory is selected. |

The **sslcertupload** command returns `0` when successful and returns a nonzero number when unsuccessful.

### Example

```
racadm sslcertupload -t 1 -f c:\cert\cert.txt
```

# sslcertview

**NOTE:** To use this subcommand, you must have **Configure iDRAC** permission.

| Subcommand | Description |
|---|---|
| sslcertview | Displays the SSL server or CA certificate that exists on the iDRAC6. |

## Synopsis

```
racadm sslcertview -t <type> [-A]
```

## Options

Table 2-17 describes the **sslcertview** subcommand options.

**Table 2-17. sslcertview Subcommand Options**

| Option | Description |
|---|---|
| **-t** | Specifies the type of certificate to view, either the CA certificate or server certificate.<br>1 = server certificate<br>2 = CA certificate for Directory Service |
| **-A** | Prevents printing headers/labels. |

## Sample Output

```
racadm sslcertview -t 1

Serial Number             : 00

Subject Information:
Country Code (CC)         : US
State (S)                 : Texas
Locality (L)              : Round Rock
Organization (O)          : Dell Inc.
```

```
Organizational Unit (OU)  : Remote Access Group
Common Name (CN)          : iDRAC6 default certificate

Issuer Information:
Country Code (CC)         : US
State (S)                 : Texas
Locality (L)              : Round Rock
Organization (O)          : Dell Inc.
Organizational Unit (OU)  : Remote Access Group
Common Name (CN)          : iDRAC6 default certificate

Valid From                : Jul  8 16:21:56 2005 GMT
Valid To                  : Jul  7 16:21:56 2010 GMT
```

```
racadm sslcertview -t 1 -A
```

```
00
US
Texas
Round Rock
Dell Inc.
Remote Access Group
iDRAC6 default certificate
US
Texas
Round Rock
Dell Inc.
Remote Access Group
iDRAC6 default certificate
Jul 8 16:21:56 2005 GMT
Jul 7 16:21:56 2010 GMT
```

# sslcsrgen

**NOTE:** To use this subcommand, you must have **Configure iDRAC** permission.

| Subcommand | Description |
|---|---|
| sslcsrgen | Generates and downloads an SSL Certificate Signing Request (CSR) from iDRAC6. |

## Synopsis

```
racadm sslcsrgen [-g] [-f <filename>]

racadm sslcsrgen -s
```

## Description

The **sslcsrgen** subcommand can be used to generate a CSR and download the file to the client's local file system. The CSR can be used for creating a custom SSL certificate that can be used for SSL transactions on iDRAC6.

## Options

Table 2-18 describes the **sslcsrgen** subcommand options.

**NOTE:** The **-f** option is not supported for the serial/Telnet/ssh console.

**Table 2-18. sslcsrgen Subcommand Options**

| Option | Description |
|---|---|
| -g | Generates a new CSR. |
| -s | Returns the status of a CSR generation process (generation in progress, active, or none). |
| -f | Specifies the filename of the location, <*filename*>, where the CSR will be downloaded. |

**NOTE:** If the **-f** option is not specified, the filename defaults to **sslcsr** in your current directory.

If no options are specified, a CSR is generated and downloaded to the local file system as **sslcsr** by default. The **-g** option cannot be used with the **-s** option, and the **-f** option can only be used with the **-g** option.

The **sslcsrgen -s** subcommand returns one of the following status codes:

- CSR was generated successfully.
- CSR does not exist.
- CSR generation in progress.

**NOTE:** Before a CSR can be generated, the CSR fields must be configured in the RACADM **cfgRacSecurity** group. For example:

```
racadm config -g cfgRacSecurity -o
cfgRacSecCsrCommonName MyCompany
```

**NOTE:** In telnet/ssh console, you can only generate and not download the CSR file

### Examples

```
racadm sslcsrgen -s
```

or

```
racadm sslcsrgen -g -f c:\csr\csrtest.txt
```

# sslkeyupload

**NOTE:** To use this subcommand, you must have **Configure iDRAC** permission.

| Subcommand | Description |
|---|---|
| sslkeyupload | Uploads SSL key from the client to the iDRAC6. |

## Synopsis

```
racadm sslkeyupload -t <type> -f <filename>
```

## Options

Table 2-19 describes the **sslkeyupload** subcommand options.

**Table 2-19. sslkeyupload Subcommand Options**

| Option | Description |
|---|---|
| -t | Specifies the key to upload.<br>1 = SSL key used to generate the server certificate |

**Table 2-19. sslkeyupload Subcommand Options**

| Option | Description |
|---|---|
| -f | Specifies the file name of the SSL key to be uploaded. |

The **sslkeyupload** command returns `0` when successful and returns a nonzero number when unsuccessful.

### Example

```
racadm sslkeyupload -t 1 -f c:\sslkey.txt
```

## testemail

| Subcommand | Description |
|---|---|
| testemail | Tests the RAC's e-mail alerting feature. |

### Synopsis

```
racadm testemail -i <index>
```

### Description

Sends a test e-mail from the iDRAC6 to a specified destination. Prior to executing the test e-mail command, ensure that the SMTP server is configured and the specified index in the RACADM **cfgEmailAlert** group is enabled and configured properly. See "cfgEmailAlert" on page 94 for more information.

Table 2-20 provides a list and associated commands for the **cfgEmailAlert** group.

**Table 2-20. testemail Configuration**

| Action | Command |
|---|---|
| Enable the alert | `racadm config -g cfgEmailAlert -o cfgEmailAlertEnable -i 1 1` |

**Table 2-20. testemail Configuration *(continued)***

| Action | Command |
|---|---|
| Set the destination e-mail address | `racadm config -g cfgEmailAlert -o cfgEmailAlertAddress -i 1 user1@mycompany.com` |
| Set the custom message that is sent to the destination e-mail address | `racadm config -g cfgEmailAlert -o cfgEmailAlertCustomMsg -i 1 "This is a test!"` |
| Ensure that the SMTP IP address is configured properly | `racadm config -g cfgRemoteHosts -o cfgRhostsSmtpServerIpAddr 192.168.0.152` |
| View the current e-mail alert settings | `racadm getconfig -g cfgEmailAlert -i <index>`<br>where *<index>* is a number from 1 to 4 |

### Options

Table 2-21 describes the **testemail** subcommand options.

**Table 2-21. testemail Subcommands**

| Option | Description |
|---|---|
| **-i** | Specifies the index of the e-mail alert to test. |

### Output

Success: Test e-mail sent successfully

Failure: Unable to send test e-mail

## testtrap

**NOTE:** To use this subcommand, you must have **Test Alerts** permission.

| Subcommand | Description |
|---|---|
| **testtrap** | Tests iDRAC6 SNMP trap alerting feature. |

## Synopsis

```
racadm testtrap -i <index>
```

## Description

The **testtrap** subcommand tests the RAC's SNMP trap alerting feature by sending a test trap from the iDRAC6 to a specified destination trap listener on the network.

Before you execute the **testtrap** subcommand, ensure that the specified index in the RACADM **cfgIpmiPet** group is configured properly. For more information, see "cfgIpmiPet" on page 130.

Table 2-22 provides a list and associated commands for the **cfgIpmiPet** group.

**Table 2-22. cfgEmailAlert Commands**

| Action | Command |
|---|---|
| Enable the alert | `racadm config -g cfgIpmiPet -o cfgIpmiPetAlertEnable -i 1 1` |
| Set the destination e-mail IP address | `racadm config -g cfgIpmiPet -o cfgIpmiPetAlertDestIpAddr -i 1 192.168.0.110` |
| View the current test trap settings | `racadm getconfig -g cfgIpmiPet -i <index>`<br>where *<index>* is a number from 1 to 4 |

## Input

Table 2-23 describes the **testtrap** subcommand options.

**Table 2-23. testtrap Subcommand Options**

| Option | Description |
|---|---|
| **-i** | Specifies the index of the trap configuration to use for the test Valid values are from 1 to 4. |

# traceroute

**NOTE:** To use this subcommand, you must have **Administrator** permission.

| Subcommand | Definition |
|---|---|
| traceroute | Traces the network path of routers that packets take as they are forwarded from your system to a destination IPv4 address. |

## Synopsis

```
racadm traceroute <IPv4 address>

racadm traceroute 192.168.0.1

traceroute to 192.168.0.1 (192.168.0.1), 30 hops max,
40 byte packets
1 192.168.0.1 (192.168.0.1) 0.801 ms 0.246 ms 0.253 ms
```

# traceroute6

**NOTE:** To use this subcommand, you must have **Administrator** permission.

| Subcommand | Definition |
|---|---|
| traceroute6 | Traces the network path of routers that packets take as they are forwarded from your system to a destination IPv6 address. |

## Synopsis

```
racadm traceroute6 <IPv6 address>

racadm traceroute fd01::1

traceroute to fd01::1 (fd01::1) from fd01::3, 30 hops
max, 16 byte packets
1 fd01::1 (fd01::1) 14.324 ms 0.26 ms 0.244 ms
```

# usercertupload

**NOTE:** To use this subcommand, you must have **Configure iDRAC** permission.

| Subcommand | Description |
|---|---|
| **usercertupload** | Uploads a user certificate or a user CA certificate from the client to the iDRAC6. |

## Synopsis

```
racadm usercertupload -t <type> [-f <filename>] -i
<index>
```

## Options

Table 2-24 describes the **usercertupload** subcommand options.

**Table 2-24. usercertupload Subcommand Options**

| Option | Description |
|---|---|
| **-t** | Specifies the type of certificate to upload, either the CA certificate or server certificate.<br>1 = user certificate<br>2 = user CA certificate |
| **-f** | Specifies the file name of the certificate to be uploaded. If the file is not specified, the **sslcert** file in the current directory is selected. |
| **-i** | Index number of the user. Valid values 1-16. |

The **usercertupload** command returns `0` when successful and returns a nonzero number when unsuccessful.

## Example

```
racadm usercertupload -t 1 -f c:\cert\cert.txt -i 6
```

# usercertview

**NOTE:** To use this subcommand, you must have **Configure iDRAC** permission.

| Subcommand | Description |
|---|---|
| usercertview | Displays the user certificate or user CA certificate that exists on the iDRAC6. |

## Synopsis

```
racadm sslcertview -t <type> [-A] -i <index>
```

## Options

Table 2-25 describes the **sslcertview** subcommand options.

**Table 2-25. sslcertview Subcommand Options**

| Option | Description |
|---|---|
| -t | Specifies the type of certificate to view, either the user certificate or the user CA certificate.<br>1 = user certificate<br>2 = user CA certificate |
| -A | Prevents printing headers/labels. |
| -i | Index number of the user. Valid values are 1-16. |

# version

| Subcommand | Description |
|---|---|
| version | Displays the RACADM version information. |

## Synopsis

```
racadm version
```

# vflashsd

**NOTE:** To use this subcommand, you must have **Access Virtual Media** privilege.

| Subcommand | Description |
|---|---|
| vflashsd | Allows you to initialize or get the status of the vflash SD card. |

## Synopsis

```
racadm vflashsd initialize
racadm vflashsd status
```

## Description

The vflashsd subcommand allows you to initialize or get the status of the vFlash SD card. The initialize operation removes all existing partitions and resets the card. The status operation displays the status of the last operation performed on the card.

# vflashpartition

**NOTE:** To use this subcommand, you must have **Access Virtual Media** privilege.

| Subcommand | Description |
|---|---|
| vflashpartition | Allows you to create, delete, list, or view the status of partitions on an initialized vFlash SD card. |

## Synopsis

```
racadm vflashpartition create <options>
racadm vflashpartition delete <options>
racadm vflashpartition status <options>
racadm vflashpartition list <options>
```

## Options

Table 2-26 describes the **sslcertview** subcommand options.

**Table 2-26. vflashpartition Subcommand Options**

| Option | Description |
|---|---|
| **-i <index>** | Index of the partition for which this command applies.<br><index> must be an integer from 1 to 16.<br>**NOTE:** For the standard SD card, the index value is 1 because only one partition of size 256 MB is supported. |
| **Options valid only with create action** | |
| **-o <label>** | Label that is displayed when the partition is mounted on the operating system.<br><label> must be a string up to six alphanumeric characters. |
| **-e <type>** | Emulation type for the partition. <type> must be floppy, cddvd, or HDD. |
| **-t <type>** | Create a partition of type <type>. <type> must be:<br>• empty – Create an empty partition. The following options are valid with the empty type:<br>  • -s <size> – Partition size in MB.<br>  • -f <type> – Format type for the partition based on the type of file system. Valid options are RAW, FAT16, FAT32, EXT2, or EXT3.<br>• image – Create a partition using an image relative to the iDRAC. The following options are valid with the image type:<br>  • -l <path> – Specifies the remote path relative to the iDRAC. The path can be on a mounted drive:<br>  SMB path: //<ip or domain>/<share_name> /<path_to_image><br>  NFS path: <ipaddress>:/<path_to_image><br>  • -u <user> – Username for accessing the remote image.<br>  • -p <password> – Password for accessing the remote image. |
| **Options valid only with status action** | |
| **-a** | Displays the status of operations on all existing partitions. |

## Description

The **vflashpartition** subcommand allows you to perform the following:

- Create an empty partition
- Create a partition using an image file
- Format a partition
- View available partitions
- Delete existing partitions
- Get the status of partitions

**NOTE:** Create partition using image file is not supported in local RACADM.

## Examples

- To create a 20MB empty partition:

  ```
  racadm vflashpartition create -i 1 -o drive1 -t
  empty -e HDD -f fat16 -s 20
  ```

- To create a partition using an image file on a remote system:

  ```
  racadm vflashpartition create –i 1 –o drive1 –e
  HDD –t image –l //myserver/sharedfolder/foo.iso –u
  root –p mypassword
  ```

- To delete a partition:

  ```
  racadm vflashpartition delete -i 1
  ```

- To delete all partitions, re-initialize the vFlash SD card.
- 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
  ```

- To list all existing partitions and its properties:

  ```
  racadm vflashpartition list
  ```

- To get the partition size:

  ```
  racadm getconfig –g cfgvflashpartition –o
  cfgvflashpartitionsize –i 1
  ```

- To display the emulation type:

  ```
  racadm getconfig -g cfgvflashpartition -I 1 -o
  cfgvflashpartitionemulatiotype
  ```

- To display the label for the partition that is visible to the operating system:

  ```
  racadm getconfig -g cfgvflashpartition  -i 1 -o
  cfgvflashPartitionlabel
  ```

- To display the format type of the partition:

  ```
  racadm getconfig -g cfgvflashpartition  -i 1 -o
  cfgvflashPartitionFormatType
  ```

- To change a read-only partition to read-write:

  ```
  racadm config -g cfgvflashpartition  -i 1 -o
  cfgvflashPartitionAccessType 1
  ```

- To attach a partition to the host operating system:

  ```
  racadm config -g cfgvflashpartition  -i 1 -o
  cfgvflashPartitionAttachState 1
  ```

# vmdisconnect

**NOTE:** To use this subcommand, you must have **Access Virtual Media** permission.

| Subcommand | Description |
|---|---|
| vmdisconnect | Closes all open iDRAC6 Virtual Media connections from remote clients. |

## Synopsis

```
racadm vmdisconnect
```

## Description

The **vmdisconnect** subcommand allows a user to disconnect another user's Virtual Media session. Once disconnected, the Web-based interface reflects the correct connection status.

The **vmdisconnect** subcommand enables a iDRAC6 user to disconnect all active Virtual Media sessions. The active Virtual Media sessions can be displayed in the iDRAC6 Web-based interface or by using the RACADM subcommands such as **remoteimage** or **getssninfo**.

# vmkey

**NOTE:** To use this subcommand, you must have **Access Virtual Media** permission.

| Subcommand | Description |
|---|---|
| vmkey | Performs Virtual Media key-related operations. |

## Synopsis

```
racadm vmkey <action>
```

If *<action>* is configured as `reset`, the vFlash memory is reset to the default size of 256 MB and removes all data from it.

**NOTE:** This command is deprecated from iDRAC6 1.5 and iDRAC6 3.0 releases onwards. The functionality of this command is now covered by `vflashsd initialize`. While execution of the `vmkey reset` command will be successful, it is recommended to use the `vflashsd initialize` command. For more information, see "vflashsd" on page 72.

## Description

When a custom Virtual Media key image is uploaded to the RAC, the key size becomes the image size. The vmkey subcommand can be used to reset the key back to its original default size, which is 256 MB on the iDRAC6.

# 3

# iDRAC6 Property Database Group and Object Definitions

The iDRAC6 property database contains the configuration information for iDRAC6. Data is organized by associated object, and objects are organized by object group. The IDs for the groups and objects that the property database supports are listed in this section for iDRAC6 Enterprise on Blade Servers and iDRAC6 Enterprise or Express on Rack and Tower Servers.

Use the group and object IDs with the RACADM subcommands to configure the iDRAC6.

Table 3-1 provides an overview of the object groups applicable for iDRAC6 Enterprise on Blade Servers and iDRAC6 on Rack and Tower Servers.

**CAUTION: Racadm sets the value of objects without performing any functional validation on them. For example, RACADM allows you to set the Certificate Validation object to 1 with the Active Directory object set to 0, even though Certificate Validation can happen only if Active Directory is enabled. Similarly, the cfgADSSOEnable object can be set to 0 or 1 even if the cfgADEnable object is 0, but it will take effect only if Active Directory is enabled.**

All string values are limited to displayable ASCII characters, except where otherwise noted.

## Displayable Characters

Displayable characters include the following set:

```
abcdefghijklmnopqrstuvwxwz
ABCDEFGHIJKLMNOPQRSTUVWXYZ
0123456789~`!@#$%^&*()_+-={}[]|\:";'<>,.?/
```

**Table 3-1. Supported Object Groups**

| Subcommand | iDRAC6 on Blade Servers | iDRAC6 on Rack and Tower Servers |
|---|---|---|
| idRacInfo | ✓ | ✓ |
| cfgLanNetworking | ✓ | ✓ |
| cfgRemoteHosts | ✓ | ✓ |
| cfgUserAdmin | ✓ | ✓ |
| cfgEmailAlert | ✓ | ✓ |
| cfgSessionManagement | ✓ | ✓ |
| cfgSerial | ✗ | ✓ |
| cfgOobSnmp | ✓ | ✓ |
| cfgRacTuning | ✓ | ✓ |
| ifcRacManagedNodeOs | ✓ | ✓ |
| cfgRacSecurity | ✓ | ✓ |
| cfgRacVirtual | ✓ | ✓ |
| cfgServerInfo | ✗ | ✓ |
| cfgActiveDirectory | ✓ | ✓ |
| cfgLDAP | ✓ | ✓ |
| cfgLdapRoleGroup | ✓ | ✓ |
| cfgStandardSchema | ✓ | ✓ |
| cfgIpmiSol | ✓ | ✓ |
| cfgIpmiLan | ✓ | ✓ |
| cfgIpmiPetIpv6 | ✓ | ✓ |

**Table 3-1. Supported Object Groups *(continued)***

| Subcommand | iDRAC6 on Blade Servers | iDRAC6 on Rack and Tower Servers |
|---|---|---|
| cfgIpmiPef | ✓ | ✓ |
| cfgIpmiPet | ✓ | ✓ |
| cfgUserDomain | ✓ | ✓ |
| cfgServerPower | ✓ | ✓ |
| cfgServerPowerSupply | ✗ | ✓ |
| cfgIPv6LanNetworking | ✓ | ✓ |
| cfgIPv6URL | ✓ | ✓ |
| cfgIpmiSerial | ✗ | ✓ |
| cfgSmartCard | ✓ | ✓ |
| cfgNetTuning | ✗ | ✓ |
| cfgSensorRedundancy | ✗ | ✓ |
| cfgVFlashSD | ✓ | ✓ |
| cfgVFlashPartition | ✓ | ✓ |

✓ = Supported; ✗=Not supported

# idRacInfo

This group contains display parameters to provide information about the specifics of the iDRAC6 being queried. One instance of the group is allowed.

The following sections provides information about the objects in the **idRACInfo** group.

### idRacProductInfo (Read Only)

| | |
|---|---|
| **Description** | A text string that identifies the product. |
| **Legal Values** | A string of up to 63 ASCII characters. |
| **Default** | Integrated Dell Remote Access Controller. |

### idRacDescriptionInfo (Read Only)

| | |
|---|---|
| **Description** | A text description of the iDRAC type. |
| **Legal Values** | A string of up to 255 ASCII characters. |
| **Default** | This system component provides a complete set of remote management functions for Dell PowerEdge servers. |

### idRacVersionInfo (Read Only)

| | |
|---|---|
| **Description** | String containing the current product firmware version. |
| **Legal Values** | A string of up to 63 ASCII characters. |
| **Default** | The current version number. |

### idRacBuildInfo (Read Only)

| | |
|---|---|
| **Description** | String containing the current product build version. |
| **Legal Values** | A string of up to 16 ASCII characters. |
| **Default** | The current iDRAC6 firmware build version. |

### idRacName (Read Only)

| | |
|---|---|
| **Description** | A user-assigned name to identify this controller. |
| **Legal Values** | A string of up to 15 ASCII characters. |
| **Default** | iDRAC |

### idRacType (Read Only)

| | |
|---|---|
| **Description** | Identifies the remote access controller type as iDRAC6. |
| **Legal Values** | Product ID |
| **Default** | For iDRAC6 on Rack and Servers: 10<br>For iDRAC6 Enterprise on Blade Servers: 8 |

## cfgLanNetworking

This group contains parameters to configure the iDRAC6 NIC.

One instance of the group is allowed. Some objects in this group may require the iDRAC6 NIC to be reset, which may cause a brief loss in connectivity. Objects that change the iDRAC6 NIC IP address settings will close all active user sessions and require users to reconnect using the updated IP address settings.

**NOTE:** For any network property changes on iDRAC6 to be successfully executed through RACADM, you must first enable iDRAC6 NIC.

The following sections provides information about the objects in the **cfgLanNetworking** group.

### cfgNicIPv4Enable (Read/Write)

| | |
|---|---|
| **Description** | Enables or disables the iDRAC6 IPv4 stack. |
| **Legal Values** | 1 (TRUE)<br>0 (FALSE) |
| **Default** | 1 |

### cfgNicSelection (Read/Write)

**NOTE:** This object is applicable only for iDRAC6 on Rack and Tower Servers and not for iDRAC6 Enterprise on Blade Servers.

**Description** Specifies the current mode of operation for the RAC network interface controller (NIC). Table 3-2 describes the supported modes.

**Legal Values** 0 = Shared

1 = Shared with Failover LOM2

2 = Dedicated

3 = Shared with Failover All LOMs (iDRAC6 Enterprise only)

**Default** 0 (iDRAC6 Express)

2 (iDRAC6 Enterprise)

**Table 3-2. cfgNicSelection Supported Modes**

| Mode | Description |
|---|---|
| Shared | Used if the host server integrated NIC is shared with the RAC on the host server. This mode enables configurations to use the same IP address on the host server and the RAC for common accessibility on the network. |
| Shared with Failover: LOM 2 | Enables teaming capabilities between host server LOM2 integrated network interface controllers. |
| Dedicated | Specifies that the RAC NIC is used as the dedicated NIC for remote accessibility. |

**Table 3-2. cfgNicSelection Supported Modes *(continued)***

| Mode | Description *(continued)* |
|---|---|
| Shared with Failover All LOMs | Enables teaming capabilities between all LOMs on the host server integrated network interface controllers.<br>The remote access device network interface is fully functional when the host operating system is configured for NIC teaming. The remote access device receives data through NIC 1 and NIC 2, but transmits data only through NIC 1.<br>Failover occurs from NIC 2 to NIC 3 and then to NIC 4. If NIC 4 fails, the remote access device fails over all data transmission back to NIC 1, but only if the original NIC 1 failure has been corrected. |

## cfgNicVLanEnable (Read/Write)

**NOTE:** For iDRAC6 Enterprise on Blade Servers, this object is read-only and VLAN settings can be configured through CMC Web Interface. iDRAC6 displays only the current VLAN settings and you cannot modify the settings from iDRAC6.

**Description** Enables or disables the VLAN capabilities of the RAC/BMC.

**NOTE:** For iDRAC6 Enterprise on Blade Servers, this object enables or disables the VLAN capabilities of iDRAC6 from CMC.

**Legal Values** 1 (TRUE)

0 (FALSE)

**Default** 0

## cfgNicVLanId (Read/Write)

**Description** Specifies the VLAN ID for the network VLAN configuration (in CMC for iDRAC6 Enterprise on Blade Servers). This property is only valid if **cfgNicVLanEnable** is set to 1 (enabled).

**Legal Values** 1-4094

**Default** 1

### cfgNicVLanPriority (Read/Write)

| | |
|---|---|
| **Description** | Specifies the VLAN Priority for the network VLAN configuration (in CMC for iDRAC6 Enterprise on Blade Servers). This property is only valid if cfgNicVLanEnable is set to 1 (enabled). |
| **Legal Values** | 0-7 |
| **Default** | 0 |

### cfgDNSDomainNameFromDHCP (Read/Write)

| | |
|---|---|
| **Description** | Specifies that the iDRAC6 DNS domain name should be assigned from the network DHCP server |
| **Legal Values** | 1 (TRUE)<br>0 (FALSE) |
| **Default** | 0 |

### cfgDNSDomainName (Read/Write)

| | |
|---|---|
| **Description** | This is the DNS domain name. This parameter is only valid if **cfgDNSDomainNameFromDHCP** is set to 0 (FALSE). |
| **Legal Values** | A string of up to 254 ASCII characters. At least one of the characters must be alphabetic. Characters are restricted to alphanumeric, '-', and '.'.<br>**NOTE:** Microsoft Active Directory only supports Fully Qualified Domain Names (FQDN) of 64 bytes or fewer. |
| **Default** | <blank> |

### cfgDNSRacName (Read/Write)

| | |
|---|---|
| **Description** | Displays the iDRAC6 name, which is rac-*service tag* by default. This parameter is only valid if **cfgDNSRegisterRac** is set to 1 (TRUE). |
| **Legal Values** | A string of up to 63 ASCII characters. At least one character must be alphabetic.<br>**NOTE:** Some DNS servers only register names of 31 characters or fewer. |
| **Default** | idrac-<service tag> |

### cfgDNSRegisterRac (Read/Write)

| | |
|---|---|
| **Description** | Registers the iDRAC6 name on the DNS server |
| **Legal Values** | 1 (TRUE)<br>0 (FALSE) |
| **Default** | 0 |

### cfgDNSServersFromDHCP (Read/Write)

| | |
|---|---|
| **Description** | Specifies if the DNS server IPv4 addresses should be assigned from the DHCP server on the network. |
| **Legal Values** | 1 (TRUE)<br>0 (FALSE) |
| **Default** | 0 |

### cfgDNSServer1 (Read/Write)

| | |
|---|---|
| **Description** | Specifies the IPv4 address for DNS server 1. This property is only valid if **cfgDNSServersFromDHCP** is set to 0 (FALSE).<br>**NOTE: cfgDNSServer1** and **cfgDNSServer2** may be set to identical values while swapping addresses. |
| **Legal Values** | String representing a valid IPv4 address. For example: 192.168.0.20. |
| **Default** | 0.0.0.0 |

## cfgDNSServer2 (Read/Write)

| | |
|---|---|
| **Description** | Retrieves the IPv4 address for DNS server 2. This parameter is only valid if **cfgDNSServersFromDHCP** is set to 0 (FALSE).<br>**NOTE: cfgDNSServer1** and **cfgDNSServer2** may be set to identical values while swapping addresses. |
| **Legal Values** | String representing a valid IPv4 address. For example: 192.168.0.20. |
| **Default** | 0.0.0.0 |

## cfgNicEnable (Read/Write)

| | |
|---|---|
| **Description** | Enables or disables the iDRAC6 network interface controller. If the NIC is disabled, the remote network interfaces to the iDRAC6 will no longer be accessible and iDRAC6 will only be available through the local RACADM interface. |
| **Legal Values** | 1 (TRUE)<br>0 (FALSE) |
| **Default** | 1 |

## cfgNicIpAddress (Read/Write)

**NOTE:** This parameter is only configurable if the **cfgNicUseDhcp** parameter is set to 0 (FALSE).

| | |
|---|---|
| **Description** | Specifies the static IPv4 address to assign to the RAC. This property is only valid if **cfgNicUseDhcp** is set to **0** (FALSE). |
| **Legal Values** | String representing a valid IPv4 address. For example: 192.168.0.20. |
| **Default** | For iDRAC6 on Rack and Tower Servers: 192.168.0.120<br>For iDRAC6 Enterprise on Blade Servers: 192.168.0.*n*, where *n* is 120 plus the server slot number. |

## cfgNicNetmask (Read/Write)

**NOTE:** This parameter is only configurable if the **cfgNicUseDhcp** parameter is set to 0 (FALSE).

| | |
|---|---|
| **Description** | The subnet mask used for the iDRAC6 IP address.<br>This property is only valid if **cfgNicUseDhcp** is set to **0** (FALSE). |
| **Legal Values** | String representing a valid subnet mask. For example: 255.255.255.0. |
| **Default** | 255.255.255.0 |

## cfgNicGateway (Read/Write)

**NOTE:** This parameter is only configurable if the **cfgNicUseDhcp** parameter is set to 0 (FALSE).

| | |
|---|---|
| **Description** | The iDRAC6 gateway IPv4 address.<br>The gateway IPv4 address used for static assignment of the RAC IP address. This property is only valid if **cfgNicUseDhcp** is set to **0** (FALSE). |
| **Legal Values** | String representing a valid gateway IPv4 address. For example: 192.168.0.1. |
| **Default** | 192.168.0.1 |

## cfgNicUseDhcp (Read/Write)

| | |
|---|---|
| **Description** | Specifies whether DHCP is used to assign the iDRAC6 IPv4 address. If this property is set to 1 (TRUE), then the iDRAC6 IPv4 address, subnet mask, and gateway are assigned from the DHCP server on the network. If this property is set to **0** (FALSE), the user can configure the **cfgNicIpAddress**, **cfgNicNetmask**, and **cfgNicGateway** properties. |
| **Legal Values** | 1 (TRUE)<br>0 (FALSE) |
| **Default** | 0 |

### cfgNicMacAddress (Read Only)

| | |
|---|---|
| **Description** | The iDRAC6 NIC MAC address. |
| **Legal Values** | String representing the iDRAC6 NIC MAC address. |
| **Default** | The current MAC address of the iDRAC6 NIC. For example, 00:12:67:52:51:A3. |

## cfgRemoteHosts

This group provides properties that allow configuration of the SMTP server for e-mail alerts.

The following sections provides information about the objects in the **cfgRemoteHosts** group.

### cfgRhostsFwUpdateTftpEnable (Read/Write)

| | |
|---|---|
| **Description** | Enables or disables the iDRAC6 firmware update from a network TFTP server. |
| **Legal Values** | 1 (TRUE)<br>0 (FALSE) |
| **Default** | 1 |

### cfgRhostsFwUpdateIpAddr (Read/Write)

| | |
|---|---|
| **Description** | Specifies the network TFTP server IPv4 or IPv6 address that is used for TFTP iDRAC6 firmware update operations. |
| **Legal Values** | A string representing a valid IPv4 or IPv6 address. For example, `192.168.0.61` |
| **Default** | For IPv4, it is 0.0.0.0 |

### cfgRhostsFwUpdatePath (Read/Write)

| | |
|---|---|
| **Description** | Specifies TFTP path where the iDRAC6 firmware image file exists on the TFTP server. The TFTP path is relative to the TFTP root path on the TFTP server.<br>**NOTE:** The server may still require you to specify the drive (for example, **C:**). |
| **Legal Values** | A string with a maximum length of 255 ASCII characters. |
| **Default** | <blank> |

### cfgRhostsSmtpServerIpAddr (Read/Write)

| | |
|---|---|
| **Description** | The IPv4 or IPv6 address of the network SMTP server. The SMTP server transmits e-mail alerts from the iDRAC6 if the alerts are configured and enabled. |
| **Legal Values** | A string representing a valid SMTP server IPv4 or IPv6 address. For example: 192.168.0.55. |
| **Default** | For IPv4, it is 0.0.0.0 |

### cfgRhostsSyslogEnable (Read/Write)

| | |
|---|---|
| **Description** | Enables or disables remote syslog. |
| **Legal Values** | 1 (TRUE)<br>0 (FALSE) |
| **Default** | 0 |

### cfgRhostsSyslogPort (Read/Write)

| | |
|---|---|
| **Description** | Remote syslog port number. |
| **Legal Values** | 1— 65535 |
| **Default** | 514 |

### cfgRhostsSyslogServer1 (Read/Write)

| | |
|---|---|
| **Description** | Name of remote syslog server. This property is only valid if **cfgRhostsSyslogEnable** is set to 1 (enabled). |
| **Legal Values** | String from 0 to 511 characters. |
| **Default** | <blank> |

### cfgRhostsSyslogServer2 (Read/Write)

| | |
|---|---|
| **Description** | Name of remote syslog server. This property is only valid if **cfgRhostsSyslogEnable** is set to 1 (enabled). |
| **Legal Values** | String from 0 to 511 characters. |
| **Default** | <blank> |

### cfgRhostsSyslogServer3 (Read/Write)

| | |
|---|---|
| **Description** | Name of remote syslog server.This property is only valid if **cfgRhostsSyslogEnable** is set to 1 (enabled). |
| **Legal Values** | String from 0 to 511 characters. |
| **Default** | <blank> |

## cfgUserAdmin

This group provides configuration information about the users who are allowed to access the iDRAC6 through the available remote interfaces.

Up to 16 instances of the user group are allowed. Each instance represents the configuration for an individual user.

The following sections provides information about the objects in the **cfgUserAdmin** group.

### cfgUserAdminIndex (Read Only)

| | |
|---|---|
| **Description** | The unique index of a user. |
| **Legal Values** | This parameter is populated based on the existing instances. |
| **Default** | <index of the instance> |

## cfgUserAdminIpmiLanPrivilege (Read/Write)

| | |
|---|---|
| **Description** | The maximum privilege on the IPMI LAN channel. |
| **Legal Values** | 2 (User)<br>3 (Operator)<br>4 (Administrator)<br>15 (No access) |
| **Default** | 4 (User 2)<br>15 (All others) |

## cfgUserAdminPrivilege (Read/Write)

| | |
|---|---|
| **Description** | This property specifies the role-based authority privileges allowed for the user. The value is represented as a bit mask that allows for any combination of privilege values. Table 3-3 describes the user privilege bit values that can be combined to create bit masks. |
| **Legal Values** | 0x00000000 to 0x000001ff, and 0x0 |
| **Default** | 0x00000000 |

**Table 3-3. Bit Masks for User Privileges**

| User Privilege | Privilege Bit Mask |
|---|---|
| Login to iDRAC | 0x00000001 |
| Configure iDRAC | 0x00000002 |
| Configure Users | 0x00000004 |
| Clear Logs | 0x00000008 |
| Execute Server Control Commands | 0x00000010 |
| Access Virtual Console | 0x00000020 |
| Access Virtual Media | 0x00000040 |
| Test Alerts | 0x00000080 |
| Execute Debug Commands | 0x00000100 |

### Examples

Table 3-4 provides sample privilege bit masks for users with one or more privileges.

**Table 3-4. Sample Bit Masks for User Privileges**

| User Privilege(s) | Privilege Bit Mask |
|---|---|
| The user is not allowed to access the iDRAC. | 0x00000000 |
| The user may only login to the iDRAC and view iDRAC and server configuration information. | 0x00000001 |
| The user may login to the iDRAC and change configuration. | 0x00000001 + 0x00000002 = 0x00000003 |
| The user may login to iDRAC, access Virtual Media, and access Virtual Console. | 0x00000001 + 0x00000040 + 0x00000080 = 0x000000C1 |

## cfgUserAdminUserName (Read/Write)

**Description** The name of the user for this index. The user index is created by writing a string into this name field if the index is empty. Writing a string of double quotes ("") deletes the user at that index. You cannot change the name. You must delete and then recreate the name. The string cannot contain / (forward slash), \ (backslash), . (period), @ (at symbol) or quotation marks.

**NOTE:** This property value must be unique among user names.

**Legal Values** A string of up to 16 ASCII characters.

**Default** root (User 2)

<blank> (All others)

### cfgUserAdminPassword (Write Only)

| | |
|---|---|
| **Description** | The password for this user. User passwords are encrypted and cannot be seen or displayed after the property is written. |
| **Legal Values** | A string of up to 20 ASCII characters. |
| **Default** | ******** |

### cfgUserAdminEnable (Read/Write)

| | |
|---|---|
| **Description** | Enables or disables an individual user. |
| **Legal Values** | 1 (TRUE)<br>0 (FALSE) |
| **Default** | 1 (User 2)<br>0 (All others) |

### cfgUserAdminSolEnable (Read/Write)

| | |
|---|---|
| **Description** | Enables or disables Serial Over LAN (SOL) user access for the user. |
| **Legal Values** | 1 (TRUE)<br>0 (FALSE) |
| **Default** | 0 |

### cfgUserAdminIpmiSerialPrivilege (Read/Write)

**NOTE:** This object is applicable only for iDRAC6 on Rack and Tower Servers and not for iDRAC6 Enterprise on Blade Servers.

| | |
|---|---|
| **Description** | The maximum privilege on the IPMI LAN channel. |
| **Legal Values** | 2 (User)<br>3 (Operator)<br>4 (Administrator)<br>15 (No access) |
| **Default** | 4 (User 2)<br>15 (All others) |

# cfgEmailAlert

This group contains parameters to configure the iDRAC6 e-mail alerting capabilities. Up to four instances of this group are allowed.

The following sections provides information about the objects in the **cfgEmailAlert** group.

### cfgEmailAlertIndex (Read Only)

| | |
|---|---|
| **Description** | The unique index of an alert instance. |
| **Legal Values** | 1-4 |
| **Default** | <instance> |

### cfgEmailAlertEnable (Read/Write)

| | |
|---|---|
| **Description** | Enables or disables the alert instance. |
| **Legal Values** | 1 (TRUE)<br>0 (FALSE) |
| **Default** | 0 |

### cfgEmailAlertAddress (Read/Write)

| | |
|---|---|
| **Description** | Specifies the destination email address for email alerts, for example, user1@company.com. |
| **Legal Values** | E-mail address format, with a maximum length of 64 ASCII characters. |
| **Default** | <blank> |

### cfgEmailAlertCustomMsg (Read/Write)

| | |
|---|---|
| **Description** | Specifies a custom message that forms the subject of the alert. |
| **Legal Values** | A string of up to 32 characters |
| **Default** | <blank> |

# cfgSessionManagement

This group contains parameters to configure the number of sessions that can connect to the iDRAC6. One instance of the group is allowed.

The following sections provides information about the objects in the **cfgSessionManagement** group.

## cfgSsnMgtRacadmTimeout (Read/Write)

**NOTE:** This object is applicable only for iDRAC6 on Rack and Tower Servers and not for iDRAC6 Enterprise on Blade Servers.

| | |
|---|---|
| **Description** | Defines the idle timeout in seconds for the Remote RACADM interface. If a remote RACADM session remains inactive for more than the specified sessions, the session will be closed. |
| **Legal Values** | 10 –1920 |
| **Default** | 60 |

## cfgSsnMgtConsRedirMaxSessions (Read/Write)

| | |
|---|---|
| **Description** | Specifies the maximum number of Virtual Console sessions allowed on the iDRAC6. |
| **Legal Values** | For iDRAC6 on Rack and Tower Servers: 1 – 4.<br>For iDRAC6 Enterprise on Blade Servers: 1-2 |
| **Default** | For iDRAC6 on Rack and Tower Servers: 4<br>For iDRAC6 Enterprise on Blade Servers: 2 |

### cfgSsnMgtWebserverTimeout (Read/Write)

| | |
|---|---|
| **Description** | Defines the Web server timeout. This property sets the amount of time in seconds that a connection is allowed to remain idle (there is no user input). The session is cancelled if the time limit set by this property is reached. Changes to this setting do not affect the current session; you must log out and log in again to make the new settings effective.<br>An expired Web server session logs out the current session. |
| **Legal Values** | 60 – 10800 |
| **Default** | 1800 |

### cfgSsnMgtSshIdleTimeout (Read/Write)

| | |
|---|---|
| **Description** | Defines the secure shell idle timeout. This property sets the amount of time in seconds that a connection is allowed to remain idle (there is no user input). The session is cancelled if the time limit set by this property is reached. Changes to this setting do not affect the current session; you must log out and log in again to make the new settings effective.<br>An expired secure shell session displays the following error message:<br>• In case of iDRAC6 on Rack and Tower Servers:<br>`Connection timed out`<br>• In case of iDRAC6 Enterprise on Blade Servers:<br>`Session timed out. Closing the session...`<br>After the message is displayed, the system returns you to the shell that generated the Secure Shell session. |
| **Legal Values** | 0 (No timeout)<br>0 – 10800 |
| **Default** | For iDRAC6 on Rack and Tower Servers: 300<br>For iDRAC6 Enterprise on Blade Servers: 1800 |

### cfgSsnMgtTelnetIdleTimeout (Read/Write)

**Description** Defines the Telnet idle timeout. This property sets the amount of time in seconds that a connection is allowed to remain idle (there is no user input). The session is cancelled if the time limit set by this property is reached. Changes to this setting do not affect the current session (you must log out and log in again to make the new settings effective).

An expired Telnet session displays the following error message:

- In case of iDRAC6 on Rack and Tower Servers:

  ```
  Connection timed out
  ```

- In case of iDRAC6 Enterprise on Blade Servers:

  ```
  Session timed out. Closing the session...
  ```

After the message is displayed, the system returns you to the shell that generated the Telnet session.

**Legal Values** 0 (No timeout)

0– 10800

**Default** For iDRAC6 on Rack and Tower Servers: 300

For iDRAC6 Enterprise on Blade Servers: 1800

# cfgSerial

This group contains configuration parameters for the iDRAC6 services. One instance of the group is allowed.

The following sections provides information about the objects in the **cfgSerial** group.

**NOTE:** The **cfgSerial** object group is applicable only for iDRAC6 on Rack and Tower Servers and not for iDRAC6 Enterprise on Blade Servers.

## cfgSerialBaudRate (Read/Write)

| | |
|---|---|
| **Description** | Sets the baud rate on the iDRAC6 serial port. |
| **Legal Values** | 9600, 28800, 57600, 115200 |
| **Default** | 57600 |

## cfgSerialConsoleEnable (Read/Write)

| | |
|---|---|
| **Description** | Enables or disables the RAC serial console interface. |
| **Legal Values** | 1 (TRUE)<br>0 (FALSE) |
| **Default** | 0 |

### cfgSerialConsoleQuitKey (Read/Write)

| | |
|---|---|
| **Description** | This key or key combination terminates text Virtual Console when using the **console com2** command. The **cfgSerialConsoleQuitKey** value can be represented by one of the following:<br>• Decimal value — For example, 95<br>• Hexadecimal value — For example, 0x12<br>• Octal value — For example, 007<br>• ASCII value — For example, ^a<br>ASCII values may be represented using the following Escape Key codes:<br>(a) ^ followed by any alphabetic (a-z, A-Z)<br>(b) ^ followed by the listed special characters: [ ] \ ^ _ |
| **Legal Values** | A string of up to 4 characters |
| **Default** | ^\ (<Ctrl><\>)<br>**NOTE:** The "^" is the <Ctrl> key. |

### cfgSerialConsoleIdleTimeout (Read/Write)

| | |
|---|---|
| **Description** | The maximum number of seconds to wait before an idle serial session is disconnected. |
| **Legal Values** | 0 = No timeout<br>60 – 1920 |
| **Default** | 300 |

### cfgSerialConsoleNoAuth (Read/Write)

| | |
|---|---|
| **Description** | Enables or disables the RAC serial console login authentication. |
| **Legal Values** | 0 (enables serial login authentication)<br>1 (disables serial login authentication) |
| **Default** | 0 |

### cfgSerialConsoleCommand (Read/Write)

| | |
|---|---|
| **Description** | Specifies a serial command that is executed after a user logs into the serial console interface. |
| **Legal Values** | A string of up to 128 characters. |
| **Default** | <blank> |

### cfgSerialHistorySize (Read/Write)

| | |
|---|---|
| **Description** | Specifies the maximum size of the serial history buffer. |
| **Legal Values** | 0 – 8192 |
| **Default** | 8192 |

### cfgSerialCom2RedirEnable (Read/Write)

| | |
|---|---|
| **Description** | Enables or disables the console for COM 2 port redirection. |
| **Legal Values** | 1 (TRUE)<br>0 (FALSE) |
| **Default** | 1 |

### cfgSerialSshEnable (Read/Write)

| | |
|---|---|
| **Description** | Enables or disables the secure shell (SSH) interface on the iDRAC6. |
| **Legal Values** | 1 (TRUE)<br>0 (FALSE) |
| **Default** | 1 |

### cfgSerialTelnetEnable (Read/Write)

| | |
|---|---|
| **Description** | Enables or disables the Telnet console interface on the iDRAC6. |
| **Legal Values** | 1 (TRUE)<br>0 (FALSE) |
| **Default** | 0 |

# cfgOobSnmp

This group contains parameters to configure the SNMP agent and trap capabilities of the iDRAC6. One instance of the group is allowed.

The following sections provides information about the objects in the **cfgOobSnmp** group.

### cfgOobSnmpAgentCommunity (Read/Write)

| | |
|---|---|
| **Description** | Specifies the SNMP Community Name used for SNMP traps. |
| **Legal Values** | A string of up to 31 characters. |
| **Default** | public |

### cfgOobSnmpAgentEnable (Read/Write)

| | |
|---|---|
| **Description** | Enables or disables the SNMP agent in the iDRAC6. |
| **Legal Values** | 1 (TRUE)<br>0 (FALSE) |
| **Default** | 0 |

# cfgRacTuning

This group is used to configure various iDRAC6 configuration properties, such as valid ports and security port restrictions.

The following sections provides information about the objects in the **cfgRacTuning** group.

### cfgRacTuneConRedirPort (Read/Write)

| | |
|---|---|
| **Description** | Specifies the port to be used for keyboard, mouse, video, and Virtual Media traffic to the iDRAC6. |
| **Legal Values** | 1 – 65535 |
| **Default** | 5900 |

### cfgRacTuneRemoteRacadmEnable (Read/Write)

| | |
|---|---|
| **Description** | Enables or disables the Remote RACADM interface in the iDRAC. |
| **Legal Values** | 1 (TRUE)<br>0 (FALSE) |
| **Default** | 1 |

### cfgRacTuneCtrlEConfigDisable

**NOTE:** This object is applicable only for iDRAC6 on Rack and Tower Servers and not for iDRAC6 Enterprise on Blade Servers.

| | |
|---|---|
| **Description** | Enables or disables the ability to disable the ability of the local user to configure the iDRAC from the BIOS POST option-ROM. |
| **Legal Values** | 1 (TRUE)<br>0 (FALSE) |
| **Default** | 0 |

### cfgRacTuneHttpPort (Read/Write)

| | |
|---|---|
| **Description** | Specifies the port number to use for HTTP network communication with the iDRAC6. |
| **Legal Values** | 10 – 65535 |
| **Default** | 80 |

### cfgRacTuneHttpsPort (Read/Write)

| | |
|---|---|
| **Description** | Specifies the port number to use for HTTPS network communication with the iDRAC6 |
| **Legal Values** | 10 – 65535 |
| **Default** | 443 |

### cfgRacTuneIpRangeEnable (Read/Write)

| | |
|---|---|
| **Description** | Enables or disables the IPv4 Address Range validation feature of the iDRAC6. |
| **Legal Values** | 1 (TRUE)<br>0 (FALSE) |
| **Default** | 0 |

### cfgRacTuneIpRangeAddr (Read/Write)

| | |
|---|---|
| **Description** | Specifies the acceptable IPv4 address bit pattern in positions determined by the "1"s in the range mask property (**cfgRacTuneIpRangeMask**). |
| **Legal Values** | An IPv4 address formatted string, for example, 192.168.0.44. |
| **Default** | 192.168.1.1 |

### cfgRacTuneIpRangeMask (Read/Write)

| | |
|---|---|
| **Description** | Standard IP mask values with left-justified bits. For example, 255.255.255.0. |
| **Legal Values** | An IPv4 address formatted string, for example, `255.255.255.0`.<br>Standard IP mask values with left-justified bits. |
| **Default** | 255.255.255.0 |

### cfgRacTuneIpBlkEnable (Read/Write)

| | |
|---|---|
| **Description** | Enables or disables the IPv4 address blocking feature of the iDRAC6. |
| **Legal Values** | 1 (TRUE)<br>0 (FALSE) |
| **Default** | 0 |

### cfgRacTuneIpBlkFailCount (Read/Write)

| | |
|---|---|
| **Description** | The maximum number of login failures to occur within the window (**cfgRacTuneIpBlkFailWindow**) before login attempts from the IP address are rejected. |
| **Legal Values** | 2 – 16 |
| **Default** | 5 |

### cfgRacTuneIpBlkFailWindow (Read/Write)

| | |
|---|---|
| **Description** | Defines the time span in seconds that the failed attempts are counted. When failure attempts age beyond this limit, they are dropped from the count. |
| **Legal Values** | 10 – 655356 |
| **Default** | 60 |

### cfgRacTuneIpBlkPenaltyTime (Read/Write)

| | |
|---|---|
| **Description** | Defines the time span in seconds that session requests from an IP address with excessive failures are rejected. |
| **Legal Values** | 10 – 655356 |
| **Default** | 300 |

### cfgRacTuneSshPort (Read/Write)

| | |
|---|---|
| **Description** | Specifies the port number used for the iDRAC6 SSH interface. |
| **Legal Values** | 1 – 65535 |
| **Default** | 22 |

### cfgRacTuneTelnetPort (Read/Write)

| | |
|---|---|
| **Description** | Specifies the port number used for the iDRAC6 Telnet interface. |
| **Legal Values** | 1 – 65535 |
| **Default** | 23 |

### cfgRacTuneConRedirEnable (Read/Write)

| | |
|---|---|
| **Description** | Enables or disables Virtual Console. |
| **Legal Values** | 1 (TRUE)<br>0 (FALSE) |
| **Default** | 1 |

### cfgRacTuneConRedirEncryptEnable (Read/Write)

| | |
|---|---|
| **Description** | Encrypts the video in a Virtual Console session. |
| **Legal Values** | 1 (TRUE)<br>0 (FALSE) |
| **Default** | 1 |

### cfgRacTuneAsrEnable (Read/Write)

**NOTE:** This object requires an iDRAC6 reset before it becomes active.

| | |
|---|---|
| **Description** | Enables or disables the iDRAC6 last crash screen capture feature. |
| **Legal Values** | 1 (TRUE)<br>0 (FALSE) |
| **Default** | 0 |

### cfgRacTuneDaylightOffset (Read/Write)

| | |
|---|---|
| **Description** | Specifies the daylight savings offset (in minutes) to use for the RAC Time. |
| **Legal Values** | 0 – 60 |
| **Default** | 0 |

### cfgRacTuneTimezoneOffset (Read/Write)

| | |
|---|---|
| **Description** | Specifies the time zone offset (in minutes) from GMT/UTC to use for the RAC Time. Some common time zone offsets for time zones in the United States are:<br>• –480 (PST—Pacific Standard Time)<br>• –420 (MST—Mountain Standard Time)<br>• –360 (CST—Central Standard Time)<br>• –300 (EST—Eastern Standard Time) |
| **Legal Values** | –720 – 7800 |
| **Default** | 0 |

### cfgRacTuneLocalServerVideo (Read/Write)

| | |
|---|---|
| **Description** | Enables (switches on) or disables (switches off) the local server video. |
| **Legal Values** | 1 (TRUE - Enables)<br>0 (FALSE- Disables) |
| **Default** | 1 |

### cfgRacTuneLocalConfigDisable (Read/Write)

| | |
|---|---|
| **Description** | Disables write access to iDRAC6 configuration data by setting to 1.<br>**NOTE:** Access can be disabled using the local RACADM or iDRAC6 Web interface; however, once disabled, access can be re-enabled only through iDRAC6 Web interface. |
| **Legal Values** | 0 (TRUE-Enables)<br>1 (FALSE-Disables) |
| **Default** | 0 |

### cfgRacTuneWebserverEnable (Read/Write)

| | |
|---|---|
| **Description** | Enables or disables the iDRAC6 web server. If this property is disabled, the iDRAC6 will not be accessible using client web browsers. This property has no effect on the Telnet/SSH or RACADM interfaces. |
| **Legal Values** | 1 (TRUE)<br>0 (FALSE) |
| **Default** | 1 |

### cfgRacTuneVirtualConsoleAuthorizeMultipleSessions (Read/Write)

**NOTE:** To modify this property, you must have **Configure iDRAC** permission. This object can be used only with remote or firmware (SSH or Telnet) RACADM and not with local RACADM or with earlier DRAC products.

**NOTE:** This object is applicable only for iDRAC6 on Rack and Tower Servers and not for iDRAC6 Enterprise on Blade Servers.

| | |
|---|---|
| **Description** | If a first user is already using the Virtual Console, the value of this object effects the privileges granted to the subsequent user's shared request after the timeout of 30 seconds. |
| **Legal Values** | 0 (If the user of the first session has not responded for session sharing request by subsequent user, the next session user will get an access denied error after the default timeout value of 30 seconds.)<br>1(If the user of the first session has not responded for session sharing request by subsequent user, the next session user will get a read only access after the default timeout value of 30 seconds.)<br>2 (If the user of the first session has not responded for session sharing request by subsequent user, the next session user will get administrator access after default timeout value of 30 seconds.) |
| **Default** | 0 |

# ifcRacManagedNodeOs

This group contains properties that describe the managed server operating system. One instance of the group is allowed.

The following sections provides information about the objects in the **ifcRacManagedNodeOs** group.

### ifcRacMnOsHostname (Read Only)

| | |
|---|---|
| **Description** | The host name of the managed server. |
| **Legal Values** | A string of up to 255 characters. |
| **Default** | <blank> |

### ifcRacMnOsOsName (Read Only)

| | |
|---|---|
| **Description** | The operating system name of the managed server. |
| **Legal Values** | A string of up to 255 characters. |
| **Default** | <blank> |

# cfgRacSecurity

This group is used to configure settings related to iDRAC6 SSL certificate signing request (CSR) feature. The properties in this group must be configured before generating a CSR from the iDRAC6.

For more information on generating certificate signing requests, see the subcommand "sslcsrgen" on page 64.

The following sections provides information about the objects in the **cfgRacSecurity** group.

### cfgRacSecCsrCommonName (Read/Write)

| | |
|---|---|
| **Description** | Specifies the CSR Common Name (CN) that must be an IP or the iDRAC name as given in the certificate. |
| **Legal Values** | A string of up to 254 characters. |
| **Default** | <blank> |

### cfgRacSecCsrOrganizationName (Read/Write)

| | |
|---|---|
| **Description** | Specifies the CSR Organization Name (O). |
| **Legal Values** | A string of up to 254 characters. |
| **Default** | <blank> |

### cfgRacSecCsrOrganizationUnit (Read/Write)

| | |
|---|---|
| **Description** | Specifies the CSR Organization Unit (OU). |
| **Legal Values** | A string of up to 254 characters. |
| **Default** | <blank> |

### cfgRacSecCsrLocalityName (Read/Write)

| | |
|---|---|
| **Description** | Specifies the CSR Loyalty (L). |
| **Legal Values** | A string of up to 254 characters. |
| **Default** | <blank> |

### cfgRacSecCsrStateName (Read/Write)

| | |
|---|---|
| **Description** | Specifies the CSR State Name (S). |
| **Legal Values** | A string of up to 254 characters. |
| **Default** | <blank> |

### cfgRacSecCsrCountryCode (Read/Write)

| | |
|---|---|
| **Description** | Specifies the CSR Country Code (CC). |
| **Legal Values** | A string of up to 2 characters. |
| **Default** | <blank> |

### cfgRacSecCsrEmailAddr (Read/Write)

| | |
|---|---|
| **Description** | Specifies the CSR email address. |
| **Legal Values** | A string of up to 254 characters. |
| **Default** | <blank> |

### cfgRacSecCsrKeySize (Read/Write)

| | |
|---|---|
| **Description** | Specifies the SSL asymmetric key size for the CSRs. |
| **Legal Values** | 1024<br>2048 |
| **Default** | 1024 |

## cfgRacVirtual

This group contains parameters to configure the iDRAC6 Virtual Media feature. One instance of the group is allowed.

The following sections provides information about the objects in the **cfgRacVirtual** group.

### cfgRacVirMediaAttached (Read/Write)

| | |
|---|---|
| **Description** | This object is used to attach virtual devices to the system via the USB bus. When the devices are attached the server will recognize valid USB mass storage devices attached to the system. This is equivalent to attaching a local USB CDROM/floppy drive to a USB port on the system. When the devices are attached you then can connect to the virtual devices remotely using the iDRAC6 Web interface or the CLI. Setting this object to **0** will cause the devices to detach from the USB bus. |
| **Legal Values** | 0 = Detach<br>1 = Attach<br>2 = Auto-Attach |
| **Default** | 0 |

### cfgVirMediaBootOnce (Read/Write)

| | |
|---|---|
| **Description** | Enables or disables the Virtual Media Boot Once feature of the iDRAC6.<br>If this property is enabled when the host server is rebooted, this feature will attempt to boot from the virtual media devices—if the appropriate media is installed in the device. |
| **Legal Values** | 1 (TRUE)<br>0 (FALSE) |
| **Default** | 0 |

### cfgVirtualFloppyEmulation (Read/Write)

**NOTE:** Virtual Media has to be reattached (using **cfgRacVirMediaAttached**) for this change to take effect.

| | |
|---|---|
| **Description** | When set to 0, the virtual floppy drive is recognized as a removable disk by Windows operating systems. Windows operating systems will assign a drive letter that is C: or higher during enumeration. When set to 1, the Virtual Floppy drive will be seen as a floppy drive by Windows operating systems. Windows operating systems will assign a drive letter of A: or B:. |
| **Legal Values** | 1 (TRUE)<br>0 (FALSE) |
| **Default** | 0 |

### cfgVirMediaKeyEnable (Read/Write)

| | |
|---|---|
| **Description** | Enables or disables the Virtual Media key feature of the RAC.<br>**NOTE:** This command is deprecated from 1.5 and 3.0 releases onwards. The functionality of this command is now covered by `cfgVFlashSDEnable`. While execution of the `cfgVirMediaKeyEnable` command will be successful, it is recommended to use the `cfgVFlashSDEnable` command. For more information, see "cfgVFlashSDEnable (Read/Write)" on page 159. |
| **Legal Values** | 1 (TRUE)<br>0 (FALSE) |
| **Default** | 0 |

### cfgSDWriteProtect (Read only)

| | |
|---|---|
| **Description** | Displays if the physical write protect latch on the SD card is enabled or disabled.<br>**NOTE:** This command is deprecated from 1.5 and 3.0 releases onwards. The functionality of this command is now covered by `cfgVFlashSDWriteProtect`. While execution of the `cfgSDWriteProtect` command will be successful, it is recommended to use the `cfgVFlashSDWriteProtect` command. For more information, see "cfgVFlashSDWriteProtect (Read Only)" on page 161. |
| **Legal Values** | 1 (TRUE)<br>0 (FALSE) |
| **Default** | 0 |

### cfgLCDriveEnable (Read/Write)

| | |
|---|---|
| **Description** | Enable/disable the USC-LCE device from showing up in the operating system. It must be disabled if your using ESXi operating system. Allows proper operation of operating system and drivers interfacing with the iDRAC/USC-LCE USB devices. |
| **Legal Values** | 1 (Enabled)<br>0 (Disabled) |
| **Default** | 1 |

## cfgServerInfo

This group allows you to select the BIOS first boot device and to boot the selected device only once.

The following sections provides information about the objects in the **cfgServerInfo** group.

### cfgServerFirstBootDevice (Read/Write)

| | |
|---|---|
| **Description** | Sets or displays the first boot device. You can also set a vFlash partition that is attached as a bootable device. For more information, see "cfgVFlashPartitionOSVolLabel (ReadOnly)" on page 162. |
| **Legal Values** | No-Override<br>PXE<br>HDD<br>DIAG<br>CD-DVD<br>BIOS<br>vFDD<br>VCD-DVD<br>iSCSI<br>VFLASH<br>FDD<br>SD |
| **Default** | No-Override |

### cfgServerBootOnce (Read/Write)

| | |
|---|---|
| **Description** | Enables or disables the server boot once feature. |
| **Legal Values** | 1 = TRUE<br>0 = FALSE |
| **Default** | 0 |

# cfgActiveDirectory

This group contains parameters to configure the iDRAC6 Active Directory feature.

The following sections provides information about the objects in the **cfgActiveDirectory** group.

## cfgADRacDomain (Read/Write)

| | |
|---|---|
| **Description** | Active Directory Domain in which the iDRAC6 resides. |
| **Legal Values** | Any printable text string of up to 254 characters, with no white space. |
| **Default** | <blank> |

## cfgADRacName (Read/Write)

| | |
|---|---|
| **Description** | Name of iDRAC6 as recorded in the Active Directory forest. |
| **Legal Values** | Any printable text string of up to 254 characters, with no white space. |
| **Default** | <blank> |

## cfgADEnable (Read/Write)

| | |
|---|---|
| **Description** | Enables or disables Active Directory user authentication on the iDRAC6. If this property is disabled, only local iDRAC6 authentication is used for user logins. |
| **Legal Values** | 1 (TRUE)<br>0 (FALSE) |
| **Default** | 0 |

### cfgADSSOEnable (Read/Write)

| | |
|---|---|
| **Description** | Enables or disables Active Directory single sign-on authentication on iDRAC6. |
| **Legal Values** | 1 (TRUE)<br>0 (FALSE) |
| **Default** | 0 |

### cfgADDomainController1 (Read/Write)

| | |
|---|---|
| **Description** | iDRAC6 uses the value you specify to search the LDAP server for user names. |
| **Legal Values** | A string of up to 254 ASCII characters representing a valid IP address or a fully qualified domain name (FQDN). |
| **Default** | No default value |

### cfgADDomainController2 (Read/Write)

| | |
|---|---|
| **Description** | iDRAC6 uses the value you specify to search the LDAP server for user names. |
| **Legal Values** | A string of up to 254 ASCII characters representing a valid IP address or a fully qualified domain name (FQDN). |
| **Default** | No default value |

### cfgADDomainController3 (Read/Write)

| | |
|---|---|
| **Description** | iDRAC6 uses the value you specify to search the LDAP server for user names. |
| **Legal Values** | A string of up to 254 ASCII characters representing a valid IP address or a fully qualified domain name (FQDN). |
| **Default** | No default value |

### cfgADAuthTimeout (Read/Write)

**NOTE:** To modify this property, you must have **Configure iDRAC** permission.

| | |
|---|---|
| **Description** | Specifies the number of seconds to wait for Active Directory authentication requests to complete before timing out. |
| **Legal Values** | 15 – 300 seconds |
| **Default** | 120 |

### cfgADType (Read/Write)

| | |
|---|---|
| **Description** | Determines the schema type to use with Active Directory. |
| **Legal Values** | 1 (Enables Active Directory with the extended schema)<br>2 (Enables Active Directory with the standard schema) |
| **Default** | 1 |

### cfgADGlobalCatalog1 (Read/Write)

| | |
|---|---|
| **Description** | iDRAC6 uses the value you specify to search the Global Catalog server for user names. |
| **Legal Values** | A string of up to 254 ASCII characters representing a valid IP address or a fully qualified domain name (FQDN). |
| **Default** | No default value |

### cfgADGlobalCatalog2 (Read/Write)

| | |
|---|---|
| **Description** | iDRAC6 uses the value you specify to search the Global Catalog server for user names. |
| **Legal Values** | A string of up to 254 ASCII characters representing a valid IP address or a fully qualified domain name (FQDN). |
| **Default** | No default value |

### cfgADGlobalCatalog3 (Read/Write)

| | |
|---|---|
| **Description** | iDRAC6 uses the value you specify to search the Global Catalog server for user names. |
| **Legal Values** | A string of up to 254 ASCII characters representing a valid IP address or a fully qualified domain name (FQDN). |
| **Default** | No default value |

### cfgADCertValidationEnable (Read/Write)

| | |
|---|---|
| **Description** | Enables or disables Active Directory certificate validation as a part of the Active Directory configuration process. |
| **Legal Values** | 1 (TRUE)<br>0 (FALSE) |
| **Default** | 1 |

### cfgADDcSRVLookupEnable (Read/Write)

| | |
|---|---|
| **Description** | Configures iDRAC6 to use pre-configured domain controllers or to use DNS to find the domain controller. If using pre-configured domain controllers, then the domain controllers to use are specified under cfgAdDomainController1, cfgAdDomainController2, and cfgAdDomainController3. iDRAC6 does not fail over to the specified domain controllers when DNS lookup fails or none of the servers returned by the DNS lookup works. |
| **Legal Values** | 1 (TRUE)—use DNS to look up domain controllers<br>0 (FALSE)—use pre-configured domain controllers |
| **Default** | 0 |

### cfgADDcSRVLookupbyUserdomain (Read/Write)

| | |
|---|---|
| **Description** | Chooses the way the user domain is looked up for Active Directory. |
| **Legal Values** | 1 (TRUE)—use user domain as the search domain to look up DCs. The user domain is chosen from the user domain list or entered by the login user.<br>0 (FALSE)—use the configured search domain **cfgADDcSrvLookupDomainName** to look up DCs. |
| **Default** | 1 |

### cfgADDcSRVLookupDomainName (Read/Write)

| | |
|---|---|
| **Description** | This is the Active Directory Domain to use when **cfgAddcSrvLookupbyUserDomain** is set to **0**. |
| **Legal Values** | String. Maximum length = 254 |
| **Default** | Null |

### cfgADGcSRVLookupEnable (Read/Write)

| | |
|---|---|
| **Description** | Determines how the global catalog server is looked up. If using pre-configured global catalog servers, then the iDRAC6 uses the values cfgAdGlobalCatalog1, cfgAdGlobalCatalog2, and cfgAdGlobalCatalog3. |
| **Legal Values** | 0(FALSE)—use pre-configured Global Catalog Servers (GCS)<br>1(TRUE)—use DNS to look up GCS |
| **Default** | 0 |

### cfgADGcRootDomain (Read/Write)

| | |
|---|---|
| **Description** | The name of the Active Directory root domain used for DNS look up, to locate Global Catalog servers. |
| **Legal Values** | String. Maximum length = 254 |
| **Default** | Null |

# cfgLDAP

This group allows you to configure settings related to the Lightweight Directory Access Protocol (LDAP).

The following sections provides information about the objects in the **cfgLDAP** group.

## cfgLdapEnable (Read/Write)

| | |
|---|---|
| **Description** | Turns LDAP service on or off. |
| **Legal Values** | 1 (TRUE)—Enable LDAP Services<br>0 (FALSE)—Disable LDAP Services |
| **Default** | 0 |

## cfgLdapServer (Read/Write)

| | |
|---|---|
| **Description** | Configures the address of the LDAP Server. |
| **Legal Values** | String. Maximum length = 1024 |
| **Default** | Null |

## cfgLdapPort (Read/Write)

| | |
|---|---|
| **Description** | Port of LDAP over SSL. Non-SSL port is not supported. |
| **Legal Values** | 1 - 65535 |
| **Default** | 636 |

## cfgLdapBasedn (Read/Write)

| | |
|---|---|
| **Description** | The Domain Name of the branch of the directory where all searches should start from. |
| **Legal Values** | String. Maximum length = 254 |
| **Default** | Null |

### cfgLdapUserAttribute (Read/Write)

| | |
|---|---|
| **Description** | Specifies the user attribute to search for. If not configured, the default is to use uid. It is recommended to be unique within the chosen baseDN, otherwise a search filter must be configured to ensure the uniqueness of the login user. If the user DN cannot be uniquely identified, login will fail with anerror. |
| **Legal Values** | String. Maximum length = 254 |
| **Default** | Null<br>*uid* if not configured. |

### cfgLdapGroupAttribute (Read/Write)

| | |
|---|---|
| **Description** | Specify which LDAP attribute is used to check for group membership. This should be an attribute of the group class. If not specified, then iDRAC6 uses the member and unique member attributes. |
| **Legal Values** | String. Maximum length = 254 |
| **Default** | Null |

### cfgLdapGroupAttributeIsDN (Read/Write)

| | |
|---|---|
| **Description** | When it is set to 1, iDRAC6 compares the userDN retrieved from the directory to compare to the members of the group; if it is set to 0, the user name provided by the login user will be used to compare to the members of the group. This does not impact the search algorithm for the bind. iDRAC6 always searches the userDN and uses the userDN to bind. |
| **Legal Values** | 1 (TRUE)—Use the *userDN* from the LDAP Server<br>0 (FALSE)—Use the *userDN* provided by the login user |
| **Default** | 1 |

### cfgLdapBinddn (Read/Write)

| | |
|---|---|
| **Description** | The distinguished name of a user used to bind to the server when searching for the login user's DN. If not provided, an anonymous bind is used. This is optional but is required if anonymous bind is not supported. |
| **Legal Values** | String. Maximum length = 254 |
| **Default** | Null |

### cfgLdapBindpassword (Write only)

| | |
|---|---|
| **Description** | A bind password to use in conjunction with the bind DN. The bind password is sensitive data, and should be properly protected. This is optional but is required if anonymous bind is not supported. |
| **Legal Values** | String. Maximum length = 254 |
| **Default** | Null |

### cfgLdapSearchFilter (Read/Write)

| | |
|---|---|
| **Description** | A valid LDAP search filter. This is used if the user attribute cannot uniquely identify the login user within the chosen baseDN. The search filter only applies to userDN search and not the group membership search. |
| **Legal Values** | String. Maximum length = 254 |
| **Default** | (objectclass=*)<br>Searches for all objects in tree. |

### cfgLDAPCertValidationEnable (Read/Write)

| | |
|---|---|
| **Description** | Controls certificate validation during SSL handshake. |
| **Legal Values** | 1 (TRUE)—iDRAC6 uses the CA certificate to validate the LDAP server certificate during SSL handshake.<br>0 (FALSE)—iDRAC6 skips the certificate validation step of SSL handshake. |
| **Default** | 1 |

# cfgLdapRoleGroup

This group allows the user to configure role groups for LDAP.

The following sections provides information about the objects in the **cfgLdapRoleGroup** group.

## cfgLdapRoleGroupIndex (Read Only)

| | |
|---|---|
| **Description** | This is the index value of the Role Group Object. |
| **Legal Values** | An integer between 1 and 5 |
| **Default** | <instance> |

## cfgLdapRoleGroupDN (Read/Write)

| | |
|---|---|
| **Description** | This is the Domain Name of the group in this index. |
| **Legal Values** | String. Maximum length = 1024 |
| **Default** | No default value |

## cfgLdapRoleGroupPrivilege (Read/Write)

| | |
|---|---|
| **Description** | A bit–mask defining the privileges associated with this particular group. |
| **Legal Values** | 0x00000000 to 0x000001ff |
| **Default** | 0x000 |

# cfgStandardSchema

This group contains parameters to configure the Active Directory standard schema settings.

The following sections provides information about the objects in the **cfgStandardSchema** group.

## cfgSSADRoleGroupIndex (Read Only)

| | |
|---|---|
| **Description** | Index of the Role Group as recorded in the Active Directory. |
| **Legal Values** | An integer between 1 and 5 |
| **Default** | <instance> |

## cfgSSADRoleGroupName (Read/Write)

| | |
|---|---|
| **Description** | Name of the Role Group as recorded in the Active Directory forest. |
| **Legal Values** | Any printable text string of up to 254 characters with no white space. |
| **Default** | <blank> |

## cfgSSADRoleGroupDomain (Read/Write)

| | |
|---|---|
| **Description** | Active Directory Domain in which the Role Group resides. |
| **Legal Values** | Any printable text string of up to 254 characters, with no white space. |
| **Default** | <blank> |

## cfgSSADRoleGroupPrivilege (Read/Write)

| | |
|---|---|
| **Description** | Use the bit mask numbers in Table 3-5 to set role-based authority privileges for a Role Group. |
| **Legal Values** | 0x00000000 to 0x000001ff |
| **Default** | <blank> |

**Table 3-5. Bit Masks for Role Group Privileges**

| Role Group Privilege | Bit Mask |
|---|---|
| Login to iDRAC | 0x00000001 |
| Configure iDRAC | 0x00000002 |
| Configure Users | 0x00000004 |
| Clear Logs | 0x00000008 |
| Execute Server Control Commands | 0x00000010 |
| Access Virtual Console | 0x00000020 |
| Access Virtual Media | 0x00000040 |
| Test Alerts | 0x00000080 |
| Execute Debug Commands | 0x00000100 |

# cfgIpmiSol

This group is used to configure the Serial Over LAN (SOL) capabilities of the system.

The following sections provides information about the objects in the **cfgIpmiSol** group.

## cfgIpmiSolEnable (Read/Write)

| | |
|---|---|
| **Description** | Enables or disables SOL. |
| **Legal Values** | 1 (TRUE)<br>0 (FALSE) |
| **Default** | 1 |

## cfgIpmiSolBaudRate (Read/Write)

| | |
|---|---|
| **Description** | The baud rate for serial communication over LAN. |
| **Legal Values** | 9600, 19200, 57600, 115200 |
| **Default** | 115200 |

### cfgIpmiSolMinPrivilege (Read/Write)

| | |
|---|---|
| **Description** | Specifies the minimum privilege level required for SOL access. |
| **Legal Values** | 2 (User)<br>3 (Operator)<br>4 (Administrator) |
| **Default** | 4 |

### cfgIpmiSolAccumulateInterval (Read/Write)

| | |
|---|---|
| **Description** | Specifies the typical amount of time that the iDRAC6 waits before transmitting a partial SOL character data packet. This value is 1-based 5ms increments. |
| **Legal Values** | 1 – 255 |
| **Default** | 10 |

### cfgIpmiSolSendThreshold (Read/Write)

| | |
|---|---|
| **Description** | The SOL threshold limit value. Specifies the maximum number of bytes to buffer before sending an SOL data packet. |
| **Legal Values** | 1 – 255 |
| **Default** | 255 |

## cfgIpmiLan

This group is used to configure the IPMI over LAN capabilities of the system.

The following sections provides information about the objects in the **cfgIpmiLan** group.

### cfgIpmiLanEnable (Read/Write)

| | |
|---|---|
| **Description** | Enables or disables the IPMI over LAN interface. |
| **Legal Values** | 1 (TRUE)<br>0 (FALSE) |
| **Default** | 0 |

### cfgIpmiLanPrivLimit (Read/Write)

| | |
|---|---|
| **Description** | Specifies the maximum privilege level allowed for IPMI over LAN access. |
| **Legal Values** | 2 (User)<br>3 (Operator)<br>4 (Administrator) |
| **Default** | 4 |

### cfgIpmiLanAlertEnable (Read/Write)

| | |
|---|---|
| **Description** | Enables or disables global e-mail alerting. This property overrides all individual e-mail alerting enable/disable properties. |
| **Legal Values** | 1 (TRUE)<br>0 (FALSE) |
| **Default** | 0 |

### cfgIpmiEncryptionKey (Read/Write)

| | |
|---|---|
| **Description** | The IPMI encryption key. |
| **Legal Values** | A string of hexadecimal digits from 0 to 40 characters with no spaces. Only an even amount of digits is allowed. |
| **Default** | 00000000000000000000000000000000000000000 |

### cfgIpmiPetCommunityName (Read/Write)

| | |
|---|---|
| **Description** | The SNMP community name for traps. |
| **Legal Values** | A string of up to 18 characters. |
| **Default** | public |

# cfgIpmiPetIpv6

This group is used to configure IPv6 platform event traps on the managed server.

The following sections provides information about the objects in the **cfgIpmiPetIpv6** group.

### cfgIpmiPetIPv6Index (Read Only)

| | |
|---|---|
| **Description** | Unique identifier for the index corresponding to the trap. |
| **Legal Values** | 1 – 4 |
| **Default** | <index value> |

### cfgIpmiPetIPv6AlertDestIpAddr

| | |
|---|---|
| **Description** | Configures the IPv6 alert destination IP address for the trap. |
| **Legal Values** | IPv6 address |
| **Default** | <blank> |

### cfgIpmiPetIPv6AlertEnable (Read/Write)

| | |
|---|---|
| **Description** | Enables or disables the IPv6 alert destination for the trap. |
| **Legal Values** | 1 (TRUE)<br>0 (FALSE) |
| **Default** | 0 |

# cfgIpmiPef

This group is used to configure the platform event filters available on the managed server.

The event filters can be used to control policy related to actions that are triggered when critical events occur on the managed server.

The following sections provides information about the objects in the **cfgIpmiPef** group.

### cfgIpmiPefName (Read Only)

| | |
|---|---|
| **Description** | Specifies the name of the platform event filter. |
| **Legal Values** | A string of up to 255 characters |
| **Default** | The name of the index filter |

### cfgIpmiPefIndex (Read/Write)

| | |
|---|---|
| **Description** | Specifies the index of a specific platform event filter. |
| **Legal Values** | For iDRAC6 on Rack and Tower Servers: 1 – 22<br>For iDRAC6 Enterprise on Blade Servers: 1-9 |
| **Default** | The index value of a platform event filter object. |

### cfgIpmiPefAction (Read/Write)

| | |
|---|---|
| **Description** | Specifies the action that is performed on the managed server when the alert is triggered.<br>**NOTE:** For iDRAC6 on Rack and Tower servers, this object is read-only for indexes 20, 21, and 22. |
| **Legal Values** | 0 (None)<br>1 (Power Down)<br>2 (Reset)<br>3 (Power Cycle) |
| **Default** | 0 |

### cfgIpmiPefEnable (Read/Write)

| | |
|---|---|
| **Description** | Enables or disables a specific platform event filter. |
| **Legal Values** | 1 (TRUE)<br>0 (FALSE) |
| **Default** | 1 |

# cfgIpmiPet

This group is used to configure platform event traps on the managed server.

The following sections provides information about the objects in the **cfgIpmiPet** group.

## cfgIpmiPetIndex (Read Only)

| | |
|---|---|
| **Description** | Unique identifier for the index corresponding to the trap. |
| **Legal Values** | 1-4 |
| **Default** | The index value of a specific platform event trap. |

## cfgIpmiPetAlertDestIpAddr (Read/Write)

| | |
|---|---|
| **Description** | Specifies the destination IPv4 address for the trap receiver on the network. The trap receiver receives an SNMP trap when an event is triggered on the managed server. |
| **Legal Values** | A string representing a valid IPv4 address. For example, `192.168.0.67`. |
| **Default** | 0.0.0.0 |

## cfgIpmiPetAlertEnable (Read/Write)

| | |
|---|---|
| **Description** | Enables or disables a specific trap. |
| **Legal Values** | 1 (TRUE)<br>0 (FALSE) |
| **Default** | 0 |

# cfgUserDomain

This group is used to configure the Active Directory user domain names. A maximum of 40 domain names can be configured at any given time.

The following sections provides information about the objects in the **cfgUserDomain** group.

### cfgUserDomainIndex (Read Only)

| | |
|---|---|
| **Description** | Represents a specific domain. |
| **Legal Values** | 1 – 40 |
| **Default** | The index value |

### cfgUserDomainName (Read Only)

| | |
|---|---|
| **Description** | Specifies the Active Directory user domain name. |
| **Legal Values** | A string of up to 255 ASCII characters. |
| **Default** | <blank> |

# cfgServerPower

This group provides several power management features.

The following sections provides information about the objects in the **cfgServerPower** group.

### cfgServerPowerStatus (Read Only)

| | |
|---|---|
| **Description** | Represents the server power state, either ON or OFF. |
| **Legal Values** | 1 (ON)<br>0 (OFF) |
| **Default** | 0 |

### cfgServerPowerAllocation (Read Only)

**NOTE:** This object is applicable only for iDRAC6 on Rack and Tower Servers and not for iDRAC6 Enterprise on Blade Servers.

| | |
|---|---|
| **Description** | Represents the available allocated power supply for server usage.<br>**NOTE:** In case of more than one power supply, this object represents the minimum capacity power supply. |
| **Legal Values** | A string of up to 32 characters. |
| **Default** | <blank> |

### cfgServerActualPowerConsumption (Read Only)

| | |
|---|---|
| **Description** | Represents the power consumed by the server at the current time. |
| **Legal Values** | A string of up to 32 characters. |
| **Default** | <blank> |

### cfgServerPowerCapEnable (Read Only)

**NOTE:** This object is applicable only for iDRAC6 on Rack and Tower Servers and not for iDRAC6 Enterprise on Blade Servers.

| | |
|---|---|
| **Description** | Enables or disables the user specified power budget threshold. |
| **Legal Values** | 0<br>1 |
| **Default** | 1 |

### cfgServerMinPowerCapacity (Read Only)

**NOTE:** This object is applicable only for iDRAC6 on Rack and Tower Servers and not for iDRAC6 Enterprise on Blade Servers.

| | |
|---|---|
| **Description** | Represents the minimum server power capacity. |
| **Legal Values** | A string of up to 32 characters. |
| **Default** | <blank> |

### cfgServerMaxPowerCapacity (Read Only)

**NOTE:** This object is applicable only for iDRAC6 on Rack and Tower Servers and not for iDRAC6 Enterprise on Blade Servers.

| | |
|---|---|
| **Description** | Represents the maximum server power capacity. |
| **Legal Values** | A string of up to 32 characters. |
| **Default** | <blank> |

### cfgServerPeakPowerConsumption (Read Only)

| | |
|---|---|
| **Description** | Represents the maximum power consumed by the server until the current time. |
| **Legal Values** | A string of up to 32 characters. |
| **Default** | <current server peak power consumption> |

### cfgServerPeakPowerConsumptionTimestamp (Read Only)

| | |
|---|---|
| **Description** | Time when the maximum power consumption was recorded. |
| **Legal Values** | A string of up to 32 characters. |
| **Default** | Maximum power consumption timestamp. |

### cfgServerPowerConsumptionClear (Write Only)

| | |
|---|---|
| **Description** | Resets the cfgServerPeakPowerConsumption (Read/Write) property to 0 and the cfgServerPeakPowerConsumptionTimestamp property to the current iDRAC time. |
| **Legal Values** | 1 (TRUE)<br>0 (FALSE) |
| **Default** | ******* |

### cfgServerPowerCapWatts (Read/Write)

| | |
|---|---|
| **Description** | Represents the server power threshold in Watts. |
| **Legal Values** | A string of up to 32 characters. |
| **Default** | Server power threshold in Watts. |

### cfgServerPowerCapBtuhr (Read/Write)

| | |
|---|---|
| **Description** | Represents the server power threshold in BTU/hr. |
| **Legal Values** | A string of up to 32 characters. |
| **Default** | Server power threshold in BTU/hr. |

### cfgServerPowerCapPercent (Read/Write)

| | |
|---|---|
| **Description** | Represents the server power threshold in percentage. |
| **Legal Values** | A string of up to 32 characters. |
| **Default** | Server power threshold in percentage. |

### cfgServerPowerLastMinAvg (Read Only)

| | |
|---|---|
| **Description** | Displays the average power value during the last minute. |
| **Legal Values** | A string of up to 32 characters. |
| **Default** | Average power value during the last minute. |

### cfgServerPowerLastHourAvg (Read Only)

| | |
|---|---|
| **Description** | Displays the average power value during the last hour. |
| **Legal Values** | A string of up to 32 characters. |
| **Default** | Average power value during the last hour. |

### cfgServerPowerLastDayAvg (Read Only)

| | |
|---|---|
| **Description** | Displays the average power value during the last day. |
| **Legal Values** | A string of up to 32 characters. |
| **Default** | Average power value during the last day. |

### cfgServerPowerLastWeekAvg (Read Only)

| | |
|---|---|
| **Description** | Displays the average power value during the last week. |
| **Legal Values** | A string of up to 32 characters. |
| **Default** | Average power value during the last week. |

### cfgServerPowerLastHourMinPower (Read Only)

| | |
|---|---|
| **Description** | Displays the minimum power value during the last hour. |
| **Legal Values** | A string of up to 32 characters. |
| **Default** | Minimum power value during the last hour. |

### cfgServerPowerLastHourMinTime (Read Only)

| | |
|---|---|
| **Description** | Displays the timestamp of minimum power value during the last minute. |
| **Legal Values** | A string of up to 32 characters.<br>Time in the format: DD MM Date YYYY HH:MM:SS<br>where,<br>• DD= Day of the week<br>• MM= Month<br>• Date=Date<br>• YYYY = Year<br>• HH = hour<br>• MM=Minutes<br>• SS = Seconds |
| **Default** | Minimum power value during the last minute. |

### cfgServerPowerLastHourMaxPower (Read Only)

| | |
|---|---|
| **Description** | Displays the maximum power value during the last hour. |
| **Legal Values** | A string of up to 32 characters. |
| **Default** | Maximum power value during the last hour. |

### cfgServerPowerLastHourMaxTime (Read Only)

| | |
|---|---|
| **Description** | Displays the timestamp of maximum power value during the last hour. |
| **Legal Values** | A string of up to 32 characters.<br>Time in the format: DD MM Date YYYY HH:MM:SS<br>where,<br>• DD= Day of the week<br>• MM= Month<br>• Date=Date<br>• YYYY = Year<br>• HH = hour<br>• MM=Minutes<br>• SS = Seconds |
| **Default** | Maximum power value during the last hour. |

### cfgServerPowerLastDayMinPower (Read Only)

| | |
|---|---|
| **Description** | Displays the minimum power value during the last day. |
| **Legal Values** | A string of up to 32 characters. |
| **Default** | Minimum power value during the last day. |

### cfgServerPowerLastDayMinTime (Read Only)

| | |
|---|---|
| **Description** | Displays the timestamp of minimum power value during the last day. |
| **Legal Values** | A string of up to 32 characters.<br>Time in the format: DD MM Date YYYY HH:MM:SS<br>where,<br>• DD = Day of the week<br>• MM= Month<br>• Date=Date<br>• YYYY = Year<br>• HH = hour<br>• MM=Minutes<br>• SS = Seconds |
| **Default** | Minimum power value during the last day. |

### cfgServerPowerLastDayMaxPower (Read Only)

| | |
|---|---|
| **Description** | Displays the maximum power value during the last day. |
| **Legal Values** | A string of up to 32 characters. |
| **Default** | Maximum power value during the last day. |

### cfgServerPowerLastDayMaxTime (Read Only)

| | |
|---|---|
| **Description** | Displays the timestamp of maximum power value during the last day. |
| **Legal Values** | A string of up to 32 characters.<br>Time in the format: DD MM Date YYYY HH:MM:SS<br>where,<br>• DD = Day of the week<br>• MM= Month<br>• Date=Date<br>• YYYY = Year<br>• HH = hour<br>• MM=Minutes<br>• SS = Seconds |
| **Default** | Maximum power value during the last day. |

### cfgServerPowerLastWeekMinPower (Read Only)

| | |
|---|---|
| **Description** | Displays the minimum power value during the last week. |
| **Legal Values** | A string of up to 32 characters. |
| **Default** | Minimum power value during the last week. |

### cfgServerPowerLastWeekMinTime (Read Only)

| | |
|---|---|
| **Description** | Displays the timestamp of minimum power value during the last week. |
| **Legal Values** | A string of up to 32 characters.<br>Time in the format: DD MM Date YYYY HH:MM:SS<br>where,<br>• DD = Day of the week<br>• MM= Month<br>• Date=Date<br>• YYYY = Year<br>• HH = hour<br>• MM=Minutes<br>• SS = Seconds |
| **Default** | Minimum power value during the last week |

### cfgServerPowerLastWeekMaxPower (Read Only)

| | |
|---|---|
| **Description** | Displays the maximum power value during the last week. |
| **Legal Values** | A string of up to 32 characters. |
| **Default** | Maximum power value during the last week. |

### cfgServerPowerLastWeekMaxTime (Read Only)

| | |
|---|---|
| **Description** | Displays the timestamp of maximum power value during the last week. |
| **Legal Values** | A string of up to 32 characters.<br>Time in the format: DD MM Date YYYY HH:MM:SS<br>where,<br>• DD = Day of the week<br>• MM= Month<br>• Date=Date<br>• YYYY = Year<br>• HH = hour<br>• MM=Minutes<br>• SS = Seconds |
| **Default** | Maximum power value during the last week. |

### cfgServerPowerInstHeadroom (Read Only)

**NOTE:** This object is applicable only for iDRAC6 on Rack and Tower Servers and not for iDRAC6 Enterprise on Blade Servers.

| | |
|---|---|
| **Description** | Displays the difference between the available power and the current power consumption. |
| **Legal Values** | A string of up to 32 characters. |
| **Default** | Difference between the available power and the current power consumption. |

### cfgServerPowerPeakHeadroom (Read Only)

**NOTE:** This object is applicable only for iDRAC6 on Rack and Tower Servers and not for iDRAC6 Enterprise on Blade Servers.

| | |
|---|---|
| **Description** | Displays the difference between the available power and the peak power consumption. |
| **Legal Values** | A string of up to 32 characters. |
| **Default** | Difference between the available power and the peak power consumption. |

### cfgServerActualAmperageConsumption (Read Only)

| | |
|---|---|
| **Description** | Displays the current power consumption. |
| **Legal Values** | A string of up to 32 characters. |
| **Default** | Current power consumption. |

### cfgServerPeakAmperage (Read Only)

| | |
|---|---|
| **Description** | Displays the current peak power consumption. |
| **Legal Values** | A string of up to 32 characters. |
| **Default** | Current peak power consumption. |

### cfgServerPeakAmperageTimeStamp (Read Only)

| | |
|---|---|
| **Description** | Displays the timestamp of the current peak power consumption. |
| **Legal Values** | A string of up to 32 characters.<br>Time in the format: DD MM Date YYYY HH:MM:SS<br>where,<br>• DD = Day of the week<br>• MM= Month<br>• Date=Date<br>• YYYY = Year<br>• HH = hour<br>• MM=Minutes<br>• SS = Seconds |
| **Default** | Timestamp of the current peak power consumption. |

### cfgServerCumulativePowerConsumption (Read Only)

| | |
|---|---|
| **Description** | Displays the cumulative power consumption. |
| **Legal Values** | A string of up to 32 characters. |
| **Default** | Cumulative power consumption. |

### cfgServerCumulativePowerConsumptionTimeStamp (Read Only)

| | |
|---|---|
| **Description** | Displays the timestamp of the cumulative power consumption. |
| **Legal Values** | A string of up to 32 characters.<br>Time in the format: DD MM Date YYYY HH:MM:SS<br>where,<br>• DD = Day of the week<br>• MM= Month<br>• Date=Date<br>• YYYY = Year<br>• HH = hour<br>• MM=Minutes<br>• SS = Seconds |
| **Default** | Timestamp of the cumulative power consumption. |

### cfgServerCumulativePowerClear (Write Only)

| | |
|---|---|
| **Description** | Clears the **cfgServerCumulativePowerConsumption** and **cfgServerCumulativePowerConsumptionTimeStamp** values. |
| **Legal Values** | A string of up to 32 characters. |
| **Default** | No default value |

### cfgServerPeakPowerClear (Write Only)

| | |
|---|---|
| **Description** | Clears the **cfgServerPeakPowerConsumption** and **cfgServerPeakPowerConsumptionTimestamp** values. |
| **Legal Values** | A string of up to 32 characters. |
| **Default** | No default value |

### cfgServerPowerPCIeAllocation (Read/Write)

**NOTE:** This object is applicable for iDRAC6 Enterprise only for specific Blade Servers and not for iDRAC6 on Rack and Tower Servers.

**NOTE:** You must have Administrator privileges to modify the value for this object.

| | |
|---|---|
| **Description** | Amount of power allocated to the PCIe cards. |
| **Legal Values** | 0W: For platforms that do not support PCIe cards.<br>100W - 500W: For platforms that support PCIe cards. |
| **Default** | 0: For platforms that do not support PCIe cards.<br>500W: For platforms that support PCIe cards. |

## cfgServerPowerSupply

This group contains information related to the power supplies. The following sections provides information about the objects in the **cfgServerPowerSupply** group.

**NOTE:** The **cfgServerPowerSupply** object group is applicable only for iDRAC6 on Rack and Tower Servers and not for iDRAC6 Enterprise on Blade Servers.

**NOTE:** The **getconfig** subcommand will always show eight **cfgServerPowerSupply** indexes, even if two power supplies are installed in the system or the system supports a maximum of two power supply units. For the uninstalled and unsupported units, all the objects in the **cfgServerPowerSupply** group displays a value of 0.

### cfgServerPowerSupplyIndex

| | |
|---|---|
| **Description** | Index of the power supply unit. |
| **Legal Values** | Integer from 1-8 |
| **Default** | No default value |

**NOTE:** Indexes from 1 – 8 are supported to support up to 8 power supply units. If any power supply unit is not present, **cfgServerPowerSupplyOnlineStatus** is absent and for all the other properties, it is **0**.

### cfgServerPowerSupplyMaxInputPower (Read Only)

| | |
|---|---|
| **Description** | Displays the AC input rated power in Watts. |
| **Legal Values** | A string of up to 32 characters. |
| **Default** | 0 |

### cfgServerPowerSupplyMaxOutputPower (Read Only)

| | |
|---|---|
| **Description** | Displays the AC output rated power in Watts. |
| **Legal Values** | A string of up to 32 characters. |
| **Default** | 0 |

### cfgServerPowerSupplyOnlineStatus (Read Only)

| | |
|---|---|
| **Description** | Displays the status of the power supply unit. |
| **Legal Values** | • 0 - Present<br>• 1 - Absent<br>• 2 - Failure<br>• 3 - Predictive failure |
| **Default** | 0 |

### cfgServerPowerSupplyFwVer (Read Only)

| | |
|---|---|
| **Description** | Displays the firmware version of the power supply unit. |
| **Legal Values** | A string up to 8 characters. |
| **Default** | Null |

### cfgServerPowerSupplyCurrentDraw (Read Only)

| | |
|---|---|
| **Description** | Displays the instantaneous current consumption in 0.1 Amps. |
| **Legal Values** | A string of up to 32 characters. |
| **Default** | 0 |

### cfgServerPowerSupplyType

| | |
|---|---|
| **Description** | Displays whether the power supply is AC or DC. |
| **Legal Values** | A string of up to 32 characters. |
| **Default** | 0 |

## cfgIPv6LanNetworking

This group is used to configure the IPv6 over LAN networking capabilities.

The following sections provides information about the objects in the **cfgIPv6LanNetworking** group.

### cfgIPv6Enable (Read/Write)

| | |
|---|---|
| **Description** | Enables or disables the iDRAC6 IPv6 stack. |
| **Legal Values** | 1 (TRUE)<br>0 (FALSE) |
| **Default** | 0 |

### cfgIPv6Address1 (Read/Write)

| | |
|---|---|
| **Description** | iDRAC6 IPv6 address. |
| **Legal Values** | String representing a valid IPv6 entry. |
| **Default** | :: |

### cfgIPv6Gateway (Read/Write)

| | |
|---|---|
| **Description** | iDRAC6 gateway IPv6 address. |
| **Legal Values** | String representing a valid IPv6 entry. |
| **Default** | :: |

### cfgIPv6PrefixLength (Read/Write)

| | |
|---|---|
| **Description** | The prefix length for iDRAC6 IPv6 address 1. |
| **Legal Values** | 1-128 |
| **Default** | 64 |

### cfgIPv6AutoConfig (Read/Write)

| | |
|---|---|
| **Description** | Enables or disables the IPv6 Auto Config option. |
| **Legal Values** | 1 (TRUE)<br>0 (FALSE) |
| **Default** | 0 |

### cfgIPv6LinkLocalAddress (Read Only)

| | |
|---|---|
| **Description** | The iDRAC6 IPv6 link local address. |
| **Legal Values** | A string representing a valid IPv6 entry. |
| **Default** | :: |

### cfgIPv6Address2 (Read Only)

| | |
|---|---|
| **Description** | An iDRAC6 IPv6 address. |
| **Legal Values** | A string representing a valid IPv6 entry. |
| **Default** | :: |

### cfgIPv6Address3 (Read Only)

| | |
|---|---|
| **Description** | iDRAC6 IPv6 address. |
| **Legal Values** | String representing a valid IPv6 entry. |
| **Default** | <blank> |

### cfgIPv6Address4 (Read Only)

| | |
|---|---|
| **Description** | iDRAC6 IPv6 address. |
| **Legal Values** | String representing a valid IPv6 entry. |
| **Default** | <blank> |

### cfgIPv6Address5 (Read Only)

| | |
|---|---|
| **Description** | iDRAC6 IPv6 address. |
| **Legal Values** | String representing a valid IPv6 entry. |
| **Default** | <blank> |

### cfgIPv6Address6 (Read Only)

| | |
|---|---|
| **Description** | iDRAC6 IPv6 address. |
| **Legal Values** | String representing a valid IPv6 entry. |
| **Default** | <blank> |

### cfgIPv6Address7 (Read Only)

| | |
|---|---|
| **Description** | iDRAC6 IPv6 address. |
| **Legal Values** | String representing a valid IPv6 entry. |
| **Default** | <blank> |

### cfgIPv6Address8 (Read Only)

| | |
|---|---|
| **Description** | iDRAC6 IPv6 address. |
| **Legal Values** | String representing a valid IPv6 entry. |
| **Default** | <blank> |

### cfgIPv6Address9 (Read Only)

| | |
|---|---|
| **Description** | iDRAC6 IPv6 address. |
| **Legal Values** | String representing a valid IPv6 entry. |
| **Default** | <blank> |

### cfgIPv6Address10 (Read Only)

| | |
|---|---|
| **Description** | iDRAC6 IPv6 address. |
| **Legal Values** | String representing a valid IPv6 entry. |
| **Default** | <blank> |

### cfgIPv6Address11 (Read Only)

| | |
|---|---|
| **Description** | iDRAC6 IPv6 address. |
| **Legal Values** | String representing a valid IPv6 entry. |
| **Default** | <blank> |

### cfgIPv6Address12 (Read Only)

| | |
|---|---|
| **Description** | iDRAC6 IPv6 address. |
| **Legal Values** | String representing a valid IPv6 entry. |
| **Default** | <blank> |

### cfgIPv6Address13 (Read Only)

| | |
|---|---|
| **Description** | iDRAC6 IPv6 address. |
| **Legal Values** | String representing a valid IPv6 entry. |
| **Default** | <blank> |

### cfgIPv6Address14 (Read Only)

| | |
|---|---|
| **Description** | iDRAC6 IPv6 address. |
| **Legal Values** | String representing a valid IPv6 entry. |
| **Default** | <blank> |

### cfgIPv6Address15 (Read Only)

| | |
|---|---|
| **Description** | iDRAC6 IPv6 address. |
| **Legal Values** | String representing a valid IPv6 entry. |
| **Default** | <blank> |

### cfgIPv6DNSServersFromDHCP6 (Read/Write)

| | |
|---|---|
| **Description** | Specifies whether cfgIPv6DNSServer1 and cfgIPv6DNSServer2 are static or DHCP IPv6 addresses. |
| **Legal Values** | 1 (TRUE)<br>0 (FALSE) |
| **Default** | 0 |

### cfgIPv6DNSServer1 (Read/Write)

| | |
|---|---|
| **Description** | An IPv6 DNS server address. |
| **Legal Values** | A string representing a valid IPv6 entry. |
| **Default** | :: |

### cfgIPv6DNSServer2 (Read/Write)

| | |
|---|---|
| **Description** | An IPv6 DNS server address. |
| **Legal Values** | A string representing a valid IPv6 entry. |
| **Default** | :: |

# cfgIPv6URL

This group specifies properties used to configure the iDRAC6 IPv6 URL.

The following sections provides information about the objects in the **cfgIPv6URL** group.

### cfgIPv6URLstring (Read Only)

| | |
|---|---|
| **Description** | The iDRAC6 IPv6 URL. |
| **Legal Values** | A string of up to 80 characters. |
| **Default** | <blank> |

# cfgIpmiSerial

This group specifies properties used to configure the IPMI serial interface of the BMC.

**NOTE:** The **cfgIpmiSerial** object group is applicable only for iDRAC6 on Rack and Tower Servers and not for iDRAC6 Enterprise on Blade Servers.

### cfgIpmiSerialBaudRate (Read/Write)

| | |
|---|---|
| **Description** | Specifies the baud rate for a serial connection over IPMI. |
| **Legal Values** | 9600, 19200, 57600, 115200 |
| **Default** | 57600 |

### cfgIpmiSerialConnectionMode (Read/Write)

| | |
|---|---|
| **Description** | When the iDRAC6 **cfgSerialConsoleEnable** property is set to 0 (disabled), the iDRAC6 serial port becomes the IPMI serial port. This property determines the IPMI defined mode of the serial port.<br>In Basic mode, the port uses binary data with the intent of communicating with an application program on the serial client. In Terminal mode, the port assumes that a dumb ASCII terminal is connected and allows very simple commands to be entered. |
| **Legal Values** | 0 (Terminal)<br>1 (Basic) |
| **Default** | 1 |

### cfgIpmiSerialChanPrivLimit (Read/Write)

| | |
|---|---|
| **Description** | Specifies the maximum privilege level allowed on the IPMI serial channel. |
| **Legal Values** | 2 (User)<br>3 (Operator)<br>4 (Administrator) |
| **Default** | 4 |

### cfgIpmiSerialFlowControl (Read/Write)

| | |
|---|---|
| **Description** | Specifies the flow control setting for the IPMI serial port. |
| **Legal Values** | 0 (None)<br>1 (CTS/RTS) |
| **Default** | 1 |

### cfgIpmiSerialHandshakeControl (Read/Write)

| | |
|---|---|
| **Description** | Enables or disables the IPMI terminal mode handshake control. |
| **Legal Values** | 0 (FALSE)<br>1 (TRUE) |
| **Default** | 1 |

### cfgIpmiSerialLineEdit (Read/Write)

| | |
|---|---|
| **Description** | Enables or disables line editing on the IPMI serial interface. |
| **Legal Values** | 0 (FALSE)<br>1 (TRUE) |
| **Default** | 1 |

### cfgIpmiSerialEchoControl (Read/Write)

| | |
|---|---|
| **Description** | Enables or disables echo control on the IPMI serial interface. |
| **Legal Values** | 0 (FALSE)<br>1 (TRUE) |
| **Default** | 1 |

### cfgIpmiSerialDeleteControl (Read/Write)

| | |
|---|---|
| **Description** | Enables or disables delete control on the IPMI serial interface. |
| **Legal Values** | 0 (FALSE)<br>1 (TRUE) |
| **Default** | 0 |

### cfgIpmiSerialNewLineSequence (Read/Write)

| | |
|---|---|
| **Description** | Specifies the newline sequence specification for the IPMI serial interface. |
| **Legal Values** | 0 (None)<br>1 (CR-LF)<br>2 (NULL)<br>3 (<CR>)<br>4 (<LF-CR>)<br>5 (<LF>) |
| **Default** | 1 |

### cfgIpmiSerialInputNewLineSequence (Read/Write)

| | |
|---|---|
| **Description** | Specifies the input newline sequence specification for the IPMI serial interface. |
| **Legal Values** | 1, 2 |
| **Default** | 1 |

# cfgSmartCard

This group specifies properties used to support access to iDRAC6 using a smart card.

The following sections provides information about the objects in the **cfgSmartCard** group.

## cfgSmartCardLogonEnable (Read/Write)

| | |
|---|---|
| **Description** | Enables, disables, or enables with Remote RACADM support for access to iDRAC6 using a smart card.<br>**NOTE:** Enabling with remote RACADM is only applicable for iDRAC6 on Rack and Tower Servers. |
| **Legal Values** | 0 (Disabled)<br>1 (Enabled)<br>2 (Enabled with Remote RACADM) - This is not applicable for iDRAC6 Enterprise on Blade Servers. |
| **Default** | 0 |

## cfgSmartCardCRLEnable (Read/Write)

**NOTE:** This object is applicable only for iDRAC6 on Rack and Tower Servers and not for iDRAC6 Enterprise on Blade Servers.

| | |
|---|---|
| **Description** | Enables or disables the Certificate Revocation List (CRL). |
| **Legal Values** | 1 (TRUE)<br>0 (FALSE) |
| **Default** | 0 |

# cfgNetTuning

This group enables users to configure the advanced network interface parameters for the RAC NIC. When configured, the updated settings may take up to a minute to become active.

The following sections provides information about the objects in the **cfgNetTuning** group.

**NOTE:** The **cfgNetTuning** object group is applicable only for iDRAC6 on Rack and Tower Servers and not for iDRAC6 Enterprise on Blade Servers.

**CAUTION: Use extra precaution when modifying properties in this group. Inappropriate modification of the properties in this group can result in your RAC NIC become inoperable.**

## cfgNetTuningNicAutoneg (Read/Write)

| | |
|---|---|
| **Description** | Enables autonegotiation of physical link speed and duplex. If enabled, autonegotiation takes priority over values set in the **cfgNetTuningNic100MB** and **cfgNetTuningNicFullDuplex** objects. |
| **Legal Values** | 1 (TRUE)<br>0 (FALSE) |
| **Default** | 1 |

## cfgNetTuningNic100MB (Read/Write)

| | |
|---|---|
| **Description** | Specifies the speed to use for the RAC NIC. This property is not used if the **cfgNetTuningNicAutoNeg** is set to 1 (enabled). |
| **Legal Values** | 0 (10 MBit)<br>1 (100 MBit) |
| **Default** | 1 |

### cfgNetTuningNicFullDuplex (Read/Write)

| | |
|---|---|
| **Description** | Specifies the duplex setting for the RAC NIC. This property is not used if the **cfgNetTuningNicAutoNeg** is set to 1 (enabled). |
| **Legal Values** | 0 (Half Duplex)<br>1 (Full Duplex) |
| **Default** | 1 |

### cfgNetTuningNicMtu (Read/Write)

| | |
|---|---|
| **Description** | The size in bytes of the maximum transmission unit used by the iDRAC6 NIC. |
| **Legal Values** | 576 – 1500 |
| **Default** | 1500 |

## cfgSensorRedundancy

This group is used to set the power supply redundancy.

The following sections provides information about the objects in the **cfgSensorRedundancy** group.

**NOTE:** The **cfgSensorRedundancy** object group is applicable only for iDRAC6 on Rack and Tower Servers and not for iDRAC6 Enterprise on Blade Servers.

### cfgSensorRedundancyIndex (Read Only)

| | |
|---|---|
| **Description** | Index for the sensor redundancy group being read. Only power supply redundancy is supported. |
| **Legal Values** | 1 |
| **Default** | No default value |

### cfgSensorRedundancyPolicy (Read/Write)

| | |
|---|---|
| **Description** | Sets the power supply redundancy policy. |
| **Legal Values** | 2 - N/A, for sytems that are not supported<br>3 - Non Redundant<br>4 - 1+1 Redundant<br>4 - 2+1 Redundant<br>16 - 2+2 Redundant |
| **Default** | 0 |

### cfgSensorRedundancyCapabilities (Read Only)

| | |
|---|---|
| **Description** | Returns the redundancy capabilities in the form of a bitmask. This bitmask allows the user to know which values can be set for cfgSensorRedundancyPolicy. |
| **Legal Values** | A bit mask. More than 1-bit can be set at a time to indicate multiple redundancy support.<br>0- N/A, for sytems that are not supported<br>1- Non Redundant<br>2- 1+1 - Redundant<br>4- 2+1 - Redundant<br>8- 2+2 - Redundant |
| **Default** | 0 |

### cfgSensorRedundancyStatus (Read Only)

| | |
|---|---|
| **Description** | Indicates the redundancy status. The status is N/A on platforms that does not support the power supply sensor redundancy. |
| **Legal Values** | String:<br>• N/A<br>• Full<br>• Lost<br>• Degraded |
| **Default** | No default value |

## cfgVFlashSD

This group is used to configure the properties for the vFlash SD card.

The following sections provides information about the objects in the cfgVFlashSD group.

### cfgVFlashSDEnable (Read/Write)

| | |
|---|---|
| **Description** | Enables or disables the vFlash SD card. |
| **Legal Values** | 0 (vFlash is disabled)<br>1 (vFlash is enabled) |
| **Default** | 1 |

### cfgVFlashSDSize (Read Only)

| | |
|---|---|
| **Description** | Displays the size of the vFlash SD card in megabytes (MB). |
| **Legal Values** | A string of upto 64 characters. |
| **Default** | <card size> |

### cfgVFlashSDLicensed (Read Only)

| | |
|---|---|
| **Description** | Displays whether a SD card or vFlash SD card is inserted. The vFlash SD card supports the new enhanced vFlash features and the SD card supports only the limited vFlash features. |
| **Legal Values** | 0 (SD card is inserted)<br>1 (vFlash SD card is inserted) |
| **Default** | No default value |

### cfgVFlashSDAvailableSize (Read Only)

| | |
|---|---|
| **Description** | Displays the available space (in MB) on the vFlash SD card that can be used to create new partitions. |
| **Legal Values** | A string of up to 64 characters. |
| **Default** | If the card is not initialized, default is 0. If initialized, displays the unused space on the card. |

### cfgVFlashSDHealth (Read Only)

| | |
|---|---|
| **Description** | Displays the current health status of the vFlash SD card. |
| **Legal Values** | String:<br>• OK<br>• Warning<br>• Critical<br>• Unknown |
| **Default** | OK |

### cfgVFlashSDWriteProtect (Read Only)

| | |
|---|---|
| **Description** | Displays whether the physical write-protect latch on the vFlash SD card is enabled or disabled. |
| **Legal Values** | 0 (vFlash is not write-protected)<br>1 (vFlash is write-protected) |
| **Default** | No default value |

## cfgVFlashPartition

This group is used to configure properties for individual partitions on the vFlash SD Card. Up to 16 partitions are supported, indexed from 1 to 16.

**NOTE:** For SD cards, the index value is limited to 1 because only a single partition of size 256 MB is allowed.

The following sections provides information about the objects in the **cfgVFlashPartition** group.

### cfgVFlashPartitionIndex (ReadOnly)

| | |
|---|---|
| **Description** | Displays the size of the partition. |
| **Legal Values** | Integer from 1-16 |
| **Default** | No default value |

### cfgVFlashPartitionSize (ReadOnly)

| | |
|---|---|
| **Description** | The index value of the partition. |
| **Legal Values** | 1MB to 4 GB |
| **Default** | No default value |

### cfgVFlashPartitionEmulationType (ReadOnly)

| | |
|---|---|
| **Description** | Displays the emulation type for the partition. |
| **Legal Values** | String:<br>• HDD<br>• Floppy<br>• CDROM |
| **Default** | No default value |

### cfgVFlashPartitionOSVolLabel (ReadOnly)

| | |
|---|---|
| **Description** | Displays the label for the partition that is visible to the operating system. |
| **Legal Values** | An alphanumeric string of up to six characters. |
| **Default** | No default value |

### cfgVFlashPartitionFormatType (ReadOnly)

| | |
|---|---|
| **Description** | Displays the format type of the partition. |
| **Legal Values** | String:<br>• FAT16<br>• FAT32<br>• EXT2<br>• EXT3<br>• CD<br>• RAW |
| **Default** | No default value |

### cfgVFlashPartitionAccessType (Read/Write)

| | |
|---|---|
| **Description** | Indicates the partition access permissions. It configures the access type to read-write. |
| **Legal Values** | 0(Read-only)<br>1(Read-write) |
| **Default** | 0 |

### cfgVFlashPartitionAttachState (Read/Write)

| | |
|---|---|
| **Description** | Displays whether the partition is attached or detached. |
| **Legal Values** | 1 (Attached)<br>0 (Detached) |
| **Default** | 0 |

# 4

# Deprecated Commands, Groups, and Objects

This section provides information about the deprecated RACADM subcommands, groups, and objects in the current release. Few commands, groups, or objects are deprecated in RACADM either due to a new command or object replacing the functionality of an existing command or object, or the feature is no longer supported.

For the deprecated command or object:

- If you run the `racadm help` command, the deprecated command is not displayed in the command list.
- If you run the `racadm help <deprecated command name>`, then the following information is displayed:

  ```
  ATTENTION: <command name> is a deprecated command!

  While execution of this command will still be
  successful we strongly encourage you to use the
  new functionality.

  The functionality of this command is now covered
  by <list of new functionality>.

  Type "racadm help <new command name>" to learn
  more.
  ```

**NOTE:** This information is displayed only for iDRAC6 on Rack and Tower servers and is not displayed for iDRAC6 Enterprise on Blade servers.

- If you run a deprecated command, it will work if the feature is supported. If the feature is not supported, an error is not returned.
- If you run the `racadm getconfig -h` command, the deprecated group is not displayed in the results.

- If you query a deprecated group or object, then the values are returned.
- If you try to configure a deprecated group or object, the configuration succeeds.
- If you request a group that contains a deprecated object, the deprecated object is not displayed in the results.

Table 4-1 lists the RACADM subcommands deprecated in the current release.

**Table 4-1. RACADM Deprecated Subcommands**

| Subcommand | Replaced With |
|---|---|
| vmkey reset | vflashsd initialize |

Table 4-2 lists the RACADM groups and objects deprecated in the current release.

**Table 4-2. RACADM Deprecated Groups and Ob jects**

| Group/Object | Replaced With |
|---|---|
| cfgVirMediaKeyEnable | cfgVFlashSDEnable |
| cfgSDWriteProtect | cfgVFlashSDWriteProtect |

# Index

## S



## U