

Dell™ Remote Access Controller

# Installation and Setup Guide



## Notes, Notices, and Cautions



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



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



**CAUTION:** A CAUTION indicates a potentially hazardous situation which, if not avoided, may result in minor or moderate injury.

---

**Information in this document is subject to change without notice.**

**© 2003 Dell Inc. All rights reserved.**

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

Trademarks used in this text: *Dell*, the *DELL* logo, *Dell OpenManage*, *PowerEdge*, and *PowerVault* are trademarks of Dell Inc.; *Microsoft*, *Windows*, and *MS-DOS* are registered trademarks of Microsoft Corporation; *Novell* and *NetWare* are registered trademarks of Novell Corporation; *Red Hat* is a registered trademark of Red Hat, Inc.; *UNIX* is a registered trademark of The Open Group in the United States and other countries.

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

# Contents

1	Introduction	
	<b>Remote Access Controller Features</b>	<b>11</b>
	<b>Supported Operating Systems</b>	<b>12</b>
	<b>Supported Web Browsers</b>	<b>13</b>
	<b>Software Components</b>	<b>13</b>
	<b>RAC Configuration Interfaces</b>	<b>14</b>
	<b>Supported Remote Access Connections</b>	<b>14</b>
	<b>Remote Access Interfaces</b>	<b>15</b>
	<b>RAC Port Numbers</b>	<b>16</b>
	<b>RAC Event Alerts</b>	<b>17</b>
	<b>Remote Access Security Features</b>	<b>18</b>
	Network Adapter Connections	18
	RAC Web-based Interface Security	18
	<b>RAC User Types</b>	<b>18</b>
	RAC Users	18
	Operating System Users	19
	<b>Other Documents You May Need</b>	<b>19</b>
2	Getting Started With Your DRAC III	
	<b>DRAC III Features</b>	<b>21</b>
	DRAC III Security Features	22
	<b>DRAC III Kit Contents</b>	<b>22</b>
	<b>Supported Systems</b>	<b>22</b>
	<b>Supported Modems</b>	<b>23</b>
	<b>Installing the DRAC III Hardware</b>	<b>23</b>
	<b>Software Installation and Configuration Overview</b>	<b>26</b>

Updating the System BIOS . . . . .	27
Installing the Software on the Managed System . . . . .	27
Configuring the RAC Network Settings . . . . .	27
Adding and Configuring RAC Users. . . . .	27
Configuring the DRAC III Optional Modem . . . . .	28
Adding and Configuring Dial-in (PPP) Users . . . . .	28
Configuring Dial-Out Alert Notification on the Management Station . . . . .	28
Installing (or Upgrading) the Software on the Management Station . . . . .	28
Configuring the Management Station's Modem . . . . .	29
Configuring the Web Browser to Connect to the Remote Access Interface . . . . .	29
Connecting to the Remote Access Interface . . . . .	29
<b>DRAC III User Types and Feature Configuration . . . . .</b>	<b>29</b>
<b>Configuring Systems to Dial In to the DRAC III . . . . .</b>	<b>30</b>
Restrictions for Microsoft PPP Clients . . . . .	30
Configuring Systems Running Windows 95 and Windows 98 to Dial In to the DRAC III . . . . .	31
Configuring Systems Running Windows 2000 to Dial In to the DRAC III . . . . .	32
Configuring Systems Running Windows Server 2003 to Dial In to the DRAC III . . . . .	32
Configuring Systems Running the Red Hat Linux Operating System to Dial In to the DRAC III . . . . .	33
<b>Configuring Management Stations Running Windows to Receive DRAC III Dial-Out Alert Notifications . . . . .</b>	<b>35</b>
Configuring Management Stations Running Windows 2000 to Receive DRAC III Dial-Out Alert Notification . . . . .	35
Configuring Management Stations Running Windows Server 2003 to Receive DRAC III Dial-Out Alert Notification. . . . .	36
<b>Configuring the Management Station Dial-Up Modem for DRAC III . . . . .</b>	<b>36</b>
Configuring the Dial-Up Modem on Management Stations Running Windows 2000 Server . . . . .	36
Configuring the Dial-Up Modem on Management Stations Running Windows Server 2003 . . . . .	37
Configuring the Dial-Up Modem on Management Stations Running Windows XP . . . . .	37
<b>Accessing a DRAC III Through a Modem . . . . .</b>	<b>37</b>
Accessing the DRAC III Through a Modem From Systems Running Windows 95 or Windows 98 . . . . .	38
Accessing the DRAC III Through a Modem From Systems Running Windows 2000 Server . . . . .	38
Accessing the DRAC III Through a Modem From Systems Running Windows Server 2003 . . . . .	39

Accessing the DRAC III Through a Modem From Systems Running Windows Server XP . . . . .	39
Accessing the DRAC III Through a Modem From Systems Running Red Hat Linux . . . . .	40
<b>Accessing the DRAC III Remote Access Interface Using VT-100 Terminal Emulation</b>	<b>40</b>
<b>Uninstalling the DRAC III Hardware</b> . . . . .	<b>40</b>
<b>Replacing the DRAC III Battery</b> . . . . .	<b>40</b>
Removing the Battery Pack . . . . .	40
Installing a New Battery Pack . . . . .	41
. . . . .	41
<b>3 Getting Started With Your DRAC III/XT</b>	
<b>DRAC III/XT Features</b> . . . . .	<b>43</b>
<b>DRAC III/XT Kit Contents</b> . . . . .	<b>43</b>
<b>Supported Systems</b> . . . . .	<b>43</b>
<b>Installing the DRAC III/XT Hardware</b> . . . . .	<b>44</b>
<b>Software Installation and Configuration Overview</b> . . . . .	<b>45</b>
Updating the System BIOS . . . . .	46
Installing the Software on the Managed System . . . . .	46
Configuring the RAC Network Settings . . . . .	46
Adding and Configuring RAC Users . . . . .	46
Installing (or Upgrading) the Software on the Management Station . . . . .	47
Configuring the Web Browser to Connect to the Remote Access Interface . . . . .	47
Connecting to the Remote Access Interface . . . . .	47
<b>Uninstalling the DRAC III/XT Hardware</b> . . . . .	<b>47</b>
<b>4 Getting Started With Your ERA</b>	
<b>ERA Features</b> . . . . .	<b>49</b>
<b>Supported Systems</b> . . . . .	<b>49</b>
<b>Software Installation and Configuration Overview</b> . . . . .	<b>49</b>
Installing the Software on the Managed System . . . . .	50
Configuring the RAC Network Settings . . . . .	50
Adding and Configuring RAC Users . . . . .	50

Installing (or Upgrading) the Software on the Management Station . . . .	51
Configuring the Web Browser to Connect to the Remote Access Interface	51
Connecting to Your RAC . . . . .	51

## 5 Getting Started With Your ERA/O

<b>ERA/O Features</b> . . . . .	<b>53</b>
<b>ERA/O Kit Contents.</b> . . . . .	<b>53</b>
<b>Supported Systems.</b> . . . . .	<b>53</b>
<b>Installing the ERA/O Hardware</b> . . . . .	<b>54</b>
<b>Software Installation and Configuration Overview</b> . . . . .	<b>54</b>
Updating the System BIOS . . . . .	54
Installing the Software on the Managed System . . . . .	55
Installing (or Upgrading) the Software on the Management Station . . . .	55
Adding and Configuring RAC Users. . . . .	55
Configuring the RAC Network Settings . . . . .	55
Configuring the Web Browser to Connect to the Remote Access Interface	56
Connecting to the RAC . . . . .	56
<b>Uninstalling the ERA/O Hardware</b> . . . . .	<b>56</b>

## 6 Installing and Configuring the RAC Software

<b>Updating the System BIOS</b> . . . . .	<b>57</b>
<b>Installing DRAC III Drivers on 64-Bit Systems</b> . . . . .	<b>57</b>
<b>Installing the Racadm Utility on Management Stations Running the Red Hat Linux Operating System</b> . . . . .	<b>58</b>
<b>Configuring RAS PPP Connection.</b> . . . . .	<b>58</b>
Configuring RAS PPP Connection on Management Stations Running Windows XP or Windows Server 2003 . . . . .	59
The <b>Routing and Remote Access</b> service should start automatically on subsequent restarts of the management station. . . . .	59
Configuring RAS PPP Connection on Management Stations Running Windows 2000 . . . . .	59
Connecting to the Management Station From the DRAC III . . . . .	60
<b>Changing the PPP Server IP Address on the Managed System</b> . . . . .	<b>60</b>

<b>Configuring the RAC Network Settings Using the Option ROM</b> . . . . .	<b>60</b>
Option Categories . . . . .	61
<b>Configuring a Web Browser to Display the Remote Access Interface</b> . . . . .	<b>62</b>
Configuring Internet Explorer 5.5 or 6.0 . . . . .	63
Configuring Mozilla 1.3 or 1.4. . . . .	63
Configuring Netscape Navigator 7.01 or 7.02 . . . . .	64
<b>Disabling the Windows Automatic Reboot Option</b> . . . . .	<b>65</b>
Disabling the Automatic Reboot Option in Windows 2000 Server . . . . .	65
Disabling the Automatic Reboot Option in Windows Server 2003 . . . . .	65
<b>Connecting to the Remote Access Interface</b> . . . . .	<b>65</b>
Accessing the Remote Access Interface Through the Network . . . . .	65
<b>Updating Your Controller Firmware</b> . . . . .	<b>66</b>
Clearing the Web Browser Cache With Internet Explorer . . . . .	66
Clearing the Web Browser Cache With Mozilla or Netscape Navigator . . . . .	66
<b>RAC Software Basics for Red Hat Linux</b> . . . . .	<b>67</b>
RAC Support in Red Hat Linux . . . . .	68

## 7 Accessing and Using a Remote Access Controller

<b>Accessing a RAC</b> . . . . .	<b>69</b>
Logging In and Out . . . . .	70
<b>Remote Access Service RAC Home Page</b> . . . . .	<b>70</b>
Status Indicator Icons . . . . .	71
Properties . . . . .	71
RAC Information . . . . .	72
System Information . . . . .	72
Watchdog Information . . . . .	72
Session Status . . . . .	73
<b>Sensors</b> . . . . .	<b>73</b>
RAC Sensors (DRAC IIIs only) . . . . .	73
Server Sensors . . . . .	74
Sensor Thresholds . . . . .	74
<b>Logs</b> . . . . .	<b>75</b>
Viewing the POST Log . . . . .	75
Viewing the RAC Log . . . . .	75

Viewing the Hardware Log . . . . .	76
Viewing the Boot Path Analysis Log . . . . .	76
Viewing the Last Crash Screen. . . . .	76
<b>Configuration . . . . .</b>	<b>77</b>
Poll Rates. . . . .	77
<b>Remote Access . . . . .</b>	<b>78</b>
Server Reset Options . . . . .	78
Remote Floppy Boot. . . . .	79
Console Redirect . . . . .	81
<b>Debug . . . . .</b>	<b>82</b>
Network Debug . . . . .	83
Command Debug . . . . .	83
Trace Log . . . . .	84
Status Check . . . . .	85
<b>Updating RAC Firmware . . . . .</b>	<b>85</b>
Updating the RAC Firmware . . . . .	86

## 8 Configuring a RAC to Use a Serial or Telnet Text Console

<b>Supported Remote Access Controllers . . . . .</b>	<b>87</b>
<b>Serial and Telnet Console Features . . . . .</b>	<b>88</b>
<b>Enabling and Configuring the Managed System to Use a Serial or Telnet Console</b>	<b>88</b>
Upgrade Your BIOS . . . . .	88
Configuring the System Setup Program on the Managed System. . . . .	89
Enabling the Serial/Telnet Console on the RAC . . . . .	89
Using Racadm to Configure the Settings for the Serial and Telnet Console	90
<b>Connecting to the Managed System Through the Serial Port or Telnet Management Station (Client System) . . . . .</b>	<b>91</b>
Connecting the DB-9 Cable . . . . .	92
<b>Configuring the Management Station Terminal Emulation Software . . . . .</b>	<b>93</b>
Configuring Red Hat Linux Minicom for Serial Console Emulation . . . . .	93
Configuring HyperTerminal for Serial Console Redirection. . . . .	95
Configuring Red Hat Linux XTerm for Telnet Console Redirection. . . . .	95
Configuring Microsoft Telnet for Telnet Console Redirection. . . . .	96
<b>Log In to the RAC . . . . .</b>	<b>96</b>



<b>Starting a Text Console</b> . . . . .	<b>96</b>
Connecting to the RAC Using the "connect com2" Command . . . . .	96
<b>Performing Actions on the Managed System</b> . . . . .	<b>97</b>
<b>Using VT-100 Terminal Emulation With a DRAC III</b> . . . . .	<b>97</b>
DRAC III VT-100 Communication Port Settings . . . . .	97
Using Terminal Emulation With Red Hat Linux . . . . .	98

## A Hardware Specifications

<b>Power Requirements</b> . . . . .	<b>99</b>
DRAC III . . . . .	99
DRAC III/XT . . . . .	99
ERA/O . . . . .	99
<b>PCI Interface</b> . . . . .	<b>99</b>
DRAC III . . . . .	99
<b>Connectors</b> . . . . .	<b>100</b>
DRAC III . . . . .	100
DRAC III/XT . . . . .	100
ERA . . . . .	100
ERA/O . . . . .	100

## B Troubleshooting

<b>Basic Troubleshooting</b> . . . . .	<b>101</b>
<b>Using the RAC Trace Log</b> . . . . .	<b>105</b>
<b>Troubleshooting Network Problems</b> . . . . .	<b>105</b>
Troubleshooting Alerting Problems . . . . .	107
<b>RAC Log Messages</b> . . . . .	<b>107</b>
<b>DRAC III LED Indicators</b> . . . . .	<b>111</b>
Nonrecoverable POST Error . . . . .	111
Repair Mode . . . . .	111
Self-Test Error Blink Codes . . . . .	112

<b>Abbreviations and Acronyms</b> . . . . .	<b>115</b>
---	------------

## Figures


Figure 2-1.	DRAC III Hardware Components . . . . .	24
Figure 3-1.	DRAC III/XT Hardware Components . . . . .	45
Figure 7-1.	Sample Remote Access Service RAC Home Page . . .	71

## Tables

Table 1-1.	RAC Software Components . . . . .	15
Table 1-2.	RAC Configuration Interfaces . . . . .	16
Table 1-3.	Supported Remote Access Connections . . . . .	17
Table 1-4.	Remote Access Interfaces . . . . .	17
Table 1-5.	RAC Ports . . . . .	18
Table 1-6.	Supported Event Alerts . . . . .	19
Table 7-1.	Remote Floppy Boot Settings . . . . .	81
Table 7-2.	Remote Floppy Boot Commands . . . . .	82
Table 7-3.	Remote Floppy Boot Configuration Settings . . . . .	82
Table 8-1.	Racadm cfgSerial Objects for Configuring the Serial/Telnet Console . . . . .	93
Table 8-2.	Required Pinout for DB-9 Null Modem Cable . . . . .	94
Table 8-3.	Minicom Settings for Serial Console Emulation . . . . .	96
Table 8-4.	Management Station COM Port Settings . . . . .	97
Table 8-5.	Differences Between "connect com2" and "connect video" Commands . . . . .	98
Table 8-6.	DRAC III VT-100 COM Port Settings . . . . .	100
Table A-1.	DRAC III Power Requirements . . . . .	101
Table A-2.	DRAC III PCI Interface . . . . .	102
Table A-3.	DRAC III Connectors . . . . .	102
Table B-1.	RAC Error Codes . . . . .	108
Table B-2.	RAC Log Messages . . . . .	110


# Introduction

The Dell™ Remote Access Card III (DRAC III), DRAC III/XT, Embedded Remote Access (ERA), and the Embedded Remote Access Option (ERA/O) are systems management hardware and software solutions designed to provide remote management capabilities for Dell PowerEdge™ systems. Collectively, these solutions are known as remote access controllers (RACs). RACs allow you to remotely manage and monitor your system even when the system is down.

 **NOTE:** Throughout the remainder of this document, the DRAC III, DRAC III/XT, ERA, and ERA/O controllers are referred to collectively as "RACs", except when it is necessary to distinguish between each controller. When information applies only to a specific RAC, it is identified explicitly. Information that refers to "RAC" applies to all of the controllers.

## Remote Access Controller Features

Your RAC provides a complete hardware and software solution for remote systems management. The RAC allows you to remotely access an inoperable system to get the system up and running as quickly as possible. The RAC can alert you when the system is down, and allows you to restart the system remotely. By communicating with the system's ESM, the RAC reports warnings or errors related to voltages, temperatures, and fan speeds. In addition, the RAC can log the probable cause of a system crash and save the most recent crash screen (for systems running the Microsoft® Windows® operating system only).

 **NOTE:** Throughout the remainder of this document, the system in which the RAC is installed or embedded is referred to as the *managed system*. A system that remotely accesses the RAC is referred to as a *management station*. The term *system console* refers to a system's keyboard, mouse, and monitor.

The following is a list of features available on all RACs. However, some RACs (such as the DRAC III), provide additional features. For a list of features that are specific to your RAC, see the features list in each individual RAC section.


- Ability to configure the RAC through the managed system's network connection.  
Using Dell OpenManage™ Server Administrator, you can access the RAC through the managed system's standard network connection and configure the RAC properties, such as RAC users and alerting options.
- Ability to manage and monitor the managed system through the RAC network adapter, serial connection, or telnet connection.

If the managed system goes down or becomes unresponsive and you want to perform crash-recovery actions, or if you want to check the status of sensor monitors when the system is running, you can launch the RAC's Web-based remote access interface.

- Ability to redirect the managed system's monitor, keyboard, and mouse to the management station using console redirection.
- Integration with other Dell systems management software products for your system, such as Server Administrator.
- Access to the hardware log and POST logs.
- Embedded Web server that supports Microsoft® Internet Explorer, Mozilla, and Netscape Navigator (for more information, see "Supported Web Browsers").
- Monitoring of the managed system's health, including voltages, temperatures, and cooling fan status, using information obtained from the managed system's ESM.
- Ability to alert you to potential problems on the managed system by sending either an e-mail message or an SNMP trap through the integrated network adapter to a management station.
- Support for DHCP assignment of the RAC IP address.
- Ability to configure the RAC and update RAC firmware locally or remotely using the racadm command-line utility, a scriptable interface. For more information about using the racadm utility, see the *Dell Remote Access Controller Racadm User's Guide*.
- Ability to perform a *boot path analysis*, which provides troubleshooting information from the managed system's boot log in the event of a boot failure.
- Ability to perform a *remote floppy boot* (RFB), which allows you to boot the managed system remotely from a diskette. Typically, the boot image is downloaded to the RAC from either a TFTP server or a management station. This feature is supported on 32-bit systems only.
- IPMI 1.0 compliance.
- Ability to perform power management functions, such as shutdown and reset, remotely from a management station.
- Password-level security management and SSL encryption.
- Operating system and domain-based RAC log-in authentication.


## Supported Operating Systems

RACs currently support the following operating systems:


- Microsoft Windows® Server 2003, Windows 2000 Server, Windows 2000 Advanced Server, and Windows Advanced Server Limited Edition (DRAC III only) operating systems
  - Novell® NetWare® 6.5 and NetWare 5.1 (Service Pack [SP] 3 or later) operating systems
-  **NOTE:** If NetWare is running on the managed system, console redirection supports text-only mode.
- Red Hat® Linux version 9 and Red Hat Enterprise Linux AS (version 2.1 and version 3.0) operating systems

 **NOTE:** MS-DOS® version 6.22 supports the RAC remote floppy boot feature (32-bit systems only).

## Supported Web Browsers

 **NOTE:** For a list of the supported Java Virtual Machine (JVM) plug-ins, see the `racread.txt` file on your *Systems Management CD* or at the Dell Support website at [support.dell.com](http://support.dell.com).

- Microsoft Internet Explorer 5.5 (SP 2 or later) and 6.0 on Microsoft Windows Server 2003, Windows 2000 Server, and Windows XP Professional
- Mozilla 1.3 and 1.4 running with Red Hat Linux 9 and Red Hat Enterprise Linux AS (version 2.1 and version 3.0)
- Netscape Navigator 7.01 and 7.02 on Windows Server 2003, Windows 2000 Server, Windows XP, and Red Hat Linux 9 and Red Hat Enterprise Linux AS (version 2.1 and version 3.0)

 **NOTE:** When using Internet Explorer or Netscape Navigator on systems running Microsoft Windows, to view localized versions of the RAC's Web-based remote access interface, open the Windows **Control Panel**, double-click the **Regional Options** icon, and select the desired locale from the **Your locale (location)** drop-down menu.

## Software Components

RACs provide software components that include a set of services for each supported operating system. The services interface with RAC hardware to allow RAC configuration and access to the managed system.

Table 1-2 summarizes the RAC software components.

**Table 1-1. RAC Software Components**


Software Component	Description
Firmware	Executes on the RAC independently of the managed system's operating system. It includes networking utilities, an embedded Web server, and an embedded file system. It provides software interfaces to all the embedded systems management functions provided by the BMC.
Managed system software	Executes on the managed system under supported operating systems and interfaces RAC firmware with other Dell systems management software. The RAC managed system software includes device drivers, agents, and services that provide a communications path for Server Administrator to configure the RAC and provides graphical console redirection screens when the system is running.
Management station software	Provides discovery of all RACs on the network and correlates all RACs with managed system addresses. It also provides a launching point for the Web-based interface and reception of RAC-generated asynchronous events.

**Table 1-1. RAC Software Components (continued)**

Software Component	Description
RAC Web-based interface	Communicates with the RAC firmware using Java applets that execute in a remote Web browser. The Java applets are loaded into the browser from the embedded Web server in the RAC firmware. The browser connects directly to the RAC when you enter the RAC IP address.

## RAC Configuration Interfaces

To configure the RAC to remotely access and manage a system, you can use one of several configuration interfaces provided with your RAC software. Table 1-2 describes these configuration interfaces. For an overview of RAC software configuration, see the section of this document that applies to your RAC.

 **NOTE:** It is recommended that you use Server Administrator to configure your RAC.

**Table 1-2. RAC Configuration Interfaces**

Interface	Description
Server Administrator	Provides a comprehensive, one-to-one systems management solution from an integrated Web-based GUI or from a CLI that allows you to configure the RAC from the management station through the RAC's network adapter. Use Server Administrator to configure your RAC (add users, modify IP addresses) through a GUI.
racadm CLI utility	A scriptable command-line utility that allows you to locally or remotely configure the RAC outside of Server Administrator. Use the racadm CLI utility to write scripts that will automatically configure multiple RACs.
Option ROM	An interface that runs on the managed system that allows you to configure only the RAC network settings during the managed system's boot sequence. Use Option ROM to configure IP addresses during system boot (before Server Administrator or the racadm CLI utility is installed).

## Supported Remote Access Connections

Three types of remote access connections are supported by RACs. Table 1-3 lists the features of each type of connection.

**Table 1-3. Supported Remote Access Connections**

<b>Connection</b>	<b>Features</b>
Network adapter	<ul style="list-style-type: none"> <li>• 10/100 Mbps Ethernet (10 Mbps for ERA/O on the PowerEdge 1650 system)</li> <li>• DHCP support</li> <li>• SNMP traps with e-mail event notification</li> <li>• Network interface for the RAC's Web server and other network applications</li> </ul>
PCMCIA modem (DRAC III only)	<ul style="list-style-type: none"> <li>• 56 Kbps PCMCIA modem</li> <li>• International support</li> <li>• PPP interface to the DRAC III Web server and other network applications</li> <li>• SNMP traps with e-mail event notification, numeric, and alphanumeric paging</li> </ul>
Serial port	<ul style="list-style-type: none"> <li>• Connection to dedicated VT-100 text menu application (DRAC III only)</li> <li>• Support for serial and racadm commands including system boot, reset, power-on, and shutdown commands</li> <li>• Support for text-only console redirection to a VT-100 terminal or terminal emulator</li> </ul>

## Remote Access Interfaces

After you configure the RAC, you can remotely access the managed system using one of three remote access interfaces. Remote access is particularly important when the managed system is down and cannot be accessed through the system's network adapter. The RAC network adapter acts as a remote access port for all RACs. Additionally, DRAC III also provides remote access through its own serial port and optional modem. Table 1-4 describes the RAC's remote access interfaces.

**Table 1-4. Remote Access Interfaces**

<b>Interface</b>	<b>Description</b>
RAC Web-based interface	Enables you to remotely access the managed system through the RAC's network adapter (or the DRAC III optional modem). For a list of supported Web browsers, see "Supported Web Browsers."

**Table 1-4. Remote Access Interfaces (continued)**

Interface	Description
racadm CLI utility	Allows (racadm remote capability option [-r]) you to connect to the managed system and execute racadm subcommands from a remote console, or management station using only the IP address of the managed system.  <b>NOTE:</b> The racadm remote capability is supported only on Windows Server 2003, Windows 2000 Server, and Red Hat Linux operating systems.
Telnet Console	Provides access through the RAC to the COM2 (RAC) port, video, and hardware management interfaces through the RAC network adapter and provides support for serial and racadm commands including <b>system boot</b> , <b>reset</b> , <b>power-on</b> , and <b>shutdown</b> commands.
Terminal Emulation Software	Provides access through the RAC to the COM2 (RAC) port, video, and hardware management interfaces through either the external serial connector or external DRAC III VT-100 serial connector. The terminal emulation software provides support for serial and racadm commands including <b>system boot</b> , <b>reset</b> , <b>power-on</b> , and <b>shutdown</b> commands.
VT-100 text menu interface (DRAC III only)	Enables you to remotely access the managed system using VT-100 terminal hardware or terminal emulation software. This interface, which resides in the DRAC III firmware, requires an optional VT-100 serial cable connection from the managed system to the management station or a client system.

## RAC Port Numbers

Table 1-5 identifies the ports used by RACs. This information is required when opening firewalls for remote access to a RAC.


**Table 1-5. RAC Ports**


RAC Port Number	Used For
80	Web-based connections and TCP.
443 (when enabled)	SSL Web-based connections and TCP.
5900 and above	Console redirection text and graphics and TCP.
32768 and above (randomly selected)	Remote floppy boot image. The port is closed when the transfer of the image is complete.



## RAC Event Alerts

An important feature of the RAC is its ability to notify you when the managed system has potential problems (for example: problems with voltage, temperature, or cooling fans). To do this, the RAC sends an alert using one or more of its remote access port connections. RAC firmware constantly monitors the IPMI hardware log to determine when to generate an event. Table 1-6 lists the RACs and the types of alerts supported on each.

 **NOTE:** E-mail alerts are sent to a specified e-mail address on an SMTP server. SNMP traps are sent to a specified IP address. Numeric and alphanumeric pages are alerts sent to a specified user.

 **NOTE:** For information about configuring SNMP, see the *Server Administrator User's Guide*.

**Table 1-6. Supported Event Alerts**

RAC	E-mail	SNMP Trap	Alphanumeric Page	Numeric Page
DRAC III (with optional modem installed)	X	X	X	X
DRAC III/XT	X	X		
ERA	X	X		
ERA/O	X	X		

Because RAC firmware has an embedded Web server, you can connect to the RAC from a management station without installing management station software (other than a supported Web browser and supported JVM plug-in). For more information, see "Supported Web Browsers."

After receiving an alert, you can view the event log to get more information on the type and severity of the event. The Web browser connects to the RAC using the 10- or 100-Mbps Ethernet network adapter (10 Mbps for ERA/O on the PowerEdge 1650) on a LAN/WAN or the optional DRAC III modem, both of which are located on the RAC.

If a system crashes, you can configure the system to enable the RAC to capture the system console screen to assist you in analyzing the cause of the failure (this feature is only supported for systems running Windows operating systems). To get the system up and running again, you can perform a remote reset or power cycle and view the boot process through the RAC Web-based (remote access) interface.

You can configure the RAC to notify different users of different events. When the RAC detects a new event, the firmware tests the event against each user's event filter and sends an alert to the appropriate users.

You can also configure RAC firmware to generate SNMP traps for specific events. After the firmware is configured, the RAC sends the SNMP traps through the LAN to the IP address specified in the RAC configuration files. DRAC III can also send the trap through dial-up networking. The telephone number, user name, password, and IP address where the dial-out trap is sent are specified in the RAC configuration files.

## Remote Access Security Features

The following subsections describe the security features available on all RACs. For a list of security features that are specific to your RAC, see the section of this document that pertains to your RAC.


### Network Adapter Connections

RACs support encrypted password authentication for TCP/IP network adapter connections.

### RAC Web-based Interface Security

The RAC Web-based remote access interface content is proprietary and does not provide direct access to the managed system's operating system. Typically, remote access to the RAC is used when an administrator is not logged locally into the managed system. If an administrator logs in locally, operating system access is protected by standard operating system security measures.

When a remote user accesses the RAC and performs a console redirection, a pop-up notification box appears on the managed system's console stating that remote console redirection is occurring.

 **NOTE:** If you are performing console redirection from a remote location and you do not want anyone to interfere with the managed system at its location, you can remotely disable the managed system's keyboard and mouse. This feature is supported only on managed systems running Windows Server 2003 or Windows 2000 Server.

### Log In Validation for the Web-based Remote Access Interface


The RAC's Web-based remote access interface requires a valid login. When establishing a remote connection to the RAC, the user enters a user name and password at the remote console. The password is then encrypted and sent to the RAC. The RAC receives the user name and encrypted password and begins authentication. The password that was saved by the RAC for this user name is also encrypted. It is then compared with the encrypted password received from the remote user. If a match occurs, the user is validated and access to the RAC is granted. Other commands are not recognized until validation occurs (except for online help). All information (except console redirection screens) is transmitted using SSL encryption.

## RAC User Types

RAC user types include RAC users as well as operating system users. DRAC III also provides two additional user/entry types. See "DRAC III User Types and Feature Configuration."

### RAC Users

RAC users can establish console redirection and perform configuration and management actions on all RACs.

 **NOTE:** The RAC Web-based interface does not accept a user name without a password. When you create a RAC user, you must assign a valid user name and password.

A RAC user is able to:

- Log into the RAC locally.
- Enter systems management commands such as power on, power off, power cycle, graceful power off, and graceful restart.
- Update the RAC firmware.
- Use the remote floppy boot feature to boot the server, configure the RAC, or perform server diagnostics.
- View POST, RAC, and hardware logs.
- Perform console redirection.
- Access the last crash screen.
- Receive event notification e-mails.



**NOTE:** DRAC III provides additional user types and events. For more information, see "DRAC III User Types and Feature Configuration."

## Operating System Users

In addition to RAC users, which are defined and stored as part of the RAC internal configuration, RACs also recognize operating system users. These users are not stored in the internal RAC database—they are stored by the operating system running on the managed system. Operating system users can perform all the functions of a RAC user with the exception of receiving event notification e-mails.

This added functionality allows a user to access any RAC by using the operating system's user name and password, provided that:

- The managed system's operating system is running.
- The RAC software for the managed system is installed and running.
- The user has valid administrator rights to the managed system.

This authentication method (operating system authentication versus RAC user authentication) operates independently of the operating system's user authentication configuration. The operating system is generally set up to attempt a connection to a domain controller to acquire the latest information about user names, passwords, and access rights before it queries the local operating system database. This connection is transparent to a RAC.

## Other Documents You May Need

In addition to this *Installation and Setup Guide*, the following documents provide additional information about the setup and operation of the RAC in your system:

- RAC online help provides information on using the Web-based remote access interface.

- The *Dell Remote Access Controller Racadm User's Guide* provides information about using the racadm command-line utility.
- The *Dell OpenManage IT Assistant User's Guide* and the *Dell OpenManage IT Assistant Reference Guide* provides information about IT Assistant.
- The *Dell OpenManage IT Assistant* provides information about IT Assistant.
- The *Dell OpenManage Server Administrator's User's Guide* provides information about installing and using Server Administrator.

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



The *System Information Guide* provides important safety and regulatory information. Warranty information may be included within this document or as a separate document.

- The *Rack Installation Guide* and *Rack Installation Instructions* included with your rack solution describes how to install your system into a rack.
- The *Getting Started Guide* provides an overview to initially set up your system.
- The *User's Guide* provides information about system features and technical specifications.
- The *Installation and Troubleshooting Guide* describes how to troubleshoot the system and install or replace system components.
- Systems management software documentation describes the features, requirements, installation, and basic operation of the software.
- Operating system documentation describes how to install (if necessary), configure, and use the operating system software.
- Documentation for any components you purchased separately provides information to configure and install these options.
- Updates are sometimes included with the system to describe changes to the system, software, and/or documentation.




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

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

## Getting Started With Your DRAC III

This section provides information specifically about DRAC III. It includes a list of DRAC III features, DRAC III kit contents, supported systems, hardware and optional hardware installation instructions, and a software configuration overview.


 **NOTE:** Throughout the remainder of this document, the system in which the RAC is installed or embedded is referred to as the *managed system*. A system that remotely accesses the RAC is referred to as a *management station*. The term *system console* refers to a system's keyboard, mouse, and monitor.

### DRAC III Features


The DRAC III is a 33-MHz PCI card with its own microprocessor and memory. The DRAC III may be preinstalled on your system, or available separately in a kit. To get started with a DRAC III that is already installed on your system, see "Software Installation and Configuration Overview." If the DRAC III is not already installed on your system, see "Installing the DRAC III Hardware" before beginning the software installation and configuration.

In addition to the features listed in "Remote Access Controller Features," the DRAC III also provides the following features:

- Ability to manage and monitor the managed system through the DRAC III network adapter and the optional modem and serial port (using the optional VT-100 cable).
- Console redirection, which can be performed using the DRAC III network adapter, optional modem, or serial port (using the optional VT-100 cable).

 **NOTE:** The serial connection supports text-only console redirection.

- A battery backup that provides power to the DRAC III for up to 30 minutes if a power failure occurs.
- An external AC power adapter that allows the DRAC III to function when the system is off.

 **NOTE:** While the DRAC III does not require an external power adapter, using one will allow the DRAC III to remain operational when the system is off, and will extend DRAC III power beyond the 30-minute limit of the battery backup.

- A PCMCIA modem socket for the optional modem.
- In addition sending alerts in the form of an e-mail message or an SNMP trap (through the integrated network adapter), the DRAC III also sends alerts as numeric or alphanumeric pages.

- On 64-bit systems, the DRAC III is equipped with a 3-pin cable that allows access to the system's IPMB. The IPMB provides remote monitoring, log in, and recovery control functions independent of the system's main processors, BIOS, and operating system. The IPMB is available for remote monitoring even when the system is off.

## DRAC III Security Features

In addition to the security provided for the RAC network adapter and Web-based interface connections (see "Remote Access Security Features"), the DRAC III also provides security for VT-100 and modem connections.

### VT-100 Connections

Password encryption is not used for this type of connection because the VT-100 connection is a direct-connect terminal emulation, and as such, does not warrant encryption. Terminal security is provided by nonencrypted authentication of the user name and password. The firmware prevents display of the password on the terminal. System power management features (such as reset and power cycle) and text console redirection are provided through the VT-100 interface. Access to a graphical operating system is not available.

### Modem Connections

DRAC III supports CHAP encryption for PPP modem connections.

## DRAC III Kit Contents

- DRAC III hardware
- IPMB cable (64-bit systems only)
- External power adapter and power cable (only in countries where certified)
- VT-100 cable (optional)
- Riser board with two PCI slots (Dell™ PowerEdge™ 1650 only)
- *Dell OpenManage Server Assistant CD*
- *Dell OpenManage Systems Management CD* (or *Server Management CD* for 64-bit systems)
- *Dell OpenManage Product Documentation CD* (or *Documentation CD* for 64-bit systems)

## Supported Systems

DRAC III supports the following PowerEdge systems: 1650, 4600, 6600, 6650, and 7150 systems.



**NOTE:** DRAC III is supported only on PowerEdge 7150 systems running Microsoft Windows Advanced Server Limited Edition.




**NOTE:** See your `racread.txt` file for the most current list of supported systems.


## Supported Modems

DRAC III supports the following PCMCIA modems:


- ActionTec (U.S. and Canada only)
- Psion Gold Card (56 K and fax)

## Installing the DRAC III Hardware


 **CAUTION:** Before you perform this procedure, you must turn off the system and disconnect it from its power source. Only trained service technicians are authorized to remove the system cover and access any of the components inside the system. Read and follow all safety precautions in your *System Information Guide*.

 **NOTICE:** Before installing a DRAC III, read the installation instructions in this document and in your system's *Installation and Troubleshooting Guide*.

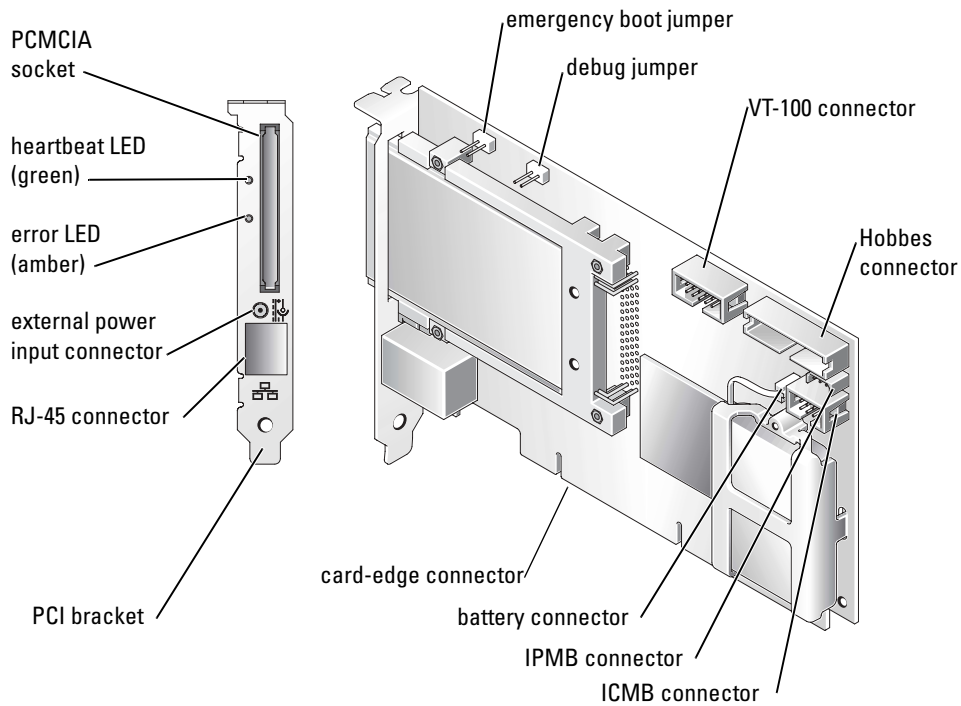
- 1 Turn off the system and all attached peripheral devices.
- 2 Disconnect the system and peripherals from electrical outlets. Disconnect any telephone or telecommunication lines from the system.

 **CAUTION:** Only trained service technicians are authorized to remove and access any components inside the system. See your *System Information Guide* for complete information about safety precautions, working inside the computer, and protecting against electrostatic discharge.

- 3 Before touching anything inside the system, touch an unpainted metal surface at the back of the system chassis to dissipate any static electricity that might harm internal components.


 **NOTICE:** Failure to dissipate static electricity may damage or destroy static-sensitive components.

- 4 Remove the system cover according to the instructions in your system's *Installation and Troubleshooting Guide*.
- 5 If your DRAC III kit included a PCMCIA modem, insert the modem into the PCMCIA socket on the DRAC III PCI bracket. See Figure 2-1 for component locations.





**Figure 2-1. DRAC III Hardware Components**

- 6 Press firmly to seat the modem card into the socket, ensuring that the pins are properly seated in the connector.
- 7 Connect the modem cable to a telephone jack.
- 8 **NOTICE:** If you are installing the DRAC III on a 32-bit system, skip steps 8 and 9. If you are installing the DRAC III on a 64-bit system and want access to the IPMB, you must complete steps 7 and 8 before installing the DRAC III into the system. If you are not sure if your system is equipped with an IPMB connector, see your system documentation.
- 8 Plug the IPMB cable into the 3-pin yellow IPMB connector on the DRAC III. See Figure 2-1. Ensure that the cable is securely connected to the DRAC III card.
- 9 Plug the free end of the IPMB cable into the 3-pin connector on the system backplane. See your system *Installation and Troubleshooting Guide* for the location of this connector.
- 10 Insert the DRAC III into PCI slot 1.
- 10 **NOTICE:** For the DRAC III to function properly, it must be installed in the 32-bit, 33-MHz PCI slot 1. The DRAC III must be inserted into PCI slot 1 because it must reside on the same bus as the video controller. If another expansion card is installed in slot 1, it must be moved to another slot before proceeding with the installation.



-  **NOTICE:** On PowerEdge 1650 systems, the DRAC III is installed on a riser board. The riser board plugs into the riser connector on the system board and is considered an extension of the system board. The riser board is equipped with one 32-bit, 33-MHz expansion slot (PCI1) for 5-V cards, and one 64-bit, 66-MHz expansion slot (PCI2). For the DRAC III to function properly, it *must* be installed in the 32-bit PCI1 slot. If you purchased the DRAC III with your PowerEdge 1650 system, the riser card and the DRAC III are preinstalled. If you purchased the DRAC III kit separately for installation on a PowerEdge 1650 system, see the instructions for installing the riser card contained in the kit.

Ensure that the card-edge connector is fully seated into the system board.

- 11 If your DRAC III kit includes the optional VT-100 serial cable, connect it to the VT-100 serial connector on the DRAC III (see Figure 2-1), and then install the cable's external port into an empty slot in your system. For more information about using a VT-100 connection, see the document included in your VT-100 serial cable kit.
-  **NOTICE:** You must use the DRAC III VT-100 serial cable specifically provided for use with the DRAC III because not all serial cables have the same pin-out specification. Using the wrong cable will result in VT-100 terminal emulation failure or DRAC III failure.
- 12 Follow the instructions in your system *Installation and Troubleshooting Guide* to reassemble the system and replace the system cover.
- 13 Connect the external power adapter to a UPS or available power receptacle. For power supply specifications, see "Power Requirements."
  -  **NOTE:** While the DRAC III does not require an external power adapter, using one allows the DRAC III to remain operational when the system is off, and extends the DRAC III power beyond the 30-minute capability of the battery pack.
  -  **NOTE:** It is recommended that you use a UPS for the most complete power protection.
- 14 Connect the power jack to the external power input connector on the DRAC III PCI bracket.
- 15 If you are using a network connection with the DRAC III, attach the twisted-pair cable to the RJ-45 connector on the DRAC III. See Figure 2-1 for location of these connectors.
  -  **NOTE:** The maximum length allowed for the LAN cable connected to the RJ-45 connector is 184 ft (56 m).
- 16 If you are going to use the optional modem with the DRAC III, attach a modem adapter cable to the PCMCIA modem socket. Next, connect the adapter cable to an analog telephone line.
- 17 Reconnect any telephone or telecommunications lines to the system, and all peripheral devices to their electrical outlets, and turn them on.

If the DRAC III installation was successful, the green heartbeat LED indicator on the back of the card connector is illuminated (see "DRAC III Hardware Components").

After completing the hardware installation procedures, you must install and configure the RAC software. For more information about the RAC software components, see "Software Components." For an overview of RAC software installation and configuration, see "Software Installation and Configuration Overview."

## Software Installation and Configuration Overview

This section provides a high-level overview of the RAC software installation and configuration process for DRAC III. Some steps give you the option of using several different tools to perform the configuration, including Server Administrator, IT Assistant, the racadm CLI utility, and your operating system utilities.

For more information about the RAC software components, see "Software Components."

Depending on the tool used to perform the configuration, see the following documents for more information:

- *Dell OpenManage Server Administrator User's Guide*
- *Dell OpenManage IT Assistant User's Guide* or the *Dell OpenManage IT Assistant Reference Guide*
- *Dell Remote Access Controller Racadm User's Guide*
- Operating system documentation

To install and configure your RAC software, perform the following steps in their numbered order.



**NOTICE:** To avoid losing the PPP connection for the DRAC III controller, you must uninstall your systems management software before you upgrade your operating system and reinstall the systems management software after the upgrade.

- 1 Update the system BIOS. See "Updating the System BIOS."
- 2 Install the software on the managed system. See "Installing the Software on the Managed System."
- 3 On managed systems running Microsoft® Windows® Server 2003, Windows XP, and Windows 2000 operating systems, add and configure the RAS. See "Configuring RAS PPP Connection."
- 4 Configure the RAC network settings. See "Configuring the RAC Network Settings."
- 5 Add and configure RAC users. See "Adding and Configuring RAC Users."
- 6 Configure the DRAC III optional modem. See "Configuring the DRAC III Optional Modem."
- 7 Add and configure dial-in (PPP) users. See "Adding and Configuring Dial-in (PPP) Users."
- 8 Configure dial-out alert notification on the management station. See "Configuring Dial-Out Alert Notification on the Management Station."
- 9 Install (or upgrade) the software on the management station. See "Installing (or Upgrading) the Software on the Management Station."
- 10 Configure the management station's modem. See "Configuring the Management Station's Modem."
- 11 Configure the Web browser to connect to the remote access interface. See "Configuring the Web Browser to Connect to the Remote Access Interface."
- 12 Connect to the remote access interface. See "Connecting to the Remote Access Interface."

## Updating the System BIOS


If you are adding a RAC to an existing managed system, it is recommended that you update the system's BIOS before installing the RAC to ensure full support for the card. See "Updating the System BIOS."

## Installing the Software on the Managed System

Install the software on the managed system using the *Systems Management* CD (32-bit systems) or the *Server Management* CD (64-bit systems).

For instructions on installing this software, see your *Server Administrator User's Guide*.


The managed system has the following components embedded or installed: the RAC, the appropriate version of Server Administrator, and the appropriate RAC agent. Depending on the operating system, the RAC agent consists of either Microsoft® Windows® services, Novell® NLMs, or Red Hat Linux drivers and daemons. The RAC agent automatically starts when you boot the managed system.

 **NOTE:** If you are configuring the DRAC III on a 64-bit system, you must install the DRAC III drivers. For more information, see "Installing DRAC III Drivers on 64-Bit Systems."

## Configuring the RAC Network Settings

Configure the RAC network settings using one of the following tools:


- Server Administrator
- IT Assistant
- racadm CLI utility
- RAC Option ROM — See "Configuring the RAC Network Settings Using the Option ROM."
- Serial and telnet consoles — See "Configuring a RAC to Use a Serial or Telnet Text Console."

 **NOTE:** If you are deploying the RAC in a Red Hat Linux environment, see "RAC Software Basics for Red Hat Linux."

## Adding and Configuring RAC Users

Add and configure RAC users using one of the following tools:

- Server Administrator
- IT Assistant
- racadm CLI utility
- Serial and telnet consoles — See "Configuring a RAC to Use a Serial or Telnet Text Console."

 **NOTE:** For more information about user types, see "RAC User Types" and "DRAC III User Types and Feature Configuration."

### **Configuring the DRAC III Optional Modem**

If your DRAC III includes the optional modem, configure the modem on the DRAC III using one of the following tools:

- Server Administrator
- racadm CLI utility
- IT Assistant

### **Adding and Configuring Dial-in (PPP) Users**

Add and configure dial-in (PPP) users using one of the following tools:

- Server Administrator
- racadm CLI utility
- IT Assistant
- Operating system utilities — See "Changing the PPP Server IP Address on the Managed System."

### **Configuring Dial-Out Alert Notification on the Management Station**

Configure dial-out alert notification on the management station using one of the following tools:

- Server Administrator
- racadm CLI utility
- IT Assistant
- Operating system utilities — See "Configuring Management Stations Running Windows to Receive DRAC III Dial-Out Alert Notifications."

### **Installing (or Upgrading) the Software on the Management Station**

If necessary, install (or upgrade) the software on the management station, including Server Administrator and IT Assistant, using the *Systems Management* CD (32-bit systems) or the *Server Management* CD (64-bit systems).

For instructions about installing this software, see your *Server Administrator User's Guide*.

A management station is a system (typically a workstation running Windows Server 2003 or Windows 2000) that has the following components installed: appropriate versions of Server Administrator (or IT Assistant), a supported Web browser (for more information, see "Supported Web Browsers"), Windows services (if applicable), Server Administrator (or IT Assistant) services, and user interface elements.

## Configuring the Management Station's Modem

To use the management station's modem for remote access to a DRAC III, you must configure the management station's modem. See "Changing the PPP Server IP Address on the Managed System" for instructions.

## Configuring the Web Browser to Connect to the Remote Access Interface

If you are using a client system that connects to the Internet through a proxy server to connect to the RAC Web-based remote access interface, you must configure your Web browser for this connection.

See "Configuring a Web Browser to Display the Remote Access Interface."

## Connecting to the Remote Access Interface

To connect to the remote access interface through the network connection, see "Connecting to the Remote Access Interface." To connect to the interface through the DRAC III optional modem, see "Accessing a DRAC III Through a Modem." To connect to the DRAC III through the optional VT-100 serial connection, see "Accessing the DRAC III Remote Access Interface Using VT-100 Terminal Emulation."

# DRAC III User Types and Feature Configuration

In addition to RAC users (see "RAC Users"), the DRAC III also supports the following users and entries:

- DRAC III dial-in users – Also called point-to-point protocol (PPP) users, dial-in user names and passwords are used to establish a dial-in connection only. After the connection is established, a RAC user name and password must be supplied to perform console redirection, configuration, and management actions.
- Demand dial-out entries – Demand dial-out entries specify a destination IP address, the telephone number of a management station, a management station user name and password, and the authentication type associated with the management station user name and password.



**NOTE:** The demand dial-out entries are *not* RAC users. Rather, they are remote management station users.





**NOTE:** It is not necessary for the destination IP address to be the remote management station that answers the telephone. The destination IP address may be the IP address of another remote management station. If the destination IP address is the IP address of another remote management station, the management station answering the telephone must be able to route to the destination IP address specified.

Some of the DRAC III features are configured within the context of a RAC user, such as alerting and paging. The following sections describe how to configure the DRAC III features and/or users outside of the Server Administrator environment.

## Configuring Systems to Dial In to the DRAC III

To provide client access to the DRAC III, you must add and configure dial-in (PPP) users. For information about configuring these users in Server Administrator, see your *Server Administrator User's Guide*. Otherwise, use the procedures in the following sections to add and configure dial-in users.

 **NOTE:** It is also possible to use the `racadm` command-line utility to add and configure dial-in users. For more information, see the *Racadm User's Guide*.

 **NOTE:** If for any reason all the DRAC III users are deleted, use the `racadm` command-line utility to create new users.


### Restrictions for Microsoft PPP Clients

The DRAC III provides network support through two different interfaces: the DRAC III network adapter, and the optional PCMCIA modem. As a result, it is possible that a network loop could be created when both connections are active. This loop makes it difficult for the DRAC III to communicate with its correspondent system running Windows.

To access the management station from the DRAC III through two distinct paths, you must assign a demand-dial route to the DRAC III from the managed system that does not conflict with the network-based local LAN route.


To assign this demand-dial route, perform the following steps:

- 1 Configure dial-up networking on the management station to assign static IP addresses for dial-in purposes. This configuration requires two addresses: one for the management station and one for the DRAC III.

 **NOTE:** It is important that the static IP addresses used by the management station be on a different subnet from the DRAC III network adapter.

Typically, the address that is numerically lower is assigned to the management station and the higher address is assigned to the DRAC III when the dial-in connection is complete.

- 2 Configure the management station's static IP address as the demand-dial destination IP address on the DRAC III. Next, configure this same address on the DRAC III as an SNMP trap destination (for SNMP trap alerts), or as the SMTP server address (for e-mail alerts).

 **NOTE:** If you use DHCP to assign these IP addresses, you must ensure that both addresses used by the management station for dialing-in are on a different subnet from the DRAC III network adapter.

The management station is now able to receive alerts from the DRAC III through both the network and the dial-in connection.

## Configuring Systems Running Windows 95 and Windows 98 to Dial In to the DRAC III

- 1** Ensure that dial-up networking is installed.
  - a** Click the **Start** button, point to **Settings**, and click **Control Panel**.
  - b** Click the **Add/Remove Programs** icon.
  - c** In the **Add/Remove Programs Properties** dialog box, click the **Windows Setup** tab, select **Communications** in the list, and then click **Details**.
  - d** In the **Communications** dialog box, ensure that **Dial-Up Networking** and **Phone Dialer** are selected (checked). If not, install these components.

It may be necessary to download **msdun13.exe** from the Microsoft website for Windows 95; this file contains patches that enhance dial-up networking.
- 2** Return to the Control Panel and click the **Network** icon.
- 3** On the **Configuration** tab, ensure that **Client for Microsoft Networks**, **Dial-Up Adapter**, and the **TCP/IP** options are installed. If not, install the components by performing one or both of the following:
  - If the **Dial-Up Adapter** option is missing, click **Add**; next, in the **Select Network Component Type** dialog box, click **Adapter**.
  - If the **TCP/IP** option is missing, click **Add**; next, in the **Select Network Component Type** dialog box, click **Protocol**.
- 4** In the **Network** dialog box, select **TCP/IP→Dial-Up Adapter** and click **Properties**.

The properties in the **TCP/IP Properties** dialog box *must* remain at their defaults. Confirm the following settings:

  - On the **IP Address** tab, ensure that **Obtain an IP Address Automatically** is selected.
  - On the **WINS Resolution** tab, ensure that **Disable WINS Resolution** is selected.
  - On the **Gateway** tab, ensure that **New gateway** is blank.
- 5** In the **TCP/IP Properties** dialog box, click **OK**.
- 6** In the **Network** dialog box, click **OK**.
- 7** Close the **Control Panel** window.
- 8** Click the **Start** button, point to **Programs**, point to **Accessories**, and click **Dial-Up Networking**.
- 9** In the **Dial-Up Networking** dialog box, click **Make New Connection** and type in the modem, name of the DRAC III, and telephone number of the DRAC III.
- 10** After you make the new connection, right-click on the connection and click **Properties**.
- 11** Click the **Server Types** tab, and ensure that only **TCP/IP** is selected (checked).
- 12** Click **TCP/IP Settings** and ensure that only **Server Assigned IP address**, **Server Assigned Name Server Addresses**, and **Use IP Header Compression** are selected (checked).

## Configuring Systems Running Windows 2000 to Dial In to the DRAC III



**NOTE:** The following instructions vary slightly depending on the system's Windows 2000 configuration.

- 1 Click the **Start** button, point to **Settings**→**Control Panel**→**Network and Dialup Connections**, and click **Make New Connection**.
- 2 Click **Next**.
- 3 Select **Dial-Up to a private network**.
- 4 Click **Next**.
- 5 Enter the telephone number of the DRAC III to which you want to connect.
- 6 Click **Next** three times.
- 7 Type a name for this connection.
- 8 Click **Finish**.
- 9 Click the **Start** button, point to **Settings**→**Control Panel**→**Network and Dialup Connections**, right-click the connection you just created and named, and select **Properties**.
- 10 Click the **Networking** tab.
- 11 Ensure that **Type of dial-up server I am calling** is set to **PPP: Windows 95/98/2000, Internet**.
- 12 Ensure that **Internet Protocol (TCP/IP)** is checked.
- 13 Click **Properties**.
- 14 Click **Advanced**.
- 15 Deselect (clear) **Use default gateway on remote network**.
- 16 Click **OK** twice.
- 17 Click the **Security** tab.
- 18 Ensure that **Allow Unsecured Password** is selected (different service pack versions of Windows 2000 may move this option around, refer to it as **Clear Text**, or present it as a check box; ensure that you find this option and select it).
- 19 Click **OK**.
- 20 Reboot your system.

## Configuring Systems Running Windows Server 2003 to Dial In to the DRAC III

- 1 Click the **Start** button, point to **Control Panel**→**Network Connections**, and click **New Connection Wizard**.
- 2 Click **Next**.
- 3 Select **Connect to the network at my workplace** and click **Next**.
- 4 Select **Dial-up connection** and click **Next**.
- 5 Enter a name in the **Company Name** field and click **Next**.



- 6 Enter the telephone number of the DRAC III to which you want to connect and click **Next**.
- 7 Select **Anyone's use** and click **Next**. If you only want the current user account to be able to use the dial-in connection, select **My use only**.
- 8 Click **Finish**. Create a shortcut on your desktop if you want one.
- 9 Click the **Start** button, point to **Connect To**, and then click the connection you just created and named.
- 10 Click **Properties**.
- 11 Click the **Security** tab.
- 12 Ensure that the **Allow Unsecured Password** option is selected.
- 13 Click **OK**.
- 14 Click the **Networking** tab.
- 15 Click **Properties**.
- 16 Click **Advanced**.
- 17 Deselect (clear) the **Use default gateway on remote network** option and click **OK**.
- 18 Enter the IP address for the PPP adapter.  
To find the IP address for the PPP adapter, open a command prompt and type `ipconfig`, and locate the IP address under **PPP adapter**.
- 19 Click **OK**.
- 20 Ensure that **Type of dial-up server I am calling** is set to **PPP: Windows 95/98/NT4/2000, Internet**.
- 21 Enable the **Internet Protocol (TCP/IP)** field and click **OK**.
- 22 Reboot your system.

## Configuring Systems Running the Red Hat Linux Operating System to Dial In to the DRAC III



**NOTICE:** Before beginning this procedure, PPP must first be configured and installed on the client system. PPP-2.3 or later is available from the Red Hat® website at [www.redhat.com](http://www.redhat.com).

- 1 Download and configure the latest PPP (2.3.11 or later) source code.
- 2 Read the `readme.cbcp` file included in the PPP software distribution.
- 3 Apply the patch included in the `readme.cbcp` file, and then make and install as usual.
- 4 To test whether your PPP daemon supports the callback protocol, open a command shell and issue the following command:

```
pppd callback 1111
```

If your PPP daemon is not properly configured, it generates an error message about the callback option.

- 5 After verifying that your PPP daemon is configured with callback support, you must set up the proper chat scripts for your environment.

An example modem setup is described at [www-cache.mppmu.mpg.de/callback/linuxanalog.html](http://www-cache.mppmu.mpg.de/callback/linuxanalog.html).

- 6 Create the file `/etc/ppp/peers/rac` with the following contents:

```
tty02 crtcts 38400

connect 'chat -v -f /etc/ppp/chat/rac'

noipdefault

nodefaultroute

lock

user <username>

remotename <rac>
```

where `<username>` is the DRAC III user name that is supplied to the DRAC III, and `<rac>` is the name preferred for the DRAC III.

- 7 Create the file `/etc/ppp/chat/rac` with the following contents, where the actual telephone number replaces 555-1212.

This chat script assumes a modem with a standard AT command set and may need to be modified if the actual modem does not support this command set:

```
ABORT "NO CARRIER"

ABORT "NO DIALTONE"

ABORT "ERROR"

ABORT "NO ANSWER"

ABORT "BUSY"


"" "at"

OK "at&d2&d1"

OK "atdt555-1212"
```


- 8 Edit the `/etc/ppp/chap-secrets` file (which lists PPP users and passwords) to include the DRAC III PPP user.

Using the following example as a guideline, add a single line to the file.

 **NOTE:** The `<username>` and `<rac>` values in the following example must match the `<username>` and `<rac>` values placed in the `/etc/ppp/peers/rac` file in step 7.

```
# client server secret IP addresses
<username> <rac> <password> *
```

where `<password>` is the password that is supplied to the DRAC III during the authentication phase of PPP negotiation.

 **NOTE:** The IP address value (indicated by the `*` symbol in the previous example) is not used when acting as a PPP client.

## Configuring Management Stations Running Windows to Receive DRAC III Dial-Out Alert Notifications

For DRAC III dial-out alert notifications, you can specify a single SMTP system for receiving e-mail with up to eight SNMP trap destinations. When you specify the IP address of the SMTP system or any of the SNMP trap addresses in a demand dial-out entry, the DRAC III dials the telephone number specified in the demand dial-out entry to deliver an e-mail or SNMP trap to the SMTP system or SNMP trap addresses. If you do not specify the IP address of the SMTP system, or any of the SNMP trap addresses in a demand dial-out entry, the DRAC III network adapter is used to deliver the e-mail or SNMP trap to the SMTP system or SNMP trap addresses.


To support the dial-out notification feature on the DRAC III, the management station must allow for dial-in. See the following subsections for instructions about configuring dial-out alert notifications.

### Configuring Management Stations Running Windows 2000 to Receive DRAC III Dial-Out Alert Notification

To configure your Windows 2000 management station so that the DRAC III can establish a connection and log an alert, you must add a new local user.

To add a new local user, perform the following steps:

- 1 At the management station, click the **Start** button, point to **Settings**→**Control Panel**→**Users and Passwords**.

 **NOTE:** You must be logged on as an administrator to access this setting.

- 2 From the **Users and Passwords** window, click the **Advanced** tab, and then click **Advanced**.
- 3 Under **Local Users and Groups**, click **Users**, and then click **Action**.
- 4 Click **New User**.

- 5 In the **New User** window, type in a **Username**, **Password**, and **Confirm Password**.
- 6 Ensure that the **User must change password at next login** check box is *not* selected.
- 7 Select the **Password Never Expires** check box.
- 8 Click **Create** to create the new user.
- 9 Click **Close**.

### **Configuring Management Stations Running Windows Server 2003 to Receive DRAC III Dial-Out Alert Notification**

To enable a Windows Server 2003 management station to receive and log an alert from a DRAC III, you must add a new local user to the management station by performing the following steps:

- 1 Log on with administrator privileges.
- 2 Click the **Start** button and select **Administrative Tools** and then click **Computer Management**.
- 3 Click the + sign to expand **Local Users and Groups**.
- 4 Select the **Users** folder.
- 5 Click **Action** at the top of the screen and select **New User**.
- 6 Enter your new user information in all of the fields and click **Create**.
- 7 Click **Close**.

### **Configuring the Management Station Dial-Up Modem for DRAC III**

If you want to use the modem on your management station to dial-up the DRAC III, you must first configure the management station's modem. The following sections provide instructions for configuring the modem on Windows 2000 Server, Windows Server 2003, and Windows XP management stations.

#### **Configuring the Dial-Up Modem on Management Stations Running Windows 2000 Server**

- 1 Click the **Start** button, point to **Settings**, point to **Control Panel**, and double-click **Phone and Modem Options**.
- 2 In the **Phone and Modem Options** dialog box, click the **Modems** tab, and click **Add**.
- 3 Follow the instructions in the **Add/Remove Hardware Wizard**.
- 4 Repeat steps 2 and 3 for each modem you want to install.

- 5 To configure a dial-up connection, click the **Start** button, point to **Settings**, click **Control Panel**, double-click **Network and Dial-up Connections**, and double-click **Make new connection**.
- 6 Follow the instructions in the Network Connection Wizard.

### **Configuring the Dial-Up Modem on Management Stations Running Windows Server 2003**

- 1 To configure a dial-up connection, click the **Start** button, point to **Control Panel**→**Network Connections**, and click **New Connection Wizard**.
- 2 Follow the instructions in the New Connection Wizard.

### **Configuring the Dial-Up Modem on Management Stations Running Windows XP**

- 1 To configure a dial-up connection, click the **Start** button, point to **Control Panel**→**Network Connections**, and click **New Connection Wizard**.
- 2 Follow the instructions in the New Connection Wizard.
- 3 Click **Create a new connection**.
- 4 In the **Network Connection** type window, select **Connect to the network at my workplace** and click **Next**.
- 5 In the **Network Connection** window, select **Dial-up connection** name and click **Next**.
- 6 Enter the telephone number of the telephone line connected to the RAC and click **Next**.
- 7 In the **Connection Availability** window, select **Anyone's use** or **My use only** depending upon your preference and click **Next**.
- 8 Click **Finish**.

## **Accessing a DRAC III Through a Modem**

When you connect to a DRAC III over a modem, the DRAC III functions as a RAS system by providing an IP address to the remote console. The DRAC III can obtain IP addresses using one of the following methods:

- Through a DHCP server, when DHCP is enabled
- From the base IP address, if it is not 0.0.0.0
- From a default IP address that is autogenerated by the DRAC III (ensuring that two DRAC III cards do not have the same IP address)



**NOTE:** By default, the IP address is autogenerated by the DRAC III on the 10.0.0.0 network.

The following sections provide instructions for accessing the managed system's DRAC III by modem from a previously-configured dial-in client. If you have not yet added and configured the client system for dial-in to the DRAC III, see "Changing the PPP Server IP Address on the Managed System."

## Accessing the DRAC III Through a Modem From Systems Running Windows 95 or Windows 98

- 1 Click the **Start** button, point to **Programs**→**Accessories**, and click **Dial-Up Networking**.
- 2 In the **Dial-Up Networking** dialog box, double-click the connection that you created and named in "Configuring the Management Station's Modem."
- 3 Enter the user name and password for the DRAC III and click **Connect**.
- 4 After the connection is accepted, open your Web browser and type the following address:  
`http://<remote_IP_address>`

where *<remote\_IP\_address>* is the DRAC III IP address.

If you do not know the IP address assigned to the DRAC III, you can calculate it by performing the following steps:

- a Click the **Start** button, point to **Programs**, and click **MS-DOS Prompt**.
- b At the MS-DOS<sup>®</sup> prompt, type the appropriate command for your operating system:  
 If you are running Windows 95, type `winipcfg`.  
 If you are running Windows 98, type `ipconfig`.
- c Press **<Enter>**.
- d In the **IP Configuration** dialog box, click the down-arrow on the drop-down menu and select **PPP Adapter**.  
 The **IP Configuration** dialog box *does not* display the remote IP address assigned to the DRAC III, but it *does* display the local IP address in the **IP Address** field.
- e Calculate the DRAC III remote IP address by incrementing the PPP adapter IP address by one.

## Accessing the DRAC III Through a Modem From Systems Running Windows 2000 Server

- 1 Click the **Start** button, point to **Settings**→**Network And Dial-Up Connections**, and click the connection that you created and named in "Configuring the Management Station's Modem."
- 2 In the screen displayed in step 1, type your user name and password if they are not already there, ensure that any **Domain** box is deselected (unchecked), and click **Dial**, **Connect**, or the equivalent.
- 3 After the connection is accepted, open your Web browser and type in the following address:  
`http://<remote_IP_address>`

where *<remote\_IP\_address>* is the DRAC III IP address.

If you do not know the IP address assigned to the DRAC III, you can calculate it by performing the following steps:

**a** Click the **Start** button, point to **Programs**, and click **Command Prompt**.

**b** At the prompt, type the following command and press <Enter>:

```
ipconfig
```

The **ipconfig** command *does not* display the remote IP address assigned to the DRAC III, but it *does* display the local IP address.

**c** Calculate the DRAC III remote IP address by incrementing the IP address by one.

### **Accessing the DRAC III Through a Modem From Systems Running Windows Server 2003**

**1** Click the **Start** button, point to **Connect To**, and click the DRAC III connection that you created and named in "Configuring the Management Station's Modem."

**2** In the screen displayed in step 1, type your user name and password if they are not displayed, ensure that any **Domain** box is deselected (unchecked), and click **Dial**, **Connect**, or the equivalent.

**3** After the connection is accepted, open your Web browser and enter in the following address:

```
http://<remote_IP_address>
```

where *<remote\_IP\_address>* is the DRAC III IP address.

If you do not know the IP address assigned to the DRAC III, you can calculate it by performing the following steps:

**a** Click the **Start** button, point to **Programs**, and click **Command Prompt**.

**b** At the prompt, type the following command and press <Enter>:

```
ipconfig
```

The **ipconfig** command *does not* display the remote IP address assigned to the DRAC III, but it *does* display the local IP address.

**c** Calculate the DRAC III remote IP address by incrementing the IP address by one.

### **Accessing the DRAC III Through a Modem From Systems Running Windows Server XP**

**1** Click the **Start** button, point to **Connect To**, and click the DRAC III connection that you created and named in "Configuring the Management Station's Modem."

**2** In the screen displayed in step 1, type your user name and password if they are not displayed, ensure that any **Domain** box is deselected (unchecked), and click **Dial**, **Connect**, or the equivalent.

**3** Double-click the connection icon in the system tray in the bottom-right corner of your screen.

**4** Click **Status** and click the **Details** tab.

**5** Note the **IP Address Value**. If you want to connect to the RAC remote Web-based interface, type this IP address to your Web browser.

## Accessing the DRAC III Through a Modem From Systems Running Red Hat Linux

- 1 Establish a connection to the DRAC III using the following command (where # is the command shell prompt):

```
# pppd call rac
```

- 2 After the connection is accepted, determine the IP address assigned to the DRAC III. Both the local and remote addresses are logged in the system log as shown in the following example:

```
Apr 7 22:59:24 myhost pppd[187]: local IP address 10.19.250.93
```

```
Apr 7 22:59:24 myhost pppd[187]: remote IP address 10.19.250.94
```

In this example, you would type the following Web address into the address box of your Web browser:

```
http://10.19.250.94.
```

## Accessing the DRAC III Remote Access Interface Using VT-100 Terminal Emulation

For information about using VT-100 terminal emulation with a DRAC III, including communication port settings, see "Using VT-100 Terminal Emulation With a DRAC III."

## Uninstalling the DRAC III Hardware


To uninstall the DRAC III from your system, follow the instructions for installing the DRAC III at the beginning of this section, and then uninstall the components and cables in the reverse order that they were installed.

## Replacing the DRAC III Battery

The following subsections describe the replacement of the DRAC III battery, including removing and installing the battery pack.

 **CAUTION:** Before removing or installing any system component, see the *System Information Guide* included with your system for important safety instructions.

### Removing the Battery Pack

 **CAUTION:** Before you perform this procedure, you must turn off the system and disconnect it from its power source. Only trained service technicians are authorized to remove the system cover and access any of the components inside the system. Read and follow all safety precautions in your *System Information Guide*.

- 1 Turn off the system and all attached external peripheral devices.



- 2 Disconnect the system and its peripherals from power sources, and any telephone or telecommunication lines from the system.
- 3 Remove the system cover according to the instructions in your system's *Installation and Troubleshooting Guide*.
- 4 Touch an unpainted metal surface at the back of the system chassis before touching anything inside the system.
- 5 Remove the DRAC III from its slot.
- 6 Disconnect the battery wire harness from the DRAC III.
- 7 Remove the two screws from the battery housing.
- 8 Squeeze the sides of the battery to release locking clips and remove.

### Installing a New Battery Pack




**CAUTION:** Before you perform this procedure, you must turn off the system and disconnect it from its power source. Only trained service technicians are authorized to remove the system cover and access any of the components inside the system. Read and follow all safety precautions in your *System Information Guide*.

- 1 Insert locking clips into slots in the card, ensuring that the wire harness is toward the top of the card.
- 2 Attach the battery pack to the card using the two screws.
- 3 Connect the battery wire harness to the header.
- 4 Insert the DRAC III into the same slot from which it was removed and reattach connectors or cables.
- 5 Replace and secure the system cover.
- 6 Reconnect the system and all associated external peripheral devices to power sources and turn them on.



## Getting Started With Your DRAC III/XT

This section provides information specifically about DRAC III/XT. It includes a list of DRAC III/XT features, DRAC III/XT kit contents, supported systems, hardware installation instructions, and a software configuration overview.

 **NOTE:** Throughout the remainder of this document, the system in which the RAC is installed or embedded is referred to as the *managed system*. A system that remotely accesses the RAC is referred to as a *management station*. The term *system console* refers to a system's keyboard, mouse, and monitor.

### DRAC III/XT Features

The DRAC III/XT is a 33-MHz PCI card with its own microprocessor and memory. Under normal operating conditions, the DRAC III/XT is powered by the system in which it is installed. For a complete list of RAC features, see "Remote Access Controller Features."

The DRAC III/XT may be preinstalled on your system, or available separately in a kit. To get started with a DRAC III/XT that is already installed on your system, see "Software Installation and Configuration Overview." If the DRAC III/XT is not installed on your system, see "Installing the DRAC III/XT Hardware" before beginning the software installation and configuration.


### DRAC III/XT Kit Contents

- DRAC III/XT hardware
- *Dell OpenManage Server Assistant* CD
- *Dell OpenManage Systems Management* CD
- *Dell OpenManage Product Documentation* CD


### Supported Systems

DRAC III/XT is supported on following systems:


- Dell™ PowerEdge™ 1600SC
- PowerEdge 650

 **NOTE:** See your `racread.txt` file for the most current list of supported systems.


## Installing the DRAC III/XT Hardware

 **CAUTION:** Only trained service technicians are authorized to remove and access any components inside the system. See your *System Information Guide* for complete information about safety precautions, working inside the computer, and protecting against electrostatic discharge.


- 1 Turn off the system and all attached peripheral devices.
- 2 Disconnect the system and peripherals from electrical outlets. Disconnect any telephone or telecommunication lines from the system.

 **CAUTION:** Only trained service technicians are authorized to remove and access any components inside the system. See your *System Information Guide* for complete information about safety precautions, working inside the computer, and protecting against electrostatic discharge.


- 3 Before touching anything inside the system, touch an unpainted metal surface at the back of the system chassis to dissipate any static electricity that might harm internal components.

 **NOTICE:** Failure to dissipate static electricity may damage or destroy static-sensitive components.

- 4 Remove the system cover according to the instructions in your system's *Installation and Troubleshooting Guide*.
- 5 Install the DRAC III/XT according to the expansion card installation instructions in your *Installation and Troubleshooting Guide*.

 **NOTE:** On the PowerEdge 1600SC system, the DRAC III/XT must be installed in PCI slot 6.

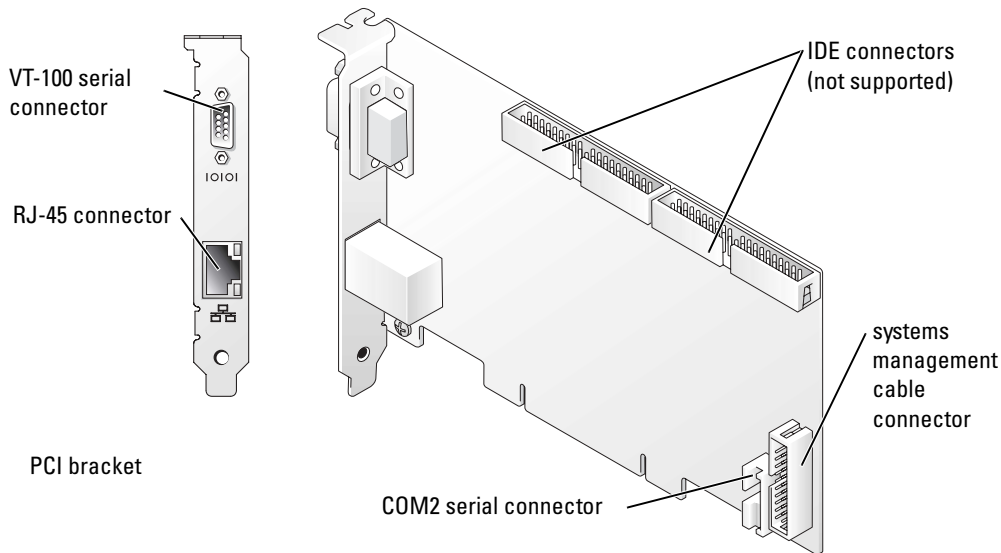
- 6 If you are using a network connection with the DRAC III/XT, attach the twisted-pair cable to the RJ-45 connector on the DRAC III/XT. See Figure 3-1 for the location of this connector.

 **NOTE:** The maximum length allowed for the LAN cable connected to the RJ-45 connector is 328 feet (100 m).

- 7 Follow the instructions in your *Installation and Troubleshooting Guide* to reassemble the system and replace the system cover.
- 8 Reconnect the system and peripheral devices to their electrical outlets, and turn them on.

After completing the hardware installation procedure, you must install and configure the RAC software. For more information on the RAC software components, see "Software Components." Before beginning the software installation and configuration, see "Software Installation and Configuration Overview."

**Figure 3-1. DRAC III/XT Hardware Components**



## Software Installation and Configuration Overview

This section provides a high-level overview of the RAC software installation and configuration process for the DRAC III/XT. Some steps give you the option of using several different tools to perform the configuration, including Server Administrator, the racadm CLI utility, and your operating system utilities.

For more information about the RAC software components, see "Software Components."

Depending on the tool used to perform the configuration, see the following documents for more information:

- *Dell OpenManage Server Administrator User's Guide*
- *Dell Remote Access Controller Racadm User's Guide*
- Operating system documentation

To install and configure your RAC software, perform the following steps in their *numbered order*:

- 1** Update the system BIOS. See "Updating the System BIOS."
- 2** Install the software on the managed system. See "Installing the Software on the Managed System."
- 3** On managed systems running Microsoft® Windows® Server 2003 and Windows 2000 operating systems, add and configure the RAS. See "Configuring RAS PPP Connection."

- 4 Configure the RAC network settings. See "Configuring the RAC Network Settings Using the Option ROM."
- 5 Add and configure RAC users. See "Adding and Configuring RAC Users."
- 6 Install (or upgrade) the software on the management station. See "Installing (or Upgrading) the Software on the Management Station."
- 7 Configure the Web browser to connect to the remote access interface. See "Configuring the Web Browser to Connect to the Remote Access Interface."
- 8 Connect to the remote access interface. See "Connecting to the Remote Access Interface."

## Updating the System BIOS

If you are adding a RAC to an existing managed system, it is recommended that you update the system's BIOS before installing the RAC to ensure full support for the card. See "Updating the System BIOS."

## Installing the Software on the Managed System

Install the software on the managed system using the *Systems Management CD*.

For instructions about installing this software, see your *Server Administrator User's Guide*.

The managed system has the following components embedded or installed: the RAC, the appropriate version of Server Administrator, and the appropriate RAC agent. Depending on the operating system, the RAC agent consists of either Microsoft® Windows® services, Novell® NLMs, or Red Hat® Linux drivers and daemons. The RAC agent automatically starts when you boot the managed system.

## Configuring the RAC Network Settings

Configure the RAC network settings using one of the following tools:

- Server Administrator
- IT Assistant
- racadm CLI utility
- RAC Option ROM — See "Configuring the RAC Network Settings Using the Option ROM."
- Serial and telnet consoles — See "Configuring a RAC to Use a Serial or Telnet Text Console."



**NOTE:** If you are deploying the RAC in a Red Hat Linux environment, see "Connecting to the Remote Access Interface."

## Adding and Configuring RAC Users

Add and configure RAC users using one of the following tools:

- Server Administrator
- IT Assistant

- racadm CLI utility
- Serial and telnet consoles — See "Configuring a RAC to Use a Serial or Telnet Text Console."



**NOTE:** For more information about user types, see "RAC User Types."

## **Installing (or Upgrading) the Software on the Management Station**

If necessary, install (or upgrade) the software on the management station, including Server Administrator, using the *Systems Management CD*.

For instructions about installing Server Administrator software, see your *Server Administrator User's Guide*.

A management station is a system (typically a workstation running Windows Server 2003 or Windows 2000) that has the following components installed: appropriate versions of Server Administrator, a supported Web browser (for more information, see "Supported Web Browsers"), Windows services (if applicable), Server Administrator services, and user interface elements.

## **Configuring the Web Browser to Connect to the Remote Access Interface**

If you are using a client system that connects to the Internet through a proxy server to connect to the RAC Web-based remote access interface, you must configure your Web browser for this connection.

See "Configuring a Web Browser to Display the Remote Access Interface."

## **Connecting to the Remote Access Interface**

To connect to the remote access interface through the network connection, see "Connecting to the Remote Access Interface."

## **Uninstalling the DRAC III/XT Hardware**


To uninstall the DRAC III/XT from your system, follow the instructions for installing the DRAC III/XT at the beginning of this section, and then uninstall the components and cables in the reverse order that they were installed.





# Getting Started With Your ERA

This section provides information specifically about ERA. It includes a list of ERA features, supported systems, and a software configuration overview.

 **NOTE:** Throughout the remainder of this document, the system in which the RAC is installed or embedded is referred to as the *managed system*. A system that remotely accesses the RAC is referred to as a *management station*. The term *system console* refers to a system's keyboard, mouse, and monitor.


## ERA Features

ERA is an embedded controller with its own microprocessor and memory that uses a proprietary bus and is powered by the system in which it is installed.

To get started installing and configuring your ERA software, see "Software Installation and Configuration Overview."

## Supported Systems

- Dell™ PowerEdge™ 2650 system
- Dell PowerVault™ 775N NAS system

 **NOTE:** See your `racread.txt` file for the most current list of supported systems.

## Software Installation and Configuration Overview

This section provides a high-level overview of the RAC software installation and configuration process for ERA. Some steps give you the option of using several different tools to perform the configuration, including Server Administrator, the `racadm` CLI utility, and your operating system utilities.

For more information about the RAC software components, see "Software Components."

Depending on the tool used to perform the configuration, see the following documents for more information:

- *Dell OpenManage Server Administrator User's Guide*
- *Dell Remote Access Controller Racadm User's Guide*
- Operating system documentation

To install and configure your RAC software, perform the following steps in their *numbered order*:

- 1 Install the software on the managed system. See "Installing the Software on the Managed System."
- 2 On managed systems running Microsoft® Windows® Server 2003 and Windows 2000 operating systems, add and configure the RAS. See "Configuring RAS PPP Connection."
- 3 Configure the RAC network settings. See "Configuring the RAC Network Settings."
- 4 Add and configure RAC users. See "Adding and Configuring RAC Users."
- 5 Install (or upgrade) the software on the management station. See "Installing (or Upgrading) the Software on the Management Station."
- 6 Configure the Web browser to connect to the remote access interface. See "Configuring the Web Browser to Connect to the Remote Access Interface."
- 7 Connect to the remote access interface. See "Connecting to the Remote Access Interface."

### Installing the Software on the Managed System

Install the software on the managed system using the *Systems Management CD*.

For instructions on installing this software, see your *Server Administrator User's Guide*.

The managed system has the following components embedded or installed: the RAC, the appropriate version of Server Administrator, and the appropriate RAC agent. Depending on the operating system, the RAC agent consists of either Microsoft® Windows® services, Novell® NLMs, or Red Hat® Linux drivers and daemons. The RAC agent automatically starts when you boot the managed system.

### Configuring the RAC Network Settings

Configure the RAC network settings using one of the following tools:

- Server Administrator
- Racadm CLI utility
- RAC Option ROM — See "Configuring the RAC Network Settings Using the Option ROM."
- Serial and telnet consoles — See "Configuring a RAC to Use a Serial or Telnet Text Console."



**NOTE:** If you are deploying the RAC in a Red Hat Linux environment, see "Connecting to the Remote Access Interface."

### Adding and Configuring RAC Users

Add and configure RAC users using one of the following tools:

- Server Administrator
- Racadm CLI utility
- Serial and telnet consoles — See "Configuring a RAC to Use a Serial or Telnet Text Console."



**NOTE:** For more information about user types, see "RAC User Types."

## **Installing (or Upgrading) the Software on the Management Station**

If necessary, install (or upgrade) the software on the management station, including Server Administrator, using the *Systems Management* CD.

For instructions about installing this software, see your *Server Administrator User's Guide*.

A management station is a system (typically a workstation running Windows Server 2003 or Windows 2000) that has the following components installed: appropriate versions of Server Administrator, a supported Web browser (for more information, see "Supported Web Browsers"), Windows services (if applicable), Server Administrator services, and user interface elements.

## **Configuring the Web Browser to Connect to the Remote Access Interface**

If you are using a client system that connects to the Internet through a proxy server to connect to the RAC Web-based remote access interface, you must configure your Web browser for this connection.

See "Configuring a Web Browser to Display the Remote Access Interface."


## **Connecting to Your RAC**

To connect to the RAC through the network connection, see "Connecting to the Remote Access Interface."



# Getting Started With Your ERA/O

This section provides information specifically about ERA/O. It includes a list of ERA/O features, ERA/O kit contents, supported systems, hardware installation instructions, and a software configuration overview.

 **NOTE:** Throughout the remainder of this document, the system in which the RAC is installed or embedded is referred to as the *managed system*. A system that remotely accesses the RAC is referred to as a *management station*. The term *system console* refers to a system's keyboard, mouse, and monitor.

## ERA/O Features

The ERA/O is an optional embedded system card with its own microprocessor and memory, and is powered by the system in which it is installed.


The ERA/O may be preinstalled on your system, or available separately in a kit. To get started with an ERA/O that is already installed on your system, see "Software Installation and Configuration Overview." If an ERA/O is not installed on your system, see the document that is included in your ERA/O kit for hardware installation instructions.

## ERA/O Kit Contents

- ERA/O hardware
- Riser board
- Plastic retention clip
- The document *Installing an ERA/O Card*
- *Dell OpenManage Server Assistant* CD
- *Dell OpenManage Systems Management* CD
- *Dell OpenManage Product Documentation* CD

## Supported Systems

- Dell™ PowerEdge™ 1650, 1750, and 2600 systems
- Dell PowerVault™ 770N NAS system

 **NOTE:** See your `readme.txt` file for the most current list of supported systems.

## Installing the ERA/O Hardware

If the ERA/O card is not already installed on your system, you must first install the hardware before configuring the software. For information on installing the ERA/O hardware, see the document "Installing an ERA/O Card" included in the ERA/O kit. After the hardware is installed, see "Software Installation and Configuration Overview" for information on installing and configuring ERA/O software.

## Software Installation and Configuration Overview

This section provides a high-level overview of the RAC software installation and configuration process for ERA/O. Some steps give you the option of using several different tools to perform the configuration, including Server Administrator, the Racadm CLI utility, and your operating system utilities.

For more information about the RAC software components, see "Software Components."

Depending on the tool used to perform the configuration, you will need to reference the following documents for more information:

- *Server Administrator User's Guide*
- *Racadm User's Guide*
- Operating system documentation

To install and configure your RAC software, perform the following steps in their *numbered order*:

- 1 Update the system BIOS. See "Updating the System BIOS."
- 2 Install the software on the managed system. See "Installing the Software on the Managed System."
- 3 Install (or upgrade) the software on the management station. See "Installing (or Upgrading) the Software on the Management Station."
- 4 On managed systems running Microsoft® Windows® Server 2003 and Windows 2000 Server operating systems, add and configure the RAS. See "Configuring RAS PPP Connection."
- 5 Add and configure RAC users. See "Adding and Configuring RAC Users."
- 6 Configure the RAC network settings. See "Configuring the RAC Network Settings."
- 7 Configure the Web browser to connect to the remote access interface. See "Configuring the Web Browser to Connect to the Remote Access Interface."
- 8 Connect to the remote access interface. See "Connecting to the Remote Access Interface."

### Updating the System BIOS

If you are adding a RAC to an existing managed system, it is recommended that you update the system's BIOS before installing the RAC to ensure full support for the card. See "Updating the System BIOS."

## Installing the Software on the Managed System

Install the software on the managed system using the *Systems Management CD*.

For instructions about installing this software, see your *Server Administrator User's Guide*.


The managed system has the following components embedded or installed: the RAC, the appropriate version of Server Administrator, and the appropriate RAC agent. Depending on the operating system, the RAC agent consists of either Windows services, Novell® NLMs, or Red Hat® Linux drivers and daemons. The RAC agent automatically starts when you boot the managed system.

## Installing (or Upgrading) the Software on the Management Station

If necessary, install (or upgrade) the software on the management station, including Server Administrator, using the *Systems Management CD*.

For instructions on installing this software, see your *Server Administrator User's Guide*.


A management station is a system (typically a workstation running Windows Server 2003 or Windows 2000) that has the following components installed: appropriate versions of Server Administrator, a supported Web browser (for more information, see "Supported Web Browsers"), Windows services (if applicable), Server Administrator services, and user interface elements.

 **NOTE:** If you use Netscape Navigator 7.01 (or later), you need to install a supported JVM. Otherwise, you cannot access the RAC Web-based interface using Netscape Navigator.

## Adding and Configuring RAC Users

Add and configure RAC users using one of the following tools:

- Server Administrator
- Racadm CLI utility
- Serial and telnet consoles — See "Configuring a RAC to Use a Serial or Telnet Text Console."

 **NOTE:** For more information on user types, see "RAC User Types."

## Configuring the RAC Network Settings

Configure the RAC network settings using one of the following tools:

- Server Administrator
- Racadm CLI utility
- RAC Option ROM — See "Configuring the RAC Network Settings Using the Option ROM."
- Serial and telnet consoles — See "Configuring a RAC to Use a Serial or Telnet Text Console."

 **NOTE:** If you are deploying the RAC in a Red Hat Linux environment, see "Connecting to the Remote Access Interface."

## **Configuring the Web Browser to Connect to the Remote Access Interface**

If you are using a client system that connects to the Internet through a proxy server to connect to the RAC Web-based remote access interface, you must configure your Web browser for this connection.

See "Configuring a Web Browser to Display the Remote Access Interface."

## **Connecting to the RAC**

To connect to the remote access interface through the network connection, see "Connecting to the Remote Access Interface."

## **Uninstalling the ERA/O Hardware**

To uninstall the ERA/O from your system, follow the instructions for installing the ERA/O at the beginning of this section, and then uninstall the components and cables in the reverse order that they were installed.




## Installing and Configuring the RAC Software

This section provides RAC configuration procedures for all RACs. For a high-level overview of these procedures, including the order in which the procedures are used and which procedures apply specifically to your RAC, see your individual RAC section.

### Updating the System BIOS

If you are adding a RAC to an existing managed system, it is recommended that you update the system's BIOS before installing the RAC to ensure full support for the card.

To update the managed system's BIOS, perform the following steps:

 **NOTE:** The managed system's BIOS can also be flashed from the management station using the remote access interface Remote Floppy Boot feature. For more information, see "Remote Floppy Boot" or the remote access interface online help.

- 1 Obtain a copy of the most current version of your system's BIOS.  
Updates are available on the Dell Support website at [support.dell.com](http://support.dell.com).
- 2 From the managed system, launch the executable file and follow the prompts to create a BIOS flash diskette.
- 3 Insert the BIOS flash diskette into the managed system's diskette drive and reboot the system.  
The system boots to the BIOS update menu.
- 4 Follow the instructions on the BIOS update menu.

### Installing DRAC III Drivers on 64-Bit Systems

When installing a DRAC III on a 64-bit system, after installing the managed system software, you must install DRAC III drivers.

To install the drivers, perform the following steps:

- 1 Right-click **My Computer** and select **Properties**.
- 2 Click the **Hardware** tab and select **Device Manager**.
- 3 From the **Device Manager** window, right-click one of the three **Unknown PCI Device** entries and click **Update Driver**.

The operating system displays a dialog box prompting you to select the type of driver:


- a Select the option for the operating system to locate the correct driver.
- b Repeat the previous step for all three devices.

When all three drivers are installed, configure the following devices under the **Dell Remote Service Card** device:

- DRSC Port
  - PCI Function 0
  - PCI Function 2
- 4 Restart the **Dell Remote Service** from the services menu or reboot the system to implement these changes.

## Installing the Racadm Utility on Management Stations Running the Red Hat Linux Operating System

You install the racadm CLI utility on a management station running Red Hat® Linux so that the remote racadm functions can be used.

 **NOTE:** The racadm CLI utility is installed automatically for all other supported operating systems when you install the *Systems Management CD*.

To install the racadm CLI utility, insert the *Systems Management CD* in the management station's CD drive and enter the following commands from a command prompt:

```
mount /mnt/cdrom
cd /mnt/cdrom/rac20/linux
rpm -ivh racadm-2.0-1.i386.rpm
```

For help with the racadm command, enter the **man racadm** or **racadm help** command after issuing the previous commands. For more information about racadm features, see the *Racadm User's Guide*.

You can uninstall the racadm CLI utility by issuing the following command from a command prompt:

```
- rpm -e racadm
```

## Configuring RAS PPP Connection

This section contains procedures for configuring RAS on the following systems:

- Management stations running the Microsoft® Windows® XP operating system
- Management stations running the Microsoft Windows Server 2003 operating system
- Management stations running the Windows 2000 operating system

## **Configuring RAS PPP Connection on Management Stations Running Windows XP or Windows Server 2003**

- 1** Click the **Start** button and right-click **My Computer**.
- 2** Click **Manage**.
- 3** Double-click **Services and Applications**.
- 4** Double-click **Services**.
- 5** If the **Startup Type** column for **Routing and Remote Access** is not set to **Automatic**, right-click **Routing and Remote Access**.
- 6** Click **Properties**.
- 7** Click the down arrow on the **Startup Type** drop-down menu.
- 8** Click **Automatic**.
- 9** Click **Apply**.
- 10** Click **OK**.
- 11** If the **Status** column for **Routing and Remote Access** does not show **Started**, right-click **Routing and Remote Access** and click **Start**.  
The **Routing and Remote Access** service should start automatically on subsequent restarts of the management station.

## **Configuring RAS PPP Connection on Management Stations Running Windows 2000**

- 1** Right-click **My Computer**.
- 2** Click **Manage**.
- 3** Double-click **Services and Applications**.
- 4** Double-click **Services**.
- 5** If the **Startup Type** column for **Routing and Remote Access** is not set to **Automatic**, right click **Routing and Remote Access**.
- 6** Click **Properties**.
- 7** In the **Routing and Remote Access (Local Computer)** dialog box, click the down arrow on the **Startup Type** drop-down menu.
- 8** Click **Automatic**.
- 9** Click **Apply**.
- 10** Click **OK**.

- 11 If the **Status** column for **Routing and Remote Access** does not show **Started**, right-click **Routing and Remote Access** and click **Start**.

The **Routing and Remote Access** service should start automatically on subsequent restarts of the management station.

### Connecting to the Management Station From the DRAC III

You can configure the DRAC III to dial out to a management station when an event occurs. In this situation, RAS on the management station assigns the IP addresses. You can configure RAS on the management station to use DHCP or to use a static address pool.

PPP authentication occurs at the time of negotiation with RAS. To allow the DRAC III to dial out to a management station for alert notification, you must create an account on the management station with the demand dial-out entry remote user name and password configured in the DRAC III for this connection.

### Changing the PPP Server IP Address on the Managed System

To change the managed system's PPP server IP address to use another network, use the `Racadm` CLI utility according to the following sample entry:

```
racadm config -g cfgRacTuning -o cfgRacTuneMnNwIpAddrBase <new_ip>
```

where `<new_ip>` is the IP address of the new network.

For more information about using the `Racadm` CLI utility, see the *Racadm User's Guide*.

### Configuring the RAC Network Settings Using the Option ROM

RACs contain an integrated 10 BASE-T/100 BASE-T Ethernet network adapter (10 BASE-T only for ERA/O on the PowerEdge 1650 system). The network adapter has a default address of 192.168.20.1 and a default gateway of 192.168.20.1.

It is possible to configure a limited number of RAC network settings using the RAC Option ROM utility.

To access the Option ROM utility, during the managed system's boot press `<Ctrl> <D>` within 5 seconds of the time the RAC banner, firmware version, and current network adapter IP address are displayed. The **Setup** screen appears. Below the screen title is the **Network Interface Properties** menu.


This menu enables you to use a set of one-key-stroke menu options to select and change various parameters in the RAC network adapter properties. The menu selections are not case sensitive.




**NOTE:** Autonegotiation is enabled by default on the DRAC III/XT, ERA, and ERA/O controllers, and cannot be changed; therefore, the network adapters for these RACs operate at a maximum of 100 Mb/s at half duplex only. If the DRAC III/XT, ERA, or ERA/O controllers are connected directly to a network switch (without hubs in between), the corresponding port on the switch should be set to autonegotiate to eliminate conflicts and improve performance.

## Option Categories

The following is a list of the available option categories available through the Option ROM utility, including submenu options within each category.


 **NOTE:** When modifying any of the following options, you can use the <Esc> key while entering the value to avoid modifying the current value. If you press <Option Edit> and it toggles a setting (changes the setting between only two possible values), press that key again to change the value back to the original setting. The <Esc> key cannot undo a modification after a new value has been entered. The <Esc> key does not have an effect on toggle options.

- **NIC TCP/IP Settings** – Displays the current IP address, netmask, and gateway assigned to the RAC.


 **NOTE:** If DHCP is enabled on the card and something is wrong with the DHCP system, the category displays **Unavailable** for each option, and the following message blinks below the option labels:

Waiting for response from DHCP Server

- **NIC TCP/IP Configuration Options**

 **NOTE:** If the RAC is configured to the same IP address as another network adapter on the same network, an IP address conflict occurs. The RAC stops responding to network commands until the IP address is changed on the RAC. If the IP address conflict is resolved by changing the address of the other network adapter, the RAC must be reset.

- **Use DHCP is** – Indicates whether the DHCP system has assigned the RAC IP address or whether the RAC is using a preset static IP address. The available settings are **Enabled** or **Disabled**. Press <D> to toggle the setting. When enabled, the three remaining options in this group are "dimmed-out" and do not display prominently. If disabled, the remaining options display at normal brightness.

 **NOTE:** When you are assigning a predefined IP address to the RAC using a DHCP server, the DHCP server normally requires that you store a client identifier token in the server's reservations table. The client (RAC, for example) has to provide the identifier token during the DHCP negotiation phase. In the case of a RAC, the RAC supplies the client identifier token as a one-byte interface number (0, 1, or 2) followed by a six-byte MAC address. The interface number for the network adapter may be 0, 1, or 2, depending on whether DHCP for PPP is currently enabled, PPP DHCP has been enabled in the past, or PPP DHCP has never been enabled. If PPP DHCP has never been enabled and is not currently enabled, ensure that the network adapter interface number is 0.

- **Static IP-Addr** – Indicates the preset static IP address that the RAC uses if DHCP is disabled. The default is 192.168.20.1. Press <I> to change this address.
- **Static Netmask** – Indicates the preset static masked IP address of the RAC if DHCP is disabled. The default is 255.255.255.0. Press <N> to change this mask.
- **Static Gateway** – Indicates the preset static gateway (router or switch address) of the RAC address if DHCP is disabled. The default is 192.168.20.1. Press <G> to change the address.

- **Ethernet Configuration Options (DRAC III only)**
  - **NIC is** – Indicates whether the RAC network adapter setting is **Enabled** or **Disabled**. Press <E> to toggle the setting. When enabled, the RAC network adapter can be used for remote access. You must enable this option to configure any of the remaining options on this screen. When disabled, all other options are "dimmed-out" and do not display prominently. If enabled, most or all of the remaining options display at normal brightness, depending upon the **Use DHCP** setting.
  - **Auto Negotiate** – Indicates whether the DRAC III automatically configures LAN speed and duplex settings. The available settings are **Enabled** and **Disabled**. If not enabled, the user settings are used. Press <A> to toggle to this setting.
  - **LAN Speed Setting** – Indicates the speed at which the DRAC III network adapter is set to communicate. The available settings are **10 Base-T** and **100 Base-T**. 10BASE-T represents a communication speed of 10 Mb per second. 100BASE-T represents a speed of 100 Mb per second. Press <S> to toggle this setting. This option is "dimmed-out" when the **Auto Negotiate** setting is enabled.
  - **LAN Duplex Setting** – Indicates the duplex setting of the RAC network adapter. The available settings are **Half Duplex** and **Full Duplex**. When set to **Half Duplex**, the network adapter communicates in one direction at a time, indicating that at any given moment it can either receive or transmit information, but not both. When set to **Full Duplex**, the network adapter communicates in both directions simultaneously. Press <X> to toggle to this setting. This option is "dimmed-out" when the **Auto Negotiate** setting is enabled.

After you have made the changes you want, you can press <R> to save the changes and reboot the RAC, or you can press <Esc> to cancel all changes and exit the setup menu. If you decide to save your changes, the following message appears:

**IMPORTANT:** In order for your changes to take effect, they need to be saved and the card needs to be reset. That should take about 25 seconds. Your computer will then continue booting normally.

Would you like to save the changes and reset the card now (<Y> or <N>)?


Press <Y> to save the changes or <N> to return to the setup menu.

## Configuring a Web Browser to Display the Remote Access Interface

If connecting to the RAC Web-based remote access interface from a client system which connects to the Internet through a proxy server, you need to configure the Web browser to connect properly to the Web-based interface. The following sections provide configuration instructions for the following browsers supported by the RAC: Microsoft Internet Explorer 5.5 (Service Pack 2 or later) and 6.0, Netscape Navigator 7.01 and 7.02, and Mozilla 1.3 and 1.4.

## Configuring Internet Explorer 5.5 or 6.0

- 1 From the Internet Explorer main window, click **Tools**, and then click **Internet Options**.
- 2 From the **Internet Options** window, click the **Connections** tab.
- 3 Under **Local Area Network (LAN) settings**, click **LAN Settings**.
- 4 If the **Use a proxy server** box is checked, check the **Bypass proxy server for local addresses** box.
- 5 Click **OK** twice.

 **NOTE:** The Internet Explorer application embedded in the Windows Advanced Server Limited Edition operating system does not support Java applets; therefore, it is not possible to use the Advanced Server Limited Edition's Internet Explorer browser to connect to a RAC over a LAN or the Internet.

## Connecting to the Internet From Internet Explorer When the RAC PPP Service Is Running


After installing Internet Explorer 5.x or later, you may notice that the automatic configuration and proxy setting information for each connection is separate from the same information used for the LAN connection. If you are using a dial-up and a LAN connection simultaneously, Internet Explorer may block your access to the Internet.

This blocking occurs because each connection in Internet Explorer 5.0 uses its own automatic configuration and proxy settings. When this has occurred and a user tries to establish any kind of PPP connection, Internet Explorer attempts to use the dial-up connection settings to access the Internet.

To correct this problem, perform *one* of the following steps:

- If you are using Internet Explorer version 5.0, 5.01 or 5.5 (SP1), you must update your browser to Internet Explorer 5.5 (SP2). You must stop the RAC service before running the update. The update is available at [windowsupdate.com](http://windowsupdate.com).

## Configuring Mozilla 1.3 or 1.4

 **NOTE:** For a list of the supported Java Virtual Machine (JVM) plug-ins, see the `racread.txt` file on your *Systems Management CD* or at the Dell Support website at [support.dell.com](http://support.dell.com).

You must install Java Runtime Environment (JRE) to use the Mozilla Web browser. Perform the following steps to install JRE:

- 1 Launch the installation script by using the following commands from the directory in which the script is located:

```
chmod a+x j2re-1_4_<version number>-linux-i586-rpm.bin
./j2re-1_4_<version number>-linux-i586-rpm.bin
```

The script displays a binary license agreement, which you are prompted to accept before continuing the installation. After you have accepted the license agreement, the installation script creates the file `j2re-1_4_<version number>-linux-i586.rpm` in the current directory.

- 2 To become the root user, run the `su` command and enter the power-user password.
- 3 Run the following `rpm` command to install the packages. This command installs the packages comprising the Java 2 Runtime Environment (J2RE):

```
rpm -iv j2re-1_4<version number>-linux-i586.rpm
```

Only one Java plug-in can be registered at a time. If you have never registered a Java plug-in, go to the next step; otherwise, go to step 5.

Most Mozilla installations use symbolic links to where the Java plug-in is located. The name of the symbolic link is `libjavaplugin_oji.so` and it can be found in the `/plugins` subdirectory of Mozilla.

For example:


```
cd /usr/lib/mozilla<version number>/plugins
rm libjavaplugin_oji.so
```

- 4 Register the Java plug-in.

Locate the `libjavaplugin_oji.so` file in the `j2re1.4<version number>` directory. Usually it is located in the `/i386/ns600` or `/i386/ns610` subdirectory. Use the **create a symbolic link** feature in Mozilla that points to the `libjavaplugin_oji.so` file in the `/i386/ns610` subdirectory.

For example:

```
cd <Mozilla>/plugins
ln s j2re1.4<version number>/plugin/i386/ns610/libjavaplugin_oji.so libjavaplugin_oji.so
```

 **NOTE:** Create the link using the `/plugins` subdirectory of Mozilla. You cannot create the link from `<JRE>` directory.

- 5 Start Mozilla and go to **Tools**→**Web Development**→**Java Console**.

The version of JRE is displayed at the top of the Java Console window. If the version that is shown is not the same as the one you downloaded, then registering did not work. The same is true if the Java Console menu option is grayed out.

## Configuring Netscape Navigator 7.01 or 7.02

Netscape Navigator 7.01 or 7.02 requires Java Virtual Machine (JVM) 1.4 or later for both Windows and Red Hat Linux operating systems.

If you use Netscape Navigator 7.01 or 7.02, you need to install a supported JVM. Otherwise, you cannot access the RAC Web-based interface using Netscape Navigator.



## Disabling the Windows Automatic Reboot Option

To ensure that the RAC Web-based interface last crash screen feature works properly, you must disable the **Automatic Reboot** option on managed systems running the Microsoft Windows 2000 Server and Windows Server 2003 operating systems.

### Disabling the Automatic Reboot Option in Windows 2000 Server


- 1 Click the **Start** button and select **Settings**→**Control Panel**→**System**→**System Properties**.
- 2 Click the **Advanced** tab.
- 3 Click the **Startup and Recovery...** button.
- 4 Deselect the **Automatically Reboot** check box.


### Disabling the Automatic Reboot Option in Windows Server 2003

- 1 Click the **Start** button and select **Settings**→**Control Panel**→**System**→**System Properties**.
- 2 Click the **Advanced** tab.
- 3 Under **Startup and Recovery**, click **Settings**.
- 4 Deselect the **Automatically Reboot** check box.

## Connecting to the Remote Access Interface

This section provides information on accessing a RAC after the hardware is installed (if applicable) and the software is configured.

 **NOTE:** The RAC default user name is `root` and the default password is `calvin`. The default domain is `Local_RAC`.

 **NOTE:** To view localized versions of the remote access interface on Windows operating systems, open the Windows control panel and select **Regional Options**. Next, select the desired location from the **Your locale (location)** drop-down menu.

### Accessing the Remote Access Interface Through the Network

You can access the RAC Web-based remote access interface through the RAC network adapter using Server Administrator or a supported Web browser, or you can access the RAC locally or remotely using the `racadm` CLI utility.

To access the RAC remote access interface using Server Administrator, first launch Server Administrator. From the system tree on the left pane of the Server Administrator home page, click **System**→**Main System Chassis**→**Remote Access Controller**. For more information about using Server Administrator remote access features, see your *Server Administrator User's Guide*.

To access the RAC using a supported Web browser, type the IP address of the RAC. Log in with your RAC user name and password (the default user name and password is `root` and `calvin`, and the default domain is `Local_RAC`). For more information about using the RAC remote access interface, see the remote access interface online help.

For information about accessing the RAC using the Racadm CLI utility, see the *Racadm User's Guide*.

## Updating Your Controller Firmware

Local (firmware) Update is not supported on a DRAC III with firmware version 1.3 or earlier. DRAC III firmware version 1.3 or earlier must be updated by using one of the following methods:

- RAC Web-based interface: Use the TFTP.
- Diskette-based update: Go to [support.dell.com](http://support.dell.com), download the appropriate RAC firmware image file, and follow the instructions to create two diskettes. Insert the first diskette into the system to be updated and follow the instructions on the screen.
- Racadm CLI utility: Use the `racadm fwupdate -p -u -f <path\firming.bin>` command.



**NOTE:** The `-f` option performs file extension checking and allows updating to any DRAC III firmware version.

For more information about updating your controller firmware, see your *Racadm User's Guide* or your Web-based interface online help.

After you perform a firmware upgrade, perform the following instructions to clear the Web browser cache to ensure that all new GUI pages are loaded.

### Clearing the Web Browser Cache With Internet Explorer

- 1 From the drop-down menu, select **Tools**→**Internet Options**.
- 2 In the **Internet Options** window under **Temporary Internet Files**, click **Delete Files...**
- 3 Click the **Delete all offline content** box.
- 4 Click **OK** twice.
- 5 Close and restart the browser.

### Clearing the Web Browser Cache With Mozilla or Netscape Navigator

- 1 From the drop-down menu, select **Edit Preferences**.
- 2 In the **Preferences** window, select **Advance**→**Cache**.
- 3 Click **Clear Disk Cache**.
- 4 Click **Clear Memory Cache**.
- 5 Click **OK**.
- 6 Close and restart the browser.

## RAC Software Basics for Red Hat Linux

The following list describes basic software information for using a RAC with the Red Hat® Linux operating system:

- To verify that the RAC driver is loaded, type the following command:  
`service racser status`
- To verify that the RAC event server for the managed system is loaded, type the following command:  
`service racsrvc status`
- To start, stop, get status of, restart, or reload the racsrvc service, type the following command:  
`service racsrvc <action>`  
where *<action>* is *start*, *stop*, *status*, *restart*, or *reload*.
- To start, stop, get status of, or probe the racser service, type the following command:  
`service racser <action>`  
where *<action>* is *start*, *stop*, *status*, or *probe*.
- For additional information on one of the three RAC services, type the following command:  
`man <service>`  
where *<service>* is *racser*, *racvnc*, or *racsrvc*.




**NOTE:** All three services (*racser*, *racsrvc*, and *racvnc*) start automatically when they are installed and when the system is booted. These services stop automatically when they are uninstalled or when the system is shut down.

- To determine which version of a particular RPM package you have installed, use a package management tool such as GnoRPM, or use the RPM query command (`rpm -q`). For example:  
`rpm -q <package_name>`
- To determine which files were installed and where they are located, type the following command:  
`rpm -ql <package_name>`
- To remove a package, type the following command:  
`rpm -e <package_name>`

## RAC Support in Red Hat Linux

RACs are supported on precompiled kernels that are a part of the Red Hat Linux distribution. RACs are not supported on recompiled kernels with other configuration options (for example, kernels configured for performance-tuning purposes).

 **NOTICE:** Red Hat Linux may fail to load when started on recompiled kernels. If this situation occurs, you must either restore the kernel and modules from backup, or you must reinstall the kernel from the Red Hat RPM packages.

# Accessing and Using a Remote Access Controller

This section provides basic information about using a RAC to monitor and manage your system, including connecting to the RAC to access system and session information, managing the RAC configurations, and performing remote access functions on the managed system. This section includes the following topics:

- Accessing a RAC
- Remote Access Service RAC Home Page
- Properties
- Sensors
- Logs
- Configuration
- Remote access
- Debug
- Updating RAC firmware

## Accessing a RAC

You can access your RAC through Server Administrator or by linking to the RAC remote Web-based interface. You can also access your RAC through a serial or telnet connection (for more information, see "Configuring a RAC to Use a Serial or Telnet Text Console.")

To link to the Remote Access Service RAC **Log in** window from the Server Administrator home page, click the **Main System Chassis** object, click the **Remote Access Controller** object, click the **Remote Connect** tab, and then click **Remote Connect**. The RAC **Log in** window appears.

To link to the RAC remote Web-based interface **Log in** window, open your Web browser and type `http://IP address` (where *IP address* is the IP address for the RAC) in the address field and press <Enter>. The RAC **Log in** window appears.

## Logging In and Out

To log into the Remote Access Service RAC home page, perform the following steps:

- 1 In the **User Name** field, enter your RAC user name.  
This field is case sensitive. The default login name is `root`.
- 2 In the **Password** field, enter your RAC password.  
This field is case sensitive. The default password is `calvin`. You can also press <Tab> to navigate to this field.
- 3 Select an appropriate entry from the **Domain** drop-down box.  
**Local RAC** is the default entry.
- 4 Click **OK** or press <Enter>.

To end your Remote Access Service session, click **Log Out** on the global navigation bar.

## Remote Access Service RAC Home Page

The Remote Access Service RAC home page defaults to the **Summary** window under the **Properties** tab.

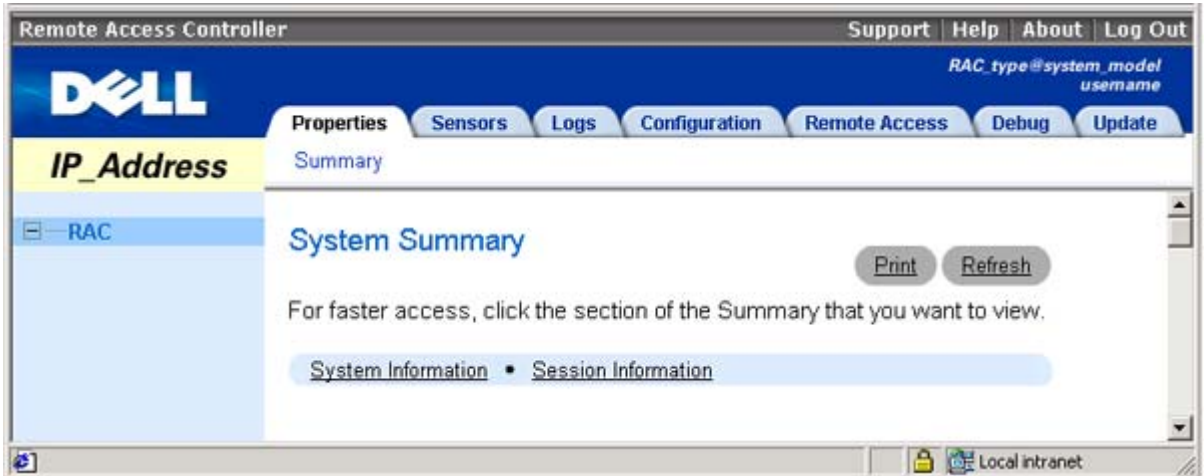
Like the Server Administrator home page, the Remote Access Service RAC home page has three main areas:

- The global navigation bar provides links to general services.
- The system tree displays the type of RAC installed in the managed system.
- The action window displays the available management actions for the system's RAC.

Additionally, when you are logged into the Remote Access Service RAC home page, the RAC type, system model, and current user's user name are displayed in the top-right corner of the window.





Figure 7-1 shows a sample Remote Access Service RAC home page layout for a user logged in to an ERA controller.

**Figure 7-1. Sample Remote Access Service RAC Home Page**



## Status Indicator Icons

The status indicator icons graphically show the status of a sensor or component (as of the latest page refresh).

-  A green check mark indicates a healthy (normal) status condition.
-  A yellow triangle containing an exclamation point indicates a warning (noncritical) status condition.
-  A red X indicates a critical (failure) status condition.
-  A blank space indicates that the status is unknown.

## Properties

From the Remote Access Service RAC home page, you can access system and sessions information. To access system and session information for your RAC, click the **Properties** tab. The following summary of information is provided:

- RAC Information
- System Information
- Watchdog Information
- Session Status

## RAC Information

- **RAC Date/Time** — Displays the RAC internal clock setting.
- **Firmware Version** — Displays the RAC firmware version.
- **Firmware Updated** — Displays the date and time that the RAC firmware was updated.
- **Hardware Version** — Displays the RAC hardware version.
- **Current IP Address** — Displays the IP address assigned to the RAC network adapter.
- **Current IP Gateway** — Displays the IP address of the gateway currently servicing the RAC network adapter.
- **Current IP Netmask** — Displays the IP address of the subnet to which the RAC is connected.
- **PCMCIA Card Information** — Displays specifications for the PCMCIA modem, if installed (DRAC III only).
- **DHCP Enabled?** — Indicates whether DHCP is enabled or disabled on the controller. Valid values are **Yes** or **No**.

## System Information

- **System ID** — Displays the system identifier for the managed system.
- **System Model** — Displays the managed system's model and type.
- **BIOS Version** — Displays the managed system's BIOS version level.
- **Asset Tag** — Displays the managed system's asset tag number.
- **Service Tag** — Displays the managed system's service tag number, if assigned.
- **OS Type** — Displays the type of operating system installed on the managed system.
- **HostName** — Displays the name of the managed system where the RAC is installed.
- **OS Name** — Displays the name of the operating system installed on the managed system, including version, build, and service pack information.
- **ESM Version** — Displays the managed system's firmware version level.

## Watchdog Information


- **Recovery Action** — Specifies whether to reset, power cycle, shut down, or take no action when the system hangs.
- **Present countdown value** — Displays the time remaining before the recovery action is initiated.
- **Initial countdown value** — Displays the time elapsed since the countdown started.



**NOTE:** Watchdog provides the same functionality as automatic recovery.



## Session Status

 **NOTE:** A RAC supports up to 16 simultaneous sessions.

- **Valid Session** — Displays the current number of active sessions (equal to the number of users that are logged on).
- **Unused Sessions** — Displays the name of the user initiating the session.
- **Session Type** — Displays the current session type (HTTP or HTTPS).
- **Session User** — Displays the name of the user initiating the session.
- **User's IP address** — Displays the IP address of the user initiating the session.
- **Login Date/Time** — Displays the time and date that the user logged in according to the RAC internal clock.
- **Active Consoles** — Lists all of the active consoles for the current session including the current redirection type (Console Redirect).

## Sensors

From the Remote Access Service RAC home page, you can access sensor data. To access sensor information, click the **Sensors** tab. The following options are available: RAC sensors, server sensors, and sensor thresholds.

### RAC Sensors (DRAC IIIs only)

This option displays a summary of temperature and voltage values and status. Click the probe name for more information about that sensor.

- **RAC Temperature Sensors** — Displays a temperature gauge that graphically represents the current temperature and normal operating threshold. The thresholds are also displayed as numerical values in the top-right corner of the sensor details box. For definitions of the RAC status indicator icons, see "Status Indicator Icons." For definitions of the sensor thresholds, see "Sensor Thresholds."
- **RAC Voltage Sensors** — Displays a voltage gauge that graphically represents the current voltage and normal operating threshold. The thresholds are also displayed as numerical values in the top-right corner of the sensor details box. For definitions of the RAC status indicator icons, see "Status Indicator Icons." For definitions of the sensor thresholds, see "Sensor Thresholds."

## Server Sensors

This option displays a summary of managed system sensors. For more information on a particular sensor, perform the following steps:

- 1 From the **Server Sensors** window, place a check mark in the **Add** box to the right of the sensor. The selected sensor appears in the **Sensors to Poll** box on the right side of the screen. To remove the sensor from the **Sensors to Poll** list, click **X**.
- 2 Click **Monitor Selected Sensors**, after you have selected all the sensors you want to monitor. A summary of the eight sensors is displayed.
- 3 Click the probe name for more information on a specific sensor.



**NOTE:** You can monitor up to eight sensors at a time.

After clicking the probe name, a graphical temperature gauge is displayed that identifies the current reading and normal operating threshold for the probe. The thresholds are also displayed as numerical values in the top-right corner of the sensor details box. For definitions of the RAC status indicator icons, see "Status Indicator Icons." For definitions of the sensor thresholds, see "Sensor Thresholds."

## Sensor Thresholds

- **Status** — Current sensor status:
  - **Normal** — The sensor value is between **Max Warning Threshold** and **Min Warning Threshold**.
  - **Low Warning** — The sensor value is between the **Min Warning Threshold** and the **Min Critical Threshold**.
  - **High Warning** — The sensor value is between the **Max Warning Threshold** and the **Max Critical Threshold**.
  - **Low Critical** — The sensor value is below the **Min Critical Threshold**.
  - **High Critical** — The sensor value is above the **Max Critical Threshold**.
  - **Disabled** — The sensor is disabled. In this case, the sensor value is usually 0.
  - **Unknown** — The state of the sensor is unknown.
- **Reading** — Current sensor value.
- **Max Critical Threshold** — Maximum value which causes component/system failure.
- **Max Warning Threshold** — Maximum value which triggers a warning alert.
- **Min Warning Threshold** — Minimum value which triggers a warning alert.
- **Min Critical Threshold** — Minimum value which causes component/system failure.


# Logs

From the Remote Access Service RAC home page, you can access RAC logs and system logs. To access log information, click the **Logs** tab. A RAC provides access to logs that are generated by both the RAC and the managed system:

- **POST** — "Viewing the POST Log"
- **RAC** — "Viewing the RAC Log"
- **Hardware** — "Viewing the Hardware Log"
- **Boot Path Analysis** — "Viewing the Boot Path Analysis Log"
- **Last Crash Screen** — "Viewing the Last Crash Screen"

## Viewing the POST Log

The POST log is generated by the managed system and lists POST events recorded during the most recent system boot. To access the POST log from the **Logs** window, click **POST**.

 **NOTE:** The POST log is not supported on all systems.

The contents of the POST log are written by the BIOS of the managed system and are overwritten during each system boot. The POST log displays the following information:

- **POST Code** — A numerical identifier associated with a particular event that occurs during system boot.
- **Description** — A brief description of the event identified by the POST code.

## Viewing the RAC Log

The RAC log is a persistent log maintained in the RAC firmware. To access the RAC log from the **Logs** window, click **RAC**.

The log contains a list of user actions (such as log in and log out) and alerts issued by the RAC. The oldest entries are overwritten when the log becomes full. If the RAC loses communication with the managed system, all entries that the RAC would have added to the Hardware log (such as power failure or RAC sensor alert) are added to the RAC log until communication is re-established.

The RAC log displays the following information:

- **Severity** — Displays a RAC status indicator icon. For definitions of the RAC status indicator icons, see "Status Indicator Icons." For definitions of the sensor thresholds, see "Sensor Thresholds."
- **Date & Time** — Displays the full date and time (for example, Thu Mar 14 14:41:47 2002). When the RAC is unable to communicate with the managed system, the letters "DSU" appear before the time, followed by the elapsed time since the RAC was started.
- **User** — Displays the name of the user logging into the RAC.

- **ID** — Displays the identifying number of the message displayed.
- **Description** — Displays a brief description of the event.

To clear the RAC log of all entries, click **Clear Log** in the top-right corner of the screen.

### Viewing the Hardware Log

The hardware log displays system-critical events that occur on the managed system. To access the hardware log from the **Logs** window, click **Hardware**.

The hardware log is generated by ESM instrumentation on the managed system and by the RAC if you have configured it to monitor any managed system events. It includes date, time, and a description of each event generated by the ESM and other instrumentation on the managed system.

The hardware log displays the following information:

- **Date & Time** — Displays the date and time that the event occurred.
- **Description** — Displays a brief description of the event.


### Viewing the Boot Path Analysis Log

The boot path analysis log displays operations performed and problems encountered during system boot. To access the boot path analysis log from the **Logs** window, click **Boot Path Analysis**.

The boot path analysis log displays the following information:

- **Severity** — Displays a RAC status indicator icon. For definitions of the RAC status indicator icons, see "Status Indicator Icons." For definitions of the sensor thresholds, see "Sensor Thresholds."
- **POST Code** — A numerical identifier associated with a particular event that occurs during system boot.
- **Description** — A brief description of the event identified by the POST code.

### Viewing the Last Crash Screen

 **NOTE:** The **Last Crash Screen** option is only available on systems running Windows operating systems.

Before viewing the Last Crash Screen, perform the instructions in "Disabling the Windows Automatic Reboot Option."

The **Last Crash Screen** option displays the most recent crash screen, allowing you to obtain information on events leading up to the system crash. This information is saved in RAC memory and made available for remote display. To access **Last Crash Screen** from the **Remote Access** window, click **Last Crash Screen**.

The **Last Crash Screen** option works in conjunction with the managed system's auto recovery (watchdog timer) functions. In order to capture a last crash screen, you must set the system's **Auto Recovery** option to **Reset**, **Server Power Cycle**, or **Server Power Off**.

To set the **Auto Recovery** option, perform the following steps:

- 1 On the Server Administrator home page, click the **System** object.
- 2 Under the **Properties** tab click **Auto Recovery**.
- 3 Specify the **Action on Hung Operating System Detection** setting:
  - **None** — Do not take action when the operating system is hung or has crashed.
  - **Reboot System** — Shut down the operating system and initiate system startup, performing BIOS checks and reloading the operating system.
  - **Power Off System** — Turn the electrical power to the system off.
  - **Power Cycle System** — Power cycle turns the electrical power to the system off, pauses, turns the power on, and reboots the system. Power cycling is useful when you want to reinitialize system components such as hard disk drives.
- 4 Type a value (minimum of 30 seconds) in the **System Reset Timer** field.
- 5 Click **Apply Changes** and then click **OK** to save your changes.



**NOTE:** If a crash screen is not available, the message `No previously captured last crash screen is available` is displayed.

## Configuration

From the Remote Access Service RAC home page, you can configure sensor poll rates. To access the RAC configuration features, click the **Configuration** tab.

### Poll Rates


The **Poll Rates** option allows you to configure the time interval for the RAC to update specific information. To access the poll rates features from the **Configuration** window, click **Poll Rates**.

Poll rate configuration allows you to set the rate at which the RAC samples status information from its integrated sensors (for DRAC IIIs only) or from the ESM sensors on the managed system. It also determines how often the RAC retrieves system information from the managed system. Use the **Poll Rates** option to change the **Session Timeout Value** and to change the frequency with which the following fields are updated:

- System Info Poll Rate
- RAC Sensor Poll Rate (DRAC IIIs only)
- Server Sensor Poll Rate
- Session Time Out

### Configuring Poll Rates

- 1 From the **Poll Rates** window, select an interval of seconds from the drop-down menu (30, 60, 90, 120, 150, or 180).
- 2 Click **Apply Changes** to save the configuration.

 **NOTE:** Poll rate settings are retained only for the current session and do not apply to any other user sessions.

## Remote Access


To access the RAC Remote Access functions, click the **Remote Access** tab on the Remote Access Service RAC home page. From the **Remote Access** window, the following options are available:

- Server Reset Options
- Remote Floppy Boot
- Configuring Remote Floppy Boot
- Console Redirect


### Server Reset Options

A RAC allows you to remotely perform a variety of power management actions on the managed system, such as graceful shutdown through the operating system or a hard reset (equivalent to pressing the reset button). To access the server reset options from the **Remote Access** window, click **Server Reset Options**.

From the **Server Reset Options** window, you can configure the following resets for the managed system by selecting from the following reset options and clicking **Apply Reset Option**.

 **NOTE:** If the **Graceful Server Shutdown** or the **Graceful Server Restart** commands are issued to systems running a supported Novell® NetWare® operating system, an MS-DOS® prompt is displayed. This prompt indicates that the operating system has been shut down, but the system must be manually turned off and on using the power button. If either of these commands are issued to systems running a supported Red Hat® Linux operating system, the operating system shuts down and then displays a message indicating that it is okay to manually turn the system off or on using the power button.

- **Graceful Server Shutdown** — Shuts down the managed system through the operating system.
- **Graceful Server Restart** — Shuts down and restarts the managed system through the operating system.

 **NOTE:** When using **Graceful Server Restart**, **Reset**, and **Server Power Cycle** options with console redirection, you must allow approximately 2 minutes for the managed system to restart before attempting to log back into the system remotely. This time allows the managed system time to re-establish a connection with the console redirection service.

- **Reset** — Resets the system (equivalent to pressing the reset button); the power is not turned off by this function.

- **Server Power Cycle** — Turns off the system power and turns it on again (equivalent to pressing the power button twice).
- **Server Power On** — Turns on the system power (equivalent to pressing the power button).
- **Server Power Off** — Turns off the system power (equivalent to pressing the power button).

## Remote Floppy Boot

The Remote Floppy Boot feature allows you to view current remote floppy boot settings, insert a new floppy boot image into the RAC, and boot a managed system from a diskette image stored on the RAC. To configure the remote floppy boot settings, see "Configuring Remote Floppy Boot."

 **NOTE:** The remote floppy boot feature is supported only on 32-bit systems.

### Viewing Current Remote Floppy Boot Settings

This section allows you to view the remote floppy boot settings in Table 7-1.

**Table 7-1. Remote Floppy Boot Settings**

Boot Setting	Options/Descriptions
Image Inserted	Indicates whether an image has been inserted into the RAC memory ( <b>Yes</b> or <b>No</b> ).
Boot Mode	<p><b>Physical Boot Device</b> – System boots from its own physical (not remote) drive.</p> <p><b>Once From Remote Floppy</b> – System boots once using the remote floppy boot image and thereafter boots from its own physical (not remote) drive.</p> <p><b>Always From Remote Floppy</b> – System always boots using the remote floppy boot image.</p>
Remote Floppy Mode	<p><b>Read Only</b> – After copying a remote floppy image from the RAC to a local file system, a user may only read the image.</p> <p><b>Read/Write</b> – After copying a remote floppy image from the RAC to a local file system, a user may read or write to the image.</p>

### Inserting a Remote Floppy Boot Image

Before using the remote floppy boot feature, you must first create a remote floppy boot image file and copy it to a logical drive. For Microsoft® Windows® 2000 Server and Windows Server 2003 operating systems, the RAC provides two utilities to create the image: **RemoteFloppyUtility.exe** (a GUI utility), and **remotefloppy.exe** (a command-line utility). These utilities are located on your managed system in the `Program Files\<Systems Management>\RAC\MN` directory, where *<Systems Management>* is the file location where your systems management software was installed, and on your management station in the `Program Files\<Systems Management>\RAC\MT` directory.

From the **Remote Floppy Boot** window, click one of the commands in Table 7-2, and then provide the requested information in the **Options** area on the right-hand side of the screen.

After selecting the appropriate options, click **Insert Image** to insert the remote floppy image into RAC memory and to continue configuring the remote floppy boot feature.

**Table 7-2. Remote Floppy Boot Commands**

Command	Options/Descriptions
Insert Remote Floppy Image	<p><b>Insert Remote Floppy Image From TFTP Server</b> – Allows you to insert a remote floppy boot image into RAC memory from a TFTP server (enter the TFTP IP address and file name).</p> <p><b>Insert Remote Floppy Image From Local File</b> – Allows you to insert a remote floppy boot image into RAC memory from a local file (enter the local file path or browse to the file).</p>

### Configuring Remote Floppy Boot

The **Insert Image** button opens the **Remote Floppy Boot Configuration** page where you can perform the following actions: select the boot mode and floppy mode, copy the remote floppy image to a local file system, and eject your remote floppy image from the RAC memory.

#### *Configuring the Boot Mode and Remote Floppy Mode*

From the **Insert Remote Floppy Image** area, configure the boot mode and floppy mode (see Table 7-3).

**Table 7-3. Remote Floppy Boot Configuration Settings**

Settings	Description/Options
Boot Mode	<p>Allows you to configure when and how the system boots from the diskette by selecting one of the following options from the drop-down menu:</p> <p><b>Physical Boot Device</b> – System boots from its own physical (not remote) drive.</p> <p><b>Once From Remote Floppy</b> – System boots once using the remote floppy boot image and thereafter boots from its own physical (not remote) drive.</p> <p><b>Always From Remote Floppy</b> – System always boots using the remote floppy boot image.</p>
Remote Floppy Mode	<p>Allows you to configure the remote floppy mode by clicking the <b>Read Only</b> or <b>Read/Write</b> option.</p> <p><b>Read Only</b> – After copying a remote floppy image from the RAC to a local file system, a user may only read the image.</p> <p><b>Read/Write</b> – After copying a remote floppy image from the RAC to a local file system, a user may read or write to the image.</p>



### Copying the Remote Floppy Image to a Local File System

To copy the remote floppy image from the RAC to a local file system, click **Copy Remote Floppy Image** at the bottom of the screen.


### Ejecting a Remote Floppy Image


Ejecting a remote floppy image disables the image saved in RAC memory. It is the same as ejecting the diskette from a system before you boot it.


To eject a remote floppy image, click **Eject Remote Floppy Image** at the bottom of the screen.

### Console Redirect

The **Console Redirect** option allows you to use the display, mouse, and keyboard on a local management station to control the corresponding devices on the remote managed system. To access the **Console Redirect** window from the **Remote Access** window, click **Console Redirect**.


 **NOTE:** For graphical redirection, the managed system is performing the redirection process; therefore, a percentage of available microprocessor time is consumed when the process is active. It is recommended that you stop console redirection when not needed so that the system is available to perform its normal tasks. In addition, you should run the managed system in a low-resolution graphics mode, such as 800 x 600, and at a maximum of 256 colors to minimize the redirection task.

 **NOTE:** If a supported Novell NetWare operating system is running on the managed system, console redirection will be displayed as text-only.

 **NOTE:** You cannot run a video memory test while console redirection is active.

Console redirection provides the following functions:

- Preboot text, video, and keyboard redirection
- Postboot graphics, video, keyboard, and mouse redirection
- Seamless operation between preboot and postboot screens

 **NOTE:** When switching between preboot and postboot screens, it may take several minutes for screen content to appear because the RAC must first connect to the RAC services on the managed system.


### Using the Console Redirect Buttons

The following buttons are available for use in the **Console Redirect** window:

- **Close** — Use this button to exit the **Console Redirect** window.
- **Refresh** — Use this button to completely update the entire remote system-screen viewport.
- **CtrlAltDel** — Use this button to send the <Ctrl> <Alt> <Delete> key combination to the remote system.
  - To apply the <Alt> key to the next keystroke sent to the remote system, click the **Alt** check box.

- To apply the <Ctrl> key to the next keystroke sent to the remote system, click the **Ctrl** check box, click in the redirected console window, and press the desired key.
- **Help** — Use this button to open the online help for the **Console Redirect** screen.
- **Enable Local Console** — Use this button to enable or disable the managed system's console keyboard and mouse functions when the console is redirected. This button operates only when the managed system is running a supported Windows operating system, and does not operate during system boot.

If the managed system is running a supported NetWare operating system and has the RAC managed system software installed and running, the button appears as **Enter Debug Mode**. Use this button to enter NetWare Debug Mode.

 **NOTICE:** Entering Network Debug Mode will stop all services on the managed system.

- **Create Snapshot** — Use this button to capture the current remote system screen to a **.jpg** file on the local system. A dialog box is displayed to allow you to save the **.jpg** file to a specified location.

### **RAC Console Redirection on Systems Running a Supported Red Hat Linux Operating System**

For Red Hat Linux, the VNC service (RACVNC) does not display the actual primary-system console of the managed system. Instead, RACVNC provides a virtual desktop that the remote user can use to execute systems management applications. This virtual desktop has all of the capabilities of any desktop that might be displayed at the actual managed system's console. This model is the generally accepted model for remote management for Red Hat Linux or UNIX®.

Only one shared systems management desktop is provided for console redirection through the RAC. Therefore, all remote, user-created console-redirection sessions through the RAC share the same desktop. If multiple management station users create console-redirection sessions at the same time, they simultaneously share the same desktop.


## **Debug**

The **Debug** option allows you to configure and perform RAC debugging and diagnostic tests for network and paging on the RAC or managed system. To access RAC debug functions from the Remote Access Service RAC home page, click **Debug**. From the **Debug** window, the following options are available:


- Network Debug
- Command Debug
- Trace Log
- Status Check

## Network Debug

The **Network Debug** option allows you to perform debugging tasks for network and paging. To access the **Network Debug** window from the **Debug** window, click **Network Debug**. From the **Network Debug** window, the following information and options are available.


 **NOTE:** After clicking one of the following options and clicking **Submit**, results of the debug tasks will be displayed in the **Status Text** box at the bottom of the page.

- **ARP** — Displays the content of the ARP table. ARP entries may not be added or deleted.
- **IPConfig** — Displays the contents of the network interface table.
- **NetStat** — Prints the contents of the routing table. If the optional interface number is provided in the text field to the right of the **NetStat** option, **NetStat** prints additional information regarding the traffic across the interface, buffer usage, and other network interface information.
- **Ping** — Verifies that the destination IP address is reachable from the RAC with the current routing-table contents. A destination IP address must be entered in the field to the right of this option. An ICMP echo packet is sent to the destination IP address based on the current routing-table contents. If the destination matches one of the demand-dial database destination IP addresses, and if the demand-dial connection is not currently active, the packet is queued, and an attempt is made to bring up the demand-dial connection.

 **NOTE:** In the case of nonactive demand-dial connections, the **ping** option might report a failure because it usually takes more than 5 seconds to establish a demand-dial connection. If **ping** is retried after the connection is established, the packet is passed across the link. Even when the connection is established, it is still possible that the destination system is not reachable and able to respond to the ICMP echo. However, if the destination system is reachable and able to respond within 5 seconds, **ping** reports success on attempts after the connection is established.

## Command Debug

The **Command Debug** option allows you to manually input debug commands. To access the **Command Debug** window from the **Debug** window, click **Command Debug**. From the **Command Debug** window, you may use any of the following case-sensitive commands. To activate a command, click **Submit**. Command responses are displayed in the **Status Text** box at the bottom of the page.

 **NOTE:** The debug selections in this group should only be used under the direction of qualified support personnel.

- **getsysinfo** — Displays general RAC information, system information, or watchdog status information, depending upon which of the following command options are entered:
  - **getsysinfo -d** — Displays RAC information.
  - **getsysinfo -s** — Displays system information.
  - **getsysinfo -w** — Displays auto recovery (watchdog) information.
  - **getsysinfo -A** — Eliminates the printing of data headers/labels.

- **getssninfo** — Displays a list of currently active or pending users and optionally includes summary-session information. The summary-session information lists the total number of sessions in each of the defined session states (**Not Used**, **Preliminary**, **Unvalidated**, **Valid**, and **Invalid**).
  - **getssninfo -A** — Eliminates the printing of data headers.
  - **getssninfo -u** (*user name*) Limits the printed output to only the detailed session records for the given user name; if an asterisk (\*) is entered as the user name, all users are listed; no summary information prints when this option is specified.
- **coredump** — Displays the last RAC crash information, including detailed information such as register values and a memory map recorded when the most recent RAC crash occurred; displays the message `No CORE dump available` if no previous card crash has occurred or if the data has been cleared with the **coredumpdelete** command.
- **coredumpdelete** — Deletes the coredump stored in the RAC. This command clears the area reserved for persistent storage of card crash information regardless of whether any card crash information is currently stored in the area reserved for this information.

For DRAC IIIs only:

- **getd3sensors** — Displays information about the sensors that are present on the RAC itself.
  - **getd3sensors -s** — Allows you to specify a single sensor to display; if no **-s** option is used, all sensors are displayed, one per line.
  - **getd3sensors -AEh** — Displays all RAC sensors as hexadecimal values without leading hexadecimal numbers.

## Trace Log

The **Trace Log** option allows you to display the dump trace log and to set debugger trace levels to identify the types of messages being sent on the local network. To access the **Trace Log** window from the **Debug** window, click **Trace Log**. From the **Trace Log** window, select one of the following options:


- **Dump Trace Log** — Selecting this option displays a UNIX-style system log. This log is a volatile, memory-resident log that contains time-stamped entries.
- **Set Trace Level** — This option allows you to set debugger trace levels to identify the types of messages being sent on the local network. Select one or more of the following options and click **Submit**:
  - **CHAT** — Traces the CHAT, a protocol used by PPP and numeric paging.
  - **DHCP** — Traces the DHCP packets sent and received.
  - **IP** — Traces IP packets sent and received on PPP links.
  - **PPP** — Traces PPP connection negotiation packets sent and received.
  - **TAP** — For DRAC IIIs only, traces TAP information sent and received.

## Status Check

The **Status Check** option allows you to perform diagnostic tasks on the RAC or managed system. To access the **Status Check** window from the **Debug** window, click **Status Check**. From the **Status Check** window, select one of the following options and click **Submit**:

- **Delete Core Dump** — Clears the area reserved for persistent storage of card crash information regardless of whether any card crash information is currently stored in the area reserved for this information.
- **Display Last Core Dump** — Displays the last RAC crash, including detailed information such as register values and a memory map recorded when the most recent RAC crash occurred; displays the message `No CORE dump available` if no previous card crash has occurred or if the data has been deleted.
- **Dump RAC Status** — Provides status and general RAC board information.
- **Reset RAC** — Issues a reset command to the RAC.

## Updating RAC Firmware


 **NOTE:** You can also update the RAC firmware using the Server Administrator Update Service. See your *Server Administrator User's Guide* for more information.


The **Update** option allows you to update the RAC firmware into the RAC flash memory. To access the firmware update from the Remote Access Service RAC home page, click the **Update** tab.

 **NOTE:** The **Firmware Updated** field in the **System Information** window is blank until a firmware update is performed.


The data included in the RAC firmware package includes the following:

- RAC firmware code and data produced by code compilation
- Expansion ROM image
- Java user interface, HTML, JPEG, and other user interface data files (including VNC Java files, if applicable)
- Default configuration files

 **NOTE:** The firmware update retains the current RAC settings.

 **NOTE:** You must have a TFTP system running to download firmware image files to the RAC. Many TFTP systems are available both commercially and without cost on the Internet. If you do not already have a TFTP system running, Dell recommends that you use one of the TFTP systems that you can find on the Microsoft website at [www.microsoft.com](http://www.microsoft.com).

## Updating the RAC Firmware

 **NOTE:** Before beginning the firmware update, you must first download the latest firmware version from Dell Support at [support.dell.com](http://support.dell.com) and then upload it to a TFTP server.

To update your RAC firmware, perform the following steps:

- 1 From the Remote Access Service RAC home page, click the **Update** tab.
- 2 From the **Firmware Update** window, type the relative path on the TFTP server where the firmware image files reside in the **Image Path** field.
- 3 Type the IP address for the TFTP server where the firmware image resides in the **TFTP Server** field.
- 4 Click **Update Firmware**.

The RAC resets after the firmware update is complete.


# Configuring a RAC to Use a Serial or Telnet Text Console

Your RAC provides serial and telnet command interfaces designed to perform all of the configuration and systems management functions that you can perform through your RAC remote access Web-based interface.

The following sections are provided to explain the serial/telnet text console features, how to configure your system to use and perform systems management actions through a serial/telnet console:

- Supported remote access controllers
- Serial and telnet console features
- Enabling and configuring the managed system to use a serial or telnet console
- Connecting to the managed system through the serial port or telnet management station
- Configuring the management station terminal emulation software
- Logging in to the RAC
- Starting a text console
- Performing actions on the managed system
- Using VT-100 terminal emulation with a DRAC III

## Supported Remote Access Controllers

 **NOTE:** The RAC serial/telnet console is not supported on Dell™ PowerEdge™ 7150 systems.

RAC serial/telnet console is supported with the following RACs:


- DRAC III (through the DRAC III VT-100 serial connector only)
- DRAC III/XT (through the DRAC III/XT VT-100 serial connector only; except on Dell PowerEdge 1600SC systems)
- ERA
- ERA/O (except on PowerEdge 1650 systems)

RAC telnet redirection is supported on all RACs.


## Serial and Telnet Console Features

The following serial and telnet console redirection features are supported on your RAC. For a list of supported RACs, see "Supported Remote Access Controllers."


- One serial client connection and up to four telnet client connections at one time
- Access to the managed system consoles through the system serial port and through the RAC network adapter
- Serial/telnet console commands that allow you to power-on, power-off, power-cycle, reset, view logs, view sensor status, or configure the RAC
- Serial/telnet console support for the `racadm` command; which is useful for scripting
- Command-line editing and history
- **Connect com2** serial command to connect, view, and interact with the managed system text console that is being output through a serial port (including BIOS and the operating system)

 **NOTE:** If you are running Red Hat® Linux on the managed system, the `connect com2` serial command provides a true Red Hat Linux console stream interface. For more information, see "Differences Between "connect com2" and "connect video" Commands."

- **Connect video** serial command to connect, view, and interact with the managed system text console that is being output by the video controller

 **NOTE:** For more information, see "Differences Between "connect com2" and "connect video" Commands."

- Menu-based VT-100 block screen interface that provides easy operation of commonly used commands including reset, power-on, and power-off

 **NOTE:** Because the `racadm` command does not have access to a file system, several options (such as reading or writing a file) are not supported by `racadm` through a serial/telnet console. For more information about supported `racadm` commands for serial/telnet console redirection, see the *Racadm User's Guide*.

## Enabling and Configuring the Managed System to Use a Serial or Telnet Console

The following subsections provide information to enable and configure serial/telnet console redirection on the managed system.

### Upgrade Your BIOS

To use the serial/telnet console, your system must have the required BIOS version depending on your system type. For the required BIOS version for your system, see the `racread.txt` file on the *Systems Management* CD or on the Dell Support website at [support.dell.com](http://support.dell.com). For instructions about how to upgrade your BIOS, see "Updating the System BIOS."



## Configuring the System Setup Program on the Managed System

To configure your System Setup program to redirect console output to a COM port, perform the following steps.



**NOTE:** Configuring the System Setup Program must be used in conjunction with the `connect com2 serial/telnet` command.

- 1 Turn on or restart your system.
- 2 Press `<F2>` immediately after you see the following message:  
`<f2> = System Setup`
- 3 Scroll down and select **Console Redirection**.
- 4 Set the **Console Redirection** screen to the following settings:  
**Console Redirection** – RAC or COM2 (depending upon your managed system BIOS, one of these options is available)  
**Remote Terminal Type** – ANSI or VT100/VT 220 depending on your specific needs  
**Redirection After Boot** – Disabled
- 5 If your managed system is a PowerEdge 1750, perform the following additional steps to enable serial/telnet console redirection; otherwise press `<Esc>` to exit the System Setup program and complete the BIOS serial/telnet text console configuration for your system.
- 6 Scroll down and select **Integrated Devices** by pressing `<Enter>`.
- 7 In the submenu, scroll down to **Serial Port 1** and set to **Off**.
- 8 Press `<Esc>` to exit the System Setup program to complete the System Setup program configuration.

## Enabling the Serial/Telnet Console on the RAC



**NOTICE:** For your new configuration settings take effect, you must restart the RAC.

You can enable the serial/telnet console locally or remotely. To enable the serial/telnet console from the managed system, enter the following local `racadm` commands from a command prompt.




**NOTE:** For detailed information about how to use the `racadm` command-line utility, serial/telnet, and `racadm` subcommands, see your *Racadm User's Guide*.

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

To enable the serial/telnet console remotely, type the following remote racadm commands from a command prompt:

```
racadm -u <root username> -p <root password> -r <RAC IP address>
config -g cfgSerial cfgSerialConsoleEnable 1
```

```
racadm -u <root username> -p <root password> -r <RAC IP address>
config -g cfgSerial cfgSerialTelnetEnable 1
```

 **NOTE:** Use the RAC IP address for your managed system; not **192.168.10.1** as shown in the example.

```
racadm -u root -p calvin -r 192.168.10.1 config -g cfgSerial -o
cfgSerialConsoleEnable 1
```

```
racadm -u root -p calvin -r 192.168.10.1 config -g cfgSerial -o
cfgSerialTelnetEnable 1
```

## Using Racadm to Configure the Settings for the Serial and Telnet Console

This subsection provides steps to configure the default configuration settings for serial/telnet console redirection. To configure the settings, enter the **racadm config** command with the appropriate group, object, and object value(s) for the setting that you want to configure. For a complete list of available serial/telnet and racadm commands, see your *Racadm User's Guide*.

You can enter racadm commands locally or remotely. When using racadm commands remotely, you must include the root user name, root password, and managed system RAC IP address.

To enter racadm commands locally, type the commands from a command prompt on the managed system:

```
racadm config -g <group> -o <object> <value>
```

To enter racadm commands remotely, type the commands from a command prompt on a management station:

```
racadm -u <rootUser> -p <root password> -r <RAC IP address> config -
g <group> -o <object> <value>
```

## Displaying Configuration Settings

To display the current settings for a particular group, type the following commands from the command prompt on the managed system:

```
racadm getconfig -g <group>
```

For example, to display a list of all of the settings for the **cfgSerial** group, enter the following:

```
racadm getconfig -g cfgSerial
```

To display the current settings for a particular group remotely, enter the following from a remote command prompt:

```
racadm -u <root user> -p <root password> -r <RAC IP address>
getconfig -g cfgSerial
```

For example, to display a list of all of the settings for the `cfgSerial` group remotely, enter the following from a management station:

```
racadm -u root -p calvin -r 192.168.0.1 getconfig -g cfgSerial
```

### Racadm Command Objects for Serial/Telnet Console Configuration

Table 8-1 lists the "objects" for the racadm object group `cfgSerial`. You can configure values for the following objects by using the racadm command locally and remotely. Change the object values to configure the serial and telnet console features. For detailed information about how to use the racadm command-line utility, serial/telnet, and racadm subcommands, see your *Racadm User's Guide*.

**Table 8-1. Racadm cfgSerial Objects for Configuring the Serial/Telnet Console**

<b>cfgSerial Object</b>	<b>Description</b>
<code>cfgSerialBaudRate</code>	Sets the baud rate for the external serial port.
<code>cfgSerialConsoleEnable</code>	Enables/disables the serial console.
<code>cfgSerialConsoleQuitKey</code>	Sets the "quit" key sequence that you will use to disconnect (quit) the RAC from the serial or telnet text console. This key sequence consists of one to three keys. Use the quit key after connecting with the <code>connect com2</code> or <code>connect video</code> commands.
<code>cfgSerialConsoleIdleTimeout</code>	Sets the time to lapse before the serial port console is automatically logged off.
<code>cfgSerialConsoleShellType</code>	Sets the serial console shell type one of the following types: VT-100 block screen, dial-in through an external modem (attached to an external serial port), or PPP dial-in through an external modem (attached to an external serial port).
<code>cfgSerialConsoleNoAuth</code>	Sets permission to allow or not allow a user to disable authentication on serial shell.
<code>cfgSerialConsoleCommand</code>	Instructs a command of your choice to autorun when a session is established (for example, <code>connect com2</code> ).
<code>cfgSerialTelnetEnable</code>	Enables/disables the telnet console.
<code>cfgSerialConsoleColor</code>	Enables/disables the color of the serial text console when connected through "connect video."
<code>cfgSerialConsoleAnsi</code>	Enables/disables the serial text console ANSI graphics mode when connected through "connect video."
<code>cfgSerialCom2RedirEnable</code>	Enables/disables COM2 port redirection (not available on the DRAC III controller).

## Connecting to the Managed System Through the Serial Port or Telnet Management Station (Client System)

Managed system internal hardware interfaces provide the RAC with access to the COM2 (RAC) port, video, and hardware management interfaces on your system and enable you to power on, power off, or reset the managed system, and access logs and sensors.

The serial console is available on most RACs (see "Supported Remote Access Controllers") through either an external serial connector or external DRAC III serial connector. Only one serial client system may be active at any given time.


The telnet console is available on all RAC versions through the RAC network adapter. Up to four telnet client systems may connect at any given time.


The management station connection to the managed system serial or telnet console requires the use of management station terminal emulation software (see "Configuring the Management Station Terminal Emulation Software" for more information).

The following subsections explain how to connect your management station to the managed system through a managed system external serial port using terminal software and a null modem cable, or by telnet using terminal software through the managed system RAC network adapter.

### Connecting the DB-9 Cable

If you want to connect to the managed system using a serial text console, you must connect a DB-9 null modem cable to the COM port that you are using on the managed system. Not all DB-9 cables carry the pinout/signals necessary for this connection. The DB-9 cable for this connection must conform to the specification shown in Table 8-2.

 **NOTICE:** You must connect the DB-9 cable to the COM2 port connector on the managed system unless the system uses the DRAC III controller. The DRAC III controller requires that you connect to the VT-100 serial connector on the DRAC III controller.

 **NOTE:** This cable may also be used for BIOS text console redirection with the RAC serial console not enabled.

**Table 8-2. Required Pinout for DB-9 Null Modem Cable**

Signal Name	DB-9 Pin	DB-9 Pin
FG (Frame Ground)	–	–
TD (Transmit data)	3	2
RD (Receive Data)	2	3
RTS (Request To Send)	7	8
CTS (Clear To Send)	8	7
SG (Signal Ground)	5	5
DSR (Data Set Ready)	6	4
CD (Carrier Detect)	1	4
DTR (Data Terminal Ready)	4	1
DTR (Data Terminal Ready)	4	6

# Configuring the Management Station Terminal Emulation Software

Your RAC supports a serial or telnet text console from a management station running one of the following types of terminal emulation software:

- Red Hat® Linux Minicom in an Xterm
- Hilgraeve's HyperTerminal Private Edition (version 6.3)
- Red Hat Linux Telnet in an Xterm
- Microsoft Telnet

Perform the steps in the following subsections to configure your type of terminal software. Configuration is not required when using Microsoft® telnet.

## Configuring Red Hat Linux Minicom for Serial Console Emulation

Minicom is the Red Hat Linux serial port access utility. The following steps are valid for configuring Minicom version 1.8. Other Minicom versions may differ slightly but require the same basic settings. Use the information in "Required Minicom Settings for Serial Console Emulation" to configure other versions of Minicom.

### Configuring Minicom Version 1.8 for Serial Console Emulation



**NOTE:** To ensure that the text displays properly, Dell recommends that you use an Xterm window to display the telnet console instead of the default window provided by the Red Hat installation.

- 1 To start a new Xterm session, type `xterm &` at the command prompt.
- 2 Drag the lower right-hand corner of the window to resize it to 80 x 25 prior to using telnet. Drag the lower right corner with the mouse.
- 3 If you do not have a Minicom configuration file, go to the next step.  
If you have a Minicom configuration file, enter `minicom <Minicom config file name>` and skip to step 20.
- 4 At the Xterm command prompt, enter `minicom`.
- 5 Select **Serial Port Setup** and press <Enter>.
- 6 Press <a> and select the appropriate serial device (for example, `/dev/ttySo`).
- 7 Press <e> and set the **Bps/Par/Bits** option to **115200 8N1** (9600 8N1 for DRAC III only).
- 8 Press <f> and set **Hardware Flow Control** to **Yes** and set **Software Flow Control** to **No**.
- 9 To exit the **Serial Port Setup** menu, press <Enter>.
- 10 To enter **Terminal Setup**, press <a>.
- 11 For the **Terminal Emulation** setting, select **ANSI**.
- 12 To exit **Terminal Setup**, press <Enter>.

- 13 Select **Modem and Dialing** and press <Enter>.
- 14 In the **Modem Dialing and Parameter Setup** menu, press <Backspace> to clear the **init**, **reset**, **connect**, and **hangup** settings so that they are blank.
- 15 To save each blank value, press <Enter>.
- 16 When all specified fields are clear, press <Enter> to exit the **Modem Dialing and Parameter Setup** menu.
- 17 Select **Save setup as config\_name** and press <Enter>.
- 18 Select **Exit From Minicom** and press <Enter>.
- 19 At the command shell prompt, enter the following: `minicom <Minicom config file name>`.
- 20 To expand the Minicom window to 80 x 25, drag the corner of the window.
- 21 To exit Minicom, press <Ctrl-A><z><x>.



**NOTE:** If using Minicom for serial text console redirection to configure the managed system BIOS, it may be useful to turn on color in Minicom. To turn on color, at the command prompt enter `minicom -c`.

Ensure that the Minicom window displays a command prompt such as `[RAC\rroot]#`. When the command prompt appears, your connection is successful and you are ready to connect to the managed system console using either the **connect com2** or **connect video** serial commands.

### Required Minicom Settings for Serial Console Emulation

Use the following information to configure any version of Minicom.

**Table 8-3. Minicom Settings for Serial Console Emulation**

Setting Description	Required Setting
Bps/Par/Bits	115200 8N1 (9600 for DRAC III only)
Hardware flow control	Yes
Software flow control	No
Terminal emulation	ANSI
Modem dialing and parameter settings	Clear the "init," "reset," "connect," and "hangup" settings so that they are blank
Window size	80 x 25 (to resize, drag the corner of the window)

## Configuring HyperTerminal for Serial Console Redirection

HyperTerminal is the Windows serial port access utility. To set the size of your console screen appropriately, use Hilgraeve's HyperTerminal Private Edition version 6.3.

To configure HyperTerminal for serial console redirection, perform the following steps:

- 1 Start the HyperTerminal program.
- 2 Enter a name for the new connection and click **OK**.
- 3 Next to **Connect using:**, select the COM port on the management station (for example, COM1) to which you have connected the DB-9 null modem cable and click **OK**.
- 4 Configure the COM port settings as shown in Table 8-4.
- 5 Click **OK**.
- 6 Click **File**→**Properties**→**and** click the **Settings** tab.
- 7 Set the **Telnet terminal ID:** to **ANSI**.
- 8 Click **Terminal Setup** and set **Screen Rows** to **26**.
- 9 Set **Columns** to **80** and click **OK**.

**Table 8-4. Management Station COM Port Settings**

Setting Description	Required Setting
Bits per second:	115200 (9600 for DRAC III only)
Data bits:	8
Parity:	None
Stop bits:	1
Flow control:	Hardware

The HyperTerminal window displays a command prompt such as [RAC\root]#. When the command prompt appears, your connection is successful and you are ready to connect to the managed system console using either the **connect com2** or **connect video** serial commands.

## Configuring Red Hat Linux XTerm for Telnet Console Redirection

When running telnet with Red Hat Linux, perform the following steps:



**NOTE:** To ensure that the text is properly displayed, Dell recommends that you use an Xterm window to display the telnet console instead of the default window provided by the Red Hat installation.

- 1 To start a new Xterm session, type `xterm &` at the command prompt.
- 2 Drag the lower right-hand corner of the window to resize it to 80 x 25 prior to using telnet. This can be done by dragging the lower right corner with the mouse.

Red Hat Linux Xterm is now ready to connect by telnet to the managed system RAC.

To connect to the RAC, at the Xterm prompt, type `telnet <RAC IP address>`.

## Configuring Microsoft Telnet for Telnet Console Redirection

Microsoft telnet does not require any configuration for using a text telnet console. To connect to the RAC, open a command prompt, type `telnet <RAC IP address>`, and press <Enter>.

## Log In to the RAC

After you have configured your management station terminal emulator software, perform the following steps to log in to the RAC:

- 1 Connect to the RAC using your management station terminal emulation software.
- 2 Enter your RAC user name and press <Enter>.
- 3 Enter your RAC password and press <Enter>.

You are now logged in to the RAC.

## Starting a Text Console

After you have logged in to the RAC through your management station terminal software or by telnet, you can redirect the managed system text console using two different methods. You can use either the `connect com2` or `connect video` serial/telnet commands.

Table 8-5 is provided to help you determine which connect type is best for you.

**Table 8-5. Differences Between "connect com2" and "connect video" Commands**


Feature	Using <code>connect com2</code>	Using <code>connect video</code>
Maximum number of client systems	Four (shared with RAC remote Web-based interface)	One
Scrolling window	No	Yes

Perform the steps in the following subsections to redirect the managed system text console.

### Connecting to the RAC Using the "connect com2" Command

To use `connect com2` to connect to the RAC, type `connect com2` from the RAC command prompt (displayed through Minicom or HyperTerminal).

Connecting to the RAC Using the "connect video" Command


 **NOTICE:** Because the console redirection feature is designed only for use with text consoles, your management console must be in text mode for console redirection to work properly.

To use `connect video` to connect to the RAC, type `connect video` from the RAC command prompt (displayed through a Red Hat Linux Xterm window or Microsoft command prompt).



The screen clears and the following message appears before the text is redirected: `Waiting for text console.`

## Performing Actions on the Managed System

 **NOTE:** Windows XP users having problems with characters in a RAC telnet session, please visit [support.microsoft.com](http://support.microsoft.com), and search the knowledge base for article number 824810 for a hot fix for this issue.

The RAC supports serial/telnet commands and `racadm` commands through a serial or telnet console. These commands can be executed on the server locally or remotely. The local `racadm` command line interface (CLI) is installed for use as a root user only.

You can use the `racadm` utility to power-on/off, reset, view logs, sensors, and configure the RAC in the same manner as the RAC command shell. In addition, it supports configuration from an ASCII configuration file (in `.ini` format), and supports the generation of a configuration file.

Common usage of the remote `racadm` command is to remotely power-on/off and reset systems that are a part of groups or clusters, or to configure groups of RACs from scripts. A challenge-response authentication protocol is used for added authentication security.


## Using VT-100 Terminal Emulation With a DRAC III

- 1 Start terminal emulation and then complete the instructions as they appear on the screen.
- 2 When prompted, type the user name and password.

A menu appears with all of the commands that can be used with the DRAC III under VT-100 terminal emulation.

- 3 Select the command number that you want and press `<Enter>`.

As a security measure, if the VT-100 interface does not sense any activity for 300 seconds (this value is user-selectable; its default value is 300 seconds), a log out warning message appears and asks if you if you want to stay connected. If you do not select to stay connected before 15 seconds elapse (this value is not user-selectable), the current session is terminated and the user is logged out.

 **NOTICE:** Because the console redirection feature is designed only for use with text consoles, your management console must be in text mode for console redirection to work properly.

- 4 Select 3 to start console redirection. To end console redirection, the DRAC III provides a configurable "quit" key sequence of one to three keys. This key sequence is displayed when you start the VT-100 console redirection session. The default value for this key is `<F3>`.

### DRAC III VT-100 Communication Port Settings

If you want to use the VT-100 terminal emulation feature on a system not running a Windows operating system, you need to know the default communication port settings to configure your terminal emulation software. The default communication port settings are:

**Table 8-6. DRAC III VT-100 COM Port Settings**

<b>Setting Description</b>	<b>Required Setting</b>
Bits per second:	9600
Data bits:	8
Parity:	None
Stop bits:	1
Flow control:	Hardware

### **Using Terminal Emulation With Red Hat Linux**

For systems running Red Hat Linux, you can use the Minicom emulator program to connect to the DRAC III using the VT-100 cable. To connect using Minicom, see "Configuring Red Hat Linux Minicom for Serial Console Emulation."

# Hardware Specifications

This section provides information on the hardware attributes and characteristics of the RACs, including power requirements, PCI interfaces, and connectors.

## Power Requirements

### DRAC III

Table A-1 shows the power requirements for the DRAC III.

**Table A-1. DRAC III Power Requirements**

Power Source	Power Requirement
System power (PCI slot only)	+5 V at 2 A maximum
External AC power adapter capacity	+6 V at 2.5 A maximum
Battery backup capacity	1400 mAh (30 minutes of operation)

### DRAC III Power Supply Specifications

- Input: 110-240 V, 50-60 Hz, 35-42 vA
- Output: +6 V, 2.5 A

### DRAC III/XT

System power: +5 V standby at 1.1 A maximum

### ERA/O

System power: +2.5 V at 2 A maximum

## PCI Interface

### DRAC III

The DRAC III is compliant with PCI Local Bus Specification 2.1. Table A-2 provides the identification values for the card.

**Table A-2. DRAC III PCI Interface**

Item	Function	Value
Subsystem device ID	0	0x0007
	1	0x0008
	2	0x0009
Subsystem vendor ID		0x1028
Class code		088000 (generic system peripheral)

## Connectors

### DRAC III

The DRAC III connectors are summarized in Table A-3.

**Table A-3. DRAC III Connectors**

Connector	Type
VT-100 serial	10-pin connector
ICMB	6-pin connector
Hobbles	20-pin connector
IPMB	3-pin connector
Battery	2-pin connector
PCMCIA	68-pin connector
Network adapter	RJ-45 connector

### DRAC III/XT

The DRAC III/XT provides an RJ-45 network adapter connector and a 10-pin VT-100 serial connector (not currently supported).

### ERA

The ERA provides an RJ-45 network adapter connector (on the system board).

### ERA/O

The ERA/O provides an RJ-45 network adapter connector (on the system board).

# Troubleshooting

The purpose of this section is to help you diagnose and solve problems that may occur with your RAC.

## Basic Troubleshooting

This section provides solutions to common problems.

### Problem

Console redirection does not work.

You may see the following message on the bottom menu of the console redirect frame:

```
Please wait - initial screen loading.
```

### Solution

If you perform a hard reset on the RAC (using the racadm **racreset** command), the RAC driver cannot communicate with the RAC controller until the system is rebooted. Therefore, the hard reset should be reserved for extreme situations (for instance, a system lockup). Before using a hard reset, you should first try using the soft reset (using the soft reset function of the Web-based interface or the racadm **racreset soft** command), which does not terminate communication between the RAC driver and the RAC controller.



**NOTE:** Both hard and soft resets terminate all user sessions. Subsequently, issuing any kind of a reset causes all user interfaces to fail (for instance, when redirecting the console through the Web-based interface). After issuing a hard or soft reset, you must first log out and wait until the RAC is back online before logging on again.

### Problem

After performing a RAC reset (using the racadm **racreset** command), you issue a command and the following message is displayed: `racadm <command name> Transport: ERROR: (RC=-1)`

### Solution

You must wait until the RAC completes the reset before issuing another command.

**Problem**

The console redirect frame shows `Please wait - initial screen loading`, and seems to hang in this mode when the managed system is up, and VNC and PPP are running on the managed system.

**Solution**

A connection may not exist between the managed system and the firmware through a PPP connection. Rebooting the managed system may correct this problem. It is not necessary to reboot the RAC.

**Problem**

Console redirection fails to show the operating system boot menu in the Chinese, Japanese, and Korean versions of Microsoft® Windows® 2000.

**Solution**

To correct this problem, on systems running Windows 2000 that can boot to multiple operating systems, you can change the default boot operating system by performing the following steps:

- 1 Right-click the **My Computer** icon and select **Properties**.
- 2 Click the **Advanced** tab.
- 3 Click **Startup and Recovery**.
- 4 Select the new default operating system from the **Startup** list.
- 5 In the **Show list for** box, type the number of seconds that the list of choices should be displayed before the default operating system automatically boots.

**Problem**

The redirected console screen does not refresh.

**Solution**

Click **Refresh** in the console redirection window.

**Problem**

The following message is displayed: `warning: remote console is not available.`

**Solution**

This warning indicates one of the following conditions:

- The managed system is rebooting.
- The managed system screen is switching between text and graphic modes.
- Communication between the browser and the RAC has failed.

After waiting a few minutes for the system to restart or the screen to change modes, try restarting the console redirect window to correct the problem.

**Problem (DRAC III only)**

The IPMI interfaces do not provide the correct information.

***Solution***

On Dell™ PowerEdge™ 1650 systems, the DRAC III is installed on a riser board. The riser board plugs into the RISER connector on the system board and is considered an extension of the system board. Two riser board configurations are available for PowerEdge 1650 systems. The first features two 64-bit, 66-MHz expansion slots. The second features one 64-bit, 66-MHz expansion slot (PCI2) and one 32-bit, 33-MHz expansion slot (PCI1) for 5-V cards. In PowerEdge 1650 systems, if the DRAC III is installed on a riser card equipped with two 64-bit slots, the card operates, but the IPMI interface information provided is incorrect. To correct this problem, ensure that the DRAC III is installed on a 5-V riser card equipped with one 32-bit slot. For more information, see "Installing the DRAC III Hardware."

**Problem (DRAC III and DRAC III/XT only)**

Text redirection is not occurring when using console redirection.

This situation could occur if the DRAC III or DRAC III/XT is not installed on the primary PCI bus. To ensure that the DRAC III is installed in the correct PCI slot, see "Installing the DRAC III Hardware." To ensure that the DRAC III/XT is installed in the correct PCI slot, see "Installing the DRAC III/XT Hardware."

***Solution***

Ensure that the DRAC III or DRAC III/XT is installed on the primary PCI bus. For more information, see "Installing the DRAC III Hardware" or "Installing the DRAC III/XT Hardware."

**Problem**

Cannot connect to the remote access interface and the DNS sends back the IP address of the RAC instead of the managed system.

***Solution***

Due to functional details that are specific to Windows Dynamic DNS servers, the RAC internal PPP IP address is broadcast to the Dynamic DNS service running on Windows 2000 systems. The Dynamic DNS service stores that IP address in its DNS lookup table and associates it with the name of the managed system hosting the RAC. This action causes problems with Active Directory under Windows. The default value for a RAC's internal PPP IP address is 192.168.234.235, and it is user configurable. This issue has been addressed by Microsoft with a hot fix and Microsoft KnowledgeBase [Q](#) article ([Q292822](#)). To solve this problem, download the hot fix and perform the steps in the [Q](#) article.


**Problem (DRAC III only)**

Cannot connect to or ping a DRAC III from the management station after the dial-out properties have been set.

**Solution**


To access the management station through two distinct paths from the DRAC III, the DRAC III must have a host-based demand-dial route that does not conflict with the network-based LAN route.

- 1 Configure dial-up networking on the management station to assign static IP addresses for dial-in purposes. This configuration requires two addresses: one for the management station and one for the DRAC III.

 **NOTE:** It is important that the static IP addresses used by the management station be on a different subnet from the DRAC III network adapter. Otherwise, a routing loop is created.

Typically, the numerically lower address is assigned to the management station and the numerically larger address is assigned to the DRAC III when the dial-in connection is completed.

- 2 Configure the static IP address assigned to the management station as the demand-dial destination IP address on the DRAC III; configure this identical address as an SNMP trap destination (for SNMP trap alerts) or as the SMTP server address (for e-mail alerts) on the DRAC III.

 **NOTE:** You can use DHCP to configure the IP addresses, but you must still ensure that both addresses used by the management station for dial-in are on a different subnet from the DRAC III NIC.

The management station is now able to receive alerts from the DRAC III through both the LAN and the dial-in connection.

**Problem**

Graphics redirection is not occurring when using console redirection.

This situation could occur if the RAC services are not installed properly or are not running.

**Solution**

After allowing several minutes for the graphics redirection to occur, ensure that the RAC services are running. Try stopping and then starting the services. If the problem persists, reboot the system.



## Using the RAC Trace Log

The internal RAC Trace Log can be used by administrators needing to debug alerting, paging, or networking from the RAC. The Trace Log can be accessed from the RAC Web-based remote access interface by clicking the **Debug** tab, and then clicking **Network Debug**. From the **Network Debug** window, select **Dump Trace Log**, and then click **Submit**. The Trace Log tracks the following information:

- **CHAT** – Traces modem interactions similar to those found on Red Hat Linux systems. The CHAT protocol includes **expect** and **send** character sequences, where certain responses from the modem are expected, and commands are sent to the modem.
- **DHCP** – Traces packets sent to and received from a DHCP server.
- **IP** – Traces only IP packets transmitted through PPP links, not packets transmitted through the network adapter.
- **PPP** – Traces negotiation packets.
- **TAP** – Traces TAP interactions used with alphanumeric paging.



**NOTE:** Settings for CHAT, DHCP, IP, PPP, and TAP (DRAC III only) can be accessed from the RAC remote access GUI by clicking the **Debug** tab, and then clicking **Trace Level**.



**NOTE:** In the RAC Trace Log, nonprintable ASCII characters are translated to printable ASCII characters. If the character code is less than **0x20**, or between **0x7f** and **0xa0** (inclusive), the value **0x40** is exclusive-or'd with the character before printing, after a **"^"** is added to the beginning. Thus, the ASCII carriage return character, **0xd**, is printed as **"^M"** in the Trace Log. Nonprintable ASCII characters may occur during tracing of the CHAT and TAP protocols, and occasionally during PPP negotiations.

Some paging services return a busy signal when a paging request is successfully accepted. This cannot be distinguished from the case where the line is busy, and the paging service never answered. Therefore, even though the chat script expects **BUSY**, this is indicated as a failure on the trace log.

A chat script time-out is considered a success indication for numeric paging, because no other error indications were detected. Since numeric paging services do not have a positive confirmation indication that can be detected by the modem, numeric paging is inherently unreliable. For this reason, up to three numeric paging attempts are made, and duplicate numeric pages may be received.

## Troubleshooting Network Problems

The RAC provides a standard set of network diagnostic tools, similar to those found on Windows or Red Hat® Linux-based systems. Using the RAC Web-based remote access interface, you can access the following network debugging tools by clicking the **Debug** tab and then clicking **Network Debug**. For more information about the Network Debug feature, see the remote access interface help.

The trace log may also contain RAC operating-system specific error codes (relating to the internal RAC operating system, not the managed system's operating system). Table B-1 can help you diagnose network problems reported by the internal RAC operating system.

**Table B-1. RAC Error Codes**

<b>Error Code</b>	<b>Description</b>
0x5006	ENXIO: No such address.
0x5009	EBADS: The socket descriptor is invalid.
0x500D	EACCESS: Permission denied.
0x5011	EEXIST: Duplicate entry exists.
0x5016	EINVALID: An argument is invalid.
0x5017	ENFILE: An internal table has run out of space.
0x5020	EPIPE: The connection is broken.
0x5023	EWOULDBLOCK: The operation would block; socket is nonblocking.
0x5024	EINPROGRESS: Socket is nonblocking; connection not completed immediately.
0x5025	EALREADY: Socket is nonblocking; previous connection attempt not complete.
0x5027	EDESTADDRREQ: The destination address is invalid.
0x5028	EMSGSIZE: Message too long.
0x5029	EPROTOTYPE: Wrong protocol type for socket.
0x502A	ENOPROTOOPT: Protocol not available.
0x502B	EPROTONO SUPPORT: Protocol not supported.
0x502D	EOPNOTSUPP: Requested operation not valid for this type of socket.
0x502F	EAFNOSUPPORT: Address family not support.
0x5030	EADDRINUSE: Address is already in use.
0x5031	EADDRNOTAVAIL: Address not available.
0x5033	ENETUNREACH: Network is unreachable.
0x5035	ECONNABORTED: The connection has been aborted by the peer.
0x5036	ECONNRESET: The connection has been reset by the peer.
0x5037	ENOBUFS: An internal buffer is required but cannot be allocated.
0x5038	EISCONN: The socket is already connected.
0x5039	ENOTCONN: The socket is not connected.
0x503B	ETOOMANYREFS: Too many references, cannot splice.
0x503C	ETIMEDOUT: Connection timed out.

**Table B-1. RAC Error Codes (continued)**

Error Code	Description
0x503D	ECONNREFUSED: The connection attempt was refused.
0x5041	EHOSTUNREACH: The destination host could not be reached.
0x5046	ENIDOWN: NI_INIT returned -1.
0x5047	ENMTU: The MTU is invalid.
0x5048	ENHWL: The hardware length is invalid.
0x5049	ENNOFIND: The route specified cannot be found.
0x504A	ECOLL: Collision in select call; these conditions already selected by another task.
0x504B	ETID: The task ID is invalid.


## Troubleshooting Alerting Problems

Use the following information to troubleshoot a particular type of RAC alert:

- **E-mail paging** – E-mail paging uses SMTP. To troubleshoot e-mail paging problems, check SMTP entries in the trace log. All interactions with the SMTP server are logged in the Trace Log by default.
- **SNMP traps** – SNMP trap deliveries are logged in the Trace Log by default. However, since SNMP does not confirm delivery of traps, it is best to trace the packets on the managed system using a network analyzer or a tool such as Microsoft's **snmputil**.
- **Numeric paging** – (DRAC III only) Numeric paging uses the CHAT protocol. To troubleshoot numeric paging problems, check CHAT entries in the trace log. To trace CHAT, first ensure that CHAT is selected under **Debug**→**Trace Log**, and then display the trace log to identify CHAT problems.
- **Alphanumeric paging** – (DRAC III only) Alphanumeric paging uses TAP. To troubleshoot alphanumeric paging problems, check TAP entries in the trace log. To trace TAP, first ensure that TAP is selected under **Debug**→**Trace Log**, and then display the trace log to identify TAP problems.

## RAC Log Messages

RAC Log messages can be used by administrators to debug alerting from the RAC. Table B-2 provides a list of RAC log message IDs, message and description, as well as corrective actions to take for a particular message.

 **NOTE:** In Table B-2, the character "L" is sometimes used in the **Message ID** column. "L" represents the severity level or type of the message, which can be one of the following: W (warning), E (error), S (severe), F (fatal), or A (always).

**Table B-2. RAC Log Messages**

<b>Message ID</b>	<b>Description</b>	<b>Corrective Action</b>
RAC186L	dhcp: no response from server, need LAN address. The network adapter cannot be enabled until a response is received from the DHCP server.	Provides information only. No specific corrective action is indicated. Ensure that the DHCP server is operational.
RAC187L	dhcp: no response from server, using default PPP addresses	Provides information only. No specific corrective action is indicated. Ensure that the DHCP server is operational.
RAC188L	dhcp: no response from server, warm starting with <IP address>	Provides information only. No specific corrective action is indicated. Ensure that the DHCP server is operational.
RAC189L	snmp: trap sent to <IP address>	Provides information only. No corrective action is necessary.
RAC191L	snmp: internal failure during trap generation	Reset the RAC and retry the operation.
RAC192L	numeric page successful	Provides information only. No corrective action is necessary.
RAC193L	numeric paging attempts failed	Ensure that the telephone number is correct and that the paging service is operational.
RAC194L	numeric paging encountered an internal error	Reset the DRAC III and retry the operation.
RAC195L	alphanumeric page successful	Provides information only. No corrective action is necessary.
RAC196L	alphanumeric paging attempts failed	Ensure that the phone number, pager ID, and password are correct. Also, ensure that Paging Central is operational.
RAC197L	alphanumeric paging encountered an internal error	Reset the DRAC III and retry the operation.
RAC198L	E-mail page successful	Provides information only. No corrective action is necessary.

**Table B-2. RAC Log Messages (continued)**

<b>Message ID</b>	<b>Description</b>	<b>Corrective Action</b>
RAC199L	E-mail paging attempts failed, SMTP protocol failure	A trace of the SMTP connection may be found in the trace log. Examine the trace log to identify the source of the protocol failure, such as the connection could not be established (SMTP server is down or an invalid IP address), an invalid e-mail destination address, an invalid domain in the e-mail address, or the SMTP server does not support forwarding e-mail. Correct the problem and try again.
RAC200L	E-mail paging encountered an internal error	Reset the RAC and retry the operation.
RAC201L	trap paging filter passed, entry <number> user paging filter passed	Provides information only. No corrective action necessary.
RAC253L	PAP peer authentication succeeded for <user> CHAP peer authentication succeeded for <user>	Provides information only. No corrective action is necessary.
RAC254L	PAP peer authentication failed for <user> CHAP peer authentication failed for <user>	Verify that the dial-in or demand dial-out entry remote user name and password are correct. This user name and password are used for the PPP connection only, and are not an administrator log in user name and password.
RAC256L	RAC hardware log event: <formatted hardware log event>	Provides information only. No corrective action is necessary, unless the contents of the hardware log indicate a problem. In this case, the corrective action is based on the problem reported; for example, battery voltage low indicates that the battery may need replacing.
RAC016A	RAC log cleared	Provides information only.
RAC030A	RAC time was set	Provides information only.
RAC048A	RAC firmware update was initiated.	Provides information only.
RAC049A	RAC Firmware Update was initiated with config to defaults option.	Provides information only.

**Table B-2. RAC Log Messages (continued)**

<b>Message ID</b>	<b>Description</b>	<b>Corrective Action</b>
RAC064A	clear crash screen	Provides information only.
RAC065A	RAC hard reset, delay <seconds> was initiated	Provides information only.
RAC066A	RAC soft reset, delay <seconds> was initiated	Provides information only.
RAC067A	RAC graceful reset, delay <seconds> was initiated	Provides information only.
RAC068A	RAC cfg2default reset, delay <seconds> was initiated	Provides information only.
RAC069A	RAC shutdown was initiated	Provides information only.
RAC114A	Requested server {powerdown powerup  powercycle hardreset  graceshutdown gracepowercycle  gracereboot}	Provides information only.
RAC115A	Could not log graceful server action to hardware log	Provides information only.
RAC122A	RAC booted	Provides information only.
RAC138A	Console redirect session enabled	Provides information only.
RAC139A	Console redirect session disabled	Provides information only.
RAC154A	Logout from <IP-address>	Provides information only.
RAC155A	Login from <IP-address>	Provides information only.
RAC156A	session cancelled from <IP- address>, max log in attempts exceeded.	Provides information only.
RAC157A	Session cancelled from <IP- address>, due to inactivity.	Provides information only.
RAC158A	Unvalidated session from <IP- address> cancelled.	Provides information only.
RAC175A	vt-100: log in {successful authentication failed}	Provides information only.
RAC176A	vt-100: log out	Provides information only.
RAC240A	RAC shutdown through hwmon	Provides information only.

**Table B-2. RAC Log Messages (continued)**

Message ID	Description	Corrective Action
RAC241A	RAC shutdown due to battery runtime limit expired	Provides information only.
RAC242A	RAC shutdown due to voltage below threshold	Provides information only.
RAC243A	RAC shutdown due to non-PCI slot presence	Provides information only.

## DRAC III LED Indicators

The DRAC III has two LEDs located on the back of the card connector. The top LED is green, and is called the heartbeat LED. The amber LED is below the green, and is called the error LED.

The following are conditions indicated by the DRAC III LEDs:

- Normal operation – Approximately 10–15 seconds after power up or reset, the two LEDs toggle for about 2 seconds. The flashing LEDs indicate that the DRAC III is running its self-test. A few seconds later, the green LED starts flashing on and off at 1-second intervals. Sometimes the green LED appears to flash sporadically; this situation may occur at start-up and at any other time the DRAC III processor is under a heavy load.
- Error condition – The error LED is illuminated when the following conditions occur:
  - An unrecoverable hardware error – The error LED is steadily illuminated.
  - A firmware problem – The LED flashes at .5-second intervals.
  - A self-test error – The error LED flashes according to a *blink code*. See "Self-Test Error Blink Codes" for a description of these codes.

### Nonrecoverable POST Error

If the amber LED is solid, it indicates a nonrecoverable error. A nonrecoverable error occurs when a POST memory test or core operation has failed, and the DRAC III cannot proceed with a boot process. The DRAC III must be replaced.

Summary for this condition:

- Amber on
- Green off

### Repair Mode

If the amber LED is flashing at .5-second intervals, it indicates that the core, firmware, database, or production sector in the DRAC III flash is corrupted. A field technician must replace the DRAC III.

Summary for this condition:

- Amber flash at .5-second intervals
- Green off

### **Self-Test Error Blink Codes**

The following sections define the blink codes that are produced by the amber error LED if an error is detected by any of the self-tests or extended self-tests.

The blink code repeats about every 10 seconds. For example, a code of 3114 (a problem in the uart loopback test) causes the amber LED to flash three times, pause, flash one time, pause, flash one time, pause, flash four times. The sequence then repeats after 10 seconds.

### **Internal DRAC III Operating System Problems**

1111 = Unable to create a self-test task.

1112 = A self-test task is currently running. (Multiple self-tests cannot be started.)

1113 = Failure creating a self-test visual signal.

1114 = Failure to allocate required DRAC III system memory.

1115 = Failure writing the D\_selftest\_BDSTATUS.

1116 = Failure attempting to send a debug message.

1117 = Error when accessing the DRAC III database.

### **Memory Test Problems**

2111 = Failure in extended memory testing — Read verify, write.

2112 = Failure in extended memory testing — Read verify write high memory to low.

2113 = Failure in extended memory testing — Read verify, write, write, low-to-high.

2114 = Failure in extended memory testing — Read verify, write, write, high-to-low.

2115 = Failure in extended memory testing — Read verify, high-to-low.

2116 = Failure in extended memory testing — Read verify, low-to-high.

2117 = Failure in marching memory test — Read verify, write.

2118 = Failure in marching memory test — Read verify in low-to-high memory.

### **VT-100 Uart Loopback Test**

3111 = Failure opening uart for external loopback.

3112 = Failure in I/O control to uart driver.

3113 = Failure writing data to the uart.

3114 = Failure reading data from the uart.



- 3115 = Transmit/receive data miscompare.
- 3116 = Failure trying to suspend VT-100 task.

### **GPIO Test**

- 4111 = Failure in the GPIO green LED test.
- 4112 = Failure in the GPIO LED test.
- 4113 = SMI connector GPIOs not reading inactive values.

### **On-Board Hardware Monitor**

- 5111 = More than one power source is selected (internal DRAC III issue).
- 5112 = A power source is shown not to be running (internal DRAC III issue).
- 5113 = Failure in the onboard hardware monitor sensors/logic. (The managed system must be powered up or the PCI voltage tests fail.)
- 5114 = Failure accessing data base for hardware monitor parameters.
- 5115 = Failure in accessing the onboard hardware monitor.
- 5121 = DRAC III battery voltage is out of range.
- 5122 = DRAC III external power adapter voltage is out of range.
- 5123 = PCI AUX 3.3 voltage is out of range.
- 5124 = PCI +5 voltage is out of range.
- 5125 = PCI -12 voltage is out of range.
- 5126 = PCI +12 voltage is out of range.
- 5127 = DRAC III temperature monitor is out of range.
- 5128 = DRAC III battery presence is not detected.
- 5129 = DRAC III external power adapter presence is not detected.

### **IPMI Tests**

- 6111 = No IPMI connector is detected.
- 6112 = IPMI Get Chassis Status command to the BMC failed.

### **EXPROM Tests**

- 7111 = Failure when loading the EXPROM image from the database into shared memory.
- 7112 = Failure when loading the EXPROM header from the database into shared memory.
- 7113 = Invalid EXPROM header signature.
- 7114 = Invalid EXPROM vendor or device ID.

### **Flash Test**

- 8111 = Failure erasing U16 (Firmware) diagnostic sector.
- 8112 = Failure writing U16 (Firmware) diagnostic sector.
- 8113 = Failure read/verify U16 (Firmware) diagnostic sector.
- 8114 = Failure erasing U17 (DataBase) diagnostic sector.
- 8115 = Failure writing U17 (DataBase) diagnostic sector.
- 8116 = Failure writing U17 (DataBase) diagnostic sector.

### **PCMCIA Tests**

- 9111 = Failure in PCMCIA to DRAC III interface.

# Abbreviations and Acronyms

## **AGP**

Abbreviation for accelerated graphics port, which is a bus specification that allows graphics cards faster access to main system memory.

## **ARP**

Acronym for Address Resolution Protocol, which is a method for finding a host's Ethernet address from its Internet address.

## **ASCII**

Acronym for American Standard Code for Information Interchange, which is a code representation used for displaying or printing letters, numbers, and other characters.

## **BIOS**

Acronym for basic input/output system, which is the part of system software that provides the lowest-level interface to peripheral devices and which controls the first stage of the system boot process, including installation of the operating system into memory.

## **BMC**

Abbreviation for baseboard management controller, which is the controller interface between the RAC and the managed system's ESM.

## **bus**

A set of conductors connecting the various functional units in a computer. Busses are named by the type of data they carry, such as data bus, address bus, or PCI bus.

## **CD**

Abbreviation for compact disc.

## **CHAP**

Acronym for Challenge-Handshake Authentication Protocol, which is an authentication method used by

PPP servers to validate the identity of the originator of the connection.

## **CIM**

Acronym for Common Information Model, which is a protocol designed for managing systems on a network.

## **CLI**

Abbreviation for command-line interface.

## **console redirection**

Console redirection is a function that directs a managed system's display screen, mouse functions, and keyboard functions to the corresponding devices on a management station. You may then use the management station's system console to control the managed system.

## **DHCP**

Abbreviation for Dynamic Host Configuration Protocol, which is a protocol that provides a means to dynamically allocate IP addresses to computers on a local area network.

## **DLL**

Abbreviation for Dynamic Link Library, which is a library of small programs, any of which can be called when needed by a larger program that is running in the system. The small program that lets the larger program communicate with a specific device such as a printer or scanner is often packaged as a DLL program (or file).

## **DRAC III**

Abbreviation for Dell™ Remote Access Card III.

## **DRAC III/XT**

Abbreviation for Dell Remote Access Card III/XT.

**DSU**

Abbreviation for disk storage unit.

**ERA**

Abbreviation for Embedded Remote Access.

**ERA/O**

Abbreviation for Embedded Remote Access Option.

**ESM**

Abbreviation for embedded systems management, which is a set of instruction coding in system software and firmware that notifies a user about potential hardware problems on a Dell system.

**GMT**

Abbreviation for Greenwich Mean Time, which is the standard time common to every place in the world. GMT nominally reflects the mean solar time along the prime meridian (0 longitude) that runs through the Greenwich Observatory outside of London, UK.

**GPIO**

Abbreviation for general purpose input/output.

**GUI**

Abbreviation for graphical user interface, which refers to a computer display interface that uses elements such as windows, dialog boxes, and buttons as opposed to a command prompt interface, in which all user interaction is displayed and typed in text.

**hardware log**

Records events generated by the RAC and ESM.

**ICMB**

Abbreviation for Intelligent Chassis Management Bus.

**ID**

Abbreviation for identifier, commonly used when referring to a user identifier (user ID) or object identifier (object ID).

**IP**

Abbreviation for Internet Protocol, which is the network layer for TCP/IP. IP provides packet routing, fragmentation, and reassembly.

**IPMB**

Abbreviation for intelligent system management bus, which is a bus used in systems management technology.

**IPMI**

Abbreviation for Intelligent Platform Management Interface, which is a part of systems management technology.

**JVM**

Abbreviation for Java Virtual Machine, which is a system-independent execution environment that converts compiled Java code (byte code) for a system processor so that it can perform a Java program instructions.

**Kbps**

Abbreviation for kilobits per second, which is a data transfer rate.

**LAN**

Abbreviation for local area network.

**LED**

Abbreviation for light-emitting diode.

**MAC**

Acronym for media access control, which is a network sublayer between a network node and the network physical layer.

**MAC address**

Acronym for media access control address, which is a unique address embedded in the physical components of a network adapter.

**managed system**

The managed system is the system in which the RAC is installed or embedded.

**management station**

The management station is a system that remotely accesses the RAC.

**Mbps**

Abbreviation for megabits per second, which is a data transfer rate.

**MIB**

Abbreviation for management information base.

**NAS**

Abbreviation for network attached storage.

**network adapter**

An adapter circuit board installed in a computer to provide a physical connection to a network.

**NLM**

Abbreviation for NetWare<sup>®</sup> Loadable Module.

**PCI**

Abbreviation for Peripheral Component Interconnect, which is a standard interface and bus technology for connecting peripherals to a system and for communicating with those peripherals.

**PCMCIA**

Abbreviation for Personal Computer Memory Card International Association, which is a technology standard for connecting PCMCIA devices to systems. PCMCIA devices are about the size of a credit card and are mainly used in notebook computers, although the DRAC III supports an optional PCMCIA modem.

**POST**

Acronym for power-on self-test, which is a sequence of diagnostic tests that are run automatically by a system when it is powered on.

**PPP**

Abbreviation for Point-to-Point Protocol, which is the Internet standard protocol for transmitting network layer datagrams (such as IP packets) over serial point-to-point links.

**RAM**

Acronym for random-access memory. RAM is general-purpose readable and writable memory on systems and the RAC.

**RAM disk**

A memory-resident program which emulates a hard drive. The RAC maintains a RAM disk in its memory.

**RAC**

Abbreviation for remote access controller.

**RAS**

Acronym for remote access service, which is a service provided by some Microsoft<sup>®</sup> Windows<sup>®</sup> operating systems that allows most of the services that would be available on a network to be accessed over a modem. The service includes support for dial-up and logon tasks and presents the same network interface as the normal network drivers used for the network adapter.

**RFB**

Abbreviation for remote floppy boot.

**ROM**

Acronym for read-only memory, which is memory from which data may be read, but to which data cannot be written.

**RPM**

Abbreviation for Red Hat<sup>®</sup> Package Manager, which is a package-management system for the Red Hat Linux operating system that helps installation of software packages. It is similar to an installation program.

**SMI**

Abbreviation for systems management interrupt.

**SMTP**

Abbreviation for Simple Mail Transfer Protocol, which is a protocol used to transfer electronic mail between systems, usually over an Ethernet.

**SNMP**

Abbreviation for Simple Network Management Protocol, which is a protocol designed to manage nodes on an IP network. RACs are SNMP-managed devices (nodes).

**SNMP trap**

A notification (event) generated by the RAC or ESM that contains information about state changes on the managed system or about potential hardware problems.

**SSL**

Abbreviation for secure sockets layer.

**TAP**

Abbreviation for Telelocator Alphanumeric Protocol, which is a protocol used for submitting requests to a pager service.

**TCP/IP**

Abbreviation for Transmission Control Protocol/Internet Protocol, which represents the set of standard Ethernet protocols that includes the network layer and transport layer protocols.

**TFTP**

Abbreviation for Trivial File Transfer Protocol, which is a simple file transfer protocol used for downloading boot code to diskless devices or systems.

**UPS**

Abbreviation for uninterruptible power supply.

**UTC**

Abbreviation for Universal Coordinated Time. *See* GMT.

**VNC**

Abbreviation for virtual network computing.

**VT-100**

Abbreviation for Video Terminal 100, which is used by the most common terminal emulation programs.

**WAN**

Abbreviation for wide area network.

## Figures

Figure 2-1.	DRAC III Hardware Components . . . . .	24
Figure 3-1.	DRAC III/XT Hardware Components . . . . .	45
Figure 7-1.	Sample Remote Access Service RAC Home Page . . .	71





## Tables

Table 1-1.	RAC Software Components . . . . .	15
Table 1-2.	RAC Configuration Interfaces . . . . .	16
Table 1-3.	Supported Remote Access Connections . . . . .	17
Table 1-4.	Remote Access Interfaces . . . . .	17
Table 1-5.	RAC Ports . . . . .	18
Table 1-6.	Supported Event Alerts . . . . .	19
Table 7-1.	Remote Floppy Boot Settings . . . . .	81
Table 7-2.	Remote Floppy Boot Commands . . . . .	82
Table 7-3.	Remote Floppy Boot Configuration Settings . . . . .	82
Table 8-1.	Racadm cfgSerial Objects for Configuring the Serial/Telnet Console . . . . .	93
Table 8-2.	Required Pinout for DB-9 Null Modem Cable . . . . .	94
Table 8-3.	Minicom Settings for Serial Console Emulation . . . . .	96
Table 8-4.	Management Station COM Port Settings . . . . .	97
Table 8-5.	Differences Between "connect com2" and "connect video" Commands . . . . .	98
Table 8-6.	DRAC III VT-100 COM Port Settings . . . . .	100
Table A-1.	DRAC III Power Requirements . . . . .	101
Table A-2.	DRAC III PCI Interface . . . . .	102
Table A-3.	DRAC III Connectors . . . . .	102
Table B-1.	RAC Error Codes . . . . .	108
Table B-2.	RAC Log Messages . . . . .	110

