

Dell™ Remote Console Switch

User's 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 potential for property damage, personal injury, or death.

Information in this document is subject to change without notice.
© 2010 Dell Inc. All rights reserved.

Third Party Software. You acknowledge that the SOFTWARE PRODUCT may contain or be provided with copyrighted software of Dell's suppliers as identified in associated documentation or other printed or electronic materials ("Third Party Software") which are obtained under a license from such suppliers. Your use of any such Third Party Software shall be subject to and you agree to comply with the applicable restrictions and other terms and conditions set forth in such documentation or materials as set forth in any "Third-Party Licenses ReadMe" file or similar file located in the installation directory for the SOFTWARE PRODUCT.

Any open source software is distributed in the hope that it will be useful, but is provided "as is" without any expressed or implied warranty; including but not limited to the implied warranty of merchantability or fitness for a particular purpose. In no event shall Dell, the copyright holders, or the contributors be liable for any direct, indirect, incidental, special, exemplary, or consequential damages (including, but not limited to, procurement of substitute goods or services; loss of use, data or profits; or business interruption) however caused and on any theory of liability, whether in contract, strict liability, or tort (including negligence or otherwise) arising in any way out of the use of this software, even if advised of the possibility of such damage.

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

Trademarks used in this text: *Avocent* is a registered trademarks of Avocent Corporation. *OSCAR* is a registered trademark of Avocent Corporation or its affiliates. *Dell*, *OpenManage*, and the *DELL* logo are trademarks of Dell Inc.; *Active Directory*, *DirectDraw*, *Internet Explorer*, *Microsoft*, *Win32*, *Windows*, *Windows NT*, *Windows Server*, and *Windows Vista* are either trademarks or registered trademarks of Microsoft Corporation in the United States and/or other countries; *Intel* and *Pentium* are registered trademarks of Intel Corporation; *Red Hat* and *Red Hat Enterprise Linux* are registered trademarks of Red Hat, Inc.; *SUSE* is a registered trademark of Novell Inc. in the United States and other countries; *UNIX* is a registered trademark of The Open Group in the United States and other countries; *Sun*, *Sun Microsystems*, and the Sun logo are trademarks or registered trademarks of Sun Microsystems, Inc. or its subsidiaries 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.

590-1049-501A

October 2010

Model 2161DS-2/4161DS/2321DS Remote Console Switch

Safety and EMC Approvals and Markings

- UL / cUL
- CE - EU
- N (Nemko)
- GOST
- C-Tick
- NOM / NYCE
- MIC (BCC)
- SASO
- GS
- IRAM
- FCC, ICES,
- VCCI
- SoNCAP
- SABS
- Bellis
- FIS/ Kvalitet
- Koncar
- KUCAS
- INSM
- Ukrtest
- STZ Z

Safety certifications and EMC certifications for this product are obtained under one or more of the following designations: CMN (Certification Model Number), MPN (Manufacturer's Part Number) or Sales Level Model designation. The designation that is referenced in the EMC and/or safety reports and certificates is printed on the label applied to this product.

Please refer to the *Dell Regulatory Technical Bulletin* included with your Remote Console Switch for more detailed EMC and EA text.

Contents

Safety Precautions.	xiii
General	xiii
Rack Mounting of Systems	xv
LAN Options.	xvi
1 Product Overview	1
Remote Console Switch Features and Benefits.	1
SIP Intelligent Module	1
Multiplatform Support	2
Interoperability with Avocent® IQ Module Intelligent Cabling	2
OSCAR Interface	2
On-board Web Interface	2
DSView® 3 Management Software Plug-in	2
Virtual Media	3
Security	3
Encryption.	3
Operation Modes	4
Video	4
.	5
FLASH Upgradeable	5
Cascade (Tier) Expansion.	5
Remote Console Switch Software Features and Benefits	5
Easy to Install and Configure	6
Powerful Customization Capabilities	6
Extensive Remote Console Switch Management	6
IPv4 and IPv6 Capabilities	6

	LDAP	6
	Interoperability with Avocent Products.	7
2	Installation.	9
	Remote Console Switch Quick Setup Checklist	9
	Remote Console Switch Installation and Setup.	10
	Getting Started	10
	Setting Up Your Network	11
	Keyboards.	11
	Rack Mounting Your Remote Console Switch Unit	11
	Installing the Remote Console Switch Unit.	15
	Video Optimization	24
	Mouse Acceleration	24
	Connecting a SIP	24
	Adding a Cascade Switch.	26
	Cascading with Legacy Switches.	29
	Adding a PEM (Optional)	30
	Connecting to the Network	32
	On-board Web Interface Installation and Setup.	32
	Supported Browsers	32
	Launching the On-board Web Interface	32
3	Controlling Your System at the Analog Ports 35	
	Viewing and Selecting Ports and Devices	35
	Selecting Devices.	37
	Soft Switching.	37
	Navigating the OSCAR Interface.	38

Configuring OSCAR Interface Menus	40
Changing the Display Behavior.	41
Setting Console Security	43
Controlling the Status Flag	45
Setting the Interface Language.	47
Assigning Device Types	47
Assigning Device Names.	49
Configuring Network Settings	50
Displaying Version Information	52
Scanning Your System.	52
Setting the Preemption Warning	54
Displaying Configuration Information.	55
Running System Diagnostics	56
Broadcasting to Servers.	57
Power Controlling Devices	59
Power window	59
PDUs window.	60
PDU Settings window.	60
PDU Inlets window	61
PDU Outlets window	62
4 Using the Viewer	65
Accessing Servers from the On-board Web Interface	65
Interacting With the Server Being Viewed	66
Viewer Window Features.	67
Adjusting the Viewer	68
Adjusting the Viewer Resolution	71

Adjusting the Video Quality	72
Minimizing Remote Video Session Discoloration.	74
Improving Screen Background Color Display	74
Setting Mouse Scaling	75
Minimizing Mouse Trailing	76
Improving Mouse Performance.	76
Viewing Multiple Servers Using the Scan Mode	77
Scanning Your Servers	77
Thumbnail View Status Indicators	79
Navigating the Thumbnail Viewer	80
Using Macros to Send Keystrokes to the Server.	81
Session Options - General Tab	82
Screen Capturing	83
Preemption	84
Preemption of Remote User by a Remote Administrator	85
Preemption of a Local User/Remote Administrator by a Remote Administrator	85
Connection Sharing.	86
5 Virtual Media	89
Common Virtual Media Terms	89
Configuring Virtual Media Locally.	90
Enabling/Disabling Virtual Media Using the OSCAR Interface	90
Setting Virtual Media Options Using the OSCAR Interface	91
Configuring Virtual Media Remotely	93
Enabling/Disabling Virtual Media Using the On-board Web Interface	93
Setting Virtual Media Options Using the On-board Web Interface	95
Launching Virtual Media.	95

Virtual Floppy Drive	97
Virtual CD/DVD Drive	98
Virtual Media Connection Status	98
Reserving a Virtual Media Session	99
Resetting the USB Bus	99

6 Managing Your Remote Console Switch Using the On-board Web Interface 101

Migrating Switches from the Remote Console Switch Software
101

Viewing and Configuring Remote Console Switch Parameters 102

Changing Remote Console Switch Parameters . . .	102
Setting Up User Accounts	104
Locking and Unlocking User Accounts	108
Enabling and Configuring SNMP	109
Enabling Individual SNMP Traps	111
Viewing and Resynchronizing Server Connections	112
Modifying a Server Name	113
Viewing and Configuring Tiered Switch Connections	114
Viewing the SIPs and IQ Modules	115

Viewing Remote Console Switch Version Information . 116

SIPs Subcategory. 117

Upgrading Firmware 120

Controlling User Status 123

Rebooting Your System 125

Managing Remote Console Switch Configuration Files 125

Managing User Databases 126

Installing a Web Certificate 128

	Managing PDUs	129
7	Migrating Your Remote Console Switch	133
	Accessing the AMP	133
	Upgrading Firmware Using the AMP	134
	Upgrading Remote Console Switch Firmware	134
	Migrating Remote Console Switches to the On-board Web Interface	135
	Using the Resync Wizard	137
8	LDAP Feature for the Remote Console Switch	139
	Overview	139
	The Structure of Active Directory	139
	Domain Controller Computers	140
	Object Classes	140
	Attributes	141
	Schema Extensions	141
	Standard Schema versus Dell Extended Schema	142
	Standard Installation	143
	Configure the Override Admin Account	144
	Configuring DNS Settings	144
	Configuring the Network Time Protocol Settings	145
	Configuring the LDAP Authentication Parameters	146
	LDAP SSL Certificates	149

Enabling SSL on a Domain Controller	149
Login Timeout.	154
CA Certificate Information Display	154
Configuring Group Objects	155
Active Directory Object Overview for Standard Schema	158
Dell Extended Schema Active Directory Object Overview	159
Configuring Active Directory with Dell Schema Extensions to Access Your RCS	164
Extending the Active Directory Schema (Optional)	164
Installing the Dell Extension to the Active Directory Users and Computers Snap-In (Optional)	165
Adding Users and Privileges to Active Directory with Dell Schema Extensions	166
Creating a SIP Object.	166
Creating a Privilege Object.	166
Using Dell Association Objects Syntax.	167
Creating an Association Object.	168
Adding Objects to an Association Object	168
Console Redirection Access Security.	169
Using Active Directory to Log In to the Remote Console Switch	170
Target Device Naming Requirements for LDAP Implementation	170
Frequently Asked Questions.	171

A Appendix A: Remote Console Switch Software

Keyboard and Mouse Shortcuts	175
B Appendix B: TCP Ports.	179
C Appendix C: MIBs and SNMP Traps . . .	181
MIB Groups	182
Enterprise Traps.	195
D Appendix D: FLASH Upgrades	211
Upgrading the Remote Console Switch.	211
Upgrading the SIP module firmware	214
E Appendix E: Technical Specifications . .	217
F Appendix F: Technical Support	221
Index	223

Safety Precautions

Use the following safety guidelines to help ensure your own personal safety and to help protect your system and working environment from potential damage.

CAUTION: The power supplies in your system may produce high voltages and energy hazards, which can cause bodily harm. Only trained service technicians are authorized to remove the covers and access any of the components inside the system. This warning applies to Dell™ PowerEdge™ servers and Dell PowerVault™ storage systems.

This document pertains only to the Dell 2161DS-2/4161DS/2321DS Console Switch. You should also read and follow the additional safety instructions.

- The *Remote Console Switch Installation Guide* included with your rack solution that describes how to install your system into a rack.
- The *User's Guide* which provides information about setting up and operating your rack mounted server system.
- The appropriate Avocent installer/user guide for your product, if applicable. Visit avocent.com/manuals for more information.

General

- Observe and follow service markings.
- Do not service any product except as explained in your system documentation.
- Opening or removing covers that are marked with the triangular symbol with a lightning bolt may expose you to electrical shock.
- Components inside these compartments should be serviced only by a trained service technician.
 - This product contains no serviceable components. Do not attempt to open.

- If any of the following conditions occur, unplug the product from the electrical outlet and replace the part or contact your trained service provider:
 - The power cable, extension cable, or plug is damaged.
 - An object has fallen into the product.
 - The product has been exposed to water.
 - The product has been dropped or damaged.
 - The product does not operate correctly when you follow the operating instructions.
- Keep your system away from radiators and heat sources. Also, do not block cooling vents.
- Do not spill food or liquids on your system components, and never operate the product in a wet environment. If the system gets wet, see the appropriate section in your troubleshooting guide or contact your trained service provider.
- Use the product only with approved equipment.
- Allow the product to cool before removing covers or touching internal components.
- Operate the product only from the type of external power source indicated on the electrical ratings label. If you are not sure of the type of power source required, consult your service provider or local power company.

NOTICE: To help avoid damaging your system, be sure the voltage selection switch (if provided) on the power supply is set for the voltage that most closely matches the AC power available in your location. Also be sure that your monitor and attached devices are electrically rated to operate.

- Be sure that your monitor and attached devices are electrically rated to operate with the power available in your location.
- Use only power cables provided with this product.
- To help prevent electric shock, plug the system and peripheral power cables into properly grounded electrical outlets. These cables are equipped with three-prong plugs to help ensure proper grounding. Do not use adapter plugs or remove the grounding prong from a cable.

- Observe extension cable and power strip ratings. Make sure that the total ampere rating of all products plugged into the power strip does not exceed 80 percent of the ampere ratings limit for the power strip.
- To help protect your system from sudden, transient increases and decreases in electrical power, use a surge suppressor, line conditioner, or uninterruptible power supply (UPS).
- Position system cables and power cables carefully. Route cables so that they cannot be stepped on or tripped over. Be sure that nothing rests on any cables.
- Do not modify power cables or plugs. Consult a licensed electrician or your power company for site modifications. Always follow your local/national wiring rules.

Rack Mounting of Systems

- Refer to the rack installation documentation accompanying the rack for specific caution statements and procedures.
- System rack kits are intended to be installed in a rack by trained service technicians. If a non-Dell rack is utilized, be sure that the rack meets the specifications of a Dell rack.
- Elevated Ambient Temperature: If installed in a closed rack assembly, the operation temperature of the rack environment may be greater than room ambient. Use care not to exceed the rated maximum ambient temperature of the unit.
- Reduced Air Flow: Installation of the equipment in a rack should be such that the amount of airflow required for safe operation of the equipment is not compromised.
- Mechanical Loading: Mounting of the equipment in the rack should be such that a hazardous condition is not achieved due to uneven mechanical loading.
- Circuit Overloading: Consideration should be given to the connection of the equipment to the supply circuit and the effect that overloading of circuits might have on overcurrent protection and supply wiring. Consider equipment nameplate ratings for maximum current.

- **Reliable Earthing:** Reliable earthing of rack mounted equipment should be maintained. Pay particular attention to supply connections other than direct connections to the branch circuit (for example, use of power strips).

LAN Options

- Do not connect or use during a lightning storm. There may be a risk of electrical shock from lightning.
- Never connect or use in a wet environment.

Product Overview

The multiuser, Dell™ 2161DS-2/4161DS/2321DS Remote Console Switch integrates Dell field-proven digital keyboard, video and mouse (KVM) switching technology with advanced cable management, flexible access for up to four simultaneous users, and a patented, next-generation user interface. The Remote Console Switch features user-side USB and PS/2 ports that support major device platforms.

Using powerful on-screen management through the Avocent™ brand OSCAR™ graphical user interface, Remote Console Switch Software, or on-board web interface provides easy system configuration and device selection.

Remote Console Switch Features and Benefits

SIP Intelligent Module

The Remote Console Switch also provides SIP intelligent module capability. The SIP module with CAT 5 design dramatically reduces cable clutter, while providing optimal resolution and video settings. The built-in memory of the SIP module simplifies configuration by assigning and retaining unique device names and Electronic ID (EID) numbers for each attached device. The SIP module is powered directly from the device and provides Keep Alive functionality even if the Remote Console Switch is not powered.

PS/2 and USB SIP modules are available allowing direct KVM connectivity to devices. A USB2 virtual media SIP is also available. Each Remote Console Switch has up to 32 Analog Rack Interface (ARI) ports for connecting SIP modules.

Utilizing the SIP module, you can attach additional switches to expand your Remote Console Switch system. This flexibility allows you to add capacity as your data center grows.

Multiplatform Support

The Dell SIP modules available for use with the Remote Console Switch support PS/2, USB and USB2 device environments. Using the OSCAR[®] interface in conjunction with these modules allows you to switch easily across platforms.

Interoperability with Avocent[®] IQ Module Intelligent Cabling

Avocent IQ module intelligent cable may also be used to connect devices to the Remote Console Switch. PS/2, USB, Sun[®], and serial cabling options are available. For more information, please refer to the appropriate Avocent installer/user guide for your product. Visit avocent.com/manuals for more information.

OSCAR Interface

You can use the Avocent brand OSCAR interface to manage the Remote Console Switch. The OSCAR interface features intuitive menus to configure your switch system and select computers. Devices can be identified by a name, EID, or port number, allowing you to assign unique device names.

On-board Web Interface

The on-board web interface provides similar management functions as the Remote Console Switch Software, but does not require a software server or any installation. The on-board web interface is launched directly from the switch, and any servers connected to the Remote Console Switch are automatically detected. You can use the on-board web interface to configure Remote Console Switches from a web browser. Launch the Viewer from the on-board web interface to establish KVM and virtual media sessions to target devices. The on-board web interface also supports LDAP authentication, which allows permissions for multiple Remote Console Switches to be managed through a single interface.

DSView[®] 3 Management Software Plug-in

The Avocent DSView 3 management software is a secure, web browser-based, centralized enterprise management solution that allows users to remotely access, manage, monitor, and control target devices through managed appliances. A session may be launched to a target device with a single point of access.

You can manage and connect to multi-vendor servers and devices from within the DSView 3 software. Include your Dell Remote Console Switch in the DSView 3 software heterogeneous network environment with the DSView 3 software plug-in. Once a Remote Console Switch is added, you can use the DSView 3 software for fault management, sessions management, firmware upgrades, and more.

Virtual Media

Virtual media allows you to view, move, or copy data located on virtual media to and from any server that is connected to the Remote Console Switch. Manage remote systems more efficiently by allowing operating system installation, operating system recovery, hard drive recovery or duplication, BIOS updating, and server backup.

Virtual media can be connected directly to USB ports on the switch or the server hosting the on-board web interface browser session. You can open a virtual media session to a server from the Viewer. The Viewer can be opened from either the on-board web interface or Remote Console Switch software.



NOTE: To open a virtual media session with a server, the server must first be connected to a Remote Console Switch using a virtual media capable USB2 SIP module.

Security

The OSCAR interface allows you to protect your system with a screen saver password. The screen saver mode engages and access is prohibited until the appropriate password is entered to reactivate the system. By typing **Help** in the password dialog, you are directed to Dell Technical Support.

Recommended usage for the Remote Console Switch is in a datacenter infrastructure protected by a firewall.

Encryption

The Remote Console Switch supports 128-bit SSL, as well as AES, DES, and 3DES encryption of keyboard/mouse, video, and virtual media sessions.

Operation Modes

The OSCAR interface provides convenient operation modes for easy system administration of the Remote Console Switch. These modes (Broadcast, Scan, Switch, and Share) allow you to manage your switching activities. Chapter 3, "Controlling Your System at the Analog Ports" on page 35, explains these modes in detail.

Video

The Remote Console Switch provides optimal resolution for analog VGA, SVGA and XGA video. You can achieve resolutions of 1024 x 768, depending on the length of cable separating your switch and servers.

Table 1-1. Maximum Resolution Refresh Rate Video Type

720 x 400 @ 70 Hz VGA
640 x 480 @ 60 Hz VGA
640 x 480 @ 72 Hz VESA
640 x 480 @ 75 Hz VESA
800 x 500 @ 60 Hz VESA
800 x 600 @ 56 Hz VESA
800 x 600 @ 60 Hz VESA
800 x 600 @ 70 Hz VESA
800 x 600 @ 75 Hz VESA
1024 x 640 @ 60 Hz VESA
1024 x 768 @ 60 Hz VESA
1024 x 768 @ 70 Hz VESA
1024 x 768 @ 75 Hz VESA
1280 x 800 @ 60 Hz VESA

FLASH Upgradeable

Upgrade your Remote Console Switch and SIP modules at any time to ensure you are always running the most current firmware version available. Flash Upgrades can be initiated through the OSCAR interface, on-board web interface, or the Serial Console. The Remote Console Switch can be configured to perform automatic firmware upgrades of SIP modules. See "Appendix D: FLASH Upgrades" on page 211 for more information.

Cascade (Tier) Expansion

The Remote Console Switch features allow you to cascade additional Dell Console Switches from each of the Analog Rack Interface (ARI) ports on the switch. The cascaded switches are attached in the same manner as any device. This additional tier of units allows you to attach up to 512 servers in one system. See "Adding a Cascade Switch" on page 26.

Remote Console Switch Software Features and Benefits



NOTE: For how to use the Remote Console Switch Software, see the Dell Remote Console Switch Software User's Guide or the help included with the software.

The Dell™ Remote Console Switch Software is a cross-platform management application that allows you to view and control the Dell Remote Console Switch and all attached servers. The cross-platform design ensures compatibility with most popular operating systems and hardware platforms. The Remote Console Switch Software provides secure switch-based authentication, data transfers, and username/password storage. Each switch handles authentication and access control individually for more decentralized system control.

The Remote Console Switch Software utilizes Explorer-like navigation with an intuitive split-screen interface, providing you with a single point of access for your entire system. From here, you can manage your existing switches, install a new switch, or launch a video session to a system server. Built-in groupings such as Servers, Sites, and Folders provide an easy way to select the units to view. Powerful search and sort capabilities allow you to easily find any unit.

Easy to Install and Configure

The Remote Console Switch Software is designed for easy installation and operation. Auto-discovery of managed switches enables you to install new units in minutes. Wizard-based installation and online help simplify initial system configuration. The intuitive graphical interface makes managing and updating switches simple and straightforward.

Powerful Customization Capabilities

Tailor the Remote Console Switch Software to fit your specific system needs. Take advantage of built-in groups or create your own. Customize unit and field names, and icons for maximum flexibility and convenience. Using names that are meaningful to you makes it easy to quickly find any system unit.

Extensive Remote Console Switch Management

The Remote Console Switch Software allows you to add and manage multiple switches in one system. Once a new switch is installed, you can configure switch parameters, control and preempt user video sessions, and execute numerous control functions, such as rebooting and upgrading your switch. The Remote Console Switch Software is designed to be compatible with the Dell OpenManage™ IT Assistant Event Viewer, allowing system administrators to consolidate system event reports.

IPv4 and IPv6 Capabilities

The Remote Console Switch is compatible with systems using either of the currently used Internet Protocol Versions, IPv4 and IPv6. You can change the network settings and choose either IPv4 or IPv6 mode via the serial port, OSCAR interface, or on-board web interface.

LDAP

The Dell Remote Console Switch Software allows permissions for multiple Remote Console Switches to be managed through a single interface rather than individually on each Remote Console Switch. For increased security and efficiency, the LDAP feature eliminates the need to update access permissions in individual Remote Console Switches by drawing permissions from a single network-wide authentication source.

The Dell Remote Console Switches can authenticate using the standard Active Directory schema, or the Dell Extended Schema in order to maximize compatibility with all of your Dell hardware.

Interoperability with Avocent Products

The Remote Console Switch Software can also be used to manage some Avocent brand switches allowing increased flexibility in the management of systems.

In addition, the Remote Console Switch Software includes support for Avocent brand IQ Modules, expanding the range of server types that can be managed. The addition of support for Avocent brand IQ modules means that the following connections are now supported:

- PS/2 modules (Dell and Avocent modules available)
- USB modules (Dell and Avocent modules available)
- Serial modules (Avocent modules available)
- Sun modules (Avocent modules available)
- PS2M modules (Avocent modules available)



NOTE: Dell SIPs are not supported on directly connected Avocent brand switches.

Installation

The Remote Console Switch system includes the Remote Console Switch, the Remote Console Switch Software, and the on-board web interface. You may choose to use either the Remote Console Switch Software or the on-board web interface to manage your system. The on-board web interface manages a single Remote Console Switch and its connections, while the Remote Console Switch Software can manage multiple switches and their connections.

If you plan to use the on-board web interface, you do not need to install the Remote Console Switch Software. If you have previously used the Remote Console Switch Software, you can migrate the database to the on-board web interface. See "Migrating Remote Console Switches to the On-board Web Interface" on page 135.



NOTE: Please ensure that all your Remote Console Switches have been upgraded to their most recent version of firmware. For information on upgrading a Remote Console Switch through the on-board web interface, please see "Upgrading Firmware" on page 120.

Remote Console Switch Quick Setup Checklist

To set up the Remote Console Switch (see the "Remote Console Switch Installation and Setup" on page 10):

- 1 Adjust mouse acceleration on each server to **Slow** or **None**.
- 2 Install the Remote Console Switch hardware, and connect a Server Interface Pod (SIP) or an Avocent brand IQ module to each server or tiered switch. Connect each SIP or IQ module to the Remote Console Switch with CAT 5 cabling and connect the keyboard, monitor, and mouse connectors to the Analog Port of the Remote Console Switch.
- 3 Connect a terminal to the configuration (serial) port on the back panel of the Remote Console Switch and set up network configuration (set network speed and address type). The IP address can be set here or from the Remote Console Switch Software. Dell recommends using a static IP address for ease of configuration.

- 4 Using the local port configuration, input all server names via the OSCAR interface.

To set up the Remote Console Switch Software, see the Dell Remote Console Switch Software User's Guide or the help included with the software.

Remote Console Switch Installation and Setup

The Remote Console Switch system uses Ethernet networking infrastructure and TCP/IP protocol to transmit keyboard, video, and mouse information between operators and connected computers. Although 10BaseT Ethernet or Gigabit may be used, Dell recommends a dedicated, switched 100BaseT network.

Getting Started

Before installing your Remote Console Switch, refer to the list below to ensure you have all items that shipped with the Remote Console Switch, as well as other items necessary for proper installation.

Supplied with the Remote Console Switch:

- Remote Console Switch unit
- Local country power cord
- 0U mounting bracket
- 1U mounting bracket
- 1U mounting bracket hardware kit
- Serial cable
- Cat5 cable
- Remote Console Switch System User's Guide on CD
- Installation Instructions
- Safety booklet
- Regulatory booklet

Additional items needed:

- One Dell SIP or IQ module per attached device
- One CAT 5 patch cable per attached device (up to 30 meters)

Optional items:

- Front Access Panel
- Port Expansion Module (PEM)



NOTE: A virtual media session cannot be opened to a server that is connected to a PEM.

Setting Up Your Network

The Remote Console Switch system uses IP addresses to uniquely identify the Remote Console Switch units and the computers running Remote Console Switch Software. The Remote Console Switch supports DHCP and static IP addressing. (If you are connecting your remote software to the previous 2161DS, you will need to use BootP instead of DHCP).



NOTE: For how to use the Remote Console Switch Software, see the Dell Remote Console Switch Software User's Guide or the help included with the software.

Keyboards

USB or PS/2 type keyboards may be connected to the Analog Port of the Remote Console Switch.



NOTE: The Remote Console Switch also supports the use of multiple keyboards and multiple mice on the Analog Port. The use of more than one input device simultaneously, however, may produce unpredictable results.

Rack Mounting Your Remote Console Switch Unit

Obtain a Switch Mounting Bracket Kit (0U or 1U) to rack-mount your Remote Console Switch unit. Before installing the Remote Console Switch and other components in the rack, stabilize the rack in a permanent location. Start rack mounting your equipment at the bottom of the rack, then work to the top. Avoid uneven loading or overloading of racks.

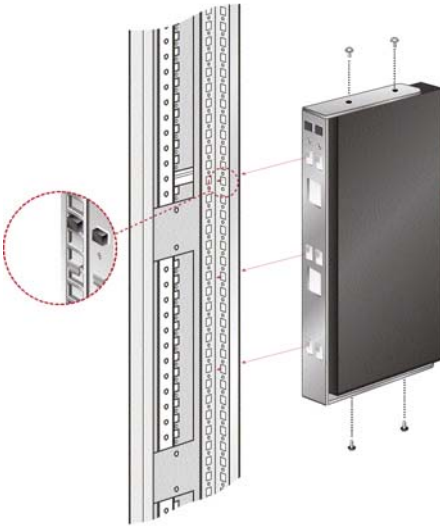


CAUTION: Before installing systems in a rack, install front and side stabilizers on stand-alone racks or the front stabilizer on racks joined to other racks. Failure to install stabilizers accordingly before installing systems in a rack could cause the rack to tip over, potentially resulting in bodily injury under certain circumstances. Therefore, always install the stabilizer(s) before installing components in the rack.

To install the 0U switch mounting bracket (shipped as default):


- 1 Line up the holes of the mounting brackets with the screw holes in the switch.
- 2 Fasten the mounting bracket to the switch using the button head socket cap screws on each side.
- 3 Mount the switch assembly to the rack by inserting the three mounting hooks on one side of the bracket into square holes in the vertical rack.
- 4 Press down until the blue push button pops out and clicks.

Figure 2-1. OU Mounting Bracket Installation



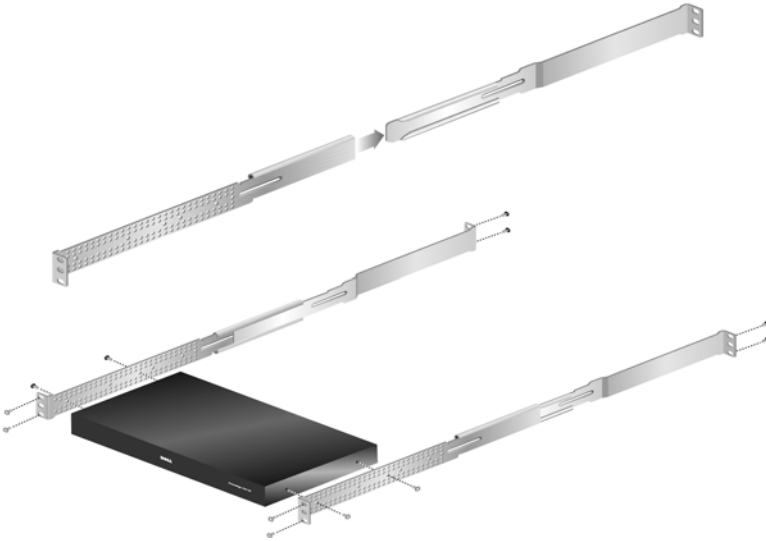
To install the 2161DS-2/4161DS Remote Console Switch 1U four point switch mounting bracket:

- 1 Remove the screws on each side of the 1U four-point switch and set them aside to attach to the front 1U bracket pieces later.
- 2 Line up the vent holes in the “long side” of the kit’s front brackets with the vent holes in the switch.

 **NOTE:** The switch vent holes must not be covered by the bracket, which will occur if installed on the wrong side of the switch.

- 3** Line up the screw holes in the bracket with the screw holes in the switch.
- 4** With a Phillips screwdriver, fasten the front mounting brackets to the switch using two screws on each side.
- 5** Attach four cage nuts or clip nuts to the rack mounting flange of the rack cabinet's front so that the nut is positioned on the inside of the rack.
- 6** Mount the switch assembly to the rack cabinet by matching the holes in the "short side" of each bracket to an appropriate set of matching holes on your rack cabinet. Next, insert the combination hex head screws through the slots in the bracket, then the holes in the mounting rail, and then into the cage nuts or clip nuts.
- 7** Attach four cage nuts or clip nuts to the rack mounting flange of the rack cabinet back so that the nut is positioned on the inside of the rack.
- 8** Slide the rear brackets into the channel of the front brackets adjusting them to fit the rack depth.
- 9** Mount the rear bracket to the rack cabinet by matching the holes in the "short side" of each bracket to an appropriate set of matching holes on your rack cabinet, ensuring the switch is level within the rack.
- 10** Insert the combination hex head screws through the slots in the bracket and the holes in the mounting rail, then into the cage nuts or clip nuts.

Figure 2-2. 2161DS-2/4161DS Remote Console Switch 1U Mounting Bracket Installation



To install the 2321DS Remote Console Switch mounting bracket:

- 1 Remove the three truss head screws from the right side of the switch chassis, and position and attach the right mounting bracket to the right side of the switch chassis with three of the flat head screws provided.

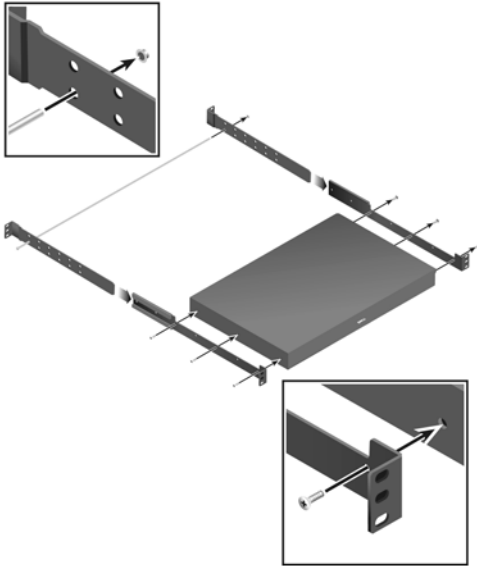


NOTE: The switch vent holes must not be covered by the bracket, which will occur if installed on the wrong side of the switch.

- 2 Repeat the procedure for the left side of the switch chassis.
- 3 Install a push nut to one end of the cable support rod. Position the extensions with their slotted mounting flanges facing in opposing directions.
- 4 Select a position hole on the lower side of the slide extensions. Slide the support rod through the selected hole and the hole on the opposite extension.
- 5 Install the remaining push nut on the other end of the cable support rod.
- 6 Slide the extension assembly into the switch chassis/bracket assembly as shown in the illustration. Be sure to orient the extension assembly so that the cable support rod is in the lower row of extension holes.

- 7 Place the complete switch chassis/bracket assembly into a level rack position and install the appropriate hardware into each of the four bracket corners (hardware not provided).

Figure 2-3. 2321DS Remote Console Switch Mounting Bracket Installation



Installing the Remote Console Switch Unit

The diagram below illustrates one possible configuration for your Remote Console Switch appliance. Follow the detailed set of procedures following Figure 2-4 to successfully install your Remote Console Switch unit.

Figure 2-4. Basic Remote Console Switch Configuration

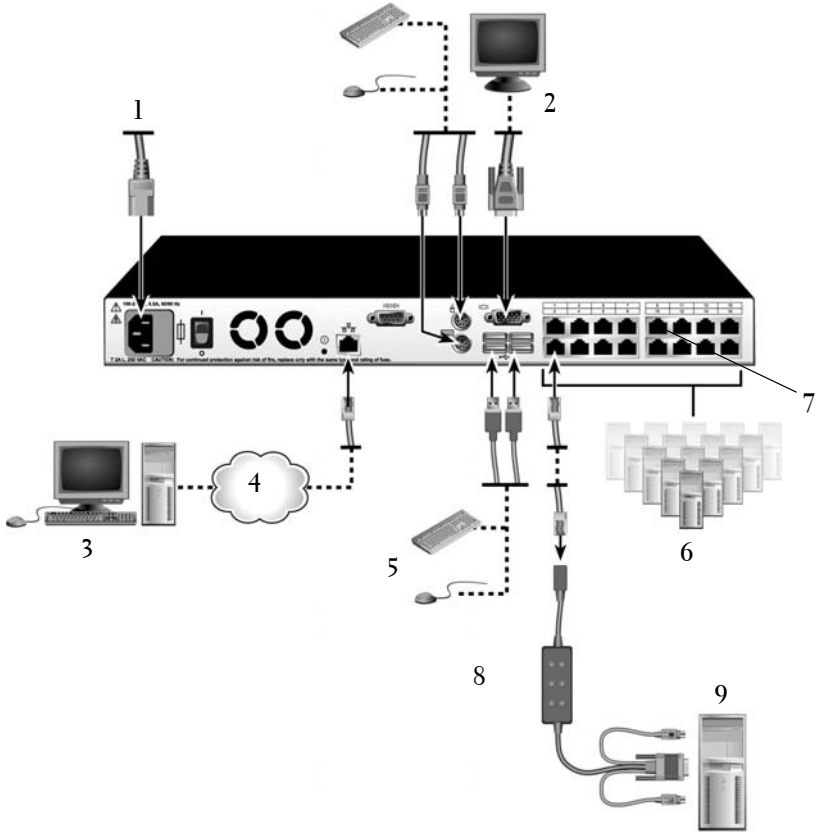


Table 2-1. Basic Remote Console Switch Configuration Descriptions

Number	Description	Number	Description
1	Power Cord	6	Servers 2-16
2	Analog User	7	ARI Port
3	Digital User	8	SIP or IQ Module
4	Network	9	Server 1
5	USB Devices		



CAUTION: To reduce the risk of electric shock or damage to your equipment, do not disable the power cord grounding plug. The grounding plug is an important safety feature. Plug the power cord into a grounded (earthed) outlet that is easily accessible at all times. Disconnect the power from the unit by unplugging the power cord from either the electrical outlet or the unit.



NOTE: If the building has 3-phase AV power, ensure that the computer and monitor are on the same phase to avoid potential phase-related video and/or keyboard problems.



NOTE: The maximum supported cable length from switch to device is 30 meters.

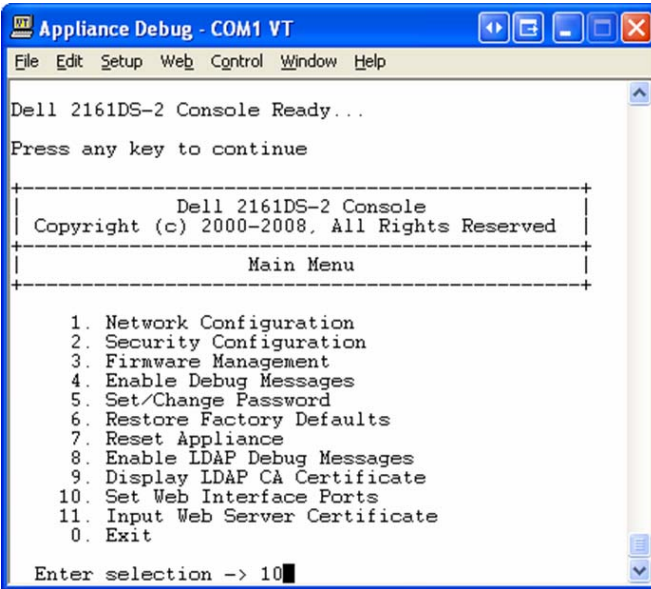
To install the Remote Console Switch hardware:



NOTE: The default username is “Admin.” There is no default password.

- 1** Connect a terminal or PC running the terminal emulation software to the configuration port on the back panel of the Remote Console Switch using the supplied serial cable. The terminal should be set to 9600 baud, 8 bits, 1 stop bit, no parity, and no flow control.
- 2** Plug the supplied power cord into the back of the Remote Console Switch unit and then into an appropriate power source.
- 3** When the power is switched on, the Power indicator on the rear of the unit will blink for 30 seconds while performing a self-test. Press the <Enter> key to access the main menu.

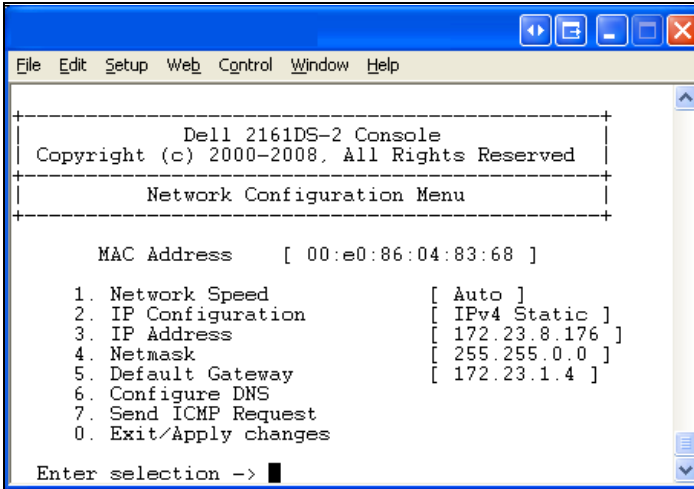
Figure 2-5. Main Menu




To configure the Remote Console Switch hardware:

- 1 You will see the Main menu with eleven options. Select option 1, Network Configuration.

Figure 2-6. Network Configuration Menu

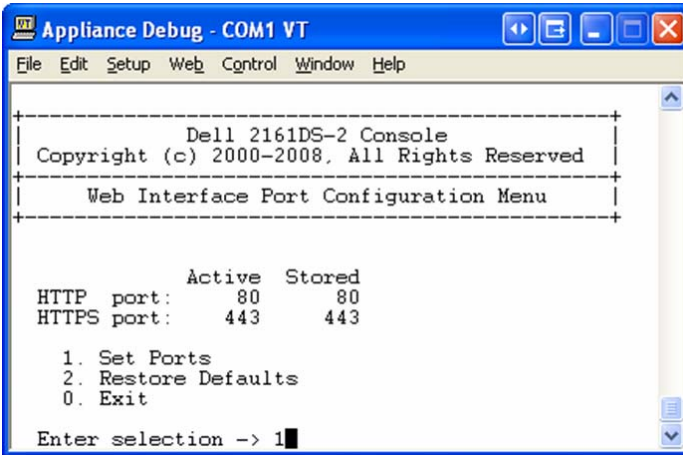


- 2** Select option 1 to set your network speed. Once you enter your selection, you will be returned to the **Network Configuration** menu.
 - 3** Select option 2 to open the **IP Configuration** menu.
 - 4** Type the appropriate number to select one of the following types of IP addresses: 1: **None**, 2: **IPv4 Static**, 3: **IPv4 Dynamic**, 4: **IPv6 Static**, or 5: **IPv6 Dynamic**.
Dell recommends using a static IP address for ease of configuration.
 - 5** Select options 3-5 from the **Terminal Applications** menu, in turn, to finish configuring your Remote Console Switch for IP address, Netmask, and Default Gateway.
 - 6** Once this is completed, type **Ø** to return to the main menu.
-  **NOTE:** Network configuration can also be performed. See "Controlling Your System at the Analog Ports" on page 35.

To configure the HTTP and HTTPS ports:

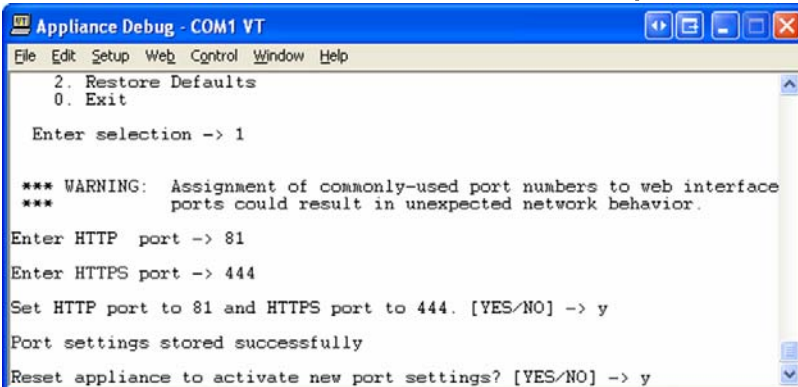
- 1** You will see the **Main** menu with eleven options. Select option 10, **Set Web Interface Ports** to open the **Web Interface Port Configuration Menu**.

Figure 2-7. Web Interface Port Configuration Menu




- 2 Select option 1 to set the port numbers. Type the port numbers you wish to use for the HTTP port and the HTTPS port.

Figure 2-8. Web Interface Port Configuration Menu - Set Ports Option



- 3 If the values are correct for your network, type <Y> and press the <Enter> key.

 **NOTE:** You will need to reboot the Remote Console Switch to use these port numbers.

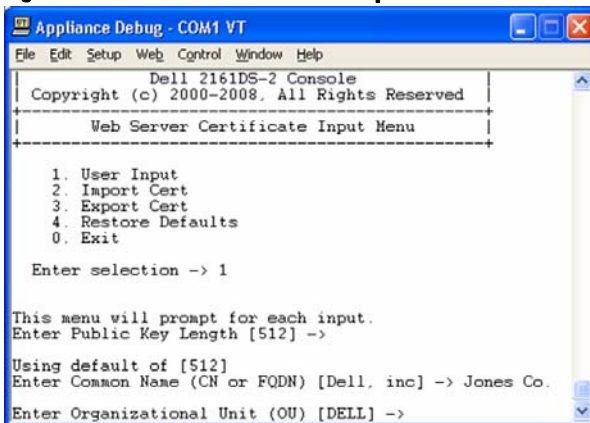


NOTE: If you change the port numbers in the Remote Console Switch, you will also need to change them in the Remote Console Switch Software (see "Switch Network Properties" in the Dell Remote Console Switch Software User's Guide or the help included with the software) or the web interface (see "Launching the On-board Web Interface" on page 32).

To input and install a web certificate:

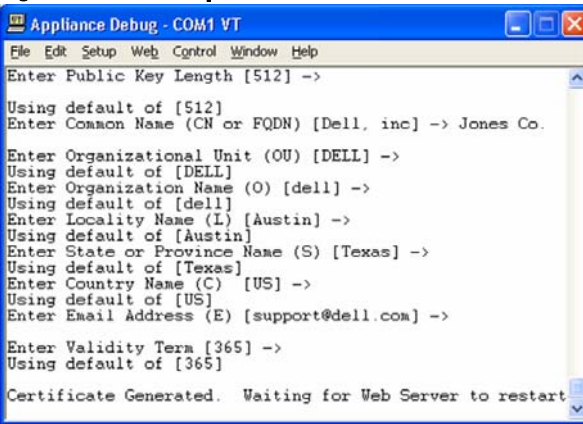
- 1 You will see the **Main** menu with eleven options. Select option 11, **Input Web Server Certificate**, to open the **Input Web Server Certificate Menu**.

Figure 2-9. Web Server Certificate Input Menu



- 2 Select option 1, **User Input**.

Figure 2-10. User Input Menu



- 3** Either press the <Enter> key to accept the default options, or enter the appropriate text in the following fields:
 - a** **Public Key Length:** the number of bits you want the certificate to be.
 - b** **Common Name:** your name. (Since this is your root certificate, use an appropriate name such as, "Company_Name Certificate Authority.")
 - c** **Organizational Unit (optional):** organization unit name (marketing, for example)..
 - d** **Organization Name:** the exact legal unabbreviated name of your organization.
 - e** **Locality Name:** the city where your organization is located.
 - f** **State or Province Name:** the unabbreviated state or province where your organization is located.
 - g** **Country Name:** the two-letter ISO abbreviation for your country.
 - h** **Email Address:** the email address for the CA to contact.
 - i** **Validity Term:** number of days the certificate is valid.
- 4** Press the <Enter> key. Wait for the Web Server to restart before continuing.

To import and install a web certificate:

- 1 You will see the **Main** menu with eleven options. Select option 11, **Input Web Server Certificate**, to open the **Input Web Server Certificate Menu**.
- 2 Select option 2, **Import Cert.** Then download a company certificate file (*.pem). Wait for the Web Server to restart before continuing.

To export a web certificate:

- 1 You will see the **Main** menu with eleven options. Select option 11, **Input Web Server Certificate**, to open the **Input Web Server Certificate Menu**.
- 2 Select option 3, **Export Cert.** to output the current certificate to the serial console. The format must be similar to the following text:

```
"-----BEGIN CERTIFICATE-----
MIIDJzCCApCgAwIBAgIBADANBgkqhkiG9w0BAQQFADBxMQswC
QYDVQQGEwJVUzEQ
..... Text removed from example
.....
3omoTQuBURERxg3vrwEzLqCUanQmw5BQJAVC6LT/DP7DNz/xi
pZoI+ZyaTgQEdR0
R0x0yYSaYETpMY53NMAVlCxETVkvkI2F/f+1sn+9Ik7GWBuPp
LbTmYfMoQ==
-----END CERTIFICATE-----
-----BEGIN RSA PRIVATE KEY-----
MIICXAIBAABKgQDI6KTAqoPfZhK7Wdd+Dzx03IVQlBqp+Vslt
n34YMDdpJ8mfqND
..... Text removed from example
.....
b6KA7Vfi jVhIt3lKcYsCQEhOjqh07hI50LmSHt3l1krGZTX+A
Cy1dlceZRkJDkyA
HqTleb5fx/i1Hu5ex99qQP9FSOP5fVsmVSRDkk2ites=
-----END RSA PRIVATE KEY-----"
```

To return to the factory defaults:

- 1 You will see the **Main** menu with eleven options. Select option 11, **Input Web Server Certificate**, to open the **Input Web Server Certificate Menu**.
- 2 Select option 4, **Restore Defaults**, to replace the current certificate with the factory defaults.

Video Optimization

To ensure optimal video quality, configure the Remote Console Switch with the same settings as the network switch. For example, if the Remote Console Switch is set to **Auto-Negotiate**, then the network switch must be set to **Auto-Negotiate** in both speed and duplex. For example, if the Remote Console Switch is set to 100MB - full duplex, then the network switch must be set to 100MB - full duplex.

Once you have made these changes, you may need to refresh/flush the Address Resolution Protocol (ARP) tables in the network before you establish a new connection with the Remote Console Switch, especially if the Remote Console Switch has been in use within the hour preceding these changes.

To refresh the ARP table, do one of the following:

Wait approximately 10 minutes for the ARP tables to rebuild automatically.

-or-

Clear the ARP table entry in a video session viewer workstation and ping the appliance at its IP address. This can be done from a DOS window.

- a** Type `ARP -d 1.2.3.4`
(where 1.2.3.4 is the IP address of the Remote Console Switch).
- b** Type `PING 1.2.3.4`

If the PING is successful, the Remote Console Switch is ready for operation.

Mouse Acceleration



NOTE: Dell highly recommends that all Microsoft® Windows® systems attached to the Remote Console Switch use the default Windows® PS/2 or USB mouse driver.

If you are experiencing slow mouse response during a remote video session, deactivate mouse acceleration in the operating system of the target device and set mouse speed to 50%.

Connecting a SIP

To connect a SIP to each server:

- 1** Locate the SIPs for your Remote Console Switch unit.
- 2** If you are using a PS/2 SIP connection, attach the SIP's color-coded ends to the appropriate keyboard, monitor, and mouse ports on the first server you will be connecting to this Remote Console Switch. If you are using a

USB connection, attach the SIP's plug to the USB port on the first server you will be connecting to this Remote Console Switch unit (Figure 2-11).

- 3** To the RJ-45 connector on the SIP, attach one end of the CAT 5 cabling that will run from your SIP to the Remote Console Switch unit (Figure 2-11).
- 4** Connect the other end of the CAT 5 cable to the desired ARI port on the back of your Remote Console Switch unit.
- 5** Repeat steps 2-4 for all servers you wish to attach.



NOTE: Power down the Remote Console Switch unit before servicing. Always disconnect the power cord from the wall outlet.



NOTE: In addition to Dell SIPs, the Remote Console Switch may also be connected to devices using IQ modules, including Sun and Serial IQ modules.

Figure 2-11. Connecting a SIP

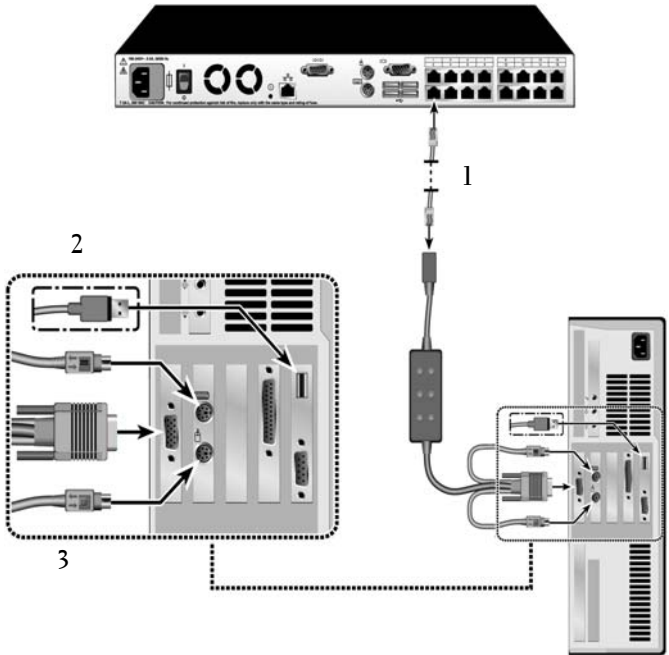


Table 2-2. Connecting a SIP Descriptions

Number	Description
1	CAT 5
2	USB Connection
3	PS/2 Connection

Adding a Cascade Switch

To add a cascade switch (optional):



NOTE: The Remote Console Switch does not support the EL80-DT.

- 1 Mount the switch into your rack. Locate a CAT 5 cable to connect your Remote Console Switch unit to the cascade switch (Figure 2-13).

- 2** Attach one end of the CAT 5 cabling to the ARI port on the Console Switch.
- 3** Connect the other end of the CAT 5 cable to the ACI port on the back of your cascade switch.
- 4** Connect the devices to your cascaded switch according to the switch manufacturer's recommendations.
- 5** Repeat steps 1-4 for all the cascade switches you wish to attach to your Remote Console Switch system.

Figure 2-12. Remote Console Switch With a Cat 5 Analog Switch

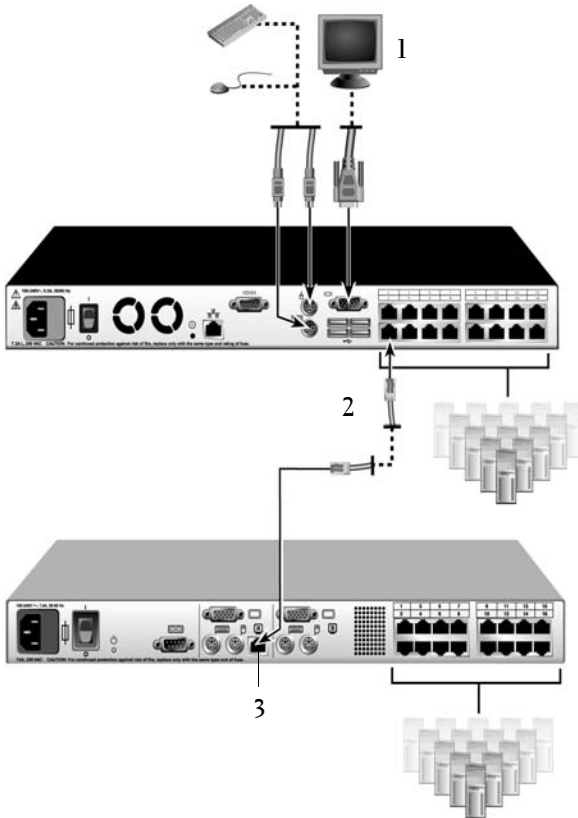


Table 2-3. Remote Console Switch With a Cat 5 Analog Switch Descriptions

Number	Description
1	Local User
2	CAT 5
3	ACI Port

NOTE: The Remote Console Switch supports only 1 switch per ARI port. You cannot cascade another switch under this first switch.



NOTE: When cascading with a Remote Console Switch, an 8-port or 16-port analog console switch is not supported as the primary unit in a cascaded configuration. The Remote Console Switch must be the primary unit.

Cascading with Legacy Switches

To add a legacy switch (optional):

- 1 Mount the switch into your rack. Locate a CAT 5 cable to connect your Remote Console Switch unit to the legacy switch (Figure 2-13).
- 2 Attach one end of the CAT 5 cabling to the ARI port on the Console Switch.
- 3 Connect the other end of the CAT 5 cable to a Dell SIP or IQ module.
- 4 Connect the SIP or IQ module to your legacy switch according to the switch manufacturer's recommendations.
- 5 Repeat steps 1-4 for all the legacy switches you wish to attach to your Remote Console Switch system.

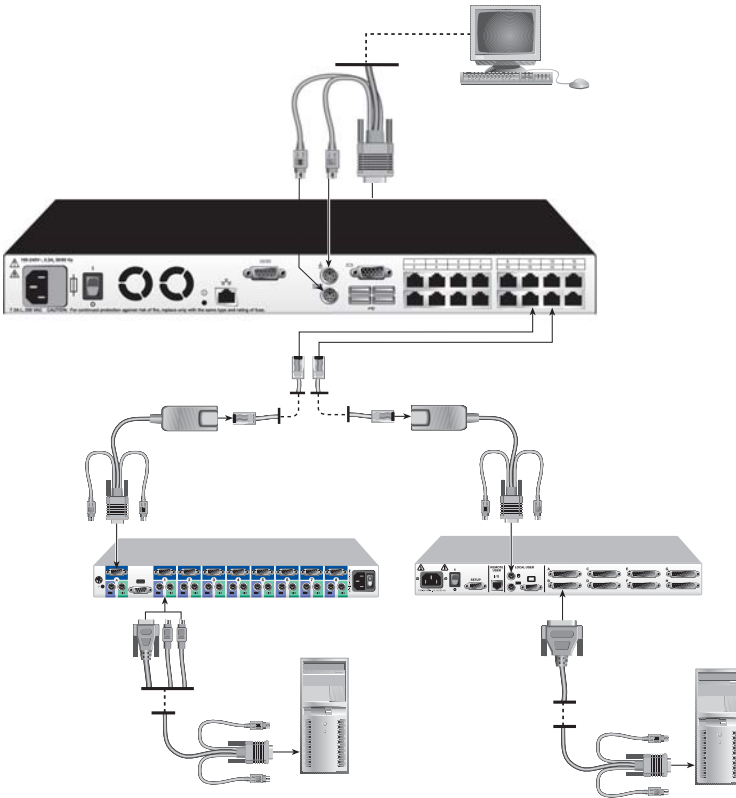


NOTE: The Remote Console Switch supports only 1 switch per ARI port. You cannot cascade another switch under this first switch.



NOTE: When cascading with a Remote Console Switch, an 8-port or 16-port analog console switch is not supported as the primary unit. The Remote Console Switch must be the primary unit.

Figure 2-13. Remote Console Switch Cascading Configuration With Legacy Console Switches



Adding a PEM (Optional)

A Port Expansion Module (PEM) allows you to expand each ARI port to accommodate up to eight devices instead of one.

NOTE: The PEM operates passively. Therefore, once a user accesses a device attached to a PEM, any subsequent users attempting to access any of the devices attached to that PEM will be blocked.

NOTE: A virtual media session cannot be opened to a server that is connected to a PEM.

To add a PEM (optional):

- 1 Mount the PEM into your rack. Using up to nine CAT 5 cables, one connects your Remote Console Switch unit to the PEM, and the other eight connect the PEM to the SIP attached to each device.
- 2 Attach one end of the CAT 5 cabling that will run between your PEM and the Remote Console Switch unit to the RJ-45 connector slightly separated from the other connectors on the PEM. Connect the remaining end of the CAT 5 cable to the desired ARI port on the back of your Remote Console Switch unit.
- 3 To one of the eight RJ-45 connectors grouped on the back of the PEM, attach the CAT 5 cabling that will run between your PEM and each device's SIP.
- 4 Connect the other end of the CAT 5 cable to the first of the SIPs.
- 5 Repeat steps 3-4 for all devices you wish to attach.

Figure 2-14. Remote Console Switch Configuration With a PEM

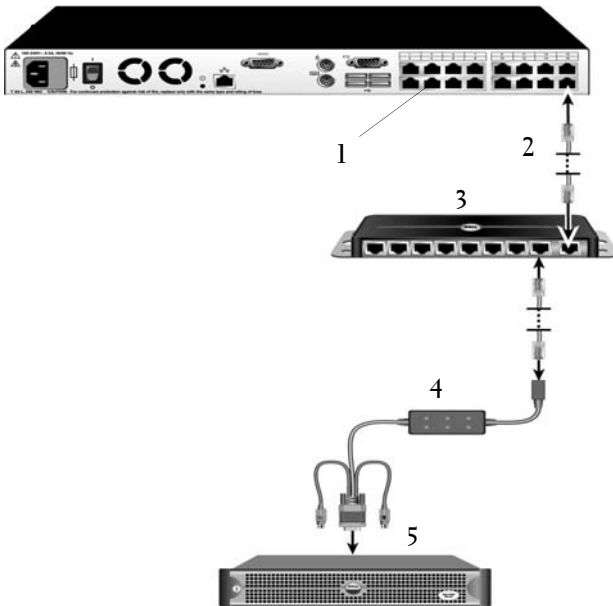



Table 2-4. Remote Console Switch Configuration With a PEM Descriptions

Number	Description
1	ARI Port
2	CAT 5e
3	PEM
4	SIP or IQ Module
5	Server

Connecting to the Network

To connect the network and power up your Remote Console Switch:

- 1 Connect your network cable to the LAN port on the rear of the Remote Console Switch to your network.
-  **NOTE:** If you are using a 2321DS Remote Console Switch, you will have two redundant LAN ports. If the first LAN port fails, the second one will take over.
- 2 Power up all attached systems in any order.
- 3 Attach your monitor and keyboard and mouse cable connectors to the appropriate ports on the back of your Remote Console Switch unit.

On-board Web Interface Installation and Setup

Once you have installed a new Remote Console Switch, you can use the on-board web interface to configure unit parameters and launch video sessions.

Supported Browsers


The on-board web interface supports the following browsers:

- Microsoft Internet Explorer® version 6.x SP1 or later
- Firefox version 2.0 or later

Launching the On-board Web Interface


To launch the on-board web interface:


- 1 Open a web browser and type the IP address of the Remote Console Switch. You can set the IP address of the switch using the OSCAR interface or the serial port; see "Controlling Your System at the Analog Ports" on page 35 for more information.


 **NOTE:** If you changed the default HTTP/HTTPS ports in the serial console and are using an IPv4 address, use this IP address format: "https://<ipaddress>:<port#>", where "*port#*" is the number you changed the port number to in the serial console. If you are using an IPv6 address, use this format: "https://[<ipaddress>]:<port#>", where "*port#*" is the number you changed the port number to in the serial console. If you are using an IPv6 address, you must enclose the address in square brackets.

- 2 The login window opens. Type your username and password and click **OK**.

- 3 The on-board web interface opens and displays the **Connections** tab.

 **NOTE:** The Remote Console Switch will attempt to detect if Java is already installed on your PC. If it is not, in order to use the on-board web interface, you will need to install it. You may also need to associate the JNLP file with Java WebStart.

 **NOTE:** Using the on-board web interface requires using Java Runtime Environment (JRE) version 1.6.0_2 or higher.

 **NOTE:** Once you have logged in to the on-board web interface, you will not have to log in again when launching new sessions unless you have logged out or your session has exceeded the inactivity timeout specified by the administrator.

Controlling Your System at the Analog Ports

The Remote Console Switch features user-side keyboard and mouse ports that allow you to connect a USB or PS/2 keyboard and mouse for direct analog access. The Remote Console Switch uses the powerful OSCAR interface, which uses intuitive menus to configure your system and select computers.

Viewing and Selecting Ports and Devices

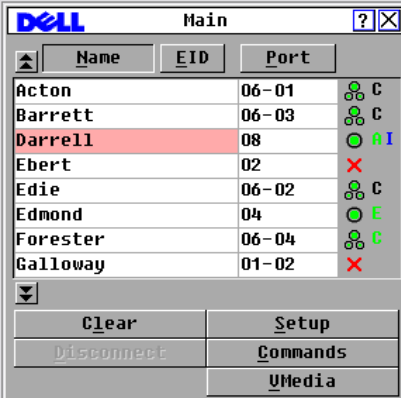
Use the OSCAR interface Main dialog box to view, configure, and control devices in the Remote Console Switch system. View your devices by name, port, or by the unique Electronic ID number (EID) embedded in each SIP module.


The Port column indicates the ARI port to which a device is connected. If you cascade a switch from the main Remote Console Switch, creating another tier, the port numbering displays the ARI port first, then the switch port to which the device is connected. For example, in Figure 3-1, devices 06-01, 06-02, 06-03, and 06-04 are connected to switches. The port numbering displays the ARI port first, then the switch port to which the device is connected. If you cascade a switch from a Port Expansion Module (PEM), you will also see multiple devices that show up on a single port.

To access the Main dialog box:

Press <Print Screen> to launch the OSCAR interface. The **Main** dialog box displays.

Figure 3-1. Example of a Main Dialog Box



 NOTE: You can also press the <Control>, <Alt>, or <Shift> keys twice within one second to launch the OSCAR interface. You can use this key sequence in any place you see <Print Screen> throughout this chapter.

Viewing the Status of Your Switch

The status of the devices in your system is indicated in the right columns of the Main dialog box. Table 3-1 describes the status symbols.

Table 3-1. OSCAR Interface Status Symbols







Symbol	Description
	SIP is online.
	SIP is offline or is not operating properly.
	Connected switch is online.
	Connected switch is offline or is not operating properly.
	SIP is unavailable.
	(green letter) Indicates which user channel is currently connected to a SIP.

Table 3-1. OSCAR Interface Status Symbols

Symbol	Description
A	(black letter) Indicates a blocked path. For instance, in Figure 3-1, user C is viewing Forester, but is blocking access to Acton, Barrett, and Edie, which are connected to the same ARI port.
I	(blue letter) Indicates a virtual media connection.

Selecting Devices

Use the **Main** dialog box to select devices. When you select a device, the appliance reconfigures the keyboard and mouse to the proper settings for that device.

To select devices:

Double-click the device name, EID, or port number.

-or-

If the display order of your device list is by port (**Port** button is depressed), type the port number and press <Enter>.

-or-

If the display order of your device list is by name or EID number (**Name** or **EID** button is depressed), type the first few characters of the name of the device or the EID number to establish it as unique and press <Enter>.



NOTE: You can connect to the selected device by pressing <Enter>.

To select the previous device:

Press <Print Screen> and then <Backspace>. This key combination toggles between the previous and current connections.

To disconnect the user from a device:

Press <Print Screen> and then <Alt+0> or click **Disconnect** in the OSCAR interface. This leaves the user in a free state, with no device selected. The status flag on your desktop displays **Free**.

Soft Switching

Soft switching is the ability to switch devices using a hot key sequence. You can soft switch to a device by pressing <Print Screen> and then typing the

first few characters of its name or number. If you have set a Screen Delay Time and you press the key sequences before that time has elapsed, the OSCAR interface will not display.

To set a screen delay time:

- 1 Press <Print Screen> to launch the OSCAR interface. The **Main** dialog box appears.
- 2 Click **Setup - Menu**. The **Menu** dialog box displays.
- 3 For **Screen Delay Time**, type the number of seconds of delay desired before the **Main** dialog box is displayed after you press <Print Screen>.
- 4 Click **OK**.

To soft switch to a device:

- 1 To select a device, press <Print Screen>. If the display order of your device list is by port (**Port** button is depressed), type the port number and press <Enter>.
-or-
If the display order of your device list is by name or EID number (**Name** or **EID** button is depressed), type the first few characters of the name of the device or the EID number to establish it as unique and press <Enter>.
- 2 To switch back to the previous device, press <Print Screen> then <Backspace>.

Navigating the OSCAR Interface

Table 3-2 describes how to navigate the OSCAR interface using the keyboard and mouse.



NOTE: You can also press the <Control>, <Alt>, or <Shift> keys twice within one second to launch the OSCAR interface. You can use this key sequence in any place you see <Print Screen> throughout this chapter.

Table 3-2. OSCAR Interface Navigation Basics

This Keystroke	Does This
<Print Screen>, Ctrl-Ctrl, Shift-Shift and/or Alt-Alt	The OSCAR interface activation sequence. By default, <Print Screen> and Ctrl-Ctrl are set as the OSCAR interface activation options. Shift-Shift and Alt-Alt must be set within OSCAR interface before use.
<Print Screen>	Press <Print Screen> twice to send the <Print Screen> keystroke to the currently selected device.
F1	Opens the Help screen for the current dialog box.
Escape	Closes the current dialog box without saving changes and returns to the previous one. In the Main dialog box, it closes the OSCAR interface and returns to the status flag. In a message box, it closes the pop-up box and returns to the current dialog box.
Alt+Hotkey	Opens dialog boxes, selects or checks options, and executes actions when used with underlined letters.
Alt+X	Closes the current dialog box and returns to the previous one.
Alt+O	Selects the OK button, then returns to the previous dialog box.
Click, Enter	In a text box, selects the text for editing and enables the left-and-right-arrow keys to move the cursor. Press <Enter> to select the entire field contents.
Enter	Completes a switch in the Main dialog box and exits the OSCAR interface.
<Print Screen>, Backspace	Toggles back to previous selection.
<Print Screen>, Alt+0	Immediately disengages a user from a server; no server is selected. Status flag displays Free . (This only applies to the 0 on the keyboard and not the keypad.)
<Print Screen>, Pause	Immediately turns on screen saver mode and prevents access to that specific console, if it is password protected.
Up/Down Arrows	Moves the cursor from line to line in lists.
Right/Left Arrows	Moves the cursor within the column when editing a text box.

Table 3-2. OSCAR Interface Navigation Basics (continued)

This Keystroke	Does This
Page Up/Page Down	Pages up and down through Name and Port lists and Help pages.
Home/End	Moves the cursor to the top or bottom of a list.
Delete	Deletes current selection in the scan list or characters in a text box.
Numbers	Type from the keyboard or keypad.

Configuring OSCAR Interface Menus

You can configure your Remote Console Switch from the **Setup** menu within the OSCAR interface. Select the **Names** button when initially setting up your appliance to identify devices by unique names. Select the other setup features to manage routine tasks for your devices from the OSCAR interface menu. See Table 3-3.

Table 3-3. Setup Features to Manage Routine Tasks for Your devices

Feature	Purpose
Menu	Change the device listing between numerically by port or EID number and alphabetically by name. Change the Screen Delay Time before the OSCAR interface displays after pressing <Print Screen>.
Security	Set passwords to restrict device access. Enable the screen saver.
Flag	Change display, timing, color, or location of the status flag.
Language	Choose the language display.
Devices	Identify the appropriate number of ports on an attached cascaded switch.
Names	Identify devices by unique names.
Keyboard	Choose your keyboard country code.
Broadcast	Set up to simultaneously control multiple devices through keyboard and mouse actions.

Table 3-3. Setup Features to Manage Routine Tasks for Your devices (continued)

Feature	Purpose
Scan	Set up a custom scan pattern for up to 100 devices.
Switch	Choose the switch mode and the share mode time-out.
Network	Choose your network speed, transmission mode, and configuration.
VMedia	Set the behavior of the appliance during a virtual media session.
PDU's (For 2321DS Remote Console Switch only.)	View which PDUs are connected to your system.

To access the Setup menu:

- 1 Press <Print Screen> to launch the OSCAR interface. The **Main** dialog box appears.
- 2 Click **Setup**. The **Setup** dialog box displays.

Figure 3-2. Setup Dialog Box



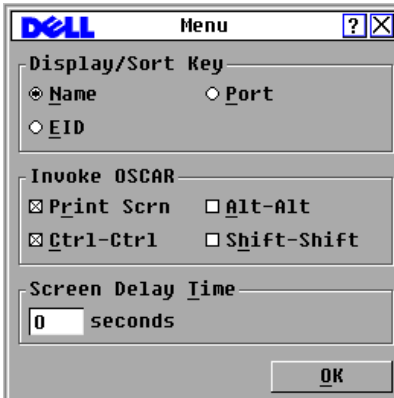
Changing the Display Behavior

Use the **Menu** dialog box to change the display order of devices, set a **Screen Delay Time** for the OSCAR interface, and change the OSCAR interface launch sequence. The display order setting alters how devices display in several screens including the **Main**, **Devices**, and **Broadcast** dialog boxes.

To access the Menu dialog box:

- 1 Click **Setup - Menu** in the **Main** dialog box. The **Menu** dialog box displays.

Figure 3-3. Menu Dialog Box



- 2 <Print Screen>, Ctrl-Ctrl, Alt-Alt, and Shift-Shift are selectable to launch the OSCAR interface. One or all of the above keyboard combinations can be selected at a time. If only one keyboard combination is selected, it cannot be de-selected until a second one is chosen.

To choose the default display order of devices:

- 1 Select **Name** to display devices alphabetically by name.
or
Select **EID** to display devices numerically by EID number.
or
Select **Port** to display devices numerically by port number.
- 2 Click **OK**.

To set a Screen Delay Time for the OSCAR interface:

- 1 Type in the number of seconds (0 to 9) to delay the OSCAR interface display after you press <Print Screen>. Enter **0** to launch the OSCAR interface without delay.
- 2 Click **OK**.

By setting a **Screen Delay Time**, you can complete a soft switch without displaying the OSCAR interface. To perform a soft switch, see "Soft Switching" on page 37 in this chapter.

Setting Console Security

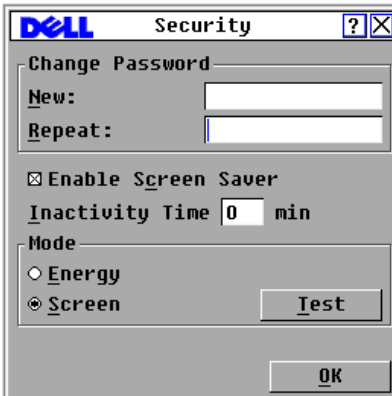
The OSCAR interface enables you to set security on your analog port console. You can establish a screen saver mode that engages after your console remains unused for a specified Inactivity Time. After it is engaged, your console remains locked until you press any key or move the mouse. You must type in your password to continue.


Use the **Security** dialog box to lock your console with password protection, set or change your password, and enable the screen saver.

To access the Security dialog box:


- 1 Press <Print Screen> to launch the OSCAR interface. The **Main** dialog box appears.
- 2 Click **Setup - Security**. The **Security** dialog box displays.

Figure 3-4. Security Dialog Box



 **NOTE:** If the New and Repeat fields contain six asterisks, a password has already been established.

To set or change the password:

 **NOTE:** If you lose or forget your password, please contact Dell Technical Support. See Appendix F: Technical Support for contact information.

- 1 Click in the **New** text box.
- 2 Type the new password in the **New** text box. Passwords must contain both alpha and numeric characters, are case sensitive, and may be up to 12 characters long. Legal characters are: A to Z, a to z, 0 to 9, and hyphen.
- 3 In the **Repeat** box, type the password again.
- 4 Click **OK** to change only your password, and then close the dialog box.

To password protect your console:

- 1 Set your password as described in the previous procedure.
- 2 Select **Enable Screen Saver**.
- 3 Type the number of minutes for **Inactivity Time** (from 1 to 99) to delay activation of password protection and the screen saver feature.
- 4 For **Mode**, select **Energy** if your monitor is ENERGY STAR[®] compliant; otherwise select **Screen**.



CAUTION: Monitor damage can result from the use of Energy mode with monitors not compliant with Energy Star[®].

- 5 (Optional) Click **Test** to activate the screen saver test, which lasts 10 seconds then returns you to the **Security** dialog box.
- 6 Click **OK**.

To log in to your console:

- 1 Press any key or move the mouse.
- 2 The **Password** dialog box displays. Type your password, then click **OK**.
- 3 The **Main** dialog box displays if the password was entered properly.

To remove password protection from your console:

- 1 From the **Main** dialog box, click **Setup - Security**.
- 2 In the **Security** dialog box, click in the **New** box. Leave the box blank. Press <Enter>.
- 3 Click in the **Repeat** box. Leave the box blank.
- 4 Click **OK** to eliminate your password.

To enable the screen saver mode with no password protection:

- 1 If your console does not require a password to gain access to the **Security** dialog box, proceed to step 2.
or
If your console is password protected, see the previous procedure, then go to step 2.
- 2 Select **Enable Screen Saver**.
- 3 Type the number of minutes for Inactivity Time (from 1 to 99) to delay activation of the screen saver.
- 4 Choose **Energy** if your monitor is ENERGY STAR® compliant; otherwise select **Screen**.



CAUTION: Monitor damage can result from the use of Energy mode with monitors not compliant with Energy Star®.

- 5 (Optional) Click **Test** to activate the screen saver test, which lasts 10 seconds then returns you to the **Security** dialog box.
- 6 Click **OK**.



NOTE: Activation of the screen saver mode disconnects the user from a device; no device is selected. The status flag displays the status “Free.”

To exit the screen saver mode:

Press any key or move your mouse. The **Main** dialog box displays and any previous device connection is restored after the password is validated by the appliance.

To turn off the screen saver:

- 1 In the **Security** dialog box, clear **Enable Screen Saver**.
- 2 Click **OK**.

To immediately turn on the screen saver:

Press <Print Screen>, then press <Pause>.

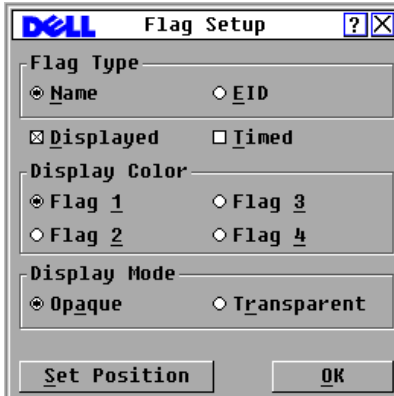
Controlling the Status Flag

The status flag displays on your desktop and shows the name or EID number of the selected device or the status of the selected port. Use the **Flag** dialog box to configure the status flag to display by device name or EID number, or to change the status flag color, opacity, display time, and location on the desktop.

To access the Flag dialog box:

- 1 Press <Print Screen> to launch the OSCAR interface. The **Main** dialog box appears.
- 2 Click **Setup - Flag**. The **Flag** dialog box displays.

Figure 3-5. Flag Dialog Box



To determine how the status flag is displayed:

- 1 Select **Name** or **EID** to determine what information will be displayed.
- 2 Select **Displayed** to show the status flag.
- 3 (Optional) Select **Timed** to display the status flag for only five seconds after switching.
- 4 Select a status flag color in **Display Color**.
- 5 In **Display Mode**, select **Opaque** for a solid color status flag or select **Transparent** to see the desktop through the status flag.
- 6 To position the status flag on the desktop:
 - a Click **Set Position** to gain access to the **Set Position Flag** screen.
 - b Click on the title bar and drag to the desired location.
-or-
Use the left and right arrows to nudge the status flag to the desired location and press <Enter>.
 - c Right-click to return to the **Flag** dialog box.



NOTE: Changes made to the status flag position are not saved until you click OK in the Flag dialog box.

- 7 Click **OK** to save settings.
or
Click **X** to exit without saving changes.

Setting the Interface Language

You can change the OSCAR interface to any one of 4 supported languages by selecting your chosen language in the **Language** dialog box.

To change the OSCAR interface language:

- 1 Press <Print Screen> to launch the OSCAR interface. The **Main** dialog box appears.
- 2 Click **Setup - Language**. The **Language** dialog box displays.

Figure 3-6. Language Dialog Box




- 3 Click to select the language you want the OSCAR interface to appear in.
- 4 Click **OK** to accept the change you have made and return to the **Setup** dialog box. The **Setup** dialog box displays in the language you have selected.

Assigning Device Types

The Remote Console Switch automatically discovers cascaded KVM switches, but you need to specify the number of ports on the cascaded switch through the **Devices** dialog box. An Sw-8 or Sw-24 in the **Type** category for

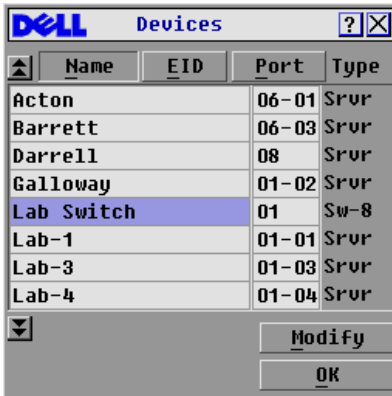
the cascaded switch is visible on screen. When you select from the list, the **Modify** button is enabled, allowing you to assign it the appropriate number of ports.

 **NOTE:** The **Modify** button is available only if a configurable switch is selected.

To access the Server dialog box:

- 1 Press <Print Screen> to launch the OSCAR interface. The **Main** dialog box appears.
- 2 Click **Setup - Devices**. The **Devices** dialog box displays.

Figure 3-7. Devices Dialog Box



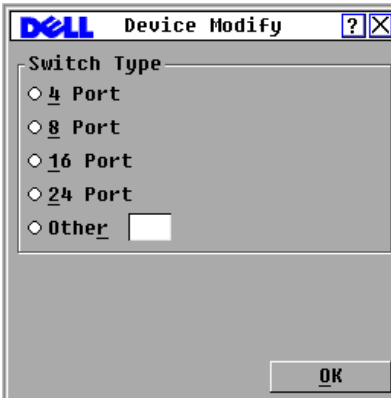
When the Remote Console Switch discovers a cascaded switch, the port numbering changes to accommodate each device under that switch. For example, if the switch is connected to ARI port 6, the switch port is listed as 06 and each device under it is numbered sequentially 06-01, 06-02 and so on.

 **NOTE:** Changes made in the Device Modify dialog box are not saved until you click **OK** in the **Devices** dialog box.

To assign a device type:

- 1 In the **Devices** dialog box, select the desired port number.
- 2 Click **Modify**. The **Device Modify** dialog box displays.


Figure 3-8. Device Modify Dialog Box



- 3 Choose or enter the number of ports supported by your cascaded switch and click **OK**.
- 4 Repeat steps 1 to 3 for each port requiring a device type to be assigned.
- 5 Click **OK** in the **Devices** dialog box to save settings.


Assigning Device Names


Use the **Names** dialog box to identify individual devices by name rather than by port number. The **Names** list is always sorted by port order. Names are stored in the SIP module, so even if you move the SIP/server to another ARI port, the name and configuration is recognized by the switch.

 **NOTE:** If a device is turned off, the respective SIP module does not appear in the **Names** list.

To access the **Names** dialog box:

- 1 Press <Print Screen> to launch the OSCAR interface. The **Main** dialog box appears.
- 2 Click **Setup - Names**. The **Names** dialog box displays.

 **NOTE:** If the server list changes, the mouse cursor turns into an hourglass as the list is automatically updated. No mouse or keyboard input is accepted until the list update is complete.

 **NOTE:** If a SIP module is not assigned a name, the EID is used as the default name.

To assign names to devices:

- 1** In the **Names** dialog box, select a device name or port number and click **Modify**. The **Name Modify** dialog box displays.
- 2** Type a name in the **New Name** box. Names of devices may be up to 15 characters long. Legal characters include: A to Z, a to z, 0 to 9, space and hyphen.
- 3** Click **OK** to transfer the new name to the **Names** dialog box. Your selection is not saved until you click **OK** in the **Names** dialog box.
- 4** Repeat steps 1 to 3 for each device in the system.
- 5** Click **OK** in the **Names** dialog box to save your changes.
or
Click **X** or press <Escape> to close the dialog box without saving changes.

Configuring Network Settings

You can change the network settings for your Remote Console Switch via the serial port or from the **Network** dialog box.

From the **Network** dialog box, you can choose either **IPv4** (default) or **IPv6** mode. You will be able to change the following network settings: **IP Address**, **Netmask** (when using **IPv4** mode) or **Prefix Length** (when using **IPv6** mode), and **Gateway**. You will also be able to choose a **Network Speed**, a **Transmission Mode**, and whether to assign a **Static** (default) IP address or, when appropriate, a **Dynamic** IP address to the Remote Console Switch.

Figure 3-9. Network (IPv4 Mode) Dialog Box

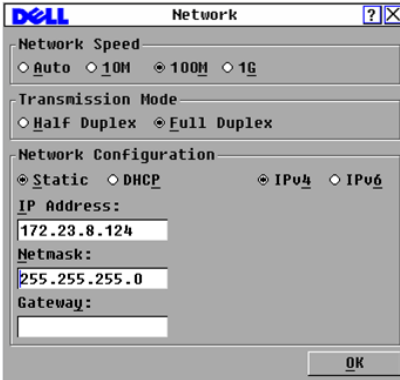
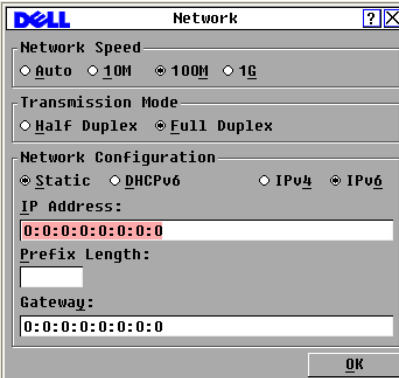


Figure 3-10. Network (IPv6 Mode) Dialog Box



Once you have made changes to the network settings, click OK. The Remote Console Switch will reboot.

Configuring Virtual Media Settings

For how to configure virtual media settings, see "Virtual Media" on page 89.

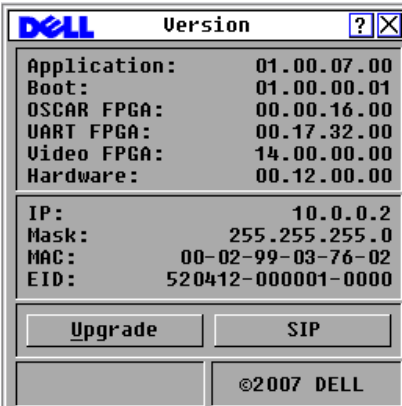
Displaying Version Information

The OSCAR interface enables you to display the versions of the Remote Console Switch and the SIP module firmware. For optimum performance, keep your firmware current. For more information, see "Appendix D: FLASH Upgrades" on page 211.

To display version information:

- 1 Press <Print Screen> to launch the OSCAR interface. The **Main** dialog box appears.
- 2 Click **Commands - Display Versions**. The **Version** dialog box displays. The top half of the box lists the subsystem versions in the appliance.

Figure 3-11. Version Dialog Box



- 3 Click the **SIP** button to view individual SIP module version information. The **SIP Select** dialog box displays.
- 4 Select a SIP module to view and click the **Version** button. The **SIP Version** dialog box displays.
- 5 Click **X** to close the **SIP Version** dialog box.

Scanning Your System

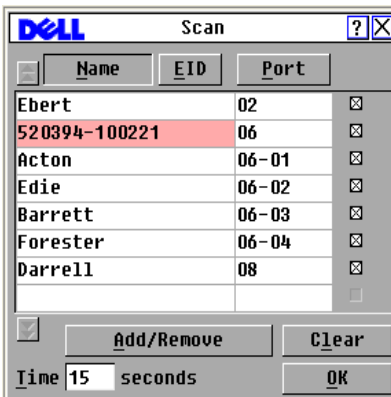
In scan mode, the appliance automatically scans from port to port (device to device). You can scan up to 100 devices, specifying which devices to scan, and the number of seconds that each device displays. The scanning order is

determined by placement of the device in the list. The list is always shown in scanning order. You can, however, choose to display the device name or EID number by pressing the appropriate button.

To add devices to the scan list:

- 1 Press <Print Screen> to launch the OSCAR interface. The **Main** dialog box appears.
- 2 Click **Setup - Scan**. The **Scan** dialog box displays.

Figure 3-12. Scan Dialog Box



- 3 The dialog box contains a list of all devices attached to your appliance. Click the checkbox next to the devices you wish to scan.
or
Double-click on a device name or port.
or
Press <Alt> and the number of the device you wish to scan. You can select up to 16 devices from the entire list.
- 4 In the **Time** box, type the number of seconds (from 3 to 99) of desired time before the scan moves to the next device in the sequence.
- 5 Click **OK**.

To remove a device from the scan list:

- 1 In the **Scan** dialog box, select the device to be removed.
or
Double-click on the device name or port.
or
Click the **Clear** button to remove all devices from the scan list.
- 2 Click **OK**.

To start the scan mode:

- 1 Press <Print Screen> to launch the OSCAR interface. The **Main** dialog box appears.
- 2 Click **Commands**. The **Commands** dialog box displays.
- 3 Select **Scan Enable** in the **Commands** dialog box.
- 4 Click **X** to close the **Commands** dialog box.



NOTE: If the Add/Remove button is clicked when a device is highlighted, the check box corresponding to the highlighted device toggles state.

To cancel scan mode:

- 1 Select a device if the OSCAR interface is open.
or
Move the mouse or press any key on the keyboard if the OSCAR interface is not open. Scanning stops at the currently selected device.
or
Press <Print Screen>. The **Main** dialog box will appear.
- 2 Click **Commands**. The **Commands** dialog box displays.
- 3 Clear **Scan Enable**.

Setting the Preemption Warning

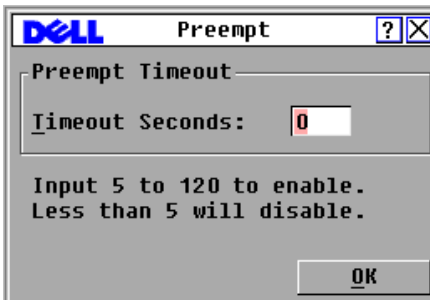
Administrators and users with equal or higher access rights than current user can preempt (disconnect) KVM sessions and take control of the target device. You can choose whether or not to warn the first user that the session will be preempted and specify how long the appliance will wait for the first user to respond to the warning.

To view or change the preemption warning settings, complete the following steps:

- 1 Press <Print Screen> to launch the OSCAR interface. The **Main** dialog box appears.

- 2 Click **Setup > Preempt**.
- 3 Enter a number of seconds in the **Timeout Seconds** field.
 - If you enter a value of 0 to 4 seconds, the first user will not be warned before the session is preempted.
 - If you enter a value of 5 to 120 seconds, the first user will be warned and will be allowed to continue using the target device for up to the amount of time in the **Timeout Seconds** field. The session will be preempted when the user clicks **OK**, or when the specified time elapses.


Figure 3-13. Preempt Dialog Box



- 4 Click **OK** to save the settings.

Displaying Configuration Information

You can view the configuration of your Remote Console Switch from the **Configuration** dialog box. This dialog box provides you with quick access to the settings you have entered and allows you to add additional features by clicking the **License Key** button and typing the license key for any additional features.

 **NOTE:** If there are no features that require a license in the firmware, the button is grayed out.

To view system configuration:

- 1 Press **<Print Screen>** to launch the OSCAR interface. The **Main** dialog box appears.
- 2 Click **Configuration**. The **Configuration** dialog box is displayed.

- 3 Click **License Key** to add a license key and enable a new feature or click **X** to close the **Configuration** dialog box and return to the **Setup** dialog box.

Running System Diagnostics

You can validate the integrity of your system through the **Run Diagnostics** command. This command checks the main board functional subsystems (memory, communications, switch control, and the video channels) for each system controller. When you select the **Run Diagnostics** option, you receive a warning indicating that all users (remote and local) will be disconnected. Click **OK** to confirm and begin the test.

The **Diagnostics** dialog box displays. The top section of the dialog box displays the hardware tests. The bottom portion divides the tested SIP modules into three categories: On-line, Offline, or Suspect.


 **NOTE:** A SIP module may appear to be offline while it is being upgraded.

Figure 3-14. Diagnostics Dialog Box



As each test is finished, a pass (green circle) or fail (red x) symbol displays to the left of each item as that test finishes. The following table details each of the tests.

Table 3-4. Diagnostic Test Details

Test	Description
Firmware CRCs	Reports on the condition of the switch firmware file

Table 3-4. Diagnostic Test Details


Test	Description
Remote User Video	Reports on whether a digital video channels are installed but not working
LAN Connection	Indicates whether LAN connection is active and whether traffic has been seen since the last run of diagnostics.
On-line SIP modules	Indicates the total number of currently connected and powered SIP modules
Offline SIP modules	Indicates the number of SIP modules that were connected successfully in the past and are turned off
Suspect SIP modules	Indicates the number of SIP modules that were detected, but are either unavailable for connection or dropped packets during the ping tests


To run diagnostic tests:


- 1** Press <Print Screen> to launch the OSCAR interface. The **Main** dialog box appears.
- 2** Click **Commands - Run Diagnostics**. A warning message displays indicating that all users will be disconnected.
- 3** Click **OK** to begin diagnostics.
or
Click **X** or press <Escape> to exit the dialog box without running a diagnostic test.
- 4** All users are disconnected and the **Diagnostics** dialog box displays.
- 5** As each test is finished, a pass (green circle) or fail (red x) symbol displays. The test is complete when the last test's symbol displays.

Broadcasting to Servers

The analog user can simultaneously control more than one server in a system to ensure that all selected servers receive identical input. You can choose to broadcast keystrokes and/or mouse movements independently.

 **NOTE:** You can broadcast up to 16 devices at a time, one device per ARI port.

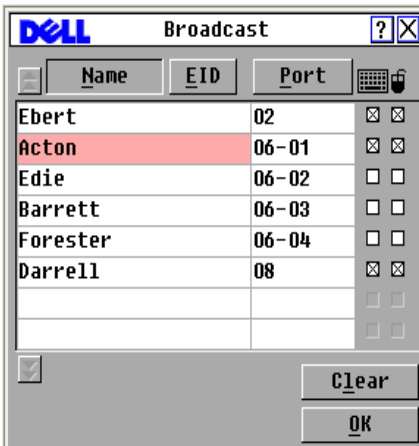
 **NOTE:** Broadcasting Keystrokes - The keyboard state must be identical for all devices receiving a broadcast to interpret keystrokes identically. Specifically, the <Caps Lock> and <Num Lock> modes must be the same on all keyboards. While the appliance attempts to send keystrokes to the selected devices simultaneously, some devices may inhibit and thereby delay the transmission.

 **NOTE:** Broadcasting Mouse Movements - For the mouse to work accurately, all systems must have identical mouse drivers, desktops (such as identically placed icons), and video resolutions. In addition, the mouse must be in exactly the same place on all screens. Because these conditions are extremely difficult to achieve, broadcasting mouse activity to multiple systems may have unpredictable results.

To access the Broadcast dialog box:

- 1 Press <Print Screen> to launch the OSCAR interface. The **Main** dialog box appears.
- 2 Click **Setup - Broadcast**. The **Broadcast** dialog box displays.


Figure 3-15. Broadcast Dialog Box



To broadcast to selected devices:

- 1 From the **Broadcast** dialog box, select the mouse and/or keyboard checkboxes for the devices that are to receive the broadcast commands.
or
Press the *up-arrow* or *down-arrow* keys to move the cursor to the target device. Then press <Alt+K> to select the keyboard checkbox and/or <Alt+M> to select the mouse checkbox. Repeat for additional devices.

- 2 Click **OK** to save the settings and return to the **Setup** dialog box. Click **X** or press <Escape> to return to the **Main** dialog box.
- 3 Click **Commands**. The **Commands** dialog box displays.
- 4 Click the **Broadcast Enable** checkbox to activate broadcasting. The **Broadcast Enable Confirm/Deny** dialog box displays.
- 5 Click **OK** to enable the broadcast. Click **X** or press <Escape> to cancel and return to the **Commands** dialog box.
- 6 If broadcasting is enabled, type the information and/or perform the mouse movements that you would like to broadcast from the user station. Only devices in the list are accessible.


 **NOTE:** Any other user is disabled when broadcast mode is enabled.

To turn broadcasting off:

From the **Commands** dialog box, clear the **Broadcast Enable** checkbox.

Power Controlling Devices




You can control supported PDUs through the OSCAR interface.


 **NOTE:** This feature is only available on the 2321DS Remote Console Switch.

Power window


Through the **Power** window, you can view which outlets control which devices and whether the outlet is on or off. You can also turn on, turn off or cycle power to a selected device. The status of each outlet is indicated by one or more status symbols in the right column. The following table describes the status symbols.

Table 3-5. Power Window Status Symbols

Symbol	Description
	Outlet is on.
	Outlet is off.
	Outlet is waiting to go on.

Symbol	Description
	Outlet is waiting to go off.




To turn on, turn off or cycle power to a device:

- 1 Press <Print Screen> to launch the OSCAR interface. The **Main** dialog box appears.
 - 2 Click **Commands - Power**.
 - 3 Select the device you wish to control.
-  **NOTE:** Multiple devices may be selected.
- 4 Click **On**, **Off**, or **Cycle**, as appropriate.

PDU window

Through the PDU window, you can view which PDUs are connected to your system. The status of each PDU is indicated by one or more status symbol in the right column. The following table describes the status symbols.

Table 3-6. PDUs Window Status Symbols

Symbol	Description
	Outlet is online.
	Outlet is offline.
	Outlet is overloaded.

To view connected PDUs:

Open the **PDUs** window. The window contains a listing of all PDUs attached to your system.

PDU Settings window


From the **PDUs** window, you can view the **PDU Settings** window, which allows you to view and modify PDU parameters.

To view/modify PDU settings:

- 1** Press <Print Screen> to launch the OSCAR interface. The **Main** dialog box appears.
- 2** Click **Setup - PDUs**.
- 3** Complete one of the following steps:
 - Select a PDU name, then click **Settings** to open the **PDU Settings** window.
 - or-
 - Select a PDU name, then press <Enter> to open the **PDU Settings** window.
 - or-
 - Double-click on the PDU name to open the **PDU Settings** window.
- 4** Complete any of the following steps:
 - a** In the **Name** field, enter the PDU name.
 - b** In the **Cycle Delay** field, enter the number of seconds you want the Remote Console Switch to wait between turning off and turning on.
- 5** Click **OK**.

PDU Inlets window

From the **Inlets** window, you can view and modify inlet parameters.

 **NOTE:** You can only modify inlet parameters on a PDU that is currently online.


To view/modify **PDU Inlet** settings:

- 1** Press <Print Screen> to launch the OSCAR interface. The **Main** dialog box appears.
- 2** Click **Setup - PDUs**.
- 3** Complete one of the following steps:
 - Select a PDU name, then click **Settings** to open the **PDU Settings** window.
 - or-
 - Select a PDU name, then press <Enter> to open the **PDU Settings** window.
 - or-
 - Double-click on the PDU name to open the **PDU Settings** window.

- 4 Click **Inlets**.
- 5 Enter an integer in the **Minimum Amps** or **Maximum Amps** fields.
- 6 Click **OK**.

PDU Outlets window

From the **Outlets** window, you can select an outlet and open the **Outlet Settings** window to set outlet-specific parameters.

 **NOTE:** You can only modify outlet parameters on a PDU that is currently online.

To view/modify **PDU Outlet** settings:

- 1 Press <Print Screen> to launch the OSCAR interface. The **Main** dialog box appears.

- 2 Click **Setup - PDUs**.

- 3 Complete one of the following steps:

Select a PDU name, then click **Settings** to open the **PDU Settings** window.

-or-

Select a PDU name, then press <Enter> to open the **PDU Settings** window.

-or-

Double-click on the PDU name to open the **PDU Settings** window.

- 4 Click **Outlets**.

- 5 Complete one of the following steps:

Select an outlet, then click **Settings** to open the **Outlet Settings** window.

-or-

Select an outlet, then press <Enter> to open the **Outlet Settings** window.

-or-

Double-click an outlet to open the **Outlet Settings** window.

- 6 Select the outlet you wish to modify.

- 7 Complete any of the following steps:

- a In the **Name** field, enter the Outlet name.

- b** In the **Power-On Interval** field, enter the number of seconds you want the Remote Console Switch to wait between turning off and turning on.



NOTE: The **Power-On Interval** must be an integer between 0 and 7200.

- 8** Click **OK**.

Using the Viewer

You can connect to a server in the Remote Console Switch system using the Viewer. The Viewer allows you full keyboard, monitor and mouse control over a server.

You can also scan through a customized list of servers by enabling individual servers to appear in the **Thumbnail Viewer**. This view contains a series of thumbnail frames, each containing a small, scaled, non-interactive version of a server's screen image. For more information, see "Viewing Multiple Servers Using the Scan Mode" on page 77.

You can launch the Viewer from the Remote Console Switch Software or the on-board web interface. This chapter describes how to use the Viewer from the on-board web interface. For how to use the Viewer from the Remote Console Switch Software, see the Dell Remote Console Switch Software User's Guide or the help included with the software.

Accessing Servers from the On-board Web Interface

The **Connections** tab in the on-board web interface allows you to view the connected servers and their status. You may click on a server name to launch the Viewer.

For how to launch the on-board web interface, see "Launching the On-board Web Interface" on page 32.

Table 4-1. On-board Web Interface Server Status Symbols




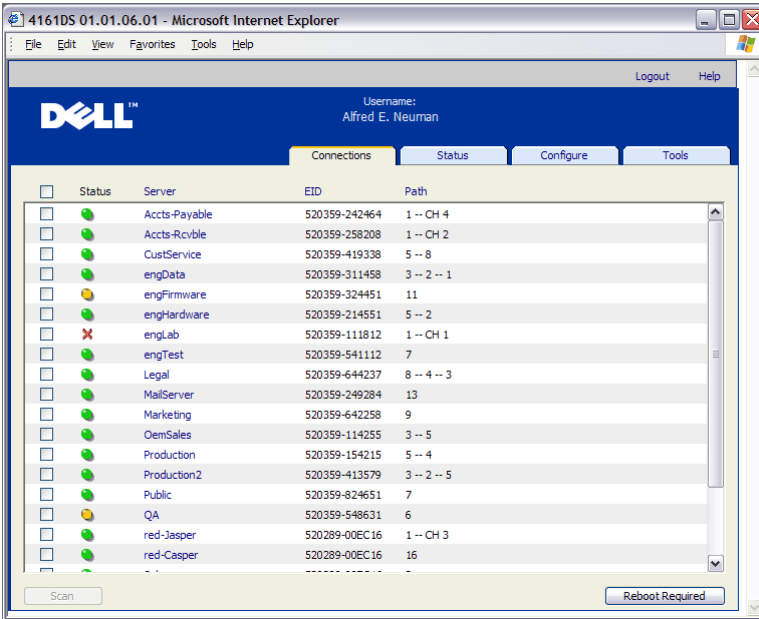
Symbol	Description
	Server is online
	Server is offline
	Server is unavailable

Figure 4-1. On-board Web Interface - Connections Tab



Interacting With the Server Being Viewed

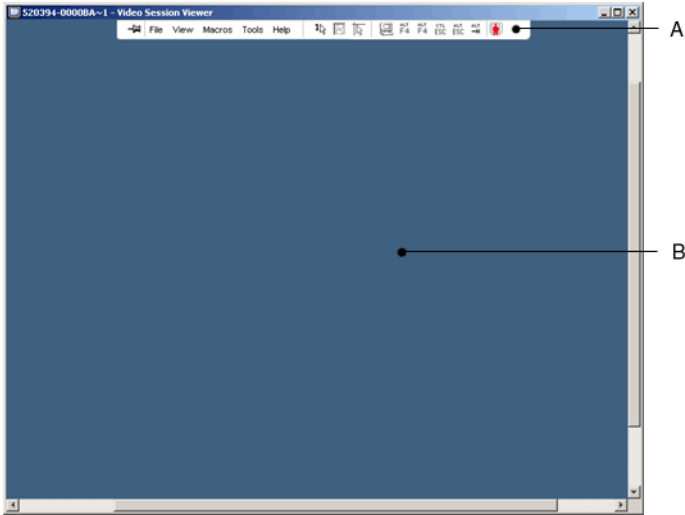
Once you have connected to a server, you will see the desktop window of the server on your screen. This opens in a separate window. You will see two cursors, the local cursor and the server's cursor. You may need to align these if they do not move together or adjust the video if they seem to jump about. From this window, you will be able to access all the normal functions of this server as if you were sitting right in front of it. You may also perform Viewer-specific tasks such as sending special macro commands to the server.



NOTE: If you are experiencing slow mouse response during a remote video session, deactivate mouse acceleration in the operating system of the target device and set mouse speed to 50%.

Viewer Window Features

Figure 4-2. Viewer Window



- A** Menu bar: Access many of the features in the Viewer.
- B** Accessed server desktop: Interact with your server through this window.

Viewer Menu bar







Figure 4-3. Viewer Menu Bar



- A** Thumbtack: Click to lock the menu bar in place. This prevents the menu bar from hiding once you have moved the mouse cursor away from the menu bar.
- B** Menu Options: The menus provides access to functions available through the Viewer.
- C** Toolbar Buttons: You may add up to 10 buttons to the tool bar. These buttons allow you to provide easy access to defined functions

and keyboard macros. By default, the Align Local Cursor, Refresh Image, and Single Cursor Mode buttons are displayed.

- D Connection Status Indicator:** The connection status indicator indicates how the user is connected to the appliance for this server. For more information see "Connection Sharing" on page 86.

Connection Status Indicator	Sharing Mode
	Exclusive Mode
	Active Connection (normal, non-sharing, non-exclusive session)
	Active Sharing (Primary User)
	Active Sharing (Secondary User)
	Passive Sharing
	Stealth Mode

Adjusting the Viewer

You can adjust the **Viewer** settings to match your requirements. This includes adjustment of the video resolution, toolbar settings, and keyboard macro settings.

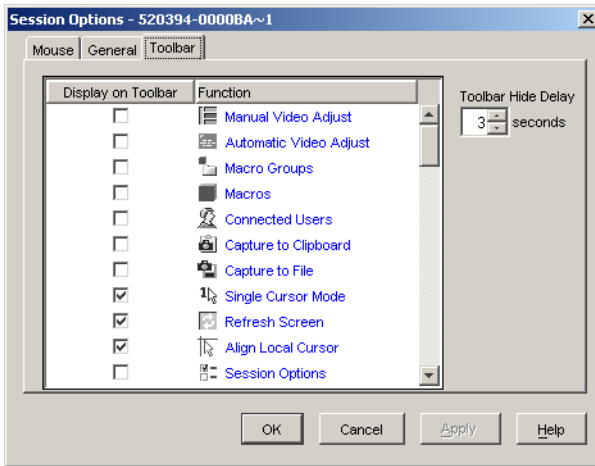
Adjusting the Viewer Toolbar

You may add up to 10 buttons to the toolbar. These buttons allow you to provide easy access to defined function and keyboard macros. By default, the **Align Local Cursor**, **Refresh Image**, and **Single Cursor Mode** buttons are displayed.

To add buttons to the toolbar:

- 1 From the **Tools** menu in the **Viewer**, choose **Session Options**. The Session Options toolbar is displayed.
- 2 Click the **Toolbar** tab.
- 3 Click to select the items you want to add to the **Viewer** toolbar.
- 4 Click **OK** to accept the changes and return to the **Viewer** main window.

Figure 4-4. Session Options Dialog Box - Toolbar Tab



Setting the Toolbar Hide Delay Time

Unless the **Thumbtack** button has been clicked, the toolbar will disappear when you remove the mouse cursor. You can change the interval between the removal of the mouse cursor and the disappearance of the toolbar by adjusting the **Toolbar Hide Delay** time.

To change the **Toolbar Hide Delay** time:

- 1 From the **Tools** menu in the **Viewer**, choose **Session Options**. The Session Options toolbar is displayed.
 - 2 Click the **Toolbar** tab.
 - 3 In the **Toolbar Hide Delay** field, type the number of seconds for which you want the toolbar to display, after the mouse cursor is removed.
- or -

Using the **Up** and **Down** button, click to increase or decrease the number of seconds for which you want the toolbar to display, after the mouse cursor is removed.

- 4 Click **OK** to accept the change you have made and return to the **Viewer** main window.

Expanding and Refreshing Your Viewer

By default, there are three buttons that display on the **Viewer** toolbar that allow you to adjust the **Viewer** display. The first button allows you to set the **Viewer** to **Single Cursor Mode**. This allows you to use the mouse in the **Viewer** as if it was the mouse on the server. When the **Viewer** is set to **Single Cursor** mode the local cursor is not displayed.

 **NOTE:** Single Cursor mode operates on Windows platforms only.

The second button allows you to align the mouse cursors, and the third allows you to refresh the video.

Figure 4-5. Viewer Toolbar- Display Adjustment Buttons



To set the **Viewer** to **Single Cursor** mode:

In the **Viewer** toolbar, click the **Single Cursor Mode** button.

To align the mouse cursors:

Click the **Align Local Cursor** button on the **Viewer** toolbar. The local cursor will align with the cursor on the remote server.

To refresh the screen:

Click the **Refresh Image** button on the **Viewer** toolbar.

-or-

From the **Viewer** menu, select **View - Refresh**. The digitized video image will be completely regenerated.

To enter full screen mode:

Click the **Maximize** button in the top right-hand corner of the **Viewer**.

-or-

From the **Viewer** menu, select **View - Full Screen**. The desktop window will

disappear and only the accessed server desktop will be visible. The screen will be resized up to a maximum of 1024x768. If the desktop has a higher resolution, then a black background will surround the full screen image. The floating toolbar will appear.

To exit full screen mode:

Press <Esc> to exit full screen mode and return to the desktop window.

Adjusting the Viewer Resolution

If **Auto Scale** is enabled, the display automatically adjusts when the **Viewer** window size changes during a session. When you access a channel using sharing, the display adjusts to match the input resolution selected by the primary user of that channel. This prevents the primary user's display from being affected. If the resolution changes any time during a session, the display is adjusted automatically.

When **Full Scale** is selected, the **Viewer** adjusts to the screen resolution of the server and sets the screen size accordingly, up to a maximum resolution of 1024 x 768.

To adjust the size of the **Viewer** window:

From the menu bar, select **View - Scaling - Auto Scale** to allow the server image to be scaled automatically.

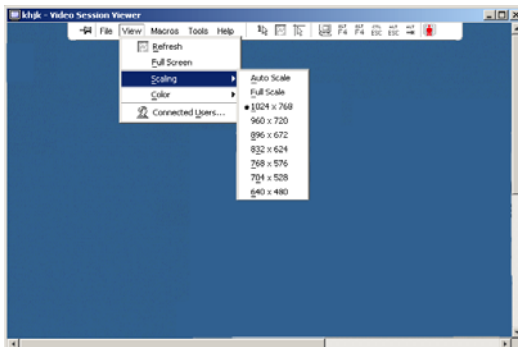
or

From the menu bar, select **View - Scaling - Full Scale**

or

Select a screen resolution from the **Scaling** sub-menu.

Figure 4-6. Viewer Scaling



Adjusting the Video Quality

The **Viewer** offers both automatic and manual video adjustment capability. Generally, the **Automatic Video Adjustment** will optimize the video for the best possible view. However, you may wish to alter the video for your specific needs. Use the slider bar for large adjustments and the **Plus (+)** and **Minus (-)** buttons are designed for fine-tuning adjustments. For more information on manual video adjustment, please see Figure 4-7

Adjusting Color Depth



NOTE: The Color command may only be used by the primary user. The command is not available to non-primary users who are sharing the session.



NOTE: If Background Refresh is enabled from the Session Options dialog, the color depth will be set automatically to Best Color Available and cannot be changed.

The **Color** sub-menu allows you to set the color depths at which the digital image can be compressed. The Remote Console Switches support the Dambrockas Video Compression (DVC) algorithm, which enables users to adjust the number of viewable colors in a remote session window. You may choose to display more colors for the best fidelity, or fewer colors to reduce the volume of data transferred on the network.

The **Viewer** window can be viewed using the **Best Color Available** (slower updates), **Best Compression** (fastest updates), a combination of **Best Color** and **Best Compression**, or in **Grayscale**.

The color depths of individual ports and channels can be specified by selecting the **View - Color** command in a **Remote Session** window. These settings are saved individually per port and channel.

To set the color depth:

From the **View** menu, choose **Color** and select a color depth from the **Color** sub-menu.

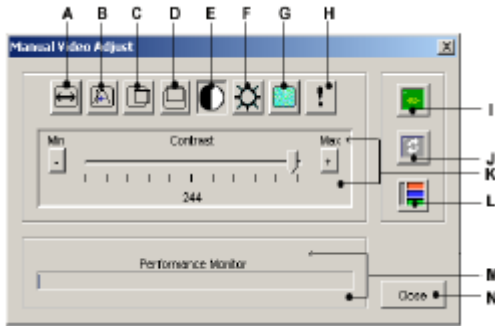
To manually adjust the video quality of the **Viewer** window:


- 1 From the **Viewer** menu, select **Tools - Manual Video Adjust**. The **Manual Video Adjust** dialog box appears.
- 2 Click the icon for the feature you wish to adjust.
- 3 Move the slider bar or click the **Minus (-)** or **Plus (+)** buttons to adjust the parameter for each icon pressed. The adjustments will display immediately in the **Viewer** window.

- 4 When finished, click Close to exit the Manual Video Adjust dialog box.

Manual Video Adjust Dialog Box Options

Figure 4-7. Manual Video Adjust Dialog Box



-  **A** Image Capture Width
- B** Pixel Sampling Fine Adjust
- C** Image Capture Horizontal Position
- D** Image Capture Vertical Position
- E** Contrast
- F** Brightness
- G** Noise Threshold
- H** Priority Threshold
- I** Automatic Video Adjustment
- J** Refresh Image
- K** Adjustment bar
- L** Video Test Pattern
- M** Performance Monitor
- N** Close box

Minimizing Remote Video Session Discoloration

When establishing remote video sessions, pixel discolorations may occur due to network conditions. This condition occurs most often with a solid color background. This condition is minimized by using a black background. If a color background is used, a small number of pixels on the screen will be discolored or white.

To minimize remote video pixel discoloration:

- 1 From the **Viewer** menu, select **Tools - Manual Video Adjust**. The **Manual Video Adjust** dialog box appears.
- 2 Choose contrast or brightness.
- 3 Incrementally, adjust the contrast and brightness until the image quality improves.
- 4 A noise threshold setting is also available under **Tools - Manual Video Adjust** for fine incremental adjustments.



NOTE: Reducing the noise threshold to zero causes constant video refresh, high network usage, and a flickering video. Dell recommends that the noise threshold be set to the highest level that allows efficient system performance, while still being able to recover pixel colors over which the mouse cursor travels.



NOTE: When adjusting the noise threshold, use the slider bar for large adjustments and the Plus (+) and Minus (-) buttons at the ends of the slider bar for fine-tuning.

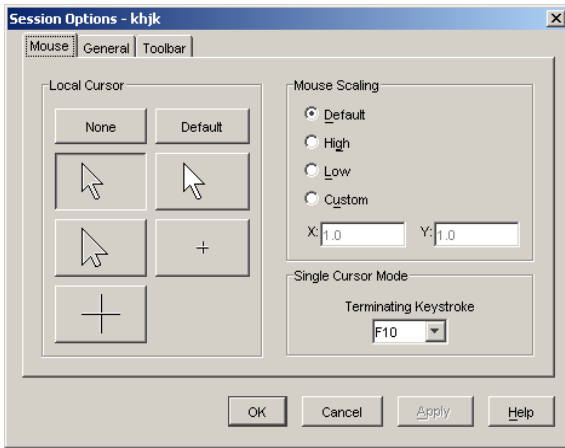
Improving Screen Background Color Display

You may experience inconsistent color display when viewing target servers where photographic images or color-intense gradient backgrounds have been selected. We recommend that you select a solid color display background via the operating system for optimal display quality and performance.

Adjusting the Mouse

The **Viewer** allows you to select between five different mouse cursor options, set up mouse scaling, and resynchronize your mouse should it no longer track properly. Dell recommends turning off the local cursor by setting the **Local Cursor** option to **None**. This will leave only one cursor on the screen, the remote cursor, and will simplify navigation.

Figure 4-8. Viewer Mouse Session Options dialog box



Setting Mouse Scaling

You can choose between three preset mouse scaling options or set your own custom scaling. The three preset settings are: **Default (1:1)**, **High (2:1)**, or **Low (1:2)**. In a 1:1 scaling ratio, every mouse movement on the desktop window will send an equivalent mouse movement to the server. In a 2:1 scaling, the same mouse movement will send a 2X mouse movement. In a 1:2 scaling, the value will be 1/2X.

To set custom mouse scaling:

- 1 From the **Viewer** menu, select **Tools - Session Options**. The **Session Options** dialog box appears.
- 2 Click the **Mouse** tab.
- 3 Click the **Custom** radio button. The **X** and **Y** fields become enabled.
- 4 Type the mouse scaling values you wish in the **X** and **Y** fields. For every mouse input, the mouse movements are multiplied by the respective **X** and **Y** scaling factors. Valid input ranges are 0.25 to 3.00.

Minimizing Mouse Trailing

During a remote video session, as the mouse moves on the screen, some pixels will remain discolored. This condition is referred to as mouse trailing, and is due to varying levels of network and other noise in different environments. To minimize mouse trailing, you may need to reduce the **Noise Threshold** in the **Manual Video Adjust** dialog box.

To reduce the Noise Threshold:

- 1 From the **Viewer** menu, select **Tools - Manual Video Adjust**. The **Manual Video Adjust** dialog box appears.
- 2 Click the **Noise Adjust Threshold** icon for the feature you wish to adjust.
- 3 Using the mouse, move the slider bar to the center of the scale, and then down to zero.
- 4 Use the **Plus (+)** and **Minus (-)** buttons at the end of the slider bar to fine-adjust the noise threshold to just above zero.



NOTE: Leaving the noise threshold at zero triggers constant video refresh, resulting in high network usage and a flickering video. It is recommended that the noise threshold be set at the highest level that allows efficient system performance, while still being able to recover pixel colors that the mouse cursor travels over.



NOTE: When adjusting the noise threshold, the slider bar is used for large adjustments and the Plus (+) and Minus (-) buttons at either end of the slider bar for fine-tuning.

Improving Mouse Performance

If you are experiencing slow mouse response or if the mouse pointers get out of sync during a remote video session, you may want to deactivate the mouse acceleration in the operating system of the target server.

Microsoft Windows:

- Turn off mouse acceleration
- Adjust mouse speed to the exact midpoint of the slider bar.



NOTE: See the documentation included with your Windows operating system for specific instructions.

Red Hat Linux:

- 1 Select the **Mouse** settings from the **Desktop Controls**.

- 2 Set **Acceleration** to 1.0.
- 3 Apply the changes and use the **Align Local Cursor/Mouse** button in the **Viewer** to resynchronize the mouse.

Viewing Multiple Servers Using the Scan Mode

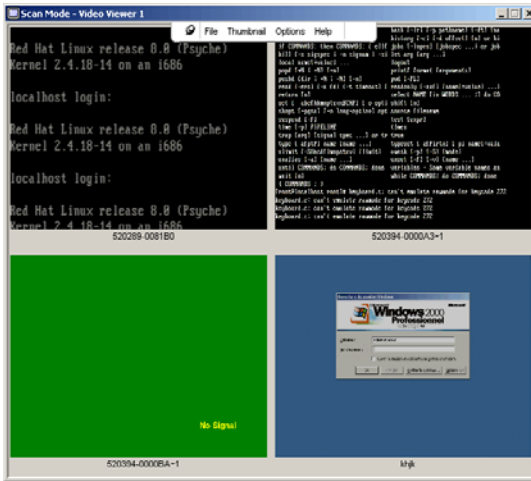
The **Viewer** allows you to simultaneously view multiple servers through the **Thumbnail Viewer** of the **Scan** mode. This view contains a series of thumbnail frames, each containing a small, scaled, non-interactive version of a server's screen image. The server name displays below each thumbnail as well as the status indicator.

Scanning Your Servers

Using the **Thumbnail Viewer**, you can set up a scan sequence of up to 16 servers to monitor your servers. The scan mode moves from one thumbnail image to the next, logging into a server and displaying an updated server image for a user-specified length of time (**View Time Per Server**), before logging out of that server and moving on to the next thumbnail image. You can also specify a scan delay between thumbnails (**Time Between Servers**). During the delay, you will see the last thumbnail image for all servers in the scan sequence, though you won't be logged into any servers.

An indicator light at the bottom of each frame displays the status of the server. The default thumbnail size is based on the number of servers in the scan list.

Figure 4-9. Viewer - Thumbnail Viewer



Scan mode is a lower priority than an active connection. If you have an interactive session with a server, that server will be skipped in the scan sequence and the scan mode will proceed to the next server. No login error messages will appear. Once the interactive session is closed, then the thumbnail will be included in the scan sequence again. If another user has an active connection to a server, the server will be skipped and a red “X” will be displayed in the indicator light below the frame.

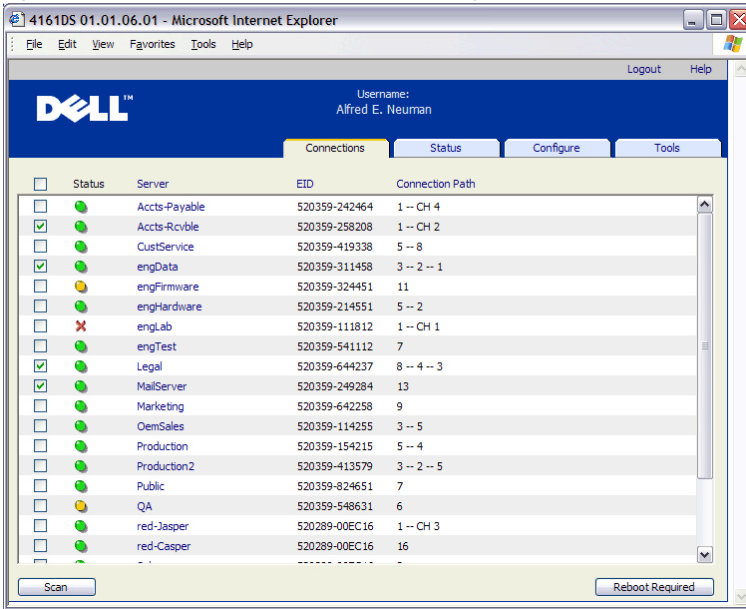
The Remote Console Switch Software can scan connected servers on multiple Remote Console Switches, while the on-board web interface can only scan connected servers on a single Remote Console Switch.



NOTE: For how to use the Remote Console Switch Software, see the Dell Remote Console Switch Software User’s Guide or the help included with the software.

Accessing Scan Mode from the On-board Web Interface

Figure 4-10. On-board Web Interface - Scanning Servers



To access Scan mode in the on-board web interface:

- 1 In the on-board web interface, click the **Connections** tab.
- 2 Select the check boxes next to the servers you want to scan.
- 3 Click **Scan**.

Thumbnail View Status Indicators

The green LED indicates that a server is currently being scanned. The red X indicates that the last scan of the server was not successful. The scan may have failed due to a credential or path failure (the server path on the Remote Console Switch was not available), or because of some other reason. When the mouse pointer is placed on the red X a tool tip appears and indicates the reason for the failure.

Setting up your Scanning Preferences

To set scan preferences:

- 1 From the Thumbnail Viewer, select **Options - Preferences**. The **Preferences** dialog box appears.
- 2 Enter the time each thumbnail will be active during the scan (10 to 60 seconds) in the **View Time Per Server** box.
- 3 Enter the length of time the scan stops between each server (5 to 60 seconds) in the **Time Between Servers** box.
- 4 Click **OK**.

Navigating the Thumbnail Viewer

When you highlight an individual thumbnail frame and select the **Thumbnail** menu, you can launch an interactive session to that server, add that server to the scan sequence or set the login credentials for that server. The **Options** menu allows you to access scanning preferences as well as pause the scan and set the thumbnail size for all servers.

To launch a server Video session:

- 1 Select a server thumbnail.
- 2 From the Thumbnail Viewer, select **Thumbnail - [server name] - View Interactive Session**.

-or-

Right-click a server thumbnail and select **View Interactive Session**. That server's video will be launched in an interactive **Viewer** window.

To enable or disable a server in the scan sequence:

- 1 Select a server thumbnail.
- 2 From the Thumbnail Viewer, select **Thumbnail - [server name] - Enable**.

-or-

Right-click a server thumbnail and select **Enable**. That server will be included/excluded in the server thumbnail scan sequence.



NOTE: The **Enable** menu item state can be toggled from checked (enabled) to unchecked (disabled) each time it is selected.



NOTE: If a server is being accessed by a user, the **Enable** menu will be disabled for that server thumbnail.

To pause or restart a scan sequence:

From the Thumbnail Viewer, select **Options - Pause Scan**. The scan sequence will pause at the current thumbnail if the Thumbnail Viewer has a scan in progress or will restart the scan if currently paused.

To change the thumbnail size:

- 1 From the Thumbnail Viewer, select **Options - Thumbnail Size**.
- 2 Select the desired thumbnail size from the menu.

Using Macros to Send Keystrokes to the Server

The **Macros** menu in the Viewer allows you an easy way to send multiple keystrokes to the server. The Viewer provides a list of default keystroke selections for Microsoft Windows systems, Linux Systems and Sun systems.

To choose which system you are using:

Click the **Macro** menu in the Viewer. Select **Display on Menu**, and select **Windows**, **Linux** or **Sun**.

To send keystrokes to the server:

Click the **Macro** menu in the Viewer and choose the name of the macro containing the keystrokes you wish to send to the server. Figure 4-11, Figure 4-12 and Figure 5-15 show the default macros.

Figure 4-11. Viewer Macro Menu Expanded - Windows Option

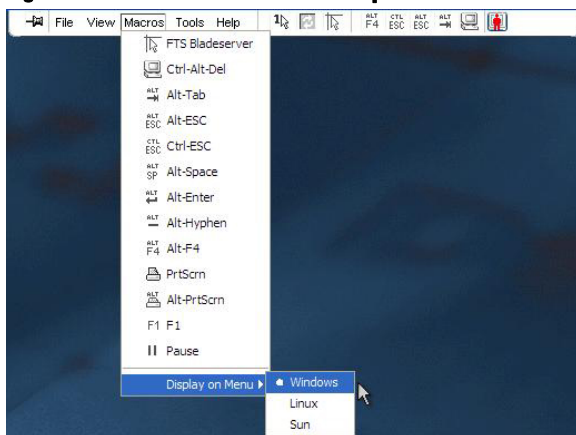


Figure 4-12. Viewer Macro Menu Expanded - Linux Option

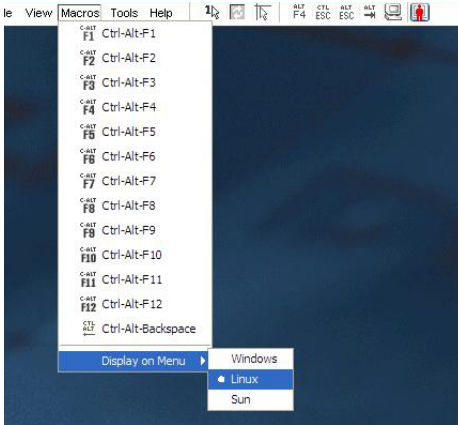
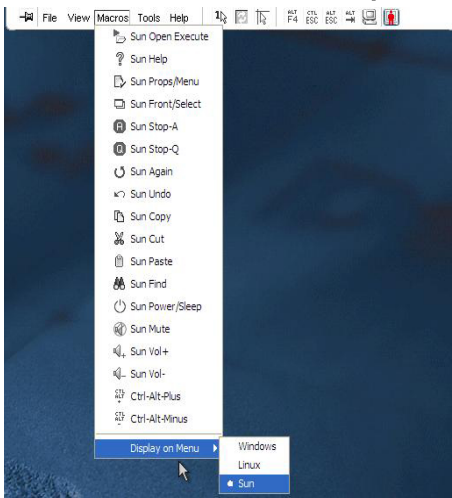


Figure 4-13. Viewer Macro Menu Expanded - Sun Option

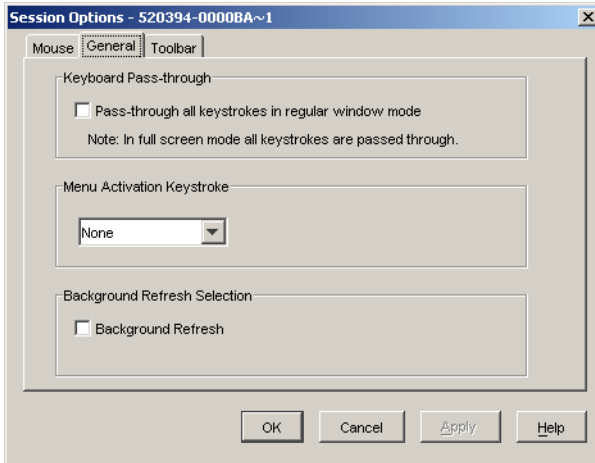


Session Options - General Tab

The **General** tab in the Session Options dialog box allows you to control the **Keyboard Passthrough** option in non-full screen mode, the **Menu Activation** keystroke, and the **Background Refresh** selection.

The **Keyboard Pass-through** check box allows you to specify whether **Keyboard Pass-through** mode is enabled, or not. The **Keyboard Pass-through** option is not selected by default.

Figure 4-14. Session Options - General Tab



The **Menu Activation Keystroke** list allows you to select a keystroke that activates the toolbar.

The **Background Refresh** check box allows you to specify whether background refreshing occurs. When this option is selected the **Viewer** is sent a constant stream of data from the device whether or not a change has occurred on the device.

To change session options:

- 1 From the **Tools** menu in the **Viewer**, choose **Session Options**. The **Session Options** toolbar is displayed.
- 2 Click the **General** tab.
- 3 Modify the session options as desired.
- 4 Click **OK**.

Screen Capturing

The **Viewer** allows you to capture the contents of the screen and to save it to a file or to copy it to the clipboard.

To capture a screen as a file:

- 1 In the **Viewer**, choose **File - Capture to File**. The **Save** dialog is displayed.
- 2 Browse to the location where you want to save the file.
- 3 In the **File Name** field, type a file name and click **Save**.

To copy a screen to the clipboard:

In the **Viewer**, choose **File - Capture to Clipboard**. The image is saved to the clipboard and can be pasted into a document or image editing application.



NOTE: The Capture to Clipboard function is not available in Linux.

Preemption

Preemption provides a means for users with sufficient privilege to take control of a server from another user with lesser or equal privilege.



NOTE: All users sharing the connection that is being preempted will be warned, but only the primary user will be able to reject the preemption (if allowed).

Table 4-2 outlines the preemption scenarios and detailed scenarios in which preemption requests can be rejected. For information about preemption and reserved or locked virtual media sessions, see "Virtual Media" on page 89.

Table 4-2. Preemption Scenarios

Current User	Preempted by	Preemption can be rejected
Remote User	Local User	No
Remote User	Remote Administrator	No
Remote User	Remote Console Switch Administrator	No
Remote Console Switch Administrator	Local User	Yes
Remote Console Switch Administrator	Remote Console Switch Administrator	Yes
Remote Administrator	Local User	No
Remote Administrator	Remote Administrator	Yes
Remote Administrator	Remote Console Switch Administrator	No

Table 4-2. Preemption Scenarios

Current User	Preempted by	Preemption can be rejected
Local User	Remote Administrator	Yes
Local User	Remote Console Switch Administrator	Yes

Preemption of Remote User by a Remote Administrator

If a remote administrator attempts to access a server that is being accessed by a remote user, a message appears asking that the administrator wait while the user is informed that they will be preempted. The remote user cannot reject the preemption request and will be disconnected. The time period given before disconnection is defined by the Video session preemption timeout setting in the **Session** dialog box. For information, see "Viewing and Configuring Remote Console Switch Parameters" on page 102.



NOTE: No time period will be displayed in cases where the server being viewed is attached to an Avocent brand switch.

Preemption of a Local User/Remote Administrator by a Remote Administrator

If an administrator attempts to access a server that is being accessed by the local user or by another remote administrator with equal privileges, the currently connected user can accept or reject the preemption request. A message appears asking the connected local user or remote administrator whether they want to accept the preemption request. If the preemption request is rejected a message appears informing the remote administrator that their request has been rejected and that they cannot access the server.



NOTE: If the server being viewed is attached to an Avocent brand switch, the user is not given the option to accept or reject preemption.



NOTE: In scenarios where a preemption request can be rejected, the **Session Preemption Request** dialog box will appear. This dialog allows you to accept the preemption request by clicking the **Accept** button or to reject the preemption request by clicking the **Reject** button or by closing the dialog box.

Connection Sharing

Connection sharing allows multiple users to interact with a target device at the same time. When you are a primary user, you may be notified by a dialog box that another user would like to share your connection. You may select **Yes** to accept sharing, **No** to reject sharing, or click the **Passive Share** box to allow the new user to share without having any control over the connection.

When you attempt to open a Video session with a device that is already being viewed by another user, you are notified that the device is already being viewed. Depending on the configuration of sharing settings, you may be offered the option to share or preempt the video session. You may also be offered the option to open a stealth Video session.



NOTE: Stealth video sessions are passive Video sessions, where the primary user is not aware of the presence of the secondary user. The ability to open a stealth video session is governed by the privilege of the user. If a user can preempt another user, they can also open a Stealth Video session.

Access to the device is governed by the nature of the current user's connection to the device. There are two types of Video session users: a Primary user and up to 11 simultaneous Secondary users (a single 2161DS-2 or 4161DS appliance supports up to 12 simultaneous sessions across all attached servers). Only the Primary user can accept or reject preemption requests for all users sharing a connection. The Primary user also maintains control of video parameters and the display resolution of the Video session.

Secondary users may be either Active users who have the ability to input mouse and keyboard data, or Passive users who may not input mouse and keyboard data.

If **Automatic Sharing** is enabled on the Remote Console Switch, Secondary Users do not need the permission of the Primary User to join the session.

If a Primary user leaves the session then the oldest Secondary user with Active user privileges will become the Primary user. If there are no Secondary users with Active user privileges sharing the session when the Primary user leaves the session, then the session will be closed.

For more information about configuring connection sharing, see "Viewing and Configuring Remote Console Switch Parameters" on page 102.

Exclusive Mode

Exclusive Mode allows you to have exclusive control of a Video session. When in **Exclusive Mode**, no other user can share the session (except in **Stealth** mode). If other users are sharing the session when you select **Exclusive Mode**, you are warned that selecting **Exclusive Mode** will cause the other users to become disconnected from the session.



NOTE: Only the Primary user can request an Exclusive session. If other users are sharing at the time **Exclusive Mode** is requested, they are disconnected, regardless of the Primary users access level.

To open a Video session in **Exclusive** mode:

In the **Viewer**, choose **Tools - Exclusive Mode**.

Virtual Media

Virtual media allows you to view, move, or copy data located on virtual media to and from any server. You can manage remote systems more efficiently by allowing operating system installation, operating system recovery, hard drive recovery or duplication, BIOS updating, and server backup. Virtual media can be connected directly to the appliance using USB ports located on the appliance. Virtual media can also be accessed remotely. You can use virtual media support to connect USB media devices to the appliance and make those devices available to any connected appliance.

Any user operating a KVM session can access any media device that is mapped to that target device. To avoid the security risk of unauthorized user access, you can lock a virtual media session to a KVM session.

To change the media in a virtual media device, you must first unmap the virtual media device. You can then insert the new media and remap the virtual media device. The media will be available in the new virtual media session.



NOTE: To use virtual media on a given server, a USB2 SIP or Avocent brand PS2M or USB2IQ module must be used to connect that server to the KVM switch.



NOTE: A virtual media session cannot be opened to a server that is connected to a PEM.

This chapter describes how to configure and launch virtual media from the OSCAR interface and the on-board web interface. Virtual media is also available from the Remote Console Switch Software. For how to use the Remote Console Switch Software, see the Dell Remote Console Switch User's Guide or the help included with the software.

Common Virtual Media Terms

- **Virtual media** - A USB media device that can be attached to the appliance and made available to any target device that is connected to the appliance
- **Virtual media session** - Two USB connections through a single cable. These connections are visible to the computer as a USB CD drive, USB DVD drive or a USB mass storage device.

- **Local media** - Virtual media sessions that use devices attached directly to the USB port of an appliance.
- **Remote media** - Virtual media sessions that use devices attached directly to the client computer.
- **Locked** - A virtual media session that is associated with a specified KVM session. If the KVM session is closed, the virtual media session will end. (For example, if the KVM session is preempted, closed by a user, or stopped when the screen saver starts, the appliance will close the associated virtual media session). However, closing a locked virtual media session will not close the corresponding KVM session.
- **Reserved** - A virtual media session that can only be accessed or closed by a specified user name or an administrator. If both Locked and Reserved are selected, the session will be reserved.

Configuring Virtual Media Locally

The local port administrator (which is anyone that has access to the local user port) will be able to enable or disable virtual media on any server connected to a USB2 SIP. This control will be maintained in the appliance after a power cycle.

Enabling/Disabling Virtual Media Using the OSCAR Interface

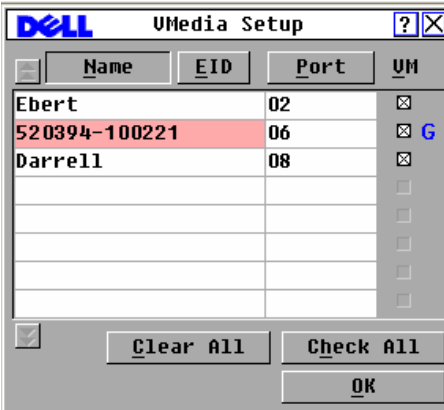
Local administrators can enable or disable virtual media on any server on a per SIP basis. This control is also maintained in the appliance after a power cycle.

The **VMedia Setup** dialog box displays the name of each virtual media SIP, as well as a checkbox that controls whether virtual media is enabled or disabled for that individual SIP. If a virtual media session is currently active, the user letter will be displayed in blue to the right of the checkbox.



NOTE: Before disabling virtual media on a server, the local user must first disconnect any active virtual media sessions via the Commands - User Status screen.

Figure 5-1. VMedia Setup Dialog Box



To enable/disable virtual media:

- 1 Press <Print Screen> to launch the OSCAR interface. The Main dialog box appears.
- 2 Click Setup - VMedia.
- 3 Select the appropriate checkbox to enable virtual media for that SIP.
or
Deselect the appropriate checkbox to disable virtual media for that SIP.
- 4 Click OK to accept the options you have selected and return to the Setup dialog box.

Setting Virtual Media Options Using the OSCAR Interface

You can determine the behavior of the appliance during a virtual media session using the options provided in the Virtual Media dialog box. Table 5-1 outlines the options that can be set for virtual media sessions.

Figure 5-2. Virtual Media Dialog Box

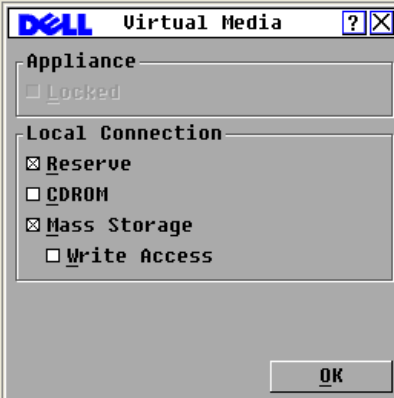


Table 5-1. OSCAR Interface Virtual Media Options

Function	Purpose
Locked	Synchronizes the KVM and virtual media sessions so that when a user disconnects a KVM connection, the virtual media connection to that server is also disconnected. A local user attempting to switch to a different server is also disconnected.
Reserve	Ensures that a virtual media connection can only be accessed with your username and that no other user can create a KVM connection to that server. When the associated KVM session is disconnected, the virtual media session may be disconnected according to the Locked setting in the Virtual Media dialog box.
CD ROM	Allows virtual media sessions to the first detected CD-ROM drive. Enable this checkbox to establish a virtual media CD-ROM connection to a server. Disable to end a virtual media CD-ROM connection to a server.
DVD ROM	Allows virtual media sessions to the first detected DVD-ROM drive. Enable this checkbox to establish a virtual media DVD-ROM connection to a server. Disable to end a virtual media DVD-ROM connection to a server. Only DVD-ROM data is supported by virtual media. Playback of DVD movies over virtual media is not supported.

Table 5-1. OSCAR Interface Virtual Media Options (continued)

Function	Purpose
Mass Storage	Allows virtual media sessions to the first detected mass storage drive. Enable this checkbox to establish a virtual media mass storage connection to a server. Disable to end a virtual media mass storage connection to a server.
Write Access	Allows a target server to write data to the virtual media during a virtual media session. Read access is always allowed during a virtual media session.

To set virtual media options using the OSCAR interface:

- 1** Press <Print Screen> to launch the OSCAR interface. The **Main** dialog box appears.
- 2** Connect a virtual media device to the USB port on the switch.
- 3** Click **VMedia**.
- 4** Click the appropriate checkbox to enable or disable each of the options. For information about each individual setting, see Table 5-1.
- 5** Click **OK** to accept the options you have selected and return to the **Main** dialog box.

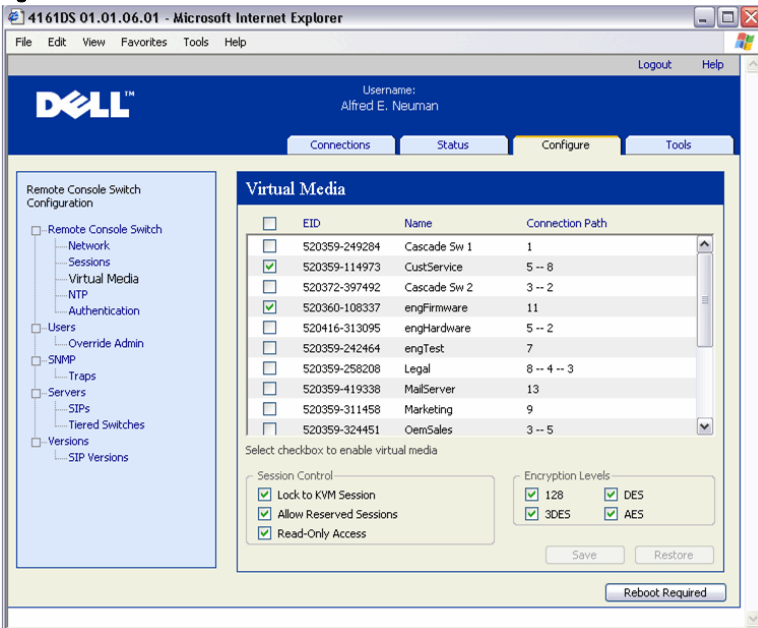
Configuring Virtual Media Remotely

Virtual media can also be configured using the on-board web interface. The on-board web interface includes options similar to those in the OSCAR interface. Users can enable or disable virtual media on any server on a per SIP basis. This control is also maintained in the appliance after a power cycle.

Enabling/Disabling Virtual Media Using the On-board Web Interface

The on-board web interface virtual media configuration screen displays the EID, name, and connection path of each virtual media SIP, as well as a check box that controls whether virtual media is enabled or disabled for that individual SIP.

Figure 5-3. Virtual Media Window - On-board Web Interface



To enable/disable virtual media:

- 1 Click the Configure tab, then click Remote Console Switch - Virtual Media.
- 2 Select the appropriate checkbox to enable virtual media for that SIP or
Deselect the appropriate checkbox to disable virtual media for that SIP.
- 3 Click Save.

Setting Virtual Media Options Using the On-board Web Interface

You can determine the behavior of the appliance during a virtual media session using the options provided in the on-board web interface virtual media configuration screen. Table 5-2 outlines the options that can be set for virtual media sessions.

Table 5-2. On-board Web Interface Virtual Media Options

Function	Purpose
Lock to KVM Session	Synchronizes the KVM and virtual media sessions so that when a user disconnects a KVM connection, the virtual media connection to that server is also disconnected. A local user attempting to switch to a different server is also disconnected.
Allow Reserved Sessions	Ensures that a virtual media connection can only be accessed with your username and that no other user can create a KVM connection to that server.
Read-Only Access	Prevents a target server from writing data to the virtual media drive during the virtual media session.
Encryption Levels	Allows the user to choose which of the SSL encryptions (128-bit, DES, 3DES, or AES) will be supported in the virtual media session.

To set virtual media options using the on-board web interface:

- 1 Click the **Configure** tab, then click **Remote Console Switch - Virtual Media**.
- 2 Click the appropriate checkbox to enable or disable each of the options. For information about each individual setting, see Table 5-2.
- 3 Click **Save**.

Launching Virtual Media

Virtual media is launched remotely from the appliance using the Viewer. The virtual media client will allow a user to map a local drive to a virtual drive on the target server.

To launch virtual media:

- 1 Launch the Viewer from the on-board web interface. (See "Using the Viewer" on page 65 for more information.)

2 Select Tools - Virtual Media.

Figure 5-4. Dell Virtual Media Client Showing No Connection

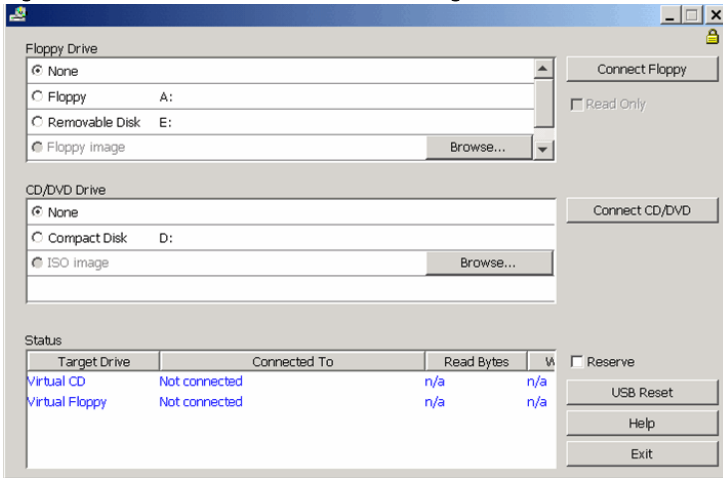
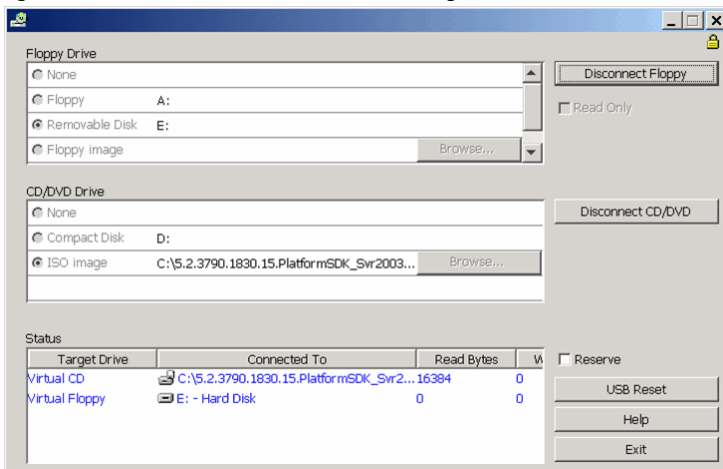


Figure 5-5. Dell Virtual Media Client Showing Two Connections



There are two devices available for mapping on the target server: a floppy/flash drive or a CD/DVD drive. The virtual media client allows one of each to be mapped at a time. Alternatively, the virtual media client will also allow a floppy image (*.img) file or a CD image (*.iso) file to be mapped to a virtual device.

The virtual media interface consists of three main areas: the Floppy Drive section, the CD/DVD section, and the Status section. If the virtual media session is locked to a KVM session, there will be a locked icon at the top right of the virtual media client screen.

Virtual Floppy Drive

The floppy drive section allows a user to select which drive to map to the virtual floppy. It includes radio buttons for selecting the type of device (Floppy, Removable, or Floppy image), as well as a browse button used for selecting the *.img image file. Only one device in the floppy drive section can be connected at one time.

The user has the option of prohibiting the target server from writing data back to the local drive by selecting the Read Only checkbox. If the administrator has configured all devices to be read only, this box will be checked and grayed out.

To connect a floppy device to the virtual media drive:

- 1 Select either **Floppy** or **Removable Disk**.
- 2 (Optional) Select **Read Only**.
- 3 Click **Connect Floppy**.

To connect a floppy image file to the virtual media drive:

- 1 Select **Floppy image**.
- 2 Click **Browse** and select the desired image *.img file.

NOTE: Image files are always read only.

- 3 Click **Connect Floppy**.

To disconnect any device or image file from the virtual media device:

Click **Disconnect Floppy**.

Virtual CD/DVD Drive

The CD/DVD drive section allows a user to select which drive to map to the virtual CD/DVD. It includes radio buttons for selecting the type of device (CD/DVD or ISO image), as well as a browse button used for selecting the *.iso image file. Only one device in the CD/DVD drive section can be connected at one time.

To connect a CD/DVD device to the virtual media drive:

- 1 Select **Compact Disk**.
- 2 (Optional) Select **Read Only**.
- 3 Click **Connect CD/DVD**.

To connect a CD/DVD image file to the virtual media drive:

- 1 Select **ISO image**.
- 2 Click **Browse** and select the desired image *.iso file.

NOTE: Image files are always read only.

- 3 Click **Connect CD/DVD**.

To disconnect any device or image file from the virtual media device:

Click **Disconnect CD/DVD**.

Virtual Media Connection Status

The status section displays specific information about the virtual media connections. If there is no current connection, the columns will read “No connection” or “n/a” as applicable.

If there is a current connection, the status section displays the following information:

- Target Drive - the virtual device connected to the target server
- Connected To - the name of the local drive connected to the virtual device
- Read Bytes - the number of bytes read by the target server from the local device
- Write Bytes - the number of bytes written to the local device by the target server

Reserving a Virtual Media Session

If you want to continue a virtual media session after the KVM session is closed, you can reserve the virtual media session. If the virtual media session is reserved, it will remain active when the associated KVM session is closed. In addition, the virtual media session can only be accessed by the user to which it is reserved.

To reserve a virtual media session:

Select the **Reserve** checkbox.

Resetting the USB Bus

The USB reset feature resets every USB device on the target device, including the mouse and keyboard. It should only be used when the target device is not responding.

To reset the USB bus:

Select **USB Reset**.

Managing Your Remote Console Switch Using the On-board Web Interface

Once you have installed a new Remote Console Switch, you have the ability to view and configure unit parameters, determine who has access and control rights, view and control currently active video sessions, and execute a variety of control functions such as rebooting and upgrading your Remote Console Switch from the on-board web interface. The on-board web interface has four tabs: **Connections**, **Configure**, **Status**, and **Tools**.

For how to launch the on-board web interface, see "Launching the On-board Web Interface" on page 32. For information about the Connections tab, see "Accessing Servers from the On-board Web Interface" on page 65.



NOTE: The on-board web interface is not supported on 2161DS Remote Console Switches so switches of this model cannot be migrated. Use the Remote Console Switch Software to manage 2161DS Remote Console Switches; see the Dell Remote Console Switch Software User's Guide or help for more information. All other Remote Console Switches support the on-board web interface and may be migrated. See "Migrating Remote Console Switches to the On-board Web Interface" on page 135 for more information.

Migrating Switches from the Remote Console Switch Software

If you have an existing installation of Remote Console Switches that supports the on-board web interface, you can migrate the switches from the Remote Console Switch Software to the on-board web interface. To do so, following the procedures in "Upgrading Firmware" on page 120, "Migrating Remote Console Switches to the On-board Web Interface" on page 135, and "Using the Resync Wizard" on page 137.



NOTICE: Once you migrate a Remote Console Switch, you will manage switches using the on-board web interface instead of the Remote Console Switch Software AMP. However, you can still use the Remote Console Switch Software to modify

server properties, manage the local database, organize your system, and connect to KVM sessions. See the Dell Remote Console Switch Software User's Guide for more information.

Viewing and Configuring Remote Console Switch Parameters

The **Configure** tab allows you to display a list of categories covering a wide range of parameters for your Remote Console Switch. When a category is selected from the list, the parameters associated with the category will be read from the unit. You will then be able to modify those parameters and send the changes securely back to the Remote Console Switch.

Changing Remote Console Switch Parameters

The **Remote Console Switch** category allows you to view the product type, and serial number for the Remote Console Switch.

From the **Network** sub-category, you can choose either **IPv4** (default) or **IPv6** mode. You will be able to change the following network settings: **IP Address**, **Subnet Mask** (when using IPv4 mode) or **Prefix Length** (when using IPv6 mode), and **Gateway**. You will also be able to choose a **LAN Speed**, specify up to three IP addresses for DNS servers, and choose whether to assign a **Static** (default) IP address or, when appropriate, a **Dynamic** IP address to the Remote Console Switch.



NOTE: After changing Network settings, the **Reboot Required** button will be displayed on all pages, indicating that the switch must be rebooted before the changes will take effect. Click the button to reboot the switch.

The **Sessions** sub-category allows you to apply controls to your video sessions. By enabling the **Video session timeout option**, you allow the Remote Console Switch to close an inactive video session after a specified number of minutes. The **Video session preemption timeout option** allows you to specify the time (5 - 120 seconds) for which a preemption warning message appears before a video session is preempted. For more information about preemption, see "Preemption" on page 84. If this option is not enabled, preemption occurs without warning.

The **Encryption Levels** option allows you to specify the type of encryption to be used for video, keyboard, and mouse sessions. You can select multiple methods when a new client connection is requested. The Remote Console Switch negotiates for the highest enabled encryption method.

The **Connection Sharing** options indicate which sharing options are enabled. **Enable Share Mode**, **Automatic Sharing**, **Exclusive Connections**, and **Stealth Connections** all appear checked when the particular option is enabled. **Automatic Sharing**, **Exclusive Connections** and **Stealth Connections** are enabled only when **Enabled Share Mode** is selected. For more information, see "Connection Sharing" on page 86.

The **Input Control Timeout** option controls the time period allowed for between inputs from an active session before another session gains control. The values range from 1-5 seconds and the option is only available if **Share Mode** is selected.

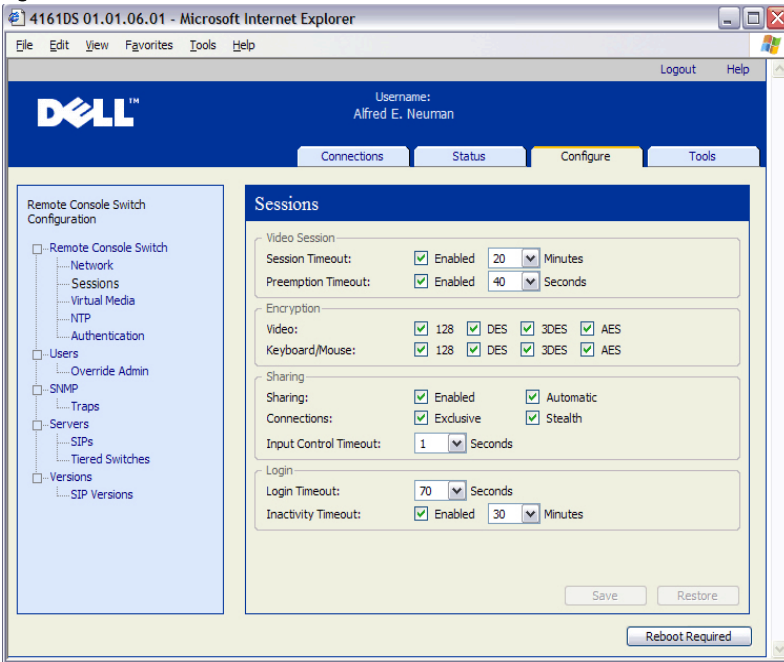
The **Login Timeout** option specifies the time period allowed for an LDAP server to respond to a log in request. The default time is 30 seconds, but some WANs may require a longer time period.

By enabling the **Inactivity Timeout** option, you may specify the time period allowed for an inactive on-board web interface session to remain open. If the specified time elapses without the user navigating to another web page or making changes, the session will close and return to the Log In window.



NOTE: Changes you make to session parameters affect future connection requests only, and not existing connections.

Figure 6-1. Remote Console Switch Sessions Window



Setting Up User Accounts

When you select the **Users** category, the on-board web interface will retrieve and display a list of usernames and current access levels from the Remote Console Switch. You can add, modify, or delete users in this listing. You can assign three access levels: **User**, **User Administrator**, and **Remote Console Switch Administrator**. The **User Administrator** and **Remote Console Switch Administrator** access levels allows you to assign individual server access rights to a user.

Table 6-1. User Access Level Rights

Operations	Remote Console Switch Administrator	User Administrator	User
Preemption	All	Equal and lesser	No

Table 6-1. User Access Level Rights

Operations	Remote Console Switch Administrator	User Administrator	User
Configure network & global settings (security mode, time-out, Simple Network Management Protocol (SNMP))	Yes	No	No
Reboot	Yes	No	No
FLASH upgrade	Yes	No	No
Administer User Accounts	Yes	Yes	No
Monitor server status	Yes	Yes	No
Target Device Access	Yes	Yes	Assigned by Admin



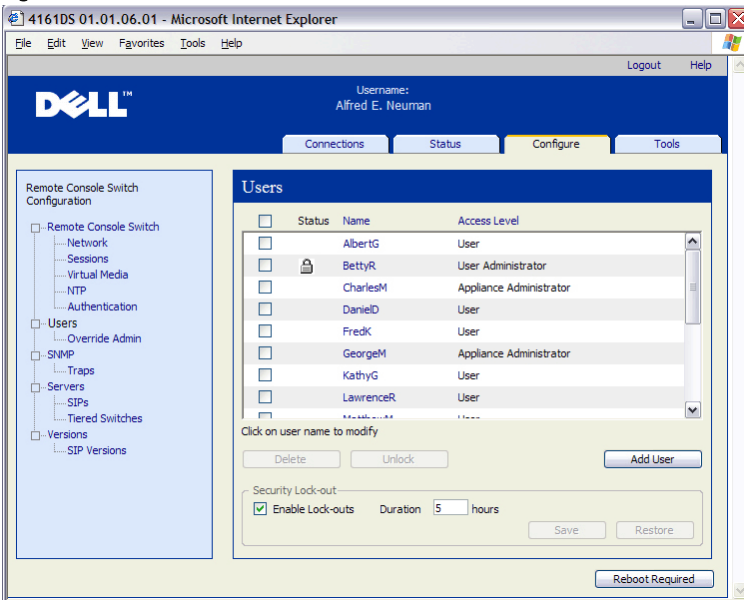
NOTE: Preemptions listed in Table 6-1 only apply to remote clients. They do not apply to users accessing the server locally.

Users can become locked out by the **Security Lock-out** feature if they try to enter an invalid password five consecutive times. You can configure **Security Lock-out** settings as well as unlock any user through the Users category.



NOTE: A User Administrator cannot add or change a Remote Console Switch Administrator account.

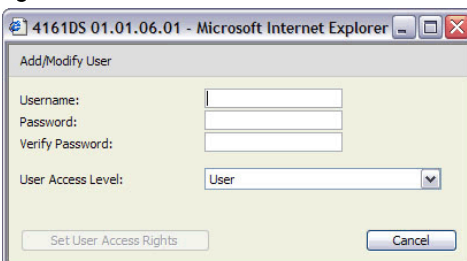
Figure 6-2. Users Window



To add or modify a user:

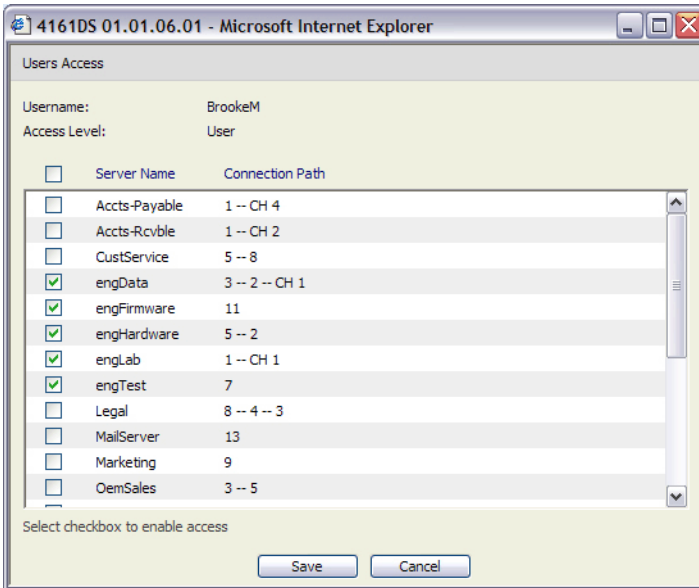
- 1 Click the **Configure** tab in the on-board web interface, then click the **Users** category in the left column.
- 2 Click the **Add User** button on the right side of the window to add a new user.
-OR-
Click a user name in the **Users** column to modify an existing user.
The **Add/Modify User** window appears.

Figure 6-3. Add User Window



- 3 Type the username and password you wish to assign to the user and then verify the password by typing it in the **Verify Password** field. The password must be 5-16 characters and contain alphabetical characters of mixed case and at least one number.
- 4 Select the appropriate access level you wish for this user from the drop-down list. If you select the **User** option, the **Set User Access Rights** button becomes active.
 - a Click the **Set User Access Rights** button to select individual servers for that user. The **User Access Rights** window appears.

Figure 6-4. User Access Rights Window



- b To allow the user access to a server, select the check box next to the server name. Alternatively, you may select the first check box to enable access on all servers.
- c To prevent the user from accessing a server, clear the check box next to the server name.
- d Click **Save**.

- 5 Click **Save** to save the settings and return to the main **on-board web interface** window.

To change the user password:

- 1 Click the **Configure** tab in the on-board web interface, then click the **Users** category in the left column.
- 2 Click a user name in the **Users** column to modify an existing user. The **Add/Modify User** window appears.
- 3 Type the password for that user in the **Password** box and then repeat the password in the **Verify Password** box. The password must be 5-16 characters and contain alphabetical characters of mixed case and at least one number.
- 4 Click **Save** to return to the on-board web interface.

To delete a user:

- 1 Click the **Configure** tab in the on-board web interface, then click the **Users** category in the left column.
- 2 Select the check box next to the user name you wish to delete.
- 3 Click the **Delete** button on the left side of the window. A confirmation window appears.
- 4 Click **Yes** to confirm the deletion.

-or-

Click **No** to exit the window without deleting the user.

Locking and Unlocking User Accounts

If a user enters an invalid password five consecutive times, the **Security Lock-Out** feature, if enabled, will temporarily disable that account. If a user attempts to log in again, an appropriate error message is displayed.



NOTE: All accounts (User, User Administrator, and Remote Console Switch Administrator) are subject to this lock-out policy.

A Remote Console Switch Administrator can specify the number of hours (1 to 99) that accounts will remain locked. When **Enable Lock-outs** is unchecked, the security lock-out feature will be disabled and no users will be locked out.

If an account becomes locked, it will remain locked until the duration time has elapsed, the Remote Console Switch is power-cycled, or an Administrator unlocks the account. A User Administrator may unlock only user accounts, whereas a Remote Console Switch Administrator may unlock any type of account.

To unlock an account:

- 1 Click the **Configure** tab in the on-board web interface, then click the **Users** category in the left column.
- 2 Select the check box next to the user name you wish to unlock.
- 3 Click the **Unlock** button. The lock icon next to the username will disappear.

To specify the length of time a user account remains locked:

- 1 Click the **Configure** tab in the on-board web interface, then click the **Users** category in the left column.
- 2 Click to enable the **Enable Lock-outs** check box.
- 3 Type the number of hours that a user will be locked out (1 to 99).



NOTE: Only Remote Console Switch Administrators may specify lock-out parameters.

To disable the Security Lockout feature:

- 1 Click the **Configure** tab in the on-board web interface, then click the **Users** category in the left column.
- 2 Clear the **Enable Lock-outs** check box. The **Duration** field is disabled.



NOTE: Disabling Security Lock-Out will have no affect on users that are already locked out.

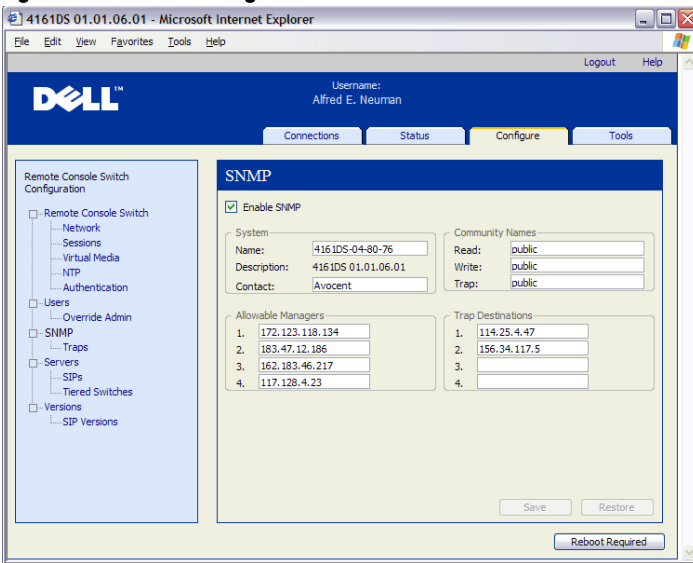
Enabling and Configuring SNMP

SNMP is a protocol used to communicate management information between network management applications and Remote Console Switches. Other SNMP managers can communicate with your Remote Console Switch by accessing MIB-II and the public portion of the enterprise MIB. When you select the **SNMP** category, the on-board web interface will retrieve the SNMP parameters from the unit.

In the SNMP category, you can enter system information and community strings. You may also designate which stations can manage the Remote Console Switch as well as receive SNMP traps from the switch. For more information on traps, see "Enabling Individual SNMP Traps" on page 111 in this chapter. If you check **Enable SNMP**, the unit will respond to SNMP requests over UDP port 161.

NOTE: The on-board web interface does not use standard SNMP to control switches and therefore does not use UDP port 161. The on-board web interface uses a secure, proprietary protocol to communicate with the Remote Console Switches over a different network port.

Figure 6-5. SNMP Configuration Window



To configure general SNMP settings:

- 1 Click the **Configure** tab in the on-board web interface, then click the **SNMP** category in the left column.
- 2 Click to enable the **Enable SNMP** check box to allow the Remote Console Switch to respond to SNMP requests over UDP port 161.
- 3 Type the system's fully qualified domain name in the **Name** field, as well as a node contact person in the **System** section.

- 4 Type the **Read**, **Write**, and **Trap** community names. These specify the community strings that must be used in SNMP actions. The **Read** and **Write** strings only apply to SNMP over UDP port 161 and act as passwords that protect access to the Remote Console Switch. The values can be up to 64 characters in length. These fields may not be left blank.
- 5 Type the address of up to four management workstations that are allowed to manage this Remote Console Switch in the **Allowable Managers** fields. Alternatively, you may leave these fields blank to allow any station to manage the Remote Console Switch.
- 6 Type the address of up to four management workstations to which this Remote Console Switch will send traps in the **Trap Destination** fields.
- 7 Click **Save** to save the settings and close the window.
-or-
Click **Restore** to cancel the changes and exit the window. The last saved settings will be restored.

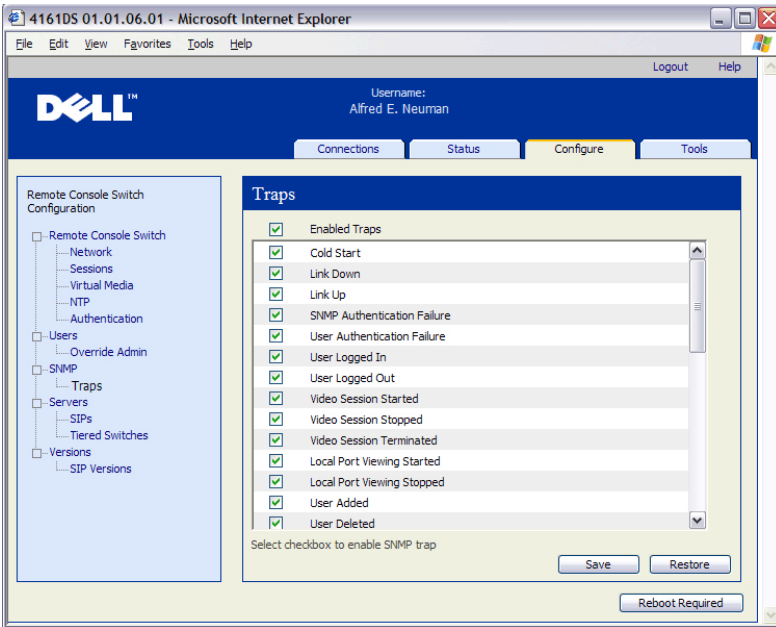


NOTE: After changing SNMP settings, the Reboot Required button will be displayed on all pages, indicating that the switch must be rebooted before the changes will take effect. Click the button to reboot the switch.

Enabling Individual SNMP Traps

An SNMP trap is a notification sent by the Remote Console Switch to a management station indicating that an event has occurred in the Remote Console Switch that may require further attention. The Dell OpenManage™ IT Assistant software is the event manager. You can specify what SNMP traps are sent to the management stations by simply clicking the appropriate check boxes in the list. Alternatively, you can select or clear the check box next to Enabled Traps to easily select or deselect the entire list.

Figure 6-6. SNMP Traps Window



Viewing and Resynchronizing Server Connections

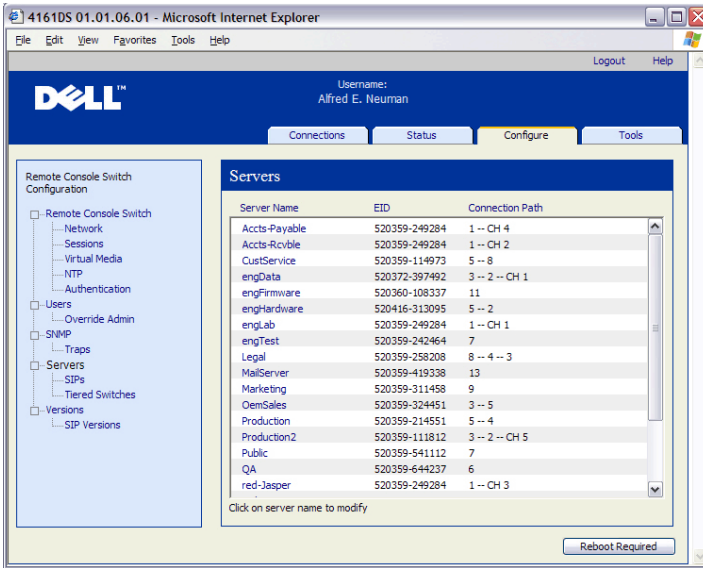
The Servers category retrieves and displays the servers that exist in the on-board web interface database as well as information on how the servers are connected to the selected Remote Console Switch.

The Path column displays the current server connection. This can be to either a SIP or a tiered switch. If connected to a SIP, the SIP's ARI port is displayed. If connected to a tiered switch, the switch channel is also displayed. Clicking on a Server Name displays a dialog that allows you to change the name of the server.



NOTE: The Reboot Required button will only appear if reboot is required.

Figure 6-7. Servers Window



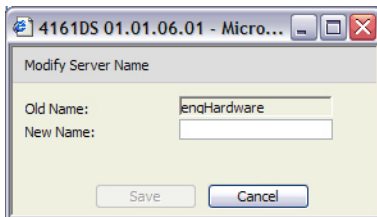
Modifying a Server Name

You can use the on-board web interface to rename a server from a remote workstation rather than from the OSCAR interface of the Remote Console Switch.

To modify a device name:

- 1 In the **Server** category, click the name of the server whose name you wish to change. The **Modify Server Name** window appears.

Figure 6-8. Modify Server Name Window



- 2 Type the name you want to assign to the server. Names must be 1-15 characters, include alphabetical characters, and may not include spaces or special characters with the exception of hyphens.
- 3 Click **Save**. The name you have supplied is updated in both the Remote Console Switch and local client database.

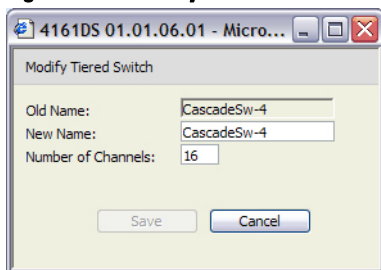
Viewing and Configuring Tiered Switch Connections

The Tiered Switches window lets you view the tiered switches in your system. Clicking on a switch name displays a window that allows you to change the Name or Number of Channels.

To configure a tiered switch connection:

- 1 Click the **Configure** tab in the on-board web interface, then click the **Tiered Switches** sub-category in the left column.
- 2 Click the name of the switch you want to configure. The Modify Tiered Switch window opens.

Figure 6-9. Modify Tiered Switch Window



- 3 Type the new name for the switch.
- 4 Type the number of channels, between 4-24, for the switch.
- 5 When you have finished configuring the switches, click **Save** to save the new settings.
-or-
Click **Cancel** to exit without saving.

Viewing the SIPs and IQ Modules

The **Server - SIPs** category lets you view the SIPs and IQ modules in your system, their port, and Electronic ID number (EID) as well as their type and connection device.

You can also view the SIP status. A green circle indicates that the SIP is online. A yellow circle indicates the SIP is being upgraded and a red X indicates that the SIP is offline. To clear offline SIPs click **Clear Offline SIPs** and click **OK** when prompted. The **Clear Offline SIPs** button is only available for Remote Console Switch Administrators.



NOTE: It is not possible to clear Offline SIPs or IQ modules that are attached to a tiered analog Console Switch.



NOTE: This operation will clear all offline SIPs on the Remote Console Switch, including those associated with any powered down Servers.



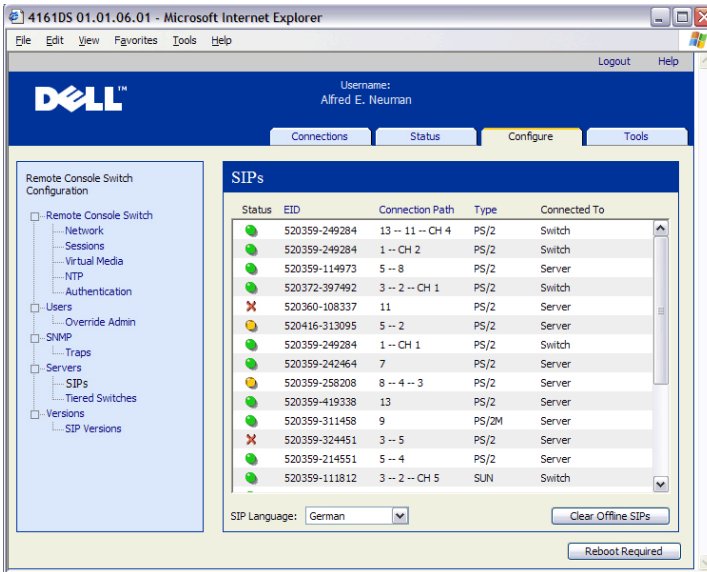
NOTE: User access rights will also be updated to remove the Servers associated with the cleared offline SIPs.

The **SIP Language** drop-down menu allows you to set language and keyboard parameters for all the Sun/USB SIPs of the whole Remote Console Switch. The **SIP Language** drop-down menu is only available for Remote Console Switch Administrators.



NOTE: Reboot Required button will only appear if reboot is required.

Figure 6-10. Servers - SIPs Window - 4161DS Console Switch



NOTE: The Remote Console Switch supports Avocent brand IQ modules as well as Dell SIPs. Therefore, although Dell SIPs are available with PS/2 and USB connections, the addition of IQ modules provides support for Sun and Serial connections.

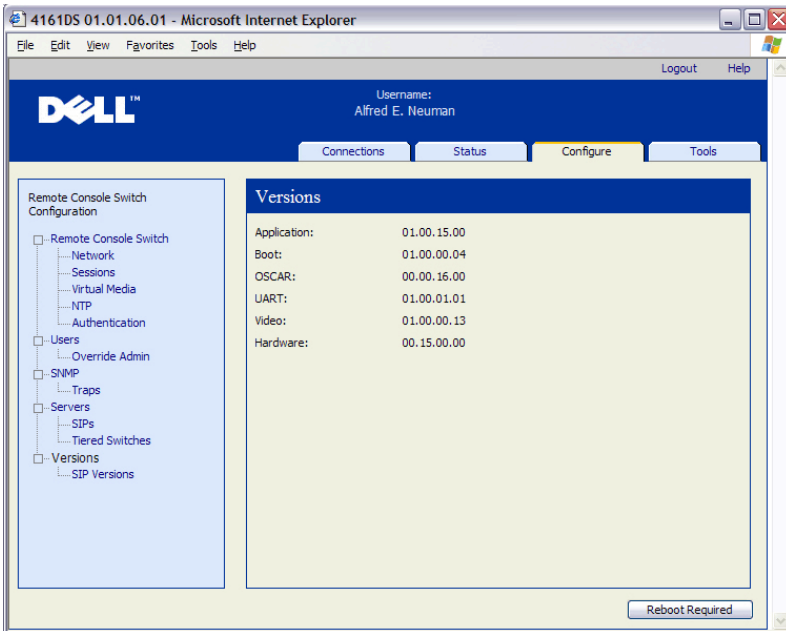
NOTE: To determine if an item identified as PS/2 or USB is a Dell SIP or an Avocent brand IQ module, access the SIPs Versions panel. For more information see "SIPs Subcategory" on page 117.

Viewing Remote Console Switch Version Information

The Versions category displays versions of the Remote Console Switch, FPGA, and ASIC firmware.

NOTE: Reboot Required button will only appear if reboot is required.

Figure 6-11. Firmware Version Window



SIPs Subcategory

The SIPs sub-category allows you to view version information. Clicking on the EID displays a window that allows you to upgrade the SIP firmware and to reset the SIPs if connected to a tiered switch.

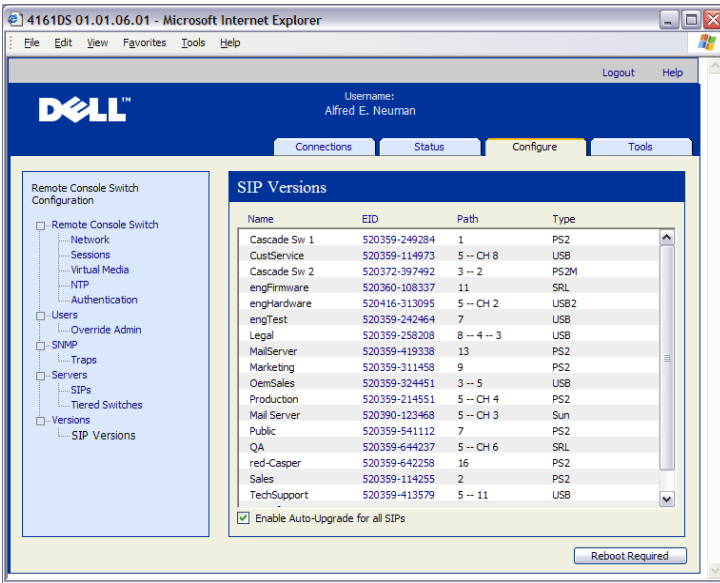
Selecting the **Enable Auto-Upgrade for all SIPs** check box causes all subsequently connected SIPs to have their firmware upgraded to that available on the Remote Console Switch. This guarantees that SIP firmware is compatible with Remote Console Switch firmware.

For information about upgrading SIPs, see "Upgrading Firmware" on page 120.



NOTE: Reboot Required button will only appear if reboot is required.

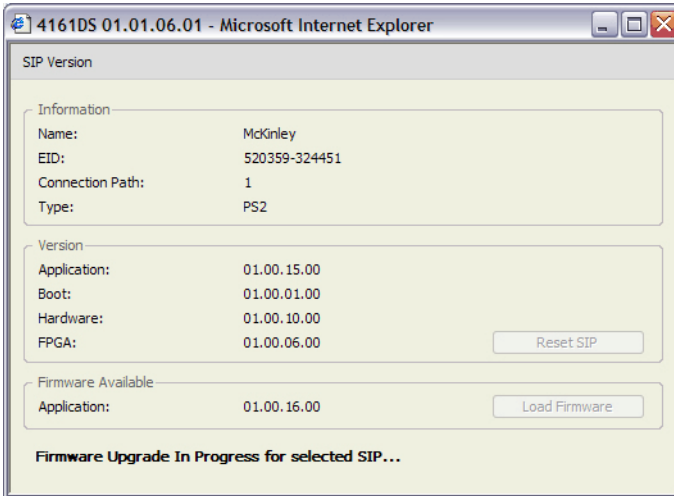
Figure 6-12. SIPs Firmware Version Window



To view version information for a SIP:

- 1 Click the **Configure** tab in the on-board web interface, then click the **SIPs** subcategory from the **Versions** category in the left column.
- 2 Click the EID of the SIP for which you want to view the firmware version.

Figure 6-13. SIP Version Window



On occasions when a tiered switch is not recognized by the Remote Console Switch, it may be necessary to reset the SIP which connects the tiered switch to the Remote Console Switch. This can be done using the **Reset SIP** button in the SIPs subcategory.



NOTE: PS/2, USB, and USB2 SIPs are available. In addition the Remote Console Switch is compatible with all IQ modules including Sun and serial IQ modules.



NOTE: The Reset SIPs button is only enabled when the SIP type is PS/2 and when a firmware upgrade is not in progress.



NOTE: This procedure is only relevant where your Remote Console Switch system involves a PS/2 SIP attached to a tiered switch. On these occasions, it may be necessary to reset the SIP when the tiered switch is not recognized.



NOTE: If a reset is performed, when a Remote Console Switch is connected directly to a server and not a Cascade Switch, the mouse/keyboard may fail to respond. When this occurs, the target server requires a reboot.

To reset a SIP:

- 1 Click the **Configure** tab in the on-board web interface, then click the **SIPs** subcategory from the **Versions** category in the left column.
- 2 Click the EID of the SIP you want to reset.

- 3 Click **Reset SIP**. A message appears warning you that this function is reserved for tiered switches and that resetting the SIP may result in the need to reboot the server.
- 4 Click **OK** to continue.
-or-
Click **Cancel** to return to the SIPs subcategory.

Upgrading Firmware

You can upgrade the firmware for either the Remote Console Switch or the SIPs. The SIPs can be upgraded individually or simultaneously. When an upgrade is initiated, you will see a progress bar. As long as an upgrade is in progress, you cannot initiate another.

The **Enable Auto-Upgrade for All SIPs** check box allows you to enable an auto-upgrade for SIP firmware. You can override the auto-upgrade at any stage using the **Load Firmware** button described in the next section.

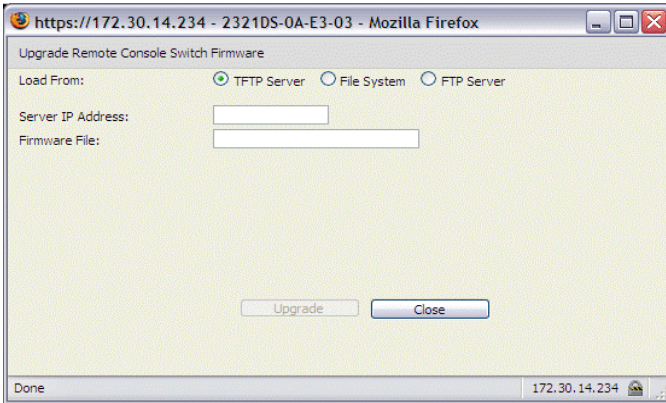


NOTE: For the 2161DS-2, 4161DS, and 2321DS, you can upload new appliance firmware using ASMP (if supported) or TFTP file transfer protocols. ASMP file transfer allows you to select the firmware from a local file system. The 2161DS TFTP file transfer allows you to specify the TFTP server address and the name of the firmware file.

To upgrade Remote Console Switch firmware:

- 1 Click the **Tools** tab in the on-board web interface. The **Tools** window appears.
- 2 Click the **Upgrade Remote Console Switch Firmware** button.
- 3 The **Upgrade Remote Console Switch Firmware** window appears. Select **TFTP Server** or **FTP Server** as the source, and type the TFTP or FTP server IP address where the firmware is located as well as the filename and directory location.
or
Click **File System** and browse to the location on your file system where the **FLASH** file is located. Click **Open**.

Figure 6-14. Upgrade Switch Firmware Window



4 Click the **Upgrade** button. The **Upgrade** button dims and a progress message and progress bar appears.

5 When the upgrade is complete, the Remote Console Switch will reboot.



NOTICE: Do not power down the Remote Console Switch while it is upgrading.

You can upgrade firmware for all SIPs of a given type.

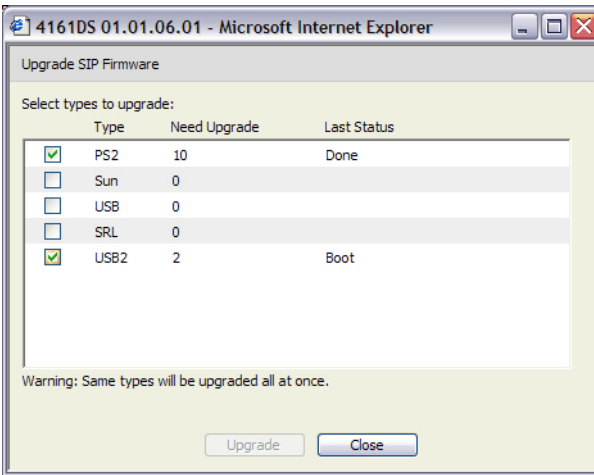
To simultaneously upgrade multiple SIPs:

- 1** Click the **Tools** tab in the on-board web interface. The **Tools** window appears.
- 2** Click the **Upgrade SIP Firmware** button. The **Upgrade SIP Firmware** window appears.
- 3** Click the check box in front of each type (PS/2, USB, USB2, Serial, or Sun) of SIP you wish to upgrade.



NOTE: A disabled check box indicates that all SIPs of that type are running the correct firmware, or that no SIP of that type exists in the system.

Figure 6-15. Upgrade SIP Firmware Window

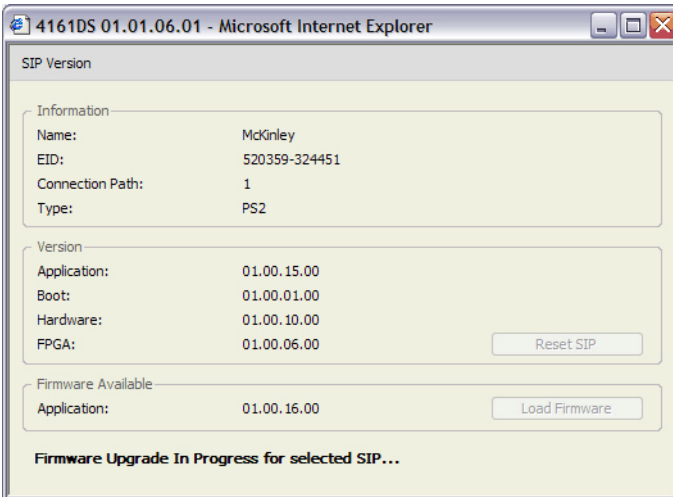


- 4 Click **Upgrade**. The **Upgrade** button dims. The Last Status column will display either In Progress or Succeeded, depending on the status of each SIP upgrade. A firmware upgrade currently in progress message displays until all of the selected SIP types are upgraded.
- 5 When complete, a message appears prompting you to confirm the upgrade completion. Once confirmed, the **Upgrade** button is again enabled.
- 6 Click **Close** to exit the **Upgrade Firmware** window.

To upgrade SIP firmware individually:

- 1 Click the **Configure** tab in the on-board web interface.
- 2 Select the **SIPs** sub-category under **Versions** in the left column.
- 3 Click the **EID** of the SIP for which you wish to view firmware information. The SIP Version window opens.

Figure 6-16. SIP Version Window

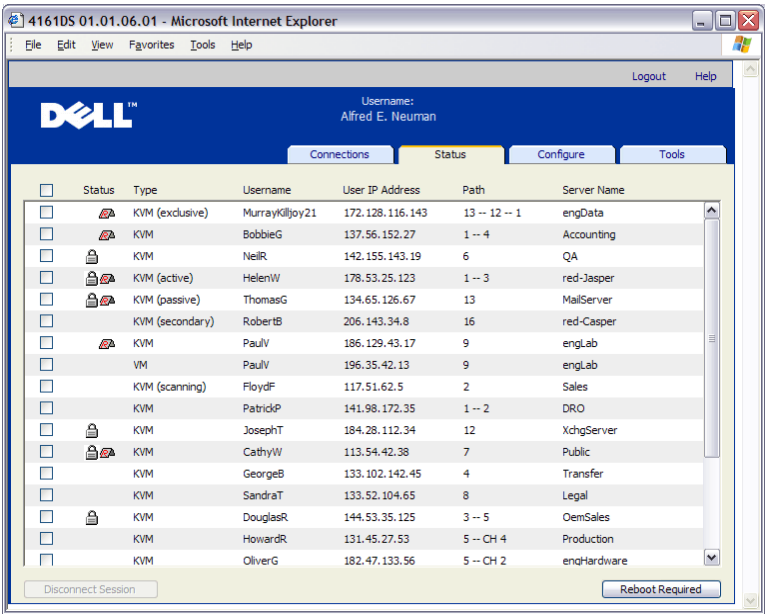


- 4 Compare the current information to the **Firmware Available** field to see the firmware upgrade available for the SIP. (You can load firmware even if the current and available versions are the same. In some cases, you can downgrade the SIP to an older, compatible version.)
- 5 Click the **Load Firmware** button.
- 6 The firmware upgrade begins. During the upgrade, a progress message is displayed below the **Firmware Available** box and the **Load Firmware** button will dim. When the upgrade is finished, a message appears indicating that the upgrade was successful.
- 7 Repeat steps 2-6 for each individual SIP you wish to upgrade.
- 8 When finished, click **OK**.

Controlling User Status

You may view and disconnect the current active user connections using the **Status** tab in the on-board web interface. You can view the session type, the server name, or SIP to which they are connected and their system address. In addition to disconnecting a user session, the on-board web interface also allows one user to take control of a server currently being used by another user. For more information, see "Preemption" on page 84.

Figure 6-17. User Status Window



To disconnect a user session:

- 1 Click the **Status** tab in the on-board web interface. A list of users and their connection information appears.
- 2 Click the check box for one or more users that you wish to disconnect.
- 3 Click the **Disconnect Session** button. A message appears prompting you to confirm the disconnect command.
- 4 Click **OK** to disconnect the user.

-or-

Click **Cancel** to exit without completing the disconnect command.



NOTE: The appropriate level of access is required to disconnect a user. If you do not have permission to disconnect a user, the check box next to that user will be disabled.

Rebooting Your System

You can reboot the Remote Console Switch through the **Tools** tab in the on-board web interface. When clicked, **Reboot Remote Console Switch** will broadcast a disconnect message to any active users, then log out the current user and immediately reboot the Remote Console Switch.

To reboot your system:

- 1 Click the **Tools** tab in the on-board web interface. The **Tools** window appears.
- 2 Click the **Reboot** button. A message prompting you to confirm this reboot appears.
- 3 Click **OK** to reboot.
-or-
Click **Cancel** to cancel the reboot.

Managing Remote Console Switch Configuration Files


Configuration files contain all of the settings for a Remote Console Switch. This includes appliance settings, SNMP settings, LDAP settings, and NTP settings. You may save your configuration file and, should you ever need to replace your Remote Console Switch, you can restore the configuration file to the new switch and avoid manually configuring it.



NOTE: User account information is stored in the user database, not in the configuration file. For more information, see "Managing User Databases" on page 126.

To read and save a configuration file from a Remote Console Switch:


- 1 Click the **Tools** tab in the on-board web interface. The **Tools** window appears.
- 2 Click the **Save Remote Console Switch Configuration** button. The **Save Remote Console Switch Configuration** window appears.
- 3 (Optional) Enter a password in the **Password** field, then repeat the password in the **Verify Password** field. This password is requested when you restore this database to a Remote Console Switch. Click **OK**.

 **NOTE:** You may leave the password field blank if you do not want to require a password for accessing the configuration file.

- 4 Click **Browse** and navigate to a location to save the Configuration file. The location appears in the **Save To** field.
- 5 Click **Save**.
- 6 The configuration file is read from the Remote Console Switch and saved to the desired location. A progress window displays.
- 7 When complete, a message appears prompting you to confirm the read completion. Click **OK** to return to the main window.

To restore a configuration file to a Remote Console Switch:


- 1 Click the **Tools** tab in the on-board web interface. The **Tools** window appears.
- 2 Click the **Restore Remote Console Switch Configuration** button. The **Restore Remote Console Switch Configuration** window box appears.
- 3 Click **Browse** and navigate to the location where you stored the saved configuration file. The file name and location appears in the **File name** field.
- 4 Click **Restore**. The Enter Password window opens.
- 5 (Optional) Enter the password you created when the configuration database was saved. Click **OK**. The configuration file is written to the Remote Console Switch. A progress window displays.

 **NOTE:** You may leave the password field blank if you do not did not create a password for the configuration file.

- 6 When complete, a message appears prompting you to confirm the write completion. Click **OK** to return to the main window.

Managing User Databases

User database files contain all user accounts assigned in a Remote Console Switch. You can save your user account database file and use it to configure users on multiple Remote Console Switches by writing the user account file to the new switch.

 **NOTE:** The user account file is encrypted and you will be prompted to create a password when you save the file. You will need to re-type this password when you write the file to a new unit.

To save a user database from a Remote Console Switch:

- 1** Click the **Tools** tab in the on-board web interface. The **Tools** window appears.
- 2** Click the **Save Remote Console Switch User Database** button. The **Save Remote Console Switch User Database** window appears.
- 3** Click **Browse** and navigate to a location to save the user database file. The location appears in the **Save To** field.
- 4** Click **Save**. The Enter Password window opens.
- 5** Enter a password in the Password field, then repeat the password in the Verify Password field. This password is requested when you restore this database to a Remote Console Switch. Click **OK**. The user database file is read from the Remote Console Switch and saved to a location. A progress window displays.
- 6** When complete, a message appears prompting you to confirm the read completion. Once confirmed, the **Save Remote Console Switch User Database** window will close and you are returned to the **Tools** window.

To restore a user database file to a Remote Console Switch:

- 1** Click the **Tools** tab in the on-board web interface. The **Tools** window appears.
- 2** Click the **Restore Remote Console Switch User Database** button. The **Restore Remote Console Switch User Database** window appears.
- 3** Click **Browse** and navigate to the location where you stored the saved user database file. The file name and location appears in the **File name** field.
- 4** Click **Restore**. The Enter Password window opens.
- 5** Enter the password you created when the user database was saved. Click **OK**. The user database file is written to the Remote Console Switch. A progress window displays.
- 6** When complete, a message appears prompting you to confirm the write completion. Once confirmed, the **Restore User Database File** window will close and you are returned to the **Tools** window.

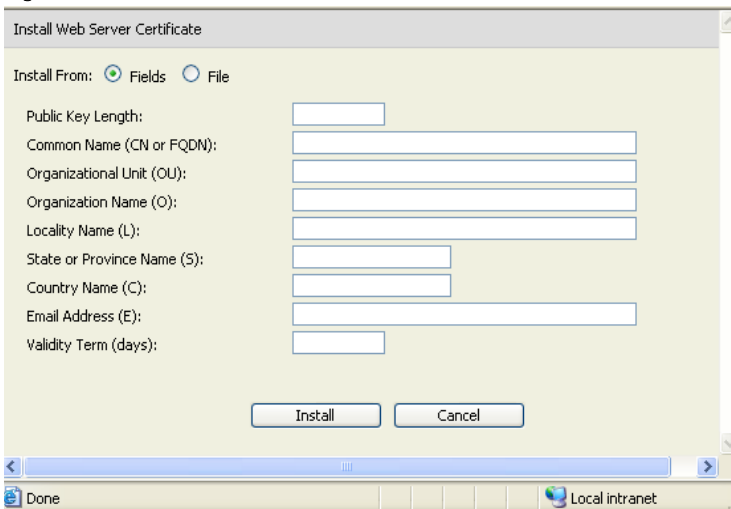
Installing a Web Certificate

A web certificate allows you to enter the on-board web interface on a web browser without having to acknowledge the Remote Console Switch as a trusted web server each time you access the on-board web interface. Using the Install Web Certificate window, you can create a self-signed openssl certificate.

To install a web certificate:

- 1 Click the **Tools** tab in the on-board web interface. The **Tools** window appears.
- 2 Click the **Install Web Server Certificate** button. The **Install Web Server Certificate** window appears.

Figure 6-18. Install Web Server Certificate Window



- 3 Select **Fields**, and enter the following fields:
 - a Public Key Length:** the number of bits you want the certificate to be.
 - b Common Name:** your name. (Since this is your root certificate, use an appropriate name such as, "Company_Name Certificate Authority.")
 - c Organizational Unit** (optional): organization unit name (marketing, for example).

- d Organization Name:** the exact legal unabbreviated name of your organization.
- e Locality Name:** the city where your organization is located.
- f State or Province Name:** the unabbreviated state or province where your organization is located.
- g Country Name:** the two-letter ISO abbreviation for your country.
- h Email Address:** the email address for the CA to contact.
- i Validity Term:** number of days the certificate is valid.

-or-

Select **File**, and download a company certificate file (*.pem).

- 4** Select **Install**. Close the web browser, then relaunch the on-board web interface again for the same IP address.



NOTE: If importing a company certificate file, it may take up to 30 seconds for the on-board web interface to relaunch.

- 5** When prompted, click to view the certificate and follow the instructions to import the certificate into the Root Certificate Authority folder. After the certificate is stored, the user should not see the certificate warning.

Managing PDUs

You can control supported PDUs through the on-board web interface. Chaining of up to nine PDUs per Remote Console Switch PDU port is supported. PDU support allows the user to turn on, turn off and cycle any server or device connected to the PDU.



NOTE: This feature is only available on the 2321DS Remote Console Switch.



NOTE: Refer to dell.avocent.com for a list of supported PDUs.

To configure a PDU:

- 1** Click the **Configure** tab in the on-board web interface, then click the **PDUs** category in the left column for a list of PDUs.
- 2** Click on the PDU you wish to access. The **PDU settings** window opens.

- 3 In the **PDU settings** box, change the PDU name, set the cycle delay time, enable or disable the current protection, enable or disable the audible alarm and set the minimum amps and maximum amps in the **Inlet Parameters** field.

To configure a device connected to a PDU:

- 1 Click the **Configure** tab in the on-board web interface, then click the **PDU**s category in the left column for a list of PDU's.
- 2 Click on the PDU you wish to access. The **PDU Settings** window opens.
- 3 Click the **Outlet Settings** button at the bottom of the **PDU Settings** window for a list of devices connected to the PDU. The **Outlet Settings** window opens.
- 4 To modify an outlet name, complete the following steps:
 - a In the **Name** column, click on the link for the outlet you wish to change. The **Modify Power Outlet Name** window opens.
 - b If the device is a server, click **Server**, then select the name by clicking on the appropriate entry in the **Server Name** column of the table
-or-
If the device is not a server, click **Other Device**, then enter the appropriate text in the **Name** text box.
 - c Click **Save**, then click **Close** to return to the **Outlet Settings** window.
- 5 To modify the power-on interval, enter the value in seconds in the text box in the **Power-On Interval** column for the outlet being configured.
- 6 Click **Save**, then click **Close** to return to the **PDU**s window.

To power-control a device connected to a PDU:

- 1 Click the **Configure** tab in the on-board web interface, then click the **Outlets** subcategory located under **PDU**s in the left column for a list of available outlets.



NOTE: An outlet only appears in this list if a name has been associated with it.

- 2 Check the box next to the outlet(s) you wish to configure.
- 3 Click the **On** button to turn on the selected outlet(s).

- or -

Click the **Off** button to turn off the selected outlet(s).


- or -

Click the **Cycle** button to reboot the selected outlet(s).

- 4** Click **Save**.


Migrating Your Remote Console Switch

If you have an existing installation of Remote Console Switches and are using the Remote Console Switch Software Appliance Management Panel (AMP), follow the procedures in this chapter to migrate the switches from the Remote Console Switch Software to the on-board web interface.


 **NOTE:** The on-board web interface is not supported on 2161DS Remote Console Switches so switches of this model cannot be migrated. Use the Remote Console Switch Software to manage 2161DS Remote Console Switches; see the Dell Remote Console Switch Software User's Guide or help for more information.

Accessing the AMP

You will start from the Remote Console Switch Software AMP to migrate the Remote Console Switch to the on-board web interface.

 To access the AMP:

- 1 Click the **Remote Console Switches** tab in the Explorer.
- 2 Double-click a Remote Console Switch from the **Unit Selector** pane.
-or-
Select a Remote Console Switch from the **Unit Selector** pane, and then click the **Manage Remote Console Switch** task button.
-or-
Right-click a Remote Console Switch in the **Unit Selector** pane. A pop-up menu appears. Select **Manage Remote Console Switch**.
-or-
Click a Remote Console Switch in the **Unit Selector** pane and press <Enter>. A password prompt appears.

 **NOTE:** If there is a **Configure** Remote Console Switch task button, rather than a **Manage** Remote Console Switch task button, that Remote Console Switch has already been migrated to the on-board web interface.

- 3 Type your username and password and click **OK**. The AMP dialog box appears.

Upgrading Firmware Using the AMP

Before starting the migration process (see "Migrating Remote Console Switches to the On-board Web Interface" on page 135), use the AMP to upgrade the firmware to a version that supports the on-board web interface.

The SIPs can be upgraded individually or simultaneously. When an upgrade is initiated, you will see a progress bar. As long as an upgrade is in progress, you cannot initiate another.



NOTE: For the 2161DS-2, 4161DS, and 2321DS, you can upload new appliance firmware using ASMP (if supported), FTP or TFTP file transfer protocols. ASMP file transfer allows you to select the firmware from a local file system. The 2161DS supports the TFTP file transfer which allows you to specify the TFTP server address and the name of the firmware file.

Upgrading Remote Console Switch Firmware

To upgrade Remote Console Switch firmware:

- 1 Click the **Tools** tab in the AMP. The **Tools** dialog box appears.
- 2 Click the **Upgrade Remote Console Switch Firmware** button.

If you have made changes in the Settings panel of the AMP, but have not yet applied them before starting an upgrade, a warning message prompts you to confirm the upgrade because the upgrade process requires an appliance reboot. If you do not apply the pending changes, they will be discarded before upgrading the firmware.

To apply those changes before the upgrade:

- a Click **No** to cancel the appliance firmware upgrade.
- b Click **Apply**.
- c Click the **Upgrade Remote Console Switch Firmware** button.

-or-

To discard those changes before the upgrade, click **Yes**.

- d The **Firmware Upgrade** dialog box appears. Select **TFTP Server** as the source, and type the Trivial File Transfer Protocol (TFTP) server IP address where the firmware is located as well as the filename and directory location.
- or

Click **File System** and browse to the location on your file system where the FLASH file is located. Click **Open**.

3 Click the **Upgrade** button. The **Upgrade** button dims and a progress message appears.

4 When the upgrade is complete, a message prompting you to confirm a reboot appears. The new firmware will not be used until the switch reboots. Click **Yes** to reboot the Remote Console Switch. The **Upgrade Firmware** dialog box will display a progress message including a message that the reboot is complete.

-or-

Click **No** to reboot at a later time. You will need to reboot in order to use the new firmware.



NOTE: When upgrading the Remote Console Switch firmware to a version that supports the on-board web interface, it is recommend not to exit the AMP until the reboot is complete. Otherwise, you must open the AMP after the reboot is complete before the switch will be available in the Migration Wizard.

5 Click **Close** to exit the **Upgrade Firmware** window.



NOTICE: Do not power down the Remote Console Switch while it is upgrading.

Migrating Remote Console Switches to the On-board Web Interface

After you have upgraded the firmware of a Remote Console Switch to a version that supports the on-board web interface, the switch will be available in the Migration Wizard. Complete the Migration Wizard to be able to launch Viewer sessions and manage switches directly from the on-board web interface.



NOTICE: Once you migrate a Remote Console Switch, you will not be able to use the Remote Console Switch Software AMP. Use the on-board web interface instead.

To migrate Remote Console Switches:

1 Select **Tools - Migrate** in the Explorer. The Migration Wizard welcome page opens. Click **Next**.

- 2 All switches that qualify for migration will appear in the **Available Remote Console Switches** list. Select the switch you wish to migrate and click the > button to move the switch to the **Remote Console Switches** to migrate list.



NOTE: If the Remote Console Switch you want to migrate is not available in the Migration Wizard, you may have exited the AMP before the firmware upgrade was complete. Close the Migration Wizard, then open the AMP to allow the upgraded firmware version to be detected. When you open the Migration Wizard again, the Remote Console Switch will be available.

- 3 Click **Next**.
- 4 It is recommend to use the Remote Console Switch information stored in the local database when migrating switches. To do so, select the check box on the Use Local Database Information window.
-or-
If you do not wish to use local database information, clear the check box.

- 5 Type the HTTP and HTTPS port numbers in the **HTTP Port** and **HTTPS Port** fields, respectively, if the port numbers were changed for the Remote Console Switch in the serial console. For more information on changing the port numbers in the serial console, see "To configure the HTTP and HTTPS ports:" on page 19.



NOTE: If you chose to add multiple Remote Console Switches, any that do not use the HTTP and HTTPS ports you specify will fail migration. You can migrate them by running the Migration Wizard again and specifying the correct ports for those Remote Console Switches.

- 6 Click **Next**.
- 7 If the migration was successful, the Completing the Migration Wizard window will open.
-or-
If the migration was not successful, the Migration Wizard was unsuccessful window will open.

- 8 Click **Finish** to exit the wizard.

The Remote Console Switch will no longer be available in the Remote Console Switch Software. You may now manage the switch using the on-board web interface; see "Managing Your Remote Console Switch Using the On-board Web Interface" on page 101.

Using the Resync Wizard

Complete the Resync Wizard to synchronize the local database and the Remote Console Switch database.



NOTE: The Resync button is only available for switches with firmware supporting the on-board web interface.

To launch the Resync Wizard:

- 1** Click the **Remote Console Switches** tab in the Explorer.
- 2** Select a Remote Console Switch from the **Unit Selector** pane, and then click the **Resync** task button.
-or-
Right-click a Remote Console Switch in the **Unit Selector** pane. A pop-up menu appears. Select **Resync**.
- 3** The Resync Wizard will open.
- 4** Click **Next**.
- 5** To include offline servers in the database, select the **Include Offline Servers** check box.
-or-
If you do not wish to include offline servers in the database, clear the **Include Offline Servers** check box
- 6** To overwrite server names in the local database, select the **Replace Database names with the names from the Remote Console Switch** check box.
-or-
To retain server names in the local database, clear the **Replace Database names with the names from the Remote Console Switch** check box.
- 7** Click **Next**. The Polling Remote Console Switch window opens.
- 8** Then Detected Changes window opens and lists changes made to the database.
- 9** Click **Finish**.

LDAP Feature for the Remote Console Switch

Overview

The Dell 2161DS, 2161DS-2, 4161DS, and 2321DS suite of Remote Console Switches can authenticate and authorize users via a local database or by an external scalable distributed directory service using the the Dell Remote Console Switch Software or on-board web interface with LDAP (Lightweight Directory Assistance Protocol) support. LDAP is a protocol standard used for accessing and updating a directory using TCP/IP. The Dell Remote Console Switch Software and on-board web interface supports both standard and Dell extended schema, and offers strong security features including authentication, privacy, and integrity.



NOTE: Windows 2008 Server is required to use LDAP in IPv6 mode.



NOTE: Only Microsoft Active Directory® is supported by the Remote Console Switches.



NOTE: Using Active Directory to recognize Remote Console Switch users is supported on the Microsoft Windows® 2000 and Windows Server 2003 operating systems.

The Structure of Active Directory

An Active Directory (AD) deployment consists of a distributed database containing hierarchical structures of objects. Each object is associated with an object class that determines what kinds of data can be stored in that object. The hierarchical structures begin with objects that represent AD domains, deployed to form a hierarchy of domain names that can be represented in a tree diagram the same way DNS name spaces are usually depicted. The suite of Dell Remote Console Switches is designed to support a single tree of domains that are deployed in either a shallow or deep hierarchical name structure.

Domain Controller Computers

Associated with the Domain hierarchy is the corresponding hierarchy of Domain Controller computers where AD provides LDAP services. Each domain may have multiple peer Domain Controllers and may also be distributed across geographical sites. The suite of Dell Remote Console Switches is designed to support both of these aspects of AD. DNS is used to determine the network coordinates of each Domain Controller so that the Dell Remote Console Switches can gracefully handle situations where some Domain Controllers are not available on the network. DNS SRV records are used for this purpose so the Dell Remote Console Switches always attempt to contact alternative Domain Controllers at the “nearest” site first, depending on the administrative settings configured in the SRV records.

Object Classes

Within each domain, there is another hierarchy of objects designed to store information about various entities and groupings of entities. Such entities are represented in AD by object classes used to define “containers” that help organize groupings of objects. Other object classes represent entities such as network users, computers, printers, or network services. Two types of container object classes are of special interest: Group and Organizational Unit (OU). These two object classes allow the AD administrator to define groupings of entities for the purpose of simplifying the application of access controls and other administrative policies. For example, a domain may be configured to have an OU container named “Engineering” which contains several Group objects named according to function, like “Hardware,” “Software,” and “Support;” each of the groups is configured with a membership list of User objects and perhaps Computer objects. Yet another level of hierarchy can be configured by “nesting” groups; a nesting is formed by including the name of a Group object in the membership of another Group object. It should be noted here that each AD Group object has an associated “scope” that is used to configure the types of nesting relationships it is allowed to have with other groups; for example, when scope is set to “Universal,” the group may participate in nesting that crosses domain boundaries but when scope is set to “Local” it may not participate in such nesting. Rules for nesting are available in the AD product documentation available from Microsoft. The suite of Dell Remote Console Switches is designed to support all nesting rules defined for AD.

Attributes

There is one more hierarchy used in AD. Associated with each object class is a set of “attributes” used to store specific information about the entity that is being represented. For example, associated with the User object class is an attribute type named SAM ACCOUNT NAME and others such as FIRST NAME, SURNAME, PASSWORD, etc. The suite of Dell Remote Console Switches uses the SAM ACCOUNT NAME and PASSWORD attributes to authenticate a user (the formal AD names for these two attributes are sAMAccountName and unicodePWD, respectively).

Schema Extensions

AD is packaged with many object classes, including default containers for Computer and User objects as well as classes for OU containers and classes to represent computer and user entities. AD can be extended to include new object classes such as those provided by Dell to simplify the administration of access controls; such extensions are usually referred to as “schema extensions” and are at the heart of the Dell Extended Schema feature described in this document. These schema extensions provide customized object classes to represent Dell Remote Console Switches, access control information, and a type of container used to associate specific access control information with specific instances of Dell Remote Console Switches and Users. It is important to note that each attribute type and object class used in AD must have a globally unique identifier, known as an Object Identifier (OID). These unique identifiers are ultimately managed by internationally recognized authorities. For AD, the OID space is managed secondarily by Microsoft. Dell has obtained OIDs for the custom object classes and attribute types used in the Dell Extended Schema feature. The following is a summary of the OIDs Dell obtained:

Dell extension is: dell

Dell base OID is: 1.2.840.113556.1.8000.1280

RCS LinkID range is: 12070 to 12079

The suite of Dell Remote Console Switches is also designed to function using only object classes present in the AD packaged classes; this option is known as the Standard Schema. Under this option, the Computer object class is used to represent Dell Remote Console Switches and standard Group objects are

used to associate specific access control information with specific instances of Dell Remote Console Switches and Users. In this case, access control information is stored in a specific attribute type in the Group object.

The hierarchical structures present in AD can complicate your ability to access information stored in the directory objects. To avoid potential delays associated with navigation of the hierarchies, the suite of Dell Remote Console Switches is designed to use an aspect of AD known as the Global Catalog (GC). The GC provides a “quick look-up” service by providing access to a subset of the data stored in the complete AD database and by “collapsing” all of the hierarchies and geographic distribution into a single relatively flat structure. The GC is queried using the same LDAP directory queries that work on the complete AD database. The AD product requires at least one of the Domain Controllers in an enterprise to also be configured to provide GC services and actual deployments of AD can have any or all of the Domain Controllers configured to provide GC services. The suite of Dell Remote Console Switches uses DNS to determine the network coordinates of each GC server so that the Dell Remote Console Switches can gracefully handle situations where some GC servers are not available on the network. DNS SRV records are used for this purpose so that the Dell Remote Console Switches always attempt to contact alternative GC servers at the “nearest” site first, depending on the administrative settings configured in the SRV records.

Standard Schema versus Dell Extended Schema

To provide the greatest flexibility in the multitude of customer environments, Dell provides a group of objects that can be configured by the user depending on the desired results. Dell has extended the schema to include an Association, Device, and Privilege object. The Association object is used to link together the users or groups with a specific set of privileges to one or more SIPs. The Device Object defines the individual Remote Console Switches within the Active Directory structure and the privilege object is linked to device objects via association objects to assign usage permissions.

This model provides an Administrator maximum flexibility over the different combinations of users, privileges, and SIPs on the Remote Console Switch without adding too much complexity.

Before installing the Dell Schema Extensions, Administrators should read through the descriptions and instructions within this chapter to determine which schema is right for their particular installation. Altering a schema

object will cause it to propagate through Active Directory so that once it is created, it cannot be deleted. It can only be deactivated. Because of this, the benefits of changing the schema should be carefully weighed before the effort is undertaken.

The primary benefit gained by installing the Dell Schema Extensions is to eliminate confusion. When using the standard Active Directory schema, a Remote Console Switch most closely matches a computer device object and is configured as one. Since the Remote Console Switch is not a computer, the schema functions will not all apply. Care will have to be taken to correctly configure a Remote Console Switch that is designated in this manner.

In addition, using the Dell Schema Extensions makes it easier to search on and identify switch devices. A switch that is configured using a computer device object will be searched on along with every computer device within the Active Directory structure.

The Remote Console Switch can authenticate equally well using either schema and no functionality is lost by using either method. Administrators are free to choose whichever method works within their particular installation. Instructions have been provided for installations with and without the Dell Schema extensions. Sections and instructions that pertain to only one schema set will be marked as such and may be ignored in installations where they are not used.


Standard Installation

Before a Dell Remote Console switch can use Active Directory for authentication:

- 1** Configure the Override Admin Account
- 2** Configure DNS Settings
- 3** Set the Network Time Protocol
- 4** Configure the Authentication Parameters
- 5** Configure Group Objects
- 6** Create and Download the CA Root certificate
- 7** Set the Login Timeout

Configure the Override Admin Account

Should a network failure occur, an account is provided that may be used regardless of the unit's ability to authenticate against an LDAP server. Before configuring other settings, this account should be configured.

 **NOTE:** You must be logged in as Admin with no password to perform this operation.

To configure the Override Admin Account in the on-board web interface:


- 1 Click the **Configure** tab, then click **Users - Override Admin**.
- 2 Type the username and password you wish to assign to the user and then verify the password by typing it in the **Verify Password** field.
- 3 Click **Save**.


Configuring DNS Settings

Before the LDAP client can resolve names, at least one DNS server must be specified.

The **Network** sub-category displays the name of the Remote Console Switch and allows you to change the network settings including the **IP address**, **Subnet Mask**, **Gateway**, **LAN speed** and **DHCP/BootP** setting. The name displayed for the Remote Console Switch will be the same as the name given in the **System Name** field in the **SNMP** category.

The **Network** sub-category allows the entry and maintenance of up to three DNS Servers. These DNS servers are used to resolve DNS names provided on the LDAP authentication panel.

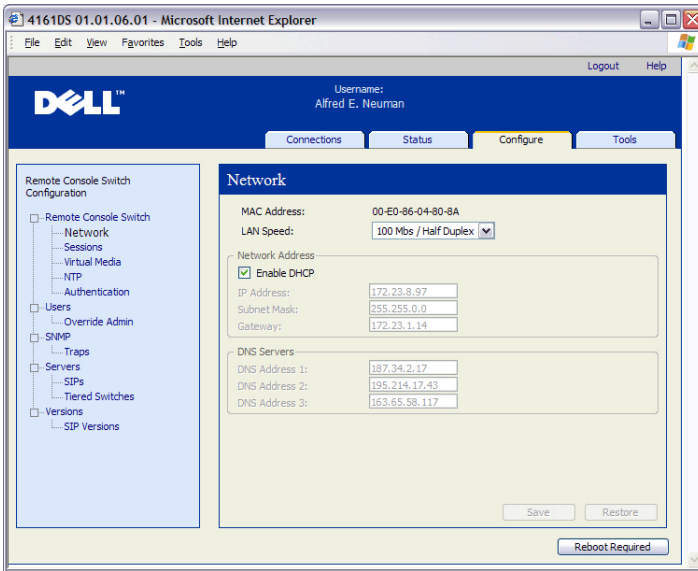
 **NOTE:** At least one DNS server must be configured for the LDAP feature to work.

 **NOTE:** You can also set DNS server addresses using the appliance's serial administrative interface. For information about using the serial administrative interface, please consult your appliance documentation.

To configure the DNS settings in the on-board web interface:

- 1 Click the **Configure** tab, then click **Remote Console Switch - Network**.
- 2 Specify the DNS settings and click **Save**.

Figure 8-1. On-board Web Interface - Network Subcategory



Configuring the Network Time Protocol Settings

The switch must have access to the current time to verify that certificates have not expired. You can configure the switch to request time updates from the network time server (NTP).

To configure NTP settings in the on-board web interface:

- 1 Click the **Configure** tab, then click **Remote Console Switch - NTP**.
- 2 Click the **Enable NTP** box.
- 3 Enter the name of your network time source in the provided boxes. You may also set an hour interval to specify how often to request time updates. If the interval is set to 0, requests will only be made during appliance startup or when changes to the **Global - NTP** menu are made.
- 4 Click **Save**.

Configuring the LDAP Authentication Parameters

The **Authentication** panel allow you to configure your authentication and authorization configuration parameters. You can send the username, password, and other information to the Remote Console Switch, which then uses LDAP to retrieve data from the Directory Service in order to determine what permissions the user has.

Enabling LDAP Authentication

The **Authentication Settings** field allows you to choose Local or LDAP Authentication. Click the **Use LDAP Authentication** checkbox to authenticate against the LDAP-enabled directory service.

Once LDAP is enabled, the RCS and Root Domains should be designated in the provided fields.

Entering Authentication Parameters

If you plan to install the Dell Extended Schema, enter only the RCS and Root Domains that will be used.

If you elect not to use the Dell Extended Schema, the RCS Switches and access controlled SIPs in your installation will be configured as Computer Objects within Active Directory. To do this, you will first need to configure an Organizational Unit to hold group objects that relate users to access controlled Remote Console Switches and their attached SIPs. This can be a previously created OU, or one created specifically for this purpose but it must be unique among all OU objects in the Group Container domain.

Next, choose an attribute within the LDAP directory to be used to contain discretionary access control information. This should be a previously unused attribute that is capable of storing a string value. (The default is the “info” attribute of the Group Object.)

Finally, you will need to enter the location for the **Group Container**, the **Group Container Domain** and the **Access Control Attribute** in the blanks provided in the **Global - Authentication** window.

For more detailed descriptions of the Authentication panel fields, see Table 8-1.

To access the **Authentication** panel in the on-board web interface:

Click the **Configure** tab, then click **Remote Console Switch - Authentication**.

Figure 8-2. On-board Web Interface - Authentication Panel Local/LDAP and Parameters

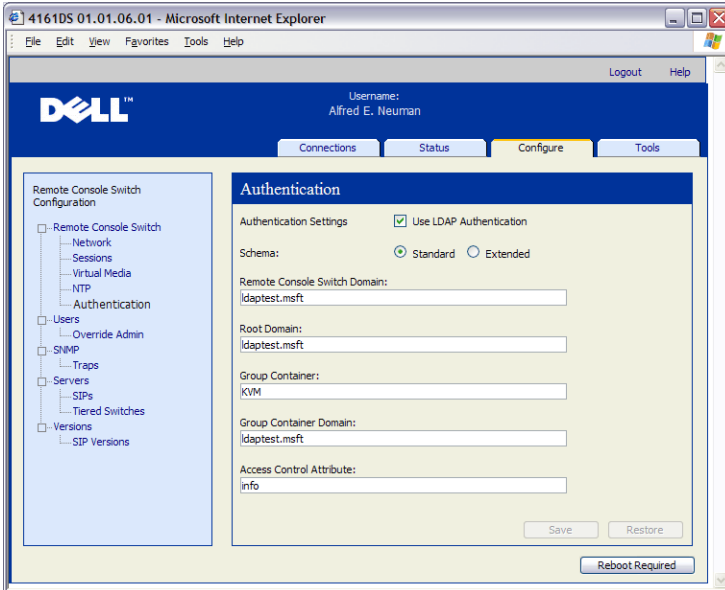


Table 8-1. Authentication Panel Field Descriptions

Field	Description
Authentication Settings	<p>Users can choose to use LDAP authentication by clicking the box shown.</p> <p>The user may still log in with the Override admin account if the LDAP servers are inaccessible.</p>
Schema	<p>Radio Button to indicate which Active Directory (AD) object classes are used to store information related to authorization. For the default Standard schema, Microsoft Active Directory objects are used. When using the Extended schema, the extra Dell object classes are added.</p>
RCS Domain	<p>The RCS Domain field contains the name of the Active Directory Domain chosen to hold all objects that represent Remote Console Switches and SIPs.</p>
Root Domain	<p>The uppermost domain within the Active Directory Forest.</p>
Group Container (Standard schema set only)	<p>This field, available when the standard schema is selected, contains part of the Distinguished Name of an Organizational Unit (OU) object in Active Directory. The OU is used to hold group objects that relate users to access controlled Remote Console Switches and their attached SIPs.</p> <p>For example, suppose the Distinguished Name of the chosen OU is: ou=KVM-AccessControls,dc=MyCom,dc=com. In this case, the Group Container field should be set to “KVM-AccessControls.” The name entered into the Group Container field must be unique among all OU objects in the Group Container domain. You may choose to use a previously created OU for the Group Container, or create one specifically for this purpose.</p> <p>The default Group Container is KVM.</p>
Group Container Domain (Standard schema set only)	<p>This field, available when the Standard schema is selected, is the DNS name of the Active Directory domain where the group container resides.</p>

Access Control Attribute (Standard schema set only)	The value of this field specifies which attribute in the LDAP directory is to be used to contain discretionary access control information and is only enabled when Standard Schema is selected.
---	---

The **Access Control Attribute** is chosen from among the attributes in the LDAP directory object representing the group whose membership includes both the user and the appliance or attached computer that you are trying to access.

When using the Standard schema, it is necessary for Group objects in the Group Container to have an attribute that is chosen to contain the permission level associated with the Group. The Access Control Attribute field, available when the Standard schema is selected, contains the name of the chosen attribute. The chosen attribute must be capable of storing a character string value; for example, the default attribute is “info” which is an attribute accessible via the Active Directory Users and Computers (ADUC) snap-in. Using ADUC, the value of the info attribute is set by accessing the “Notes” property of the Group object.

LDAP SSL Certificates

All LDAP protocol exchanges (between a Remote Console Switch and Active Directory servers) are secured by SSL. When the LDAP protocol is being protected by SSL, it is referred to as LDAPS (Lightweight Directory Access Protocol over SSL). Each LDAPS connection begins with a protocol handshake that triggers a security certificate transmission from the responding Active Directory server to the Remote Console Switch. Once received, the Remote Console Switch is responsible for verifying the certificate. In order to verify the certificate, the appliance must be configured with a copy of the root Certification Authority's (CA) certificate. Before this can be done, the certificate must first be generated.

Enabling SSL on a Domain Controller

If you plan to use Microsoft Enterprise Root CA to automatically assign all your domain controllers SSL certificate, you must perform the following steps to enable SSL on each domain controller if you have not previously done so.

- 1 Install a Microsoft Enterprise Root CA on a Domain Controller.

- a** Select **Start - Control Panel - Add or Remove Programs**.
 - b** Select **Add/Remove Windows Components**.
 - c** In the Windows Components Wizard, select the **Certificate Services** check box.
 - d** Select **Enterprise root CA** as CA Type and click **Next**.
 - e** Enter Common name for this CA, click **Next**, and click **Finish**.
- 2** Enable SSL on each of your domain controllers by installing the SSL certificate for each controller.
- a** Click **Start - Administrative Tools - Domain Security Policy**.
 - b** Expand the Public Key Policies folder, right-click **Automatic Certificate Request Settings** and click **Automatic Certificate Request**.
 - c** In the Automatic Certificate Request Setup Wizard, click **Next** and select **Domain Controller**.
- 3** Click **Next** and click **Finish**.

A certificate/private key file can be created using openssl using Linux. Openssl can be downloaded from openssl.org. Any instructions below with text in <> is where a user would need to set a value based on the criteria at the end of that line.

To create a certificate to import:

- 1** From the Linux command prompt, type openssl and hit Enter. The user should be at the OpenSSL prompt.

```
OpenSSL> genrsa -out privatekey.pem <512>
```

```
Generating RSA private key, 512 bit long modulus
```

```
.....+++++
```

```
.....+++++
```

```
e is 65537 (0x10001)
```

```
OpenSSL> req -new -key privatekey.pem -x509 -out certificate.pem -batch -days <365>
```

- 2 Enter the information that will be incorporated into your certificate request in the Distinguished Name or DN. There may be a default value for some fields. If you wish, you may type '!' to leave a field blank.

```
Country Name (2 letter code) [GB]:<US>
State or Province Name (full name) [Berkshire]:<Texas>
Locality Name (eg, city) [Newbury]:<Austin>
Organization Name (eg, company) [My Company Ltd]:<Dell, Inc.>
Organizational Unit Name (eg, section) []:<Round Rock>
Common Name (eg, your name or your server's hostname) []:<Appliance
DNS Name or IP>
Email Address []:<support@dell.com>
OpenSSL> quit
```


- 3 From the Linux command prompt, type 'cat certificate.pem privatekey.pem > webserver.pem', then convert the file from UNIX linefeed to DOS carriage return/linefeed by typing 'unix2dos webserver.pem'.

To export the CA certificate:

- 1 Within the Windows operating system, open the Certificate Authority management tool:
Start - All Programs - Administrative Tools - Certificate Authority.
- 2 You may view properties of the certificate authority by right clicking on the authority in the tree view and selecting **Properties**. The CA Properties dialog box will open.
- 3 Click the **General** tab and the **View Certificate** button to open the Certificate dialog box.
- 4 Click the **Details** tab then the **Copy To File** button. The Certificate Export Wizard will open.
- 5 Click **Next** to begin using the wizard.
- 6 On the Export File Format screen select the **Base-64 encoded X.509 (.CER)** radio button and press the **Next** button.

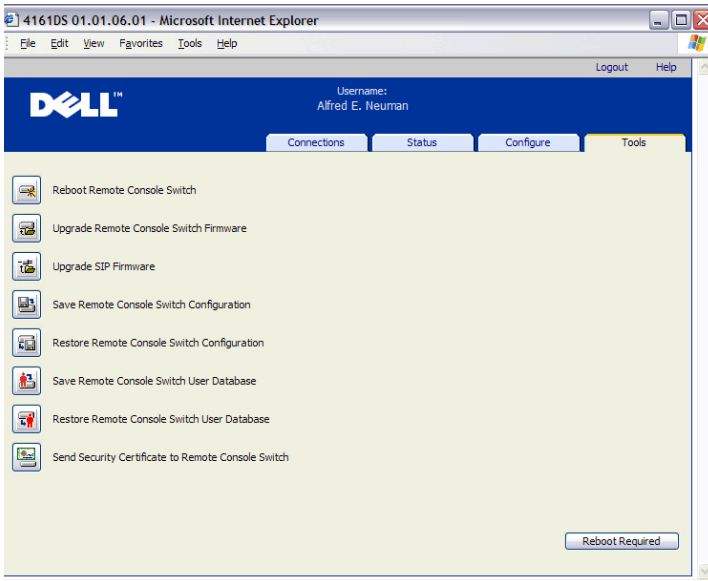
- 7 On the File To Export screen enter or browse to a filename and path for the exported certificate. Press the **Next** button.
- 8 Press the **Finish** button.

The resulting certificate file is properly formatted and readable by OpenSSL. In general, it will be necessary to upload the CA certificate only once; however, it will have to be uploaded again if the certificate is revoked, if it expires, or if “**Restore Factory Defaults**” is selected from the serial console menu.

 **NOTE:** The instructions above are written for a Microsoft Root CA certificate. For other CAs, please check with the CA vendor.

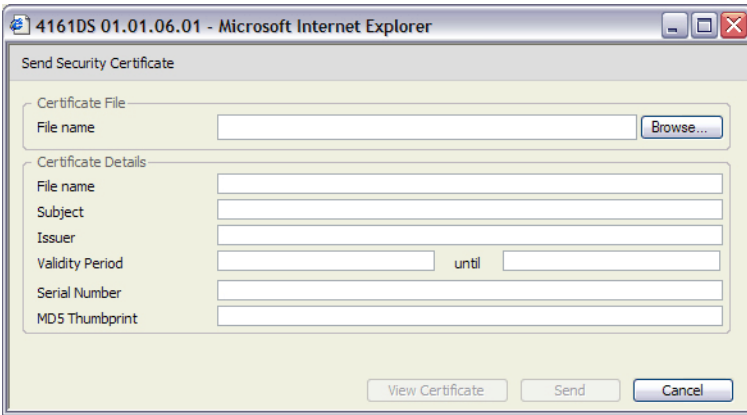
 **NOTE:** The Network Time Protocol (NTP) must be enabled for LDAPS to function.

Figure 8-3. On-board Web Interface - Send Security Certificate



After sending the Security Certificate, the following window displays.

Figure 8-4. On-board Web Interface - Send Certificate



Button	Description
Browse	Browse to a certificate file by opening a File Chooser dialog and allowing a user to choose a certificate file.
View Certificate	Displays the current Remote Console Switch certificate.
Send	Sends the certificate to the Remote Console Switch.
Cancel	Closes the dialog.

You can browse to a certificate and open it. Once the certificate is open and its contents are displayed, the user can then send the certificate to the appliance.

Field	Description
File	Path and name of the certificate file opened with the browse (File Chooser) button.
Subject	Subject of the opened certificate.
Issuer	Person or entity that issued the certificate.
Validity Period	Period that the certificate is valid for.
Serial Number	Serial number of the certificate.
SHA-1 Thumbprint	SHA-1 Thumbprint derived from the certificate.
MD5 Thumbprint	MD5 Thumbprint derived from the certificate.

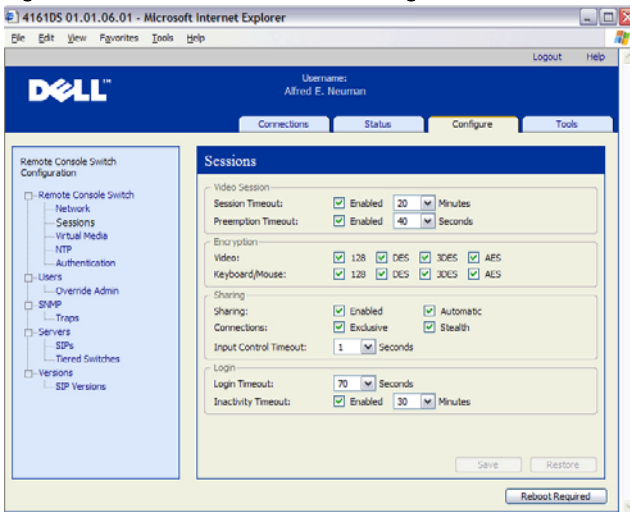
Login Timeout

In cases where there is a large enough directory tree to cause LDAP authentication to perform slowly, the Sessions window includes a Login Timeout function with a default timeout of 30 seconds. The login timeout is the time from which the user presses the **OK** button on the Login dialog box until there is no response from the appliance. The appliance will also use this value to determine the timeout on a LDAP request for authentication.

To specify the login timeout in the on-board web interface:

- 1 Click the **Configure** tab, then click **Remote Console Switch - Sessions**.
- 2 Specify the number of seconds in the **Login Timeout** menu.
- 3 Click **Save**.

Figure 8-5. On-board Web Interface - Login Timeout



CA Certificate Information Display

The Remote Console Switch can only display complete CA Certificate Information in this window when the public key length is less than or equal to 2048 bits. When the key is greater than 2048 bits, the subject, issuer, and validity period data in this window will be incomplete.

The following display is an example of the CA certificate information:

- 1 From the Client, download CA certificate into the appliance.
- 2 From the serial console Main Menu, type option 8 to display the LDAP CA Certificate.

The appliance will display the following types of information:

```
Begin CA certificate information display
subject= /DC=msft/DC=ldaptest/CN=MyCertificate
issuer= /DC=msft/DC=ldaptest/CN=MyCertificate
notBefore=Dec 7 20:09:56 2005 GMT
notAfter=Dec 7 20:18:34 2010 GMT
serial=7BA146C0221A08B447B989292074329F
MD5 Fingerprint=
CB:6D:70:30:31:E5:1B:C0:90:BB:DB:32:B2:C9:D1:5A
End CA certificate information display
```

Perform the steps in the following instructions for enabling the installation of RCS Software on Microsoft Windows Server 2003 platforms:

- 1 Select the **Start** menu.
- 2 Right-click on **My Computer** and select **Properties**.
- 3 Select the **Advanced** tab.
- 4 Click the **Performance Settings** button.
- 5 Select the **Data Execution Prevention** tab.
- 6 Select the radio button for **Turn on DEP for essential Windows programs and services only**
- 7 Click **OK**.
- 8 Click **OK** again on the System Properties dialog box.

Configuring Group Objects

Access control is applied to a specific Active Directory user account by including that user in the membership of a Group in the Group Container. The Group membership must also contain the objects representing the Remote Console Switch(es) and the SIP(s) the user is allowed to access. The level of access granted is determined by the value of a specific attribute in the Group object (Standard Schema) or Association Object (Extended Schema).

There are three permission levels available. In increasing order of access they are, “KVM User”, “KVM User Admin” and, the most powerful level, “KVM Appliance Admin.”



NOTE: If the KVM User access level is not being used, SIP objects will not need configuration as both Administrator permissions have access to all SIPs by default.

Table 8-2. LDAP (Group Attribute Authorization)

Operation	KVM Appliance Admin	KVM User Admin	KVM User
Preemption	Allowed to preempt another Appliance Admin or a User Admin. Permission must be configured for each target device by including the TD in the appropriate Group object in the Directory.	Allowed to preempt another User Admin. Permission must be configured for each target device by including the target device in the appropriate Group object in the Directory.	No
Configure network parameters and global settings	Yes – Permission must be configured for each appliance by including the appliance in the appropriate Group object in the Directory.	No	No
Restart	Yes – Permission must be configured for each appliance by including the appliance in the appropriate Group object in the Directory.	No	No
FLASH Upgrade	Yes – Permission must be configured for each appliance by including the appliance in the appropriate Group object in the Directory.	No	No
Administer user accounts	Yes – Permission must be configured for each appliance by including the appliance in the appropriate Group object in the Directory.	Yes – Permission must be configured for each appliance by including the appliance in the appropriate Group object in the Directory.	No

Configure port settings	Yes – Permission must be configured for each appliance by including the appliance in the appropriate Group object in the Directory.	Yes – Permission must be configured for each appliance by including the appliance in the appropriate Group object in the Directory.	No
Target Device Access	Yes – Permission must be configured for each appliance by including the appliance in the appropriate Group object in the Directory.	Yes – Permission must be configured for each appliance by including the appliance in the appropriate Group object in the Directory.	Yes, if configured by Administrator Permission must be configured for each target device by including the TD in the appropriate Group object in the Directory.

An AD user account must be configured to receive appliance administrator permission before that account will be allowed to modify any of the fields in the Authentication Panel. In particular, only an appliance administrator is allowed to modify the Authentication Settings.

Active Directory Object Overview for Standard Schema

For each of the physical Remote Console Switches on the network that you want to integrate with Active Directory for Authentication and Authorization, you must create at least one Computer Object to represent it. You will also need to create a computer object for each SIP attached to the RCS that will be controlled using the “KVM User” privilege level. Computer objects representing SIPs are not required for the Administrator level groups. Users in the KVM User Group will only have access to SIPs that are also in the KVM User Group. Users with Administrator privileges will have access to all SIPs by default.

To set up the Group Objects for a Remote Console Switch:

- 1 If you have not already, create the Organizational Unit that will contain the Group Objects related to your switch installation.

- 2 Within this Organizational Unit, create three group objects to represent user privilege levels. One for KVM Appliance Administrators, KVM User Administrators and KVM Users respectively.
- 3 Using the MSADUC tool, open the KVM Appliance Administrator Group Object and select the Notes property. Type the access level (“KVM Appliance Admin”) for that group in the Notes field and save. Repeat this step for the other two Group Objects using their respective names.

NOTE: The single syntax for all access control attribute values is:

"[<arbitrary text string> <delimiter>] < privilege level> [<delimiter> <arbitrary text string>]"

Where: <privilege level> := "KVM User" or "KVM User Admin" or "KVM Appliance Admin"

<delimiter> ::= one or more of any of the following: <newline> or <c/r> or <comma> or <semicolon> or <tab>

<arbitrary text string> is any string of alphanumeric characters and may be the null (i.e., empty) string.

Square brackets indicate optional items; for example, the following template indicates an optional string and delimiter followed by a required privilege level: "[<arbitrary text string> <delimiter>] < privilege level1>".

- 4 Create a computer object to represent the Remote Console Switch.
- 5 Create a computer object for each SIP attached to a server to be access restricted at the KVM User privilege level.
- 6 Add the computer object that represents the switch to the appropriate group objects.
- 7 Add user objects to the appropriate group object for their access level.
- 8 Add the computer objects for the access controlled SIPs to the KVM User Group.

Dell Extended Schema Active Directory Object Overview

For each of the physical Remote Console Switches on the network that you want to integrate with Active Directory for Authentication and Authorization, you must create at least one RCS Device Object to represent

the physical switch and one Association Object. The Association object is used to link together the users or groups with a specific set of privileges to one or more SIPs. This model provides an Administrator maximum flexibility over the different combinations of users, RCS privileges, and SIPs on the Remote Console Switch without adding too much complexity.

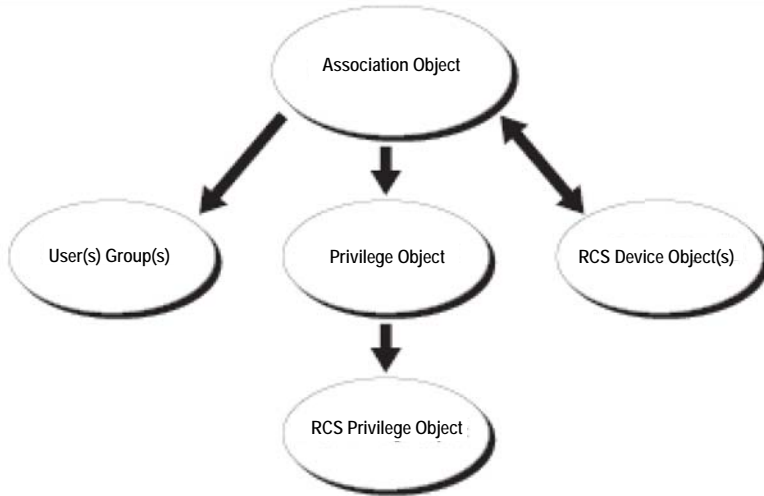
The RCS Device Object is the link to the Remote Console Switch for querying Active Directory for authentication and authorization. When a Remote Console Switch is added to the network, the Administrator must configure the Remote Console Switch and its device object with its Active Directory name so that users can perform authentication and authorization with Active Directory. The Administrator will also need to add the Remote Console Switch to at least one Association Object in order for users to authenticate.

You can create as many Association Objects as you want, and each Association Object can be linked to as many users, groups of users, or RCS Device Objects as desired. The users and RCS Device Objects can be members of any domain in the enterprise.

However, each Association Object may be linked (or, may link users, groups of users, or RCS Device Objects) to only one Privilege Object. A Privilege Object allows an Administrator to control which users have what kind of privileges on specific SIPs.

Figure 8-6 illustrates that the Association Object provides the connection that is needed for all of the Authentication and Authorization.

Figure 8-6. Typical Setup for Active Directory Objects

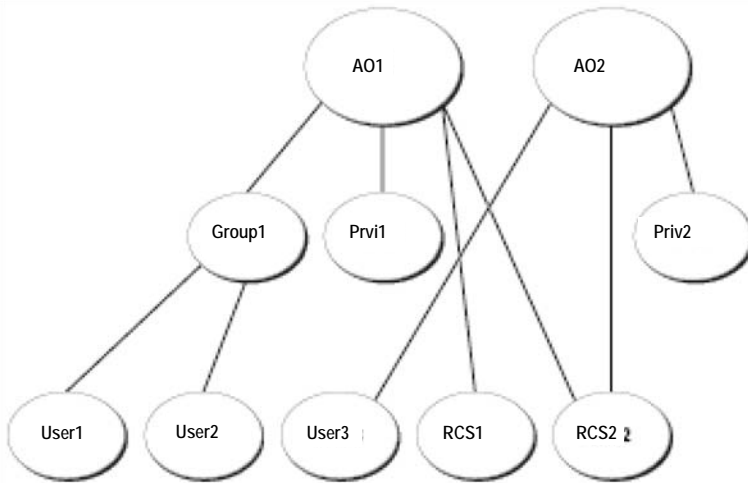


You can create as many or as few association objects as you want or need. However, you must create at least one Association Object, and you must have one RCS Device Object for each Remote Console Switch on the network that you want to integrate with Active Directory for Authentication and Authorization. The Association Object allows for as many or as few users and/or groups as well as RCS Device Objects. However, the Association Object only has one Privilege Object per Association Object. The Association Object connects the “Users” who have “Privileges” on the RCSs.

In addition, you can set up Active Directory objects in a single domain or in multiple domains. For example, you have two Remote Console Switches (RCS1 and RCS2) and three existing Active Directory users (user1, user2, and user3). You want to give user1 and user2 an administrator privilege to both Remote Console Switches and give user3 a login privilege to the RCS2.

Figure 8-7 shows how you set up the Active Directory objects in this scenario.

Figure 8-7. Setting Up Active Directory Objects in a Single Domain



To set up the objects for the single domain scenario, perform the following tasks:

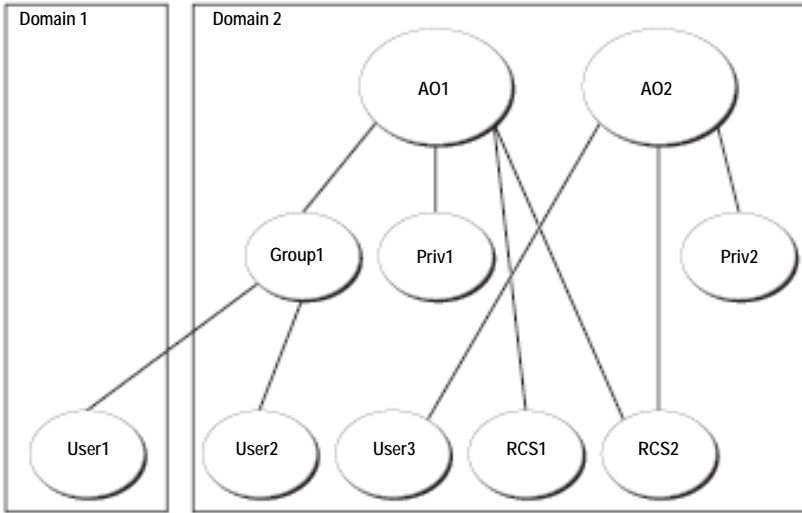
- 1 Create two Association Objects.
- 2 Create two RCS Device Objects, RCS1 and RCS2, to represent the two Remote Console Switches.
- 3 Create two Privilege Objects, Priv1 and Priv2, in which Priv1 has all privileges (administrator) and Priv2 has login privileges.
- 4 Group user1 and user2 into Group1.
- 5 Add Group1 as Members in Association Object 1 (AO1), Priv1 as Privilege Objects in AO1, and RCS1 and RCS2 as RCS Devices in AO1.
- 6 Add user3 as Members in Association Object 2 (AO2), Priv2 as Privilege Objects in AO2, and RCS2 as RCS Devices in AO2.

See “Adding Remote Console Switch Users and Privileges to Active Directory with Dell Schema Extensions” for detailed instructions.

Figure 8-8 shows how you can set up the Active Directory Objects in multiple domains. In this scenario, you have two Remote Console Switches (RCS1 and RCS2) and three existing Active Directory users (user1, user2, and user3).

User1 is in Domain1, and user2 and user 3 are in Domain2. You want to give user1 and user 2 an administrator privilege to both Remote Console Switches and give user3 a login privilege to the RCS2.

Figure 8-8. Setting Up Active Directory Objects in Multiple Domains



To set up the objects for the multiple domain scenario, perform the following tasks:

- 1** Ensure that the domain forest function is in Native or Windows 2003 mode.
- 2** Create two Association Objects, AO1 (of Universal scope) and AO2, in any domain. The figure shows the objects in Domain2.
- 3** Create two RCS Device Objects, RCS1 and RCS2, to represent the two Remote Console Switches.
- 4** Create two Privilege Objects, Priv1 and Priv2, in which Priv1 has all privileges (administrator) and Priv2 has login privileges.
- 5** Group user1 and user2 into Group1. The group scope of Group1 must be Universal.
- 6** Add Group1 as Members in Association Object 1 (AO1), Priv1 as Privilege Objects in AO1, and RCS1, RCS2 as RCS Devices in AO1.

- 7 Add user3 as a Member in Association Object 2 (AO2), Priv2 as Privilege Objects in AO2, and RCS2 as RCS Devices in AO2.


Configuring Active Directory with Dell Schema Extensions to Access Your RCS

Before you can use Active Directory to access your Remote Console Switch, you must configure the Active Directory software and the Remote Console Switch by performing the following steps in their numbered order:


- 1 Extend the Active Directory schema.
- 2 Extend the Active Directory Users and Computers Snap-in.
- 3 Add RCS users and their privileges to Active Directory.

Extending the Active Directory Schema (Optional)

Extending your Active Directory schema will add a Dell organizational unit, schema classes and attributes, and example privileges and association objects to the Active Directory schema.

 **NOTE:** Before you extend the schema, you must have Schema Admin privileges on the Schema Master Flexible Single Master Operation (FSMO) Role Owner of the domain forest.

You can extend your schema using two different methods. You can use the Dell Schema Extender utility or you can use the LDIF script file.


 **NOTE:** The Dell organizational unit will not be added if you use the LDIF script file.

The LDIF files and Dell Schema Extender can be obtained at dell.com/support.

To use the LDIF files, see the instructions in the readme that is in the LDIF files directory. To use the Dell Schema Extender to extend the Active Directory Schema, perform the steps in “Using the Dell Schema Extender.”

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

Using the Dell Schema Extender

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

- 1 Click **Next** on the Welcome screen.

- 2 Read the warning and click **Next** again.
- 3 Either select **Use Current Log In Credentials** or enter a user name and password with schema administrator rights.
- 4 Click **Next** to run the Dell Schema Extender.
- 5 Click **Finish**.

Installing the Dell Extension to the Active Directory Users and Computers Snap-In (Optional)

When you extend the schema in Active Directory, you must also extend the Active Directory Users and Computers snap-in so that the administrator can manage Remote Console Switch devices, Users and User Groups, Remote Console Switch Associations, and SIP Privileges. The Dell Extension to the Active Directory User's and Computers Snap-In is an option that can be installed when you install your systems management software using the Dell Systems Management Consoles CD. See the Dell OpenManage Software Quick Installation Guide for further instructions on installing systems management software.



NOTE: You must install the Administrator Pack on each system that is managing the Active Directory Remote Console Switch Objects. The installation is described in the following section, "Opening the Active Directory Users and Computers Snap-In." If you do not install the Administrator Pack, then you cannot view the Dell SIP Object in the container.



NOTE: For more information about the Active Directory Users and Computers snap-in, see your Microsoft documentation.

Opening the Active Directory Users and Computers Snap-In

To open the Active Directory Users and Computers snap-in, perform the following steps:

If you are on the domain controller, click **Start -Admin Tools - Active Directory Users and Computers**. If you are not on the domain controller, you must have the appropriate Microsoft Administrator Pack installed on your local system. To install this Administrator Pack, click **Start - Run**, type **MMC** and press **Enter**. This opens the Microsoft Management Console (MMC).

- 1 Click **File** (or **Console** on systems running Windows 2000) in the Console 1 window.

- 2 Click **Add/Remove Snap-in**.
- 3 Select the **Active Directory Users and Computers** snap-in and click **Add**.
- 4 Click **Close** and click **OK**.

Adding Users and Privileges to Active Directory with Dell Schema Extensions

The Dell-extended Active Directory Users and Computers snap-in allows you to add Remote Console Switch users and privileges by creating SIP, Association, and Privilege objects. To add each type of object, perform the steps in each subsections.

Creating a SIP Object

- 1 In the MMC Console Root window, right-click a container.
- 2 Select **New - Dell SIP Object**. This opens the New Object window.
- 3 Type a name for the new object. This name must match the Remote Console Switch Name that you will type in step 4 of “Configuring the Remote Console Switch.”
- 4 Select **SIP Device Object**.
- 5 Click **OK**.

Creating a Privilege Object

Privilege Objects must be created in the same domain as the Association Object to which it is associated.

- 1 In the Console Root (MMC) window, right-click a container.
- 2 Select **New - Dell SIP Object** to open the New Object window.
- 3 Type a name for the new object.
- 4 Select **Privilege Object**.
- 5 Click **OK**.
- 6 Right-click the privilege object that you created, and select **Properties**.
- 7 Click the **RCS Privileges** tab and select the Remote Console Switch privileges that you want the user to have.

Using Dell Association Objects Syntax

Using the Dell Association Objects syntax, object types default to User and Group in the Dell LDAP Schema. In the Dell Extended Schema, Dell has added unique Object IDs for four new object classes:

- KVM Appliance Objects
- KVM SIP Objects
- Privilege Objects
- Association Objects

Each of these new object classes is defined in terms of various combinations (hierarchies) of default Active Directory classes, together with Dell unique attribute types. Each of the Dell unique attribute types is defined in terms of a default Active Directory attribute syntax.

The default Microsoft Active Directory object classes used include User and Group. The User class generally denotes Active Directory objects that contain information about single entities. The Group class represents containers used for nesting and contain information about collections of objects.

Each KVM Appliance Object represents an individual Remote Console Switch within Active Directory. Since these are single entities, in the LDAP default language they are User objects rather than Group objects.

Each Privilege Object defines a distinct composite set of privileges. Each set is treated as a discrete entity, therefore it is a User object rather than a Group object.

An Association Object contains a collection of information about the privileges granted to a specific user accounts with respect to a specific appliance (or appliances) and/or specific SIP (or SIPs). User accounts in an Appliance Object may be specified in terms of any combination of the following:

- Individual account
- Active Directory security group of user accounts
- Multiple Active Directory security groups of user accounts

Similarly, for the appliances and/or SIPs in an Association Object and because the Association Object has the ability to use security groups in the same way, it is defined as a group object itself.

Creating an Association Object

The Association Object is derived from a Group and must contain a Group Type. The Association Scope specifies the Security Group Type for the Association Object. When you create an Association Object, you must choose the Association Scope that applies to the type of objects you intend to add. Selecting Universal, for example, means that association objects are only available when the Active Directory Domain is functioning in Native Mode or above.

To create an association object:

- 1 In the Console Root (MMC) window, right-click a container.
- 2 Select **New - Dell SIP Object** to open the New Object window.
- 3 Type a name for the new object.
- 4 Select **Association Object**.
- 5 Select the scope for the Association Object.
- 6 Click **OK**.

Adding Objects to an Association Object

By using the Association Object Properties window, you can associate users or user groups, privilege objects, and SIP devices or SIP device groups.



NOTE: When using Windows 2000 mode or higher, you must use Universal Groups to span domains with your users or SIP objects.

You can add groups of Users and SIP devices. Creating Dell-related groups is done the same way you create other groups.

To add users or User Groups:

- 1 Right-click the Association Object and select **Properties**.
- 2 Select the **Users** tab and click **Add**.
- 3 Type the user or User Group name and click **OK**.

Click the **Privilege Object** tab to add the privilege object to the association that defines the user's or user group's privileges when authenticating to a SIP device.




NOTE: You can add only one privilege object to an association object.

To add a privilege:

- 1 Select the **Privileges Object** tab and click **Add**.
- 2 Type the Privilege Object name and click **OK**.

Click the **Products** tab to add one or more SIP devices to the association. The associated devices specify the SIP devices connected to the network that are available for the defined users or user groups.

 **NOTE:** You can add multiple SIP devices to an association object.

To add SIP devices or SIP device groups:

- 1 Select the **Products** tab and click **Add**.
- 2 Type the SIP device or SIP device group name and click **OK**.
- 3 In the Properties window, click **Apply** and then **OK**.

Console Redirection Access Security

In any Remote Console Switch installation, any user privilege allows the user to launch the on-board web interface. The on-board web interface functionality for that user is limited by the User Privilege level established in the Remote Console Switch. LDAP with Dell Extended Schema adds an extra level of security to appliance management by allowing administrators to limit a user's access to the on-board web interface.

Authorization to use the on-board web interface is defined by whether User Privilege level is or is not configured in the KVM Appliance Privileges tab of the Dell Privilege Object (DPO). The Console Redirection Access checkbox in the KVM SIP Privileges tab of the DPO provides the means for a user who cannot view the on-board web interface to launch Video Viewer sessions to a subset of SIPs through the RCS Client. This authorization is controlled by a combination of the configuration parameters set in the DPO and the SIP Objects contained in the Dell Association Object (DAO).

If you do not wish a user to have authorization to access the on-board web interface, but you do wish them to be able to launch viewer sessions from the RCS Client, perform the following steps:

- 1 Create a Dell SIP object for each SIP that the User(s) is (are) allowed to access.
- 2 Create an Active Directory User account for each of the users to be controlled.

- 3 Create a DPO. Do not check any of the three boxes on the “KVM Appliance Privileges” tab. Check the Console Redirection Access box on the “KVM SIP Privileges” tab.

NOTE: If you check any of the KVM Appliance Privileges check boxes *and* you check the Console Redirection Access box, the normal User Privileges associated with the privilege level checked in the KVM Appliance Privileges box will take precedence over the Console Redirection Access checkbox, and the user will still be able to view the AMP.

- 4 Create a DAO.
- 5 Open the properties dialog for the DAO created in step 4.
 - a Add all the user accounts created in step 2.
 - b Add the DPO created in step 3.
 - c Add the SIP objects created in step 1.

Using Active Directory to Log In to the Remote Console Switch

You can use Active Directory to log in to the Remote Console Switch through the Remote Console Switch Software or on-board web interface.

The login syntax is consistent for all three methods:

<username@domain> or <domain>\<username> or <domain>/<username>
(where username is an ASCII string of 1–256 bytes). No white space and no special characters (such as \, /, or @) are allowed in either the username or the domain name.



NOTE: You cannot specify NetBIOS domain names, such as Americas, since those names cannot be resolved.



NOTE: If a domain name is not included, the local database in the Remote Console Switch will be used to authenticate the user.

Target Device Naming Requirements for LDAP Implementation

If you experience the following error:

Login Failure. Reason: Access cannot be granted due to Authentication Server errors

Please verify that the SIP object was created in the Active Directory and its name exactly matches the name assigned to that SIP via the OSCAR interface at the console switch.

The Dell Standard Schema and the Dell Extended Schema use specific object classes in the Microsoft Windows Active Directory to represent SIPs. The Microsoft standard naming conventions for these object classes prohibit the use of special characters or spaces. If you intend to use LDAP in a deployed environment where target device names in SIPs currently include spaces or special characters, you will need to rename them without spaces or special characters.

Renaming a target device in a SIP should be done through the on-board web interface or OSCAR interface at the console switch and then resynchronized through the Remote Console Switch Software. Instructions for renaming a target device in a SIP can be found in "Assigning Device Names" on page 49. It is important to note that while OSCAR interface will allow you to enter spaces into the names assigned to the SIPs, Active Directory does not. You must name SIP objects according to the Microsoft Active Directory rules.

Frequently Asked Questions

Table 8-3 lists frequently asked questions and answers.

Table 8-3. Using the RCS with Active Directory: FAQ

Can I log into the Remote Console Switch using Active Directory across multiple forests?

The RCS Active Directory query algorithm only supports a single tree in a single forest.

Does the login to the Remote Console Switch using Active Directory work in mixed mode (that is, the domain controllers in the forest run different operating systems, such as Microsoft Windows NT® 4.0, Windows 2000, or Windows Server 2003)?

Yes. In mixed mode, all objects used by the Remote Console Switch querying process (among user, SIP Device Object, and Association Object) have to be in the same domain.

The Dell-extended Active Directory Users and Computers snap-in checks the mode and limits users in order to create objects across domains if in mixed mode.

Does using the Remote Console Switch with Active Directory support multiple domain environments?

Yes. The domain forest function level must be in Native mode or Windows 2003 mode. In addition, the groups among Association Object, Remote Console Switch user objects, and SIP Device Objects (including Association Object) must be universal groups.

Can these Dell-extended objects (Dell Association Object, Dell Remote Console Switch Device, and Dell Privilege Object) be in different domains?

The Association Object and the Privilege Object must be in the same domain. The Dell-extended Active Directory Users and Computers snap-in forces you to create these two objects in the same domain. Other objects can be in different domains.

Are there any restrictions on Domain Controller SSL configuration?

Yes. All Active Directory servers' SSL certificates in the forest must be signed by the same root CA since Remote Console Switch only allows uploading one trusted CA SSL certificate.

What can I do if I cannot log into the Remote Console Switch using Active Directory authentication? How do I troubleshoot the issue?

Troubleshoot as follows:

- If no domain name is specified, the local database is used. To login when AD authentication isn't working, use the default local admin account.
- Ensure that you have checked the Enable Active Directory check box (Remote Console Switch Software) or the Use LDAP Authentication check box (on-board web interface) on the Remote Console Switch Active Directory configuration page.
- Ensure that the DNS setting is correct on the Remote Console Switch Networking configuration page.
- Ensure Network Time Protocol is enabled on at least one server specified on the NTP panel.
- Ensure that you have uploaded the Active Directory certificate from your Active Directory root CA to the Remote Console Switch.
- Check the Domain Controller SSL certificates to ensure that they have not expired.
- Ensure that your “Remote Console Switch Name”, “Root Domain Name”, and “Remote Console Switch Domain Name” match your Active Directory environment configuration.
- Ensure that you use the correct user domain name during a login and not the NetBIOS name.

Appendix A: Remote Console Switch Software Keyboard and Mouse Shortcuts

Table B.1: Divider Pane Keyboard and Mouse Shortcuts

Operation	Description
F6	Navigates between the split-screens and gives focus to the last element that had focus.
F8	Gives focus to the divider.
Left or Up Arrow	Moves the divider left if the divider has the focus.
Right or Down Arrow	Moves the divider right if the divider has the focus.
Home	Gives the right pane of the split-screen all of the area (left pane disappears) if the divider has the focus.
End	Gives the left pane of the split-screen all of the area (right pane disappears) if the divider has the focus.
Click + Mouse Drag	Moves the divider left or right.

Table B.2: Tree View Control Keyboard and Mouse Shortcuts

Operation	Description
Mouse Single-Click	Deselects the existing selection and selects the node the mouse pointer is over.
Mouse Double-Click	Toggles the expand/collapse state of an expandable node (a node that has children). Does nothing on a leaf node (a node that does not have children).
Up Arrow	Deselects the existing selection and selects the next node above the current focus point.

Table B.2: Tree View Control Keyboard and Mouse Shortcuts

Operation	Description
Down Arrow	Deselects the existing selection and selects the next node below the current focus point.
Spacebar	Alternately selects/deselects the node that currently has the focus.
Enter	Alternately collapses/expands the node that has focus. Only applies to nodes that have children. Does nothing if the node does not have children.
Home	Deselects the existing selection and selects the root node.
End	Deselects the existing selection and selects the last node displayed in the tree.

Table B.3: Keyboard and Mouse Operations for the Unit List

Operation	Description
Enter or Return	Launches the default action for the selected unit.
Up Arrow	Deselects current selection and moves selection up one row.
Down Arrow	Deselects current selection and moves selection down one row.
Page Up	Deselects current selection and scrolls up one page then selects the first item on the page.
Page Down	Deselects current selection and scrolls down one page then selects the last item on the page.
Delete	Performs the Delete function. Works the same as the Edit->Delete menu function. Please see that section for more information.
Ctrl + Home	Moves the focus and the selection to the first row in the table.
Ctrl + End	Moves the focus and the selection to the last row in the table.
Shift + Up Arrow	Extends selection up one row.
Shift + Down Arrow	Extends selection down one row.
Shift + Page Up	Extends selection up one page.

Table B.3: Keyboard and Mouse Operations for the Unit List

Operation	Description
Shift + Page Down	Extends selection down one page.
Shift + Mouse Click	Deselects any existing selection and selects the range of rows between the current focus point and the row the mouse pointer is over when the mouse is clicked.
Ctrl + Mouse Click	Toggles the selection state of the row the mouse pointer is over without affecting the selection state of any other row.
Mouse double-click	Launches the default action for the selected unit.

Appendix B: TCP Ports

The following table lists the functions performed by the Remote Console Switch and which ports are used.

Table B-1. Ports Used

Port	Function
TCP 80/443	Default HTTP/HTTPS.
TCP 2068/8192	Video Viewer video, keyboard, mouse, user authentication, and virtual media.
TCP/UDP 3211	Discovery, AMP user authentication.
TCP 3871	Plug-in support.


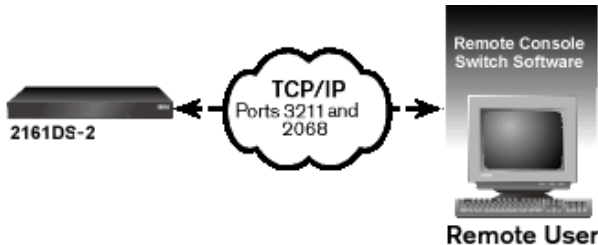

 **NOTE:** Most data on ports 2068 and 3211 is encrypted using the Secure Socket Layer (SSL) protocol.

Figure C-1. TCP Port Communication



 **NOTE:** The TCP/IP ports are fixed and cannot be altered.

Appendix C: MIBs and SNMP Traps

This appendix provides formatted information drawn from the Management Information Bases (MIBs) written for Dell 2161DS-2/4161DS/2321DS Remote Console Switches. Sections in this guide follow MIB groups and provide explanation and definitions for the terms used to define MIB objects. You can access MIB-11 and MIB databases while using IPv4 or IPv6 and can add IPv4 or IPv6-specific traps.

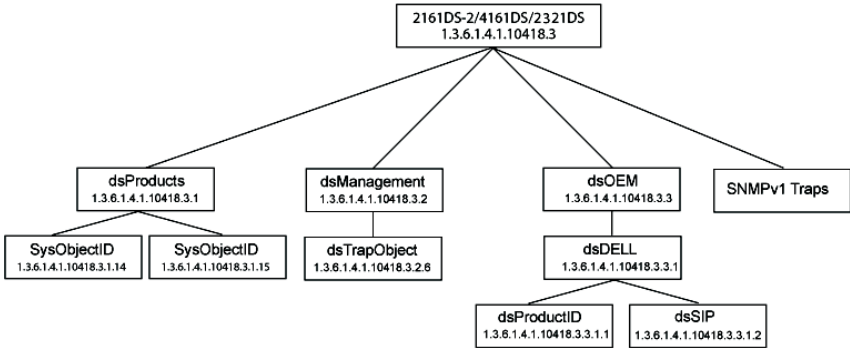
MIB is a virtual database of managed objects contained within the SNMP agent. It is a collection of objects that defines the properties of the managed devices.

The Remote Console Switch MIB definitions use the structure described in the following Request For Comments (RFCs).

- RFC-1155-SMI
Describes the common structures and identification scheme for the definition of management information for use with TCP/IP-based Internets.
- RFC-1212
Describes the format for producing concise and descriptive MIB modules.
- RFC-1213-MIB
Describes the Internet standard MIB-II for use with network management protocols in TCP/IP-based internetworks.
- RFC-1215
Describes the SNMP standardized traps and provides a means for defining enterprise-specific traps.

The private Remote Console Switch MIB is represented by the object identifier 1.3.6.1.4.1.10418.3, which include the subtrees dsProducts (1), dsManagement (2), dsOEM (3), and SNMP Traps as shown in Figure C-1.

Figure C-1. Dell Remote Console Switch MIB Structure



MIB Groups

Product ID Group (dsProductID) 1.3.6.1.4.1.10418.3.3.1.1

Product ID group objects are shown in Table C-1. The primary purpose of the Product ID group is for management station to uniquely identify the manufacturer, model, product version and firmware version of the Remote Console Switch. Product ID group object types may be useful for inventory purposes, or for automatically detecting incompatibilities or version mismatches between various hardware and software components on a system.

Table C-1. Product IP Group Objects

Object Type	Description	OID
dsProductIDDisplayName	Product name in UTF8.	1.3.6.1.4.1.10418.3.3.1.1.1
dsProductIDVendor	Product vendor name in UTF8.	1.3.6.1.4.1.10418.3.3.1.1.3
ProductIDProductVersion	Global product version in UTF8.	1.3.6.1.4.1.10418.3.3.1.1.4
dsProductIDModuleFWVersion	The D module firmware version string in UTF8.	1.3.6.1.4.1.10418.3.3.1.1.5
dsProductIDMainboardFWVersion	The main board firmware version string in UTF8.	1.3.6.1.4.1.10418.3.3.1.1.6
dsProductIDStatus	Reports the operating state of the product based on a mapping of the private MIB variable dsServerStatus as follows: dsServerStatus ready (1) startupInProgress (2) subsystemUpgrading (3) kdbMseSubsystemFailure (4) videoSubsystemFailure (5)	1.3.6.1.4.1.10418.3.3.1.1.7 dsProductIDStatus ok (3) the product is operational. unknown (2) the product is starting up and is not operational. non-critical (4) the product is upgrading its flash and is not operational. non-recoverable (6) a subsystem failure has occurred. The product is not fully operational. non-recoverable (6) a subsystem failure has occurred. The product is not fully operational.
dsProductIDDescription	Product description in UTF8.	1.3.6.1.4.1.10418.3.3.1.1.2

Object Type	Description	OID
dsProductIDVendor	Product vendor name in UTF8.	1.3.6.1.4.1.10418.3.3.1.1.3
ProductIDProductVersion	Global product version in UTF8.	1.3.6.1.4.1.10418.3.3.1.1.4
dsProductIDDDModuleFWVersion	The D module firmware version string in UTF8.	1.3.6.1.4.1.10418.3.3.1.1.5
dsProductIDMainboardFWVersion	The main board firmware version string in UTF8.	1.3.6.1.4.1.10418.3.3.1.1.6
dsProductIDStatus	Reports the operating state of the product based on a mapping of the private MIB variable dsServerStatus as follows:	1.3.6.1.4.1.10418.3.3.1.1.7
	dsServerStatus ready (1)	dsProductIDStatus ok (3) the product is operational.
	startupInProgress (2)	unknown (2) the product is starting up and is not operational.
	subsystemUpgrading (3)	unknown (2) the product is starting up and is not operational.
	kdbMseSubsystemFailure (4)	non-critical (4) the product is upgrading its flash and is not operational.
	videoSubsystemFailure (5)	non-recoverable (6) a subsystem failure has occurred. The product is not fully operational. non-recoverable (6) a subsystem failure has occurred. The product is not fully operational.

SIP Group (dsSIP) 1.3.6.1.4.1.10418.3.3.1.2

SIP group objects are shown in Table C-2. The SIP group objects are structured in a table format and contain information on SIPs connected to the Remote Console Switch, such as SIP's boot, application and hardware version.

Table C-2. SIP Group Objects

Object Type	Description	OID
dsSipTable	Table containing SIPs information.	1.3.6.1.4.1.10418.3.3.1.2.1
dsSipTableEntry	An entry in the SIP table.	1.3.6.1.4.1.10418.3.3.1.2.1.1
dsSipTableIndex	A unique index representing an entry into the SIP table.	1.3.6.1.4.1.10418.3.3.1.2.1.1.1
dsSipTableInputPort	An input port number. Designates the port to which the SIP is connected.	1.3.6.1.4.1.10418.3.3.1.2.1.1.2
dsSipTableEID	The EID of the SIP.	1.3.6.1.4.1.10418.3.3.1.2.1.1.3
dsSipTableBootImageVersion	The SIP's boot image version in UTF8.	1.3.6.1.4.1.10418.3.3.1.2.1.1.4
dsSipTableAppImageVersion	The SIP's application image version in UTF8.	1.3.6.1.4.1.10418.3.3.1.2.1.1.5
dsSipTableHardwareVersion	The SIP's hardware version in UTF8.	1.3.6.1.4.1.10418.3.3.1.2.1.1.6
dsSipTableStatus	The status of the SIP.	1.3.6.1.4.1.10418.3.3.1.2.1.1.7

SNMP Trap Object Group

This section describes the variables sent to Dell 2161DS-2/4161DS Remote Console Switches. It provides additional information about a trap or an alert generated by an event on the RCS. The following objects are for generation of traps. The objects are sent in traps and are not accessible in any other way.

User Name	
Variable Name	dsTrapObjectUserName
OID	1.3.6.1.4.1.10418.3.2.6.1

User Name

Description	This object is sent in a trap to identify the name of the user for which the trap condition occurred. If the trap condition occurred as a result of activity on the local port (OSD), then the value of this object will be the following string: local port.
Syntax	UTF8String (SIZE (3.16))

Target User Name

Variable Name	dsTrapObjectTargetUserName
OID	1.3.6.1.4.1.10418.3.2.6.2
Description	This object is sent in a trap to identify the name of the target user for which a trap condition occurred.
Syntax	UTF8String (SIZE (3.16))

Image Type

Variable Name	dsTrapObjectImageType
OID	1.3.6.1.4.1.10418.3.2.6.3
Description	This object is sent in a trap to identify the type of software image for which the trap condition occurred.
Syntax	UTF8String (SIZE (0.64))

New Image Version

Variable Name	dsTrapObjectImageNewVersion
OID	1.3.6.1.4.1.10418.3.2.6.4
Description	UTF8String (SIZE (0.32))
Syntax	This object is sent in a trap to identify the version of the new software image for which the Remote Console Switch is being upgraded.

Current Image Version

Variable Name	dsTrapObjectImageCurrentVersion
---------------	---------------------------------

Current Image Version

OID	1.3.6.1.4.1.10418.3.2.6.5
Description	This object is sent in a trap to identify the version of the software image that the Remote Console Switch is currently running.
Syntax	UTF8String (SIZE (0.32))

Image Upgrade Results

Variable Name	dsTrapObjectImageUpgradeResults
OID	1.3.6.1.4.1.10418.3.2.6.6
Description	This object is sent in a trap to report the results of an FTP, TFTP, or ASMP image upgrade.
Syntax	UTF8String (SIZE (0.64))

Session Identifier

Variable Name	dsTrapObjectSessionIdentifier
OID	1.3.6.1.4.1.10418.3.2.6.7
Description	<p>This object is sent in a trap to identify the session for which the trap condition occurred. The value will be the name of a server if the server name is known, otherwise the value will be the connection path to a server.</p> <p>If the value is a connection path it will have the following format: SIP s:Channel c</p> <p>Where s is the ID of the SIP, and c is the tiered switch channel number (0 if there is no switch in the path).</p>
Syntax	UTF8String (SIZE (0.32))

SIP Identification

Variable Name	dsTrapObjectSipId
OID	1.3.6.1.4.1.10418.3.2.6.8

SIP Identification

Description	This object is sent in a trap to identify the SIP for which the trap condition occurred.
Syntax	UTF8String (SIZE (0.32))

Tiered Switch Identification

Variable Name	dsTrapObjectTieredSwitchName
OID	1.3.6.1.4.1.10418.3.2.6.9
Description	This object is sent in a trap to identify the tiered switch for which the trap condition occurred.
Syntax	Syntax UTF8String (SIZE (0.15))

Tiered Switch Old Identification

Variable Name	dsTrapObjectOldTieredSwitchName
OID	1.3.6.1.4.1.10418.3.2.6.10
Description	This object is sent in a trap to identify the old name of a tiered switch whose name was changed.
Syntax	UTF8String (SIZE (0.15))

Server Identification

Variable Name	dsTrapObjectServerName
OID	1.3.6.1.4.1.10418.3.2.6.11
Description	This object is sent in a trap to identify the server for which the trap condition occurred.
Syntax	UTF8String (SIZE (0.15))

Server's Old Identification

Variable Name	dsTrapObjectOldServerName
OID	1.3.6.1.4.1.10418.3.2.6.12

Server's Old Identification

Description	This object is sent in a trap to identify the old name of a server whose name was changed.
Syntax	UTF8String (SIZE (0.15))

Filename Identification

Variable Name	dsTrapObjectFileName
OID	1.3.6.1.4.1.10418.3.2.6.13
Description	This object is sent in a trap to identify the name of a file for which the trap condition occurred.
Syntax	DisplayString (SIZE (0.12))

Firmware Condition

Variable Name	dsTrapObjectFirmwareCondition
OID	1.3.6.1.4.1.10418.3.2.6.14
Description	<p>This trap message contains data for application specific diagnostics. It is designed in provision for diagnostic help for installation-specific problems. It would require the operator to install firmware provided to isolate their particular problems, and to enable the trap to report conditions.</p> <p>The contents will be a Dell Application Message Packet with the address, size, and command header removed. The parameters of the message will depend on the specific problem the firmware is designed to detect and report.</p>
Syntax	OCTET STRING (SIZE (0.64))

Device Identification

Variable Name	dsTrapObjectDeviceId
OID	1.3.6.1.4.1.10418.3.2.6.15

Device Identification

Description	This object is sent in a trap to identify the device for which the trap condition occurred.
Syntax	UTF8String (SIZE (0.32))

Warning/Alarm Condition

Variable Name	dsTrapObjectAlarmCondition
OID	1.3.6.1.4.1.10418.3.2.6.16
Description	This object is sent in a trap to identify Warning/Alarm activity for the device on which the trap condition occurred. Alarm sets the alarm, OK indicates the condition has cleared up.
Syntax	SyntaxINTEGER {alarm(1),ok(2)}

Warning/Alarm Explanation

Variable Name	dsTrapObjectAlarmDescription
OID	1.3.6.1.4.1.10418.3.2.6.17
Description	This object is sent in a trap to explain the warning or alarm condition for which the trap condition occurred. This is intended for display or logging.
Syntax	UTF8String (SIZE (0.64))

User Account Lock Reason

Variable Name	dsTrapObjectLockReason
OID	1.3.6.1.4.1.10418.3.2.6.18
Description	This object is sent in a trap to explain the reason for which a user account has been locked.
Syntax	UTF8String (SIZE (0.64))

User Account Unlocked Reason

Variable Name	dsTrapObjectUnlockReason
OID	1.3.6.1.4.1.10418.3.2.6.19
Description	This object is sent in a trap to explain the reason for which a user account has been unlocked.
Syntax	UTF8String (SIZE (0.64))

IP Address

Variable Name	dsTrapObjectIPAddress
OID	1.3.6.1.4.1.10418.3.2.6.20
Description	This object is sent in a trap to identify the IP address for which a trap condition occurred.
Syntax	UTF8String (SIZE (0.256))

SIP Image Upgrade Result

Variable Name	dsTrapObjectSipImageUpgradeResult
OID	1.3.6.1.4.1.10418.3.2.6.21
Description	This object is sent in a trap to report the result of an SIP image upgrade.
Syntax	SyntaxINTEGER { sipUpgradeNoFirmwareImage(1), -- No firmware image present sipUpgradeLostContact(2), -- Lost communication with the SIP sipUpgradeFailedRestart(3), -- The SIP did not restart after upgrade sipUpgradeFailedVerify(4), -- The SIP failed to upgrade to correct Version sipUpgradeSuccess(9999) -- Success }

Type of SIP Image

Variable Name	dsTrapTrapObjectTypeOfImage
OID	1.3.6.1.4.1.10418.3.2.6.22
Description	This object is sent in a trap to report the type of software image for which the trap condition occurred.
Syntax	SyntaxINTEGER {boot(1),app(2)}

Virtual Media Drive Access Mode

Variable Name	dsTrapObjectVirtualMediaDriveAccessMode
OID	1.3.6.1.4.1.10418.3.2.6.23
Description	This object is sent in a trap to report the access mode associated with a remote virtual drive for which the trap condition occurred.
Syntax	SyntaxINTEGER {readonly(1),readwrite(2)}

Virtual Media Drive Type

Variable Name	dsTrapObjectVirtualMediaDriveType
OID	1.3.6.1.4.1.10418.3.2.6.24
Description	This object is sent in a trap to report the type associated with a remote virtual drive for which the trap condition occurred.
Syntax	SyntaxINTEGER {floppy_memorykey(1),cd_dvd_rom(2),generic(3)}

Image Upgrade Result Code

Variable Name	dsTrapObjectImageUpgradeResultsCode
OID	1.3.6.1.4.1.10418.3.2.6.25
Description	This object is sent in a trap to report the results of a FTP, TFTP or ASMP image upgrade.

Image Upgrade Result Code (continued)

Syntax	SyntaxINTEGER { imageUpgradeTftpNoSocket(1), -- TFTP No Socket imageUpgradeTftpConnectFailure(2), -- TFTP server TFTP connect failed imageUpgradeTftpRequestDenied(3), -- TFTP server request denied imageUpgradeTftpBadPacket(4), -- TFTP err - non-data packet received imageUpgradeTftpOOS(5), -- TFTP err - too many packets out of sequence imageUpgradeTftpTooBig(6), -- TFTP err - transferred data exceeds file size imageUpgradeTftpTimeout(7), -- TFTP err - timeout during transfer, retries exceeded imageUpgradeAlreadyInProgress(8), -- Update already in progress imageUpgradeCannotStart(9), -- Update thread did not start imageUpgradeMemoryError(10), -- Update memory allocation error imageUpgradeTftpProtocolError(11), -- TFTP protocol error occurred could not complete transfer imageUpgradeBadType(12), -- The Image type does not match the region (BOOT or APP) to update imageUpgradeInvalidAppDowngrade(13), -- Invalid downgrade version imageUpgradeChecksumError(14), -- Checksum Error imageUpgradeFlashError(15), -- Flash Error imageUpgradeInternalError(16), -- Internal error imageUpgradeFileNotFound(17), -- File not found
--------	---

Image Upgrade Result Code (continued)

Syntax (continued)	imageUpgradeBadHeader(18),	-- Invalid image header
	imageUpgradeIncompatibleHeader(19),	-- Header is not compatible
	imageUpgradeTftpXferFail(20),	-- TFTP transfer failed
	imageUpgradeTftpSvrNoResponse(21),	-- No response from TFTP server
	imageUpgradeNetworkUnreachable(22),	-- Network unreachable
	imageUpgradeSuccess(9999)	-- Success
	}	

Enterprise Traps

SNMP traps enable an agent to notify the management station of significant system events. To enable an SNMP management application to interpret system events through SNMP traps, the management application needs to know the names and types of objects in the Remote Console Switch. This is made possible by the MIB modules, which contain variables that can be set or read to provide information on the RCS.

This section describes the traps that are generated by the Dell 2161DS-2/4161DS SNMP agent. The enterprise-specific traps described in Table C-3 belong to the MIB enterprise identified by OID 1.3.6.1.4.1.10418.3.2.6, and are sent with the trap variables documented in "SNMP Trap Object Group" on page 186.

Table C-3. Enterprise Specific Traps

Trap ID	Trap Message	Severity	Description
1	The Remote Console Switch is rebooting. Command issued by user: %s.	Informational	The Remote Console Switch is in the process of rebooting. The name of the user who initiated the reboot is contained in dsTrapObjectName.
2	User logged into the Remote Console Switch. User: %s.	Informational	A user logged into the Remote Console Switch. The name of the user who logged in is contained in dsTrapObjectName.
3	User logged out of the Remote Console Switch. User: %s.	Informational	A user logged out of the Remote Console Switch. The name of the user who logged out is contained in dsTrapObjectName.
4	Video session started. User: %s. Server: %s.	Informational	A video session has started. The name of the user who is connected to the session is contained in dsTrapObjectName. The session identifier is contained in dsTrapObjectSessionIdentifier.
5	Video session stopped. User: %s. Server: %s	Informational	A video session has stopped. The name of the user who was connected to the session is contained in dsTrapObjectName. The session identifier is contained in dsTrapObjectSessionIdentifier.

Trap ID	Trap Message	Severity	Description
6	Video session terminated. Command issued by user: %s. Terminated user: %s. Server: %s.	Informational	A video session has been terminated by another user. The name of the user who terminated the session is contained in dsTrapObjectName. The name of the user who was terminated from the session is contained in dsTrapObjectTargetUserName. The session identifier is contained in dsTrapObjectSessionIdentifier.
7	Viewing started on the local port. Server: %s.	Informational	A user on the local port has started viewing a server. The session identifier is contained in dsTrapObjectSessionIdentifier.
8	Viewing stopped on the local port. Server: %s.	Informational	A user on the local port has stopped viewing a server. The session identifier is contained in dsTrapObjectSessionIdentifier.
9	FTP, TFTP, or ASMP image upgrade started. Command issued by user: %s. Image type: %s. New version: %s. Current version: %s	Informational	The Remote Console Switch has started an FTP, TFTP, or ASMP upgrade of an image. The name of the user who initiated the FTP, TFTP, or ASMP image upgrade is contained in dsTrapObjectName. The type of image that is being upgraded is contained in dsTrapObjectType. The version of the image that the Remote Console Switch is upgrading to is contained in dsTrapObjectImageNewVersion. The version of the image that the Remote Console Switch is currently running is contained in dsTrapObjectImageCurrentVersion.

Trap ID	Trap Message	Severity	Description
10	Result text: %s. Results code: %d.	Informational	The result of an FTP, TFTP, or ASMP image upgrade.
11	New user added to local user database. Command issued by user: %s. New user: %s.	Informational	A new user has been added to the local user database. The name of the user who added the new user is contained in dsTrapObjectUserName. The name of the new user is contained in dsTrapObjectTargetUserName.
12	User deleted from local user database. Command issued by user: %s. Deleted user: %s.	Informational	A user has been deleted from the local user database. The name of the user who deleted the user is contained in dsTrapObjectUserName. The name of the user who was deleted is contained in dsTrapObjectTargetUserName.
13	User modified in local user database. Command issued by user: %s. Modified user: %s.	Informational	A user was modified. The name of the user who modified the user is contained in dsTrapObjectUserName. The name of the user who was modified is contained in dsTrapObjectTargetUserName.
14	User authentication failed with the Remote Console Switch. User: %s.	Informational	A user failed to authenticate with the Remote Console Switch. The name of the user who failed to authenticate is contained in dsTrapObjectUserName.
15	SIP added. SIP ID: %s.	Informational	An SIP was added. The ID of the SIP which was added is contained in dsTrapObjectSipId.
16	SIP removed. SIP ID: %s.	Informational	An SIP was removed. The ID of the SIP which was removed is contained in dsTrapObjectSipId.

Trap ID	Trap Message	Severity	Description
17	Server name changed. Old name: %s. New name: %s. Attached to SIP: %s.	Informational	<p>The name of a server has changed.</p> <p>The previous name of the server is contained in dsTrapObjectOldServerName.</p> <p>The new name of the server is contained in dsTrapObjectServerName.</p> <p>The ID of the SIP the server is attached to is contained in dsTrapObjectSipId.</p>
18	Tiered switch added. Tiered switch name: %s. Attached to SIP: %s.	Informational	<p>A tiered switch was added.</p> <p>The name of the switch which was added is contained in dsTrapObjectTieredSwitchName.</p> <p>The ID of the SIP the switch was added to is contained in dsTrapObjectSipId.</p>
19	Tiered switch removed. Tiered switch name: %s. Was attached to SIP: %s.	Informational	<p>A tiered switch was removed.</p> <p>The name of the switch which was removed is contained in dsTrapObjectTieredSwitchName.</p> <p>The ID of the SIP the switch was attached to is contained in dsTrapObjectSipId.</p>
20	Tiered switch name changed. Old name: %s. New name: %s. Attached to SIP: %s.	Informational	<p>The name of a tiered switch has changed.</p> <p>The previous name of the tiered switch is contained in dsTrapObjectOldTieredSwitchName.</p> <p>The new name of the tiered switch is contained in dsTrapObjectTieredSwitchName.</p> <p>The ID of the SIP the switch is attached to is contained in dsTrapObjectSipId.</p>

Trap ID	Trap Message	Severity	Description
21	Configuration file loaded in the Remote Console Switch. Command issued by user: %s. Name of file loaded: %s.	Informational	<p>The Remote Console Switch has loaded a configuration file.</p> <p>The name of the user who commanded the Remote Console Switch to load the configuration file is contained in dsTrapObjectUserName.</p> <p>The name of the file that was loaded is contained in dsTrapObjectFileName.</p>
22	User database file loaded in the Remote Console Switch. Command issued by user: %s. Name of file loaded: %s.	Informational	<p>The Remote Console Switch has loaded a user database file.</p> <p>The name of the user who commanded the Remote Console Switch to load the user database file is contained in dsTrapObjectUserName.</p> <p>The name of the file that was loaded is contained in dsTrapObjectFileName.</p>
23	Invalid connection detected. Device ID: %s.	Informational	<p>The Remote Console Switch has detected an invalid connection.</p> <p>This can include two SIP devices on a port where one or more have a legacy KVM Switch, or some other illegal setup condition.</p> <p>Information about the nature of the failure is stored in the dsTrapObjectFirmwareCondition object.</p> <p>NOTE: This trap is deprecated and is no longer sent.</p>

Trap ID	Trap Message	Severity	Description
24	Subsystem Upgrade started. Device ID: %s.	Informational	<p>The Remote Console Switch has started a Subsystem Upgrade.</p> <p>This can be a download from the DModule to the main board, or an SIP or other subsystem download from the main board.</p> <p>Information about the subsystem being updated is stored in the dsTrapObjectFirmwareCondition object.</p> <p>NOTE: This trap is deprecated and is no longer sent.</p>
25	Subsystem restarting. Device ID: %s.	Informational	<p>The Remote Console Switch has completed a download and is restarting the subsystem specified in the dsTrapObjectFirmwareCondition object.</p> <p>NOTE: This trap is deprecated and is no longer sent.</p>
26	Communication problems in the system configuration. Device ID: %s.	Major	<p>The Remote Console Switch has detected communication problems in the system configuration. This can be used to indicate install problems that might result in perceived problems with the switch.</p>
27	Memory problem. Device ID: %s	Critical	<p>The Remote Console Switch has detected a memory problem, the nature of which has been described in the dsTrapObjectFirmwareCondition object.</p>
28	Watchdog reset. Device ID: %s.	Critical	<p>The Remote Console Switch has detected a watchdog reset condition. This indicates a catastrophic failure in the firmware/hardware preventing normal operation of the Remote Console Switch.</p>
29	Special condition was trapped. Device ID: %s.	Informational	<p>The Remote Console Switch has detected a special condition to be trapped for diagnostics. The condition has been recorded is stored in the dsTrapObjectFirmwareCondition object.</p>

Trap ID	Trap Message	Severity	Description
30	Subsystem upgrade failed. Device ID: %s.	Informational	The Remote Console Switch has detected a special condition resulting in a failed subsystem update. The condition has been recorded is stored in the dsTrapObjectFirmwareCondition object.
31	Warning condition. Device ID: %s. Alarm condition: %d. Alarm description: %s.	Minor	The Remote Console Switch has detected a special condition to be trapped for warning the operator. The condition indicates some parameter outside of normal operation, such as over temperature range. These are not expected to result in unusual behavior, but may be precursor to a subsequent urgent condition.
32	Urgent condition. Device ID: %s. Alarm condition: %d. Alarm description: %s.	Critical	The Remote Console Switch has detected a special condition to be trapped for alerting the operator. The condition indicates some parameter outside of normal operation that is expected to result in unpredictable system behavior.
33	User account has been locked. Client IP Address: %s. Locked user: %s. Reason: %s.	Minor	A user account has been locked. The IP address of the client is contained in dsTrapObjectIPAddress. The name of the user who was locked is contained in dsTrapObjectTargetUserName. The reason for which the user account has been locked is contained in dsTrapObjectLockReason.

Trap ID	Trap Message	Severity	Description
34	User account has been unlocked. Client IP Address: %s. Command issued by user: %s. Unlocked user: %s. Reason: %s.	Minor	<p>A user account has been unlocked.</p> <p>The IP address of the client that originated the unlock request is contained in dsTrapObjectIPAddress.</p> <p>When the user account is unlocked by an appliance reboot or by the expiration of the lockout period (as specified in the dsTrapObjectUnlockReasonobject), the IP address will be blank.</p> <p>The name of the user who unlocked the user is contained in dsTrapObjectUserName.</p> <p>When the user account is unlocked by an appliance reboot or by the expiration of the lockout period (as specified in the dsTrapObjectUnlockReason object), the name of the user will be blank.</p> <p>The name of the user who was unlocked is contained in dsTrapObjectTargetUserName.</p> <p>The reason for which the user account has been unlocked is contained in dsTrapObjectUnlockReason.</p>

Trap ID	Trap Message	Severity	Description
35	SIP image upgrade started. Command issued by user: %s. Image type: %s. New version: %s. Current version: %s. Server: %s. SIP ID: %s.	Informational	<p>A software image upgrade has started on an SIP.</p> <p>The name of the user who initiated the SIP upgrade is contained in dsTrapObjectUserName.</p> <p>The type of software image being upgraded is contained in dsTrapObjectSipTypeOfImage.</p> <p>The software image version the SIP is upgrading to is contained in dsTrapObjectImageNewVersion.</p> <p>The software image version the SIP is currently running is contained in dsTrapObjectImageCurrentVersion.</p> <p>The name of the server connected to the SIP being upgraded is contained in dsTrapObjectServerName.</p> <p>The ID of the SIP being upgraded is contained in dsTrapObjectSipId</p>

Trap ID	Trap Message	Severity	Description
36	SIP image upgrade result. Result: %d. Upgrade was started by user: %s. Upgrade image type: %d. Upgrade version: %s. Running version: %s. Server: %s. SIP ID: %s.	Informational	<p>The result of an SIP software image upgrade.</p> <p>The image upgrade result is contained in dsTrapObjectSipImageUpgradeResult.</p> <p>The name of the user who initiated the SIP upgrade is contained in dsTrapObjectUserName.</p> <p>The type of software image the upgrade result is for contained in dsTrapObjectTypeOfImage.</p> <p>The software image version the SIP attempted to upgrade to, is contained in dsTrapObjectImageNewVersion.</p> <p>The software image version the SIP is running is contained in dsTrapObjectImageCurrentVersion.</p> <p>If the software image upgrade was successful then this version will match the version reported in dsTrapObjectImageNewVersion.</p> <p>The name of the server connected to the SIP is contained in dsTrapObjectServerName.</p> <p>The ID of the SIP the result is for is contained in dsTrapObjectSipId.</p>
37	SIP restarted. Server: %s. SIP ID: %s.	Informational	<p>An SIP has restarted</p> <p>An SIP will restart after an SIP image upgrade completes.</p> <p>The name of the server connected to the SIP is contained in dsTrapObjectServerName.</p> <p>The ID of the SIP that restarted is for is contained in dsTrapObjectSipId.</p>

Trap ID	Trap Message	Severity	Description
38	Remote virtual media session started. User: %s. Server: %s. SIP: %s.	Informational	<p>A remote Virtual Media session to a server has started. A video session to the server must have been established by the same user prior to starting the VM session.</p> <p>The name of the user who connected to the VM session is contained in dsTrapObjectUserName.</p> <p>The name of the server the user connected to is contained in dsTrapObjectServerName.</p> <p>The ID of the SIP the video session is using is contained in dsTrapObjectSipId.</p>
39	Remote virtual media session stopped. User: %s. Server: %s.	Informational	<p>A remote virtual media session to a server has stopped.</p> <p>The name of the user who was connected to the VM session is contained in dsTrapObjectUserName.</p> <p>The name of the server the user was connected to is contained in dsAvrTrapObjectServerName.</p>
40	Remote video session terminated. Command issued by user: %s. Terminated user: %s. Server: %s.	Informational	<p>A remote virtual media session has been terminated or preempted by another user.</p> <p>The name of the user who terminated or preempted the VM session is contained in dsTrapObjectUserName if available. An empty string is reported if a user name is not available. A user name will not be available if the remote session was terminated or preempted from the OSCAR interface and OSCAR interface authentication is disabled.</p> <p>The name of the user who was terminated or preempted from the VM session is contained in dsTrapObjectTargetUserName.</p> <p>The name of the server the user was connected to contained in dsTrapObjectServerName.</p>

Trap ID	Trap Message	Severity	Description
41	Remote virtual media session has been reserved. User: %s. Server: %s.	Informational	<p>A user established a reserved remote virtual media session.</p> <p>The name of the user who has established a reserved virtual media session is contained in dsTrapObjectUserName.</p> <p>The name of the server the user was connected to is contained in dsTrapObjectServerName.</p>
42	User has established a non-reserved virtual media session to server. User: %s. Server: %s.	Informational	<p>A user established a non-reserved remote virtual media session.</p> <p>The name of the user who has established a non-reserved virtual media session is contained in dsTrapObjectUserName.</p> <p>The name of the server the user was connected to is contained in dsTrapObjectServerName.</p>
43	Remote virtual media drive has been mapped. User: %s. Server: %s Drive Type: %s. Drive Access Mode: %s.	Informational	<p>A remote virtual media drive has been mapped.</p> <p>The name of the user who has established the virtual media session is contained in dsTrapObjectUserName.</p> <p>The name of the server the user was connected to is contained in dsTrapObjectServerName.</p> <p>The type of drive that has been mapped is contained in dsTrapObjectVirtualMediaDriveType.</p> <p>The access mode for the drive that has been mapped is contained in dsTrapObjectVirtualMediaDriveAccessMode.</p>

Trap ID	Trap Message	Severity	Description
44	Remote virtual media drive has been unmapped. User: %s. Server: %s Drive Type: %s. Drive Access Mode: %s.	Informational	<p>A remote virtual media drive has been unmapped.</p> <p>The name of the user who has established the virtual media session is contained in dsTrapObjectUserName.</p> <p>The name of the server the user was connected to is contained in dsTrapObjectServerName.</p> <p>The type of drive that has been unmapped is contained in dsTrapObjectVirtualMediaDriveType.</p> <p>The access mode for the drive that has been unmapped is contained in dsTrapObjectVirtualMediaDriveAccessMode.</p>
45	Virtual Media Drive Mapped on the local port. Server: %s.	Informational	<p>A user on the local port has mapped a virtual media drive to the server.</p> <p>The session identifier is contained in dsKvmTrapObjectSessionIdentifier.</p> <p>The type of drive that has been unmapped is contained in dsTrapObjectVirtualMediaDriveType.</p> <p>The access mode for the drive that has been unmapped is contained in dsTrapObjectVirtualMediaDriveAccessMode.</p>
46	Virtual Media Drive Unmapped on the local port. Server: %s.	Informational	<p>A user on the local port has unmapped a virtual media drive to the server.</p> <p>The session identifier is contained in dsTrapObjectSessionIdentifier.</p> <p>The type of drive that has been unmapped is contained in dsTrapObjectVirtualMediaDriveType.</p> <p>The access mode for the drive that has been unmapped is contained in dsTrapObjectVirtualMediaDriveAccessMode.</p>

Trap ID	Trap Message	Severity	Description
47	Local video session terminated. Command issued by user: %s. Server: %s.	Informational	<p>A local virtual media session has been terminated or preempted by another user.</p> <p>The name of the user who terminated or preempted the VM session is contained in dsTrapObjectName if available. An empty string is reported if a user name is not available. A user name will not be available if the remote session was terminated or preempted from the OSCAR interface and OSCAR authentication is disabled.</p> <p>The name of the server the user was connected to contained in dsTrapObjectServerName.</p>
48	Local virtual media session has been reserved. Server: %s.	Informational	<p>A local user has reserved a virtual media session.</p> <p>The name of the server the user was connected to is contained in dsTrapObjectServerName.</p>
49	Local virtual media session has been unreserved. Server: %s.	Informational	<p>A user has unreserved a local virtual media session.</p> <p>The name of the server the user was connected to is contained in dsTrapObjectServerName.</p>
50	Local Port Video session terminated. Command issued by user: %s. Server: %s.	Informational	<p>A local user video session has been terminated by another user.</p> <p>The name of the user who terminated the session is contained in dsTrapObjectName.</p> <p>The session identifier is contained in dsTrapObjectSessionIdentifier.</p>

Trap ID	Trap Message	Severity	Description
51	CA Certificate file loaded in the Remote Console Switch. Command issued by user: %s.	Informational	The Remote Console Switch has loaded a CA Certificate file. The name of the user who commanded the Remote Console Switch to load the CA Certificate file is contained in dsTrapObjectName.

Appendix D: FLASH Upgrades

Upgrading the Remote Console Switch

The Remote Console Switch FLASH upgrade feature allows you to update your Remote Console Switch with the latest firmware available.

You can upgrade the switch firmware either through a serial console or directly in the OSCAR interface or the on-board web interface.



NOTE: If the Enable SIP Autoupdate option is selected, all attached SIPs are automatically upgraded when the firmware is upgraded. For information about enabling and disabling the Enable SIP Autoupdate option, see "Upgrading the SIP module firmware" on page 214.

Upgrade Firmware Using the On-board Web Interface

See "Upgrading Firmware" on page 120.

Upgrading Firmware Using a Serial Console

Items needed for the upgrade:

- Server running serial terminal application
- Available serial port (COM port) on the server
- Serial cable
- Firmware update

To upload a new FLASH file:



CAUTION: The Remote Console Switch begins the FLASH upgrade process. On screen indicators display the upgrade process. When the upload is complete, the switch resets and upgrades the internal sub-systems.

- 1** Connect a terminal or PC running terminal emulation software to the configuration port on the back panel of the Remote Console Switch. The terminal should be set to 9600 bps, 8 bits, 1 stop bit, no parity and no flow control.
- 2** Connect the LAN port on the Remote Console Switch to an Ethernet hub that is also connected to the PC being used as the TFTP or FTP server.

- 3** Launch both the server TFTP or FTP software and the terminal emulation software.
- 4** Verify that the Remote Console Switch is turned on. After approximately 40 seconds, the Remote Console Switch sends a message, **Dell Remote Console Switch Ready ... Press any key to continue**. Press any key to access the main menu. The Remote Console Switch main menu appears.
- 5** Get the IP address of the TFTP or FTP server.
- 6** Assign the IP address in the Remote Console Switch, if needed:
 - a** In the **HyperTerminal** window, type **1** to select **Network Configuration**.
 - b** Note the Remote Console Switch IP address. The first three numbers must be the same as in the server IP address from step 5. The last number must be different. If the Remote Console Switch IP address is not correct, change it as follows: type **3** to select **IP address**, then enter the correct address.
 - c** Type **0** to exit the **Network Configuration** menu. If you changed the IP address, follow the directions on the screen.
- 7** From the main menu, type **2** to select **Firmware Management**. The current version of your firmware displays in the **Firmware Management** screen.
- 8** From the **Firmware Management** menu, type **1** to select **FLASH Download (TFTP)** or type **2** to select **FLASH Download (FTP)**.
- 9** Type the IP address of the TFTP or FTP server and press **<Enter>**.
- 10** Type the name of the **FLASH** file and press **<Enter>**.
- 11** If using an **FTP** server, type the **FTP** server username and password and press **<Enter>**.
- 12** Confirm the **TFTP** or **FTP** download by typing **y** or **yes** and pressing **<Enter>**.
- 13** The Remote Console Switch verifies the file you downloaded is valid. You are prompted to confirm the upgrade. Type **y** or **yes** and **<Enter>**.
- 14** The Remote Console Switch will begin the **FLASH** upgrade process. On screen indicators displays the upgrade process. When the upload is complete, the Remote Console Switch resets and upgrades the internal subsystems.

- 15 When the upgrade is complete, the startup message from step 4 appears on the terminal screen.

Upgrading Remote Console Switch Firmware in the OSCAR interface

You can upgrade the Remote Console Switch firmware version directly from the OSCAR interface. If using IPv4 mode, you may use either a TFTP server or an FTP server. If using IPv6 mode, you must use an FTP server. To upgrade the firmware, you need to know the IP address of the server, the filename of the firmware FLASH file, and, if using an FTP server, the username and password for the FTP server. You will also need to make sure that the file is in the appropriate folder.

To upgrade the Remote Console Switch firmware:

- 1 Press <Print Screen>. The **Main** dialog box displays.
- 2 Click **Commands - Display Versions**. The **Versions** dialog box displays.
- 3 Click **Upgrade**. The **Download** dialog box is displayed.

Figure D-1. Download Dialog Box



- 4 If you are in IPv4 mode and are using a TFTP server, select **TFTP**.
- or-

If you are in IPv4 mode and are using an FTP server, select **FTP**.



NOTE: If you are in IPv6 mode, the FTP button will automatically be selected and the TFTP button will be grayed out and may not be selected.

- 5 In the **IP address** field, type the IP address of the TFTP or FTP server where the Remote Console Switch firmware FLASH file is located.
- 6 In the **Filename** field, type the directory path and filename of the firmware FLASH file.
- 7 If you are using an FTP server, enter the username and password for the FTP server in the **Username** and **Password** fields.
- 8 Click **Download**. The firmware upgrade proceeds.
- 9 A Warning window opens. Click **OK**. Once the firmware upgrade has completed, the Remote Console Switch will automatically reboot.

Recovering From a Failed Flash Upgrade



NOTE: You may only recover from a failed Flash upgrade when using IPv4 mode.



NOTE: If the green power LED on the front and back panel of the Remote Console Switch blinks continuously, the Remote Console Switch is in recovery mode.

To recover from a failed Flash upgrade:

- 1 Download the latest Flash firmware.
- 2 Save the Flash upgrade file to the appropriate directory on the TFTP server.
- 3 Set up the TFTP server with the server IP address 10.0.0.3.
- 4 Rename the downloaded file CMN-xxxx.fl, where xxxx is the number on the agency label on the underside of the Remote Console Switch, and place it into the TFTP root directory of the TFTP server.
- 5 If the Remote Console Switch is not on, turn it on now. The recovery process should start automatically.

Upgrading the SIP module firmware

The SIP modules can be upgraded individually or simultaneously.

To simultaneously upgrade multiple SIP modules:

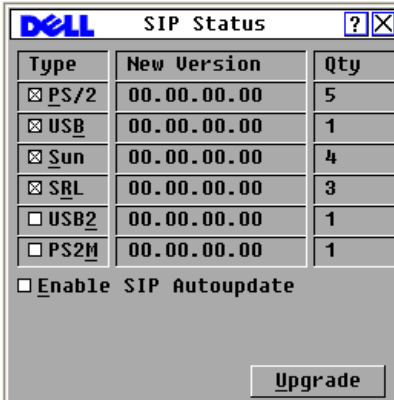
- 1 Press <Print Screen>. The **Main** dialog box displays.
- 2 Click **Commands - SIP Status**. The **SIP Status** dialog box displays.



NOTE: When the Enable SIP Autoupdate option is enabled in the SIP Status dialog box, SIP firmware is automatically upgraded when the Remote Console Switch firmware is upgraded or when a new SIP is discovered by the Remote Console

Switch after an firmware upgrade. SIPs that have already been discovered but which are not attached to the Remote Console Switch during the firmware upgrade must be upgraded manually.

Figure D-2. SIP Status Dialog Box

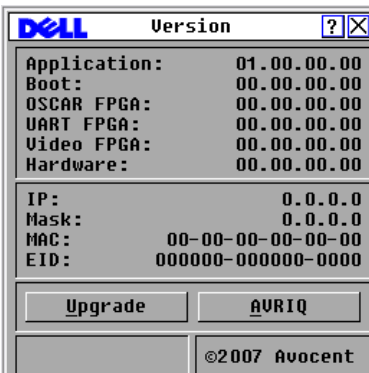


- 3 Click one or more types of modules to upgrade. Click **Upgrade**.
- 4 The **SIP Upgrade** dialog box displays. Click **OK** to initiate the upgrade and return to the **SIP Status** dialog box.

To upgrade SIP module firmware individually:

- 1 Press <Print Screen>. The **Main** dialog box will appear.
- 2 Click **Commands - Display Versions**. The **Version** dialog box displays.

Figure D-3. Version Dialog Box



- 3** Click **SIP** to view individual SIP module version information. The **SIP Select** dialog box displays.
- 4** Select a SIP module to upgrade and click the **Version** button. The **SIP Version** dialog box displays.
- 5** Click the **Load Firmware** button. The **SIP Load** dialog box displays.
- 6** Click **OK** to initiate the upgrade and return to the **Status** dialog box.



NOTE: During an upgrade, the SIP status indicator in the **Main** dialog box is yellow. The SIP module is unavailable while an upgrade is in progress. When an upgrade is initiated, any current connection to the server via the SIP module is terminated.



NOTE: If you wish to return a SIP to its factory settings, click **SIP** in the **Version** dialog box. The **SIP Version** dialog box displays. Click **Decommission** and then **OK** to restore factory defaults to the SIP.

Appendix E: Technical Specifications

Table E-1. 2161DS-2/4161DS Remote Console Switch Product Specifications

Server Ports

Number	16
Types	Dell PS/2 and USB SIP modules. Avocent brand PS/2, PS2M, USB, Sun and serial IQ modules.
Connectors	RJ-45
Sync Types	Separate horizontal and vertical
Plug and Play	DDC2B
Video Resolution	Analog Port Maximum 1280 x 800 @ 60Hz

Network Configuration Port

Number	1
Type	Serial RS-232
Connector	DB9 Female

Analog Port Sets

Number	1
Type	PS/2, USB, VGA and ACI
Connectors	PS/2 miniDIN, 15 pin D, RJ-45

Dimension

Dimensions (H x W x D)	4.45 x 43.18 x 27.94 cm 1U form factor (1.75 x 17.00 x 11.00 in.)
Weight	3.6 kg (8 lb) without cables
Heat Dissipation	92 BTU/Hr
Airflow	8 cfm
Power Consumption	12.5 W

Table E-1. 2161DS-2/4161DS Remote Console Switch Product Specifications

AC-input power	40 W maximum
AC-input voltage rating	100 to 240 VAC Autosensing
AC-input current rating	0.5 A
AC-input cable	18 AWG three-wire cable, with a three-lead IEC-320 receptacle on the power supply end and a country or region dependent plug on the power resource end
AC-frequency	50/60 HZ
Temperature	0° to 50° Celsius (32° to 122° Fahrenheit) operating -20° to 60° Celsius (-4° to 140° Fahrenheit) nonoperating
Humidity	20 to 80% noncondensing operating 5 to 95% noncondensing nonoperating

Safety and EMC Approvals and Markings

UL / cUL, CE - EU, N (Nemko), GOST, C-Tick, NOM / NYCE, MIC (BCC), SASO, TUV-GS, IRAM, FCC, ICES, VCCI, SoNCAP, SABS, Bellis, FIS/ Kvalitet, Koncar, CKT, INSM, Ukrtest, STZ

Table E-2. 2321DS Remote Console Switch Product Specifications

Remote Console Switch Product Specifications

Server Ports

Number	32
Types	Dell PS/2 and USB SIP modules. Avocent brand PS/2, PS2M, USB, Sun and serial IQ modules.
Connectors	RJ-45
Sync Types	Separate horizontal and vertical
Plug and Play	DDC2B
Video Resolution	Analog Port Maximum 1280 x 800 @ 60 Hz

Network Configuration Port

Number	1
--------	---

Table E-2. 2321DS Remote Console Switch Product Specifications

Remote Console Switch Product Specifications	
Type	Serial RS-232
Connector	RJ-45
Analog Port Sets	
Number	1
Type	PS/2, USB, VGA and ACI
Connectors	PS/2 miniDIN, 15 pin D, RJ-45
Serial Power Control (PDU) Port	
Number	2
Type	RS-232 serial
Connector	8-pin modular (RJ45)
Dimension	
Dimensions (H x W x D)	4.37 x 43.18 x 35.62 cm 1U form factor (1.72 x 17.00 x 14.025 in)
Weight	10 lbs (4.5 kg) without cables
Heat Dissipation	45.0 BTU/hr
Airflow	8 cfm
Power Consumption	13.2 W
AC-input power	40 W maximum
AC-input voltage rating	100 to 240 VAC Autosensing
AC-input current rating	1.25 A
AC-input cable	18 AWG three-wire cable, with a three-lead IEC-320 receptacle on the power supply end and a country or region dependent plug on the power resource end
AC-frequency	50/60 HZ
Temperature	0° to 50° Celsius (32° to 122° Fahrenheit) operating -20° to 60° Celsius (-4° to 140° Fahrenheit) nonoperating
Humidity	20 to 80% noncondensing operating 5 to 95% noncondensing nonoperating

Table E-2. 2321DS Remote Console Switch Product Specifications

Remote Console Switch Product Specifications

Safety and EMC Approvals and Markings

UL / cUL, CE - EU, N (Nemko), GOST, C-Tick, NOM /
NYCE, MIC (BCC), SASO, GS, IRAM, FCC, ICES,
VCCI, SoNCAP, SABS, Bellis, FIS/ Kvalitet, Koncar,
KUCAS, INSM, Ukrtest, STZ

Appendix F: Technical Support

Our Technical Support staff is ready to assist you with any installation or operating issues you encounter with your Dell product. If an issue should develop, follow the steps below for the fastest possible service.

To resolve an issue:

- 1** Check the pertinent section of this manual to see if the issue can be resolved by following the procedures outlined.
- 2** Check our web site at dell.com/support to search the knowledge base or use the on-line service request.
- 3** Call the Dell Technical Support location nearest you.

Index

Numerics

- 2161DS-2 or 4161DS With a Cat 5 Analog Switch, 28
- 2161DS2/4161DS2 Console Switch
 - Configuring, 18
 - Installing, 17
- 2161DS2/4161DS2 Console Switch Unit
 - Installing, 15

A

- Access Rights
 - using the on-board web interface, 107
- Active Directory
 - adding users and privileges with Dell Schema Extensions, 166
 - configuring group objects with, 155
 - configuring with Dell Schema Extensions, 164
 - frequently asked questions, 171
 - installing, 143
 - logging in to the remote console switch with, 170
 - structure of, 139
- Address Resolution Protocol. See ARP.

AMP

- accessing, 133
- migrating switches to the on-board web interface with, 135
- Appliance Management Panel.
See AMP.
- ARI, 1, 5, 25, 30, 35
- ARP, 24

B

- Broadcasting, 57
- Browsers
 - supported by the on-board web interface, 32

C

- CA certificate, 149, 151, 154
- Cascade switch, 26
- CAT 5, 1
- Clear Offline button
 - using the on-board web interface, 115
- Configuration files
 - using the on-board web interface reading and saving, 125-126

Configuration information, 55

Connection sharing, 86

Console security, 43

D

Database

- using the on-board web interface
managing, 126

Dell Extended Schema

- AD object overview, 159

- comparing standard schema
with, 142

- using Dell Association Objects
syntax, 167

Dell Schema Extensions

- adding remote console switch
users and privileges with, 166

- configuring AD with, 164

Display behavior, 41

DNS settings, 144

DSView 3 software, 2

E

EID, 1-2

Encryption

- using the on-board web
interface, 103

- using virtual media, 95

Enterprise Traps, 195

Ethernet, 10

F

Firmware

- upgrading using the AMP, 134

- upgrading using the on-board web
interface, 120

FLASH upgrade

- overview, 5

- using a serial console, 211-212

- using the OSCAR interface, 213

G

Group objects, 155

I

Installation and setup

- of the on-board web interface, 32

- of the Remote Console Switch, 10

IQ module, 1, 7, 10

K

Keep Alive functionality, 1

Keyboard

- shortcuts, 175

- types, 11

Keystrokes

- broadcasting, 57

- using macros, 81

L

Language

- setting using the on-board web interface, 115
- setting using the OSCAR interface, 47

LDAP

- authentication parameters, 146
- overview, 6, 139
- SSL certificates, 149

M

Macros, 81

- Manage Remote Console Switch task button
 - launching the AMP, 133

- Management Information Bases.
 - See MIBs.

MIBs, 181

Mouse

- acceleration, 9, 24
- shortcuts, 175
- using the Viewer
 - adjusting, 74
 - improving performance, 76
 - minimizing trailing, 76
 - setting the scaling, 75

N

Network configuration, 9, 18

Network settings

- configuring using the OSCAR interface, 50

Network time protocol settings, 145

Noise Adjust Threshold, 76

O

On-board web interface

- migrating switches from the Remote Console Switch Software, 101
- overview, 2
- viewing and configuring Remote Console Switch parameters, 102
- viewing version information, 116

OpenManage IT Assistant Event Viewer

- enabling SNMP traps using the on-board web interface, 111
- overview, 6

Operation modes, 4

OSCAR interface

- configuring menus, 40
- navigating, 38
- overview, 2

Override admin account, 144

P

PEM, 11, 30

Port Expansion Module. See PEM.

Power indicator, 17

Preemption

using the on-board web interface, 104

using the OSCAR interface, 54

using the Viewer, 84

Privileges, 166

R

Rack mounting, 11

Reboot system

using the on-board web interface, 125

Remote Console Switch

basic configuration, 16

features and benefits, 1

viewing and configuring parameters using the on-board web interface, 102

Remote Console Switch

Software

features and benefits, 5

setup, 10

Resync Wizard, 137

S

Scan mode

using the on-board web interface, 79

using the OSCAR interface, 52

using the Viewer, 78

Screen capturing, 83

Screen Delay Time, 42

Screen saver, 45

Secure Socket Layer. See SSL

Security

overview, 3

setting using the OSCAR interface, 43

Security Lock-Out feature

using the on-board web interface, 105, 108

Server

using OSCAR

viewing/selecting, 35

using the on-board web interface

accessing, 65

using the OSCAR interface

assigning names, 49

broadcasting to, 58

disconnecting from, 37

selecting, 37-38

viewing the status of, 36

using the Viewer

interacting with, 66

scanning, 77

Set Position flag, 46

SIP

connecting to, 24

overview, 1

viewing

using the on-board web interface, 115

- SNMP
 - enterprise Traps, 195
 - MIBs, 181
 - traps, 111, 181
 - using the on-board web interface
 - configuring settings, 110
 - enabling/configuring, 109
 - Soft switching, 37
 - SSL certificates, 149
 - Status
 - of server using the Viewer, 79
 - of switch using the OSCAR interface, 36
 - using the on-board web interface of server, 65, 115
 - Status flag, 45
 - System diagnostics, 56
- T**
- TCP ports, 179
 - Technical specifications, 217
 - Technical support, 221
 - Terminal applications, 18-19, 21, 23
 - Thumbnail Viewer
 - navigating, 80
 - overview, 65
 - scanning servers, 77
 - viewing status indicators, 79
 - Tiered switch
 - using the on-board web interface
 - resetting a connected
 - SIP, 117
 - viewing and configuring connections, 114
 - Time Between Servers, 77, 80
 - Toolbar Hide Delay Time, 69
 - Trap Destination
 - using the on-board web interface, 111
- U**
- User accounts
 - using the on-board web interface
 - adding/modifying, 106
 - changing password, 108, 123
 - deleting, 108
 - locking/unlocking, 108
 - setting up, 104
 - using the OSCAR interface
 - setting the password, 43
- V**
- Version information
 - viewing using the on-board web interface, 116
 - viewing using the OSCAR interface, 52
 - Video
 - adjusting using the Viewer, 72
 - overview, 4
 - Video Optimization, 24
 - View Time Per Server, 77, 80

Viewer

- adjusting, 68
- adjusting resolution, 71
- expanding and refreshing, 70
- features of, 67

Virtual media

- configuring using the on-board web interface, 93
- configuring using the OSCAR interface, 90
- launching using the Viewer, 95
- overview, 3, 89