Dell™ Server Console Switch
User's Guide

Notes, Cautions, and Warnings

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

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

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

Contents

1

Product Overview

The Dell 1081AD/2161AD Server Console Switch (SCS) is an analog keyboard, video, and mouse (KVM) switch that provides flexible, centralized local access to data center servers. It can also provide centralized remote access to data center servers when used in conjunction with the optional Remote Access Key (RAK).

Features and Benefits

Reduce Cable Bulk

With device densities continually increasing, cable bulk remains a major concern for network administrators. The SCS significantly reduces KVM cable volume in the rack by utilizing the innovative Server Interface Pod (SIP) and single, industry-standard Unshielded Twisted Pair (UTP) cabling. This allows a higher device density while providing greater airflow and cooling capacity.

SIP Intelligent Modules

The SCS supports SIPs that are powered directly from the target device and provide Keep Alive functionality when the SCS is not powered. The SIPs with CAT 5 design dramatically reduce cable clutter while providing optimal resolution and video settings. The built-in memory of SIPs simplifies configuration by assigning and retaining unique device names and Electronic ID (EID) numbers for each attached device.

PS/2 and USB SIPs are available allowing direct KVM connectivity to devices. The USB2+CAC SIP is also available. The SCS is offered with 8 or 16 ARI

ports that are used to connect SIPs to the SCS. Then utilizing the SIPs, you can attach additional switches to expand your SCS system. This flexibility allows you to add capacity as your data center grows.

Multiplatform Support

Dell SIPs are available for use with the SCS to support PS/2, USB, USB2, and USB2+CAC device environments.

Interoperability with Avocent® IQ Module Intelligent Cabling may also be used to connect local devices to the SCS. PS/2, USB, and Sun® module options are available. For more information, please refer to the appropriate Avocent installer/user guide for your product or visit avocent.com/manuals for more information.

User Interfaces

The SCS is equipped with two "point-and-click" interfaces to manage the SCS locally. They are the local user interface (UI), referred to as OSCAR™, and the on-board web interface (OBWI). Using the configuration options provided by these interfaces, you can tailor your SCS to your specific application. The OBWI can also be used to access and control any attached devices, and handle all basic KVM needs remotely.

> **NOTE:** Remote KVM sessions via the OBWI requires the installation of the Dell RAK.

OSCAR Interface

The OSCAR interface, accessed using the local port, features intuitive menus and operation modes to configure your SCS and devices. Devices can be identified by name, EID, or port number.

The OSCAR interface allows you to protect your system with a screen saver password. When the screen saver mode engages, 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 SCS is in a data center infrastructure protected by a firewall.

OBWI

You can also use the OBWI to manage your SCS. The OBWI is launched directly from the SCS and does not require a software server or any installation. With the addition of the optional Dell RAK installed, you can also establish remote KVM and virtual media sessions to target devices. For more information, see "Dell Remote Access Key (RAK)" on page 4.

Terminal Console Interface

The terminal console interface is accessed through the "10101" setup port. A terminal screen or a PC running terminal emulation software can be used to access these screens.

Virtual Media and Smart Card-capable Switches

The SCS allows you to view, move, or copy data located on local media and smart cards. Smart cards are pocket-sized cards that store and process information including identification and authentication information to enable access to computers, networks, and secure rooms or buildings.

A virtual media or a smart card reader can be connected directly to the USB ports on the SCS. In addition, virtual media or smart card readers may be connected to any remote workstation that is running the remote OBWI, SCS Software, or Avocent management software, and is connected to the SCS using an Ethernet connection.

NOTE: To open a virtual media or smart card session with a target device, you must first connect the target device to an SCS using a USB 2.0 or USB+CAC SIP.

IPv4 and IPv6 Capabilities

The SCS is compatible with systems using either of the currently used Internet Protocol Versions, IPv4 or IPv6. You can change the network settings and choose either IPv4 or IPv6 mode via the terminal console, OSCAR interface, or OBWI.

Access the SCS Using a Standard TCP/IP Network

The device is accessible for configuration via the standard TCP/IP Network. If the optional Dell RAK is installed, you can access all attached systems via Ethernet. See "Dell Remote Access Key (RAK)" on page 4.

NOTE: The client connects to the SCS using an Internet browser.

NOTE: KVM over IP sessions are supported when the Dell RAK is installed.

Upgradeable

Upgrade your SCS and SIPs at any time to ensure you are always running the most current firmware version available. Upgrades can be initiated through the OSCAR interface, OBWI, or the terminal console screens. The SCS can also be configured to perform automatic firmware upgrades of SIPs. For more information, see "Tools - Rebooting and Upgrading" on page 65.

Two-tier Expansion

The SCS allows you to tier one additional SCS, CS, or RCS from each ARI port on the primary SCS. Each tiered SCS is 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 "Tiering Your Switch Using a SIP" on page 26.

Dell Remote Access Key (RAK)

The optional Dell RAK, installed in the USB port, supports the following features.

KVM Remote Access

A single KVM remote user is supported using the RAK. With the RAK, you can manage remote operating system installation, operating system recovery, hard drive recovery or duplication, BIOS updating, and server backup.

Avocent Management Software Plug-in

Avocent management software may be used with the SCS to allow IT administrators to securely and remotely access and monitor target devices on multiple platforms through a single, web-based user interface. A session may be launched to a device from a single point of access. For more information, see the Technical Bulletin for the management software plug-in.

Local Video Scaling

The SCS digitizes a video signal with a maximum pixel resolution of up to 1600 x 1200 or 1680 x 1050 (widescreen), depending on the length of cable separating your SCS and devices.

Encryption

The SCS supports 128-bit SSL(ARCFOUR), AES, DES, and 3DES encryption of keyboard/mouse, video, and virtual media sessions.

Figure 1.1: Example Server Console Switch Configuration
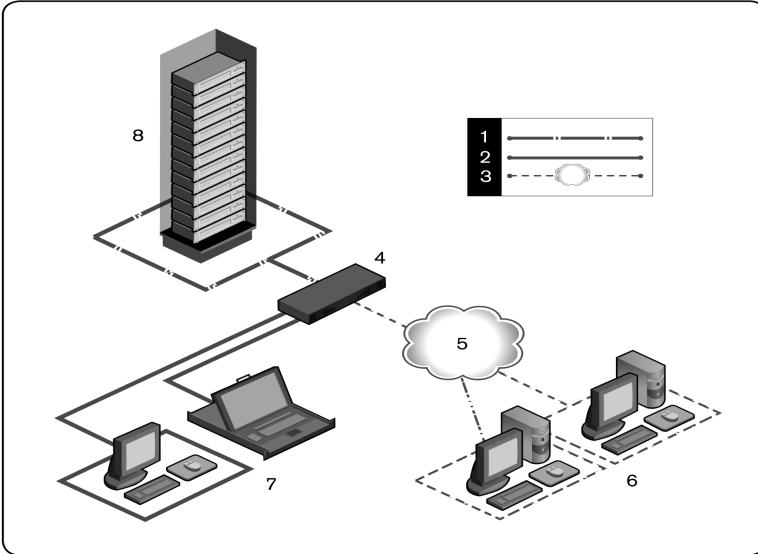
Table 1.1: Descriptions for Figure 1.1

Number	Description	Number	Description
1	UTP Connection	5	Ethernet
2	Local KVM Connection to the Server Console Switch	6	Digital Users (computer with Internet Browser for OBWI or RCS Software and/or Avocent Management Software Server [requires the Dell RAK])
3	Remote IP Connection	7	Local Analog Users (OSCAR Interface and/or Local LCD Tray)
4	Server Console Switch (2161AD shown)	8	Servers/Target Devices

Safety Precautions

This document pertains only to the Dell 1081AD/2161AD Server Console Switch. You should also refer to the following additional safety instructions.

- Dell Safety Sheet
- Dell RTF Regulatory Tech Bulletin

General

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 the Dell™ Server Console Switch, Dell™ PowerEdge™ server, and Dell PowerVault™ storage system.

- 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.

> **NOTE:** 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 adaptor 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.

LAN Related Precautions

- 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.

2

Installation

The SCS uses TCP/IP for communication over Ethernet. For the best system performance, use a dedicated, switched 100BaseT network. You can also use 10BaseT Ethernet.

You may use the terminal software, OSCAR interface, or the OBWI to manage your SCS system. The OBWI manages a single switch and its connections. With the optional Dell RAK, you can also perform KVM and serial switching tasks using the OBWI or Avocent management software. For more information about Avocent management software, visit http://www.avocent.com/dell.

NOTE: The RCS software can be used to manage other switches. For more information, please refer to the appropriate installer/user guide for your product.

NOTE: Ensure that every switch has been upgraded to the most recent version of firmware. For information on upgrading the switch using the OBWI, see "Tools - Rebooting and Upgrading" on page 65.

Getting Started

The following items are supplied with the SCS. Before installing your SCS, locate the necessary items for proper installation.

- Server Console Switch

- Power Cord

- 0U Mounting Bracket Kit

- 1U Mounting Bracket Kit (two additional rails are pre-mounted to the SCS assembly)

- Cable and Adaptors for the 10101 Console Setup Port

- User Documentation CD

- Server Console Switch Quick Installation Guide

- Dell Rack Mounting Quick Installation Guide

- Dell Safety Sheet

- Dell RTF Regulatory Technical Bulletin

Additional items needed:

- One Dell SIP or Avocent IQ module per attached device

- One CAT 5 Patch Cable (up to 30 meters) per attached device

Optional Items:

- Dell Remote Access Key (RAK)

- Port Expansion Module (PEM)

> **NOTE:** You cannot open a virtual media session or a CAC session if the device is connected via a PEM.

Setting Up Your Network

The SCS uses IP addresses to uniquely identify the SCS and attached devices. The SCS supports both Dynamic Host Configuration Protocol (DHCP) and static IP addressing. Make sure that an IP address is reserved for each SCS and that each IP address remains static while the SCS is connected to the network.

Keyboards

A USB keyboard and mouse can be connected to the analog ports of the SCS.

> **NOTE:** The SCS 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.

SCS Quick Setup

The following is a quick setup list. For detailed rack mounting and installation instructions, see "Rack Mounting the Switch" on page 14.

1   Unpack the SCS and verify that all components are present and in good condition.

2   Install the SCS hardware and connect a SIP or Avocent IQ module to each target device or tiered SCS. Connect each SIP or Avocent IQ module to the SCS with CAT 5 cabling and connect the keyboard, monitor, and mouse connectors to the analog ports of the SCS.

3   Connect the local port peripherals to the appropriate ports on the back panel of the SCS and set up the network configuration. The IP address can be set here or from the RCS software. Dell recommends using a static IP address.

4   For the local port connection, input all device names using the OSCAR interface or the OBWI.

5   Adjust mouse acceleration on each device to **Slow** or **None**.

To set up the RCS software (see the Remote Console Switch Software User's Guide):

1   Install the RCS software on each client workstation.

2   From one client workstation, launch the RCS software.

3   If you have installed the RAK, click the **New Server Console Switch** task button to add the new switch to the RCS software database. If you configured the IP address as described above, select **Yes**, the product already has an IP address; otherwise select **No**, the product does not have an IP address.

   The RCS software will find the switch and all SIPs connected to it and display the names in the Explorer.

NOTE: Using RCS software you can add and manage the Dell SCS, Dell RCS, and some Avocent switches.

4   Set properties and group devices as desired into locations, sites, or folders through the Explorer.

5   Create user accounts through the OBWI. For more information, see "Local User Account Settings" on page 75.

6   If the local user adds, deletes, or renames any SIPs after you have loaded this file, you can resynchronize your local SCS by selecting the SCS and clicking **Resync**. To control a connected device, select it in the Explorer and click the **Connect Video** task button to launch a device session in the Viewer.

7   Select **View - Scaling** to adjust the resolution and select **View - Color** of the device video quality in the Viewer.

Rack Mounting the Switch

You may either place the switch on the rack shelf or mount the switch directly into a 19" wide, EIA-310-E compliant rack (four-post, two-post, or threaded methods). The Dell ReadyRails™ system is provided for 1U front-rack, 1U rear-rack, and two-post installations. The ReadyRails system includes two separately packaged rail assemblies and two rails that are shipped attached to the sides of the switch. In addition, one mounting bracket is provided for 0U configurations, and one blanking panel is provided for rear-rack installations.

⚠ **WARNING: This is a condensed reference. Read the safety instructions in your Safety, Environmental, and Regulatory Information booklet before you begin.**

NOTE: The illustrations in this document are not intended to represent a specific switch.

Rack Mounting Safety Considerations

- Rack Loading: Overloading or uneven loading of racks may result in shelf or rack failure, causing damage to equipment and possible personal injury. Stabilize racks in a permanent location before loading begins. Mount

components beginning at the bottom of the rack, then work to the top. Do not exceed your rack load rating.

- Power considerations: Connect only to the power source specified on the unit. When multiple electrical components are installed in a rack, ensure that the total component power ratings do not exceed circuit capabilities. Overloaded power sources and extension cords present fire and shock hazards.

- Elevated ambient temperature: If installed in a closed rack assembly, the operating temperature of the rack environment may be greater than room ambient. Use care not to exceed the 50°C maximum ambient temperature of the switch.

- Reduced air flow: Install the equipment in the rack so that the amount of airflow required for safe operation of the equipment is not compromised.

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

- Product should not be mounted with the rear panel facing in the downward position.

Installing the Dell ReadyRails System

The ReadyRails system is provided to easily configure your rack for installation of your switch. The ReadyRails system can be installed using the 1U tool-less method or one of three possible 1U tooled methods (two-post flush mount, two-post center mount, or four-post threaded).

1U Tool-less Configuration (Four-post Square Hole or Unthreaded Round Hole)

1   With the ReadyRails flange ears facing outward, place one rail between the left and right vertical posts. Align and seat the rear flange rail pegs in the rear vertical post flange. In Figure 2.1, item 1 and its extractions illustrate how the pegs appear in both the square and unthreaded round holes.

Figure 2.1: 1U Tool-less Configuration
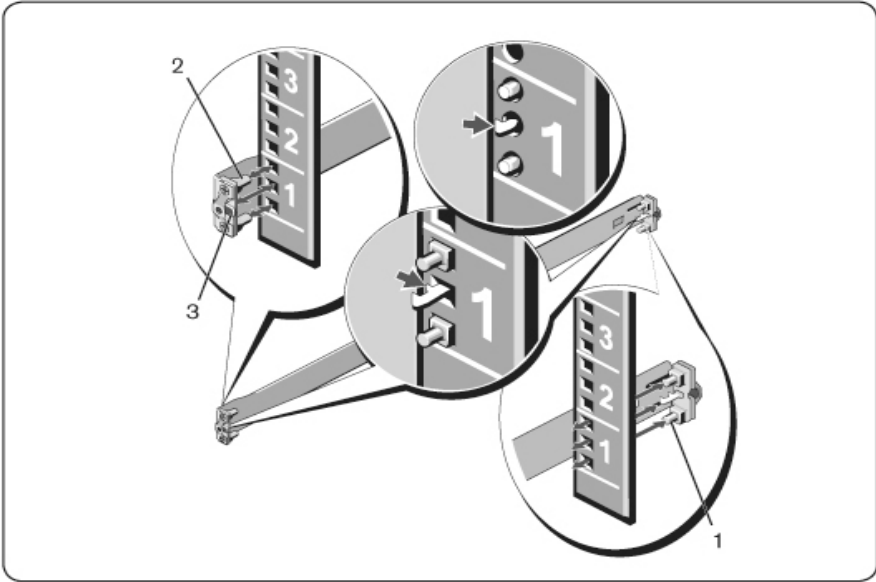
2   Align and seat the front flange pegs in the holes on the front side of the vertical post (item 2).

3   Repeat this procedure for the second rail.

4   To remove each rail, pull on the latch release button on each flange ear (item 3) and unseat each rail.

Two-Post Flush-Mount Configuration

1   For this configuration, the castings must be removed from the front side of each ReadyRails assembly (Figure 2.2, item 1). Use a Torx™ driver to remove the two screws from each front flange ear (on the switch side of the rail) and remove each casting. Retain castings for future rack requirements. It is not necessary to remove the rear flange castings.

Figure 2.2: Two-post Flush-mount Configuration
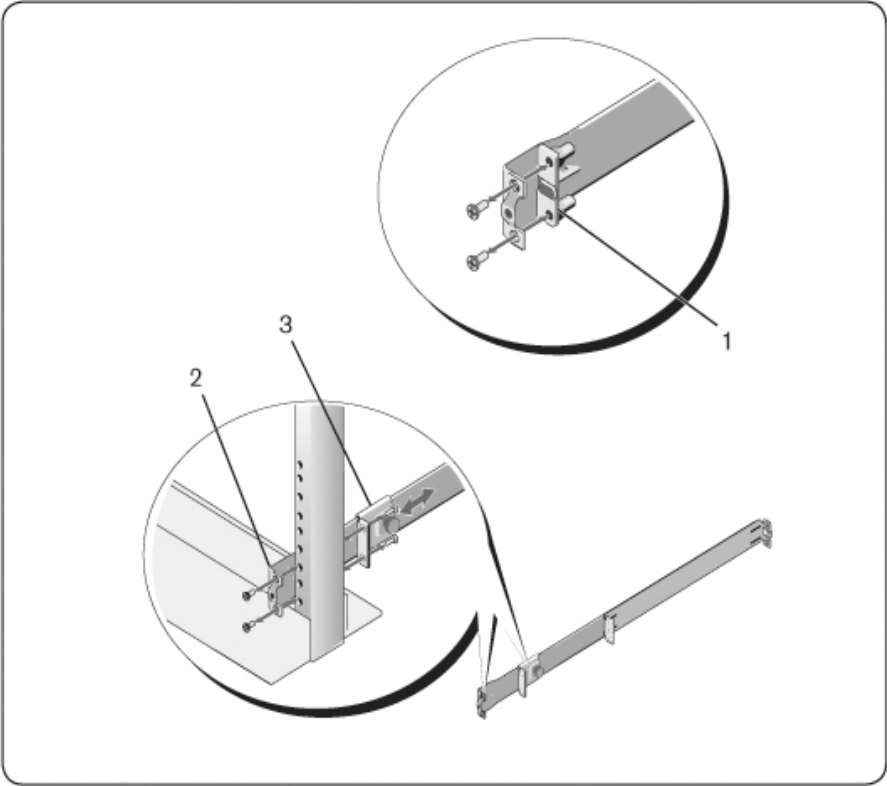
2   Attach one rail to the front post flange with two user-supplied screws (item 2).

3   Slide the plunger bracket forward against the vertical post and secure the plunger bracket to the post flange with two user-supplied screws (item 3).

4   Repeat this procedure for the second rail.

Two-post Center-mount Configuration

1   Slide the plunger bracket rearward until it clicks into place and secure the bracket to the front post flange with two user-supplied screws (Figure 2.3, item 1).

Figure 2.3: Two-post Center-mount Configuration
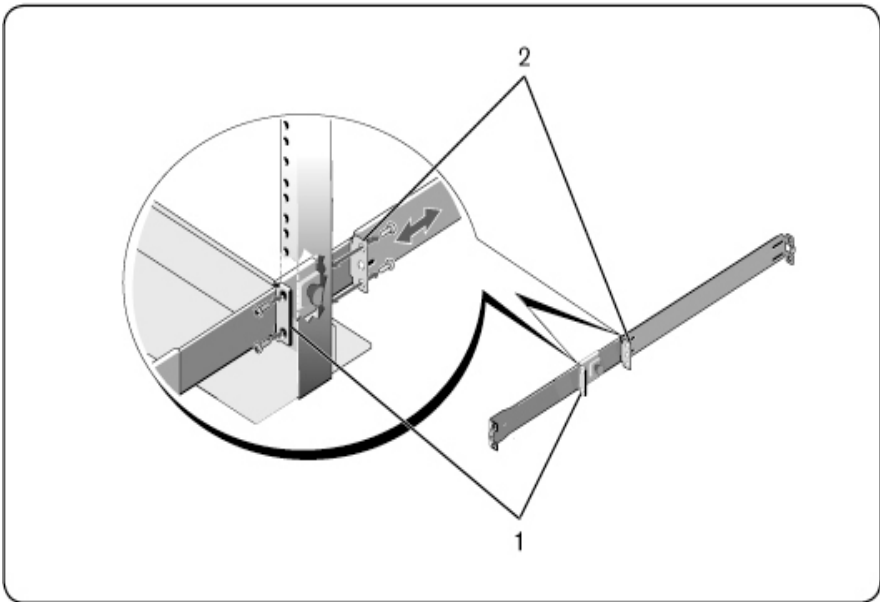
2   Slide the back bracket towards the post and secure it to the post flange with two user-supplied screws (item 2).

3   Repeat this procedure for the second rail.

Four-post Threaded Configuration

1   For this configuration, the flange ear castings must be removed from each end of the ReadyRails assemblies. Use a Torx™ driver to remove the two

screws from each flange ear and remove each casting (Figure 2.4, item 1).
Retain castings for future rack requirements.

2   For each rail, attach the front and rear flanges to the post flanges with two
user-supplied screws at each end (item 2).

Figure 2.4: Four-post Threaded Configuration
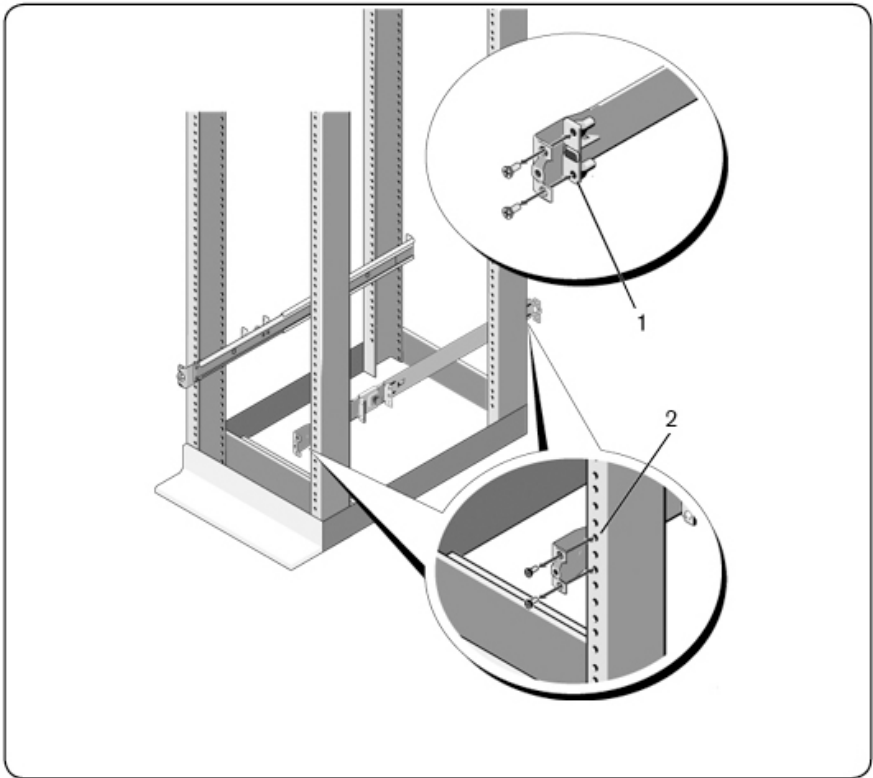
Installing the Switch

The switch may be mounted in the 1U rear-rack, 1U front-rack, 1U two-post (flush and center), and 0U configurations. The following are examples of 1U rear-rack, 1U front-rack, and 0U configurations. For 1U two-post (flush and center) configurations, you can slide the switch into the rails in the same manner as the four-post configurations.

1U Rear-rack Installation

1   Insert the ends of the rails that are attached to the switch into the ReadyRails assembly and push the switch into the rack (Figure 2.5, item 1).

Figure 2.5: 1U Rear-rack Installation
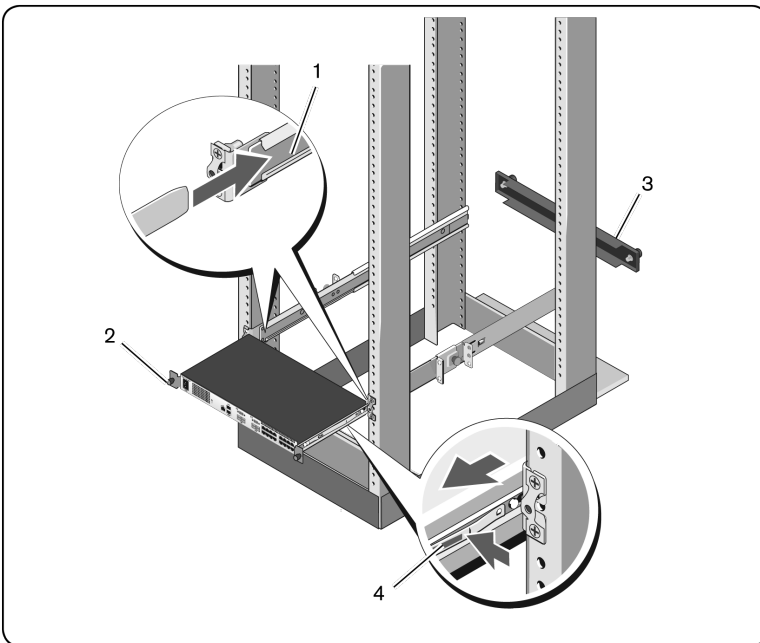
2   Secure each switch rail with the thumbscrew (item 2).

3 (Optional) Assemble the blanking panel to the rails on the front side of the rack and tighten the thumbscrews (item 3).

To remove the switch from the rack:

1 Unscrew the thumbscrews and pull the switch assembly out of the rack until the travel stops are reached. The travel stop position is intended to provide the opportunity to reposition the rail grip; it is not intended for service.

2 Locate the blue tabs on the sides of the switch rails (item 4).

3 Push the tabs inward and continue pulling the assembly until the switch rails are clear of the ReadyRails assemblies.

1U Front-rack Installation

Before installation, the rails that are attached to the switch must be re-configured.

1 On each switch rail, lift the tab under the front standoff and slide the rail forward as you lift the rail from the switch (Figure 2.6, item 1).

Figure 2.6: Rotating the Switch Rails
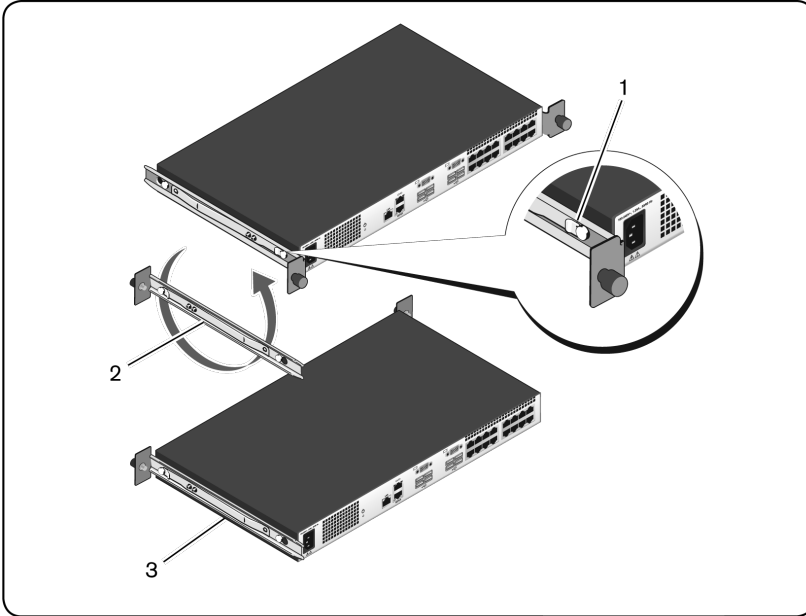
2   Rotate each rail 180° (item 2) and then reassemble each rail to the switch (item 3).

3   Refer to the 1U rear-rack instructions to insert and remove the switch assembly from the ReadyRails system.

📝 **NOTE:** No blanking panel is required for this configuration.

0U Installation

1   Align and assemble the 0U mounting bracket to the switch rails (Figure 2.7, item 1). Tighten the thumbscrews (item 2).

2   Insert the mounting bracket hooks into the rack holes and push down until the blue button pops out and locks the bracket into place.

Figure 2.7: 0U Installation
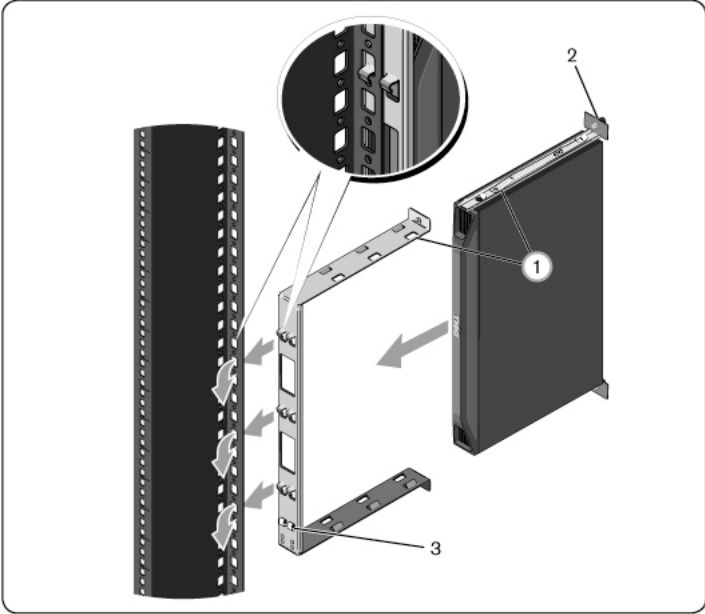
To remove the switch assembly, press the blue button (item 3) to unseat the bracket and then lift the assembly from the posts.

Connecting the SCS Hardware

Figure 2.8 illustrates an example configuration for the SCS.

Figure 2.8: Basic SCS Configuration

Table 2.1: Basic SCS Configuration Descriptions

Number	Description	Number	Description
1	SCS (16-Port Model Shown)	7	ACI Connection
2	Power Cord	8	External Virtual Media - USB Connections
3	Analog Users (2)	9	Target Device Ports
4	Digital User (requires the RAK)	10	SIPs
5	LAN/Network	11	Servers/Target Devices
6	10101 Console Setup Port		

NOTE: The SCS switch supports connecting to another appliance via an ACI connection. This connection requires that the secondary appliance in the tier have an ACI connector on the user side.

To connect and turn on your SCS:

CAUTION: To reduce the risk of electric shock or damage to your equipment, do not disable the jumper cord grounding plug. The grounding plug is an important safety feature. Plug the jumper cord into a grounded (earthed) outlet that is easily accessible at all times. Disconnect the power from the unit by unplugging the jumper cord from either the power source 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 SCS to server is 30 meters.

- Do not disable the power grounding plug. The grounding plug is an important safety feature.

- Connect the jumper cord into a grounded (earthed) outlet that is easily accessible at all times.

- Disconnect the power from the product by unplugging the jumper cord from either the power source or the product.

- This product has no user-serviceable parts inside the product enclosure. Do not open or remove product cover.

1 Connect your VGA monitor and USB keyboard and mouse cables to the appropriately labeled ports.

2 Connect one end of a UTP cable (4-pair, up to 98 ft/30 m) to an available numbered port. Connect the other end to an RJ-45 connector of a SIP.

3 Connect a SIP to the appropriate port on the back of a device. Repeat steps 2 and 3 for all devices you want to connect.

NOTE: When connecting to a Sun Microsystems server, you must use a multi-sync monitor in the local port to accommodate Sun computers that support both VGA and sync-on-green or composite sync.

4 Connect a user-supplied UTP cable from the Ethernet network to the LAN port on the back of the SCS. Network users will access the SCS through this port.

5 Turn on each device, then locate the jumper cord that came with the SCS. Connect one end to the power socket on the rear of the SCS. Connect the other end into an appropriate power source.

6 (Optional) Connect the virtual media or smart card readers to any of the USB ports on the SCS.

NOTE: For all virtual media sessions, you must use a USB2 or USB2+CAC SIP.

Tiering Your Switch Using a SIP

Figure 2.9 illustrates a typical SIP connection between the SCS and a device.

To connect a SIP to each device:

NOTE: When tiering devices, the SCS closest to the actual user is the primary SCS.

1   Locate the SIPs for your SCS.

2   If you are using a PS/2 SIP connection, attach the color-coded ends of the SIP cable to the appropriate keyboard, monitor, and mouse ports on the first device you will be connecting to this SCS. If you are using a USB connection, attach the plug from the SIP to the USB port on the first device you will be connecting to this SCS.

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 SCS. See "SIP Connection" on page 28.

4   Connect the other end of the CAT 5 cable to the desired ARI port on the back of your SCS.

5   Repeat steps 2-4 for all devices you wish to attach.

> **NOTE:** Turn off the switch before servicing. Always disconnect the jumper cord from the power source.

> **NOTE:** In addition to Dell SIPs, the switch may also be connected to devices using Avocent IQ modules, including Sun IQ modules.

Figure 2.9: SIP Connection
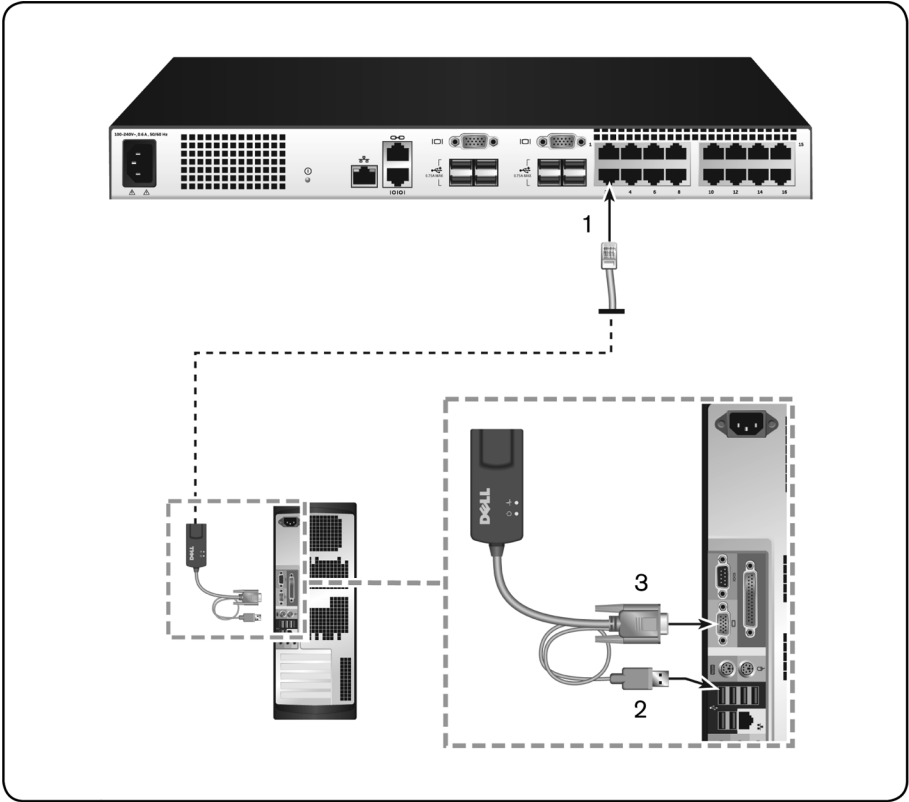
Table 2.2: Descriptions for Figure 2.9

Number	Description
1	CAT 5
2	USB Connection
3	VGA Connection

Adding a Tiered Switch

![note icon] **NOTE:** The SCS does not support the EL80-DT.

You can tier up to two levels of switches (Figure 2.10), enabling users to connect to up to 512 devices. In a tiered system, each device port on the main switch will connect to the ACI port on each tiered switch. Each tiered switch can then be connected to a device with a SIP or Avocent IQ module.

To tier multiple switches:

1   Attach one end of a UTP cable (up to 30 meters in length) to a device port on the switch.

2   Connect the other end of the UTP cable to the ACI port on the back of your tiered switch.

3   Connect the devices to your tiered switch.

4   Repeat these steps for all the tiered switches you wish to attach to your system.

![note icon] **NOTE:** The system will automatically "merge" the two switches. All switches connected to the tiered switch will display on the main switch list in the local UI.

![note icon] **NOTE:** The switch supports one tiered switch per device port of the main switch. You cannot attach a switch to the tiered switch.

Figure 2.10: Tiering the SCS With a UTP Analog Switch
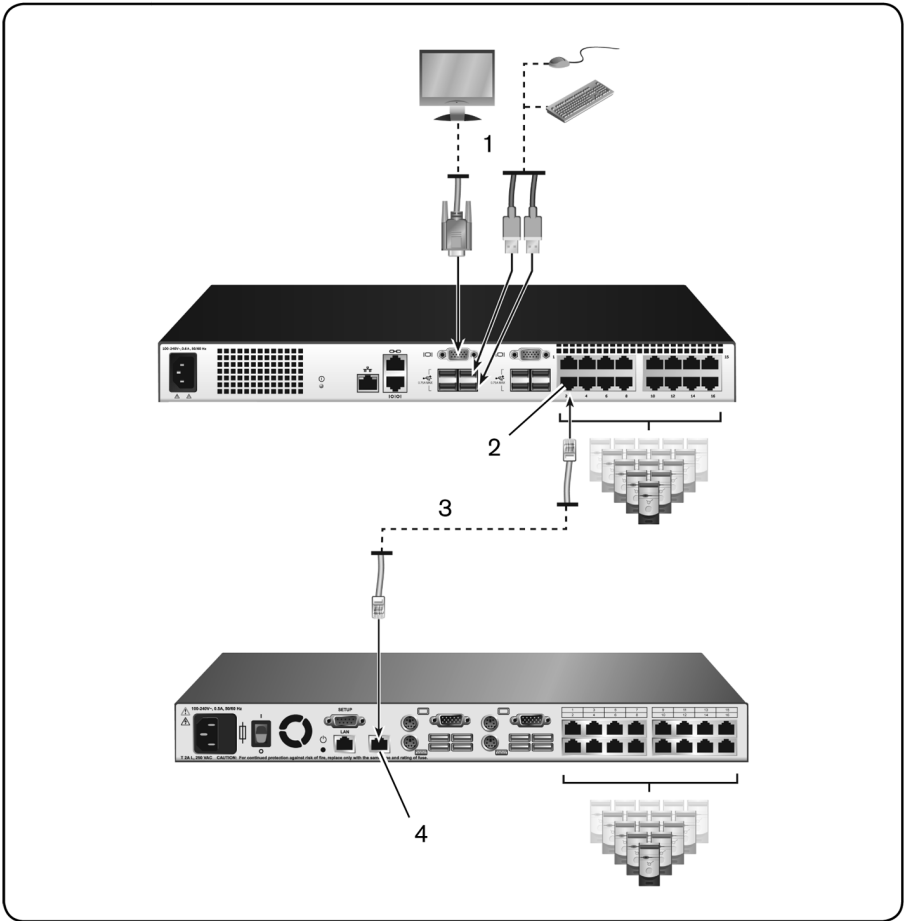
Table 2.3: Descriptions for Figure 2.10

Number	Description
1	Local User
2	ARI Connection
3	UTP Connection
4	ACI Connection (chain icon)

Adding a Tiered Legacy Switch

Figure 2.11 illustrates a tiered legacy switch configuration.

To add a legacy switch (optional):

1 Mount the SCS into your rack. Locate a UTP cable (up to 30 meters) to connect your switch to the legacy switch.

2 Attach one end of the UTP cabling to the ARI port on your switch.

3 Connect the other end of the UTP cable to a PS/2 SIP.

4 Connect the SIP to the 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 switch.

NOTE: The primary SCS supports only one switch per ARI port or USB port. You cannot tier a switch to a tiered switch.

Figure 2.11: Tiering Legacy Switches
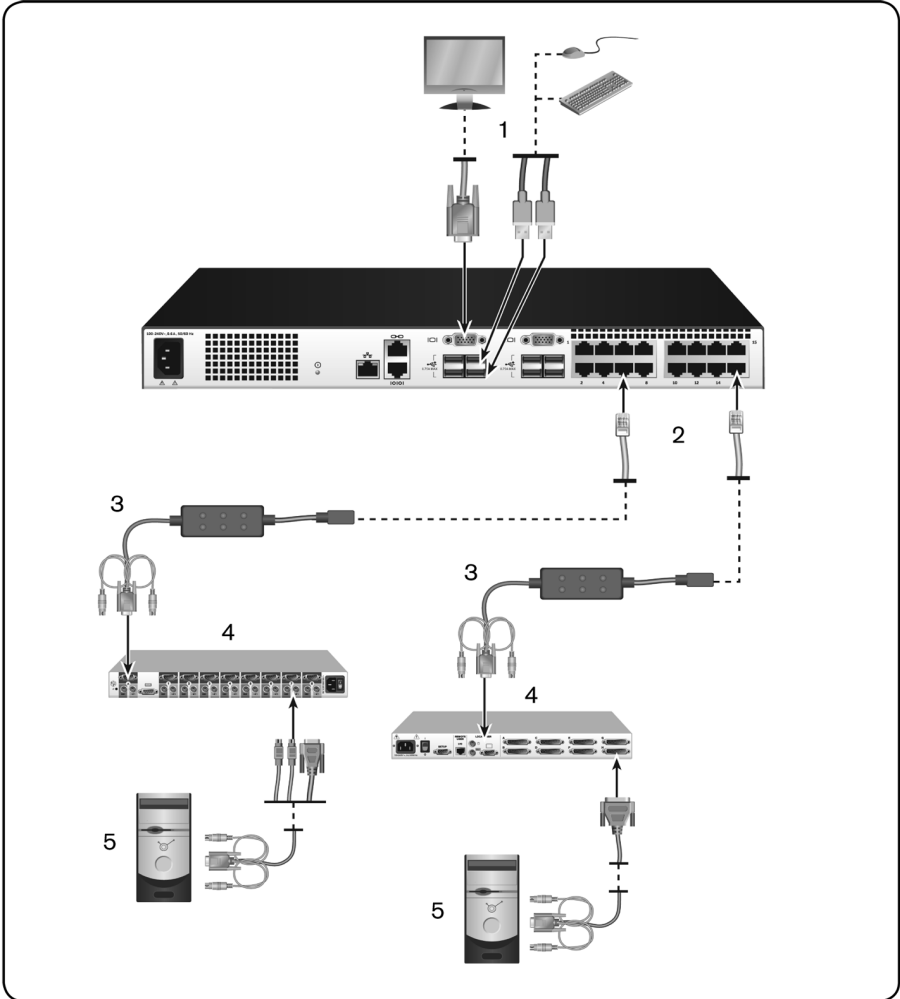
Table 2.4: Descriptions for Figure 2.11

Number	Description
1	Local User
2	ARI Connection
3	SIP
4	PS2 Connection
5	Target Device Connection

Adding a Port Expansion Module (Optional)

A Port Expansion Module (PEM) allows you to expand each ARI port to accommodate up to eight devices instead of one. See Figure 2.12 and its description table.

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: You cannot open a virtual media session or a CAC session if the device is connected via a PEM.

To add a PEM (optional):

1   Mount the PEM into your rack. Using up to nine UTP cables, one connects your SCS to the PEM, and the other eight connect the PEM to the SIP attached to each device.

2   Attach one end of the UTP cabling (up to 30 meters in length) that will run between your PEM and the SCS to the RJ-45 connector, slightly separated from the other connectors on the PEM. Connect the remaining end of the UTP cable to the desired ARI port on the back of your SCS.

3   To one of the eight RJ-45 connectors grouped on the back of the PEM, attach the UTP cabling that will run between the PEM and each SIP connected to each device.

4   Connect the other end of the UTP cable to the first SIP.

5 Repeat steps 3 and 4 for all devices you wish to attach.

Figure 2.12: SCS Configuration With a PEM
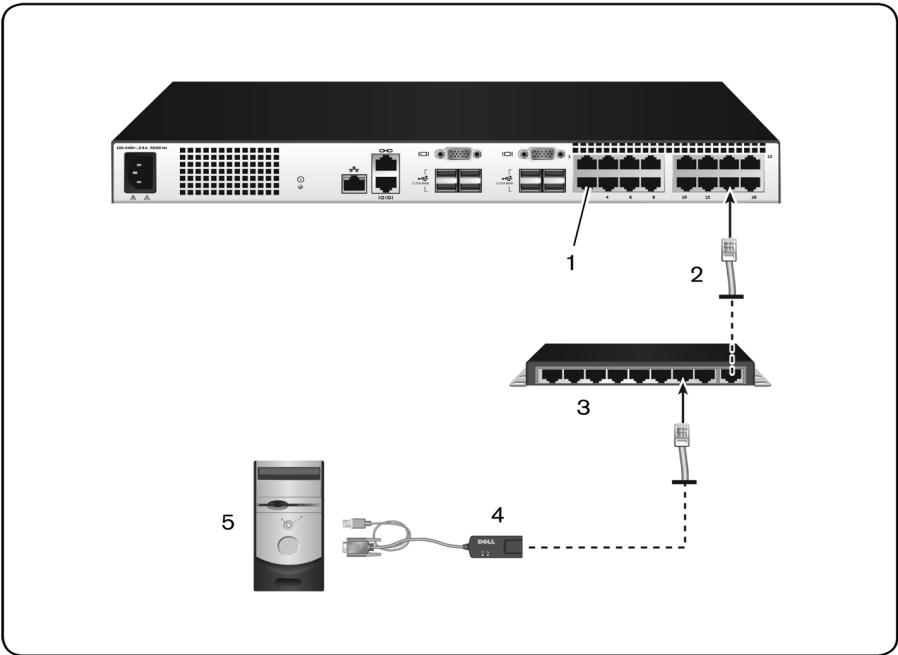
Table 2.5: Descriptions for Figure 2.12

Number	Description
1	ARI Port
2	UTP
3	PEM
4	SIP
5	Target Device

Configuring Your SCS

Once all physical connections have been made, you will need to configure the SCS for use in the overall SCS system. This can be accomplished using serial interface, OBWI, OSCAR, or Avocent management software. When configuring the SCS using OSCAR, see "Network Settings" on page 68. When using Avocent management software, the Dell RAK is required. See the applicable Avocent Installer/User Guide for detailed instructions.

Setting Up the Built-in Web Server

You can access the SCS using the OBWI for most day-to-day switch tasks. Before using the OBWI to access the SCS, specify an IP address through the 10101 setup port on the back panel of the SCS using the local UI. To use the SCS UI, see "Local OSCAR User Interface" on page 39.

Connecting to the OBWI Through a Firewall

For SCS installations that use the OBWI for access, the following ports must be opened in a firewall, if outside access is desired.

Table 2.6: OBWI Ports With a Firewall

Port Number	Function
TCP 80	Used for the initial downloading of the Video Viewer. The SCS Admin can change this value.
TCP 443	Used by the web browser interface for managing the switch and launching KVM sessions. The SCS Admin can change this value.
TCP 2068	Transmission of KVM session data (mouse and keyboard) or transmission of video on switches (requires the RAK).
TCP/UDP 3211	Discovery (requires the RAK).

The following figure and table provide a typical configuration where the user's computer is located outside of the firewall and the switch resides inside the firewall.

Figure 2.13: Typical SCS Firewall Configuration
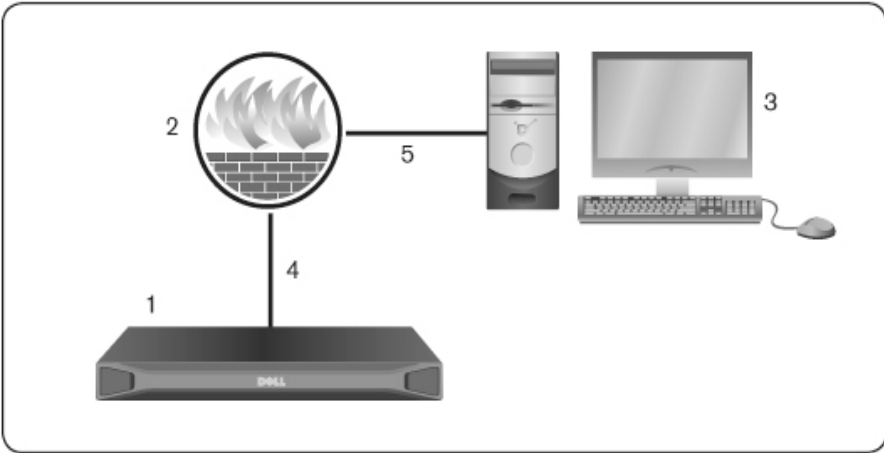
Table 2.7: Descriptions for Figure 1

Number	Description
1	Server Console Switch.
2	Firewall.
3	User's computer.
4	Firewall forwards HTTP requests and KVM traffic to the switch.
5	User browses to IP address outside the firewall.

To configure the firewall:

To access the switch from outside a firewall, configure your firewall to forward ports 80 and 443 from its external interface to the KVM switch through the firewall's internal interface. Consult your firewall manual for specific port forwarding instructions.

> ![NOTE icon] **NOTE:** Ports 80 and 443 can be reconfigured by an administrator. You must reboot for a port change to take effect.

For information on launching the OBWI, see "OBWI Operation" on page 57.

Verifying Power Status

The switch has one power supply. The LED illuminates when the switch is turned on and operating normally.

Adjusting Mouse Settings on Target Devices

Before a computer connected to the switch can be used for remote user control, you must set the mouse speed and turn off acceleration. For machines running Microsoft® Windows® (Windows NT®, 2000, XP, or Server 2003), use the default USB mouse driver.

To ensure that the local mouse movement and remote cursor display remain in sync, mouse acceleration must be set to none for all user accounts accessing a remote system through a KVM switch. Mouse acceleration must also be set to none on every remote system. Special cursors should not be used and cursor visibility options, such as pointer trails, Ctrl key cursor location animations, cursor shadowing, and cursor hiding, should also be turned off.

> ![NOTE icon] **NOTE:** If you are not able to disable mouse acceleration from within a Windows operating system, or if you do not wish to adjust the settings of all your target devices, you may use the Tools - Single Cursor Mode command available in the Video Viewer window. This command places the Video Viewer window into an "invisible mouse" mode, which allows you to manually toggle control between the mouse pointer on the device system being viewed and the mouse pointer on the client computer.

3

Local OSCAR User Interface

The SCS features user-side keyboard and mouse ports that allow you to connect a USB keyboard and mouse for direct analog access. The SCS uses the OSCAR interface to configure your system and devices. You can use the OSCAR interface to access devices that are attached to the SCS.

Main Dialog Box Functions

To access the OSCAR interface **Main** dialog box:

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

> **NOTE:** If the OSCAR password has been enabled, you will be prompted to enter a password before you can launch the OSCAR interface.

Viewing and Selecting Ports and Devices

Use the OSCAR **Main** dialog box to view, configure, and control devices in the SCS system. View your devices by name, port, or by the unique EID number embedded in each SIP.

In the following figure, the Port column indicates the ARI port to which a device is connected. If you tier a switch from the main SCS, creating another tier, the ARI port on the switch is listed first, and is followed by 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. The port number list indicates the ARI port number first, and then names the switch port to which the device is connected.

If you tier a switch from a PEM, you will also see multiple devices that show up on a single port, as is shown for Edie and Galloway.

Figure 3.1: OSCAR Interface Main Dialog Box
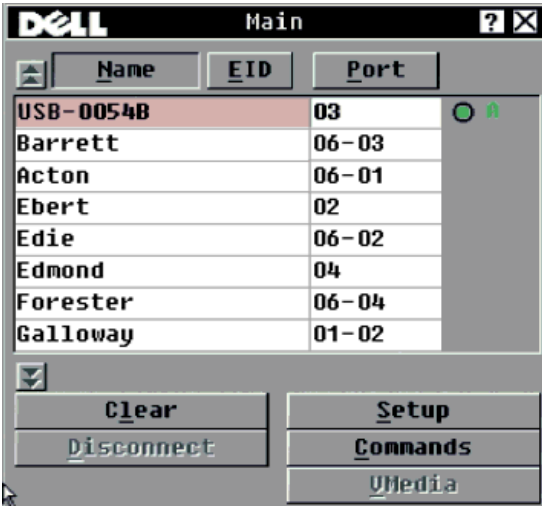
NOTE: You can press the <Control>, <Alt>, or <Shift> keys twice within one second to launch the OSCAR interface. You can use this key sequence when you see <Print Screen> throughout this chapter.

Table 3.1: Main Dialog Box Functions

Button	Function
Name	Name of device.
EID	Unique EID in a module.
Port	The port to which a device is connected.
Clear	Clear all offline SIPs.
Disconnect	Disconnect the KVM session.
Setup	Access the Setup dialog box and configure the OSCAR interface.
Commands	Access the Commands dialog box.
VMedia	Control virtual media connection.

Viewing Switch System Status

The status of devices in your system is indicated in the right column of the **Main** dialog box. The following table describes the status symbols.

Table 3.2: OSCAR Interface Status Symbols

Symbol	Description
🟢	(green circle) device connected, turned on, and the SIP is online.
✖	Connected device is turned off or is not operating properly, and the SIP is offline.
⛁	Connected switch is online.
⛌	Connected switch is offline or not operating properly.

Symbol	Description
○	(yellow circle) The designated SIP is being upgraded. When this symbol displays, do not cycle power to the switch or connected devices and do not disconnect the SIP. Doing so may render the module permanently inoperable and require the SIP to be returned to the factory for repair.
A	(green letter) SIP is being accessed by the indicated user channel.
A	(black letter) SIP is blocked by the indicated user channel.

Selecting Devices

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

To select a device:

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

or-

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

-or-

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

To select the previous device:

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

To disconnect from a device:

Press <Print Screen> and then <Alt+0> (zero). This leaves the user in a free state, with no device selected. The status flag on your desktop displays the word Free.

Soft Switching

Soft switching is the ability to switch devices using a hotkey sequence. You can soft switch to a device by pressing <Print Screen>, and then depending on the method you've selected, typing the first few characters of its name or number. If you have set a Screen Delay Time for the OSCAR interface and you press the key sequences before that time has elapsed, the OSCAR interface will not be displayed.

To soft switch to a device:

Press <Print Screen>, type the port number and the first few letters of the name of the device, to establish it as unique and press <Enter>.

To switch back to the previous device, press <Print Screen> and then <Backspace>.

Navigating the OSCAR Interface

The following table describes how to navigate the OSCAR interface using the keyboard and mouse.

Table 3.3: OSCAR Interface Navigation Basics

Keystroke	Function
Print Screen, Ctrl+Ctrl, Shift+Shift and/or Alt+Alt	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 the OSCAR interface before use.
F1	Opens the Help screen for the current dialog box.

Keystroke	Function
Escape	Closes the current dialog box without saving changes and returns to the previous one. If the Main dialog box is displayed, pressing <Escape> closes the OSCAR interface and displays a status flag if status flags are enabled. See "Commands Dialog Box Functions" on page 52 for more information. In a message box, pressing <Escape> closes the pop-up box and returns to the current dialog box.
Alt	Opens dialog boxes, selects or checks options, and executes actions when used with underlined or other designated letters.
Alt+X	Closes current dialog box and returns to previous one.
Alt+O	Selects the OK button, then returns to the previous dialog box.
Enter	Completes a switch operation in the Main dialog box and exits the OSCAR interface.
Single-click, Enter	In a text box, single-clicking an entry and pressing <Enter> selects the text for editing and enables the left and right arrow keys to move the cursor. Press <Enter> again to quit the Edit mode.
Print Screen, Backspace	Toggles back to previous selection.
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 between columns. When editing a text box, these keys move the cursor within the column.
Page Up/Page Down	Pages up and down through Name and Port lists and Help pages.

Keystroke	Function
Home/End	Moves the cursor to the top or bottom of a list.
Backspace	Erases characters in a text box.

Connecting Local Virtual Media

You can connect virtual media directly to the switch using a USB port on the switch.

NOTE: All USB ports are assigned to a single virtual media session and cannot be independently mapped.

To start a local virtual media session, complete the following steps:

1 Press <Print Screen> to start the OSCAR interface and open the Main window.

2 Connect the user to the device with which you want to establish a virtual media session.

3 Use the arrow keys to highlight the device name, and then press <Enter>.

4 Press <Print Screen> to start the OSCAR interface again. The Virtual Media window is displayed.

5 Select one or more of the following checkboxes:

- Locked - Select this checkbox to specify that when the user is disconnected from a device, the virtual media is also disconnected.

- Reserve - Select this checkbox to specify that the virtual media connection can be accessed only by your user name and that no other user can connect to that device. If both Locked and Reserved are selected, the session will be reserved.

- CD ROM - Select this checkbox to establish a virtual media CD connection to a device. Clear this checkbox to end the connection.

- Mass Storage - Select this checkbox to establish a virtual media mass-storage connection to a device. Clear this checkbox to end the connection.

- Write Access - Select this checkbox to enable the connected device to write data to the virtual media during a virtual media session. Read access is always enabled during virtual media sessions.

6. Click **OK**.

Setup Dialog Box Functions

You can configure your SCS system from the **Setup** dialog box within the OSCAR interface. Select the **Names** button when initially setting up your SCS to identify devices by unique names. Select the other setup features to manage routine tasks for your devices from the OSCAR interface menu. The following table lists the functions accessed using each of the buttons in the Setup dialog box.

To access the OSCAR interface **Setup** dialog box, click **Setup** on the **Main** dialog box.

Table 3.4: Setup Dialog Box Features

Feature	Purpose
Menu	Change the Main dialog box list sorting option by toggling numerically between port number, EID number, or alphabetically by name. Change the Screen Delay Time before the OSCAR interface displays after pressing Print Screen. You can also change how the OSCAR interface activation sequence is invoked.
Security	Set passwords to protect or restrict access or enable the screen saver.
Devices	Identify the appropriate number of ports on an attached tiered switch.
Names	Identify devices by unique names.

Feature	Purpose
Keyboard	Set the keyboard country code value for the USB devices.
Broadcast	Set up to simultaneously control multiple devices through keyboard and mouse actions.
Switch	Change how local port connections are managed by the switch. Control Local to Local Share Mode.
Network	Choose your network speed, transmission mode, and configuration.
Scan	Set up a custom Scan pattern for multiple devices.
VMedia	Set the behaviour of the switch during a virtual media session.

Changing the Display Behavior

Use the **Menu** dialog box to change the order of displayed devices, change how the OSCAR interface is invoked, or set a **Screen Delay Time** for the OSCAR interface. This setting alters how devices are displayed in several dialog boxes, including the **Main**, **Devices**, and **Scan List** boxes.

To access the OSCAR interface **Menu** dialog box, activate the OSCAR interface and click **Setup > Menu** in the **Main** dialog box.

To choose the 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**.

Depending on the display method selected, the corresponding button will be depressed in the **Main** dialog box.

To change how the OSCAR interface is invoked:

1 Select the checkbox next to one of the listed methods.

2 Click **OK**.

To set a Screen Delay Time for the OSCAR interface:

1 Type in the number of seconds (0-9) to delay the OSCAR interface display after you press Print Screen. Enter <0> to launch the OSCAR interface with no delay.

2 Click **OK**.

Setting a Screen Delay Time enables you to complete a soft switch without the OSCAR interface. To perform a soft switch, see "Soft Switching" on page 43.

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 flag to display by device name or EID number, or to change the flag color, opacity, display time, and location on the desktop.

To access the OSCAR interface **Flag** dialog box:

Activate the OSCAR interface and click **Setup > Flag** to open the **Flag** dialog box.

To determine how the status flag is displayed:

1 Select **Name** or **EID** to determine what information will be displayed. The following interface **Status Flags** are available.

- Flag Description

- Flag type by name

- Flag type by EID number

- Flag indicating that the user has been disconnected from all systems

2 Select **Displayed** to activate the flag display. After a switch, the flag will remain on the screen until the user switches to another device. Selecting

Timed will cause the flag to display for five seconds when a switch is made and then disappear.

3   Select a flag color under Display Color. The following flag colors are available:

- • Flag 1 - Gray flag with black text
- • Flag 2 - White flag with red text
- • Flag 3 - White flag with blue text
- • Flag 4 - White flag with violet text

4   In Display Mode, select **Opaque** for a solid color flag or **Transparent** to see the desktop through the flag.

5   To position the status flag on the desktop:

- a.   Click **Set Position** to gain access to the position flag screen.
- b.   Left-click on the title bar and drag it to the desired location.
- c.   Right-click to return to the **Flag** dialog box.

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

6   Click **OK** to save settings.

-or-

Click **X** to exit without saving changes.

Setting the Keyboard Country Code

NOTE: Using a keyboard code that supports a language different from that of your switch firmware will cause incorrect keyboard mapping.

By default, the switch sends the US keyboard country code to USB modules attached to devices, and the code is applied to the devices when they are turned on or rebooted. Codes are then stored in the SIP. Issues may arise when you use the US keyboard country code with a keyboard of another country.

For example, the Z key on a US keyboard is in the same location as the Y key on a German keyboard. The **Keyboard** dialog box enables you to send a different keyboard country code than the default US setting. The specified country code is sent to all devices attached to the SCS when they are turned on or rebooted, and the new code is stored in the SIP.

> *NOTE:* If a SIP is moved to a different device, the keyboard country code will need to be reset.

Assigning Device Types

To access the OSCAR interface **Devices** dialog box:

Activate the OSCAR interface and click **Setup > Devices** to open the **Devices** dialog box.

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

When the switch discovers a tiered switch, the numbering format changes from SCS port to [SCS port]-[switch port] to accommodate each device under that switch.

For example, if a switch is connected to SCS port 6, each device connected to it would be numbered sequentially. The device using SCS port 6, switch port 1, would be 06-01, the device using SCS port 6, switch port 2, would be 06-02, and so on.

To assign a device type:

1 In the **Devices** dialog box, select the desired port number.

2 Click **Modify** to open the **Device Modify** dialog box.

3 Choose the number of ports supported by your switch and click **OK**.

4 Repeat steps 1-3 for each port requiring a device type to be assigned.

Assigning Device Names

Use the **Names** dialog box to identify devices by name rather than by port number. The **Names** list is always sorted by port order. You can toggle between

displaying the name or the EID number of each SIP, so even if you move the SIP/device to another port, the name and configuration will be recognized by the switch.

✎ **NOTE:** When it is initially connected, a device will not appear in the Names list until it is turned on. Once an initial connection has been made, it will appear in the Names list even when turned off.

To access the OSCAR interface **Names** dialog box, activate the OSCAR interface and click **Setup > Names**.

✎ **NOTE:** If new SIPs are discovered by the switch, the on-screen list will be automatically updated. The mouse cursor will change into an hourglass during the update. No mouse or keyboard input will be accepted until the list update is complete.

To assign names to devices:

1   In the **Names** dialog box, select a device name or port number and click **Modify** to open the **Name Modify** dialog box.

2   Type a name in the **New Name** box. Names of devices may contain all printable characters.

3   Click **OK** to assign the new name.

4   Repeat steps 1-3 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 exit the dialog box without saving changes.

Configuring Network Settings

Use the **Network** dialog box to set the Network Speed, Transmission Mode, and Network Configuration feature.

To change network settings:

1   If the OSCAR interface is not open, press <Print Screen> to open the **Main** dialog box.

2   Click **Setup > Network** to open the **Network** dialog box.

3 Make desired changes and click **OK** to confirm or click **X** to exit without saving.

NOTE: Changing the network settings will cause the switch to reboot.

4 Click **OK** in the **Devices** dialog box to save settings.

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

NOTE: Changes made in the Name Modify dialog box are not saved to the switch until you click OK in the Names dialog box.

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

Commands Dialog Box Functions

From the OSCAR interface **Commands** dialog box, you can manage your switch system and user connections, enable the Scan mode, and update your firmware.

Table 3.5: Commands to Manage Routine Tasks for Your Devices

Features	Purpose
Scan Enable	Begin scanning your devices. Set up a device list for scanning in the Setup dialog box. You must have at least two devices selected in the Setup - Scan List menu to enable device scanning.
User Status	View and disconnect users.
SIP Status	Display the currently available firmware for each type of SIP.
Display Versions	View version information for the switch as well as view and upgrade firmware for individual SIPs.
Display Config	View current configuration parameters.
Device Reset	Re-establish operation of keyboard and mouse on the local port.

To access the OSCAR interface **Commands** dialog box:

Activate the OSCAR interface and click **Commands** to open the dialog box.

Selecting Devices for Scan Mode

The **Scan** dialog box allows the local user to define a custom list of devices to include while in Scan mode and the number of seconds to display each device. The creation of the Scan list does not start Scan mode. You must enable Scan mode using the **Scan Enable** checkbox on the **Commands** dialog box. The Scan list is displayed in the manner set from the **Menu** dialog box. It can be changed in the **Scan** dialog box to sort either by name, EID, or port by choosing one of the buttons. If a device on the list is unavailable, it is skipped. Watch mode views a device unless a conflicting network user blocks the path to that device. If a conflict is detected in Watch mode (or the device is unavailable), the device to be viewed is skipped.

To add devices to the Scan list:

1   Activate the OSCAR interface and click **Setup > Scan** to open the **Scan** dialog box.

2   The dialog box contains a listing of all devices attached to your switch. Click the checkbox to the right of the device, double-click on the desired entry, or highlight the device, and click the **Add/Remove** button to toggle the **Scan** checkbox setting. You can select up to 100 devices for inclusion in the Scan list.

   📝 **NOTE:** Click the **Clear** button to remove all devices from the Scan list.

3   In the Time field, type the number of seconds (from 3 - 255) to display each device while scanning. The default is 15 seconds per device.

4   Click **OK**.

   📝 **NOTE:** The order in which the devices appear in the **Scan** dialog box is based on the order in which they were selected. Scanning a single device multiple times during a loop is not supported. Scan time must be the same for all devices.

Enabling or Disabling Scan Mode

To start the Scan mode:

1   Activate the OSCAR interface and click **Commands**. The **Commands** dialog box is displayed.

2   Select **Scan Enable** in the **Commands** dialog box. Scanning will begin.

3   Click **X** to close the **Commands** dialog box.

To cancel Scan mode:

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 will stop at the currently selected device.

-or-

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

Viewing and Disconnecting User Connections

You can view and disconnect users through the **User Status** dialog box. The username (U) and server (S) will always be displayed when connected to a device (local or remote). You can display either the device name or EID number to which a user is connected. If there is no user currently connected to a channel, the username and device fields will be blank.

To view current user connections, activate the OSCAR interface and click **Commands > User Status** to open the **User Status** dialog box.

To disconnect a user:

1   On the **User Status** dialog box, click the letter corresponding to the user to disconnect. The **Disconnect** dialog box will appear.

2   Click **Disconnect** to disconnect the user and return to the **User Status** dialog box.

-or-

Click **X** or press **Escape** to exit the dialog box without disconnecting a user.

Displaying Version Information and Upgrading Firmware

For troubleshooting and support, the OSCAR interface enables you to display the version number of the switch firmware and any auxiliary devices connected to the switch, as well as upgrade your firmware for optimum performance.

To display version information and upgrade firmware:

1 Activate the OSCAR interface and click **Commands > Display Versions**. The top half of the box lists the subsystem version in the switch. The lower half displays the current IP address, Mask, MAC, and EID.

2 If you want to upgrade the firmware, click **Upgrade** and then click **OK** to open the download box. You will be prompted for an FTP or TFTP device IP address and the related information.

3 Click **Download**. After the firmware is downloaded, the **Upgrade** dialog box will appear.

4 Click the **Upgrade** button.

  NOTE: The switch will reboot when the upgrade is complete.

To upgrade individual SIPs:

1 Click the **SIP** button to view individual SIP version information.

2 Select the **SIP** button to view and click the **Version** button.

3 Click the **Load Firmware** button.

4 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 SIPs are unavailable when an upgrade is in progress. When an upgrade is initiated, any current connection to the device using the SIP is terminated.

To simultaneously upgrade multiple SIPs:

1   Activate the OSCAR interface, click **Commands > SIP Status** and click one or more types of SIPs to upgrade.

2   Click **Upgrade**.

    NOTE: When the Enable SIP Auto update option is enabled in the SIP Status dialog box, SIP firmware is automatically upgraded when the switch firmware is upgraded or when a new SIP is discovered by the switch after a firmware upgrade. SIP modules that have already been discovered but which are not attached to the switch during the firmware upgrade must be upgraded manually.

3   The SIP **Upgrade** dialog box is displayed. Click **OK** to initiate the upgrade and return to the SIP **Status** dialog box.

To return a SIP to factory default status:

1   Click **SIP** in the **Version** dialog box.

2   Select a SIP, then click **Decommission**.

3   Click **OK** to restore factory defaults. You will see the SIP go offline briefly and return.

    - or-

    Click **X** or press **Escape** to cancel the operation.

4   Click **X** to close the SIP **Select** dialog box.

4

OBWI Operation

The OBWI for the SCS is a remote, web browser-based user interface. For details on setting up your system, see "Connecting the SCS Hardware" on page 23. The following table lists the operating systems and browsers that are supported by the OBWI. Make sure that you are using the latest version of your Web browser.

Table 4.1: Operating Systems Supported by the OBWI

Operating System	Browser	
	Microsoft® Internet Explorer® Version 6.0 SP1 and Later	Firefox Version 2.0 and Later
Microsoft Windows 2000 Workstation or Server with Service Pack 2	Yes	Yes
Microsoft Windows Server® 2003 Standard, Enterprise, or Web Edition	Yes	Yes
Microsoft Windows Server® 2008 Standard, Enterprise, or Web Edition	Yes	Yes
Windows XP Professional with Service Pack 3	Yes	Yes

	Browser	
Operating System	**Microsoft® Internet Explorer® Version 6.0 SP1 and Later**	**Firefox Version 2.0 and Later**
Windows Vista® Business with Service Pack 1	Yes	Yes
Red Hat Enterprise Linux® 4 and 5 Standard, Enterprise or Web Edition (Smart card may not be supported by the operating system)	No	Yes
Sun Solaris® 9 and 10 (Smart card may not be supported by the operating system)	No	Yes
Novell SUSE Linux Enterprise 10 and 11 (Smart card may not be supported by the operating system)	No	Yes
Ubuntu 8 Workstation (Smart card may not be supported by the operating system)	No	Yes

To log in to the SCS OBWI:

1   Launch a web browser.

2   In the address field of the browser, enter the IP address or host name assigned to the switch you wish to access. Use https://xxx.xx.xx.xx or https://hostname as the format.

NOTE: If using IPv6 mode, you must include square brackets around the IP address. Use https://[<ipaddress-] as the format.

3   When the browser makes contact with the switch, enter your username and password, then click **Login**. The switch OBWI will appear.

NOTE: The default username is Admin with no password.

To log in to the switch OBWI from outside a firewall, repeat the above procedure, entering the external IP address of the firewall instead.

NOTE: The SCS will attempt to detect if Java is already installed on your PC. If it is not, in order to use the OBWI, you will need to install it. You may also need to associate the JNLP file with Java WebStart.

NOTE: Using the OBWI requires using Java Runtime Environment (JRE) version 1.6.0_11 or higher.

NOTE: Once you have logged in to the OBWI, 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.

Using the OBWI

After you have been authenticated, the user interface appears. You may view, access, and manage your switch, as well as specify system settings and change profile settings. Figure 4.1 shows the user interface window areas. Screen descriptions are provided in the following table.

Figure 4.1: OBWI Window
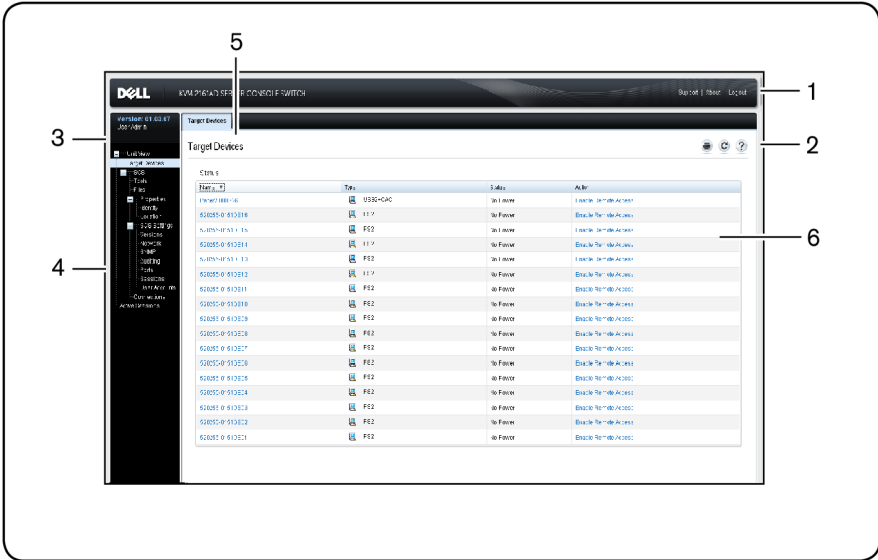
Table 4.2: Figure 4.1

Number	Description
1	Top option bar: Use the top option bar to contact Technical Support, view the software general information, or log out of an OBWI session.
2	Second option bar: Use this bar to print a web page, refresh the current web page or access the Help tool.
3	Version block: The firmware version of the product and the username of the user currently logged in appears on the left side of the top option bar.

Number	Description
4	Side navigation bar: Use the side navigation bar to select the information to be displayed. You can use the side navigation bar to display windows in which you can specify settings or perform operations.
5	Navigation tabs: The selected tab displays the system information in the content area. Some tabs provide sub tabs that can be clicked to display and revise details within a category.
6	Content area: Use the content area to display or make changes to the switch OBWI system.

Viewing System Information

You can view switch and target device information from the following screens in the user interface.

Table 4.3: System Information

Category	Select This:	To View This:
Target Devices	Unit View - Target Devices	List of connected devices, as well as the name, type, status, and action of each device. Click on a target device to view the following information: name, type, EID, available session option, and the connection path.
SCS	Unit View - SCS - Tools	Name, type, and the switch tools (Maintenance-Overview/Reboot/Reset and Upgrade, Certificates, and Trap MIB).
	Unit View - SCS - Files	Configuration and User Database for the switch.

Category	Select This:	To View This:
	Unit View - SCS - Properties - Identity	Part number, serial number, and status of the Dell RAK (default setting is disabled).
	Unit View - SCS- Properties - Location	Site, department, and location of each unit.
	Unit View - SCS Settings - Versions	Current application, boot, build, hardware, UART, and video ASIC versions.
	Unit View - SCS Settings - Network	Network address, LAN speed, and web server ports.
	Unit View - SCS Settings - SNMP	System description, SNMP setting, contact, read/write and trap settings, and designations for allowed managers.
	Unit View - SCS Settings - Auditing	Events list and status and SNMP trap destinations.
	Unit View - SCS Settings - Ports	Status, EID, name, port, application and interface type for each SIP; name, port, type, channels, and status for each tiered switch.
	Unit View - SCS Settings Sessions	General session timeout and sharing details; KVM encryption levels and keyboard language; virtual media settings, drive mappings, encryption level, and SIP access.
	Unit View - SCS - User Accounts	Security and user lock-out for the local account; authentication server assignments for Avocent management software, and override admin username and password in case of a failed operation.

Category	Select This:	To View This:
	Unit View - SCS - Connections	Connection path name and type.
	Active Sessions	Server, owner, remote host, duration, and type of each active session.

Scan Mode

📝 **NOTE:** Scan mode is supported when the Dell RAK is installed.

In Scan mode, the switch scans multiple target devices. The scanning order is determined by placement of the target device in the list. You can also configure the amount of time before the scan moves to the next target device in the sequence.

To add target devices to the Scan list:

1 From the side navigation bar, select **Unit View - Target Devices** to open the Target Devices screen.

2 Select the checkboxes next to the names of the target devices you wish to scan.

3 Click **Scan**.

Generating a Certificate

A web certificate allows you to access the OBWI without having to acknowledge the SCS as a trusted web device each time you access it. Using the Install Web Certificate window, you can generate a new self-signed openssl or upload a certificate. Uploaded certificates must be in OpenSSL PEM format with an unencrypted private key.

To install a web certificate:

1 Click the **Tools** tab in the OBWI.

2 Click the **Update** button.

3 Select the **Generate a new Self-Signed Certificate** radio button and enter the following fields:

- Common Name: your name. (Since this is your root certificate, use an appropriate name such as, "Company_Name Certificate Authority.")

- Organization: organization unit name (marketing, for example).

- City or Locality: the city where your organization is located.

- State or Province: the unabbreviated state or province where your organization is located.

- Country: the two-letter ISO abbreviation for your country.

- Email Address: the email address for the Certificate Authority (CA) to contact.

4 Click **Generate** to create the certificate.

To upload a new certificate:

1 Click the **Upload a New Certificate** radio button.

2 Select the method (Filesystem, TFTP, FTP, or HTTP).

3 Click **Browse** to search for the certificate or enter the certificate filename.

4 Select **Install**. Close the web browser, then launch the OBWI again for the same IP address.

NOTE: If importing a company certificate file, it may take up to 30 seconds for the OBWI to launch.

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.

Tools - Rebooting and Upgrading

From the Tools - Maintenance - Overview screen, you can view the switch name and type. You can also perform the following tasks.

Rebooting the SCS

To reboot the SCS:

1   From the side navigation bar, click **Unit View - SCS - Tools - Maintenance - Overview** to open the Unit Maintenance screen.

2   Click the **Reboot** button.

3   A dialog box appears, warning you that all active sessions will be disconnected. Click the **OK** button.

> **NOTE:** If you are using the local UI, the screen will be blank while the switch reboots. If you are using the remote OBWI, a message will appear to let you know that the interface is waiting on the switch to complete the reboot.

Upgrading SCS Firmware

You can update your switch with the latest firmware available.

After the memory is reprogrammed with the upgrade, the switch performs a soft reset, which terminates all SIP sessions. A target device experiencing a SIP firmware update may not display, or may display as disconnected. The target device will appear normally when the update is completed.

Attention: Disconnecting a SIP during a firmware update or cycling power to the target device will render the module inoperable and require the SIP to be returned to the factory for repair.

To upgrade the switch firmware:

1   From the side navigation bar, click **Unit View - SCS - Tools - Maintenance - Upgrade** to open the Upgrade SCS Firmware window.

2   Select one of the following methods to load the firmware file: **Filesystem**,
    TFTP, **FTP**, or **HTTP**.

    ![NOTE icon] **NOTE:** The Filesystem option is only available on the remote OBWI.

3   If you selected Filesystem, select **Browse** to specify the location of the
    firmware upgrade file.

    -or-

    If you selected TFTP, enter the Server IP Address and Firmware File
    you wish to load.

    -or-

    If you selected FTP or HTTP, enter the Server IP Address and
    Firmware File you wish to load, as well as the User Name and User
    Password.

4   Click the **Upgrade** button.

Saving and Restoring SCS Configurations and User Databases

You may save the switch configuration to a file. The configuration file will
contain information about the managed switch. You may also save the local user
database on the switch. After saving either file, you may also restore a previously
saved configuration file or local user database file to the switch.

To save a managed switch configuration or user database of a managed switch:

1   From the side navigation bar, click **Unit View - SCS - Files**.

2   Click either the **SCS Configuration** tab or the **User Database** tab, then
    click the **Save** tab.

3   Select the file save method: **Filesystem**, **TFTP**, **FTP**, or **HTTP PUT**.

4   If you selected TFTP, enter the Server IP Address and Firmware Filename
    you wish to load.

    -or-

    If you selected FTP or HTTP, enter the Server IP Address, Username,
    User Password, and Firmware Filename you wish to load.

5   Enter an encryption password if you wish to encrypt the data before download.

6   Click the **Download** button. The **Save As** dialog box will open.

7   Navigate to the desired location and enter a name for the file. Click the **Save** button.

To restore a managed switch configuration or user database of a managed switch:

1   From the side navigation bar, click the **Unit View - SCS - Files** tab.

2   Click either the **SCS Configuration** tab or the **User Database** tab, then click the **Restore** tab.

3   Select the file save method: **Filesystem**, **TFTP**, **FTP**, or **HTTP**.

4   If you selected Filesystem, click the **Browse** button to specify the location of the firmware upgrade file.

     -or-

     If you selected TFTP, enter the Server IP Address and Firmware Filename you wish to load.

     -or-

     If you selected FTP or HTTP, enter the Server IP Address, User Name, User Password, and Firmware Filename you wish to load.

5   Click the **Browse** button. Navigate to the desired location and select the file name. Click the **Upload** button.

6   Enter the decryption password if the original file was encrypted.

7   After the success screen appears, reboot the managed switch to enable the restored configuration. See "Tools - Rebooting and Upgrading" on page 65.

To recover from an Update failure:

If after an update, the SCS does not boot into the new firmware version, you may use the following steps to revert to the previous firmware version.

1   Connect a serial cable to the 10101 port on the rear panel of the switch.

2   Run a terminal program on the PC connected to the 10101 port. The serial port settings should be: 9600 baud, 8 data bits, 1 stop bit, no parity, and no flow control.

3   Turn on the switch.

4   In the terminal program, when the prompt "Hit any key to stop autoboot" appears, press any key. A menu will be displayed.

5   Enter <1> (Boot Alternate) and press <Enter>. The SCS will automatically reboot to the previous firmware version.

6   After the SCS reboots, attempt the upgrade.

Property Identity and Location Settings

The switch can report most device properties directly through the switch web browser. Clicking Identity displays the Unit Identification Properties screen and provides the Part Number, Serial Number, and status of the Dell Remote Access Key. The Unit Location Properties screen displays the Site, Department, and Location.

NOTE: After changing network settings, the switch must be rebooted.

Viewing Version Information

The Version screen displays version information of the Current Application, Boot, Build, Hardware, UART, and Video ASIC versions. This screen is a read-only screen.

Network Settings

NOTE: Only SCS administrators can make changes to the Network dialog box settings. Other users will have view only access.

From the side navigation bar, click **Network** to display the General, IPv4, and IPv6 tabs.

To configure general network settings:

1   Click the **Network** tab, then click the **General** tab to display the SCS General Network Settings screen.

2   Select one of the following options from the LAN Speed drop-down menu: **Auto-Detect**, 10 Mbps Half Duplex, 10 Mbps Full Duplex, 100 Mbps Half Duplex, or 100 Mbps Full Duplex.

NOTE: You must reboot if you change the Ethernet mode.

3   Select either **Enabled** or **Disabled** in the ICMP Ping Reply drop-down menu.

4   Verify or modify the HTTP or HTTPS ports. The settings will default to HTTP 80 and HTTPS 443.

5   Click **Save**.

To configure IPv4 network settings:

1   Click the **Network** tab, then click the **Address** tab to display the IPv4 Settings screen.

2   Click the **IPv4** button.

3   Click to fill or clear the **Enable IPv4** checkbox.

4   Enter the desired information in the Address, Subnet, and Gateway fields. IPv4 addresses are entered as the xxx.xxx.xxx.xxx dot notation.

5   Select either **Enabled** or **Disabled** from the DHCP drop-down menu.

NOTE: If you enable DHCP, any information that you enter in the Address, Subnet, and Gateway fields will be ignored.

6   Click **Save**.

To configure IPv6 network settings:

1   Click the **IPv6** button.

2   Enter the desired information in the Address, Subnet, and Prefix Length fields. IPv6 addresses are entered as the FD00:172:12:0:0:0:0:33 or abbreviated FD00:172:12::33 hex notation.

3   Select either **Enabled** or **Disabled** from the DHCP drop-down menu

✎   **NOTE:** If you enable DHCPv6, any information that you enter in the Address, Gateway, and Prefix length fields will be ignored.

4   Click **Save**.

SNMP Settings

SNMP is a protocol used to communicate management information between network management applications and the switch. Other SNMP managers can communicate with your switch by accessing MIB-II. When you open the SNMP screen, the OBWI will retrieve the SNMP parameters from the unit.

From the SNMP screen, you can enter system information and community strings. You may also designate which stations can manage the switch as well as receive SNMP traps from the switch. If you select **Enable SNMP**, the unit will respond to SNMP requests over UDP port 161.

To configure general SNMP settings:

1   Click **SNMP** to open the SNMP screen.

2   Click to enable the **Enable SNMP** checkbox to allow the switch to respond to SNMP requests over UDP port 161.

3   Enter the system's fully qualified domain name in the Name field, as well as a node contact person in the Contact field.

4   Enter 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 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 switch in the Allowable Managers fields. Alternatively, you may leave these fields blank to allow any station to manage the SCS.

6   Click **Save**.

Auditing Event Settings

An event is a notification sent by the switch to a management station indicating that something has occurred that may require further attention.

To enable individual events:

1   Click **Auditing** to open the Events screen.

2   Specify the events that will generate notifications by clicking the appropriate checkboxes in the list.

    -or-

    Select or clear the checkbox next to **Event Name** to select or deselect the entire list.

3   Click **Save**.

Setting Event Destinations

You can configure audit events to be sent to SNMP trap destinations and Syslog devices. The events enabled on the Events screen are sent to all the devices listed on the Event Destination screen.

1   Click **Auditing** and the **Destinations** tab to open the Event Destinations screen.

2   Type the address of up to four management workstations to which this switch will send events in the SNMP Trap Destination fields, as well as up to four Syslog devices.

3   Click **Save**.

Ports Settings- Configuring a SIP

From the SCS you can display a list of the attached SIPs, as well as the following information about each SIP: Health, EID, Port, Status, Application, and Interface Type. You can click on one of the SIPs to view the following additional information: Switch Type, Boot Version, Application Version, Hardware Version, FPGA Version, Version Available, and Upgrade Status.

You can also delete an offline SIP, enable auto-upgrade, and upgrade the SIP firmware.

Deleting SIPs

To delete an offline SIP:

1   From the side navigation bar, click **Ports - SIPs** to open the SIP screen.

2   Click in the applicable SIP checkbox.

3   Click **Delete Offline**.

Upgrading SIPs

The SIP Upgrade feature allows SCS Administrators to update the SIP with the latest firmware available. This update can be performed using the switch user interface or Avocent management software.

After the memory is upgraded, the switch performs a soft reset, which terminates all SIP sessions. A device experiencing a SIP firmware update may or may not be shown as disconnected. The device will appear normally when the update is completed.

If the SCS is configured to Auto-Upgrade SIPs, the SIPs will automatically update when the switch is updated. To update your switch firmware, see "Tools - Rebooting and Upgrading" on page 65 or the Avocent Management Software Online Help. If issues occur during the normal upgrade process, SIPs may also be force-upgraded when needed.

> **NOTE:** Check http://www.dell.com for firmware upgrade files.

To change the SIP Auto-Upgrade feature:

1   From the side navigation bar, click **Ports - SIPs** to open the SIPs screen.

2   Select the checkboxes next to the SIPs that you wish to upgrade and click **Enable Auto-Upgrade**.

Attention: Disconnecting a SIP during a firmware update or cycling power to the device will render the module inoperable and require the SIP to be returned to the factory for repair.

To upgrade the SIP firmware:

1   From the side navigation bar, click **Ports - SIPs** to open the SIPs screen.

2   Select the checkboxes next to the SIPs that you wish to modify.

3   Select **Choose an operation** and select **Upgrade**.

4   If the settings are correct, click **Upgrade**.

To set the USB Speed:

Ø **NOTE:** This section only applies to the USB2 SIP.

1   From the side navigation bar, click **Ports - SIPs** to open the SIPs screen.

2   Select the checkboxes next to the SIPs that you wish to modify.

Launching a Session

Ø **NOTE:** Java 1.6.0_11 or later is required to launch a session.

To launch a session:

1   From the side navigation bar, select **Target Devices**. A list of available devices will appear.

2   The applicable action, KVM Session, will be displayed in the Action column, and will depend on the target device that was selected to launch the session. If more than one action is available for a given target device, click the drop-down arrow and select the applicable action from the list.

If the target device is currently in use, you may be able to gain access by forcing a connection to the device if your preemption level is equal to or higher than the current user's.

To switch to the active session from the local UI (local users only):

1   From the side navigation bar, select **Local Session**.

2   Select the **Resume Active Session** checkbox. The Video Viewer window will appear.

    NOTE: The Dell RAK is required for KVM remote access.

    NOTE: From the Active Sessions screen, you can view a list of active sessions. The following information is listed about each session: Target Device, Owner, Remote Host, Duration, and Type.

General Sessions Settings

To configure general session settings:

1   From the side navigation bar, select **Sessions - General**. The General Session Settings screen appears.

2   Select or deselect the **Enable Inactivity Timeout** checkbox.

3   In the Inactivity Timeout field, enter the amount of inactive time you want to pass before the session closes (from 1 to 90 minutes).

4   In the Login Timeout field, enter the amount of inactive time you want to pass before you must log in again (from 21 to 120 seconds).

5   Select or deselect the **Enable Preemption Timeout** checkbox.

6   In the Preemption Timeout field, enter the amount of time (from 1 to 120 seconds) that a prompt will be displayed to inform you that your session is going to be preempted.

7   Select the applicable session sharing options (Enabled, Automatic, Exclusive, or Stealth).

8   Select the Input Control Timeout from 1 to 50, with 1 representing one tenth of a second.

9   Click **Save**.

Local User Account Settings

> **NOTE:** User Account settings are supported when the Dell RAK is installed.

The OBWI provides local and login security through administrator-defined user accounts. By selecting **User Accounts** on the side navigation bar, administrators may add and delete users, define user preemption, and access levels, and change passwords.

Access Levels

> **NOTE:** Multiple access levels are supported when the Dell RAK is installed.

When a user account is added, the user may be assigned to any of the following access levels: SCS Administrators, User Administrators, and Users.

Table 4.4: Allowed Operations by Access Level

Operation	SCS Administrator	User Administrator	Users
Configure Interface System-level Settings	Yes	No	No
Configure Access Rights	Yes	Yes	No
Add, Change and Delete User Accounts	Yes, for all Access Levels	Yes, for Users and User Administrators only	No
Change Your Own Password	Yes	Yes	Yes
Access Server	Yes, all Servers	Yes, all Servers	Yes, if allowed

To add a new user account (User Administrator or SCS Administrator only):

1   On the side navigation bar, select **User Accounts - Local User Accounts** to open the Local User Accounts screen.

2   Click the **Add** button.

3   Enter the name and password of the new user in the blanks provided.

4   Select the access level for the new user.

✎ **NOTE:** Multiple access levels are supported when the Dell RAK is installed.

5   Select any of the available devices that you wish to assign to the user account and click **Add**.

✎ **NOTE:** User Administrators and SCS Administrators can access all devices.

6   Click **Save**.

To delete a user account (User Administrator or SCS Administrator only):

1   On the side navigation bar, select **User Accounts - Local Accounts** to open the Local User Accounts screen.

2   Click the checkbox to the left of each account that you wish to delete, then click **Delete**.

To edit a user account (Administrator or active user only):

1   On the side navigation bar, select **User Accounts - Local Accounts**. The Local User Accounts screen is displayed.

2   Click the name of the user you wish to edit. The user profile will appear.

3   Fill out the user information on the screen, then click **Save**.

Virtual Media Session Settings

To set virtual media options:

1   From the side navigation bar, select **Sessions - Virtual Media** to open the Virtual Media Session Settings screen.

2   Either enable or disable the **Virtual Media locked to KVM Sessions** checkbox.

3   Either enable or disable the **Allow Reserved Sessions** checkbox.

4   Select one of the following options from the Virtual Media Access Mode from the drop-down menu: **Read-Only** or **Read-Write**.

5   Select one of the Encryption Levels that you wish to be supported.

6   Click **Save**.

7   Select the checkbox next to each SIP for which you want to enable virtual media and click **Enable VM**.

    -or-

    Select the checkbox next to each SIP for which you want to disable virtual media and click **Disable VM**.

Virtual Media Options

You can determine the behavior of the switch during a virtual media session using the options provided in the Virtual Media Session Settings screen. The following table outlines the options that can be set for virtual media sessions.

Local Users

Local users can determine the behavior of virtual media from the Local Session screen. In addition to connecting and disconnecting a virtual media session, you can configure the settings that are listed in the following table.

Table 4.5: Local Virtual Media Session Settings

Setting	Description
CD ROM/ DVD ROM	Allows virtual media sessions to the first detected CD-ROM or DVD-ROM (read-only) drives. Enable this checkbox to establish a virtual media CD-ROM or DVD-ROM connection to a device. Disable to end a virtual media CD-ROM or DVD-ROM connection to a device.
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 device. Disable to end a virtual media mass storage connection to a device.

Avocent User Account Settings

> **NOTE:** User account settings are supported when the Dell RAK is installed.

You can contact and register an unmanaged switch with an Avocent management software device by specifying the IP address of the management software device.

To configure the device IP address:

1   On the side navigation bar, select **User Accounts - Avocent**. The Avocent Management Software Settings screen is displayed.

2   Enter the device IP addresses that you want to contact. Up to four addresses are allowed.

3   Use the scroll bar to select the desired retry interval.

4   To disassociate the SCS that has been registered with the device, click the **Disassociate** button.

5   Click **Save**.

Override Admin

> **NOTE:** Override Admin is supported when the Dell RAK is installed.

To be prepared in case a network failure should occur, configure the Override Admin Account before any other settings.

To configure the Override Admin Account in the OBWI:

1   Click **User Accounts**, then click **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**.

Active Sessions

From the Active Sessions screen, you can view a list of active sessions and the following information about each session: Target Device, Owner, Remote Host, Duration, and Type.

Closing a Session

To close a session:

1 From the side navigation bar, select **Active Sessions** to display the SCS Active Sessions screen.

2 Click the checkbox next to the desired target device(s).

3 Click **Disconnect**.

✎ **NOTE:** If there is an associated locked virtual media session, it will be disconnected.

To close a session (local users only):

1 From the side navigation bar, select **Local Session**.

2 Select the **Disconnect Active Session** checkbox.

5

Video Viewer

The Video Viewer is used to conduct a KVM session with the target devices attached to a switch using the OBWI. With the Dell RAK installed, the OBWI will display the "KVM Session" links on the "Target Devices" page, which is also referred to as the home page. In addition to the list of devices, additional options/pages associated with remote KVM access will become available. When you connect to a device using the Video Viewer, the target device desktop appears in a separate window containing both the local and the target device cursors.

NOTE: To use the remote access feature, the Dell RAK must be installed and you will need to configure the network settings using OSCAR or the Setup port. The 1081AD/2161AD switch can be managed at a reduced level without the Dell RAK once the network settings have been configured.

The switch OBWI software uses a Java-based program to display the Video Viewer window. The switch OBWI automatically downloads and installs the Video Viewer the first time it is opened.

NOTE: Java 1.6.0_11 or later is required to launch a session.

NOTE: The switch OBWI does not install the Java Resource Engine (JRE). The JRE is available as a free download from http://www.sun.com.

NOTE: The switch OBWI uses system memory to store and display images within Video Viewer windows. Each opened Video Viewer window requires additional system memory. An 8-bit color setting on the client device requires 1.4 MB of memory per Video Viewer window, a 16-bit color setting requires 2.4 MB and a 32-bit color setting requires 6.8 MB. If you attempt to open more Video Viewer windows than your system memory allows (usually four), you will receive an out-of-memory error and the requested Video Viewer window will not open.

If the device you are attempting to access is currently being viewed by another user, you will be prompted to preempt the other user if your preemption level is equal to or greater than the other user's preemption level. Also, the SCS Administrator can disconnect an active user via the Active Session page. For more information, see "Active Sessions" on page 79.

Figure 5.1: Video Viewer Window (normal window mode)
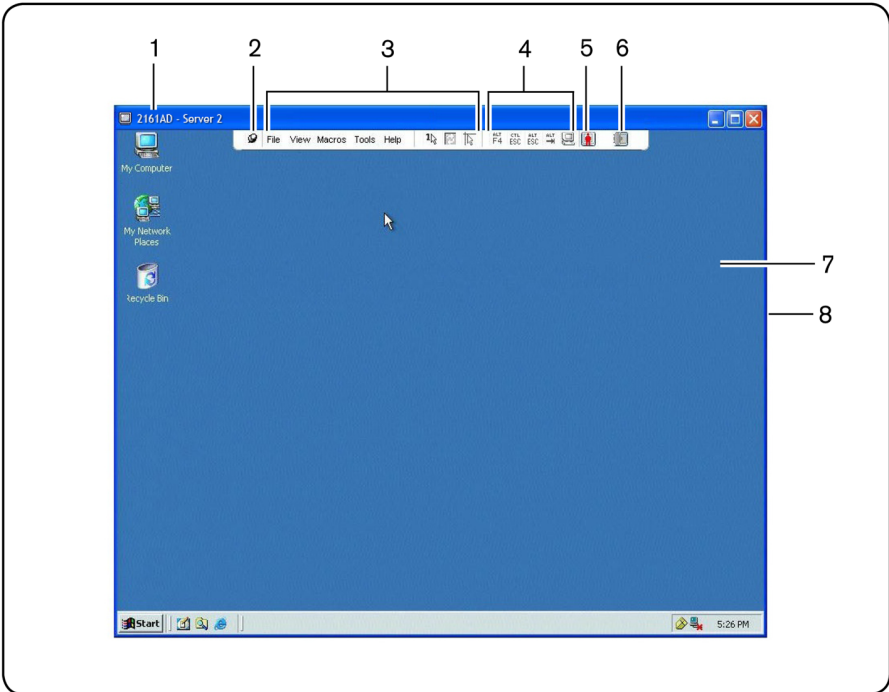
Table 5.1: Video Viewer Descriptions

Number	Description
1	Title Bar: Displays the name of the target device being viewed. When in Full Screen mode, the title bar disappears and the target device name appears between the menu and toolbar.
2	Thumbtack icon: Locks the display of the menu and toolbar so that it is visible at all times.
3	Menu and toolbar: Enables you to access many of the features in the Video Viewer window. The menu and toolbar is in a show/hide state if the thumbtack has not been used. Place your cursor over the toolbar to display the menu and toolbar. Up to ten commands and/or macro group buttons can be displayed on the toolbar. By default, the Single Cursor Mode, Refresh, Automatic Video Adjust and Align Local Cursor buttons appear on the toolbar. For more information, see "Video Viewer" on page 81 and "Macros" on page 103.
4	Macro buttons: Commonly used keyboard sequences that can be sent to the target device.
5	Connection Status Indicator: Indicates the status of the user that is connected to the SCS for this device. The modes are exclusive, basic active connection, primary active sharing, secondary active sharing, passive sharing, stealth, and scanning.
6	Smart Card Status Indicators: Indicate whether or not a smart card is in the smart card reader. The Video Viewer screen smart card icon is greyed out and indicates that the smart card option is unavailable or disabled. The icon is green if the smart card is mapped.
7	Display area: Accesses the device desktop.
8	Frame: Resizes the Video Viewer window by clicking and holding on the frame.

Changing the Toolbar

You can choose the amount of elapsed time before the toolbar hides in the Video Viewer window when it is in show/hide state (that is, not locked in place by the thumbtack).

To specify a toolbar hide time:

1   Select **Tools - Session Options** from the Video Viewer window menu.

    -or-

    Click the **Session Options** button.

    The **Session Options** dialog box appears.

2   Click the **Toolbar** tab.

3   Use the arrow keys to specify the number of elapsed seconds prior to hiding the toolbar.

4   Click **OK** to save your changes and close the dialog box.

Window Size

 NOTE: The View - Scaling command is not available if the Video Viewer window is in Full Screen mode.

When the switch OBWI is used for the first time, any open Video Viewer windows have a display resolution of 1024 x 768 until the user changes the value. Each Video Viewer window can be set to a different resolution.

The switch OBWI automatically adjusts the display if the window size changes during a session as long as auto-scaling is enabled. If the target device resolution changes any time during a session, the display adjusts automatically.

To change the Video Viewer window resolution:

1   Select the **View - Scaling** command.

2   Select the desired resolution.

Adjusting the View

Using menus or task buttons in the Video Viewer window, you can do the following:

- Align the mouse cursors.

- Refresh the screen.

- Enable or disable Full Screen mode. When Full Screen mode is enabled, the image adjusts to fit the desktop up to a size of 1600 x 1200 or 1680 x 1050 (widescreen). If the desktop has a higher resolution, the following occurs:

  - The full-screen image is centered in the desktop and the areas surrounding the Video Viewer window are black.

  - The menu and toolbar are locked to be visible at all times.

- Enable automatic, full, or manual scaling of the session image:

  - With full scaling, the desktop window remains fixed and the device image scales to fit the window.

  - With automatic scaling, the desktop window is sized to match the resolution of the target device being viewed.

  - With manual scaling, a drop-down menu of supported image scaling resolutions is displayed.

- Change the color depth of the session image.

To align the mouse cursors:

Click the **Align Local Cursor** button in the Video Viewer window toolbar. The local cursor should align with the cursor on the remote device.

NOTE: If cursors drift out of alignment, turn off mouse acceleration in the attached device.

To refresh the screen, click the **Refresh Image** button in the Video Viewer window, or select **View - Refresh** from the Video Viewer window menu. The digitized video image is completely regenerated.

To enable Full Screen mode, click the **Maximize** button, or select **View - Full Screen** from the Video Viewer window menu. The desktop window disappears and only the accessed device desktop is visible. The default resolution is 1024 x 768. The screen resizes up to a maximum of 1600 x 1200 (standard) or 1680 x 1050 (widescreen). If the desktop has a higher resolution, then a black background surrounds the full screen image. The floating toolbar appears.

To disable Full Screen mode, click the **Full Screen Mode** button on the floating toolbar to return to the desktop window.

To enable full scaling, select **View - Scaling** from the Video Viewer window menu and select **Full Scale**. The device image automatically scales to the resolution of the target device being viewed.

To enable manual scaling, select **View - Scaling** from the Video Viewer window menu. Choose the dimension to scale the window. The available manual scaling sizes will vary according to your system.

Refreshing the Image

Clicking the **Refresh Image** button in the **Manual Video Adjust** dialog box completely regenerates the digitized video image.

NOTE: You can also select **View - Refresh** from the Video Viewer window menu to refresh the image.

Video Settings

Generally, the Video Viewer window automatic adjustment features optimize the video for the best possible view. However, users can fine-tune the video with the help of Dell Technical Support by selecting the **Tools - Manual Video Adjust** command in the Video Viewer window menu or clicking the **Manual**

Video Adjust button. This displays the **Manual Video Adjust** dialog box. Video adjustment is a per device setting.

Users can also verify the level of packets per second required to support a static screen by observing the packet rate located in the lower left-hand corner of the dialog box.

To manually adjust the video quality of the window:

> ![note icon] **NOTE:** The following video adjustments should be made only with the help of Dell Technical Support.

1   Select **Tools - Manual Video Adjust** from the Video Viewer window menu.

    -or-

    Click the **Manual Video Adjust** button.

    The **Manual Video Adjust** dialog box (Figure 5.2) will appear.

Figure 5.2: Manual Video Adjust Dialog Box
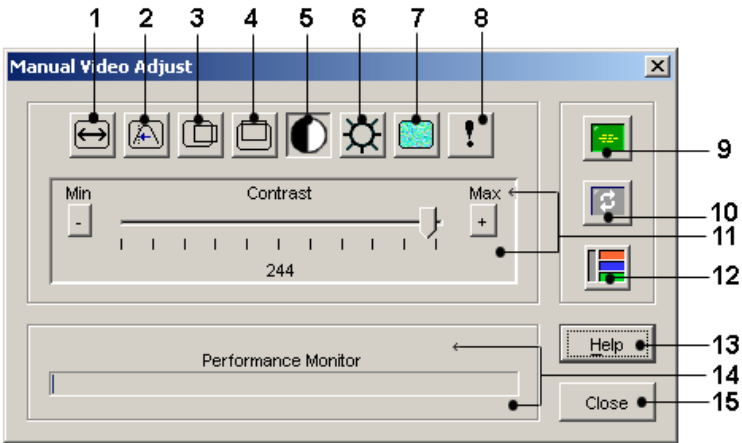
Table 5.2: Descriptions for Manual Video Adjust Dialog Box

Number	Description	Number	Description
1	Image Capture Width	9	Automatic Video Adjustment
2	Pixel Sampling/Fine Adjust	10	Refresh Image
3	Image Capture Horizontal Position	11	Adjustment bar
4	Image Capture Vertical Position	12	Video Test Pattern
5	Contrast	13	Help
6	Brightness	14	Performance Monitor
7	Noise Threshold	15	Close Button
8	Priority Threshold		

2   Click the icon corresponding to the feature you wish to adjust.

3   To move the Contrast slider bar and then fine-tune the setting, click the **Min** (-) or **Max** (+) button to adjust the parameter for each icon pressed. The adjustments display immediately in the Video Viewer window.

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

Target Video Settings

The Image Capture Width, Pixel Sampling/Fine Adjust, Image Capture Horizontal Position and Image Capture Vertical Position adjustments affect how the device video is captured and digitized. They are seldom changed.

The image capture parameters are automatically changed by the Automatic Adjustment function. A special image is required on the device in order to make accurate adjustments independently.

Automatic Video Adjustment

In most cases, you do not need to alter the Video Settings from the default settings. The system automatically adjusts and uses the optimal video parameters. The switch OBWI performs best when the video parameters are set such that no (0) video packets are transmitted for a static screen.

To adjust your video parameters, click on the **Auto Adjust Video** button in the **Manual Video Adjust** dialog box.

NOTE: You can also select Tools - Automatic Video Adjust from the Video Viewer window menu or click the Automatic Video Adjust toolbar icon to automatically adjust the video.

Video Test Pattern

To toggle the video test pattern, click the **Video Test Pattern** button in the **Manual Video Adjust** dialog box.. Click the **Video Test Pattern** button again to toggle back to a normal video image.

Vendor-specific Video Settings

Video settings vary significantly among manufacturers. Dell maintains an online database of optimized video settings for various video cards, particularly Sun-specific ones. This information can be obtained from the Dell online knowledge base or by calling Dell Technical Support.

Color Settings

The Dambrackas Video Compression® (DVC) algorithm enables users to adjust the number of viewable colors in a remote session window. You can choose to display more colors for the best fidelity or fewer colors to reduce the volume of data transferred on the network.

Video Viewer windows 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.

You can specify the color depths of individual ports and channels by selecting the **View Color** command in a remote session window. These settings are saved individually per channel.

Contrast and Brightness

If the image in the Video Viewer window is too dark or too light, select **Tools - Automatic Video Adjust** or click the **Automatic Video Adjust** button. This command is also available in the **Video Adjustments** dialog box. In most cases, this corrects video issues.

When clicking **Auto Adjust** several times does not set the contrast and brightness as desired, adjusting the contrast and brightness manually can help. Increase the brightness. Do not go more than 10 increments before moving the contrast. Generally, the contrast should be moved very little.

Noise Settings

In some cases, noise in the video transmission keeps the packets/sec count up, which is indicated by small dots changing in the area of the cursor when it is moved. Varying the threshold values may result in "quieter" screens and can improve cursor tracking.

You can modify Noise Threshold and Priority Threshold values if you are using standard video compression. You can restore default threshold values by clicking **Auto Adjust Video**.

![icon] **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.

![icon] **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 are used for fine-tuning.

See "Adjusting the View" on page 85 for information about changing the color depth.

Mouse Settings

The Video Viewer window mouse options affect cursor type, Cursor mode, scaling, alignment, and resetting. Mouse settings are device-specific; that is, they may be set differently for each device.

> **NOTE:** If the device does not support the ability to disconnect and reconnect the mouse (almost all newer PCs do), then the mouse will become disabled and the device will have to be rebooted.

Cursor Type

The Video Viewer window (Figure 5.3) offers five appearance choices for the local mouse cursor. You can also choose no cursor or the default cursor.

In Single Cursor mode, the display of the local (second) cursor in the Video Viewer window turns off and only the target device mouse pointer is visible. The only mouse movements that appear are those of the target device remote cursor. Use Single Cursor mode when there is no need for a local cursor.

Figure 5.3: Video Viewer Window With Local and Remote Cursors
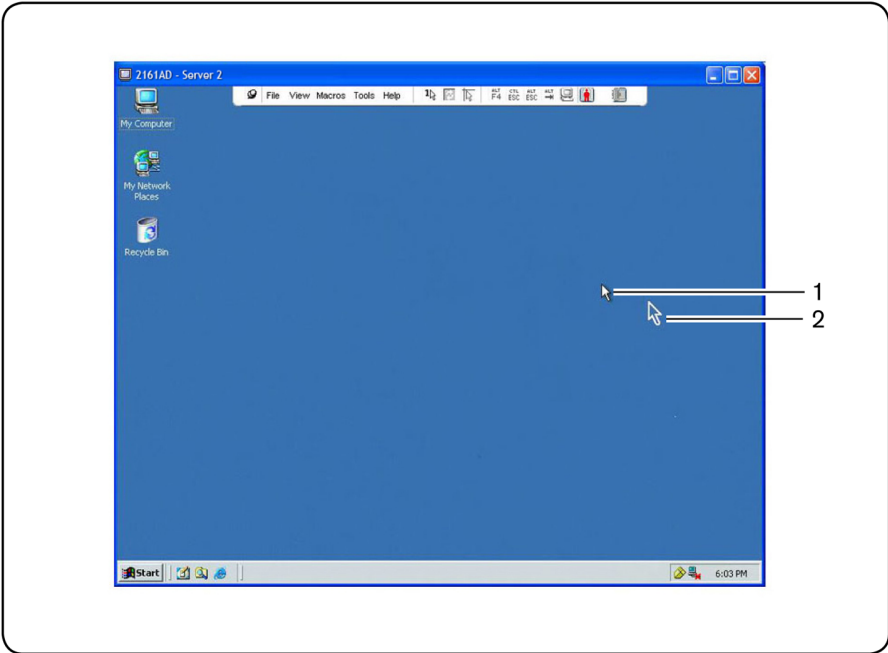
Table 5.3: Descriptions for Figure 5.3

Number	Description
1	Remote Cursor
2	Local Cursor

The Cursor mode status of the Video Viewer window displays in the title bar, including the keystroke that will exit Single Cursor mode. You can define the keystroke that will exit Single Cursor mode in the **Session Options** dialog box.

⬛ **NOTE:** When using a device that captures keystrokes before they reach the client device, you should avoid using those keys to restore the mouse pointer.

To enter Single Cursor mode, select **Tools - Single Cursor Mode** from the Video Viewer window menu, or click the **Single Cursor Mode** button. The local cursor does not appear and all movements are relative to the target device.

To select a key for exiting Single Cursor mode:

1   Select **Tools - Session Options** from the Video Viewer window menu.

   -or-

   Click the **Session Options** button.

   The **Session Options** dialog box appears.

2   Click the **Mouse** tab.

3   Select a terminating keystroke from the drop-down menu in the Single Cursor mode area.

4   Click **Save** to save settings.

When you enable Single Cursor mode, you can press the specified key to return to Regular Desktop mode.

To exit Single Cursor mode, press the key on the keyboard that is identified in the title bar.

To change the mouse cursor setting:

1   Select **Tools - Session Options** from the Video Viewer window menu.

   -or-

   Click the **Session Options** button.

   The **Session Options** dialog box appears.

2   Click the **Mouse** tab.

3   Select a mouse cursor type in the Local Cursor panel.

4   Click **OK** to save settings.

Mouse Scaling

Some earlier versions of Linux did not support adjustable mouse accelerations. For installations that must support these earlier versions, you can choose among three pre-configured mouse scaling options or set your own custom scaling. The pre-configured 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 sends an equivalent mouse movement to the target device.

- In a 2:1 scaling ratio, the same mouse movement sends a 2X mouse movement.

- In a 1:2 scaling ratio, the value is 1/2X.

To set mouse scaling:

1 Select **Tools - Session Options** from the Video Viewer window menu.

   -or-

   Click the **Session Options** button.

   The **Session Options** dialog box appears.

2 Click the **Mouse** tab.

3 To use one of the pre-configured settings, check the appropriate radio button.

   -or-

   To set custom scaling:

   a. Click the **Custom** radio button to enable the X and Y fields.

   b. Type a scaling value 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 range is 0.25-3.00.

Mouse Alignment and Synchronization

Because the switch OBWI cannot get constant feedback from the mouse, there are times when the mouse on the switch may lose sync with the mouse on the

host system. If your mouse or keyboard no longer responds properly, you can align the mouse to reestablish proper tracking.

Alignment causes the local cursor to align with the remote target device's cursor. Resetting causes a simulation of a mouse and keyboard reconnect as if you had disconnected and reconnected them.

To realign the mouse, click the **Align Local Cursor** button in the Video Viewer window toolbar.

Virtual Media

The virtual media feature allows the user on the client device to map a physical drive on that machine as a virtual drive on a target device. The client device may also add and map an ISO or floppy image file as a virtual drive on the target device. You may have one CD drive and one mass storage device mapped concurrently.

- A CD/DVD drive, disk image file (such as an ISO or floppy image file) is mapped as a virtual CD/DVD-ROM drive.
- A floppy drive, USB memory device or other media type is mapped as a virtual mass storage device.

For information on configuring virtual media settings using the OBWI, see "Virtual Media Session Settings" on page 76.

Requirements

The device must support virtual media and be connected to the KVM switch with a USB2 or USB2+CAC SIP.

The target device must be intrinsically able to use the types of USB2-compatible media that you virtually map. In other words, if the target device does not support a portable USB memory device, you cannot map that on the client device as a virtual media drive on the target device.

The user (or user group to which the user belongs) must have permission to establish virtual media sessions and/or reserved virtual media sessions to the target device. See "Local User Account Settings" on page 75.

Only one virtual media session may be active to a target device at one time.

Sharing and Preemption Considerations

The KVM and virtual media sessions are separate; therefore, there are many options for sharing, reserving, or preempting sessions. The Avocent management software has the flexibility to accommodate the system needs.

For example, the KVM and virtual media sessions may be locked together. In this mode, when a KVM session is disconnected, so is the associated virtual media session. If the sessions are not locked together, the KVM session can be closed but the virtual media session will remain active. This could be desirable if a user is performing a time-intensive task using the virtual media session (such as an operating system load), and wants to establish a KVM session with a different target device to perform other functions while the operating system load progresses.

Once a target device has an active virtual media session without an associated active KVM session, two situations can occur - the original user (User A) can reconnect or a different user (User B) can connect to that channel. You may set an option in the **Virtual Media** dialog box (Reserved) that allows only the User A to access that channel with a KVM session.

If User B is allowed to access that session (the Reserved option is not enabled), User B could control the media that is being used in the virtual media session. By using the Reserved option in a tiered environment, only User A could access the lower switch and the KVM channel between the upper switch and lower switch would be reserved for User A.

Virtual Media Dialog Box

The **Virtual Media** dialog box allows you to manage the mapping and unmapping of virtual media. The dialog box displays all the physical drives on

the client device that can be mapped as virtual drives. You may also add ISO and floppy image files and then map them using the **Virtual Media** dialog box.

After a device is mapped, the **Virtual Media** dialog box Details View displays information about the amount of data transferred and the time elapsed since the device was mapped.

You may specify that the virtual media session is reserved. When a session is reserved, and the associated KVM session is closed, another user cannot launch a KVM session to that target device. If a session is not reserved, another KVM session may be launched.

You may also reset the SIP from the **Virtual Media** dialog box. This action will reset every form of USB media on the target device. It should be used with caution and only when the target device is not responding.

Opening a Virtual Media Session

To launch a virtual media session:

Select **Tools - Virtual Media** from the Video Viewer menu. The **Virtual Media** dialog box (Figure 5.4) will appear. To make this a reserved session, click **Details,** then select the **Reserved** checkbox.

Figure 5.4: Video Viewer Virtual Media Dialog Box
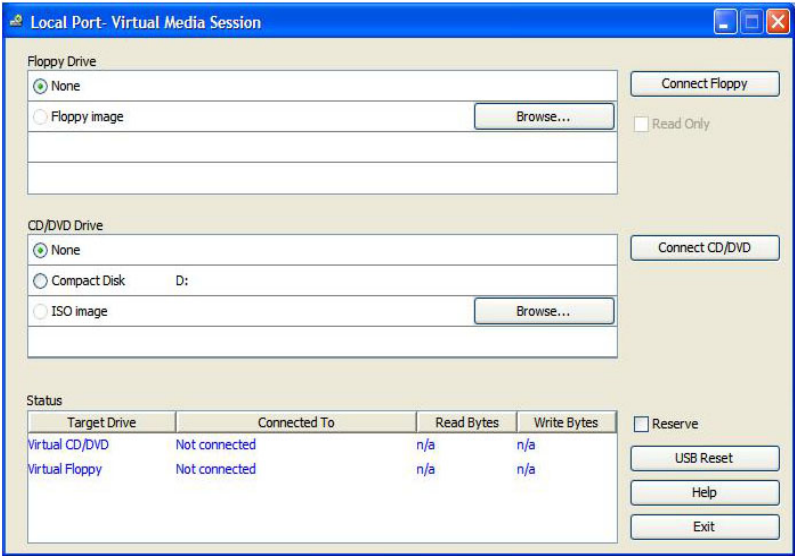
To map a virtual media drive:

1   Open a virtual media session from the Video Viewer menu by selecting
    Tools - Virtual Media.

2   To map a physical drive as a virtual media drive:

    a.   In the **Virtual Media** dialog box, click the **Mapped** checkbox next to
         the drive(s) you wish to map.

    b.   If you wish to limit the mapped drive to read-only access, click the
         Read Only checkbox next to the drive. If the virtual media session
         settings were previously configured so that all mapped drives must be
         read only, this checkbox will already be enabled and cannot be changed.

         You might wish to enable the **Read Only** checkbox if the
         session settings enabled read and write access, but you wished
         to limit a particular drive's access to read only.

3   To add and map an ISO or floppy image as a virtual media drive:

a. In the **Virtual Media** dialog box, click **Add Image**.

b. The common file dialog box will appear, with the directory containing disk image files (that is, those ending in .iso or .img) displayed. Select the desired ISO or floppy image file and click **Open**.

-or-

If the client device's operating system supports drag-and-drop, select the desired ISO or floppy image file from the common file dialog box, and drag it onto the **Virtual Media** dialog box.

c. The file's header is checked to ensure it is correct. If it is, the common file dialog box will close and the chosen image file will appear in the **Virtual Media** dialog box, where it can be mapped by clicking the **Mapped** checkbox.

d. Repeat steps a through c for any additional ISO or floppy images you wish to add. You may add any number of image files (up to the limits imposed by memory), but you may only have one virtual CD or DVD or virtual mass storage mapped concurrently.

If you attempt to map too many drives (one CD or DVD and one mass storage device) or too many drives of a particular type (more than one CD or DVD or mass storage device), a message will be displayed. If you still wish to map a new drive, you must first unmap an existing mapped drive, then map the new drive.

After a physical drive or image is mapped, it may be used on the target device.

To unmap a virtual media drive:

1 In the **Virtual Media** dialog box, uncheck the **Mapped** checkbox next to the drive you wish to unmap.

2 You will be prompted to confirm. Confirm or cancel the unmapping.

3 Repeat for any additional virtual media drives you wish to unmap.

To display virtual media drive details:

In the **Virtual Media** dialog box, click **Details**. The dialog box expands to display the Details table. Each row indicates:

- Target Drive - Name used for the mapped drive, such as Virtual CD 1 or Virtual CD 2.
- Mapped to - Identical to Drive information that appears in the Client View Drive column.
- Read Bytes and Write Bytes - Amount of data transferred since the mapping.
- Duration - Elapsed time since the drive was mapped.

To close the Details view, click **Details** again.

To reset all USB devices on the target device:

NOTE: 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.

1   In the **Virtual Media** dialog box, click **Details**.

2   The Details View will appear. Click **USB Reset**.

3   A warning message will appear, indicating the possible effects of the reset. Confirm or cancel the reset.

4   To close the Details view, click **Details** again.

Closing a Virtual Media Session

To close the **Virtual Media** dialog box:

1   Click **Exit**.

2   If you have any mapped drives, a message is displayed, indicating that the drives will be unmapped. Confirm or cancel the operation.

If a user attempts to disconnect a virtual media session or an active KVM session that has an associated locked virtual media session, a confirmation message is displayed, indicating that any virtual media mappings will be lost.

Smart Cards

You can connect a smart card reader to an available USB port on the client device and access attached target devices on the switch system. You can then launch a KVM session to open the Video Viewer and map a smart card.

NOTE: For all smart card readers, you must use a Dell USB2+CAC SIP or an Avocent VMC IQ module.

The smart card status is indicated by the smart card icon at the far right of the Video Viewer toolbar. The following table describes the smart card status icons.

Table 5.4: Smart Card Icons

Icon	Description
	A smart card is not in the smart card reader, or a smart card reader is not attached.
	A smart card is in the smart card reader but has not been mapped yet.
	A smart card is mapped (green icon).

To map a smart card:

1   Open a KVM session to display the Video Viewer window menu.

2   Insert a smart card into the smart card reader attached to your client device.

3   Click **Tools - Map Smart Card** on the Video Viewer window menu.

4   If no smart card is mapped to the target device, the No Card Mapped option will have a dot beside it. Select your smart card, listed below this option, to map the smart card.

To unmap a smart card, close out the KVM session by clicking **X** in the Video Viewer window menu, selecting **Tools - No Card Mapped**, and either removing

the smart card from the smart card reader or disconnecting the smart card reader from the client server.

Keyboard Pass-through

Keystrokes that a user enters when using a Video Viewer window may be interpreted in two ways, depending on the Screen mode of the Video Viewer window.

- If a Video Viewer window is in Full Screen mode, all keystrokes and keyboard combinations except <Ctrl-Alt-Del> are sent to the remote target device being viewed.

- If a Video Viewer window is in Regular Desktop mode, Keyboard Pass-through mode can be used to control whether the remote target device or local computer recognizes certain keystrokes or keystroke combinations.

Keyboard pass-through must be specified using the **Session Options** dialog box. When enabled, keyboard pass-through sends all keystrokes and keystroke combinations except <Ctrl-Alt-Del> to the remote target device being viewed when the Video Viewer window is active. When the local desktop is active, keystrokes and keystroke combinations entered by the user affect the local computer.

NOTE: The Ctrl-Alt-Del keyboard combination can be sent only to a remote target device by using a macro.

NOTE: The Japanese keyboard ALT-Han/Zen keystroke combination is always sent to a remote target device regardless of the Screen mode or keyboard pass-through setting.

To specify keyboard pass-through:

1   Select **Tools - Session Options** from the Video Viewer window menu.

-or-

Click the **Session Options** button.

The **Session Options** dialog box appears.

2   Click the **General** tab.

3   Select **Pass-through all keystrokes in regular window mode**.

4   Click **OK** to save setting.

Macros

The switch OBWI comes pre-configured with macros for the Windows, Linux, and Sun platforms.

To send a macro, select **Macros - <desired macro>** from the Video Viewer window menu, or select the desired macro from the buttons available on the Video Viewer menu.

Saving the View

You can save the display of a Video Viewer either to a file or to the clipboard for pasting into a word processor or other program.

To capture the Video Viewer window to a file:

1   Select **File - Capture to File** from the Video Viewer window menu.

-or-

Click the **Capture to File** button.

The **Save As** dialog box appears.

2   Enter a filename and choose a location to save the file.

3   Click **Save** to save the display to a file.

To capture the Video Viewer window to your clipboard, select **File - Capture to Clipboard** from the Video Viewer window menu, or click the **Capture to Clipboard** button. The image data is saved to the clipboard.

Closing a Session

To close a Video Viewer window session:

Select **File - Exit** from the Video Viewer window.

6

Terminal Operation

Each SCS may be configured at the switch level through the Terminal Console menu interface, which is accessed through the 10101 setup port. All terminal commands are accessed through a terminal screen or a PC running terminal emulation software.

NOTE: The preferred method is to make all configuration settings in the local UI.

To connect a terminal to the switch:

1 Using a DB-9 M/F serial adaptor, connect a terminal or a PC that is running terminal emulation software, such as HyperTerminal software, to the 10101 port on the back panel of the switch. The terminal settings are 9600 bits per second (bps), 8 bits, 1 stop bit, no parity and no flow control.

2 Turn on the switch and each target device. When the switch completes initialization, the Console menu will display the following message: **Press any key to continue.**

Network Configuration

To configure network settings using the Console menu:

1 When you turn on the SCS, the switch initializes for approximately one minute. After it completes initialization, press any key on the terminal or on the computer running the terminal emulation software to access the Console menu interface.

The terminal may be connected at any time, even when the switch is already turned on.

2   Once the Console Main Menu is displayed, type the number corresponding to Network Configuration and press <Enter>.

3   Type 1 and press <Enter> to set your network speed. For best performance, set the SCS at the same speed as the Ethernet switch to which it is attached. Press <Enter> to return to the Console Network Configuration menu.

4   Type 2 and press <Enter> to specify whether you are using a static or DHCP address.

    A static IP configuration may be used to provide a user-defined IP address, netmask, or prefix length, and default gateway for the SCS.

    DHCP is a protocol that automates the configuration of TCP/IP-enabled computers. When DHCP is selected, the IP address, netmask or prefix length, and default gateway settings are automatically assigned to the SCS and may not be modified by a switch user.

    If you are using the DHCP option, configure your DHCP device to provide an IP address to the switch and then go to step 6.

5   Select the remaining options from the Network Configuration menu to finish the configuration of your SCS with an IP address, netmask or prefix length, and default gateway.

6   Type 0 (zero) and press <Enter> to return to the Console Main menu.

Other Console Main Menu Options

Besides the Network Configuration option, the Console Main Menu of the SCS features the following menu items: Firmware Management, Enable Debug Messages, Set/Change Password, Restore Factory Defaults, Reset Switch, Set Web Interface Ports, and Exit. Each menu item is discussed in this section.

Firmware Management

This menu contains the Flash Download selection. For more information, see "Tools - Rebooting and Upgrading" on page 65.

Enable Debug Messages

This menu option turns on console status messages. Because this can significantly reduce performance, only enable debug messages when instructed to do so by Technical Support. When you are finished viewing the messages, press any key to exit this mode.

Set/Change Password

This menu option allows enabling and disabling of serial port security, which locks the serial port with a user-defined password.

Restore Factory Defaults

This menu option will restore all switch options to the default settings.

Reset Switch

This menu option allows you to execute a soft reset of the SCS.

Set Web Interface Ports

The SCS uses ports 80 and 443 for HTTP and HTTPS port numbers, respectively. The user can modify or specify alternate ports.

NOTE: A reboot of the SCS is required to use new port numbers.

Exit

This menu selection will return you to the ready prompt. If the Console menu interface password is enabled, you must exit the Console Main menu so that the next user will be prompted with the Password login screen.

A

Appendix A: MIB and SNMP Traps

The SCS has the ability to send audit events to an SNMP Manager. The SNMP traps are defined in an SNMP Trap MIB.

The Trap MIB file may be uploaded from the SCS using the Save Trap MIB function. The uploaded Trap MIB file may then be loaded into an SNMP Trap Receiver application.

This appendix describes the trap events that may be generated by the SCS. Although care has been taken to keep the information in this appendix up to date, the actual Trap MIB file will contain the most accurate trap information.

An SNMP manager may access MIB-II objects of the SCS using the IPv4 or IPv6 protocols.

By design, the enterprise specific MIB objects within the SCS cannot be accessed using SNMP.

The SCS trap 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 Internet.

*   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 inter-networks.

- RFC-1215

  Describes the SNMP standardized traps and provides a means for defining enterprise-specific traps. The specific objects reported by each trap are defined in the Trap MIB file which is uploaded from the SCS. The following table is a list of the generated trap events.

Table A.1: Generated Trap Events

Trap Event	Trap Number
User Authentication Failure	1
User Login	2
User Logout	3
Target Session Started	4
Target Session Stopped	5
Target Session Terminated	6
Traps 7-8 are Unused	7-8
User Added	9
User Deleted	10
User Modified	11
Reboot Started	12
Image File Upgrade Started	13
Image File Upgrade Results	14

Trap Event	Trap Number
SIP Added	15
SIP Removed	16
Target Device Name Changed	17
Tiered Switch Added	18
Tiered Switch Removed	19
Tiered Switch Name Changed	20
Configuration File Loaded	21
User Database File Loaded	22
Traps 23-32 are Unused	23-32
User Locked	33
User Unlocked	34
SIP Upgrade Started	35
SIP Image Upgrade Result	36
SIP Restarted	37
Virtual Media Session Started	38
Virtual Media Session Stopped	39
Virtual Media Session Terminated	40
Virtual Media Session Reserved	41
Virtual Media Session Unreserved	42

Trap Event	Trap Number
Virtual Media Session Mapped	43
Virtual Media Drive Unmapped	44
Traps 45-75 are Unused	45-75
Smart Card Inserted	76
Smart Card Removed	77
Traps 78-79 are Unused	78-79
Aggregated Target Device Status Changed	80

B

Appendix B: Setup Port Pinouts

The SCS 10101 setup port is an 8-pin modular jack. The setup port pinouts and descriptions are provided in the following figure and table.

Figure B.1: Setup Port Pinouts
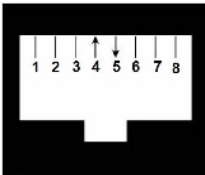
Table B.1: Console/Setup Port Pinout Descriptions

Pin Number	Description	Pin Number	Description
1	No Connection	5	Transmit Data (TXD)
2	No Connection	6	Signal Ground (SG)
3	No Connection	7	No Connection
4	Receive Data (RXD)	8	No Connection

C

Appendix C: Using Avocent Serial IQ Modules

The serial IQ module is a serial-to-VGA converter that allows VT100-capable devices to be viewed from the switch local port, the OBWI, or by using the switch software. All serial data coming from the device is read-only. The data is displayed in a VT100 window, placed into a video buffer, and sent to the switch as though it came from a VGA device. Likewise, keystrokes entered on a keyboard are sent to the attached device as though they were typed on a VT100 terminal.

Serial IQ Module Modes

The following modes can be accessed from the serial IQ module:

* On-Line: This mode enables you to send and receive serial data.

* Configuration: This mode enables you to specify switch communication parameters, the appearance of the Terminal Applications menu, and key combinations for specific actions and macros.

* History: This mode enables you to review serial data.

Configuring the Serial IQ Module

NOTE: The serial IQ module is a DCE device and only supports VT100 terminal emulation.

Pressing <Ctrl-F8> will activate the Configuration screen of the IQ module's Terminal Applications menu, which enables you to configure your serial IQ module.

Within the Terminal Applications menu's Configuration screen, you can modify the following options:

- Baud Rate: This option allows you to specify the serial port communications speed. Available options are 300, 1200, 2400, 9600, 19,200, 34,800, 57,600 or 115,200 bps. The default value is 9600.

- Parity: This option allows you to specify the communications parity for the serial port. Available options are EVEN, ODD or NONE. The default value is NONE.

- Flow Control: This option allows you to specify the type of serial flow control. Available options are NONE, XOn/XOff (software) and RTS/CTS (hardware). The default value is NONE. If you select a bps rate of 115,200, the only available flow control is RTS/CTS (hardware).

- Enter Sends: This option enables you to specify the keys that are transmitted when Enter is pressed. Available options are <CR> (Enter), which moves the cursor to the left side of the screen, or <CR><LF> (Enter-Linefeed), which moves the cursor to the left side of the screen and down one line.

- Received: This option enables you to specify how the module translates a received Enter character. Available options are <CR> (Enter) or <CR><LF> (Enter-Linefeed).

- Background: This option changes the screen's background color. The currently selected color displays in the option line as it is changed. Available colors are Black, Light Grey, Yellow, Green, Teal, Cyan, Blue, Dark Blue, Purple, Pink, Orange, Red, Maroon and Brown. The default color is Black. This value cannot be identical to the Normal Text or Bold Text value.

- Normal Text: This option changes the screen's normal text color. The currently selected color displays in the option line as it is changed. Available colors are Grey, Light Grey, Yellow, Green, Teal, Cyan, Blue, Dark Blue,

Purple, Pink, Orange, Red, Maroon and Brown. The default color is Grey. This value cannot be identical to the Bold Text or Background value.

- Bold Text: This option changes the screen's bold text color. The currently selected color displays in the option line as it is changed. Available colors are White, Yellow, Green, Teal, Cyan, Blue, Dark Blue, Purple, Pink, Orange, Red, Maroon, Brown and Light Grey. The default color is White. This value cannot be identical to the Normal Text or Background value.

- Screen Size: This option allows you to specify the screen's text width size. Available values are widths of 80 columns or 132 columns. The length for both widths is 26 lines.

The following options for the Terminal Application menu's Configuration screen enable you to define the function keys that will perform a selected action. To specify a new function key, press and hold the <Ctrl> key, then press the function key that you want to associate with the action. For example, if you want to change the Configuration (Config) Key Sequences option from <Ctrl-F8> to <Ctrl-F7>, press and hold the <Ctrl> key and then press <F7>.

- Config Key Sequences: This option allows you to define the key combination that makes the Terminal Application menu's Configuration screen appear. The default key sequence is <Ctrl-F8>.

- On-Line Key Sequence: This option allows you to define the key sequence that displays the On-Line mode. The default key sequence is <Ctrl-F10>.

- Help Key Sequence: This option allows you to define the key combination that displays the Help System screen. The default key sequence is <Ctrl-F11>.

- History Key Sequence: This option allows you to define the key combination that enables History mode. The default key sequence is <Ctrl-F9>.

- Clear History Key Sequence: This option allows you to define the key combination that clears the history buffer while in History mode. The default key sequence is <Ctrl-F11>.

- Break Key Sequence: This option allows you to configure the key combination that generates a break condition. The default key sequence is <Alt-B>.

To configure a serial IQ module:

1   Press <Ctrl-F8>. The Configuration Screen will appear.

2   Select a parameter to change. You can navigate the Configuration Screen using the <Up Arrow> and <Down Arrow> keys.

3   Modify the selected value using the <Left Arrow> and <Right Arrow> keys.

4   Repeat steps 2 and 3 to modify additional values.

5   Press <Enter> to save your changes and exit the Configuration Screen.

   -or-

   Press <Escape> to exit the Configuration Screen without saving the changes.

Creating a Serial IQ Module Macro

Pressing the <Page Down> key when the Terminal Applications menu's Configuration screen is displayed will provide access to the Macro Configuration screen. The serial IQ module can be configured with up to 10 macros. Each macro can be up to 128 characters in length.

To create a macro:

1   Select the serial IQ module you wish to configure and press <Ctrl-F8> to activate the Terminal Applications menu's Configuration screen.

2   When the Terminal Applications menu appears, press <Page Down> to view the Macro Configuration screen. The Macro Configuration screen shows the 10 available macros and the associated key sequences, if any, for each.

3   Using the <Up Arrow> and <Down Arrow> keys, scroll to an available macro number and highlight the listed keystroke sequence. Type the new

macro keystroke sequence over the default. Any combination of <Ctrl> or <Alt> and a single key may be used. When you have finished entering the keystroke sequence that will activate the new macro, press the <Down Arrow> key.

4   On the line below the macro keystroke sequence you just entered, type the keystroke sequence that you wish the macro to perform.

5   Repeat steps 3 and 4 to configure additional macros.

6   When finished, press <Enter> to return to the previous screen.

Using History Mode

History mode allows you to examine the contents of the history buffer, which contains the events that have occurred.

The serial IQ module maintains a buffer containing 240 lines minimum, or 10 screens, of output. When the history buffer is full, it will add new lines at the bottom of the buffer and delete the oldest lines at the top of the buffer.

NOTE: The Config Key Sequence, On-Line Key Sequence and Clear History Key Sequence used in the following procedure are the default values. These key combinations can be changed using the Terminal Applications menu.

To use History mode:

1   Press <Ctrl-F9>. The mode will display as History.

2   Press one of the following key combinations to perform the indicated action:

   •   Home: Move to the top of the buffer.

   •   End: Move to the bottom of the buffer.

   •   Page Up: Move up one buffer page.

   •   Page Down: Move down one buffer page.

   •   Up Arrow: Move up one buffer line.

   •   Down Arrow: Move down one buffer line.

- <Ctrl-F8>: Enters Configuration mode. The Configuration screen will appear.

- <Ctrl-F9>: While in Configuration mode, returns to the previous screen with History mode enabled.

- <Ctrl-F10>: While in Configuration mode, returns to the previous screen with On-Line mode enabled.

- <Ctrl-F11>: Clears the history buffer. If you choose this option, a warning screen will appear. Press <Enter> to delete the history buffer or <Escape> to cancel the action. The previous screen will reappear.

3   When finished, press <Ctrl-F10> to exit History mode and return to On-Line mode.

Serial IQ Module Pinouts

The following table lists the pinouts for the serial IQ module.

Table C.1: Serial IQ Module Pinouts

DB9-F Pin	Host Signal Name Description	Signal Flow	SRL Signal Name Description
1	DCD - Data Carrier Detect	Out of SRL	DTR - Data Terminal Ready
2	RXD - Receive Data	Out of SRL	TXD - Transmit Data
3	TXD - Transmit Data	In to SRL	RXD - Receive Data
4	DTR - Data Terminal Ready	In to SRL	DSR - Data Set Ready
5	GND - Signal Ground	N/A	GND - Signal Ground
6	DSR - Data Set Ready	Out of SRL	DTR - Data Terminal Ready
7	RTS - Request to Send	In to SRL	CTS - Clear to Send
8	CTS - Clear to Send	Out of SRL	RTS - Request to Send
9	N/C - Not Connected	N/A	N/C - Not Connected

D

Appendix D: Sun Advanced Key Emulation

Certain keys on a standard Type 5 (US) Sun keyboard can be emulated by key press sequences on the local port USB keyboard. To enable Sun Advanced Key Emulation mode and use these keys, press and hold <Ctrl+Shift+Alt> and then press the <Scroll Lock> key. The Scroll Lock LED blinks. Use the indicated keys in the following table as you would use the advanced keys on a Sun keyboard. For example: For <Stop+A>, press and hold <Ctrl+Shift+Alt> and press <Scroll Lock>, then <Fl+A>.

These key combinations will work with the Dell USB, USB2, and USB2+CAC SIPs and Avocent USB, USB2, and VMC IQ modules. With the exception of <F12>, these key combinations are not recognized by Microsoft Windows. Using <F12> performs a Windows key press. When finished, press and hold <Ctrl+Shift+Alt> and then press the <Scroll Lock> key to toggle Sun Advanced Key Emulation mode off.

Table D.1: Sun Key Emulation

Compose	Application(1)
Compose	keypad
Power	F11
Open	F7
Help	Num Lock

Props	F3
Front	F5
Stop	F1
Again	F2
Undo	F4
Cut	F10
Copy	F6
Paste	F8
Find	F9
Mute	keypad /
Vol.+	keypad +
Vol.-	keypad -
Command (left)(2)	F12
Command (left)(2)	Win (GUI) left(1)
Command (right)(2)	Win (GUI) right(1)

ENDNOTES:

(1) Windows 95 104-key keyboard.

(2) The Command key is the Sun Meta (diamond) key.

E

Appendix E: UTP Cabling

This appendix discusses various aspects of connection media. The SCS system utilizes UTP cabling. The performance of the system depends on high quality connections. Poor quality or poorly installed or maintained cabling can diminish SCS system performance.

NOTE: This appendix is for information purposes only. Please consult with your local code officials and/or cabling consultants prior to any installation.

UTP Copper Cabling

The following are basic definitions for the three types of UTP cabling that the SCS supports.

- CAT 5 (4-pair) high performance cable consists of twisted pair conductors, used primarily for data transmission. The twisting of the pairs gives this cable some immunity from the infiltration of unwanted interference. CAT 5 cable is generally used for networks running at 10 or 100 Mbps.

- CAT 5E (enhanced) cable has the same characteristics as CAT 5, but is manufactured to somewhat more stringent standards.

- CAT 6 cable is manufactured to tighter requirements than CAT 5E cable. CAT 6 has higher measured frequency ranges and significantly better performance requirements than CAT 5E cable at the same frequencies.

Wiring Standards

There are two supported wiring standards for 8-conductor (4-pair) RJ-45 terminated UTP cable: EIA/TIA 568A and B. These standards apply to

installations utilizing UTP cable specifications. The SCS system supports either of these wiring standards. The following table describes the standards for each pin.

Table E.1: UTP wiring standards

Pin	EIA/TIA 568A	EIA/TIA 568B
1	white/green	white/orange
2	green	orange
3	white/orange	white/green
4	blue	blue
5	white/blue	white/blue
6	orange	green
7	white/brown	white/brown
8	brown	brown

Cabling Installation, Maintenance, and Safety Tips

The following is a list of important safety considerations that should be reviewed prior to installing or maintaining your cables:

- Keep all UTP runs to a maximum of 30 meters each.

- Maintain the twists of the pairs all the way to the point of termination, or no more than one-half inch untwisted. Do not skin off more than one inch of the jacket while terminating.

- If bending the cable is necessary, make it gradual with no bend sharper than a one inch radius. Allowing the cable to be sharply bent or kinked can permanently damage the cable's interior.

- Dress the cables neatly with cable ties, using low to moderate pressure. Do not over tighten the ties.

- Cross-connect cables where necessary, using rated punch blocks, patch panels, and components. Do not splice or bridge the cable at any point.

- Keep the UTP cable as far away as possible from potential sources of EMI, such as electrical cables, transformers, and light fixtures. Do not tie the cables to electrical conduits or lay the cables on electrical fixtures.

- Always test every installed segment with a cable tester. Toning alone is not an acceptable test.

- Always install jacks so as to prevent dust and other contaminants from settling on the contacts. The contacts of the jack should face up on the flush mounted plates, or left/right/down on surface mount boxes.

- Always leave extra slack on the cables, neatly coiled in the ceiling or nearest concealed location. Leave at least five feet at the work outlet side and 15 feet at the patch panel side.

- Choose either 568A or 568B wiring standard before beginning. Wire all jacks and patch panels for the same wiring scheme. Do not mix 568A and 568B wiring in the same installation.

- Always obey all local and national fire and building codes. Be sure to firestop all the cables that penetrate a firewall. Use plenum-rated cable where it is required.

F

Appendix F: Technical Specifications

Table F.1: SCS Technical Specifications

Number of Ports	1081AD: 8 AHI/ARI
	2161AD: 16 AHI/ARI
Type	Dell PS/2, USB, USB2, and USB2+CAC SIPs
	Avocent PS/2, PS2M, USB, Sun, USB2, and VMC modules
Connectors	8-pin modular (RJ-45)
Sync Types	Separate horizontal and vertical
Input Video Resolution	Standard 640 x 480 @ 60 Hz 800 x 600 @ 75 Hz 960 x 700 @ 75 Hz 1024 x 768 @ 75 Hz 1280 x 1024 @ 75 Hz 1600 x 1200 @ 60 Hz Widescreen 800 x 500 @ 60 Hz 1024 x 640 @ 60 Hz 1280 x 800 @ 60 Hz 1440 x 900 @ 60 Hz 1680 x 1050 @ 60 Hz

Target Resolutions	Standard
	1024 x 768 @ 60 Hz (preferred)
	1280 x 1024 @ 60 Hz (preferred)
	1600 x 1200 @ 60 Hz (preferred)
	Widescreen
	1280 x 800 @ 60 Hz (preferred)
	1680 x 1050 @ 60 Hz (preferred)
Supported Cabling	4-pair UTP, 30 meters maximum length

Dimensions

Form Factor	1U or 0U rack mount
Dimensions	1.70 x 17.00 x 9.42 inches (Height x Width x Depth)
	(4.32 x 43.18 x 23.93 cm)
Weight (without cables)	1081AD: 5.98 lb (2.71 kg); 2161AD: 6.16 lb (2.79 kg)

10101 Setup Port

Number	1
Protocol	RS-232 serial
Connector	8-pin modular (RJ-45)

Local Port

	8 Port	16 Port
Number/Type	1 VGA - HDD15	2 VGA - HDD15
	4 USB	8 USB

Network Connection

Number	2
Protocol	10/100 Ethernet
Connector	8-pin modular (RJ-45)
USB Port	
Number	4
Protocol	USB 2.0
Power Specifications	
Connectors	1081AD: 1 IEC C14 2161AD: 2 IEC C14
Type	Internal
Power	18W
Heat Dissipation	47 BTU/hr
AC Input Range	100 - 240 VAC
AC Frequency	50/60 Hz auto-sensing
AC Input Current Rating	0.6A
AC Input Power (Maximum)	20 W
Ambient Atmospheric Condition Ratings	

Temperature	Operating: 32 to 122 degrees Fahrenheit (0 to 50 degrees Celsius)
	Non-operating: -4 to 158 degrees Fahrenheit (-20 to 70 degrees Celsius)
Humidity	Operating: 20% to 80 % relative humidity (non-condensing)
	Non-operating: 5% to 95% relative humidity, 38.7 degrees Celsius maximum wet bulb temperature
Safety and EMC Standard Approvals and Markings	UL / cUL, CE - EU, N (Nemko), GOST, C-Tick, NOM / NYCE, KCC, SASO, Nemko GS, IRAM, FCC, ICES, VCCI, SoNCAP, SABS, Bellis, Koncar, INSM, STZ, KUCAS 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 are printed on the label applied to this product.

G

Appendix G: 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.