Hewlett Packard Enterprise

HPE G4 KVM IP Console Switch Installation and User Guide

Abstract

This document is for the person who installs, administers, and troubleshoots servers and storage systems. Hewlett Packard Enterprise assumes you are qualified in the servicing of computer equipment and trained in recognizing hazards in products with hazardous energy levels.

Part Number: P03253-001
April 2018
Edition: 1

Contents

Before You Begin

Overview

This document provides installation instructions and configuration instructions to qualified personnel for installing a Hewlett Packard Enterprise (HPE) Keyboard, Video, and Mouse (KVM) Console Switch into a datacenter rack. Please read all instructions before operating the equipment and save this manual for future reference.

Important safety information

See the complete regulatory compliance notices in *Safety and Compliance Information for Server, Storage, Power, Networking, and Rack Products* on the Hewlett Packard Enterprise website (http://www.hpe.com/support/Safety-Compliance-EnterpriseProducts). In addition, follow the safety precautions that are specific to this device.

WARNING: To reduce the risk of electric shock or damage to your equipment:

- Do not disable the power grounding plug. The grounding plug is an important safety feature.
- Plug the power cord into a grounded (earthed) outlet that is easily accessible at all times.

RACK MOUNT SAFETY CONSIDERATIONS: If mounting this product in an equipment rack, the following considerations shall apply for safe installation and use of this product:

- Elevated ambient temperature: If installed in a closed rack assembly, the operation temperature of the rack environment may be greater than room ambient. Use care not to exceed the rated maximum operating temperature for this product.
- Reduced air flow: Installation of the equipment in a rack should be such that the amount of air flow required for safe operation of the equipment is not compromised.
- Mechanical loading: Mounting of the equipment in the rack should be such that a hazardous condition is not achieved due to uneven mechanical loading.
- Circuit overloading: Consideration should be given to the connection of the equipment to the supply circuit and the effect that overloading of circuits might have on overcurrent protection and supply wiring. Consider equipment nameplate ratings for maximum current.
- Reliable earthing: Reliable earthing of rack mounted equipment should be maintained. Pay particular attention to supply connections other than direct connections to the branch circuit (for example, use of power strips).
- Product should not be mounted with the rear panel facing in the downward position. Product maybe rack mounted in a 1U configuration.
- Disconnect the power from the product by unplugging the power 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 the product cover.

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

Required tools

The following tools are required for some procedures:

- Phillips screwdriver
- Cage nut insertion tool (included with your original rack hardware kit)

Required items not included

- Interface adapters - one interface adapter is needed for each server or device.
  - USB connection
  - Serial connection

    - HPE BladeSystem connection
- UTP CAT 5 cable or higher

Product overview

The HPE KVM Console Switch is a keyboard, video and mouse console switch that provides flexible, centralized local access to datacenter servers.

Features

The HPE KVM provides the following features:

- **Reduces KVM cable volume** – utilizes the interface adapter and single, industry-standard Unshielded Twisted Pair (UTP) cabling while providing greater airflow
- **Provides keep alive functionality** – supports interface adapters that are powered directly from the target device providing functionality when the console switch is not powered
- **Direct connectivity to devices** – PS/2 and USB interface adapters allow connection to devices
- **Flexibility to add capacity to the data center** – 8 or 16 target device ports which can be utilized to attach additional console switches via the interface adapters
- **Virtual media and smart card support** – reader can be connected directly to the USB ports
- **Two tier expansion** – tier one additional console switch from each target device port on the primary console switch allowing attachment of up to 256 servers in one system
- **Local management user interfaces** – tailor the console switch to specific applications via the local console User Interface (UI), or On-Screen Display (OSD).
- **Remote access support** – single user can remotely manage the KVM On-Board Web Interface (OBWI) -
- **Local video scaling** – digitizes a video signal with a maximum pixel resolution of up to 1600 x 1200 or 1680 x 1050 (wide window)

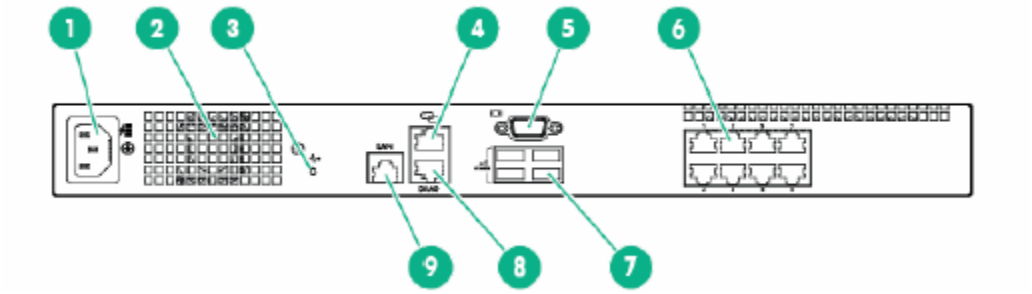
KVM console switch models

Details of the HPE KVM models that are covered within this document.

KVM Models	Description	Details
Q1P54A	HPE 1X1X8 G4 KVM IP CNSL SWITCH	Single console management via one local interface with eight digital output connections.
Q1P55A	HPE 1X2X16 G4 KVM IP CNSL SWITCH	Single console management via two local interfaces with sixteen digital output connections.

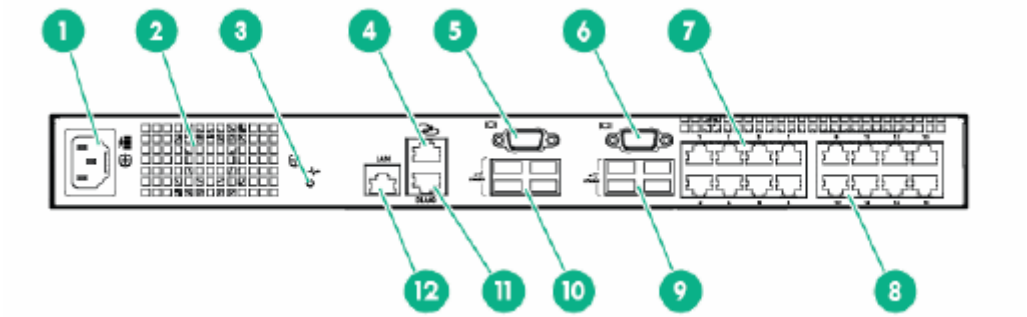
Console switch components

Q1P54A – HPE 1X1X8 G4 KVM IP CNSL SWITCH



Item	Description	Item	Description
1	Power cord connector	6	Server connection ports 1-8
2	Fan	7	Console port USB ports
3	System health LED	8	DIAG port
4	RJ-45 tiering port	9	LAN port
5	Console port video connector		

Q1P55A – HPE 1X1X16 G4 KVM IP CNSL SWITCH – Q1P55A



Item	Description	Item	Description
1	Power cord connector	7	Server connection ports 1-8
2	Fan	8	Server connection ports 9-16
3	System health LED	9	Console port USB ports
4	RJ-45 tiering port	10	Console port USB ports
5	Console port A video connector	11	DIAG port
6	Console port B video connector	12	LAN port

Interface Adapter (IA) models

Details of the HPE IA models that are covered within this document.

KVM Models	Description	Details
Q5T66A	HPE KVM SFF USB Adapter	Small form factor USB interface adapter
Q5T67A	HPE 8 PK KVM SFF USB Adapter	Small form factor USB interface adapter - 8 pack

Installing the KVM

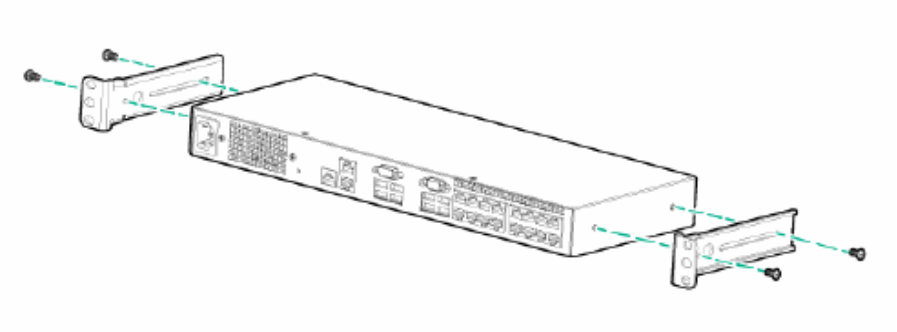
WARNING: For safe use, do not mount this product with the rear panel, which is the side of the console switch with I/O connectors and the AC power inlet, facing downward (facing the floor).

Before installing the KVM Console Switch into the rack, connect the KVM Console Switch to a power source, using the power cords provided, and power on the unit. The system health LED illuminates after a few seconds. If the system health LED does not illuminate, be sure that the power is on, the power cord is connected, and the power source is valid.

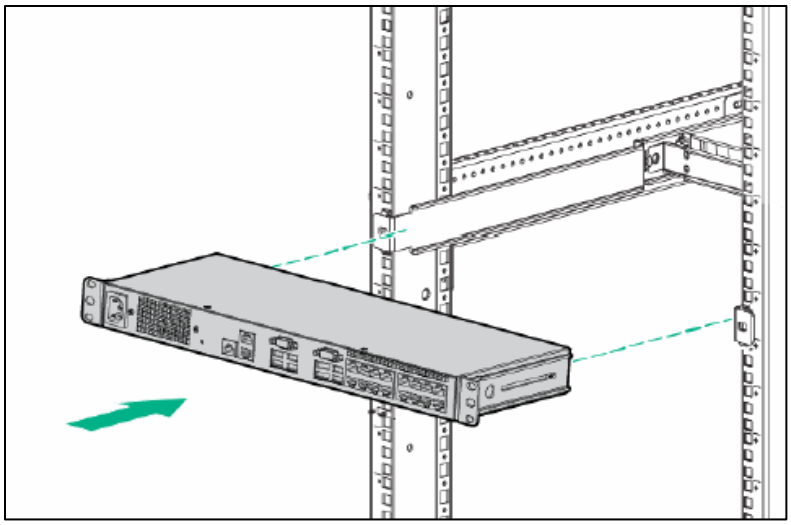
The following mounting installations are supported: standard-mount, cantilever-mount, and side-mount.

Performing a standard-mount installation

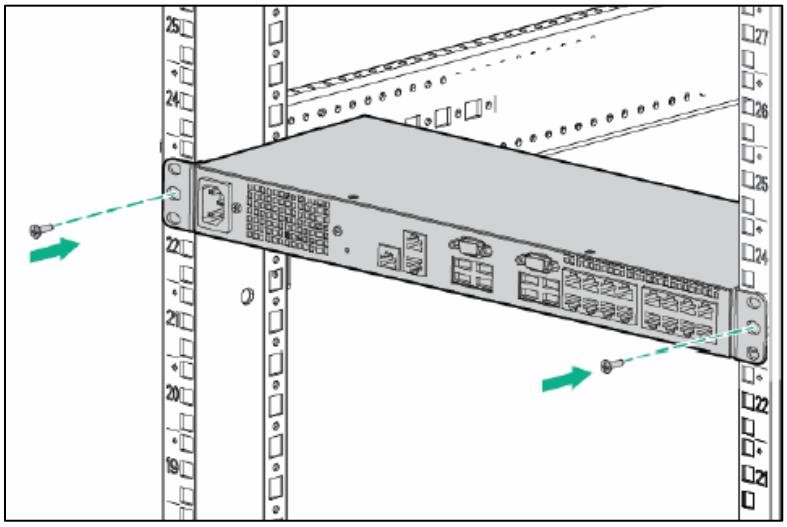
1. Remove the four screws, two on each side, from the console switch.
2. Attach the short 1U brackets to the console switch using the four screws you removed.



3. If not already installed, install a cage nut behind each rear rail.
4. Slide the console switch into the rear of the 1U product.

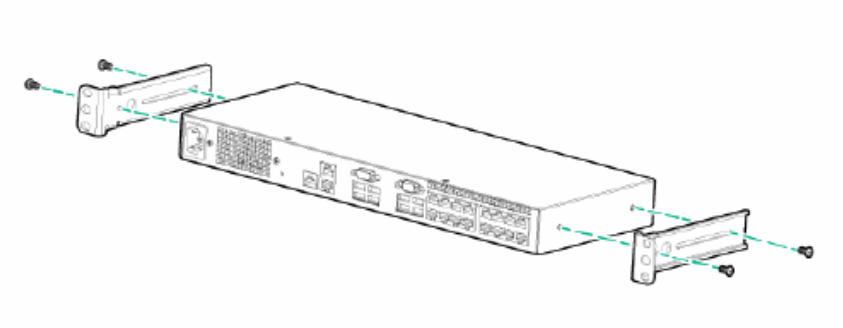


5. Secure the console switch to the rails using two M-6 screws, one on each side.

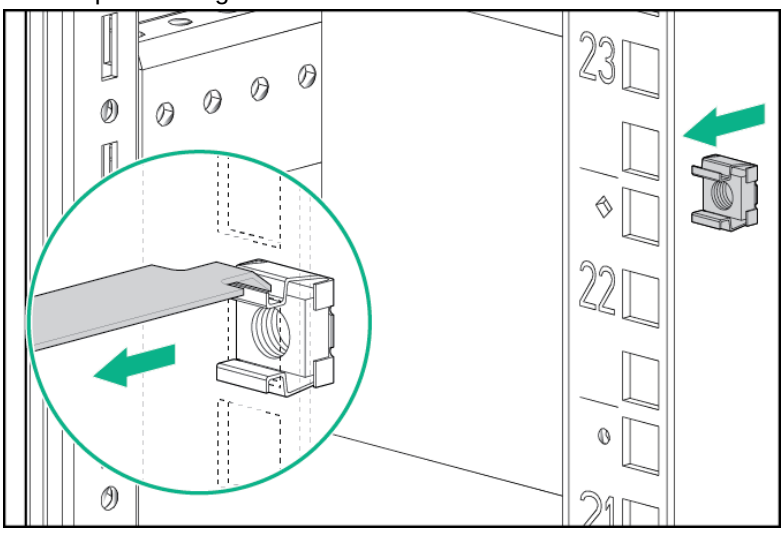


Performing a cantilever-mount installation

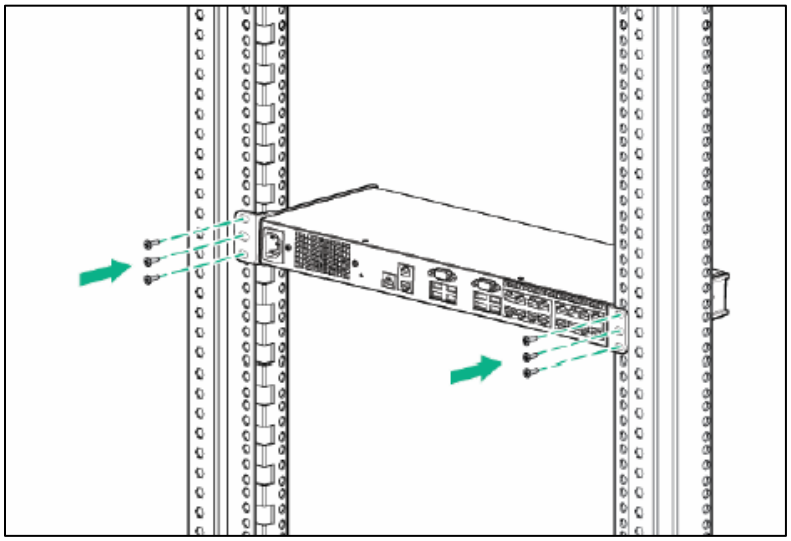
1. Remove the four screws, two on each side, from the console switch.
2. Attach the short 1U brackets to the console switch.



3. Install up to six cage nuts.

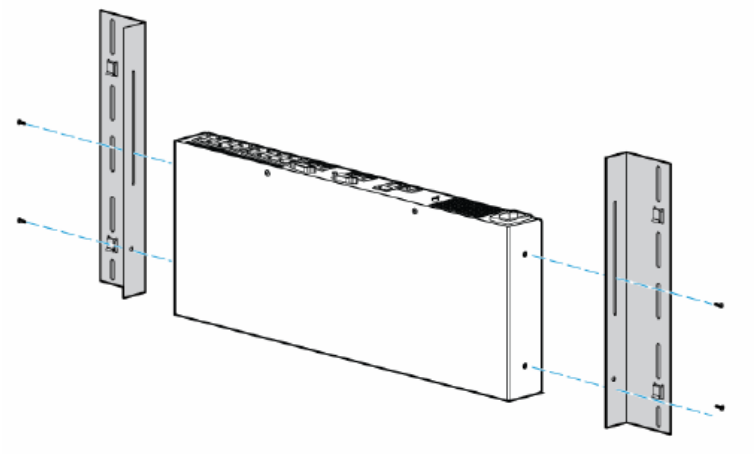


4. Secure the console switch to the rails using the appropriate number of M-6 screws.

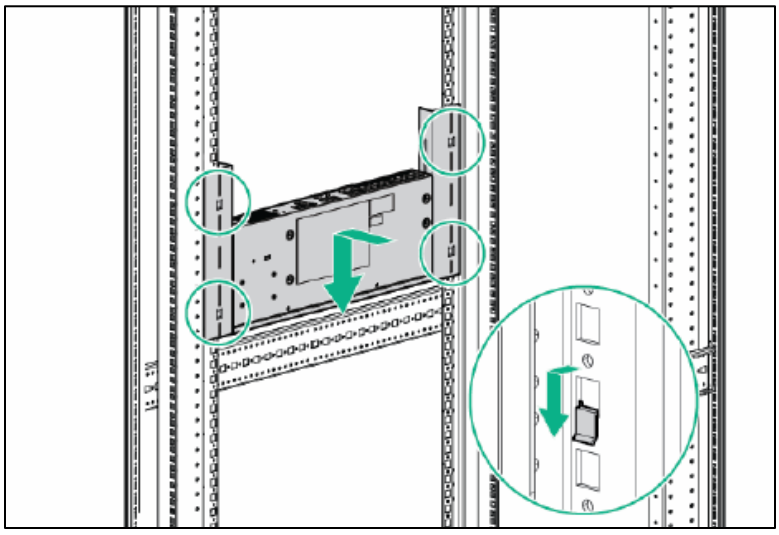


Performing a side-mount installation

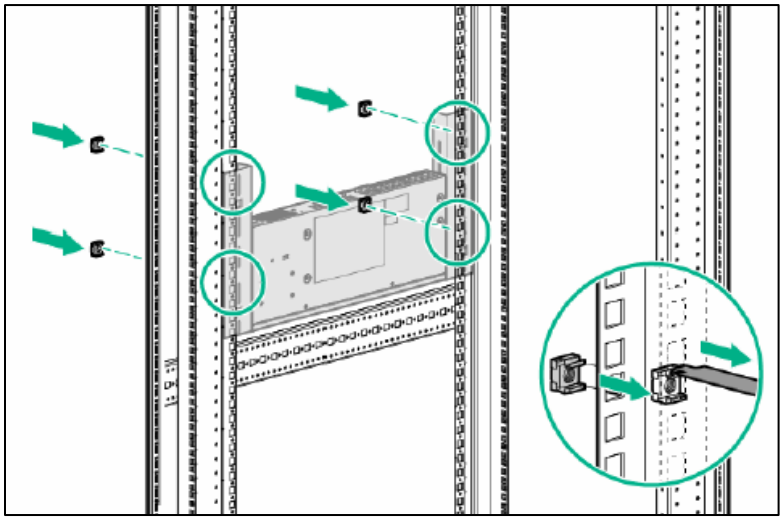
1. Remove the four screws, two on each side, from the console switch.
2. Attach the side-mounting brackets to the console switch using the four screws you removed.



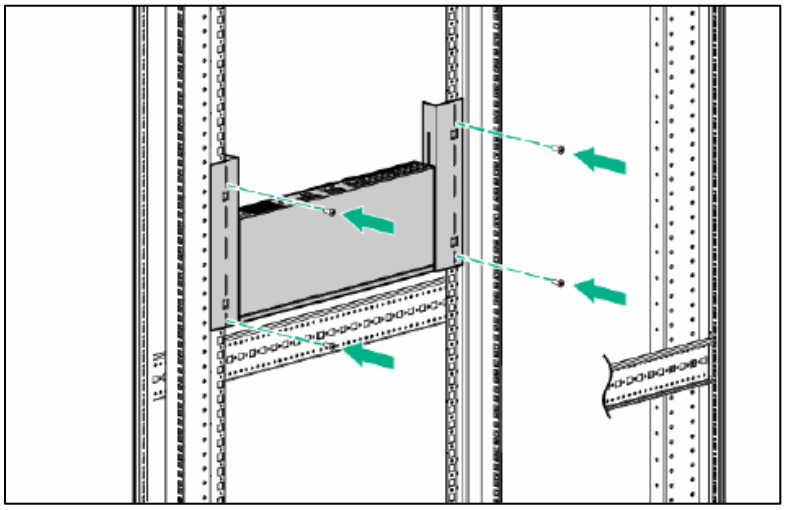
3. Slide the side-mounting bracket tabs into the U locations on each side of the rack.



4. Install four cage nuts into the side-mounting bracket U locations.



5. Secure the console switch to the rails, using four M-6 screws, two on each side.
   On some racks enable you to use four sheet metal screws in place of M-6 screws and cage nuts.



Installing the interface adapter

Integrating the IA

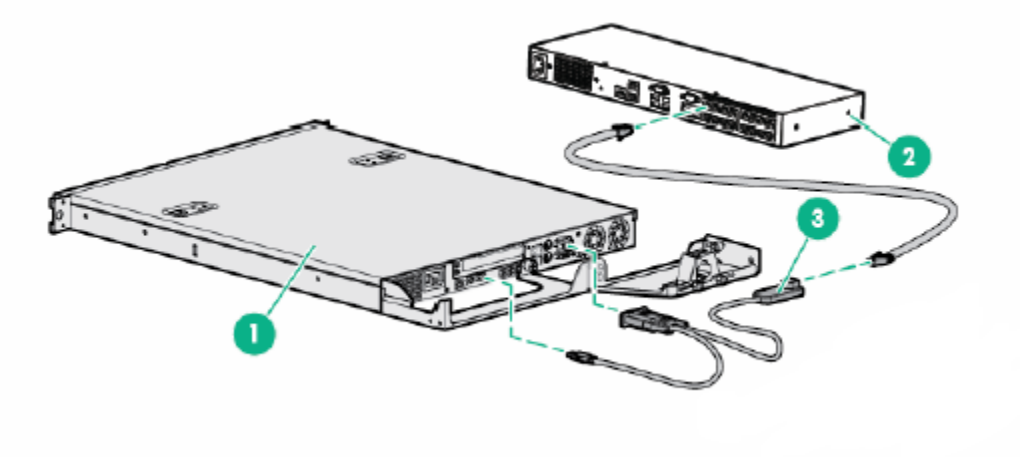
An IA (sold separately) is required for the KVM Console Switch system to function properly. An IA connects to the KVM Console Switch using UTP CAT5 or higher cables. The IA connects to the keyboard, video, and mouse interfaces of the server.

Connecting the IA

To connect the IA:

1. Connect a UTP CAT5 cable or higher to the server connection port on the KVM Console Switch.
2. Connect the other end of the cable to the RJ-45 connector on the IA.
3. Connect the IA to the appropriate connectors on the server.
4. Repeat these steps to connect additional servers to this system, if needed.

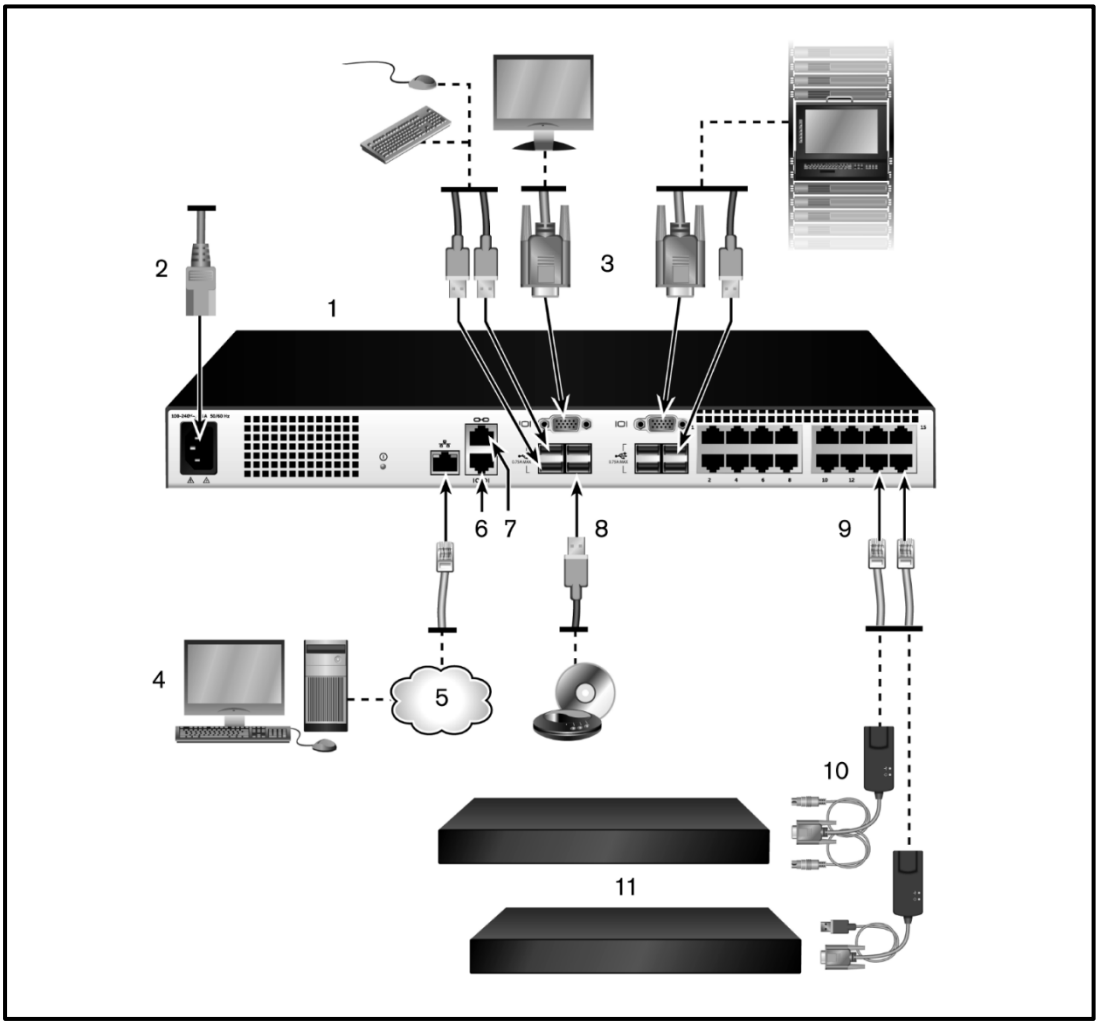
The following figure shows one possible configuration for the KVM Console Switch system with an IA.



Item	Description
1	Server
2	Console switch
3	USB IA

Basic configuration of the console switch hardware

The figure below illustrates an example of the basic configuration utilizing the 16 port KVM Console Switch (Q1P55A).



Item	Description	Item	Description
1	Console switch (16-port model shown)	7	Tiering
2	Power cord	8	Virtual media or Keyboard/Mouse - USB connections
3	Analog users (2)	9	Target device ports
4	Digital user	10	Interface adapters
5	LAN/network	11	Servers/target devices
6	DIAG console port		

NOTE: The KVM console switch supports connecting to another KVM appliance via the tiering port of the other HPE KVM.

Network installation

The console switch uses TCP/IP for communication over Ethernet. For the best system performance, use a dedicated, switched 10/100/1000 Ethernet network.

Terminal software, OSD interface, or the OBWI can be used to manage the console switch system. The OBWI manages a single console switch and its connections. KVM and serial switching tasks can be performed using the OBWI or DSView management software.

NOTE: Ensure that every console switch has been upgraded to the most recent version of firmware.

Setting up your network

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

Keyboards

A USB keyboard and mouse can be connected to the local ports of the KVM Console Switch. The console switch also supports the use of multiple keyboards and multiple mice. The use of more than one input device simultaneously, however, can produce unpredictable results.

Quick setup guide:

1. Unpack the KVM Console Switch and verify that all components are present and in good condition.
2. Install the console switch hardware and connect an interface adapter to each target device or tiered console switch. Connect each interface adapter to the console switch with CAT5 cabling and connect the keyboard, monitor and mouse connectors to the ports of the console switch.
3. Connect the local port peripherals to the appropriate ports on the back panel of the console switch and set up the network configuration. The IP address can be set here. Using a static IP address is recommended.
4. For the local port connection, input all device names using the OSD interface or the OBWI.

To connect and turn on your console switch:

1. Connect your VGA monitor and USB keyboard and mouse cables to the appropriately labeled ports.
2. Connect one end of a UTP cable to an available numbered port. Connect the other end to an RJ45 connector of an interface adapter.
3. Connect an interface adapter to the appropriate port on the back of a device. Repeat steps 2 and 3 for all devices you want to connect.
4. Connect a user-supplied UTP cable from the Ethernet network to the LAN port on the back of the console switch. Network users access the console switch through this port.
5. Connect power to the console switch.
6. (Optional) Connect the virtual media or smart card readers to any of the USB ports on the console switch.

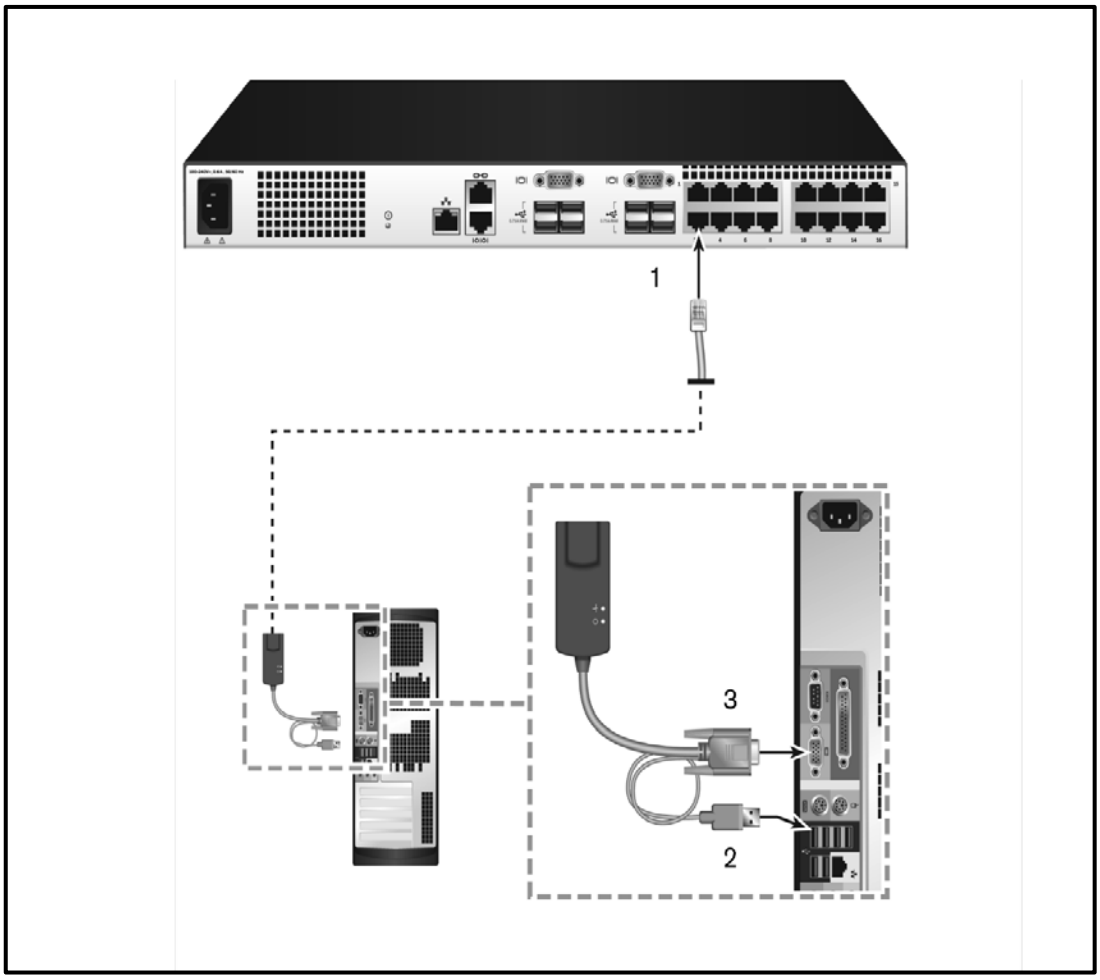
NOTE: For all virtual media sessions, you must use a virtual media capable interface adapter.

Attaching a server to a KVM

To connect an interface adapter to each device:
NOTE: When tiering devices, the console switch closest to the actual user is the primary KVM Console Switch.

1. Locate the interface adapter for your KVM Console Switch.
2. To the RJ45 connector on the interface adapter, attach one end of the CAT5 cable to run from your IA to the console switch.
3. Connect the other end of the CAT5 cable to the desired target port on the back of your console switch.
4. Repeat steps 2-4 for all devices you wish to attach.

NOTE: Turn off the console switch before servicing. Always disconnect the power cord from the power source.



Item	Description
1	CAT5
2	USB Connection
3	VGA Connection

Adding a tiered console switch

You can tier up to two levels of console switches, enabling you connect a console switch to up to 256 devices. In a tiered system, each target device port on the main console switch connects to the ACI port on each tiered console switch. Each tiered console switch can then be connected to a device with an interface adapter.

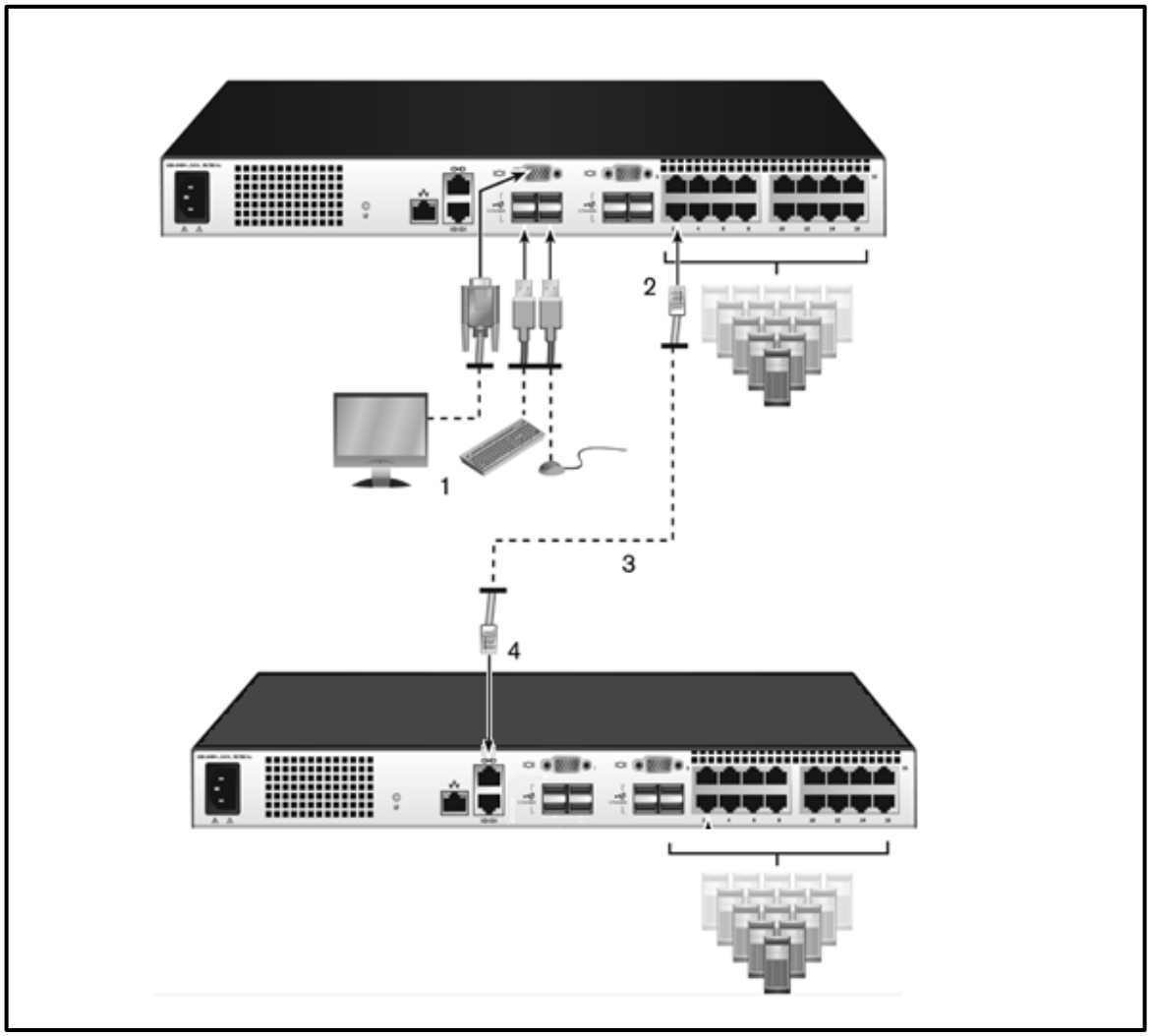
To tier multiple console switches:

1. Attach one end of a UTP cable to a target device port on the console switch.
2. Connect the other end of the UTP cable to the target device port on the back of your tiered console switch.
3. Connect the target devices to your tiered console switch.

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

NOTE: The system automatically “merges” the two console switches. All console switches connected to the tiered console switch are displayed on the main switch list in the local UI.

NOTE: The console switch supports one tiered console switch per device port of the main console switch. You cannot attach a console switch to the tiered console switch.



Item	Description
1	Local User
2	Target Port
3	UTP Connection
4	Tiering Port

Configuring the KVM Console Switch

Once all physical connections have been made, you need to configure the console switch for use in the overall system. This can be accomplished by using the serial interface, OBWI, OSD interface or the DSView management software.

Setting up the built-in web server

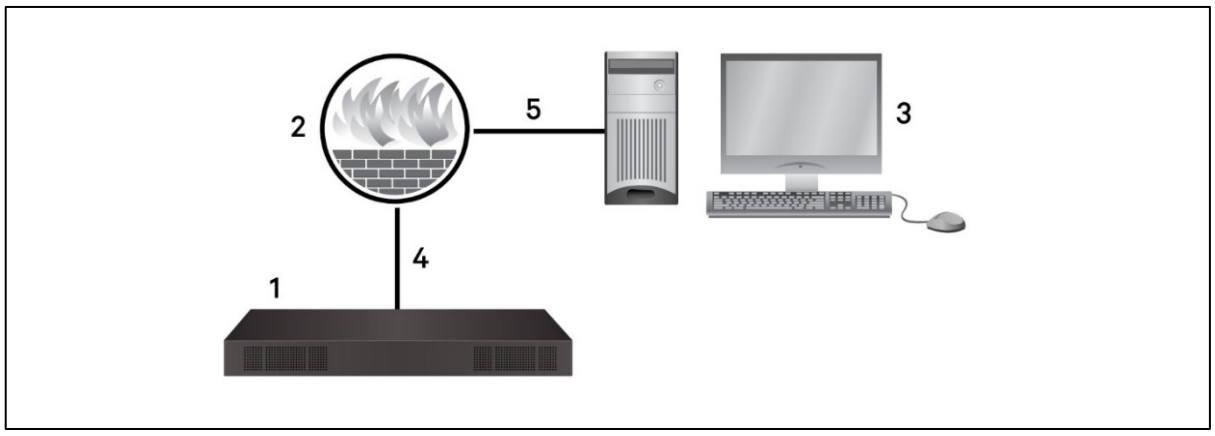
Before using the OBWI to access the console switch, the IP address must be specified using the DIAG port on the back panel of the console switch or through the local user interface or OSD.

Connecting to the OBWI through a firewall

For console switch installations that use the OBWI for access, the following ports must be opened in a firewall if outside access is desired. See the table below.

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

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



Item	Description
1	Console switch
2	Firewall
3	Computer
4	Firewall forwards HTTP requests and KVM traffic to the switch
5	Connection to an IP address outside the firewall

To configure the firewall:

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

NOTE: Ports 80 and 443 can be reconfigured by an administrator. You must reboot for a port change to take effect.

Verifying power status

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

Adjusting mouse settings on target devices

Before a computer connected to the console switch can be used for remote user control, you must either enable Module Sync (see Mouse Settings for additional information) or set the target 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 Console 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: 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 can 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.

Local OSD user interface

Main dialog box functions

To access the OSD interface Main dialog box:

1. Press Print Screen to launch the OSD interface. The Main dialog box will appear.
   -or-
   Press the **Alt**, **Shift**, or **Ctrl** key twice within one second to launch the OSD. (Use this key sequence where you see **Print Scrn**.)

NOTE: If the OSD password has been enabled, you are prompted to enter a password before you can launch the OSD interface.

Viewing and selecting ports and devices

Use the OSD *Main* dialog box to view, configure and control target devices in the console switch system. View your devices by name, port or by the unique EID number embedded in each interface adapter.

In the following figure, the Port column indicates the target device port to which a device is connected. If you tier a console switch from the main console switch, creating another tier, the target device port on the console switch is listed first and is followed by the console switch port to which the device is connected. Figure below illustrates the OSD interface main dialog box.

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 interface adapters
Disconnect	Disconnect the KVM session
Setup	Access the Setup dialog box and configure the OSD interface
Commands	Access the Commands dialog box
VMedia	Control virtual media connection

Viewing console 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.

Symbol	Description
	(Green circle) device connected, turned on and the interface adapter is online.
	Connected device is turned off or is not operating properly and the interface adapter is offline.
	Connected console switch is online.

Symbol	Description
	Connected console switch is offline or not operating properly.
	(Yellow circle) The designated interface adapter is being upgraded. When this symbol displays, do not cycle power to the console switch or connected devices and do not disconnect the interface adapter. Doing so can render the module permanently inoperable and require the interface adapter to be returned to the factory for repair.
	(Green letter) interface adapter is being accessed by the indicated user channel.
	(Black letter) interface adapter is blocked by the indicated user channel.
	(Red letter) Smart card support is available.

Selecting target devices

From the Main dialog box, select the specific target device. When you select a target device, the console switch reconfigures the KVM to the settings for that target device.

To select a target device:

- Double-click the device name, EID or port. Highlight a server using the up or down arrow keys, and then press the **Enter** key.

  -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 you 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 target devices using a hotkey sequence. You can soft switch to a device by pressing Print Screen, entering the first few characters of the target device name or number. If you have set a Screen Delay Time for the OSD interface and you press the key sequences before that time has elapsed, the OSD interface is not 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 OSD interface

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

Keystroke	Function
Print Screen, Ctrl + Ctrl, Shift + Shift and/or Alt + Alt	OSD interface activation sequence. By default, Print Screen and Ctrl + Ctrl are set as the OSD interface activation options. Shift + Shift and Alt + Alt must be set within the OSD interface before use.
F1	Opens the Help window for the current dialog box.
Esc	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 OSD interface and displays a status flag if status flags are enabled. 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 console switch operation in the Main dialog box and exits the OSD 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 the previous selection.
Print Screen, Pause	Immediately turns on Screen Saver mode and prevents access to that specific console, if it is password protected.
Up or Down Arrows	Moves the cursor from line to line in lists.
Right or Left Arrows	Moves the cursor between columns. When editing a text box, these keys move the cursor within the column.
Page Up or Page Down	Pages up and down through names, ports and Help pages.
Home or 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 console switch using a USB port.

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 OSD interface and open the Main window.
2. Connect to the target device with which you want to establish a virtual media session.
3. Use the arrow keys to highlight the target device name and press Enter.
4. Press Print Screen to start the OSD 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 is 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*.

Configuring the Setup dialog box

You can configure the KVM Console Switch and manage tasks for your servers from the Setup dialog box within the OSD. Select the *Names* button when initially setting up the console switch to identify target devices by unique names. Select the other setup features to manage routine tasks for your target devices from the OSD interface menu. The following table lists the functions accessed using each of the buttons in the Setup dialog box.

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

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

Changing the display behavior

From the Menu dialog box, the display order of servers, KVM Console Switch connection mode, and a time to delay display of the OSD after pressing the **Print Scrn** key can be changed. The display order setting alters how servers display in several screens, including the Main, Devices, and Broadcast dialog boxes.

To access the OSD interface:

1. Select *Setup* - *Menu* in the *Main* dialog box to activate the OSD interface. The Menu dialog box appears.

To choose the display order of target devices:

1. Select *Name* to display target devices alphabetically by name.
   -or-
   Select *EID* to display target devices numerically by EID number.
   -or-
   Select *Port* to display target devices numerically by port number.
2. Click *OK* to save settings.
   -or-
   Click X to exit or press the Esc key to exit without saving settings.

To change how the OSD is invoked:

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

2. Click *OK*.

To set a screen delay time for the OSD interface:

Setting a time to delay the display of the OSD enables you to complete a soft switch without displaying the OSD interface. It is strongly recommended to leave the number of seconds (0-9) the OSD is delayed to the default (0).

1. From the Main dialog box, enter the number of seconds (0-9) to delay the OSD interface display after you press Print Screen. Enter 0 to launch the OSD interface with no delay.
2. Click *OK* to save settings.
   -or-
   Click X to exit, or press the Esc key to exit without saving settings.

Controlling the status flag

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

To access the OSD interface flag dialog box:

1. Activate the OSD 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 is displayed. The following interface *Status Flags* are available:
   - Flag description
   - Flag type by name
   - Flag type by EID number
   - Flag indicating that you have been disconnected from all systems
2. Select *Displayed* to activate the flag display. After a switch, the flag remains on the window until you switch to another device. Selecting *Timed* causes the flag to display for five seconds when a switch is made and then disappears.
3. Select a flag color under Display Color. The following flag colors are available:
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 window.
   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 console switch firmware causes incorrect keyboard mapping.

By default, the console 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 interface adapter. Issues can 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 console switch when they are turned on or rebooted and the new code is stored in the interface adapter.

NOTE: If an interface adapter is moved to a different device, the keyboard country code needs to be reset.

Assigning device types

To access the OSD interface devices dialog box:

1. Activate the OSD interface and click *Setup - Devices* to open the *Devices* dialog box.

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

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

For example, if a console switch is connected to port 6 of the console switch, each device connected to it would be numbered sequentially. The device using console switch port 6 and console switch port 1 is 06-01. The device using console switch port 6 and console switch port 2 is 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 console 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 interface adapter, so even if you move the interface adapter/device to another port, the name and configuration is recognized by the console switch.

NOTE: When it is initially connected, a target device does not appear in the Names list until it is turned on. Once an initial connection is made, it appears in the Names list even when turned off.

To access the OSD interface *Names* dialog box, activate the OSD interface and click *Setup - Names*.

NOTE: If new interface adapters are discovered by the console switch, the on-window list is automatically updated. The mouse cursor changes into an hourglass during the update. No mouse or keyboard input is 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 can 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 OSD 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 causes the console switch to reboot.
4. Click *OK* in the *Devices* dialog box to save settings.

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

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

Commands dialog box functions

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

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

To access the OSD commands dialog box:

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

Selecting target 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 OSD interface and click *Setup - Scan* to open the *Scan* dialog box.
2. The dialog box contains a listing of all devices attached to your console 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.

Activating scan mode

To start the scan mode:

1. Activate the OSD interface and click *Commands*.
2. In the Commands dialog box, select *Scan Enable* in the *Commands* dialog box.

3. After scanning begins, click *X* to close the *Commands* dialog box.

Deactivating scan mode

To cancel scan mode:

1. If the OSD interface is open, select a target device.
   -or-
   If the OSD interface is not open, move the mouse or press any key on the keyboard. Scanning stops at the currently selected target device.
   -or-
   From the *Commands* dialog box, clear the Scan Enable checkbox. Any active connections on the local port are disconnected.

Viewing and disconnecting user connections

You can view and disconnect users through the *User Status* dialog box. The username (U) and server (S) is always 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 are blank.

To view current user connections, activate the OSD 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.
2. In the Disconnect dialog box, 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 OSD interface enables you to display the version number of the console switch firmware and any target devices connected to the console switch, as well as upgrade your firmware for optimum performance.

To display version information and upgrade firmware:

1. Activate the OSD interface and click *Commands - Display Versions*. The top half of the box lists the subsystem version in the console 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 are 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 appears.
4. Click the *Upgrade* button.

NOTE: The console switch reboots when the upgrade is complete.

To upgrade individual interface adapters:

1. Click the *IA* button to view individual interface adapter version information.
2. Select the *IA* 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 interface adapter status indicator in the Main dialog box is yellow. The interface adapters are *unavailable* when an upgrade is in progress. When an upgrade is initiated, any current connection to the device using the interface adapter is terminated.

To simultaneously upgrade multiple interface adapters:

1. Activate the OSD interface, click *Commands – IA Status* and click one or more types of interface adapters to upgrade.
2. Click *Upgrade*.

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

3. In the IA *Upgrade* dialog box, click *OK* to initiate the upgrade and return to the IA *Status* dialog box.

To return an interface adapter to factory default status:

1. Click *IA* in the *Version* dialog box.
2. Select an interface adapter, then click *Decommission*.
3. Click *OK* to restore factory defaults. The interface adapter goes offline briefly and returns.
   - or-
   Click *X* or press *Escape* to cancel the operation.
4. Click *X* to close the IA *Select* dialog box.

Using the on-board Web interface (OBWI)

The OBWI for the console switch is a remote, web browser-based user interface. 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.

	Browser		
Operating System	**Microsoft® Internet Explorer® Version 9.0**	**Firefox Version 10 and later**	**Google Chrome Version 19 and later**
Microsoft Windows Server® 2003 Standard, Enterprise or Web Edition	Yes	Yes	Yes
Microsoft Windows XP Home Edition or Professional	Yes	Yes	Yes
Microsoft Windows 7 or 8	Yes	Yes	Yes
Microsoft Windows Server® 2012	Yes	Yes	Yes
Microsoft Windows 2008	Yes	Yes	Yes
Red Hat Enterprise Linux® 5 and 6	No	Yes	No
Canonical Ubuntu 12.04	No	Yes	No
Sun Solaris® 10 and 11	No	Yes	No
Novell SUSE Linux Enterprise 10 and 11	No	Yes	No
Apple Mac OS X Tiber 10.4+	No	Yes	No

To log in to the KVM Console Switch OBWI:

1. Launch a web browser.
2. In the address field of the browser, enter the IP address or host name assigned to the console 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 console switch, enter your username and password, then click *Login*.

NOTE: The default username is Admin with no password.

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

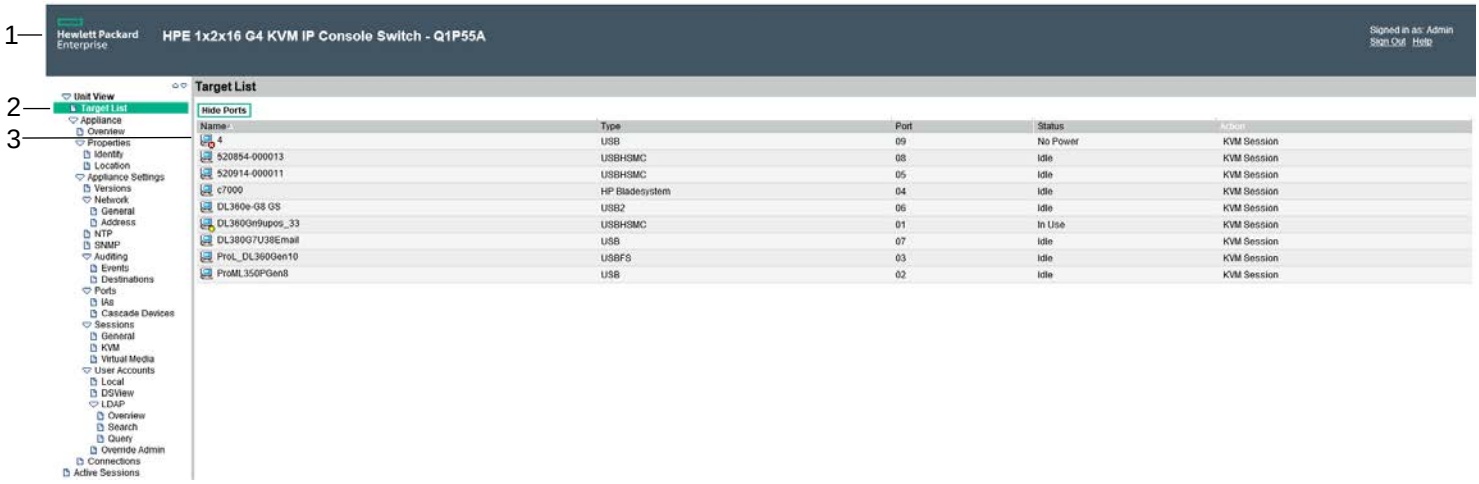
NOTE: The console switch attempts to detect if Java is already installed on your PC. If it is not, in order to use the OBWI, need to install it. You can also need to associate the JNLP file with Java WebStart.

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 do 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 can view, access and manage your console switch, as well as specify system settings and change profile settings. The following figure shows the user interface window areas. The window descriptions are provided in the following table.



Item	Name	Description
1	Top option bar	Use the top option bar to contact Technical Support, view the software general information, log out of an OBWI session or access the Help tool
2	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.
3	Content area	Use the content area to display or make changes to the console switch OBWI system.

Viewing system information

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

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.
Switch	Unit View - Appliance - Tools	Name, type and the console switch tools (Maintenance-Overview/Reboot/Reset and Upgrade, Certificates and Trap MIB).
Switch	Unit View - Appliance - Files	Configuration and User Database for the console switch.
Switch	Unit View - Appliance - Properties - Identity	Part number and serial number

Category	Select This:	To View This:
Switch	Unit View - Appliance - Properties - Location	Site, department and location of each unit.
Switch	Unit View - Appliance Settings - Versions	Current application, boot, build, hardware, UART and video ASIC versions.
Switch	Unit View – Appliance Settings - Network	Network address, LAN speed and web server ports.
Switch	Unit View - Appliance Settings - SNMP	System description, SNMP setting, contact, read/write and trap settings and designations for allowed managers.
Switch	Unit View - Appliance Settings - Auditing	Events list and status and SNMP trap destinations.
Switch	Unit View - Appliance Settings - Ports	Status, EID, name, port, application and interface type for each IA; name, port, type, channels and status for each tiered console switch.
Switch	Unit View - Appliance Settings Sessions	General session timeout and sharing details; KVM encryption levels and keyboard language; virtual media settings, drive mappings, encryption level and IA access.
Switch	Unit View - Appliance - User Accounts	Security and user lock-out for the local account; authentication server assignments for DSView management software and override admin username and password in case of a failed operation.
Switch	Unit View - Appliance - Connections	Connection path name and type.
	Active Sessions	Server, owner, remote host, duration and type of each active session.

Generating a certificate

A web certificate allows you to access the OBWI without having to acknowledge the console switch 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. From the side navigation bar, select *Unit View - Appliance - Overview*.
2. Click *Manage Appliance Web Certificate*.
3. Click *Update*.
4. 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 (for example, “marketing”).
   - 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.
5. Click *Generate* to create the certificate.

To upload a new certificate:

1. Select 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 can 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.

Rebooting and upgrading the KVM console switch

From the *Unit View - Appliance - Overview* window, you can view the console switch name and type. You can also perform the following tasks.

Rebooting the KVM console switch

To reboot the KVM Console Switch:

1. Click *Unit View - Appliance - Overview* to open the Unit Maintenance window.
2. Click the *Reboot* button.
3. A dialog box appears, warning you that all active sessions is disconnected. Click the *OK* button.

NOTE: If you are using the local UI, the window is blank while the KVM console switch reboots. If you are using the remote OBWI, a message indicates that the interface is waiting on the console switch to complete the reboot.

Upgrading the console switch firmware

Update the console switch with the latest available firmware.

After the firmware is updated, the console switch performs a soft reset, which ends all IA sessions. A target device experiencing an IA firmware update might not appear, or might appear as disconnected. The target device appears normally when the update completes.

CAUTION: Disconnecting an IA during a firmware update or while cycling power to the target device renders the IA inoperable. The IA must be returned to the factory for repair.

To upgrade the console switch firmware:

1. From the side navigation bar, click *Unit View - Appliance - Overview* to open the Unit Maintenance window.
2. Click *Upgrade Firmware*.
3. Select one of the following methods to load the firmware file: *Filesystem*, *TFTP*, *FTP* or *HTTP*.

NOTE: The Filesystem option is only available on the remote OBWI.

4. If you selected Filesystem, select *Browse* to specify the location of the firmware upgrade file.
   If you selected TFTP, enter the server IP address and firmware file you wish to load.
   If you selected FTP or HTTP, enter the server IP address and firmware file you wish to load, as well as the username and password.
5. Click the *Upgrade* button.

Saving and restoring configurations and user databases

The console switch configuration and local user database can be saved to files. Once saved, the configuration file or local user database can be restored to the console switch.

Saving a managed console switch configuration or user database

To save a KVM Console Switch configuration or the local user database of a KVM Console Switch:

1. Click *Unit View - Appliance - Overview*.
2. Click either the *Save Appliance Configuration* or *Save Appliance User Database*, 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.
   If you selected FTP or HTTP, enter the Server IP address, username, password and firmware filename you wish to load.
5. Click the *Download* button.
6. In the Save As dialog box, navigate to the desired location and enter a name for the file. Click the *Save* button.

Restoring a managed console switch configuration or user database:

1. From the side navigation bar, click the *Unit View - Appliance - Overview*.
2. Click either the *Restore Appliance Configuration or Restore Appliance User Database*, 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.
   If you selected TFTP, enter the server IP address and firmware filename you wish to load.
   If you selected FTP or HTTP, enter the server IP address, username, 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. After the success window appears, reboot the managed console switch to enable the restored configuration.

Recovering from a failed flash upgrade

NOTE: You can only recover from a failed Flash upgrade when using IPv4 mode. If the green power LED on the front and back panel of the remote console switch blinks continuously, the remote console switch is in recovery mode.

To recover from a failed flash upgrade:

1. Download the latest Flash firmware.
2. Save the Flash upgrade file to the appropriate directory on the TFTP server.
3. Set up the TFTP server with the server IP address 10.0.0.20.
4. Rename the downloaded file “CMN-1095.fl” and place it into the TFTP root directory of the TFTP server.
5. If the remote console switch is not on, turn it on now. The recovery process should start automatically.

Property identity and location settings

The console switch can report most device properties directly through the console switch web browser. Clicking *Identity* displays the Unit Identification Properties window and provides the part number and serial number. The Unit Location Properties window displays the site, department and location.

Viewing version information

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

Network settings

NOTE: Only administrators can make changes to the Network dialog box settings. Other users 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 console switch General Network Setting’s window.
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 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 window.
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 is 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 is ignored.

4. Click *Save*.

SNMP

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

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

Configuring SNMP parameters

1. Click *SNMP* to open the SNMP window.
2. Click to enable the *Enable SNMP* checkbox to allow the console 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 console switch. The values can be up to 64 characters in length. These fields cannot be left blank.
5. Type the address of up to four management workstations that are allowed to manage this console switch in the Allowable Managers fields. Alternatively, you can leave these fields blank to allow any station to manage the console switch.
6. Click *Save*.

Auditing event settings

An event is a notification sent by the KVM Console Switch to a management station indicating that something has occurred that can require further attention.

To enable individual events:

1. Click *Auditing* to open the Events window.
2. Specify the events that generate notifications by clicking the appropriate checkboxes in the list. Select or clear the checkbox next to *Event Name* to select or deselect the entire list.
3. Click *Save*.

Setting event destinations

Configure audit events to be sent to SNMP trap destinations and Syslog devices. The events enabled on the Events window are sent to all the devices listed on the Event Destination window.

To set event destinations:

1. Click *Auditing* and the Destinations tab to open the Event Destinations window.
2. Type the address of up to four management workstations to which this console switch sends events in the SNMP Trap Destination fields, as well as up to four Syslog devices.
3. Click *Save*.

Configuring an IA

The console switch displays a list of the attached IAs, as well as the following information about each IA:

- EID
- Port
- Status
- Application Version
- Interface Type.

Click on one of the IA to view the following additional information:

- Switch Type
- Boot Version
- Application Version
- Hardware Version
- FPGA Version
- Version Available
- Upgrade Status.

Deleting an IA

To delete an offline IA:

1. Click *Ports – IA* to open the IA window.
2. Click in the applicable IA checkbox.
3. Click *Delete Offline*.

Upgrading an IA

The IA automatically updates when the console switch is updated. If issues occur during the normal upgrade process, the IA can also be force-upgraded when needed.

CAUTION: Disconnecting an IA during a firmware update or cycling power to the device renders the module inoperable and require the IA to be returned to the factory for repair.

To upgrade the IA firmware:

1. From the side navigation bar, click *Ports - IA* to open the IA window.
2. Select the checkboxes next to the IA that you wish to upgrade.
3. Select *Operations* and select *Upgrade*.
4. If the settings are correct, click *Upgrade*.

To set the USB speed (applies only for USB 2.0 IAs):

1. From the side navigation bar, click *Ports – IA* to open the IA window.
2. Select the checkboxes next to the IA that you wish to modify.
3. Select *Operations* and select the USB speed.

Launching a session

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 appears.
2. The applicable action, KVM Session, is displayed in the Action column and depends 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 can 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 appears.

NOTE: From the Active Sessions window, 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 session settings

To configure general session settings:

1. From the side navigation bar, select *Sessions - General*. The General Session Settings window 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. Click *Save*.

Local user account settings

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

Access levels

When a user account is added, the user can be assigned to any of the following access levels:

- Appliance Administrators
- User Administrators
- Users

Operation	Appliance 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 Appliance Administrator only):

1. Select *User Accounts - Local User Accounts* to open the Local User Accounts window.
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.
5. Select any of the available devices that you wish to assign to the user account.
6. Click *Add*.
   NOTE: User Administrators and Appliance Administrators can access all devices.
7. Click *Save*.

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

1. Select *User Accounts - Local Accounts* to open the Local User Accounts window.
2. Click the checkbox to the left of each account that you wish to delete.
3. Click *Delete*.

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

1. From the side navigation bar, select *User Accounts - Local Accounts*. The Local User Accounts window is displayed.
2. Click the name of the user you wish to edit. The user profile appears.
3. Fill out the user information on the window.
4. 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 window.
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 IA for which you want to enable virtual media and click Enable VM.
   Select the checkbox next to each IA for which you want to disable virtual media and click Disable VM.

Virtual media options

You can determine the behavior of the console switch during a virtual media session using the options provided in the Virtual Media Session Settings window. 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 window. In addition to connecting and disconnecting a virtual media session, you can configure the settings that are listed in the following table.

Settings	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.

DSView software settings

Contact and register an unmanaged console switch with a DSView management software device by specifying the IP address of the management software device.

To configure the device IP address:

1. Select *User Accounts - DSView*. The DSView management software Settings window 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 console switch that has been registered with the device, click the *Disassociate* button.
5. Click *Save*.

LDAP

LDAP is a vendor-independent protocol standard used for accessing, querying and updating a directory using TCP/IP. Based on the X.500 Directory Services model, LDAP is a global directory structure that supports strong security features including authentication, privacy and integrity.

If individual user accounts are stored on an LDAP-enabled directory service such as Active Directory, you can use the directory service to authenticate users. The default values given for the LDAP search and query parameters are defined for use with Active Directory.

The settings made in the OBWI let you configure your authentication configuration parameters. The software sends the username, password and other information to the appliance, which then determines whether the user has permission to view or change configuration parameters for the appliance in the OBWI.

NOTE: Unless otherwise specified, the LDAP default values should be used unless Active Directory has been reconfigured. Modifying the default values can cause LDAP authentication server communication errors.

Configuring LDAP in the User Interface

LDAP overview parameters

On the LDAP Overview window in the OBWI, you can configure the LDAP authentication priority and the parameters that define LDAP server connection information.

LDAP authentication priority

In the LDAP Priority section of the OBWI, you can disable LDAP or you can set the authentication priority by choosing whether local authentication or LDAP authentication should happen first.

To configure LDAP authentication priority parameters:

1. Select Appliance - Appliance Settings - User Accounts - LDAP Accounts - Overview.
2. Select either LDAP Disabled, LDAP before Local or LDAP after Local for the LDAP Priority.
3. Click Save.

LDAP servers

The Address fields specify the host filenames or IP addresses of the primary and secondary LDAP servers. The secondary
LDAP server is optional.

The Port fields specify the User Datagram Protocol (UDP) port numbers that communicate with the LDAP servers. The default value is 389 for non-secure LDAP and 636 for secure LDAP (LDAPS). The default Port ID is automatically entered by the software when an access type is specified.

The Access Type radio buttons specify how a query is sent to each LDAP target device. When using LDAP, all usernames, passwords and other information sent between an appliance and an LDAP server are sent as non-secure clear text. Use LDAPS for secure encrypted communication between an appliance and an LDAP server.

To configure LDAP server parameters:

1. Select Appliance - Appliance Settings - User Accounts - LDAP Accounts - Overview.
2. Identify the primary and secondary server address, port and access type in the appropriate fields or radio buttons.
3. Click Save.

LDAP search parameters

On the LDAP Search window, you can configure the parameters used when searching for LDAP directory service users.

Use the Search DN field to define an administrator-level user that the appliance uses to log into the directory service. Once the appliance is authenticated, the directory service grants it access to the directory to perform the user authentication queries specified on the LDAP Query page. The default values are cn=Administrator, cn=Users, dc=yourDomainName and dc=com and can be modified. For example, to define an administrator Distinguished Name (DN) for test.view.com, enter cn=Administrator, cn=Users, dc=test, dc=view and dc=com. Each Search DN value must be separated by a comma.

The Search Password field is used to authenticate the administrator or user specified in the Search DN field.

Use the Search Base field to define a starting point from which LDAP searches begin. The modifiable default values are dc=yourDomainName and dc=com. For example, to define a search base for test.com, type dc=test then dc=com. Each Search Base value must be separated by a comma.

The UID Mask field specifies the search criteria for User ID searches of LDAP target devices. The format should be in the form <name>=<%1>. The default value is sAMAccountName=%1, which is correct for use with Active Directory. This field is required for LDAP searches.

To configure LDAP search parameters:

1. Select Appliance - Appliance Settings - User Accounts - LDAP Accounts - Search.
2. Enter the appropriate information in the Search DN, Search Password, Search Base and UID Mask fields.

3. Click Save.

NOTE: These options cannot be changed if the LDAP Priority is set to LDAP Disabled on the Overview window.

LDAP query parameters

On the LDAP Query window, you can configure the parameters used when performing user authentication queries.

The appliance performs two different types of queries. Query Mode (Appliance) is used to authenticate administrators and users attempting to access the appliance itself. Query Mode (Target Device) is used to authenticate users that are attempting to access attached target devices. Additionally, each type of query has three modes that utilize certain types of information to determine whether or not an LDAP user has access to an appliance or connected target devices.

You can configure the following settings on the LDAP Query window:

- The Query Mode (Appliance) parameters determine whether or not a user has access to the appliance.
- The Query Mode (Target Device) parameters determine whether or not a user has user access to target devices connected to an appliance. The user does not have access to the appliance unless granted by Query Mode (Appliance).
- The Group Container, Group Container Mask and Target Mask fields are only used for group query modes and are required when performing an appliance or device query.
- The Group Container field specifies the organizational unit (ou) created in Active Directory by the administrator as the location for group objects.
    - Group objects are Active Directory objects that can contain users, computers, contacts and other groups. Group Container is used when Query Mode is set to Group Attribute. Each group object, in turn, is assigned members to associate with a particular access level for member objects (people, appliances and target devices). The access level associated with a group is configured by setting the value of an attribute in the group object.
    - For example, if the Notes property in the group objects list is used to implement the access control attribute, the Access Control Attribute field on the LDAP Query window should be set to info. Setting the Notes property to KVM User Admin causes the members of that group to have user administration access to the appliances and target devices that are also members of that same group.
- The Notes property is used to implement the access control attribute. The value of the Notes property, available in group and user objects shown in Active Directory Users and Computers (ADUC), is stored internally in the directory, in the value of the info attribute. ADUC is a Microsoft Management Console snap-in for configuring Active Directory. It is started by selecting *Start - Programs - Administrative Tools - Active Directory Users and Computers*. This tool is used to create, configure and delete objects such as users, computers and groups.
- The Group Container Mask field defines the object type of the Group Container, which is normally an organizational unit. The default value is ou=%1.
- The Target Mask field defines a search filter for the target device. The default value is cn=%1.
- The Access Control Attribute field specifies the name of the attribute that is used when the query modes are set to User Attribute or Group Attribute. The default value is info.

To configure LDAP query parameters:

1. Select Appliance - Appliance Settings - User Accounts - LDAP Accounts - Query.
2. Select either Basic, User Attribute or Group Attribute for the Appliance Query Mode and the Target Device Query Mode.
3. Enter the appropriate information in the Group Container, Group Container Mask, Target Mask and Access Control Attribute fields.
4. Click Save.

NOTE: These options cannot be changed if the LDAP Priority is set to LDAP Disabled on the Overview window.

Appliance and target device query modes

One of three different modes can each be used for Query Mode (Appliance) and Query Mode (Target Device):

- Basic – A username and password query for the user is made to the directory service. If they are verified, the user is given appliance administrator access to the appliance and any attached target devices for Query Mode (Appliance) or to any selected target device for Query Mode (Target Device).
- User Attribute – A username, password and Access Control Attribute query for the appliance user is made to the directory service. The Access Control Attribute is read from the user object (the user account) in Active Directory.

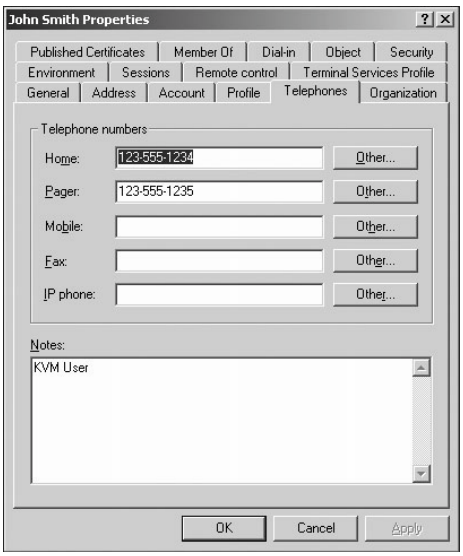
  If the KVM Appliance Admin value is found, the user is given appliance administrator access to the appliance and any attached target devices for Query Mode (Appliance) or to any selected target device for Query Mode (Target Device).

  If the KVM User Admin value is found, the user is given user administrator access to the appliance and attached target devices for Query Mode (Appliance) or to any selected target device for Query Mode (Target Device).

  If the KVM User value is found, the user is given user access to the appliance for Query Mode (Appliance) or to any selected target device for Query Mode (Target Device).

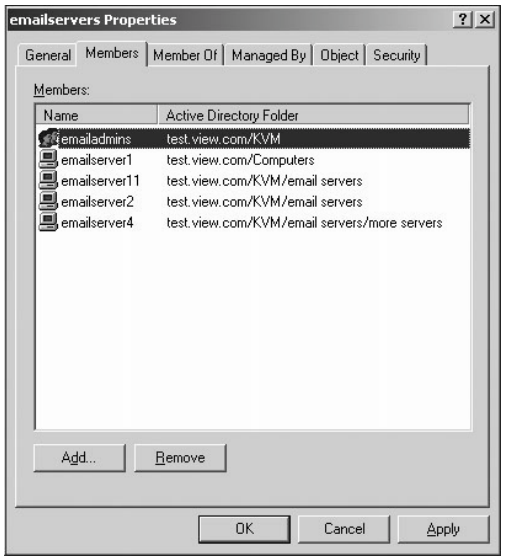
NOTE: If none of the three values are found, the user is given no access to the appliance and target devices for Query Mode (Appliance) or to any selected target device for Query Mode (Target Device), unless the user has User Admin or Appliance Admin privileges to the appliance.

You can access the ADUC by selecting *Start - Programs - Administrative Tools - Active Directory Users and Computers*.



- Group Attribute – A username, password and group query is made to the directory service for an appliance and attached target devices when using Query Mode (Appliance) or for a selected target device when using Query Mode (Target Device). If a group is found containing the user and the appliance name, the user is given access to the appliance or attached target devices, depending on the group contents, when using Query Mode (Appliance). If a group is found containing the user and target device IDs, the user is given access to the selected target device connected to the appliance when using Query Mode (Target Device).

  Groups can be nested to a maximum of 16 levels in depth. Use nesting to create groups within other groups. For example, you can have a top-level group named Computers that contains a member named R&D, which is a group. The R&D group can contain a member named Domestic, which is a group and so on.



Setting up active directory for performing queries

Before you can use any of the querying modes for units, you must first make changes to Active Directory so that the selected querying mode can assign the applicable authorization level for the user.

To set up group queries:

1. Log into Windows with administrator privileges.
2. Open the Active Directory software.
3. Create an organizational unit to be used as a group container.
4. Create a computer object in Active Directory with a name identical to the switching system name for querying appliances (specified in the Appliance Overview window of the OBWI) or identical to the attached target devices for querying target devices. The name must match exactly, including case.
5. The appliance names and target device names used for group queries are stored in the appliance. The appliance name specified in the Appliance Overview window of the OBWI and target device names must identically match the object names in Active Directory. Each appliance name and target device name can be comprised of any combination of upper-case and lower-case letters (a-z, A-Z), digits (0-9) and hyphens (-). You cannot use spaces and periods (.) or create a name that consists entirely of digits. These are Active Directory constraints.
   NOTE: The factory default name in earlier versions contains a space that must be removed by editing the switching system name in the Appliance Overview window of the OBWI.
6. Create one or more groups under the group container organizational unit.
7. Add the usernames and the target device/appliance objects to the groups you created in step 5.
8. Specify the value of any attribute being used to implement the access control attribute. For example, if you are using info as the attribute in the Access Control Attribute field and using the Notes property in the group object to implement the access control attribute, the value of the Notes attribute in Active Directory can be set to one of the three available access levels (KVM User, KVM User Admin or KVM Appliance Admin) for the group object. The members of the group can then access the appliances and target devices at the specified access level.

Active sessions

From the Active Sessions window, 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 Appliance Active Sessions window.
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 is disconnected.

To close a session (local users only):

1. From the side navigation bar, select *Local Session*.
2. Select the *Disconnect Active Session* checkbox.

KVM video viewer

The following procedure helps you launch a KVM Video Viewer session. For more information about using the KVM Video Viewer, see the KVM Video Viewer Technical Bulletin.

To open a KVM session:

1. From the side navigation bar of the console switch web user interface (UI), click *Unit View - Target List*.
2. Click the KVM Session link for the target device you wish to view.
3. The KVM Video Viewer launches in a new window.

Terminal operation

Each console switch can be configured at the console switch level through the Terminal Console menu interface, which is accessed through the DIAG port. All terminal commands are accessed through a terminal window 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 console switch:

1. Using a serial adaptor, a terminal or a PC that is running terminal emulation software, such as HyperTerminal software, to the DIAG port on the back panel of the console 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 console switch and each target device. When the console switch completes initialization, the Console menu displays the following message: *Press any key to continue.*

Network configuration

To configure network settings using the console menu:

1. When you turn on the console switch, it 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 can be connected at any time, even when the console 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 console switch 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 can be used to provide a user-defined IP address, netmask or prefix length and default gateway for the console switch.

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 console switch and cannot be modified by a console switch user.

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

5. Select the remaining options from the Network Configuration menu to finish the configuration of your console switch 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 console switch 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.

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 restores all console switch options to the default settings.

Reset appliance

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

Set web interface ports

The console switch 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 console switch is required to use new port numbers.

Exit

This menu selection returns 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 is prompted with the Password login window.

Appendix A: MIB SNMP Traps

The console switch 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 can be uploaded from the console switch using the Save Trap MIB function. The uploaded Trap MIB file can then be loaded into an SNMP Trap Receiver application.

This appendix describes the trap events that can be generated by the console switch. The actual Trap MIB file contains the most accurate trap information.

An SNMP manager can access MIB-II objects of the console switch using the IPv4 or IPv6 protocols.

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

The console switch 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 console switch. The following table is a list of the generated trap events.

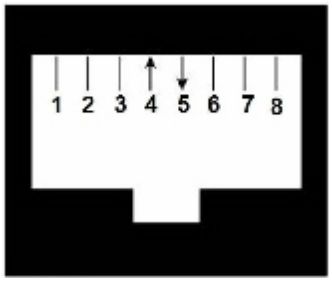
Trap Event	Trap Number
User Authentication Failure	1
User Login	2
User Logout	3
Target Session Started	4
Target Session Stopped	5
Target Session Terminated	6
Traps 7-8 are Unused	7-8
User Added	9
User Deleted	10
User Modified	11
Reboot Started	12
Image File Upgrade Started	13
Image File Upgrade Results	14
Interface Adapter Added	15
Interface Adapter Removed	16
Target Device Name Changed	17
Tiered Switch Added	18
Tiered Switch Removed	19

Trap Event	Trap Number
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
Interface Adapter Upgrade Started	35
Interface Adapter Image Upgrade Result	36
Interface Adapter 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
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

Appendix B: DIAG port pinouts

The console switch DIAG port is an 8-pin modular jack. The DIAG port pinouts and descriptions are provided in the following figure and table.

Figure DIAG Port Pinouts



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

Appendix C: Using serial interface adapters

The serial interface adapter is a serial-to-VGA converter that allows VT100-capable devices to be viewed from the console switch local port, the OBWI or by using the console 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 console 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 interface adapter modes

The following modes can be accessed from the serial interface adapter:

- On-Line: This mode enables you to send and receive serial data.
- Configuration: This mode enables you to specify console 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 interface adapter

NOTE: The serial interface adapter is a DCE device and only supports VT100 terminal emulation.

Pressing Ctrl-F8 activates the Configuration window of the interface adapter's Terminal Applications menu, which enables you to configure your serial interface adapter.

NOTE: When any Terminal Applications menu is active, pressing Enter saves changes and returns you to the previous window. Pressing Escape returns you to the previous window without saving changes.

Within the Terminal Applications menu's Configuration window, 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 window or CR LF (Enter-Linefeed), which moves the cursor to the left side of the window 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 window'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 window'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 window'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.

- Window Size: This option allows you to specify the window'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 window enable you to define the function keys that 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 window 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 window. 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 interface adapter:

1. Press Ctrl-F8. The Configuration window appears.
2. Select a parameter to change. You can navigate the Configuration window 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 window.
   -or-
   Press Escape to exit the Configuration window without saving the changes.

Creating a serial interface adapter macro

Pressing the Page Down key when the Terminal Applications menu's Configuration window is displayed provides access to the Macro Configuration window. The serial interface 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 interface adapter you wish to configure and press Ctrl-F8 to activate the Terminal Applications menu's Configuration window.
2. When the Terminal Applications menu appears, press Page Down to view the Macro Configuration window. The Macro Configuration window 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 can be used. When you have finished entering the keystroke sequence that activates 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 window.

Using history mode

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

The serial interface adapter maintains a buffer containing 240 lines minimum or 10 windows of output. When the history buffer is full, it adds 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 displays 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 window.
   - Page Down: Move down one buffer window.
   - Up Arrow: Move up one buffer line.
   - Down Arrow: Move down one buffer line.
   - Ctrl-F8: Enters Configuration mode. The Configuration window appears.
   - Ctrl-F9: While in Configuration mode, returns to the previous window with History mode enabled.
   - Ctrl-F10: While in Configuration mode, returns to the previous window with On-Line mode enabled.
   - Ctrl-F11: Clears the history buffer. If you choose this option, a warning window appears. Press Enter to delete the history buffer or Escape to cancel the action. The previous window reappears.
3. When finished, press Ctrl-F10 to exit History mode and return to On-Line mode.

Serial interface adapter pinouts

The following table lists the pinouts for the serial interface adapter.

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

Appendix D: UTP Cabling

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

- CAT5 (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. CAT5 cable is generally used for networks running at 10 or 100 Mbps.
- CAT5E (enhanced) cable has the same characteristics as CAT5, but is manufactured to somewhat more stringent standards.
- CAT6 cable is manufactured to tighter requirements than CAT5E cable. CAT6 has higher measured frequency ranges and significantly better performance requirements than CAT5E cable at the same frequencies.

Wiring standards

There are two supported wiring standards for 8-conductor (4-pair) RJ45 terminated UTP cable: EIA/TIA 568A and B. These standards apply to installations utilizing UTP cable specifications. The console switch system supports either of these wiring standards. The following table describes the standards for each pin.

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.

Warranty and regulatory information

Warranty information

HPE ProLiant and x86 Servers and Options (http://www.hpe.com/support/ProLiantServers-Warranties)
HPE Enterprise Servers (http://www.hpe.com/support/EnterpriseServers-Warranties)
HPE Storage Products (http://www.hpe.com/support/Storage-Warranties)
HPE Networking Products (http://www.hpe.com/support/Networking-Warranties)

Regulatory information

Safety and regulatory compliance

For important safety, environmental, and regulatory information, see *Safety and Compliance Information for Server, Storage, Power, Networking, and Rack Products*, available at the Hewlett Packard Enterprise website (http://www.hpe.com/support/Safety-Compliance-EnterpriseProducts).

Belarus Kazakhstan Russia marking

Manufacturer and Local Representative Information
Manufacturer information:
Hewlett Packard Enterprise Company, 3000 Hanover Street, Palo Alto, CA 94304 U.S.

Local representative information Russian:

- **Russia:**

  ООО «Хьюлетт Паккард Энтерпрайз», Российская Федерация, 125171, г. Москва, Ленинградское шоссе, 16А, стр.3, Телефон/факс: +7 495 797 35 00

- **Belarus:**

  ИООО «Хьюлетт-Паккард Бел», Республика Беларусь, 220030, г. Минск, ул. Интернациональная, 36-1, Телефон/факс: +375 17 392 28 20

- **Kazakhstan:**

  ТОО «Хьюлетт-Паккард (К)», Республика Казахстан, 050040, г. Алматы, Бостандыкский район, проспект Аль-Фараби, 77/7, Телефон/факс: + 7 727 355 35 52

Local representative information Kazakh:

- **Russia:**

  ЖШС "Хьюлетт Паккард Энтерпрайз", Ресей Федерациясы, 125171, Мәскеу, Ленинград тас жолы, 16А блок 3, Телефон/факс: +7 495 797 35 00

- **Belarus:**

  «HEWLETT-PACKARD Bel» ЖШС, Беларусь Республикасы, 220030, Минск қ., Интернациональная көшесі, 36/1, Телефон/факс: +375 17 392 28 20

- **Kazakhstan:**

ЖШС «Хьюлетт-Паккард (К)», Қазақстан Республикасы, 050040, Алматы к., Бостандық ауданы, Әл-Фараби даңғ ылы, 77/7, Телефон/факс: +7 727 355 35 52

Manufacturing date:
The manufacturing date is defined by the serial number.
CCSYWWZZZZ (serial number format for this product)
Valid date formats include:

- YWW, where Y indicates the year counting from within each new decade, with 2000 as the starting point; for example, 238: 2 for 2002 and 38 for the week of September 9. In addition, 2010 is indicated by 0, 2011 by 1, 2012 by 2, 2013 by 3, and so forth.
- YYWW, where YY indicates the year, using a base year of 2000; for example, 0238: 02 for 2002 and 38 for the week of September 9.

Turkey RoHS material content declaration

Türkiye Cumhuriyeti: EEE Yönetmeliğine Uygundur

Ukraine RoHS material content declaration

Обладнання відповідає вимогам Технічного регламенту щодо обмеження використання деяких небезпечних речовин в електричному та електронному обладнанні, затвердженого постановою Кабінету Міністрів України від 3 грудня 2008 № 1057

Korean notice

Class A equipment

A급 기기 (업무용 방송통신기기)	이 기기는 업무용(A급)으로 전자파적합등록을 한 기기이오니 판매자 또는 사용자는 이 점을 주의하시기 바라며, 가정 외의 지역에서 사용하는 것을 목적으로 합니다.

Class B equipment

B급 기기 (가정용 방송통신기기)	이 기기는 가정용(B급)으로 전자파적합등록을 한 기기로서 주로 가정에서 사용하는 것을 목적으로 하며, 모든 지역에서 사용할 수 있습니다.

아보센트 코어퍼레이션

Support and other resources

Accessing Hewlett Packard Enterprise Support

- For live assistance, go to the Contact Hewlett Packard Enterprise Worldwide website (http://www.hpe.com/assistance).
- To access documentation and support services, go to the Hewlett Packard Enterprise Support Center website (http://www.hpe.com/support/hpesc).

Information to collect

- Technical support registration number (if applicable)
- Product name, model or version, and serial number
- Operating system name and version
- Firmware version
- Error messages
- Product-specific reports and logs
- Add-on products or components
- Third-party products or components

Accessing updates

- Some software products provide a mechanism for accessing software updates through the product interface. Review your product documentation to identify the recommended software update method.
- To download product updates, go to either of the following:
    - Hewlett Packard Enterprise Support Center **Get connected with updates** page (http://www.hpe.com/support/e-updates)
    - Software Depot website (http://www.hpe.com/support/softwaredepot)
- To view and update your entitlements, and to link your contracts and warranties with your profile, go to the Hewlett Packard Enterprise Support Center **More Information on Access to Support Materials** page (http://www.hpe.com/support/AccessToSupportMaterials).

IMPORTANT: Access to some updates might require product entitlement when accessed through the Hewlett Packard Enterprise Support Center. You must have an HP Passport set up with relevant entitlements.

Websites

- Hewlett Packard Enterprise Information Library (http://www.hpe.com/info/enterprise/docs)
- Hewlett Packard Enterprise Support Center (http://www.hpe.com/support/hpesc)
- Contact Hewlett Packard Enterprise Worldwide (http://www.hpe.com/assistance)
- Subscription Service/Support Alerts (http://www.hpe.com/support/e-updates)
- Software Depot (http://www.hpe.com/support/softwaredepot)
- Customer Self Repair (http://www.hpe.com/support/selfrepair)
- Insight Remote Support (http://www.hpe.com/info/insightremotesupport/docs)
- Serviceguard Solutions for HP-UX (http://www.hpe.com/info/hpux-serviceguard-docs)
- Single Point of Connectivity Knowledge (SPOCK) Storage compatibility matrix (http://www.hpe.com/storage/spock)

- Storage white papers and analyst reports (http://www.hpe.com/storage/whitepapers)

Remote support

Remote support is available with supported devices as part of your warranty or contractual support agreement. It provides intelligent event diagnosis, and automatic, secure submission of hardware event notifications to Hewlett Packard Enterprise, which will initiate a fast and accurate resolution based on your product's service level. Hewlett Packard Enterprise strongly recommends that you register your device for remote support.

For more information and device support details, go to the Insight Remote Support website (http://www.hpe.com/info/insightremotesupport/docs).

Documentation feedback

Hewlett Packard Enterprise is committed to providing documentation that meets your needs. To help us improve the documentation, send any errors, suggestions, or comments to Documentation Feedback (mailto:docsfeedback@hpe.com). When submitting your feedback, include the document title, part number, edition, and publication date located on the front cover of the document. For online help content, include the product name, product version, help edition, and publication date located on the legal notices page.