HP IP and Server Console Switches G2
User Guide

Abstract

This document is for the person who installs racks and rack products. This procedure is performed only by trained personnel. HP assumes you are qualified in performing installations and trained in recognizing hazards in rack products.

Contents

Product features

Overview of features

HP offers two types of console switches that provide flexible, centralized control of data center servers and infrastructure appliances:

- HP IP Console Switch G2
- HP Server Console Switch G2

> **NOTE:** Unless otherwise specified, **console switch** refers to both the HP IP Console Switch and the HP Server Console Switch.

The following features are available for the new generation console switches:

- Local and remote KVM console access
- True serial capability
- Dual power supplies for redundancy
- Virtual media capability
- Smart card (CAC) capability
- Enhanced video resolution support
- Dual Gigabit NICs for transparent network failover (HP IP Console Switch G2 only)

KVM switching capabilities

The console switch supports several interface adapters, powered directly from the target device to provide Keep Alive functionality when the switch is not powered. The following interface adapters are supported:

- C-Class Blade KVM
- PS2
- USB
- Serial
- PS2 with Virtual Media
- USB with Virtual Media
- PS2 with Virtual Media and CAC
- USB with Virtual Media and CAC
- Serial G2

For more information on interface adapters, see Selecting an interface adapter (on page 23).

True serial capabilities

The console switch supports the HP Serial G2 Adapter, which provides true serial capabilities. You can directly launch an SSH or Telnet session or launch a serial viewer from the local console UI or remote OBWI to establish a serial console session.

Local and remote user interfaces

To configure and manage your console switch, you can use either the local console UI or the remote OBWI.

The two user interfaces share a similar look and feel for optimal user experience.

Virtual media capabilities

You can view, move, or copy data located on virtual media to and from any target device. This functionality enables you to manage remote systems more efficiently for standard tasks such as operating system installation, operating system recovery, hard drive recovery or duplication, BIOS updating, and target device backup.

> **NOTE:**   To open a virtual media session with a target device, you must first connect the target device to a console switch using a virtual media capable interface adapter.

You can connect virtual media for the local console to the console switch using local USB ports, or you can connect virtual media remotely from the client computer.

Smart card capabilities

You can use a smart card, also referred to as a CAC, with your console switch when two-factor authentication is required.

> **NOTE:**   To use a smart card reader with a target device, you must first connect the target device to a console switch using a smart card capable interface adapter.

You can connect smart card readers directly to the console switch using local USB ports, or you can connect smart card readers to any remote workstation. The smart card reader must be connected prior to starting a console session with the server. For more information about smart cards, see Using Smart Cards (on page 64).

FIPS cryptographic module

The KVM switch supports FIPS 140-2 Level 1 cryptographic security requirements. The FIPS mode of operation can be enabled or disabled via the OBWI or local port and executed after a reboot. When FIPS is enabled, a reboot of the switch requires approximately two additional minutes to complete a FIPS mode integrity check. Also, when FIPS is enabled, if the keyboard, mouse, or video encryption is set to 128-bit SSL (ARCFOUR) or DES, the encryption level is automatically changed to the encryption level AES.

> **IMPORTANT:**   The FIPS mode can be changed via the DSView software plug-in.

IMPORTANT: The FIPS mode of operation is initially disabled and must be enabled to operate.

IMPORTANT: The Setup port factory default setting automatically disables the FIPS module.

KVM switches use an embedded FIPS 140-2 validated cryptographic module (Cerificate #1051) running on a Linux PPC platform per FIPS 140-2 Implementation Guidance section G.5 guidelines (http://csrc.nist.gov/groups/STM/cmvp/documents/fips140-2/FIPS1402IG.pdf).

The FIPS mode can be enabled or disabled via the OBWI, Local Port, or DSView plug-in. A reboot is required to enable or disable the FIPS mode. A firmware upgrade to this version or setting the state to the default state (Setup Port menu) disables the FIPS mode.

In FIPS mode, encryption ciphers are restricted to AES or 3DES. When FIPS is enabled, if the keyboard, mouse, or video encryption is set to 128-bit SSL or DES, the encryption level is automatically changed to AES. With FIPS enabled, the files are saved, or restored, using AES, a FIPS compatible algorithm. When FIPS is disabled, the User Database and Appliance Configuration files saved from or restored to the appliance as external files are encrypted, or decrypted, using DES.

The external files are encrypted even when the user does not fill in the Password parameter in the Save (or Load) dialog on the OBWI, in which case a default OEM password is used for encryption or decryption.

One result of enabling the FIPS module is to render previously saved User Database and Appliance Configuration files incompatible. In this case, temporarily disable the FIPS module.

To disable the FIPS module:
1. Reboot the appliance.
2. Restore the previously saved database or configuration file.
3. Re-enable the FIPS module.
4. Reboot the appliance.
5. Save the file externally again while the FIPS module is enabled.

The new saved external file is compatible with the appliance as long as the appliance is running with the FIPS mode enabled. Database and configuration files saved with the FIPS module enabled are not compatible for restoring a database or configuration file to an appliance without the FIPS module enabled or to an appliance with older firmware not supporting the FIPS module.

Component identification

HP Server G2 Console Switch components
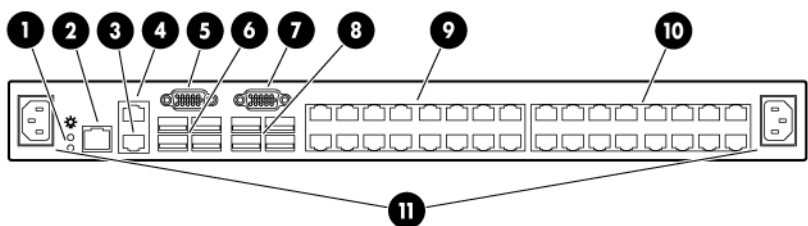
Item	Description
1	Power supply status indicator LEDs
2	LAN connector
3	Tiering chain port
4	RJ-45 serial setup port
5	Console A VGA connector
6	Console A USB ports
7	Console B VGA connector
8	Console B USB ports
9	Interface adapter ports (1-16)
10	Interface adapter ports (17-32)
11	Power connectors A & B

HP IP G2 Console Switch components

1x1Ex8
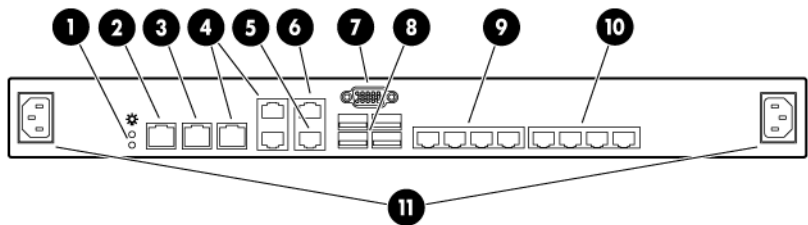
Item	Description
1	Power supply status indicator LEDs
2	LAN 1
3	LAN 2
4	S1, S2, and S3 (reserved for future use)
5	Tiering chain port
6	RJ-45 serial setup port
7	Local console VGA
8	Local console USB ports
9	Interface adapter ports (1-4)
10	Interface adapter ports (5-8)
11	Power connectors A & B

2x1Ex16 or 4x1Ex32
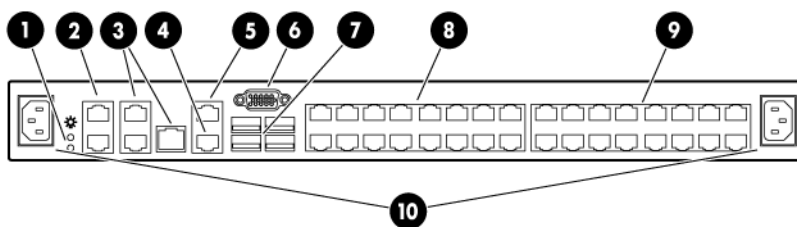
Item	Description
1	Power supply status indicator LEDs
2	LAN 1 and LAN 2
3	S1, S2, and S3 (reserved for future use)
4	Tiering chain port
5	RJ-45 serial setup port
6	Local console VGA
7	Local console USB ports
8	Interface adapter ports (1-16)
9	Interface adapter ports (17-32)
10	Power connectors A & B

Interface adapters

Interface adapters that support Virtual Media have two LEDs on the front of the RJ-45 connector.
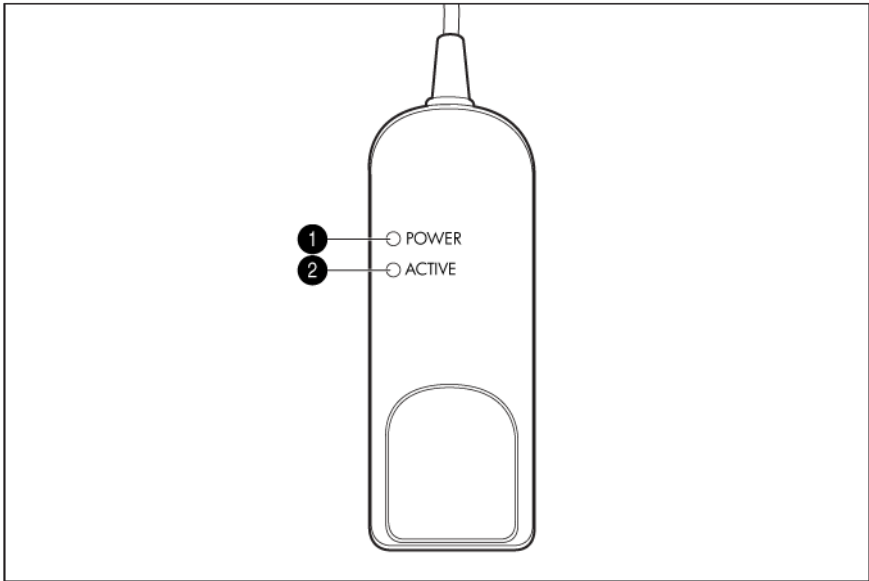
Item	Description
1	When lit, this LED indicates that the interface adapter has power from the server.
2	When lit, this LED indicates that there is an active console session with the interface adapter. When flashing, this LED indicates that the interface adapter firmware is being upgraded.

USB 2.0 interface adapter with Virtual Media
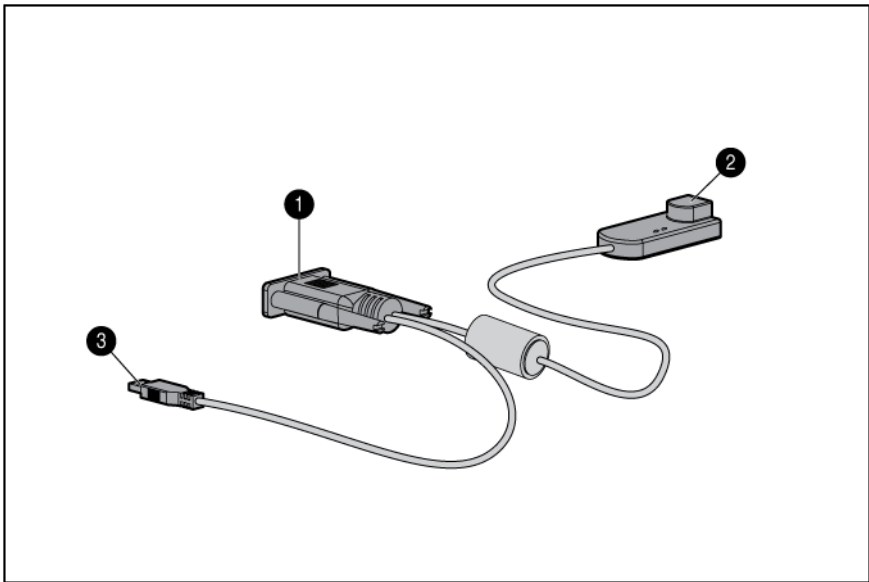
Item	Description
1	Video connector

Item	Description
2	RJ-45 connector
3	USB connector

PS2 interface adapter with Virtual Media
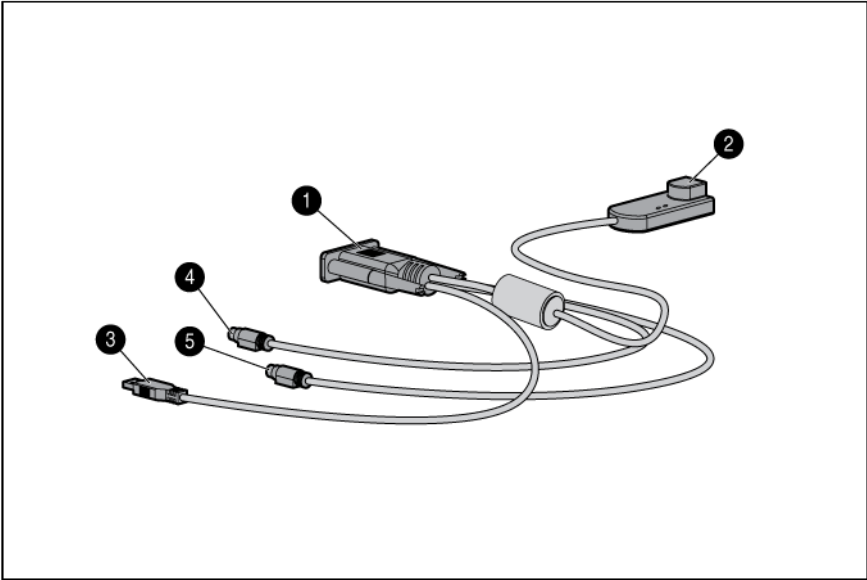
Item	Description
1	Video connector
2	RJ-45 connector
3	USB connector (for Virtual Media only)
4	Mouse connector
5	Keyboard connector

Serial interface adapter G2
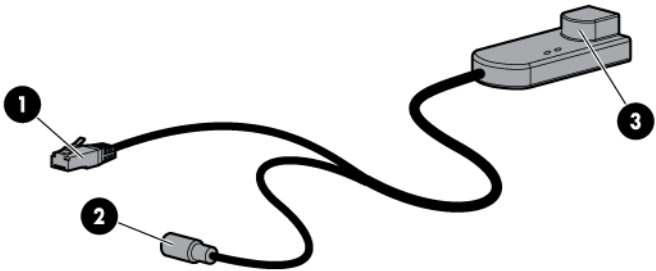
Item	Description
1	RJ-45 serial connector (to RJ-45/DB9 adapter or to a Cisco appliance)
2	Power connector (mate to USB power connector or power supply)
3	RJ-45 connector (for CAT5 to switch)

USB interface adapter with Virtual Media and CAC
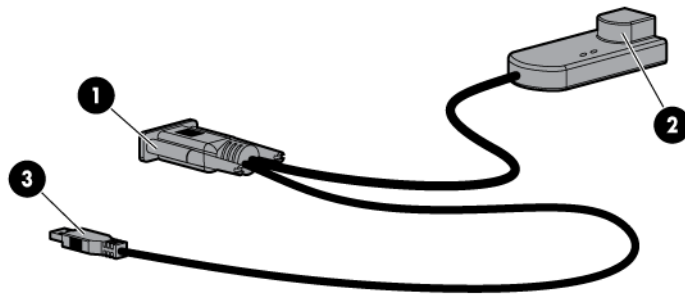
Item	Description
1	Video connector
2	RJ-45 connector
3	USB connector

PS2 interface adapter with Virtual Media and CAC
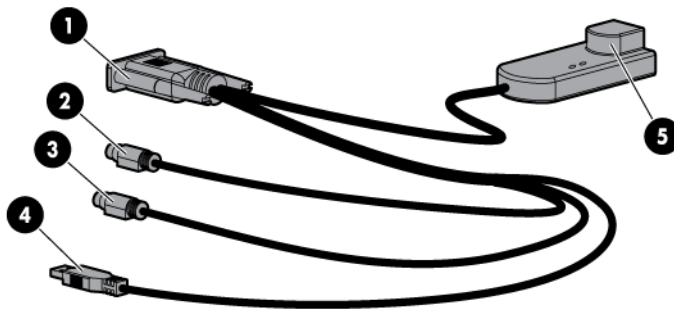
Item	Description
1	Video connector
2	Mouse connector
3	Keyboard connector
4	USB connector (for Virtual Media only)
5	RJ-45 connector

To determine which interface adapter you should use, see Selecting an interface adapter (on page 23).

Installing the console switch

Installation overview

This product ships with rack-mounting brackets for easy integration into the rack. Before installing this product and other components in the rack cabinet (if they are not already installed), stabilize the rack in a permanent location. Begin installing the equipment at the bottom of the rack cabinet, and then work to the top. Avoid uneven loading or overloading of the rack cabinets.

Rack-mount safety instructions

When rack-mounting a console switch, consider the following factors:

- Elevated operating ambient temperature—If the equipment is installed in a closed or multi-unit rack assembly, the operating ambient temperature of the rack environment might be greater than room ambient temperature. Install the equipment in an environment compatible with the operating temperature.

- Reduced air flow—In the rack, the rate of air flow required for safe operation of the equipment must not be compromised.

- Mechanical loading—Avoid a potentially hazardous condition caused by uneven mechanical loading by carefully mounting the equipment in the rack.

- Circuit overloading—When connecting the equipment to the supply circuit, consider the effect that overloading of the circuits might have on overcurrent protection and supply wiring. Consider the equipment nameplate ratings when addressing this concern.

- Reliable earthing—Maintain reliable earthing of rack-mounted equipment. Pay particular attention to supply connections other than direct connections to the branch circuit, such as the use of power strips.

Installation checklist

Before installation, refer to the following lists to be sure that all of the listed components were received.

Console switch kit contents

- Console switch
- Power cords
- Rack mounting kit
- CAT 5 serial adapter
- Documentation kit

This kit might contain extra hardware for your convenience.

Required items not included

- Interface adapters ("Installing the interface adapter" on page 23)

  One interface adapter is needed for each server or device.
  - USB
  - PS2
  - Serial
  - HP BladeSystem
- UTP CAT 5 or better cable
- Cage nuts and M6 screws (included with your original rack hardware kit)

Required tools

The following tools are required for some procedures:

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

Rack-mounting the console switch

⚠ **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).

1. Before installing the console switch into the rack, connect the console switch to a power source using the power cords provided.

   An activity indicator light is displayed after a few seconds. If the activity indicator light does not display, be sure that the power cord is connected, and the power source is valid.
2. Choose one of the following configurations:
   - Standard-mount
   - Cantilever-mount
   - Side-mount

Performing a standard-mount installation

1. Remove the six screws, three on each side, from the console switch.

2. Attach the long 1U brackets to the console switch using four of the screws you removed. Discard the two remaining screws.
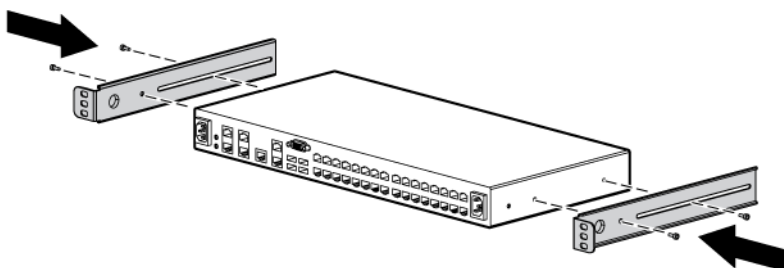
3. If not already installed, install a cage nut behind each rear rail.
4. Slide the console switch into the rear of the 1U product.
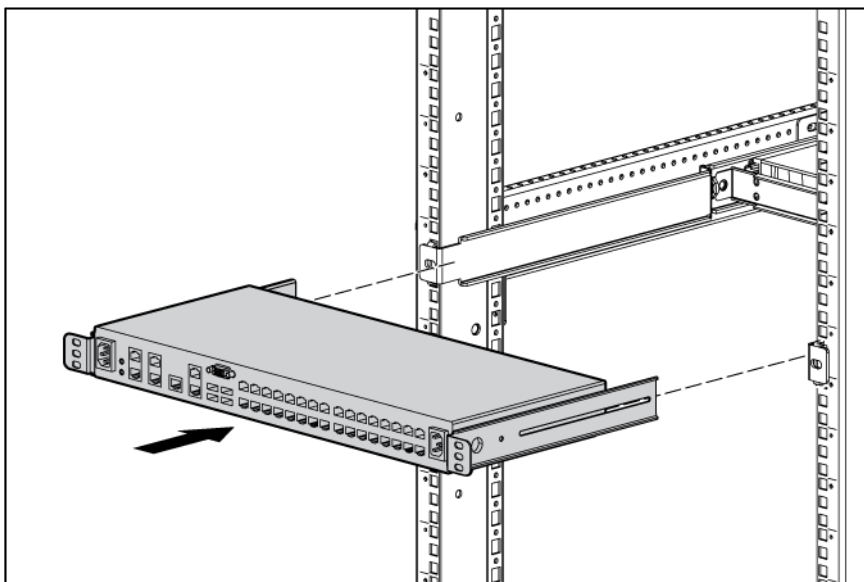
5. Secure the console switch to the rails using two M-6 screws, one on each side.
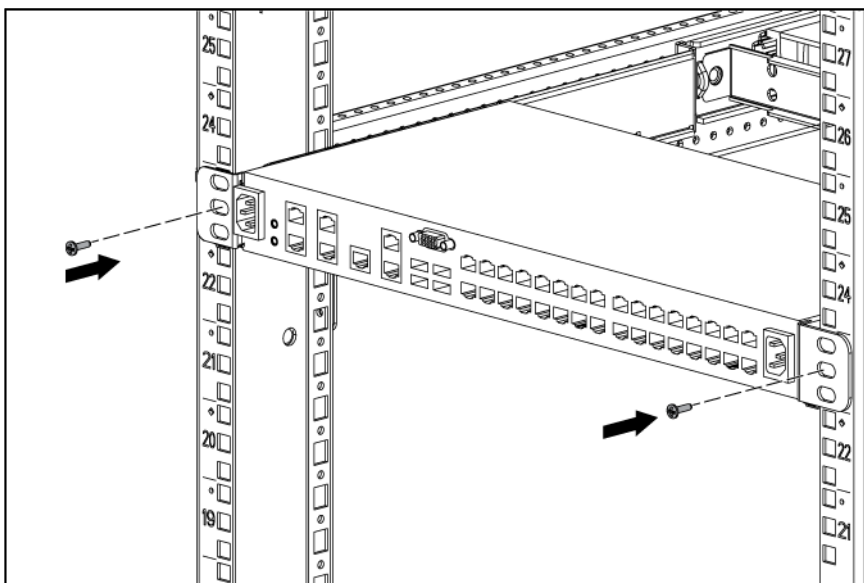
Performing a cantilever-mount installation

1. Remove the six screws, three on each side, from the console switch.
2. Attach the long 1U brackets to the console switch using four of the screws you removed. Discard the two remaining screws.
3. Install up to six cage nuts.
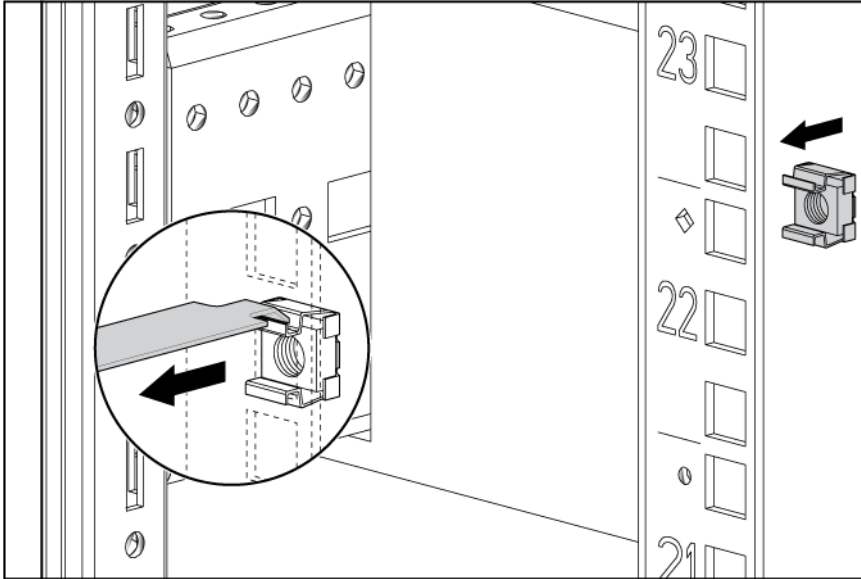
4. Secure the console switch to the rails using the appropriate number of M-6 screws.
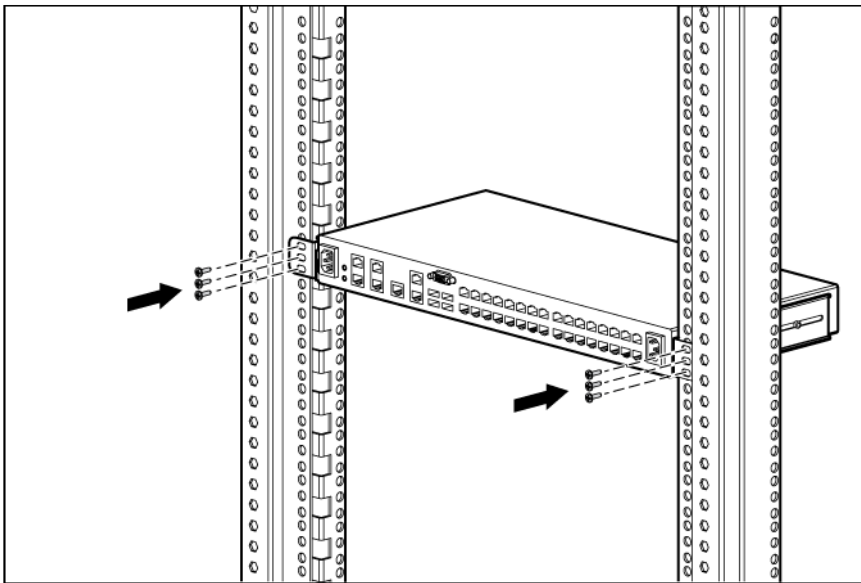
Performing a side-mount installation

1. Remove the six screws, three on each side, from the console switch.

2. Attach the side-mounting brackets to the console switch using four of the screws you removed. Discard the two remaining screws.
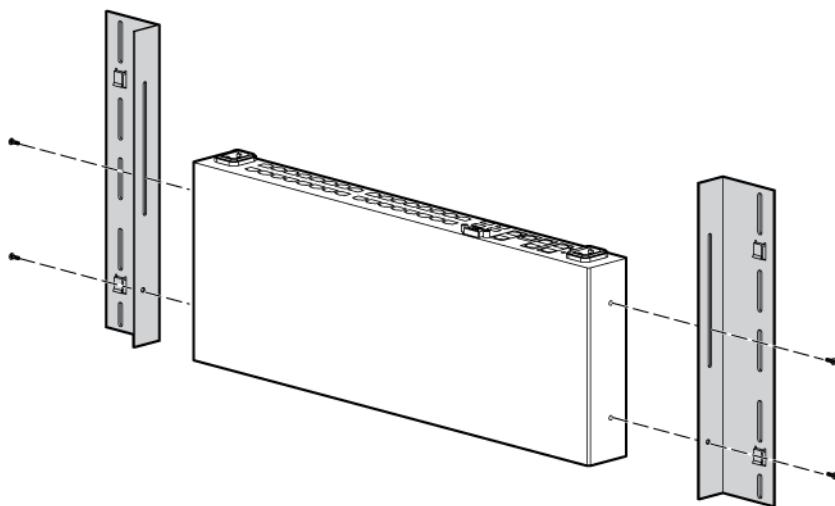
3. Slide the side-mounting bracket tabs into the U locations on each side of the rack.
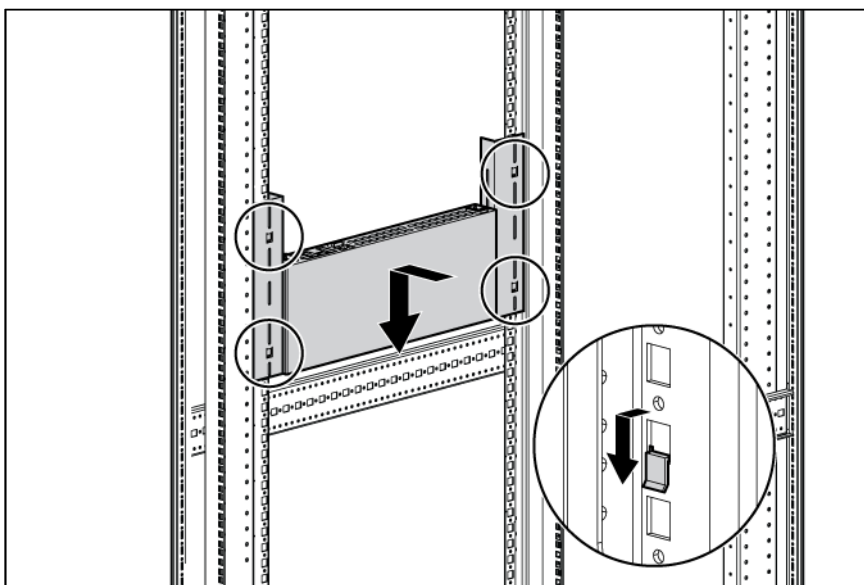
4. Install four cage nuts into the side-mounting bracket U locations.
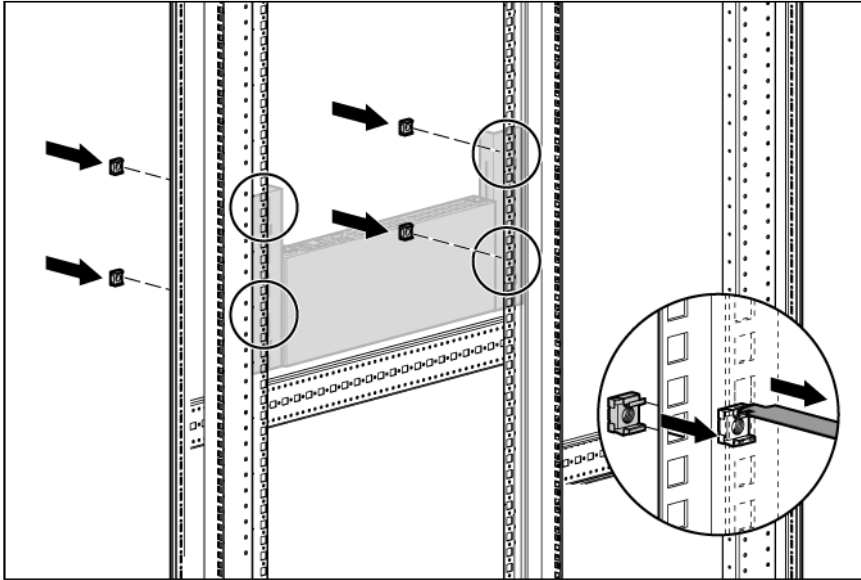
5. Secure the console switch to the rails, using four M-6 screws, two on each side.
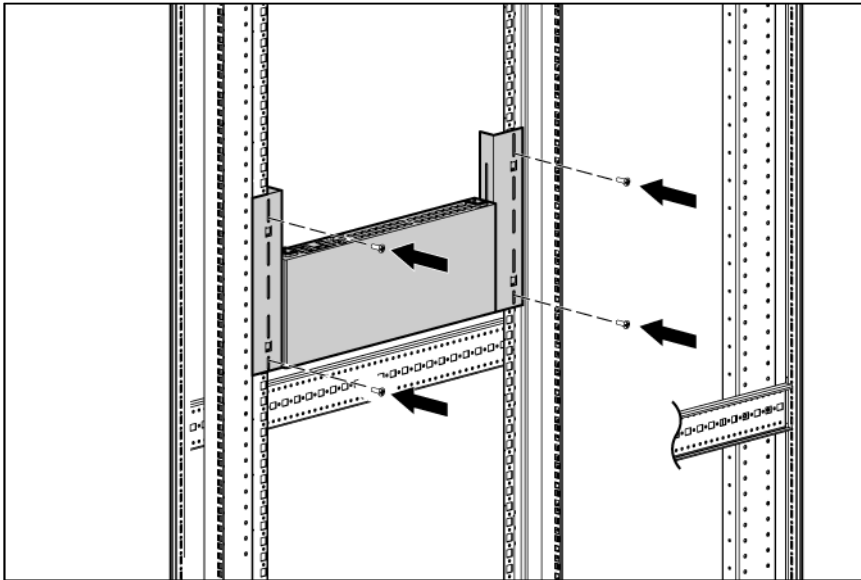
NOTE: Some racks enable you to use four sheet metal screws in place of M-6 screws and cage nuts.

Connecting the console switch

1. Connect the local keyboard, video, and mouse to the console switch.

WARNING: To reduce the risk of electric shock or damage to the equipment:
- Do not disable the power cord grounding plug. The grounding plug is an important safety feature.
- Plug the power cord into a grounded (earthed) electrical outlet that is easily accessible at all times.
- Unplug the power cord from the power supply to disconnect power to the equipment.
- Do not route the power cord where it can be walked on or pinched by items placed against it. Pay particular attention to the plug, electrical outlet, and the point where the cord extends from the storage system.

2. Plug the console switch power cord into a power source. The power supply status indicator LED illuminates.

NOTE: UTP CAT5 cables are used throughout the examples in this guide. However, UTP CAT5 or better cables can be used for any connection.

3. Connect a UTP CAT5 cable to the LAN connector on the console switch.

NOTE: For console switches that have 2 LAN connectors, you must connect them to 2 Ethernet switches on the same subnet.

4. Connect the other end of that same UTP CAT5 cable to an Ethernet switch.

The following figure shows one possible configuration for your console switch system.
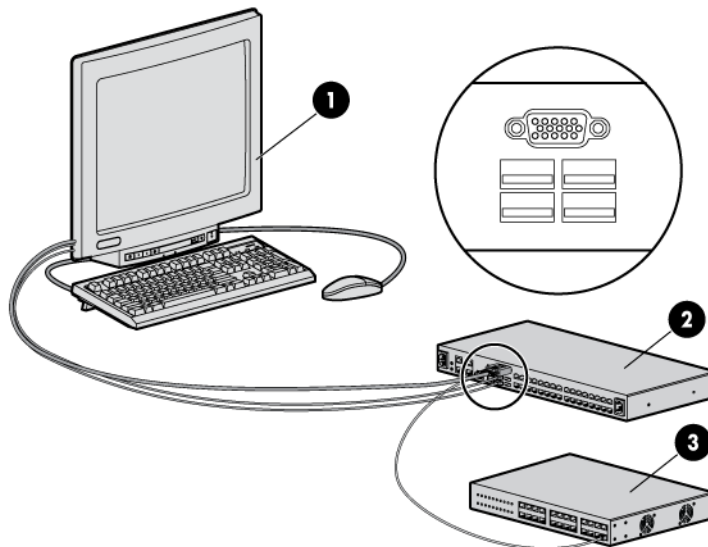
Item	Description
1	Local console
2	Console switch
3	Ethernet switch

Verifying connections

The following LEDs illuminate to indicate connection status.

Rear panel power status LEDs

The rear panel features two power supply status indicator LEDs. The LEDs illuminate green in the following patterns:

- Solid green—Both power supplies have power.
- Blinks Morse code SOS—The power supply whose indicator LED is not blinking does not have power or has failed.
- Blinks consistently—A firmware upgrade is in process.

Rear panel Ethernet connection LEDs

The rear panel of the switch features two LEDs that indicate the Ethernet connection for LAN1 and two LEDs that indicate the Ethernet connection for LAN2.

The green LEDs illuminate when a valid connection to the network is established and blink when activity occurs on the port.

The bi-color LEDs either illuminate green or amber.

- Green illumination—The communication speed is 1000 Mbps.
- Amber illumination—The communication speed is 100 Mbps.
- No illumination—The communication speed is 10 Mbps.

Virtual media and serial interface adapters LEDs

Typically, interface adapters feature two LEDs:

- Power LED—Illuminates green when the interface adapter is connected and receiving power.
- Active LED:
  - Illuminates green when the interface adapter is in an active session
  - Flashes green when the interface adapter firmware is flashed. Do not interrupt power to the interface adapter during a firmware update.

⚠ **CAUTION:** Do not disconnect an interface adapter during a firmware upgrade or power cycling. The interface adapter becomes inoperable and must be returned to the factory for repair.

HP IP Console Viewer overview

If you want the HP IP Console Viewer software to configure your console switch, you must install it. The HP IP Console Viewer enables you to remotely organize and manage your local KVM and serial appliances, as well as any device connected to them within your datacenter. For more information, see the *HP IP Console Viewer User Guide* included on the CD provided with this product.

NOTE: The local console port does not require the HP IP Console Viewer software for operation. The local console port uses the local console UI. For more information, see Configuring the console switch (on page 29).

The console switch system uses Ethernet networking infrastructures and the TCP/IP protocol to transmit keyboard, video, and mouse information between operators and connected computers. Although 10Base-T

Ethernet can be used, a dedicated, switched 100Base-T or 1000Base-T network provides improved performance.

Installing the interface adapter

Interface adapter overview

An interface adapter is required for the console switch system to function properly. However, an interface adapter is not included in the console switch kit. The interface adapter is connected to a console switch using a CAT5 cable.

> **NOTE:** UTP CAT5 cables are used throughout the examples in this guide. However, UTP CAT5 or better cables can be used for any connection.

Selecting an interface adapter

Several interface adapters are available for use with the console switch. The following chart describes the functionality and optimal uses for each adapter.

Interface adapter	Type	Part number	Prime function	Optimal use
HP c-Class Blade	Blade c-Class	AF605A	Local console access to a blade server	For server blades to connect to a KVM for local access
HP PS2	PS2	262588-B21	KVM console access	For servers that have PS/2 connectors
HP USB	USB	336047-B21	KVM console access	For servers that have USB connectors
HP Serial	Serial	373035-B21	Connecting to a serial interface	For managing serial devices through a serial interface
HP PS2 with Virtual Media	PS2M	AF604A	KVM and Hi-Speed Virtual Media (approximately 12x CD-ROM) for servers with PS/2 connectors	For servers that have PS/2 connectors and require Hi-Speed Virtual Media
HP USB with Virtual Media*	USB2	AF603A	KVM and Hi-Speed Virtual Media (approximately 12x CD-ROM) for servers that do not have PS/2 connectors	For servers that do not have PS/2 connectors, but require Hi-Speed Virtual Media
HP PS2 with Virtual Media and CAC	PS2MC	AF624A	Full-Speed Virtual Media (approximately 6x CD-ROM) and CAC support for servers with PS/2 connectors	For servers that have PS/2 connectors and require Full-Speed Virtual Media and CAC support
HP USB with Virtual Media and CAC	USBMC	AF623A	Full-Speed Virtual Media (approximately 6x CD-ROM) and CAC support for servers with USB connectors	For servers that have USB connectors and require Full-Speed Virtual Media and CAC support
HP Serial G2	True serial	AF625A	Provides access to the serial console	For servers that require access to the serial console and all serial-managed devices

*Not supported for use with HP ProLiant G7 servers or earlier

Connecting the interface adapter

> **NOTE:**   If you use the HP USB with Virtual Media interface adapter to connect to your ProLiant server, test the functionality of your keyboard and mouse at the BIOS level before you load your operating system.

1. Connect a UTP CAT5 cable to the interface adapter connection port on the console switch.
2. Connect the other end of that same UTP CAT5 cable to the RJ-45 connector on the interface adapter.
3. Connect the interface adapter to the appropriate connectors on the server.
4. Repeat steps 1 through 3 to connect any other servers or appliances to the console switch.

The following figure shows an example configuration for the console switch system with an interface adapter.
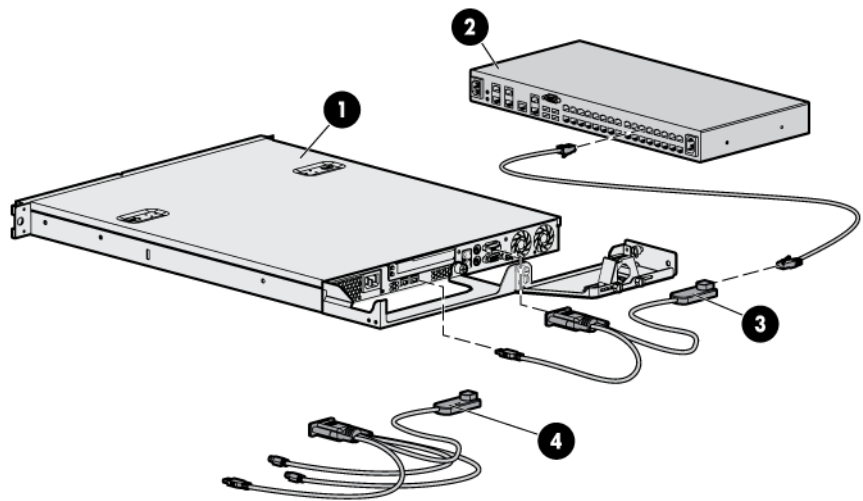
Item	Description
1	Server
2	Console switch
3	USB 2.0 interface adapter with Virtual Media
4	PS2 interface adapter with Virtual Media

Cascading console switches

Cascading console switches overview

The G2 console switches support two levels of cascading or tiering devices. You can cascade multiple console switches to increase the number of devices available from a single access point.

When cascading console switches with Virtual Media, verify the following:

- Interface adapters are not be used to cascade console switches. If interface adapters are used to cascade console switches, you do not have seamless integration, and you lose Virtual Media support. Use interface adapters with Virtual Media capability if you require Virtual Media.

- All cascaded console switches and interface adapters must have the most current firmware. To upgrade console switch firmware, see Upgrading the firmware.

Cascading console switches matrix

General rules of cascading console switches include:

- You can either cascade a newer console switch over an older console switch, or cascade switches of the same generation. An older console switch cannot be the primary console switch over a newer secondary switch.

- IP console switches cannot be cascaded under other IP console switches.

- In order for a particular feature to function, such as Virtual Media, all console switches and interface adapters in the cascade must support the feature.

  > **NOTE:** The Virtual Media speed on an interface adapter that also supports smart cards is only Full-Speed (approximately 6x CD-ROM). To use Hi-Speed Virtual Media (approximately 12x CD-ROM), you must use a Virtual Media only interface adapter.

For configurations to work properly, you must have an interface adapter with Virtual Media connecting each server to the console switch. For more information, see Using Virtual Media (on page 60).

HP Server Console Switches and Compaq Server Console Switches are not Virtual Media capable and cannot be used as a primary console switch over any of the Virtual Media capable console switches.

The following table shows several two-level cascade configurations.

Primary console switch	Secondary console switch	Supported features*
HP IP Console Switch G2 with Virtual Media	HP Server Console Switch G2 with Virtual Media	Virtual Media Smart Card
HP IP Console Switch G2 with Virtual Media	HP Server Console Switch with Virtual Media	Virtual Media
HP IP Console Switch G2 with Virtual Media	HP Server Console Switch G2	KVM
HP IP Console Switch G2 with Virtual Media	HP Server Console Switch	KVM

Primary console switch	Secondary console switch	Supported features*
HP Server Console Switch G2 with Virtual Media	HP IP Console Switch G2 with Virtual Media	Virtual Media Smart Card
HP Server Console Switch G2 with Virtual Media	HP Server Console Switch G2 with Virtual Media	Virtual Media Smart Card
HP Server Console Switch G2 with Virtual Media	HP Server Console Switch with Virtual Media	Virtual Media
HP Server Console Switch G2 with Virtual Media	HP Server Console Switch G2	KVM
HP Server Console Switch G2 with Virtual Media	HP Server Console Switch	KVM

*The listed supported features are only available if you cascade using an appropriate interface adapter that also supports the listed feature. For example, if you want Virtual Media support, you must use an interface adapter that supports Virtual Media.

Cascading two HP Server Console Switches G2

The following figure shows two HP Server Console Switches G2 cascaded together. The top console switch is the primary console switch and the bottom console switch is the secondary console switch.

Do not use interface adapters to cascade console switches. If interface adapters are used to cascade console switches, you do not have a seamless integration, and you lose Virtual Media support.
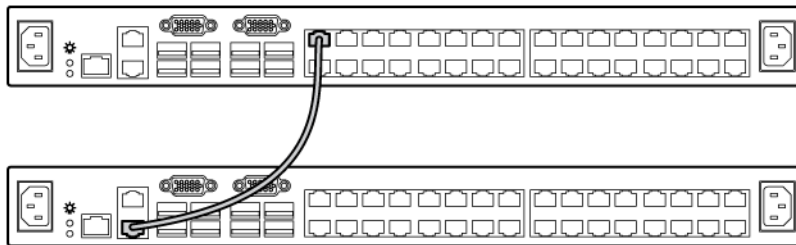
To cascade the console switches:
1. Connect a UTP CAT5 or better cable to the interface adapter port on the primary console switch.
2. Connect the other end of the cable to the tiering port on the secondary console switch.

Example of an HP Server Console Switch G2 cascade configuration
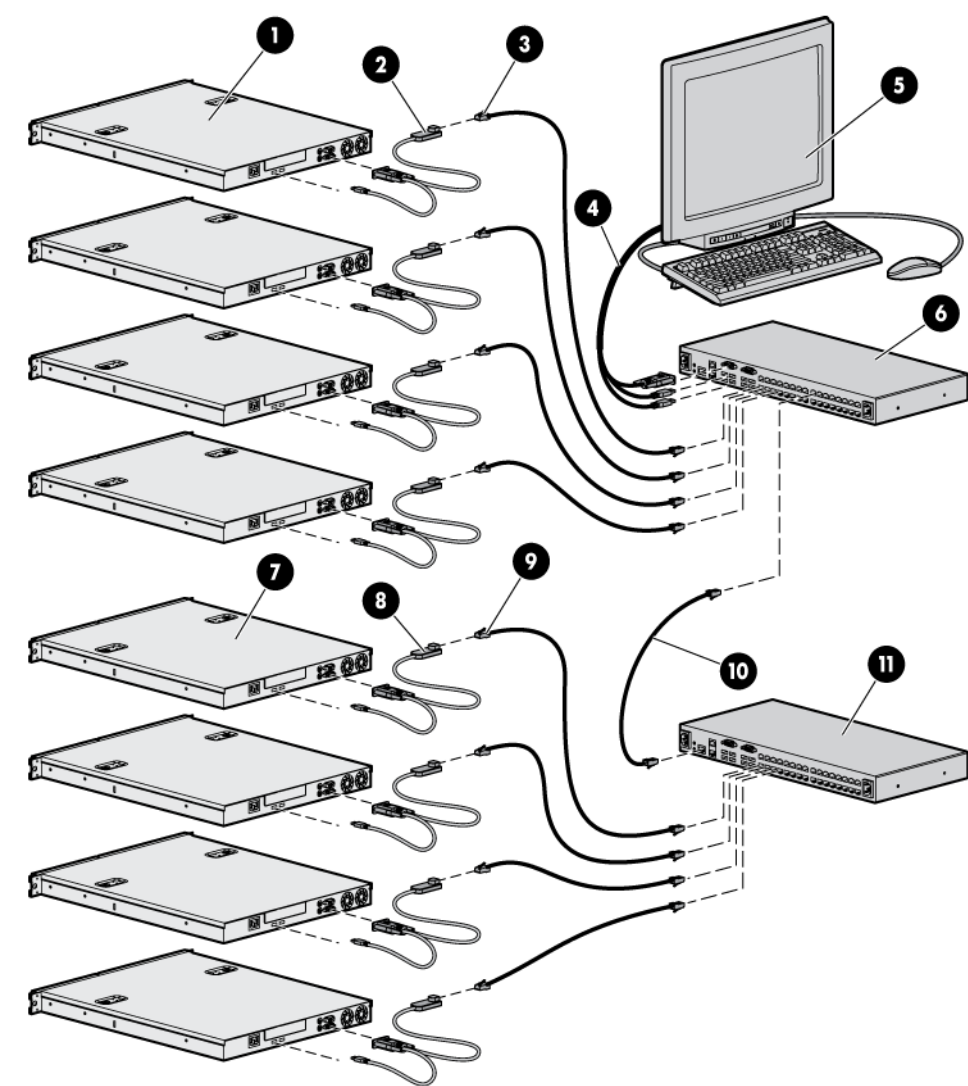
Item	Description
1	Servers
2	Interface adapters (USB 2.0 interface adapter with Virtual Media or PS2 interface adapter with Virtual Media)
3	UTP CAT5 cable
4	Local console KVM cables
5	Local console monitor
6	Primary console switch
7	Servers
8	Interface adapters (USB 2.0 interface adapter with Virtual Media or PS2 interface adapter with Virtual Media)
9	UTP CAT5 cable
10	UTP CAT5 cable (tiering cable)

Item	Description
11	Secondary console switch

Cascading an HP Server Console Switch G2 under an HP IP Console Switch G2

The following figure shows an HP Server Console Switch G2 cascaded to an HP IP Console Switch G2.

Do not use interface adapters to cascade console switches. If interface adapters are used to cascade console switches, you do not have a seamless integration, and you lose Virtual Media support.
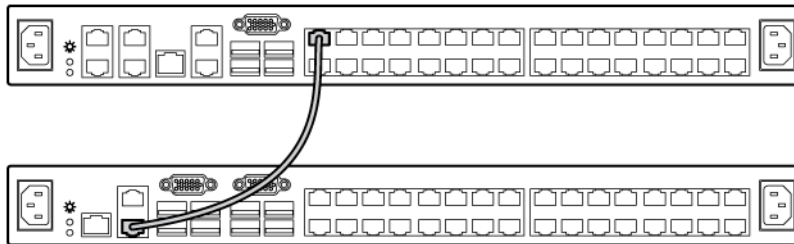
To cascade the console switches:

1. Connect a UTP CAT5 or better cable to the interface adapter port on the console switch.
2. Connect the other end of the cable to the tiering port on the secondary console switch.

Configuring the console switch

The user interfaces

To configure and manage your console switch, you can use either the local console UI or the remote OBWI.

The two user interfaces share a similar look and feel for optimal user experience. The information in this chapter applies to both user interfaces.

From the interface, you can configure the console switch for your specific application, manage attached devices, and handle all basic KVM or serial switching.

The following sessions are available from either interface:

- KVM—Enables you to control the keyboard, monitor, and mouse functions of individual target devices that are connected to the switch during real-time operation. For more information, see the *HP IP Console Viewer User Guide*.

- Serial—Enables you to manage individual target devices using the serial console.

Configuring the console switch using the local console UI

For detailed instructions on using the local console UI to configure the initial network setup, see Network settings (on page 36).

To launch the local console UI interface:

> **NOTE:** The HP IP and Server Console Switches G2 do not have PS/2 connectors for the keyboard and mouse. You must use USB connections for your keyboard, mouse, media devices, and smart card readers.

1. Connect your keyboard, monitor, and mouse to the local port on the rear of the console switch. For more information, see Connecting the console switch (on page 19).

   > **NOTE:** To change the keystrokes that launch the local console UI, see Local console UI settings (on page 41).

2. Select one of the keystrokes to launch the local console UI:
   - **PrtSc**
   - **Ctrl** + **Ctrl**

3. If local UI authentication is enabled, enter your username and password. The local console UI interface opens.

4. Configure the network settings for either IPv4 or IPv6. For more information, see General network settings (on page 36).

Configuring the console switch using the remote OBWI

The remote OBWI supports the following operating systems and browsers.

Operating System	Microsoft Internet Explorer version 9.0	Mozilla Firefox version 10 or later	Google Chrome version 19 or 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 and 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 Tiger (10.4+)	No	Yes	No

To log in to the remote OBWI:

1. Launch a web browser.

   If you are working in IPv6 mode, you must include square brackets around the IP address.

   Example: https://[XXX.XX.XX.XX]

2. In the address bar of the browser, enter the IP address or host name assigned to the switch you want to access.

   Examples: https://XXX.XX.XX.XX or https://hostname

   The default username is Admin with no password.

3. When the browser connects to the switch, enter your user name and password.

4. Select **Login**. The remote OBWI appears.

Connecting to the remote OBWI through a firewall

Any console switch installation that uses the remote OBWI for outside access must have four ports opened in a firewall.

TCP port number	Function
22	Used by SSH during serial sessions to an MPUIQ-SRL module
80	Used for the initial downloading of the Video Viewer (for downloading the Java™ applet)
443	Used by the web browser interface for managing the switch and launching KVM sessions
2068	Transmission of KVM session data or transmission of video on switches

In some configurations, the workstation is located outside of the firewall and the console switch is inside the firewall. To configure the firewall, forward ports 22, 80, 443, and 2068 from the external interface to the KVM switch through the firewall internal interface. For specific port forwarding instructions, see your firewall documentation.

Using the user interfaces

After you have successfully logged into either the local console UI or the remote OBWI, the user interface appears.
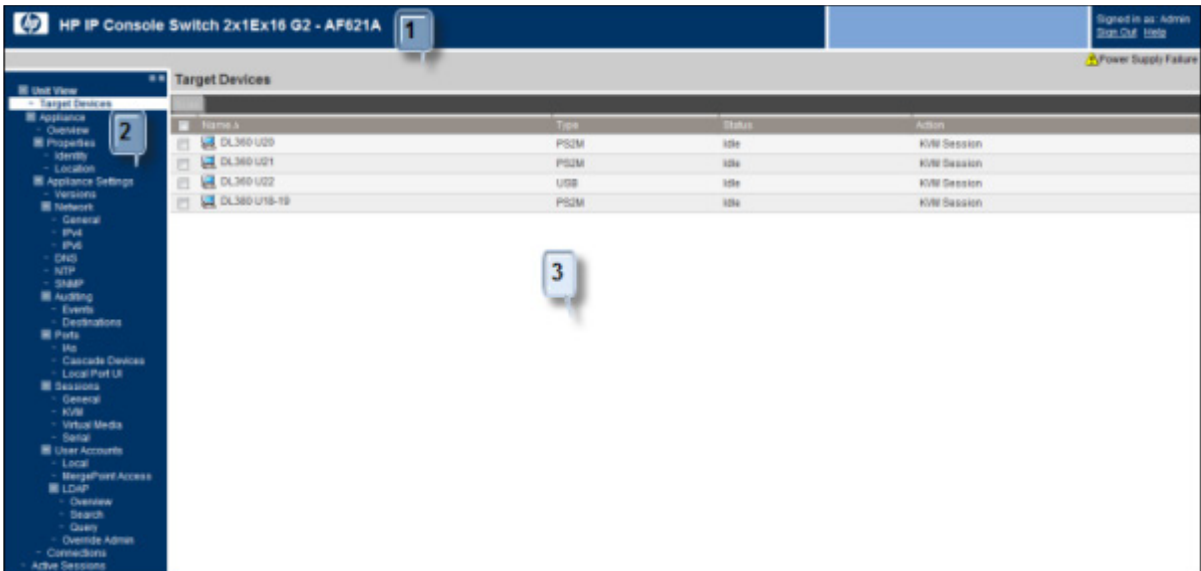
Callout	Component	Description
1	Heading bar	Displays the console switch you are logged into
2	Side navigation bar	Displays system information, available configuration and settings options, and operations.
3	Content area	Displays the content for the category selected in the side navigation bar

Local console user interface

The local console user interface has two modes for viewing the list of target devices:

- **Target list—Full** provides a full listing of the Interface adapter settings and information.
- **Target list—Basic** provides a basic view and allows faster selection of the target device using up and down arrow key navigation through the list and a search filter field to search by name.

The default view can be set in the Local Port UI settings page.

Target devices

> **NOTE:** The Target Devices page is the default view when you launch a console switch session, using either the local console UI or the remote OBWI.

The Target Device page enables you to view the name, type, and status of every interface adapter visible to the console switch. If you are connected to an HP IP Console Switch, you can launch a session with an interface adapter.

To view system information for the connected target devices:

1. Select **Unit View>Target Devices**. The Target Device page appears.

   > **NOTE:** HP recommends editing the interface adapter name so that it matches the name of the device it is connected to.

2. Select the name of the interface adapter you want to view. The Unit Overview page appears. The following properties appear:

   o Device name—Edit to match the name of the interface adapter it is connected to

   o Type—Lists the type of interface adapter

   o EID—Lists the identification number of the interface adapter

   o Sessions—Enables you launch an interface adapter session
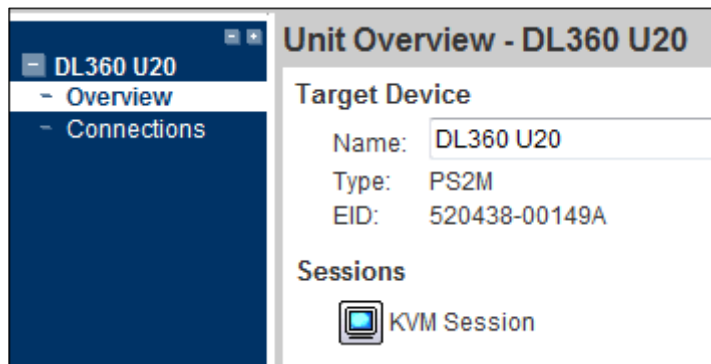
3. From the side navigation bar, select **Connections** to view the device connection path.

Filtering target devices

Filtering provides a shorter list of items. To filter the list of target devices, enter a text string to retrieve matching items. During filtering, the **Name** column is searched. The search is not case-sensitive. When filtering, you may use an asterisk (*) before or after text strings as a wild card. For example, entering **emailserver*** and clicking **Filter** displays items with emailserver at the beginning, such as emailserver and emailserverbackup.

Appliance tools

Select **Unit View>Appliance>Overview** to view the name and type of console switch you are logged in to.

You can also perform basic appliance tasks, using the following tools:

- Reboot
- Upgrade Firmware ("Upgrading the console switch firmware" on page 33)
- Run Diagnostics
- Ping

- Save Appliance Configuration ("Saving the console switch configuration or user database" on page 34)

- Restore Appliance Configuration ("Restoring the console switch configuration or user database" on page 35)

- Save Appliance User Database ("Saving the console switch configuration or user database" on page 34)

- Restore Appliance User Database ("Restoring the console switch configuration or user database" on page 35)

- Manage Appliance Web Certificate

- Save Application Trap MIB

Upgrading the console switch firmware

HP recommends updating your console switch with the latest firmware available.
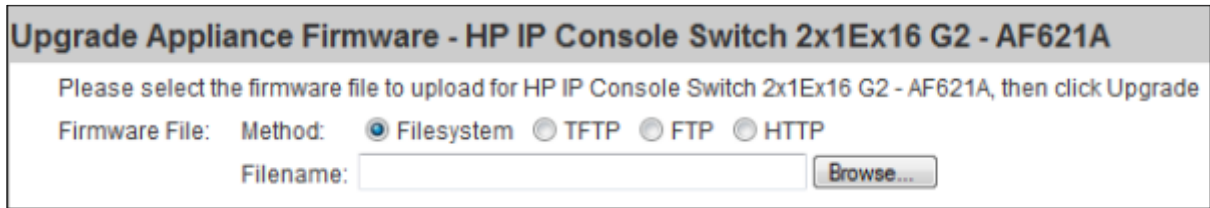
⚠ **CAUTION:** Do not disconnect an interface adapter during a firmware upgrade or power cycling. The interface adapter becomes inoperable and must be returned to the factory for repair.

After the Flash memory is reprogrammed with the upgrade, the console switch performs a soft reset, terminating all interface adapter sessions. Any console switch receiving a firmware update might appear disconnected or might not appear. The console switch appears again with a normal status once the Flash update is complete.

To update the console switch firmware:

1. Select **Unit View>Appliance>Overview**. The Unit Overview page appears.

2. From the Tools list, select **Upgrade Firmware**.

Upgrade Appliance Firmware - HP IP Console Switch 2x1Ex16 G2 - AF621A

Please select the firmware file to upload for HP IP Console Switch 2x1Ex16 G2 - AF621A, then click Upgrade

Firmware File: Method: ◉ Filesystem   ○ TFTP   ○ FTP   ○ HTTP

Filename: [   ] [Browse...]

> **NOTE:** The Filesystem option is only available if you are logged in from the remote OBWI.

3. Select one of the following options to load the firmware file:

   o **Filesystem**—Select Browse to specify the location of the firmware upgrade file.

   o **TFTP**—Enter the server IP address and firmware file to load.

   o **FTP**—Enter the server IP address and firmware file to load. A username and password is required for authentication.

   o **HTTP**—Enter the server IP address and firmware file to load. A username and password is required for authentication.

Saving the console switch configuration or user database

To save or restore the console switch configuration or user database, you must be logged in to the console switch from the remote OBWI. You can save the configuration of a switch, the managed devices, and the local user database to a file. By saving your configurations to a file, you can restore previous configurations to your console switch.

To save the console switch configuration or user database:

1. Select **Unit View>Appliance>Overview**. The Unit Overview page appears.

> **IMPORTANT:** While upgrading the firmware, do not power off the console switch or attempt any operations.

2. Select either **Save Appliance Configuration** or **Save Appliance User Database**. The Save Appliance Configuration or Save Appliance User Database page appears.

Save Appliance Configuration - HP IP Console Switch 2x1Ex16 G2 - AF621A

Select where the appliance configuration file should be saved for HP IP Console Switch 2x1Ex16 G2 - AF621A.

Configuration File: Method: ◉ Filesystem   ○ TFTP   ○ FTP   ○ HTTP PUT

Encryption Password: [   ]

3. Select the type and location where you want the file saved:

   o Filesystem

   o TFTP

   o FTP

   o HTTP PUT

4. Enter an Encryption Password.

Restoring the console switch configuration or user database

NOTE: To save or restore the console switch configuration or user database, you must be logged in to the console switch from the remote OBWI.

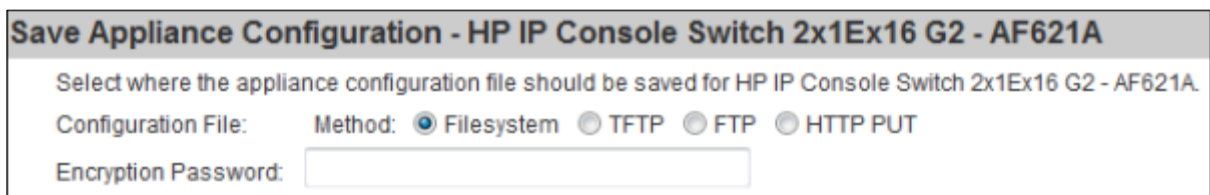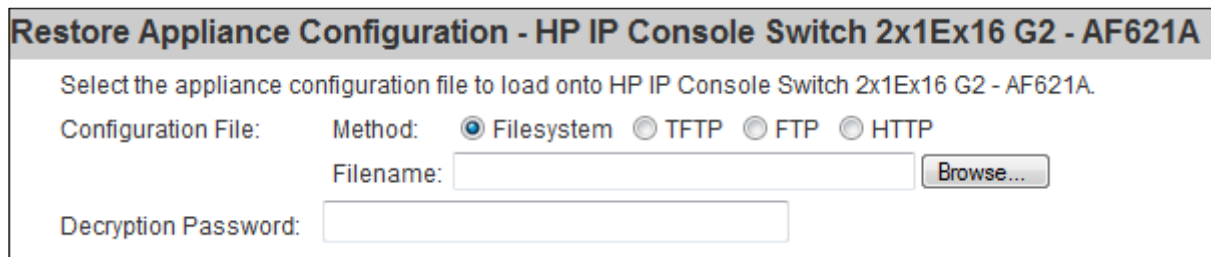To restore a previously saved console switch configuration or user database:

1. Select **Unit View>Appliance>Overview**. The Unit Overview page appears.

2. Select either **Restore Appliance Configuration** or **Restore Appliance User Database**. The Restore Appliance Configuration or Restore Appliance User Database page appears.

3. Select the type and location of the file you want to restore:
   - Filesystem
   - TFTP
   - FTP
   - HTTP

4. Enter the Decryption Password. The file is uploaded to the console switch.

5. Reboot the console switch ("Appliance tools" on page 32) to enable the restored configuration.

Viewing system information

1. Select **Unit View>Appliance>Properties>Identity**. The following properties appear:
   - Part number
   - Serial number
   - EID

   NOTE: HP recommends completing the Location information for the appliance, so that all appliances can be logically organized in the software.

2. Select **Unit View>Appliance>Properties>Location**. The following properties appear:
   - Site
   - Department
   - Location

3. Select **Unit View>Appliance Settings>Versions** to view the current firmware version. The current firmware version is listed under the Application Version. The larger the version number, the more current the firmware.

System alerts

In the top right-hand header of the interface, any current system alert appears.

⚠ Power Supply Failure
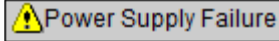
The following alerts might appear:

- Power supply failure
- Elevated ambient temperature
- Fan failure

Network settings

Only Administrators can make changes to the network settings. All other users can view network settings, but cannot make changes.

General network settings

To configure General network settings:

1. Select **Unit View>Appliance>Appliance Settings>Network>General**. The Appliance General Network Settings page appears.
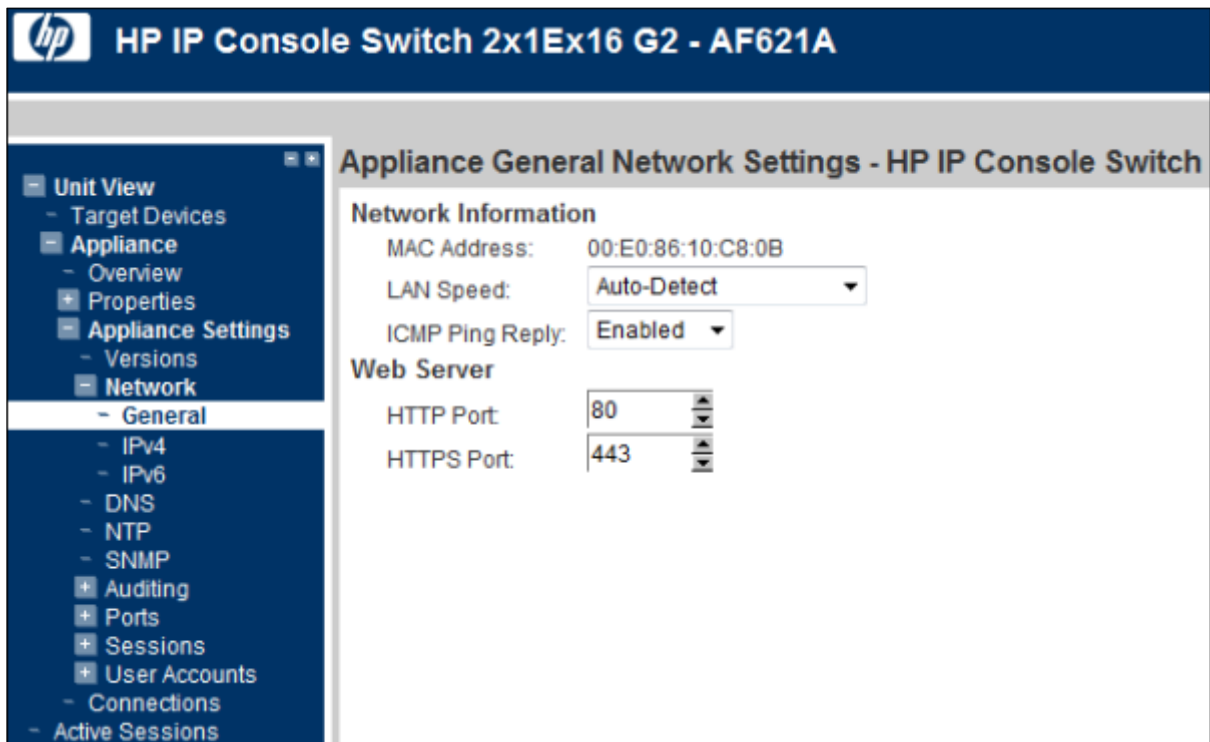
NOTE: If you change the LAN speed, you must reboot the console switch.

2. Configure the following parameters:
   - LAN Speed

- o   ICMP Ping Reply
- o   HTTP Port
- o   HTTPS Port

3. Configure the network settings for either IPv4 or IPv6 mode. The default setting is IPv4 with BOOTP enabled. The console switch is dual-stack capable, so both can be configured simultaneously.

DNS settings

To configure DNS settings:

1. Select **Unit View>Appliance>Appliance Settings>DNS**. The Appliance DNS Settings page appears.
2. Select the DNS Assignment Mode:
    - o   Manual
    - o   BOOTP
    - o   DHCPv6
3. Enter the DNS server addresses in the Primary, Secondary, and Tertiary fields.

NTP settings

To configure NTP settings:

1. Select **Unit View>Appliance>Appliance Settings>NTP**. The NTP page appears.
2. To enable NTP, select the **Enable NTP** checkbox.
3. Enter the name/address of the NTP servers in the NTP Server 1 and NTP Server 2 fields.
4. To enable the update interval, select the checkbox, and select the number of minutes for the update interval.

SNMP settings

SNMP is a protocol used to communicate management information between network management applications and the console switch. Other SNMP managers can communicate with your switch by accessing MIB-II and the public portion of the enterprise MIB. You can designate which stations can manage the switch as well as receive SNMP traps from the switch. If you enable SNMP, the console switch responds to all SNMP requests over UDP port 161.

To configure your SNMP settings:

1. Select **Unit View>Appliance>Appliance Settings>SNMP**. The SNMP page appears.

2. To enable SNMP, select the **Enable SNMP** checkbox.

3. Enter the appropriate information in the following fields:

    o   Name

    o   Description

    o   Contact

    > **NOTE:** The community name fields can be up to 64 characters in length. If SNMP is enabled, these fields cannot be left blank.

4. Enter the Read, Write, and Trap community names to specify the community strings that must be used in SNMP actions. These community names only apply to SNMP over UDP port 161, and they act as a password to protect the console switch.

    > **NOTE:** To enable any workstation to manage the console switch, leave the Allowable Managers fields blank.

5. In the Allowable Managers fields, enter the addresses of up to four workstations that are allowed to manage this console switch.

Enabling SNMP traps

An SNMP trap is a notification sent by the console switch to a management station indicating that an event has occurred in the switch that might require attention.

To enable individual SNMP traps:

1. Select **Unit View>Appliance>Appliance Settings>Auditing>Events**. The Events page appears.
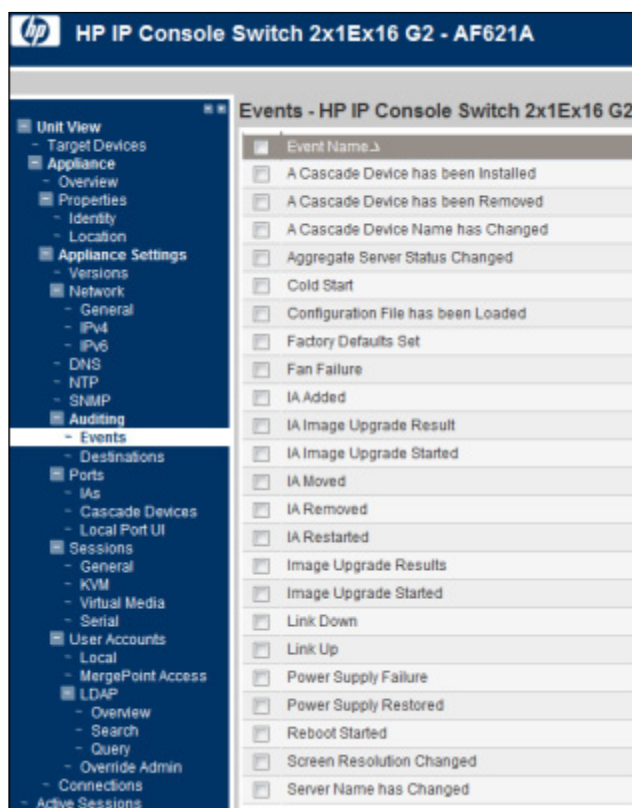
2. Select the checkbox for each SNMP trap you want sent to the management station.

3. Select **Unit View>Appliance>Appliance Settings>Auditing>Destinations**. The Event Destination page appears.
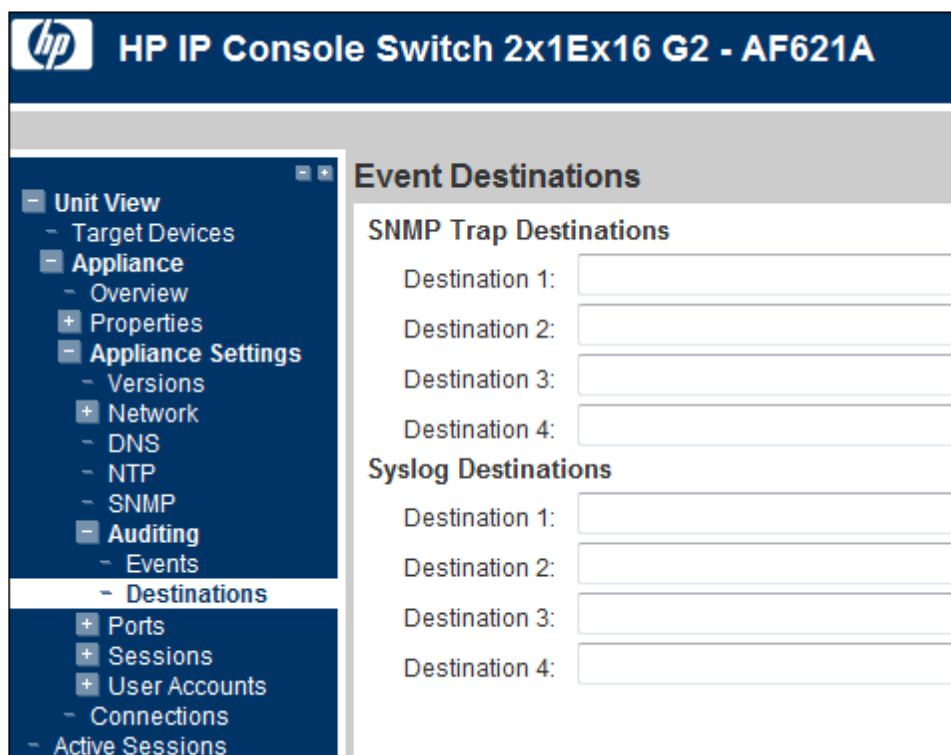
4. Enter up to four addresses of the management stations where you want the SNMP traps and Syslog information sent.

Ports

You can view and edit the information for the following console switch ports:

- Interface adapters
- Cascade devices
- Local console port UI

Interface adapter ports

To view the port location of each interface adapter attached to the console switch:

Select **Unit View>Appliance>Appliance Settings>Ports>IAs**. The Appliance IAs page appears.

Deleting offline interface adapters

1. Select **Unit View>Appliance>Appliance Settings>Ports>IAs**. The Appliance IAs page appears.
2. Select **Delete Offline**.

Configuring interface adapter USB speed

> **NOTE:** Configuring the interface adapter speed is only applicable to the HP USB with Virtual Media Interface Adapter (AF603A) and the HP PS2 with Virtual Media Interface Adapter (AF604A).

1. Select **Unit View>Appliance>Appliance Settings>Ports>IAs**. The Appliance IAs page appears.
2. Select the checkbox next to the interface adapter you want to edit.
3. Select either **Set USB 1.1 Speed** or **Set USB 2.0 Speed**.

Upgrading the interface adapter firmware

If Auto-Upgrade is enabled, interface adapters can be updated automatically when the console switch firmware is upgraded. If issues occur during the normal upgrade procedure, interface adapters might require a force upgrade.

> **⚠ CAUTION:** Do not disconnect an interface adapter during a firmware upgrade or power cycling. The interface adapter becomes inoperable and must be returned to the factory for repair.

To upgrade the interface adapter firmware:

1. Select **Unit View>Appliance>Appliance Settings>Ports>IAs**. The Appliance IAs page appears.
2. Select the checkbox next to the interface adapter you want to upgrade.
3. Select **Upgrade**.

Interface adapter serial session settings

To configure the serial session settings of an individual interface adapter:

1. Select **Unit View>Appliance>Appliance Settings>Ports>IAs**. The Appliance IAs page appears.
2. Select the interface adapter you want to configure, by clicking the name under the EID column. The IA page appears.
3. From the navigation tree on the left, select **Settings.** The IA Settings page appears.
4. Configure the following settings for the interface adapter:
   - Baud Rate
   - Data Bits
   - Parity
   - Stop Bits
   - Flow Control
   - DTR Mode
   - Pinout
     — If you are managing a Cisco device, select **Cisco** and connect the RJ-45 connector directly to the management port of the appliance.
     — If you are connecting to a DB9 Male DTE device, select **ACS** and connect the DB9 to RJ-45 adapter to the RJ-45 serial connector, and then connect it to the appliance.

Cascade devices ports

To view the port location of all cascaded appliances from the console switch:

Select **Unit View>Appliance>Appliance Settings>Ports>Cascade Devices**. The Appliance Cascade Devices page appears.

You can edit the names of the cascaded devices by selecting the **Name** hyperlink.

Local console UI settings

Only the Administrator can make changes to the local port UI settings, such as:

- Enabling/Disabling local port user authentication, requiring users to log in to the interface.
- Select a User Access Level, determining what user level can disconnect another user's KVM or serial session with a target device.

To configure local port UI settings:

1. Select **Unit View>Appliance>Appliance Settings>Ports>Local Port UI**. The Local Port UI Settings page appears.

2. In the Invoke Local Port UI, select the checkbox of one or more methods of launching a local console UI session.
3. Configure the following parameters:
   o Local port user settings
   o Scan mode
   o Keyboard
   o Setup port settings

Configuring sessions

You can configure settings for the following session types:

* General
* KVM
* Virtual Media
* Serial

Configuring General Session settings

1. Select **Unit View> Appliance> Appliance Settings> Sessions> General**. The Appliance General Session Settings page appears.

HP IP Console Switch 2x1Ex16 G2 - AF621A

Unit View
- Target Devices
- Appliance
  - Overview
  - Properties
  - Appliance Settings
    - Versions
    - Network
    - DNS
    - NTP
    - SNMP
    - Auditing
    - Ports
    - Sessions
      - General
      - KVM
      - Virtual Media
      - Serial
    - User Accounts
  - Connections
- Active Sessions

Appliance General Session Settings - HP IP Console Switch

Inactivity Timeouts

☑ Enable Inactivity Timeout

Inactivity Timeout (minutes):   15

Login Timeouts

Login Timeout (seconds):   120

Session Timeouts

☐ Enable Preemption Timeout

Preemption Timeout (seconds):   20

Sharing

☑ Enabled   ☐ Automatic   ☑ Exclusive   ☑ Stealth

Input Control Timeout (1/10 secs):   10

2.   Configure the following parameters:

o   In the Enable Inactivity Timeout checkbox, select or clear the checkbox.

o   In the Inactivity Timeout field, select the number of minutes of inactive time you want to pass before the session closes.

o   In the Login Timeouts field, select the number of seconds of inactive time you want to allow before failing an authentication request. For more information, see LDAP query (on page 51).

o   In the Enable Preemption Timeout checkbox, select or clear the checkbox.

o   In the Preemptive Timeout field, select the number of seconds you want to pass before the session times out.

o   In the Sharing field, select each checkbox you want to enable.

Configuring KVM Session settings

1. Select **Unit View> Appliance> Appliance Settings> Sessions> KVM**. The KVM Session Settings page appears.
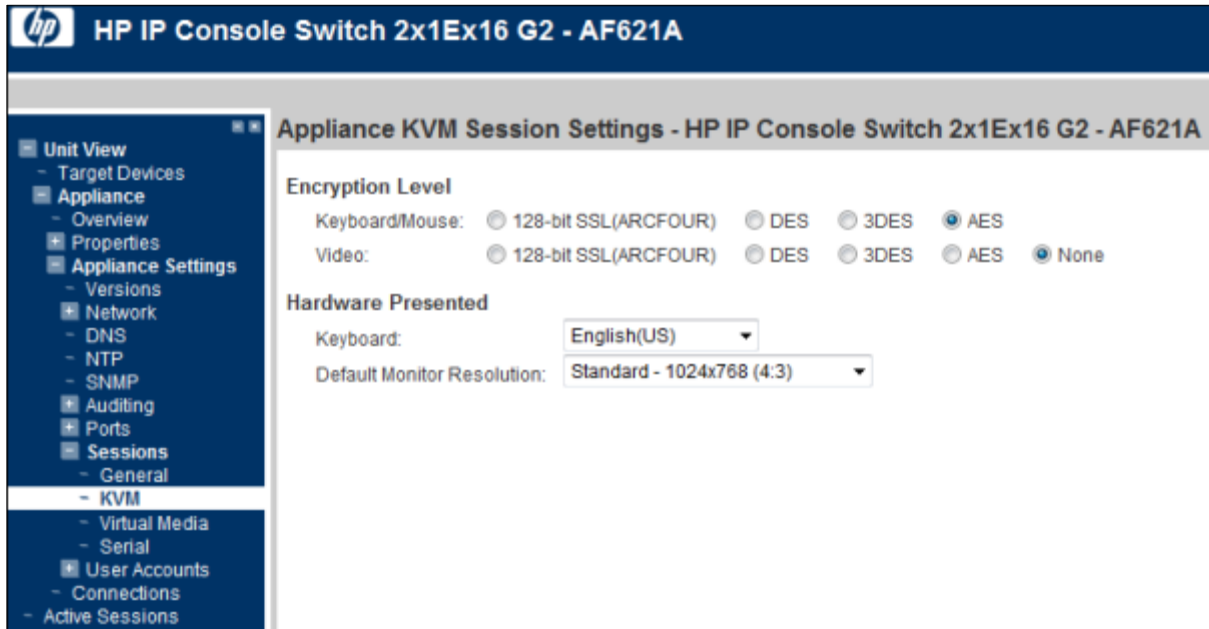
2. Configure the following parameters:
   o Select an Encryption Level for your keyboard and mouse.
   o Select an Encryption Level for your video.
   o Select the language of the keyboard you are using.
   o Select the monitor resolution you are using: either Standard or Widescreen. This resolution becomes the default resolution for the local console.

Configuring Virtual Media Session settings

NOTE: You can disable the Virtual Media functionality on an individual interface adapter for security purposes.

1. Select **Unit View> Appliance> Appliance Settings> Sessions> Virtual Media**. The Appliance Virtual Media Session Settings page appears.
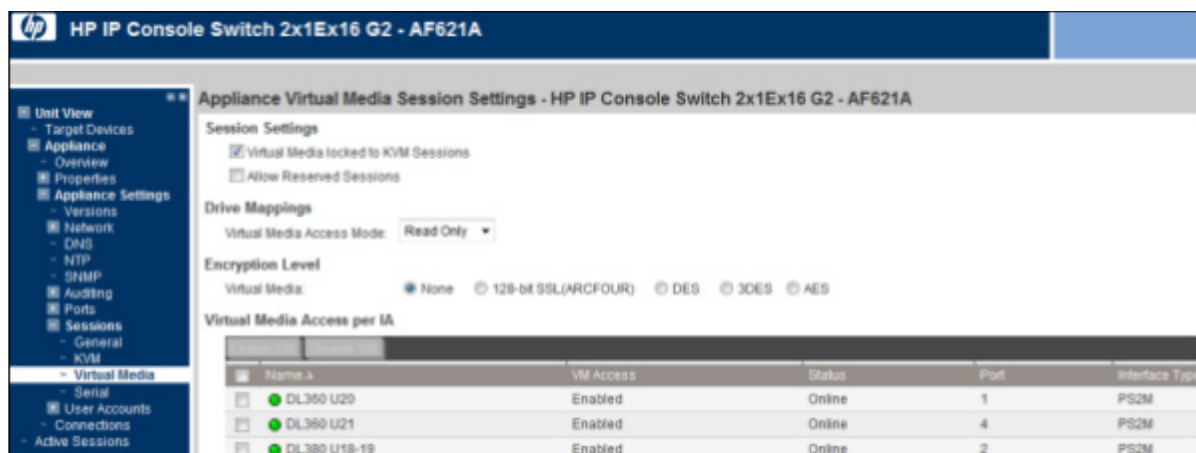
2. Configure the Session Settings:
   o Locked sessions—Locks the Virtual Media session to the KVM session. If you enable the Locked session setting, your Virtual Media session is disconnected if the KVM session is disconnected.
   o Reserved—Ensures that a Virtual Media connection can only be accessed by the user that established the session. If you enable the Reserved setting, no other use can create a KVM connection to that device.

3. Select the Virtual Media Access Mode:
   o Read Only
   o Read/ Write

4. Set the encryption level:
   o None
   o 128 bit
   o DES
   o 3DES
   o AES

Configuring Serial Session settings

1. Select **Unit View> Appliance> Appliance Settings> Sessions> Serial**. The Appliance Serial Session Settings page appears.
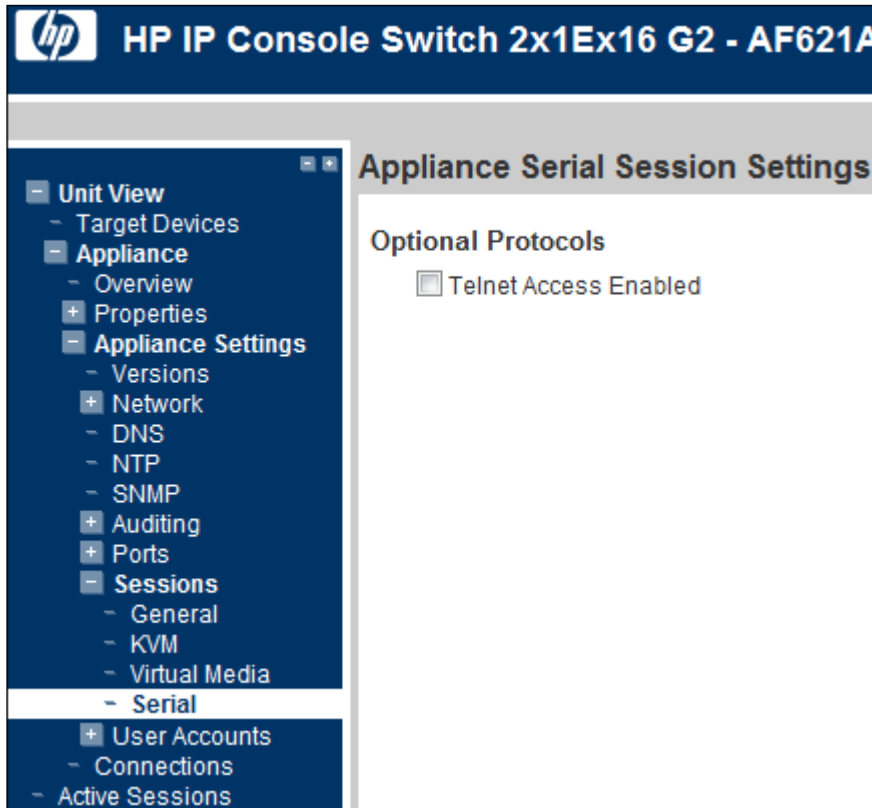

2. Select the Telnet Access Enabled checkbox, if you want to enable Telnet.

   SSH communication is enabled by default. To connect to the console switch using SSH, you must have a password assigned to the user account, as required by SSH.

   Telnet is not a secure communication protocol. However, you can use any Telnet or SSH compliant software, such as PuTTY or an OS command prompt to connect to the console switch. After authentication, you are prompted for the name of the interface adapter you want to connect to.

Setting up serial access from a command line

For serial access from a command line or using a utility like PuTTY, set up a connection with the KVM by starting an SSH session with KVM.

    Example: *SSH 192.168.1.222*

At the login prompt, provide the user and the target information in the following syntax:

    user:target

The target can either be the name of the serial interface adapter or the EID of the adapter.

    Example: demouser: DL380G8-Dev2 (case-sensitive)

User accounts

The local console UI and remote OBWI require login security through administrator-defined user accounts. Administrators can add or delete users, as well as define users' preemption and access levels.

The following allowed operations are defined by user level:

Operation	Access level: Appliance Administrator	Access level: Users
Configure interface system-level settings	Yes	No
Configure access rights	Yes	No
Add, change, and delete user accounts	Yes	No
Change your password	Yes	Yes
Access target device	Yes	Yes*

*Users can access a target device as long as the administrator has not reserved the device. For more information, see Local virtual media settings.

Local user accounts

To configure local user accounts:

1. Select **Unit View>Appliance>Appliance Settings>User Accounts>Local**. The Appliance Local User Accounts page appears.

2. Configure Security Lock-outs. If you enable security lock-outs, the lock-out is activated on the fifth failed login attempt, per user account.

To add a user:
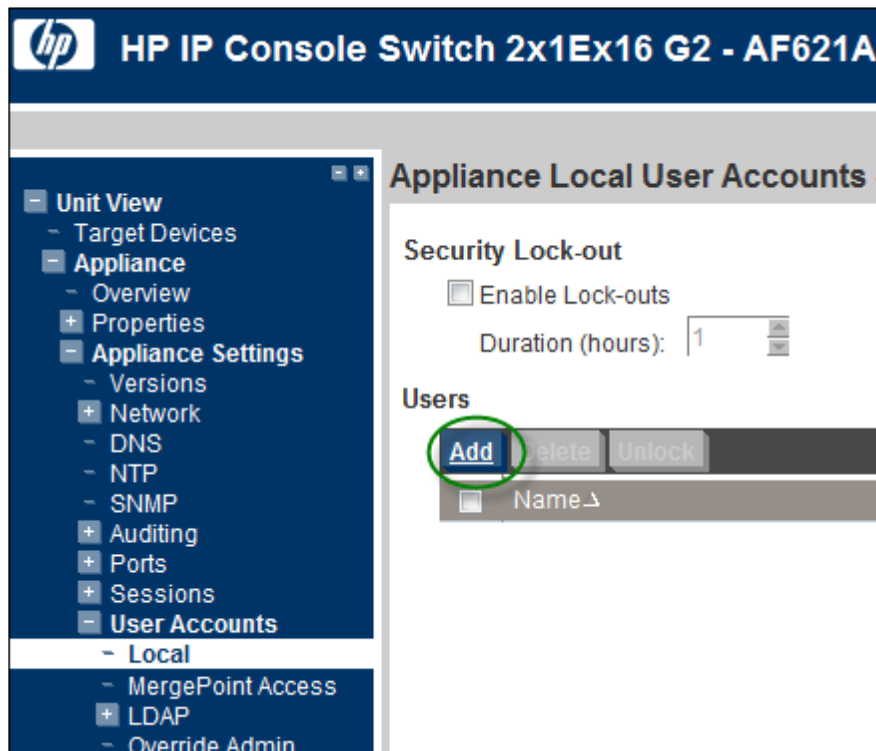
1. Select **Add.** The Add Appliance Local User Account page appears.

2. Enter the Username and Password of the new user.
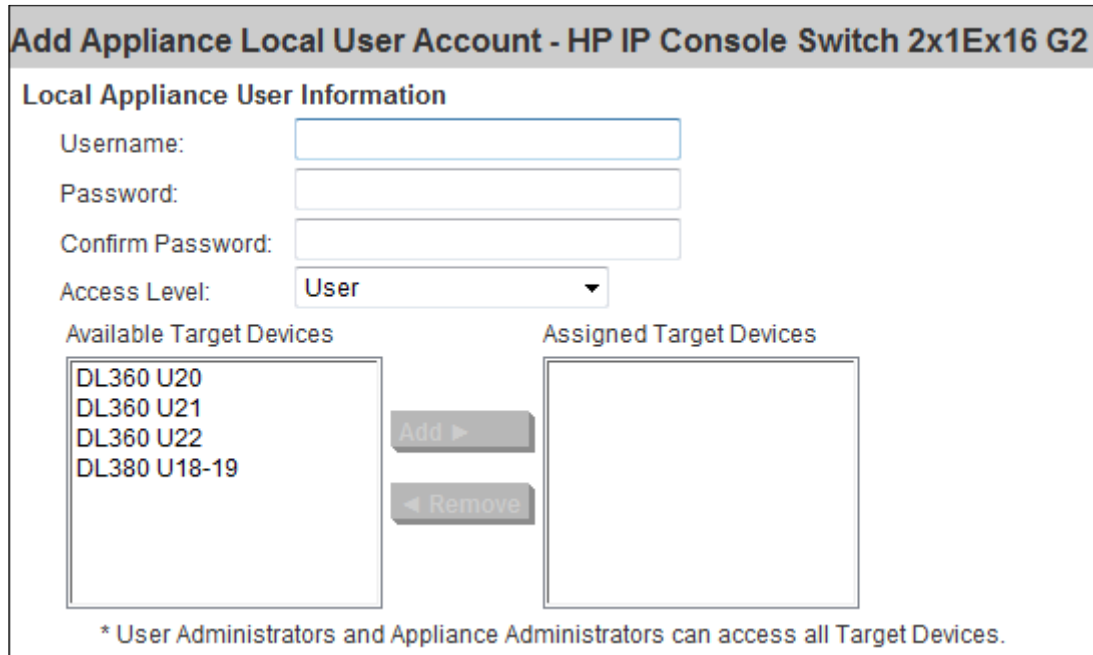3. Select the Access Level.
4. Highlight all available target devices the user is assigned to, and then select **Add.**

To edit a user:

1. Select the checkbox next to the user you want to edit.
2. Select **Edit,** and then modify the user account.

To delete a user:

1. Select the checkbox next to the user you want to delete.
2. Select **Delete.**

MergePoint Access settings

Use MergePoint Access Settings to connect to Avocent DSView software.

To configure MergePoint Access settings:

1. Select **Unit View>Appliance>Appliance Settings>User Accounts>MergePoint Access**. The Appliance MergePoint Access Settings page appears.
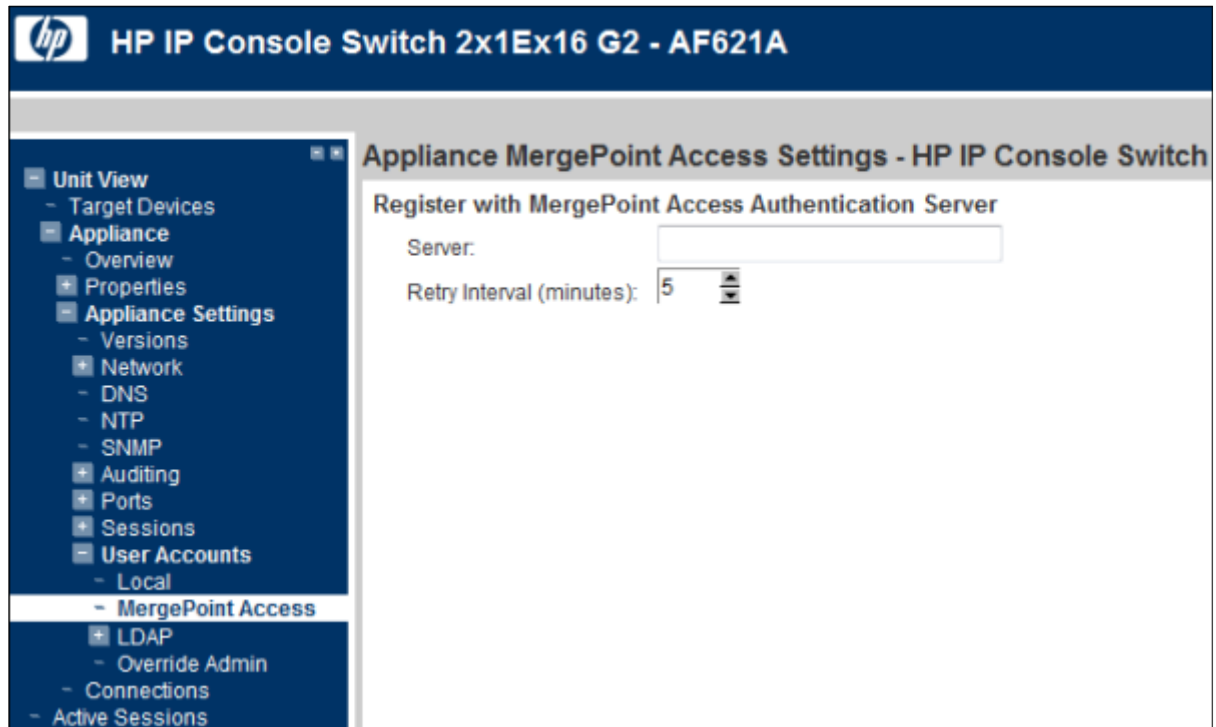
2. Configure MergePoint Access settings.

Configuring LDAP

> **NOTE:** Unless otherwise specified, use the LDAP default values, unless Active Directory has been reconfigured. Modifying the default values might cause LDAP authentication server communication errors.

You can configure the LDAP authentication priority and server connection information.

1. Select **Unit View>Appliance>Appliance Settings>User Accounts>LDAP**. The Appliance LDAP Overview page appears.

2. Configure the LDAP authentication priority by selecting either **Use Local Authentication** or **Use LDAP Authentication**.

> **NOTE:** The secondary LDAP server is optional.

3. Configure the LDAP servers information:
   o Address—Specifies the host names or IP addresses of the primary and secondary LDAP servers.
   o Port—Specifies the UDP port numbers that communicate with the LDAP servers. The default port ID for non-secure LDAP is 389 and the default port ID for secure LDAPS is 636.
   o Access Type—Specifies how a query is sent to each LDAP target device. When using LDAP, all usernames, passwords, and other information sent between the LDAP server and the target device are sent as non-secure clear text. Use LDAPS for secure encrypted communication.

For more information about LDAP configuration, see the *HP IP Console Viewer User Guide*.

LDAP search

To configure the parameters when searching for LDAP directory service users:

1. Select **Unit View>Appliance>Appliance Settings>User Accounts>LDAP>Search**. The Appliance LDAP Search page appears.

> **NOTE:** The LDAP Search and Query parameters can only be configured if LDAP Authentication is enabled on the LDAP Overview ("Configuring LDAP" on page 49) page.

2. Configure the Search parameters:
   o Search DN—Defines the administrator-level user that the target device uses to log into the directory service. Once the target device 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=DomainName, and dc=com. Each search value must be separated by a comma.
   o Search Password—Used to authenticate the administrator or user specified in the Search DN field.
   o Search Base—Defines a starting point from which all LDAP searches begin. The default values are dc=yourDomainName and dc=com. Each search value must be separated by a comma. For example, to define a search base for test.com, your values are dc=test, dc=com.
   o UID Mask—Specifies the search criteria for user ID searches of LDAP target devices. The format is <name>=<%1>. The default value is sAMAccountName=%1, which corresponds to Active Directory.

LDAP query

To configure LDAP query parameters:

1. Select **Unit View>Appliance>Appliance Settings>User Accounts>LDAP>Query.** The Appliance LDAP Query page appears.

> **NOTE:** The LDAP Search and Query parameters can only be configured if LDAP Authentication is enabled on the LDAP Overview ("Configuring LDAP" on page 49) page.

2. Configure the Query Mode parameters for:

   o Appliance—Used to authenticate administrators and users attempting to access the console switch itself.

   o Target Device—Used to authenticate users attempting to access attached target devices.
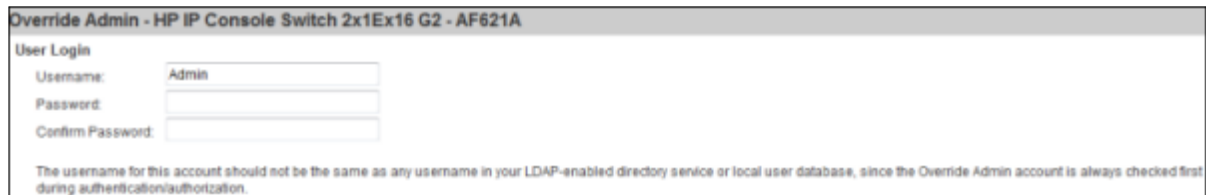
   There are three different modes available:

   o Basic—A username and password query for the user is sent to the directory service. Once verified, the user is given access to the appliance and any attached target devices.

   o User Attribute—A username, password, and Access Control Attribute query for the user is sent to the directory service. The Access Control Attribute is read from the user object in Active Directory. If no values are found, the user is given no access to the appliance or target devices, unless the user has User Admin privileges to the appliance.

   o Group Attribute—A username, password, and group query sent to the directory service for an appliance and attached target devices when using Appliance query mode or for a selected target device when using Target Device query mode. If a group is found containing the user and appliance name, the user is given access to either the appliance or target devices when using Appliance query mode. If a group is found containing the user and target device IDs, the user is given access to the selected target device when using Target Device query mode.

3. Configure the Group Configuration parameters:

- Group Container—Specifies the OU created in Active Directory by the administrator as the location for group objects. Group objects can contain users, computers, contacts, and other groups, each assigned with a certain access level.
- Group Container Mask—Defines the object type of the Group Container, normally an OU. The default value is ou=%1.
- Target Device Mask—Defines a search filter for the target device. The default value is cn=%1.
- Access Control Attribute—Specifies the name of the attribute used when the query modes are set to User Attribute or Group Attribute. The default value is info.
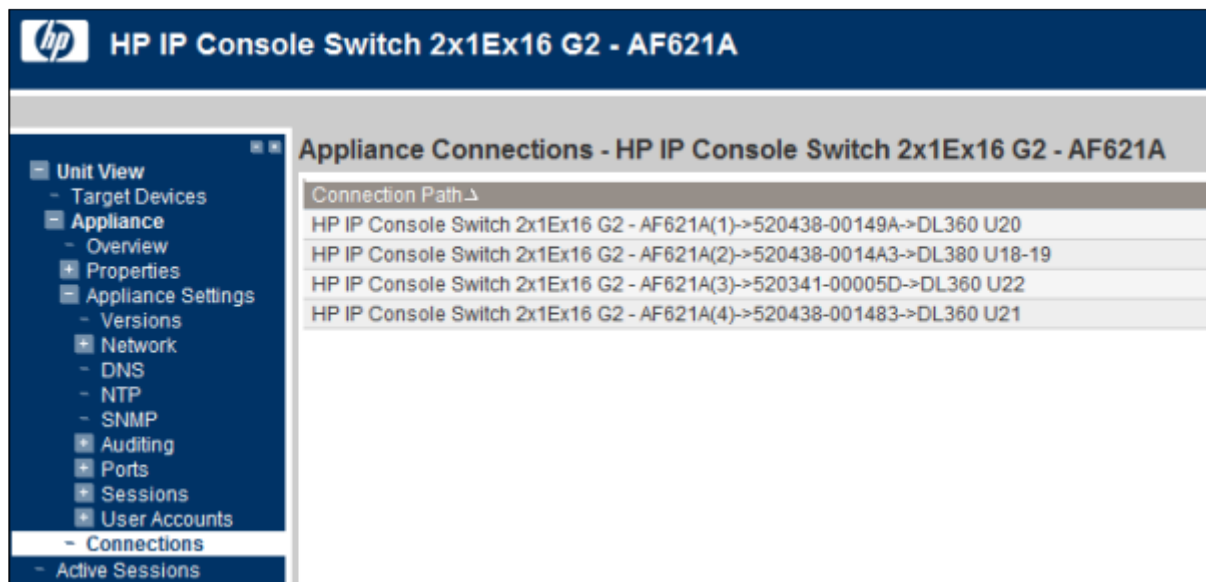
Override admin

The Override Admin account is the administrative account built in to the console switch. It only authenticates locally in the console switch.

Override Admin - HP IP Console Switch 2x1Ex16 G2 - AF621A

User Login

Username:	Admin
Password:	
Confirm Password:	

The username for this account should not be the same as any username in your LDAP-enabled directory service or local user database, since the Override Admin account is always checked first during authentication/authorization.

Connections

To view all connections from the console switch, select **Unit View>Appliance>Appliance Settings>Connections**. The Appliance Connections page appears.

HP IP Console Switch 2x1Ex16 G2 - AF621A

Appliance Connections - HP IP Console Switch 2x1Ex16 G2 - AF621A

Unit View
- Target Devices
- Appliance
  - Overview
  - Properties
  - Appliance Settings
    - Versions
    - Network
    - DNS
    - NTP
    - SNMP
    - Auditing
    - Ports
    - Sessions
    - User Accounts
  - Connections
- Active Sessions

Connection Path
HP IP Console Switch 2x1Ex16 G2 - AF621A(1)->520438-00149A->DL360 U20
HP IP Console Switch 2x1Ex16 G2 - AF621A(2)->520438-0014A3->DL380 U18-19
HP IP Console Switch 2x1Ex16 G2 - AF621A(3)->520341-00005D->DL360 U22
HP IP Console Switch 2x1Ex16 G2 - AF621A(4)->520438-001483->DL360 U21

Active sessions

To view a list of active sessions, select **Unit View>Active Sessions**. For each active session, the following properties appear:

- Target device—The device in active session.

- Owner—The user logged in and activating the session.
- Remote host—The IP address of the computer where the active session is running.
- Duration—Amount of time the device has been in active session.
- Type—The type of session (KVM or Serial)

To launch a new active session:

> **NOTE:** Java™ 1.5.0_11 or later is required to launch an active session when operating a Linux or Mac operating system.

1. Select **Unit View>Target Devices**. A list of available devices appears.
2. On the Target Devices screen, under the Action column, select either **KVM Session** or **Serial Session**.

   If the target device is currently in an active session, the user attempting to gain access can force a connection to the device if the user's preemption level is equal to or higher than the current user's.

Local sessions

After you have established an active session, you can view the Local Session page from the local console UI. The Local Session page only appears if there is an active session. The Local Session page provides the following features:

- Connect Virtual Media
- Reset the USB interface
- Resume an active session
- Disconnect the active session

To launch a new active session at the local console and access the Local Session page:

1. Select one of the keystrokes to launch the local console UI:
   - **PrtSc**
   - **Ctrl + Ctrl**

   The Local Session page appears.
2. Select **Unit View>Target Devices**. A list of available devices appears.
3. Select a different device and launch a **KVM Session**.

Scan mode

> **NOTE:** Scan mode is only available when you are using the local console UI or the HP IP Console Viewer software. If you are using remote OBWI, the Scan button is disabled.

In Scan mode, the console switch automatically scans from port to port (target device to target device). You can scan multiple devices or specify exactly which devices to scan. The scanning order is determined by the placement of target devices in the scanning list. You can also configure the time interval for the scan.

To add target devices to the scan list:

1. Select **Unit View>Target Devices**. The Target Devices page appears.
2. Select the checkbox next to each device that you want to scan.
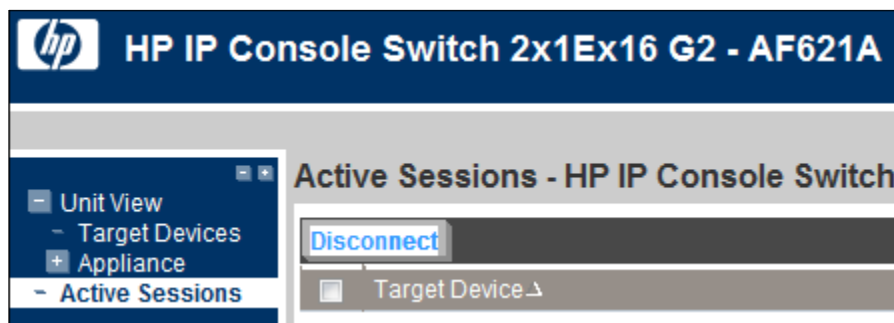
3. Select **Scan.**
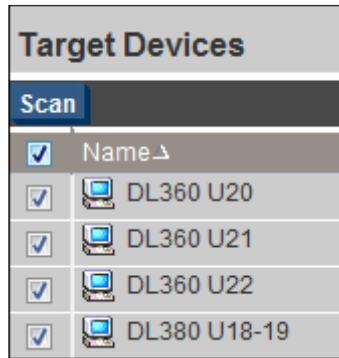
To configure the scan time interval, see Local console UI settings (on page 41).

Disconnecting an active session

1. Select **Unit View>Active Sessions**. The Appliance Sessions page appears.

2. Select the checkbox next to the target device session you want to close.

3. Select **Disconnect.**

Video Session Viewer

The Video Session Viewer overview

The Video Session Viewer is used to conduct a KVM session with target devices attached to a console switch using the remote OBWI. When you connect to a target device using the Video Session Viewer, the device desktop appears in a separate window containing both the local and target device cursors.

> **NOTE:** Java™ 1.5.0_11 or later is required to launch an active session when operating a Linux or Mac operating system.

The remote OBWI software uses a Java™-based program to display the video Viewer window. The remote OBWI automatically downloads and installs the Video Session Viewer the first time it is opened. The console switch does not install JRE, though it is available for download.

The remote OBWI uses system memory to store and display images within the Video Session Viewer windows. Each opened Video Session Viewer window requires additional system memory:

- 8-bit color setting requires 1.4 MB of memory per window
- 16-bit color setting requires 2.4 MB of memory per window
- 32-bit color setting requires 6.8 MB of memory per window

HP recommends having no more than three simultaneous Video Session Viewer windows open. More than four windows open simultaneously might affect system performance. You might receive an out-of-memory error, and the requested Video Session Viewer window will not open.

If the target device you want to access is currently being viewed by another used, you are prompted to preempt the other user if your preemption level is equal or greater than the other user's level. An appliance administrator can disconnect an active user from the Active Session page of the remote OBWI.

The following view of the Video Session Viewer is in normal window mode.
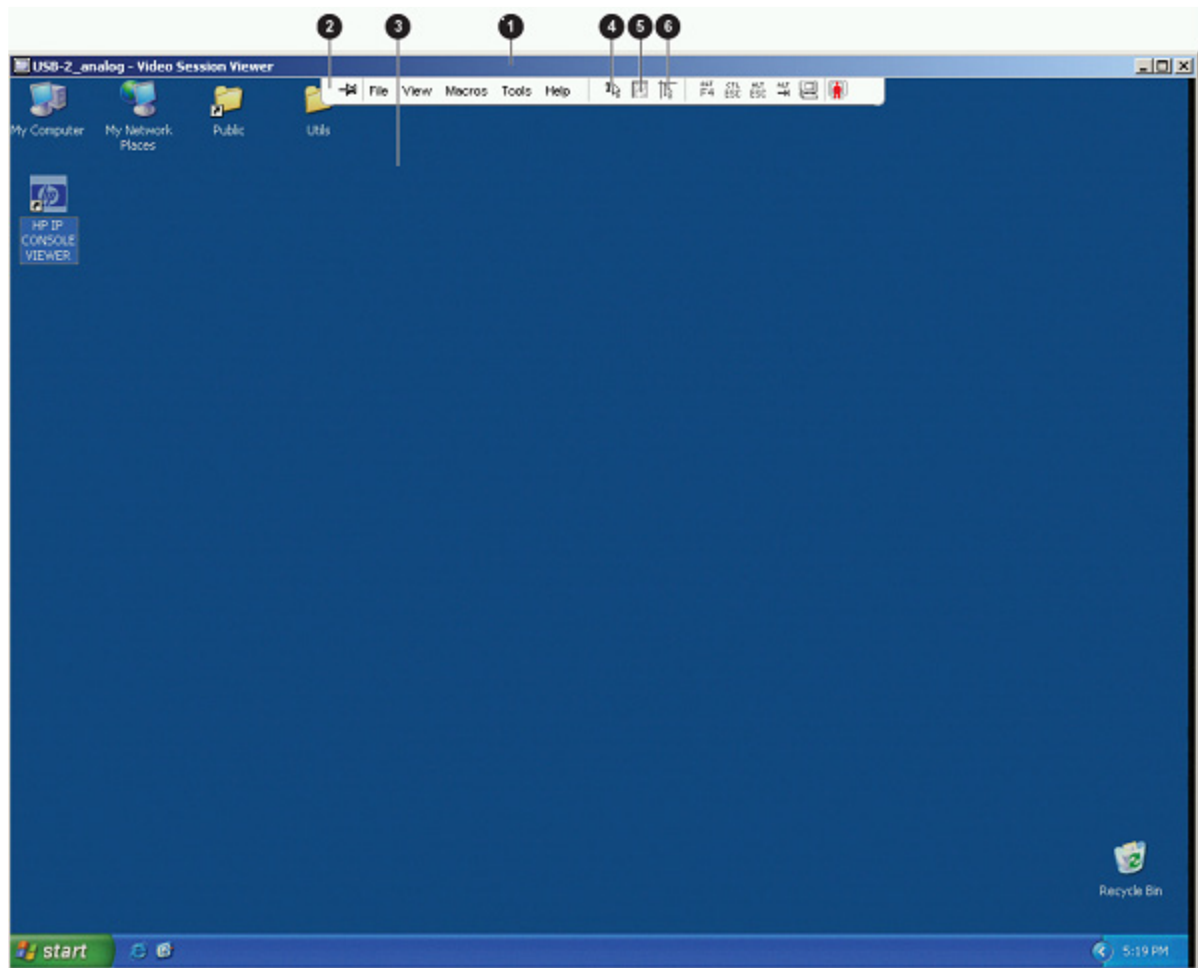
Item	Description
1	Title bar—Displays the name of the server you are viewing To access the menu bar, place your cursor in the middle bottom of the title bar.
2	Menu bar—Enables you to access features
3	Server desktop—Enables you to interact with the server through this desktop
4	Align Local Cursor icon—Enables you to reestablish proper tracking of the local cursor to the remote server cursor
5	Refresh Video icon—Enables you to regenerate the digitized video image of the server desktop
6	Full Screen mode icon—Enables you to expand the accessed server desktop to fill the entire screen

Changing the toolbar

You can adjust the amount of time that passes before the toolbar hides in the Video Session Viewer window when it is not locked by thumbtack.

1. Choose one of the following options:
   o From the Video Viewer window menu, select **Tools>Session Options**.
   o Select the **Session Options** button.

   The Session Options page appears.
2. Select the **Toolbar** tab.
3. Use the arrow keys to specify the number of minutes you want to pass before hiding the toolbar.
4. Select **OK** to save and close.

Launching a session

NOTE: If a user connects to a target device with a higher screen resolution than the local computer, the Video Session Viewer window displays a portion of the target device screen, with scroll bars for the remainder of the screen. The user can view the entire screen by adjusting the resolution on the target device, the local computer, or both.

To launch a Video Session Viewer session from the remote OBWI, see Active sessions (on page 53).

Session time-out

A remote session might time-out when there is no activity in a session window within a specified time. The session time-out value is configured through remote OBWI.

To enable, disable, or configure the time value for your session time-out, see Configuring General Session settings (on page 42).

Adjusting the view

When using a non-proxied connection, video performance over a slower network connection might be less than optimal. Certain color settings such as Grayscale use less network bandwidth than others, such as Best Color. Therefore, adjusting the color setting can increase video performance.

To adjust the view of the Video Viewer, the following options are available:

- Align the mouse cursors.
- Refresh the screen.
- Enable or disable Full Screen mode. When Full Screen mode is enabled, the image adjusts to fit the desktop up to a size of 1280 x 1024. If the desktop has a higher resolution, the full-screen image is centered in the desktop and the areas around the Video Viewer are blank. The menu and toolbar are locked to remain visible.
- Enable automatic, full, or manual scaling of the session image.
  o Automatic scaling—The desktop window is sized to match the resolution of the target device being viewed.
  o Full scaling—The desktop window remains fixed and the device image scales to fit the window.
  o Manual scaling—A menu of supported image scaling resolutions appears.
- Change the color depth of the session image.

Window size

Each Video Viewer window can be set to a different resolution. The default resolution is 1024 x 768.

If autoscaling is enabled, the remote OBWI automatically adjusts the display if the window size changes during a session. If the target device resolution changes during a session, the display automatically adjusts.

To change the Video Viewer window resolution:

1. From the Video Viewer, select **View>Scaling.**
2. Select the desired resolution.
3. Select **OK** to save and close.

Video Session Viewer tasks

For a complete list of tasks and operations handled through the Video Session Viewer, see the "Managing remote servers through the Video Session Viewer" section in the *HP IP Console Viewer User Guide.*

Closing a session

To close a Video Viewer session, select **File>Exit**.

Using Virtual Media

Virtual Media overview

In this section on Virtual Media, the remote console for HP Server Console Switches with Virtual Media is only available if the console switch is tiered underneath an HP IP Console Switch with Virtual Media.

The console switch enables you to connect shared media to a server using a USB connection. This capability enables you to manage systems more efficiently by performing operating system installation, operating system recovery, program installation, file transfers, and BIOS updates from the local or remote console.

You can connect Virtual Media directly to the console switch using one of the USB ports located on the rear of the console switch. In addition, you can connect Virtual Media from any remote workstation that is running the HP IP Console Viewer and is connected to a server using an HP IP Console Switch with Virtual Media. All USB ports of a local console are assigned to a single Virtual Media session and cannot be mapped independently to different servers.

To open a Virtual Media session with a server, you must first connect the server to the console switch using an interface adapter with Virtual Media and establish a local console session.

Using a console switch with Virtual Media, you can map a removable mass storage device or a CD/DVD type device on the console as a virtual drive on a target server. You can also add and map an .iso or floppy image file on the local client as a virtual drive on the target server if you are using the HP IP Console Viewer.

Limitations of using USB 2.0 composite devices with Virtual Media

The default functionality for Virtual Media for a USB 2.0 interface adapter with Virtual Media capability is the composite high-speed USB 2.0 capability of the USB protocol. The BIOS and particular operating systems and installation programs of various target servers do not support composite USB 2.0 devices. If your target server BIOS or operating system does not support such devices, then you must perform one of the following actions:

- Purchase a PS2 interface adapter with Virtual Media and map a single Virtual Media device, which operates in standard USB 2.0 mode.
- Disable the USB 2.0 function of the USB 2.0 interface adapter with Virtual Media from the console switch local OSD, enabling the interface adapter to operate in USB 1.1 mode.

AMD Opteron™-based HP ProLiant servers and Red Hat Enterprise Linux 4 (before Update 5) do not currently support composite USB 2.0 devices. However, the target server BIOS for Intel®-based HP ProLiant G4 and later servers support composite USB 2.0 devices. If the server BIOS supports USB 2.0 composite devices, but the operating system installation program does not, a failure occurs when the keyboard and mouse control is switched from the BIOS to the installation program.

HP recommends using the PS2 interface adapter with Virtual Media for AMD Opteron™-based HP ProLiant servers and Red Hat Enterprise Linux 4 (before Update 5), as well as older and third-party servers.

Virtual Media resources

Virtual Media resources cannot be shared between a local console and a remote console. For example, a remote user using the HP IP Console Viewer cannot use a Virtual Media resource attached to the local console USB hub. Only Virtual Media resources directly connected to the client's computer, running the HP IP Console Viewer, can be mapped to a target server.

You can have one CD-type device and one mass-storage-type device mapped concurrently.

- A CD-type device includes a CD/DVD drive or an .iso image of a CD.

- A mass-storage-type device includes a floppy drive, floppy image file, USB memory device, or other removable media type, such as an external USB hard drive.

Configuring Virtual Media

Virtual Media is configured through the remote OBWI or the local console UI. For more information on configuring virtual media, see Configuring Virtual Media Session settings (on page 44).

Sharing and preemption considerations

The KVM and virtual media sessions are separate, creating many options for sharing, reserving, and preempting sessions.

The KVM and virtual media sessions might be locked together. In this mode, when a KVM session is disconnected, so is the virtual media session. If the sessions are not locked together, the KVM session can be closed, but the virtual media session might remain active. Use this option when you are performing a time-intensive task using the virtual media session, such as loading an operating system, and want to establish a KVM session with a different target device to perform other functions while the operating system is loaded.

When a target device has an active virtual media session without an associated active KVM session, either the original user (User A) can reconnect or a different user (User B) can connect to that channel. You can set an option in the Virtual Media Session settings ("Configuring Virtual Media Session settings" on page 44) to reserve sessions, allowing only User A to access that channel with a KVM session. By using the reserved option in a tiered environment, only User A can access the lower switch and the KVM channel between the upper switch and lower switch.

If User B is allowed to access the session, User B can control the media used in the virtual media session.

Virtual Media dialog box

The following options are available from the Virtual Media dialog box:

- You can manage the mapping and unmapping of virtual media. The dialog box displays all of the physical drives on the client server that can be mapped as virtual drives. You can also add ISO and floppy image files and then map to them using the Virtual Media dialog box. After a device is mapped, the Virtual Media dialog box Details View displays information about the amount of data transferred and the time elapsed since the device was mapped.

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

- You can reset the USB 2.0 interface adapter. However, this action resets every form of USB media on the target device. Use this option with caution, and only when the target device is not responsive.

Using Virtual Media through the Video Session Viewer

You can launch a Virtual Media session and perform several tasks through the Video Session Viewer. For more information, see the *HP IP Console Viewer User Guide*.

Using local Virtual Media

For local Virtual Media to work properly, you must have an HP Server Console Switch with Virtual Media or an HP IP Console Switch with Virtual Media as the console switch. You must also have an interface adapter with Virtual Media connecting each server to the console switch.
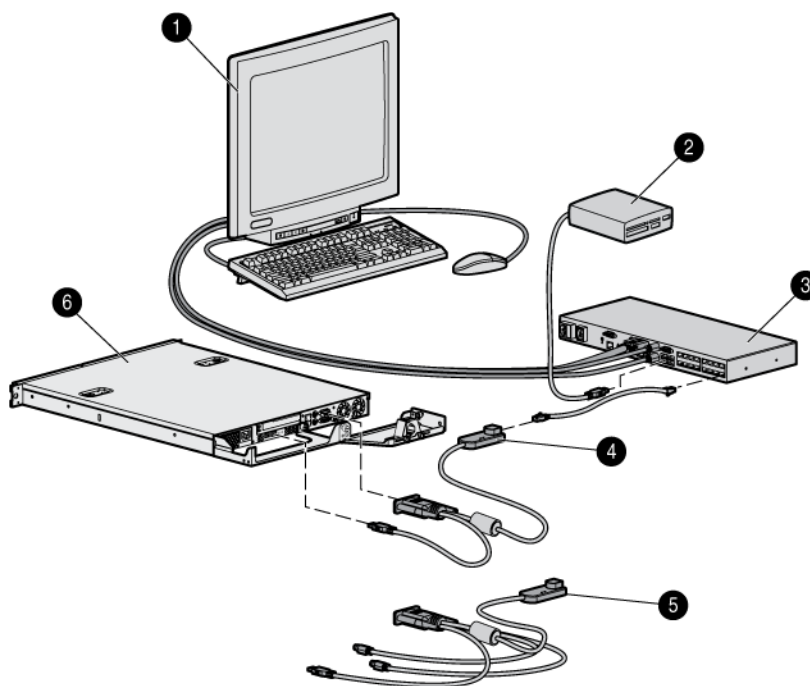
Item	Description
1	Local user
2	USB media device
3	Console switch (HP Server Console Switch with Virtual Media or HP IP Console Switch with Virtual Media)
4	USB 2.0 interface adapter with Virtual Media
5	PS2 interface adapter with Virtual Media
6	Server

Using Virtual Media in a two-level cascade configuration

For Virtual Media to work properly in a two-level cascade configuration, you must have:

- A console switch with Virtual Media as the primary console switch
- A console switch with Virtual Media as the secondary console switch
- An interface adapter with Virtual Media connecting each server to the console switch

For more information on cascading, see Cascading console switches (on page).
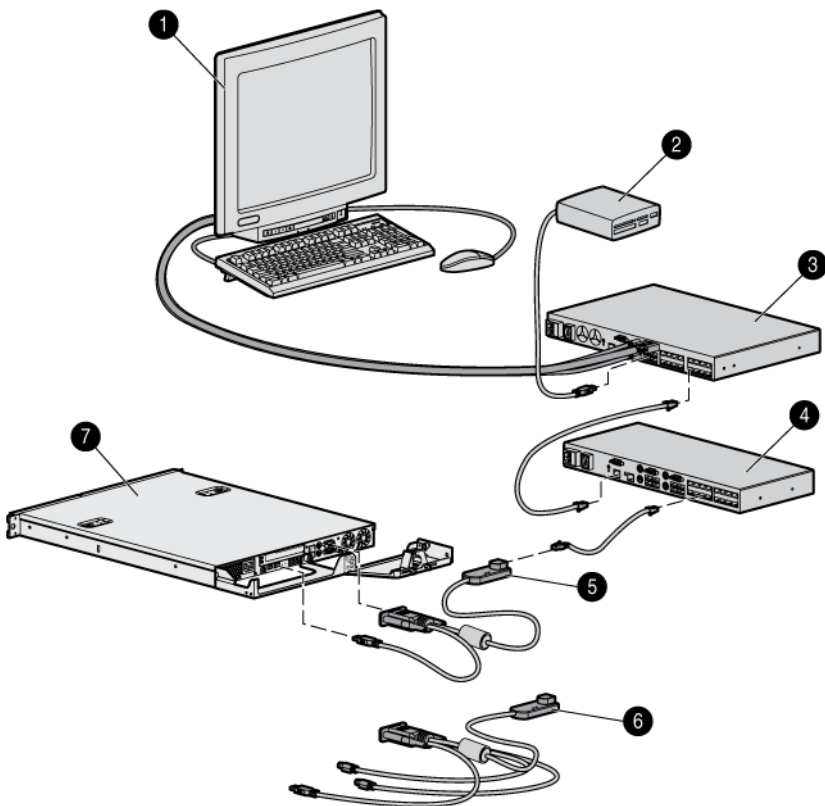
Item	Description
1	Local user
2	USB media device
3	Console switch (HP Server Console Switch with Virtual Media or HP IP Console Switch with Virtual Media)
4	Secondary console switch (HP Server Console Switch with Virtual Media)
5	USB 2.0 interface adapter with Virtual Media
6	PS2 interface adapter with Virtual Media
7	Server

Using smart cards

Smart card overview

You can use a smart card, also referred to as a CAC, with your console switch when two-factor authentication is required.

> **NOTE:** To use a smart card reader with a target device, you must first connect the target device to a console switch using a smart card capable interface adapter.

You can connect smart card readers directly to the console switch using local USB ports, or you can connect smart card readers to any remote workstation. The smart card reader must be connected prior to starting a console session with the server. For more information about smart cards, see Using Smart Cards (on page 64).

Using a smart card through Video Session Viewer

After you connect a smart card reader to an available USB port on the client server and are able to access target devices, you can launch a KVM session to open the Video Session Viewer and map a smart card.

The smart card status is indicated by the icon at the far right of the Video Session Viewer toolbar. One of the following status icons appears.

Icon	Description
	A smart card is not in the smart card reader, or a smart card reader is not attached.
	A smart card is in the smart card reader, but it has not been mapped.
	A smart card is mapped.A smart card is mapped.

To map a smart card:

1. Launch a KVM session. The Video Session Viewer window appears.
2. Insert a smart card in to the smart card reader attached to your client server.
3. From the Video Session Viewer, select **Tools>Map Smart Card.**
4. Select your smart card, listed below the No Card Mapped option, to map the smart card.

To unmap a smart card you can:

- Close the KVM session by clicking the **X** in the Video Session Viewer window.
- From the Video Session Viewer, select **Tools>No Card Mapped**.
- Remove the smart card reader, or disconnect the smart card reader from the client server.

LDAP

LDAP overview

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.

You can configure and define your authentication parameters through the remote OBWI. The software sends the username, password, and other information to the target device, which then determines whether the user has permission to view or change configuration parameters for the target device through the remote OBWI.

LDAP configuration

LDAP authentication, search, and query parameters are configured through the remote OBWI. For more information, see Configuring LDAP (on page 49).

Setting up Active Directory for performing queries

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

To set up group queries:

1. Log in to Windows® with administrator privileges.
2. Open Active Directory software.
3. Create an organizational unit to be used as group container.
4. Create a computer object in Active Directory with a name identical to the switching system name for querying appliances or identical to the attached target devices for querying target devices. The name must match exactly and is case-sensitive.
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 screen of the remote OBWI and target device names must be comprised of any combination of upper-case and lower-case letters, digits, and hyphens, and must match the object names in Active Directory,
6. Create one or more groups under the group container organizational unit.
7. Add the usernames and the target device and appliance objects to the groups you created in step 5.
8. Specify the value of any attribute used to implement the Access Control Attribute.

Console switch serial management

Establishing LAN connections

> **NOTE:** Although 10Base-T Ethernet can be used, HP recommends a dedicated, switched 100Base-T or 1000Base-T network for improved performance.

Connect the network cable from the LAN port on the rear panel of the console switch to an Ethernet switch, and power on the console switch. For more information, see the *HP IP Console Viewer User Guide* included on the CD provided with this kit.

Connecting to the serial management and setup port

Requirements:

- The G2 console switches use an RJ-45 serial port instead of the DB9 port. A DB9 DCE female to RJ-45 serial adapter is included with the console switch.
- A UTP CAT5 or better cable, with standard CAT5 pinouts

To connect to the serial management and setup port:

1. Connect the DB9 adapter to an available COM port on the computer you will use to manage the switch.
2. Connect the DB9 adapter to the console switch setup port, using a CAT5 or better UTP cable.
3. Configure the terminal emulation software, such as HyperTerminal ("Configuring HyperTerminal" on page 66) or Minicom ("Configuring Minicom" on page 66).
4. Verify that the console switch is receiving power. After a few minutes, the console switch boots up.
5. Press the **Enter** key to access the Main Menu.

Configuring HyperTerminal

To configure the HyperTerminal:

1. From the desktop screen, select **Start>Programs>Accessories>Communications>HyperTerminal.** The Connection Description window appears.
2. Enter a name for the description, and click **OK.** The Connect To window appears.
3. Select the Communication Port that is connected to the console switch through a serial cable, then click **OK.** The COM1 Properties window appears.
4. Select **9600** for the Bits Per Second, **8** for Data Bits, **None** for Parity, **1** for Stop Bits, and **None** for Flow Control, then click **OK.** The HyperTerminal auto-connects to the console switch.
5. Press the **Enter** key to access the console switch option menu.

Configuring Minicom

NOTE: The following example uses Red Hat Linux 3.0. For more information, refer to your Linux operating system Help or documentation.

IMPORTANT: Minicom is a utility that is loaded during the installation of Linux. However, if you do not select the option to install the Linux Utilities during the operating system installation, you cannot use Minicom without downloading the Minicom X.X.i386.rpm file from the Red Hat website. (Refer to the procedure for installing RPMs on the Red Hat website.)

To configure Minicom:

1. Log in to a Linux console or open a terminal, and enter `minicom-s` at the command prompt. The Configuration menu appears.
2. Select **Serial Port Setup.** The Change which setting? menu appears.
3. Select **Option A (Serial Device).** Manually change the device type from "dev/modem" to "/dev/ttyS0" and press **Enter**.
4. Select **Option E (Bps/Par/Bits).** The Comm Parameters menu appears.
5. Select **E (Speed 9600 Bps),** and press **Enter**. The designation 9600 8N1 appears next to Option E.
6. Select **Option F (Hardware Flow Control).**

   Be sure that the Change which setting? menu is configured as follows:

   A—Serial Device: /dev/ttyS0

   B—Lockfile Location: /var/lock

   C—Callin Program:

   D—Callout Program:

   E—Bps/Par/Bits: 9600 8N1

   F—Hardware Flow Control: No

   G—Software Flow Control: No
7. Press the **Enter** key to return to the Configuration menu. Scroll down to the Save setup as dfl option, and press the **Enter** key.
8. From the Configuration menu, scroll down to the Exit the Minicom option, and press **Enter**.
9. From the command prompt, enter `Minicom`. As soon as a connection is established, the main menu for the console switch appears. Follow the on-screen options to configure the console switch.

Using the Main Menu

The following configuration options are available from the Console Switch Main Menu:

- Network configuration
- Enable debug messages
- Reset appliance
- Exit

To access the Main Menu:

1. Establish a terminal session, and then press **Enter**. The Main Menu appears.
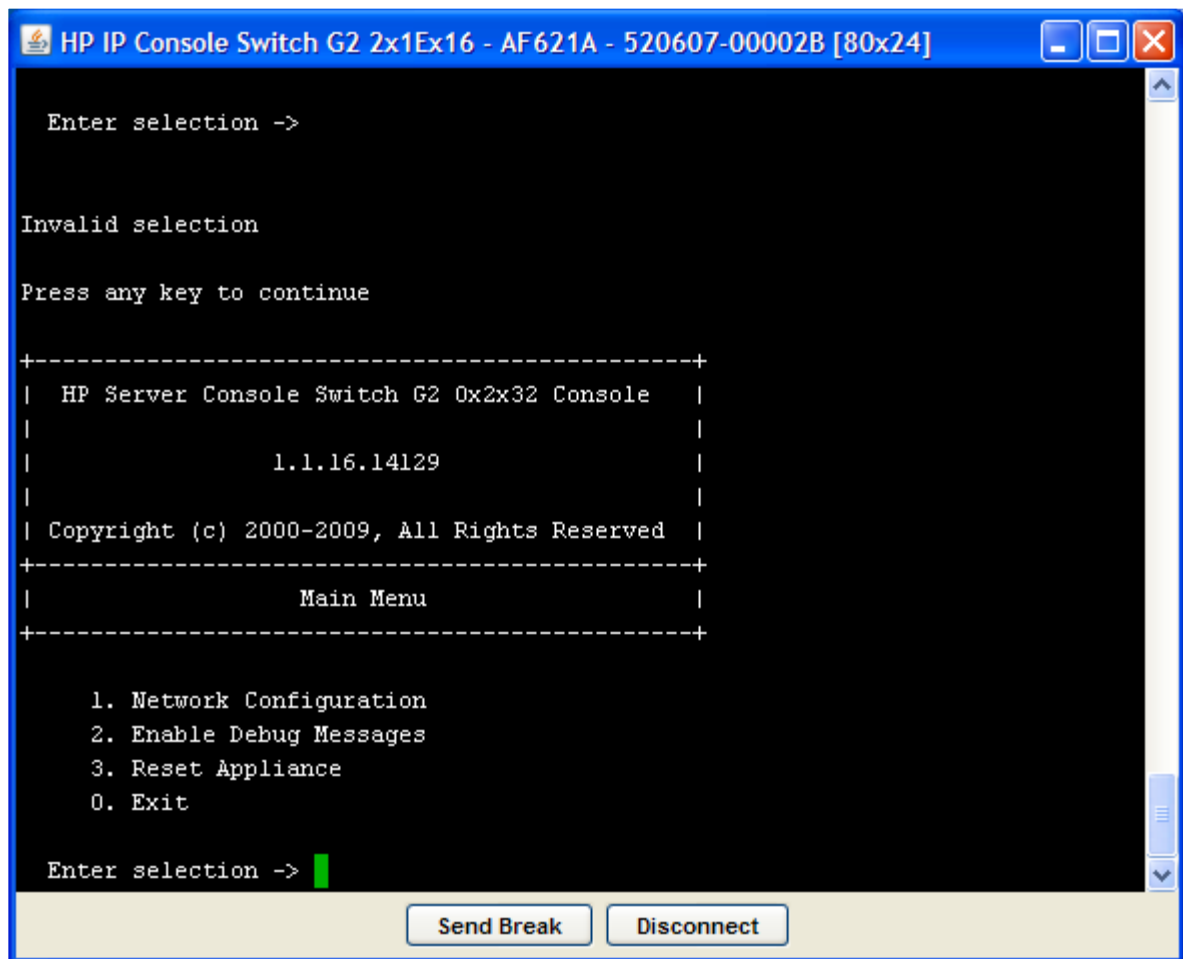
Network Configuration

The Network Configuration option enables you to set the network speed and either IPv4 or IPv6 settings.

Enable Debug Messages

The Enable Debug Messages option enables you to debug the system. Select **yes** to debug the system.

Reset Appliance

The Reset Appliance option reboots the server console switch.

Exit

The Exit option allows you to exit the Main Menu.

Configuring the console switch NIC

1. Establish a terminal session and then press the **Enter** key. The Main Menu appears.

2. Select **Option 1—Network Configuration.** The Network Configuration Menu appears.

3. Select **Option 1—Network Speed** to set the network speed. When possible, set the connection manually without relying on the auto negotiate feature. After you enter a selection, return to the Network Configuration menu.

4. To specify an IPv4 or IPv6 IP address, select **Option 2—IP Configuration**, and then select the IP address you want to configure. HP recommends using a static IP address for IPv4. The console switch has Dual Stack capability.

5. If you are using a static IPv4 address, perform the following steps:

   a. To specify an IP address, select **Option 3—IP Address**.

   b. To specify a netmask, select **Option 4—Netmask**.

   c. To specify a default gateway, select **Option 5—Default Gateway**.

   When this configuration is complete, enter **0** to apply the changes and return to the Main Menu.

6. If you are using a static IPv6 address, perform the following steps:

   a. To specify an IP address, select **Option 3—IP Address**.

   b. To specify a prefix length, select **Option 4—Prefix Length**.

   c. To specify a default gateway, select **Option 5—Default Gateway**.

   When this configuration is complete, enter **0** to apply the changes and return to the Main Menu.

7. To exit to the Main Menu or to apply changes you made, select **Option 0—Exit/Apply changes**.

8. If you made any changes to the network speed you must reboot the console switch.

Recovering a lost console switch serial management password

1. Establish a terminal session, and press the **Enter** key. You are prompted to enter the console switch serial management password.

2. Enter `HELP`. A 16-bit key and the EID number of the console switch appear.

3. Call the HP technical support phone number (1-800-474-6836). Give the service person your 16-bit key and EID number of the console switch. A one-time password, which is specific to your console switch, is given to you.

4. Enter the one-time password. Your previous console switch serial management password is deleted.

For more information on recovering lost passwords through the local UI or remote OBWI, change the Setup Port Settings through the Local console UI settings (on page 41).

Firmware

Upgrading the firmware

The console switch upgrade feature enables you to upgrade the console switch and interface adapters with the latest available firmware through the local UI or remote OBWI. For more information, see "Upgrading the console switch firmware (on page 33)" or "Upgrading the interface adapter firmware (on page 40)."

> △ **CAUTION:** Do not disconnect an interface adapter during a firmware upgrade or power cycling. The interface adapter becomes inoperable and must be returned to the factory for repair.

Before beginning the upgrade procedure, be sure that the Secure TFTP Server is installed and that the GET access permissions are selected for the folder where the updated file is located. Also, be sure that the console switch is on the same network as the computer that is being used for the upgrade. After the TFTP has been enabled, then upgrade the console switch firmware.

To enable TFTP for Microsoft Windows, see "Enabling TFTP for Microsoft Windows operating systems (on page 70)."

To enable TFTP for Linux, see "Enabling TFTP for Linux operating systems (on page 70)."

Enabling TFTP for Microsoft Windows operating systems

To enable TFTP for Microsoft® Windows® operating systems, follow the instructions in the \TFTP\TFTP Install Instructions.txt file on the CD included with this kit or the Softpaq TFTP directory.

Enabling TFTP for Linux operating systems

TFTP is provided by the TFTP server RPM (RPM-IVH/Redhat/RPMS/) for most systems using RPM packages. Depending on the type of distribution, the Internet services daemon is provided by xinetd.

> **NOTE:** The following example uses Red Hat Linux 3.0. For more information, refer to your Linux operating system Help or documentation.

> **NOTE:** By default, TFTP executes in secure mode and only provides readable files under the /tftpboot directory. Other directories can be specified through the /etc/xinetd.d/tftp files. In secure mode, TFTP expects the file to be relative to the/tftpboot directory.

To enable TFTP for Linux operating systems (GNOME):

1. In the GNOME viewer go to the main menu and select **Programs>System>Service Configuration.**
2. In the Service Configuration menu, verify that the xinetd checkbox is selected to start at boot.

   -or-

   If the checkbox is not selected, select the box and click **Save.**
3. Find **TFTP** in the list of services and highlight it.
4. Select the checkbox to start TFTP at boot, and then click **Save.**

To enable TFTP for Linux operating systems (KDE):

1. Go to the main menu and select **Control Panel>Services.**
2. In the Service Configuration menu, verify that the xinetd checkbox is selected to start at boot.

    -or-

    If the checkbox is not selected, select the box and click **Save.**
3. Find TFTP in the list of services and highlight it.
4. Select the checkbox to start TFTP at boot, and then click **Save**.

Verifying TFTP for Linux operating systems

> **NOTE:** The following example uses Red Hat Linux 3.0. For more information, refer to your Linux operating system Help or documentation.

1. Verify that the `in.tftpd` service is running with the following `ps -ef | grep tftpd`.

    By default the `/etc/xinetd.d/tftp` configuration file uses `/tftpboot` as the directory.
2. Create a `/tftpboot` directory (if it doesn't exist) and set the permissions for public access.
3. Copy the firmware file to `/tftpboot`.
4. Cd to `/tmp`.
5. From the shell prompt, enter `tftp localhost` (or name of local system).
6. Download the file by entering the following command: `get/tftpboot/filename`
7. Enter `quit`.
8. From the shell prompt, check to see if the file is in the `/tmp` directory.

If the TFTP is configured correctly, the preceding steps transfer the file to the current directory.

Troubleshooting

Console switch troubleshooting

Problem	Troubleshooting
The console switch is not working properly.	**1** Determine whether the console switch has power. **2** Determine if all the cables are properly connected.
The console switch hangs after reboot.	Reboot the console switch again by removing the power cable and then plugging it back in to a power source.
One of the power supply status indicator LEDs does not appear and the other blinks irregularly.	One of the power supplies does not have power or is defective. The LED blinking irregularly is blinking the Morse code SOS.
The system does not recognize the cascaded console switches.	Verify that all of the console switches are HP switches, and are upgraded with the latest firmware.
Servers are still listed although they have been disconnected.	Delete the offline interface adapters ("Deleting offline interface adapters" on page 40) through either the local console UI or remote OBWI.
The console switch serial port password is lost.	Reset the password through the Local console UI settings (on page 41).
The video displays all green or red, or the colors are all wrong.	• Look for breaks or bad crimps in the UTP CAT5 cable. • Look for bent pins in the VGA connection. • Be sure that the cable is not a cross-over network cable.
The mouse does not align.	Verify that there is no mouse acceleration or enhanced pointed precision. The mouse speed must be 50%.
The mouse and keyboard lose functionality after the Device Reset button is pressed while operating a UNIX® based platform.	The Device Reset button is a Microsoft® Windows® based function. To regain mouse and keyboard functionality, restart the desktop.

Problem	Troubleshooting
When connecting a serial interface adapter to a server running Red Hat Linux, SLES, or HPUX, the numeric keypad keys on a PC keyboard do not map to VT100 emulation under the Linux shell. Using the numeric keypad with the vi text editor causes function characters to appear rather than numbers.	Use the `printenv` command to show the TERM assigned under Linux. It can be matched appropriately with other termcap entries by editing the profile or setting the TERM equal to `"ansi"`. For PC keyboards, ANSI is the most compatible emulation. -or- Edit your /etc/inittab as s0:2345:respawn:/sbin/agetty -h ttyS0 115200, 9600 ansi Where `ttyS0` is the serial device name under Linux where the serial interface adapter is connected. At a shell prompt, enter `init q`, or reboot the system.
Virtual Media is not working properly.	Be sure that you are using the following: • Console switches with Virtual Media • A USB interface adapter with Virtual Media, or a PS2 interface adapter with Virtual Media • A server and operating system that supports high-speed composite USB 2.0 devices You must be able to see a Virtual Media CD drive and a mass storage drive on the target server to be able to map a local resource to the remote server.
Options in the Virtual Media dialog box are not available.	See Configuring Virtual Media Session settings (on page 44).
The keyboard does not respond after opening a Virtual Media session.	See USB 2.0 composite device limitations.
The video resolution is distorted.	See Connection length table (on page 73).

Connection length table

The console switch offers optimum video performance when the distance between the server and console switch is 15 m (50 ft) or less. The system is capable of operation at distances up to 30.5 m (100 ft), at reduced video resolutions.

Standard 4x3

Total cable length	1600 x 1200 @ 85 Hz	1280 x 1024 @ 85 Hz	1024 x 768 @ 85 Hz	800 x 600 @ 85 Hz
3 m (10 ft)	X	X	X	X
15 m (50 ft)	X	X	X	X
30.5 m (100 ft)	—	—	—	X

Widescreen 16x9 or 16x10

Total cable length	1680 x 1050 @ 60 Hz	1440 x 900 @ 60 Hz	1280 x 800 @ 60 Hz	1024 x 640 @ 60 Hz	800 x 500 @ 60 Hz
3 m (10 ft)	X	X	X	X	X

Total cable length	1680 x 1050 @ 60 Hz	1440 x 900 @ 60 Hz	1280 x 800 @ 60 Hz	1024 x 640 @ 60 Hz	800 x 500 @ 60 Hz
15 m (50 ft)	X	X	X	X	X
30.5m (100 ft)	—	—	—	—	X

Frequently asked questions

Console switch frequently asked questions

Question	Answer
Are the interface adapters hot-pluggable?	Yes, they are hot-pluggable to the console switch. Using PS2 connections to servers might not be hot-pluggable.
Are the keyboard, monitor, and mouse connections on the console switch hot-pluggable?	Yes
Are the server connections on the console switch hot-pluggable?	Yes
Can the console switch be mounted in a round-hole rack?	Yes, the console switch can be mounted in a round-hole rack using the standard-mount installation ("Performing a standard-mount installation" on page 15).
Can the console switch be side-mounted in a round-hole rack?	No
How do I access the local console UI?	• Press the **Print Scrn** key. • Press the **Ctrl** key twice within one second.
How do I cascade console switches?	See Cascading console switches (on page 25).
How do I change the keyboard language?	Language-specific keyboard emulation in the interface adapter is determined by the keyboard language chosen in the Local console UI settings (on page 41).
How do I know which port my cascaded console switch is connected to?	View the Port column of either the Interface adapter ports (on page 40) or Cascade devices ports (on page 41).
How do I locally connect a cascaded console switch?	Use a CAT5 or better cable to connect from an interface adapter connection port on the primary console switch to the tiering port on the secondary console switch.
How do I view my console switch firmware version?	See Viewing system information.
How do I view my interface adapter firmware version?	View the Application column of the Appliance IAs ("Interface adapter ports" on page 40) page.
What kind of UTP cables are supported?	Only UTP, CAT5, CAT5e, CAT6, and CAT7 cables are supported.

Regulatory information

Safety and regulatory compliance

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

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

Warranty information

HP ProLiant and X86 Servers and Options (http://www.hp.com/support/ProLiantServers-Warranties)

HP Enterprise Servers (http://www.hp.com/support/EnterpriseServers-Warranties)

HP Storage Products (http://www.hp.com/support/Storage-Warranties)

HP Networking Products (http://www.hp.com/support/Networking-Warranties)

Support and other resources

Before you contact HP

Be sure to have the following information available before you call HP:

- Active Health System log (HP ProLiant Gen8 or later products)

  Download and have available an Active Health System log for 3 days before the failure was detected. For more information, see the *HP iLO 4 User Guide* or *HP Intelligent Provisioning User Guide* on the HP website (http://www.hp.com/go/ilo/docs).

- Onboard Administrator SHOW ALL report (for HP BladeSystem products only)

  For more information on obtaining the Onboard Administrator SHOW ALL report, see the HP website (http://www.hp.com/go/OAlog).

- Technical support registration number (if applicable)

- Product serial number

- Product model name and number

- Product identification number

- Applicable error messages

- Add-on boards or hardware

- Third-party hardware or software

- Operating system type and revision level

HP contact information

For United States and worldwide contact information, see the Contact HP website (http://www.hp.com/go/assistance).

In the United States:

- To contact HP by phone, call 1-800-334-5144. For continuous quality improvement, calls may be recorded or monitored.

- If you have purchased a Care Pack (service upgrade), see the Support & Drivers website (http://www8.hp.com/us/en/support-drivers.html). If the problem cannot be resolved at the website, call 1-800-633-3600. For more information about Care Packs, see the HP website (http://pro-aq-sama.houston.hp.com/services/cache/10950-0-0-225-121.html).

Acronyms and abbreviations

AC
alternating current

BOOTP
Bootstrap Protocol

CAC
Common Access Card

CRC
cyclic redundant checks

EID
electronic identification number

G2
Generation 2

GNOME
GNU Network Object Model Environment

HP SIM
HP Systems Insight Manager

IA
interface adapter

ID
identification

KVM
keyboard, video, and mouse

LDAP
Lightweight Directory Access Protocol

OBWI

on-board Web interface

OSD

on-screen display

RPM

Red Hat Package Manager

SIM

Systems Insight Manager

SLES

SUSE Linux Enterprise Server

SSH

Secure Shell

TFTP

Trivial File Transfer Protocol

USB

universal serial bus

UTP

unshielded twisted pair

Documentation feedback

HP 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@hp.com). Include the document title and part number, version number, or the URL when submitting your feedback.

Index