LANTRONIX®

Spider™ and SpiderDuo®
KVM-over-IP Device User Guide

Part Number 900-495
Revision L October 2023

Copyright and Trademark

Lantronix is a registered trademark of Lantronix, Inc. in the United States and other countries.

Patented: www.lantronix.com/legal/patents. Additional patents pending.

Windows and *Microsoft Edge* are registered trademarks of Microsoft Corporation. *Mozilla* and *Firefox* are registered trademarks of the Mozilla Foundation. *Chrome* is a trademark of Google, Inc. *Safari* is a registered trademark of Apple, Inc. All other trademarks and trade names are the property of their respective holders.

LINUX GPL Compliance

Certain portions of source code for the software supporting the Lantronix® Spider™ family are licensed under the GNU General Public License (GPL) Version 3, available at https://www.gnu.org/licenses/gpl-3.0.en.html.

Lantronix has made modifications to this source code (2022-2023); additional details are available upon request.

Warranty

For details on the Lantronix warranty replacement policy, go to https://www.lantronix.com/technical-support/warranty.

Contacts

Lantronix, Inc.
Corporate Headquarters

48 Discovery, Suite 250
Irvine, CA 92618, USA

Toll Free: 800-526-8766
Phone: 949-453-3990
Fax: 949-453-3995

Technical Support
Online: https://www.lantronix.com/technical-support

Sales Offices

For a current list of our domestic and international sales offices, go to the Lantronix web site at https://www.lantronix.com/about/contact.

Disclaimer and Revisions

Operation of this equipment in a residential area is likely to cause interference, in which case the user, at his or her own expense, will be required to pay for to take whatever measures may be required to correct the interference.

This equipment has been tested and found to comply with the limits for Class A digital device pursuant to Part 15 of the FCC Rules. These limits are designed to provide reasonable protection against harmful interference when the equipment is operated in a commercial environment.

This equipment generates, uses, and can radiate radio frequency energy and, if not installed and used in accordance with this User Guide, may clause interference to radio communications. Operation of this equipment in a residential area is likely to cause interference, in which case the user will be required to correct the interference at his own expense.

The user is cautioned that changes and modifications made to the equipment without approval of the manufacturer could void the user's authority to operate this equipment.

Changes or modifications to this device not explicitly approved by Lantronix will void the user's authority to operate the device.

Documentation Changes

The information in this guide may change without notice. The manufacturer assumes no responsibility for any errors that may appear in this guide. For the latest revision of product documents, please check our online documentation at https://www.lantronix.com/support/documentation.

Revision History

Date	Rev.	Comments
March 2007	A	Initial Document
November 2007	B	Changed baud rate default to 9600; added Detector utility for assigning IP address; added ability to enable drive redirection, configure backup/restore, and reset factory defaults; introduced a CLI and commands.
April 2008	C	Added Direct KVM; KVM-only mode; Spider device network web page; ability to preserve network settings for factory defaults; country code support; iGoogle gadget; instructions for using the mounting kit.
May 2009	D	Updated to firmware version 2.2, VIP access.
September 2009	E	Updated and added SpiderDuo.
March 2010	F	Updated to firmware version 3.01.
November 2013	G	Updated product name and trademark information. Removed mention of ManageLinx, VIP and DSM.
December 2022	H	Updated to firmware version 5.0.0.0. Removed Java from system requirements. Added ConsoleFlow support. ***Caution:*** ***Beginning with Rev. H, this user guide is for devices running firmware release 5.0.0.0 and newer. Devices with the Kira chip running firmware version 4.X and older CANNOT be upgraded to 5.0.0.0; doing so may render the device inoperable.*** ***To confirm, go to Maintenance > Device Status; if the "Kira Device Revision" field is present, the device cannot be upgraded to 5.0.0.0. Please contact Lantronix Technical Support at www.lantronix.com/technical-support to request the previous revision of this user guide.***
January 2023	J	Updated to firmware version 5.0.0.1. Updated KVM Console Virtual Key feature. Updated product labels.

Date	Rev.	Comments
June 2023	K	Updated to firmware version 5.1.0.0. Power supply part numbers updated. Spider power requirements, LED light behavior updated. Added Group Based System Access Control, PCU Safety Information, Spider Duo declarations of conformity.
October 2023	L	Updated Keyboard/Mouse settings. Added Virtual Media settings.

List of Figures

List of Tables

1: About This Guide

This guide describes how to install, configure, use, and update the Lantronix® Spider™ and SpiderDuo® distributed keyboard, video, and mouse (KVM) -over-IP devices. It describes how to remotely and securely provide monitoring and control of one target computer system by one or more remote users.

This chapter contains the following sections:

Note: *The information contained in this guide apply to the Spider and SpiderDuo devices unless otherwise noted.*

Caution: ***This version of the user guide is for devices running firmware release 5.0.0.0 and newer. Devices with the Kira chip running firmware version 4.x and older CANNOT be upgraded to 5.0.0.0; doing so may render the device inoperable. To confirm, go to Maintenance > Device Status; if the "Kira Device Revision" field is present, the device cannot be upgraded to 5.0.0.0. Please contact Lantronix Technical Support at www.lantronix.com/technical-support to request the previous revision of this user guide.***

Chapter and Appendix Summaries

Table 1-1 lists and summarizes each chapter and appendix.

Table 1-1 Chapter/Appendix and Summary

Chapter/Appendix	Summary
Chapter 2: Overview	Describes the Spider and SpiderDuo features and supported protocols.
Chapter 3: Installing the Spider Device	Provides technical specifications; describes connection formats and power supplies.
Chapter 4: Installing the SpiderDuo Device	Provides technical specifications; describes connection formats and power supplies.
Chapter 5: Web Browser Access	Describes method to access the Web browser.
Chapter 6: Remote System Control	Describes the remote system control.
Chapter 7: Interfaces	Provides instructions for configuring network ports, firewall and routing settings, and date and time.
Chapter 8: User Accounts	Provides instructions for configuring user accounts.
Chapter 9: Services	Provides instructions for configuring services, such as date and time, security settings, and certificates.

Table 1-1 Chapter/Appendix and Summary (continued)

Chapter/Appendix	Summary
Chapter 10: Maintenance	Provides instructions for upgrading firmware, viewing system logs and diagnostics, and generating reports. Includes information about web pages and commands used to shut down and reboot the Spider and SpiderDuo devices.
Chapter 11: Command Reference	Lists and describes all of the commands available on the Spider or SpiderDuo Device command line interface.
Appendix A: Troubleshooting	Describes troubleshooting methods.
Appendix B: Supported Resolutions and Refresh Rates	Lists the resolutions and refresh rates that are supported.
Appendix C: Mounting Bracket Kit	Describes how to mount the Spider or SpiderDuo Device in a rack.
Appendix D: PCU Safety Information	Provides PCU safety information.
Appendix E: Technical Support	Lists technical support telephone and fax numbers.
Appendix F: Compliance	Provides information about the Spider and SpiderDuo device compliance with industry standards.

Conventions

Table 1-2 lists and describes the conventions used in this book.

Table 1-2 Conventions Used in This Book

Convention	Description
Bold text	Default parameters.
Brackets [ ]	Optional parameters.
Angle Brackets < >	Possible values for parameters.
Pipe |	Choice of parameters.
Warning	***Warning:*** ***Before you work on any equipment, you must be aware of the hazards involved with electrical circuitry and familiar with standard practices for preventing accidents.***
Note	***Note:*** *Notes contain helpful suggestions, information, or references to material not covered in the publication.*
Caution	***Caution:*** ***You might do something that could result in faulty equipment operation, or loss of data.***
Screen Font (Courier New)	CLI terminal sessions and examples of CLI input.

Additional Documentation

Visit the Lantronix web site at www.lantronix.com/support/documentation for the latest documentation and the following additional documentation:

- ***Spider View User Guide***—Details instructions on using the Spider View utility.

  Note: *Spider View 2.0.0 is required to manage Spider devices running firmware 5.0.0.0 and newer.*

- ***Spider Quick Start Guide***—Provides an overview of using the Spider device.
- ***SpiderDuo Quick Start Guide***—Provides an overview of using the SpiderDuo.

2: Overview

Lantronix Spider and SpiderDuo distributed KVM-over-IP devices are designed to remotely and securely provide monitoring and control of one target computer system by one or more remote users. The remote user (client) accesses the Spider or SpiderDuo device over a local or wide area network connection using a standard web browser.

Spider and/or SpiderDuo device is an evolution of the traditional remote KVM device into a compact package. It is light enough to be cable-supported from the back of a server and takes up no rack space.

Both devices differ from other KVM-over-IP devices in several ways. Unlike rack mounted KVM-over-IP devices, the allocation of one Spider device per computer allows add-as-you-grow scalability and guarantees non-blocked BIOS-level access to mission-critical servers regardless of the number of remote users or servers that need access.

This chapter contains the following sections:

Note: *The terms Remote Console and KVM Console are synonymous and used interchangeably throughout the User Guide.*

Spider Overview

The Spider device features, functionality, system configuration and cables, and technical specifications are described in the following sections:

Features

The Spider device incorporates two hardware-switched Ethernet ports, one for the primary network connection and the second for daisy-chaining Spider devices, or aggregating other Ethernet connections (for example, a dedicated management LAN port on the controlled system). This provides a cost-effective solution in environments in which numerous cable drops and distance limitations are challenging when adding servers.

The Spider device comes in the following four models:

- One model with both PS/2 and USB keyboard and mouse interfaces (software selectable), cable length of 21” or 59”
- One model for USB-only systems, cable length of 21” or 59”

The color-coded cable plugs for the keyboard, mouse, USB port and video are designed to plug directly into the target server.

Additional features:

- Secure, full BIOS-level control of remote servers over an IP network
- Space–saving “zero footprint” package attaches directly to the server that saves rack space
- Guaranteed non-blocked access to remote servers that ensures lowest “cost-per-remote user”
- Browser–based, no client software or special licensing required
- Direct KVM minimizes the number of clicks to the remote–server console
- Built-in RS-232 serial port that can be configured for serial console port access and host pass-through access
- Ideal for distributed IT system environments such as small branch offices, campuses, test labs, and server hosting environments

Functionality

The Spider device captures the video output from the attached computer, compresses and sends it over the network to a KVM console window launched by the browser or to a command line interface on the user system, which displays a replica of the server video output on the user monitor.

The Spider device also uses KVM console to accept keystrokes and mouse movements on the user system; recognizes those intended for the target computer; transmits the keystrokes and mouse movements; and emulates a physically attached keyboard and mouse.

System Configuration and Cables

Figure 2-1 shows the Spider system configuration, and *Figure 2-2* shows the cable dimensions.

Figure 2-1 Spider System Configuration

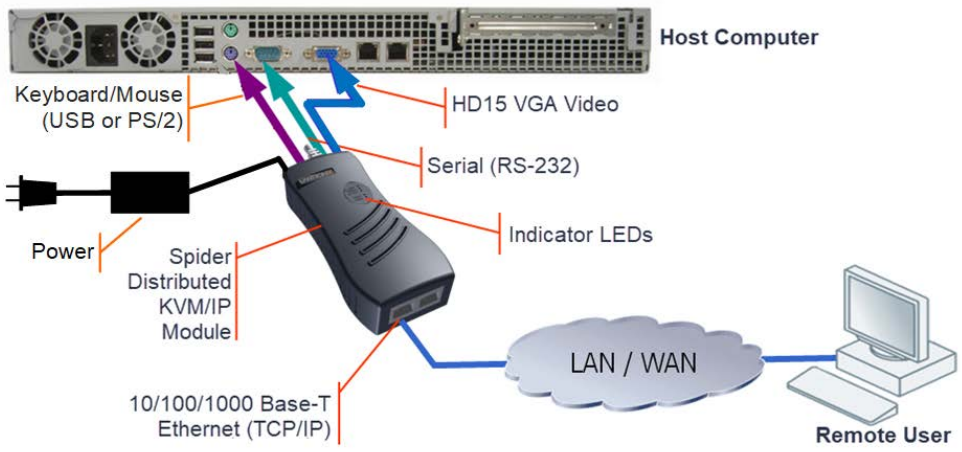


Figure 2-2 Spider Cable Dimensions

Technical Specifications

Table 2-3 lists the components and general specifications.

Table 2-3 Spider Technical Specifications

Component	Specification
Security	◆ Remote Authentication: LDAP, RADIUS, Active Directory ◆ User/Group management with permissions control ◆ Configurable port numbers (HTTPS, Telnet, SSH) ◆ Selective disable of Telnet/SSH ◆ Secure encryption of keyboard, mouse, and video data ◆ AES used as cipher for SSH/SSL communications
Target Server Requirements	◆ Multiple Operating Systems supported: Windows 10, Unix, Linux, or MAC OS X ◆ Keyboard/mouse: 2 USB ports; or 1 PS/2 keyboard connector and 1 PS/2 mouse connector ◆ Video Interface: HD15 VGA video output
Client System Requirements	◆ Microsoft Edge, Mozilla Firefox 100+, Safari 15+, Google Chrome 107+ ◆ Telnet/SSH client for command line (CLI) access
Optional Items	◆ Replacement mounting bracket kit (see *Appendix C: Mounting Bracket Kit*)
Interfaces	◆ Network: One 10/100/1000 Base-T Ethernet Port with activity indicators (RJ45) ◆ Cascade: One 10/100/1000 Base-T Ethernet Port with activity indicators (RJ45) ◆ Serial: RS-232, up to 115,200 bps ◆ Keyboard/Mouse: PS/2 or USB ◆ Video: HD15 VGA ◆ Physical device reset switch (accessible via pinhole)
Power Requirements	◆ Input: 5 VDC @ 2A max. (Target server powered HD15 VGA)
Environmental	◆ Operating: 0º to 45º C (32º to 115º F) ◆ Storage: -20º to 70º C (-4º to 158º F) ◆ Humidity: 0 to 95% RH (non-condensing) ◆ Heat Dissipation: 6 Watts (20 BTU/hr)
Dimensions (H x W x D)	◆ 13.2 x 5.8 x 3.1 cm (5.2 x 2.3 x 1.2 in) (See *Figure 2-2* for cable dimensions.)
Weight	◆ 185g (6.6 oz)
Shipping Weight	◆ .5 kg (1.0 lbs)

SpiderDuo Overview

The SpiderDuo features, functionality, system configuration and cables, and technical specifications are described in the following sections:

- *Features*
- *Functionality*
- *System Configuration and Cables*
- *Technical Specifications*

Features

SpiderDuo provides secure, remote KVM and over-IP capabilities as well as transparent local access. Coupled with the optional single port power control unit (PCU), remote users can also initiate system power cycles over the network. SpiderDuo allows complete local, plus remote management of the host machine anytime,from virtually anywhere.

There are two SpiderDuo models: one model with both PS/2 and USB keyboard and mouse interfaces (software selectable), and one model for USB-only systems. They have the following features:

- Secure, full BIOS-level control of remote servers over an IP network plus transparent local access
- Space–saving “zero footprint” package attaches directly to the server that saves rack space
- Guaranteed non-blocked access to remote servers that ensures lowest “cost-per-remote user”
- Browser–based, no client software or special licensing required
- Direct KVM minimizes the number of clicks to the remote–server console
- Built-in RS-232 serial port that can be configured for serial console port access and host pass-through access
- Ideal for distributed IT system environments such as small branch offices, campuses, test labs, and server hosting environments
- Local access and up to 8 simultaneous remote users
- Optional power control unit (PCU)

Functionality

The SpiderDuo provides local access for distributed server management in addition to the following functionality:

- Captures the video output from the attached computer.
- Compresses the video and sends it over the network to a KVM console window launched by the browser or to a command line on the user system, which draws a replica of the server video output on the user monitor.
- Uses KVM console to accept keystrokes and mouse movements on the user system; recognize those intended for the target computer; transmit the keystrokes and mouse movements; and emulate a physically attached keyboard and mouse.

System Configuration and Cables

Figure 2-4 shows a SpiderDuo system configuration, *Figure 2-5* shows the PS/2 cable dimensions, and *Figure 2-6* shows the USB cable dimensions.

Figure 2-4 SpiderDuo System Configuration

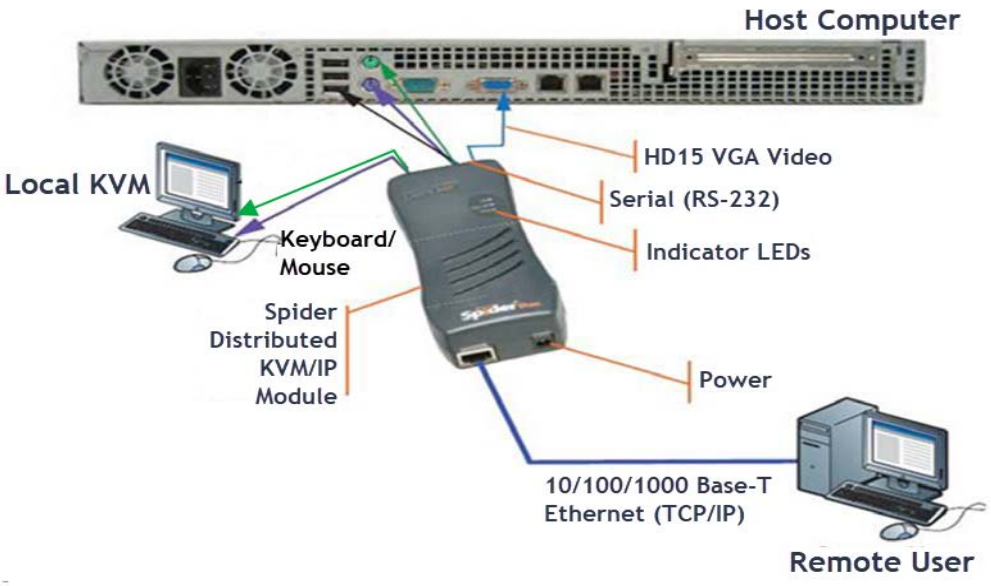


Figure 2-5 shows the PS/2 cable dimensions.

Figure 2-5 SpiderDuo PS/2 Cable Dimensions

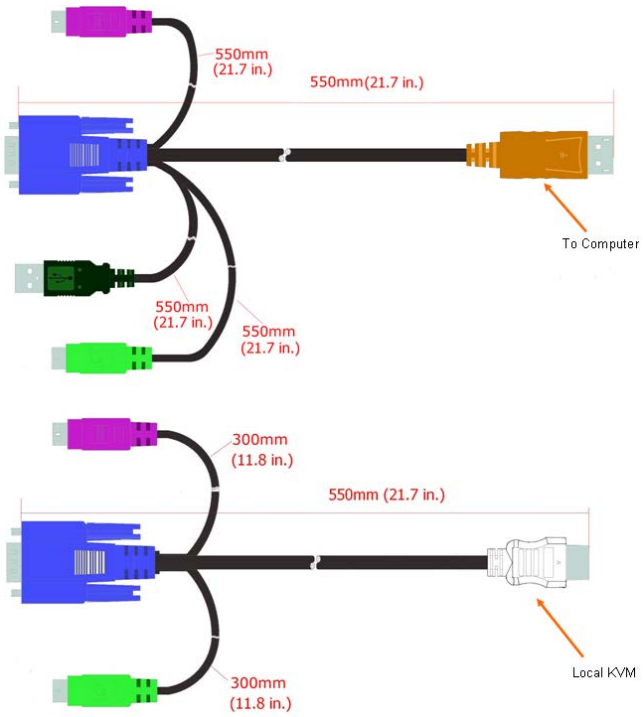
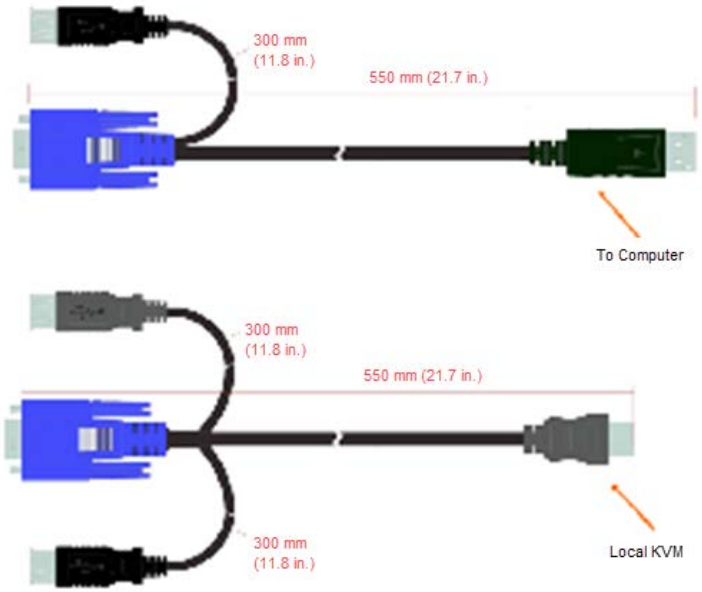


Figure 2-6 shows the USB cable dimensions.

Figure 2-6 SpiderDuo USB Cable Dimensions



Note: *The PS/2 cables and USB cables cannot be mixed and matched with each other due to the unique properties of each. Use the cables that come with your SpiderDuo.*

Technical Specifications

Table 2-7 lists the general components and the specifications.

Table 2-7 SpiderDuo Technical Specifications

Component	Specification
Security	◆ Hardware based encryption of keyboard, mouse and video data ◆ Remote Authentication: LDAP, RADIUS, Active Directory ◆ User/Group management with permissions control ◆ Configurable port numbers (HTTPS, Telnet, SSH) ◆ Selective disable of Telnet/SSH
Target Server Requirements	◆ Multiple Operating Systems supported: Windows 10, Unix, Linux, or MAC OS X ◆ Power/keyboard/mouse: 2 USB ports; or 1 USB and 1 PS/2 keyboard and 1 PS/2 mouse connector ◆ Video Interface: HD15 VGA video output (up to 1600 x 1200 at 60Hz)
Client System Requirements	◆ Microsoft Edge, Mozilla Firefox 100+, Safari 15+, Google Chrome 107+ ◆ Telnet/SSH client for command line (CLI) access
Optional Items	◆ Replacement mounting bracket kit (See *Appendix C: Mounting Bracket Kit*.) ◆ PS/2 extended length cable: 1500mm, (59 in.) part number 500-199-R ◆ USB extended length cable: 1500mm, (59 in.) part number 500-200-R
Interfaces	◆ Network: One 10/100/1000 Base-T Ethernet Port with activity indicators (RJ45) ◆ Serial: RS-232, up to 115,200 bps ◆ Keyboard/Mouse: PS/2 or USB ◆ Video: HD15 VGA ◆ Physical device reset switch (accessible via pinhole)
Environmental	◆ Operating: 0º to 45º C (32º to 115º F) ◆ Storage: -20º to 70º C (-4º to 158º F) ◆ Humidity: 0 to 95% RH (non-condensing) ◆ Heat Dissipation: 6 Watts (20 BTU/hr)
Power Requirements	◆ Input 5VDC 2A Wall Adaptor, part number 520-0184-00.
Dimensions (H x W x D)	◆ 13.2 x 5.8 x 3.6 cm (5.2 x 2.3 x 1.4 in) (See *Figure 2-5* (PS/2) and *Figure 2-6* (USB) for cable dimensions.)
Weight	◆ USB: 269g (9.50 oz) ◆ PS/2: 278g (9.80 oz)
Shipping Weight	◆ 1.5 kg (3.3 lbs)

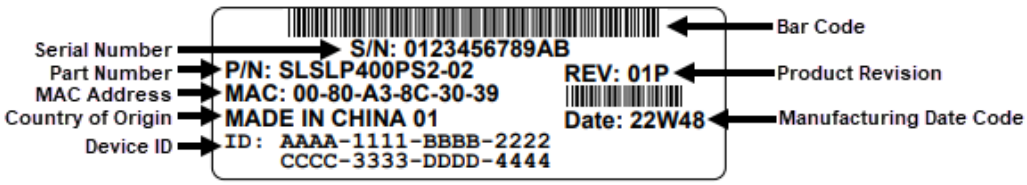
Product Information Label

The Product Information Label on the back of the Spider family units contains the following information:

- Serial Number
- Part Number
- MAC Address
- Country of Manufacturing Origin
- Device ID
- Bar Code
- Product Revision
- Manufacturing Date Code

Figure 2-8 shows the Product Information Label.

Figure 2-8 Spider Family Product Information Label



Features in 4.x vs 5.x Firmware

This section lists the differences between Spider models running firmware version 4.x and earlier and models running firmware version 5.x and newer.

- 5.x has enhanced security algorithms for TLS and SSH.
- 5.x has expanded CLI functionality, with additional diagnostics, logging, release notes, and status information.
- 5.x has full HTML5 support and does not require a Java runtime environment to be installed on the client system.
- 5.x supports ConsoleFlow for centralized management of multiple Lantronix out-of-band devices.
- 5.x Virtual Media supports CD-ROM ISO files.
- Spider devices running 4.x can be powered via the USB connection to the target server; Spider devices running 5.x require an external AC/DC power supply.

3: Installing the Spider Device

This chapter describes how to install the Lantronix Spider KVM-over-IP device. It contains the following sections:

- *Package Contents*
- *Installing the Spider*
- *Target Computer Setup*
- *Client Server Setup*
- *Network Environment*
- *Spider Power*

For technical specifications of the Spider KVM-over-IP device, see *Chapter 2: Overview*.

Package Contents

In addition to the Spider distributed KVM -over-IP module, the package contains the following items:

- Null modem DB9F to RJ45 serial cable (30.48 mm;120 in)
- AC Power Cables (1830 ± 30 mm;72 ± 1.2 in)
- Mounting kit (see *Appendix C: Mounting Bracket Kit*)
- External AC/DC power supply
- *Quick Start Guide*

Note: *This product is intended to be supplied by a Listed Power Adapter or DC power source marked "L.P.S." (Limited Power Source), rated 5 VDC, min. 2.0 A, maximum ambient temperature 40C minimum. Please contact Lantronix for further assistance. When a Class I adapter is used, the power cord of the adapter should be connected to a socket with an earthing connection.*

Note: *The Spider device should be used with UL-listed Information Technology Equipment only.*

Installing the Spider

Consider the following factors when planning the installation of the Spider device.

- USB Keyboard and Mouse Interfaces—Provides better remote cursor tracking. Some older systems may not support USB devices or there may not be two USB ports available. In these cases, the PS/2-interface model may be required. You configure either interface by using the software.
- Serial Port—Supports initial configuration of the Spider via a PC or laptop running a terminal emulator, e.g. HyperTerminal. Also supports management of the target host via Telent or SSH - the target host console port can be connected to the Spider serial port, and remote users can Telnet or SSH to the Spider and then connect directly to the target host console port, thus

providing a backup connection in case the primary LAN connection to the target host is unavailable.

- Ethernet Ports—Connects to the LAN. The Spider device contains a hardware Ethernet switch that connects to the external ports and an internal CPU. The first port is required for network connection. The second port can be used for the following:
  - Tie all of the Spider units in a rack together so that one network connection only is required. While this configuration is a “daisy” chain physically, logically each Spider device has its own IP address on the network. Because the Spider device data that comes from the end of the chain traverses all of the switches, latency increases and responsiveness degrades depending on the number of devices in the chain.

    Lantronix recommends a maximum of 16 Spider devices in a chain. But, if the network switch that connects to the Spider device chain supports Spanning Tree, the first and last devices in the chain can connect to the same network switch to provide resilience against a single-point failure.
  - Connect to the LAN management port on the server, so that an external management network can interface to the Spider device and the server by using one cable.
  - Connect to the main LAN port on the server. If physical isolation of management and user data is not a concern, a single LAN cable can provide connectivity to the Spider device and server conserving a switch or router port.
  - Aggregate any other Ethernet connection as a general-purpose switch port.
- Batch vs. Individual Setup—Deploying a batch of Spider devices at once should be performed as a stage before attaching to the computers. The staging can be performed on a bench prior to configuration. Consider the following tips for configuring a batch of Spider devices:
  - Keyboard, video, and mouse connections are not required for setup. All you need are a source of power and a serial connection to set up the network parameters, and an Ethernet connection to access the administration user interface.
  - Tag each Spider device with its IP address or write it on the serial number label on the bottom.

Perform the following steps to install the Spider device and configure the initial network settings.

1. Plug the RJ45 cable into the Spider serial port which is shown in *Figure 3-1*. The RS-232 protocol is the standard for serial binary data signals.

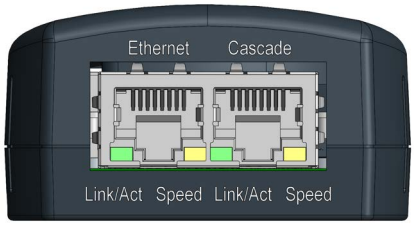
Figure 3-1 Spider RS-232 Serial Port and Pinouts

Pinouts	
1 RTS	(out)
2 --	(out)
3 TX	(out)
4 GND	
5 GND	
6 RX	(in)
7 --	(in)
8 CTS	(in)

2. Plug the DB9F cable into the serial (COM) port of a PC or laptop running a terminal emulator, for example, HyperTerminal. The default serial port settings are: 9600 bits per second, 8 data bits, no parity, 1 stop bit, no flow control. Plug the power adapter into the Spider’s power connector.

3. Plug an Ethernet cable connected to your network into the Ethernet port. The Link/Act LED in the RJ45 illuminates. The RJ45 jack is shown in *Figure 3-2*.

Figure 3-2 Spider RJ45 Ethernet and Cascade Ports



4. Plug the Spider video, USB, and PS/2 keyboard and mouse cables into the target computer. The Spider device boots.
5. The SysOK LED flashes green to indicate that the Spider device is booting. Bootup should complete within one minute. The SysOK LED stops flashing and remains illuminated. *Table 3-3* lists the LED labels, colors, and actions.

Table 3-3 Spider LEDs

Label	Color	Action
Pwr1	**Blue**	Steady to indicate external power is connected.
Pwr2	**Blue**	Steady to indicate external power is connected.
SysOK	**Green**	Blinks upon bootup. Steady to indicate device is up and healthy.
Video	**Green**	Indicates that video (VSync) is transmitting from target server. Off during bootup; steady to indicate connection to target server; off when not connected.
Unit ID	**Orange**	Location beacon to assist in finding unit. Off by default; steady if System Identifier is on - see *Device Status on page 77*.

6. When the bootup process completes, the terminal window displays the login prompt as shown in *Figure 3-4*.

Figure 3-4 Spider Login Window

```
Welcome!
Choose a command for the following features:
-Initial IP configuration: "config".
-Change default sysadmin password: "password".
-Exit quick setup: "quit".
[172.18.0.100 SLSa38bffdc]>
```

7. To change the default IP auto-configuration settings, type **`config`** at the login prompt and press Enter. At the IP configuration prompt, follow the prompts as shown in *Figure 3-5*:

Figure 3-5 Spider Prompts

```
[172.18.0.100 SLSa38bffdc]> config
IP autoconfiguration (none/dhcp) [dhcp]: none
IP [172.18.0.100]:
NetMask [255.255.255.0]:
Gateway (0.0.0.0 for none) [172.18.0.100]:
LAN interface speed (auto/10/100/1000) [auto]:
LAN interface duplex mode [auto/half/full) [auto]:
Are the entered values correct? Enter y for Yes, n for No or c to Cancel: y

Configuring device ...
Done.
```

- To change the default IP configuration from DHCP to a static IP address, type **none** and press Enter.
  - Follow the remaining prompts to enter the IP address, subnet mask, default gateway, and LAN interface setting, pressing Enter after each entry. To accept the displayed setting, press Enter at each prompt to skip to the next option.
  - Press **y** to accept the changes. The system takes several seconds to update the internal protocol stack and display the updated information.

8. To change the sysadmin user password, type **password** at the login prompt and press Enter. At the prompt, type your password, and press Enter. Retype your password when prompted and press Enter again to confirm.
9. To leave the quick setup menu, type **quit** at the login prompt and press Enter.

Target Computer Setup

Setting up the target computer involves ensuring that the video resolution and refresh rates are correct for the target computer monitor; that the mouse-to-cursor movement is synced properly; that the Telnet/SSH connections match the Spider device; and, that the cable connections are correct. Each of these items are discussed in more detail in the following:

- *Video Resolutions and Refresh Rates Configuration*
- *Mouse-to-Cursor Synchronization*
- *Telnet/SSH Connections to Serial Ports*
- *Cable Connections for KVM and USB*

Video Resolutions and Refresh Rates Configuration

The Spider device recognizes video resolutions on the target computer up to a maximum of 1600 x 1200 at 60 Hz. For the complete list of supported video resolutions and refresh rates, see *Appendix B: Supported Resolutions and Refresh Rates*.

Note: *Other supported resolutions and refresh rates are recognized by the Spider device, but could be difficult if the timing does not comply with the extended display identification data (EDID) standard that Spider device supports.*

Perform the following steps to configure the video resolution and refresh rate.

- **Windows Server**

1. Select **Control Panel > Display > Settings**. Modify the screen resolution value as required.
2. Select **Control Panel > Display > Settings > Advanced > Monitor**. Modify the screen refresh rate. Because the server video card is driving the Spider device and not a monitor, a refresh rate higher than 60 Hz has no effect.

- **Linux Server**

1. Edit the Xfree86 file “XF86Config” to disable formats that are not supported or not VESA standard timing.
2. Reboot is required.

Notes:

- Background wallpaper and desktop appearances do not have any particular limitations.
- Microsoft Active Desktop and Linux virtual desktop are not supported. If bandwidth is a concern, plain backgrounds are preferred.
- If you are using a special video card or OS, consult the documentation.

Mouse-to-Cursor Synchronization

Mouse-to-cursor synchronization can be an issue with digital KVM interfaces because PS/2 mice transmit incremental information about movement over a period of time rather than an absolute measurement.

The OS driver translates acceleration-to-distance based on the local screen resolution and applies linear or nonlinear acceleration mappings. When a remote client communicates with the target server, settings and screen resolutions on both sides of the connection must be taken into account to get natural mouse-to-cursor tracking.

Use the USB keyboard and mouse when supported by the target computer. Unlike the PS/2 interface, a USB mouse uses absolute coordinates rather than relative coordinates and does not present translation issues between the local and remote computers.

The PS/2 Spider model sets the keyboard and mouse interface to Auto. When it first attempts to use the USB interface, and if it does not detect a USB interface, it falls back to PS/2.

There are no restrictions on the mouse settings of the client systems and no special care must be taken when setting mouse parameters of target servers for USB mice. The PS/2 interface performance (tracking) and synchronization can be optimized by removing any special acceleration or nonlinear ballistics.

Perform the following steps to configure the mouse-to-cursor synchronization.

- **Windows Server**

1. Select **Control Panel > Mouse > Pointer Options**.
2. Set the pointer speed to medium and disable **Enhanced pointer precision**.

- **Linux Server**

1. Set **Mouse Acceleration** to exactly 1 and threshold to exactly 1.
2. Select **Other Operating Systems** on the Spider mouse settings page.

- **Solaris Server**

1. Set the mouse settings by using the CDE control panel to “1:1, no acceleration” or “xset m 1”.

- **Mac OS X Server**

1. Set the Spider device to **Single Mouse Mode**.

Telnet/SSH Connections to Serial Ports

To use Telnet/SSH to access the target computer serial port, you must Telnet/SSH to the Spider serial port first and use `connect serial` CLI. This connects your Spider device to the target computer serial port. The serial port must be put in passthrough mode with the appropriate connection parameters and cabling, with Telnet and/or SSH access allowed. The default settings are 9600 bps, 8 data bits, 1 stop bit, no parity, and no flow control. The pinout of the included Spider cables match a standard DB9 COM port.

Cable Connections for KVM and USB

Connections for KVM and USB are integrated into the Spider device. Do not use extension cables. Plug the Spider device directly into the ports on the host server. If using the Spider serial port, plug the cable into the COM port on the server.

The second Cascade Ethernet port can connect to the Spider device to the target computer management LAN port, or to a main LAN port, or to a Spider device chain. When connecting the Ethernet ports, straight through or crossover cables can be used, because the Spider device has auto-polarity and auto-crossover correction. Although the port marked Ethernet and the port marked Cascade are both Ethernet interfaces, you must use the port marked Ethernet to supply an IP connection to the Spider device. This could be through a switch, router, or another Spider device in a daisy chain that eventually connects to a switch or a router.

Perform the following steps when daisy chaining Spider devices.

1. Plug the outside network cable into the left Ethernet port of the first Spider device.
2. Connect the right Cascade port to the left port of the next Spider device in the chain.
3. Repeat as necessary. The last Spider device in the chain should have its right port unoccupied, unless cabling in a loop for redundant connection.

Device Failure or Cable Break in the Daisy Chain

If a device fails or there is a cable break in the daisy chain, there could be a loss of network connectivity for all devices downstream from the cable break or device failure. Avert this issue by installing Spanning Tree in the switch or router to which the initial Spider device in the daisy chain attaches. Then, connect the last Spider device from its Cascade port to the same switch so that there is a redundant outside connection.

Spanning Tree protocol implemented in the switch disables one of the two network connections while the loop remains complete. Data flows in one direction only around the loop. If the loop breaks, Spanning Tree activates both connections, so that data flows in both directions. All devices in the Spider device chain are accessible except the one immediately downstream from the cable break or failed device. Do not try this workaround without Spanning Tree installed.

Client Server Setup

Two mechanisms provide the monitoring of client servers that are connected through the Spider device: platform-dependent management and platform-independent management.

- Platform-dependent management—Spider View software is a standalone Windows 10 or later application that locates, manages, and accesses multiple Spider devices in an integrated

view. Spider View software requires ActiveX controls enabled. Refer to the *Spider View User Guide* at https://www.lantronix.com/support/documentation.html for instructions on installation and operation of Spider View software.

- Platform-independent management—Each Spider device contains an embedded web server that delivers web pages, a KVM Remote Console program, and a terminal program. To access and manage the client server, a web browser running the latest version is required (Chrome, Edge, Firefox, Safari).

Network Environment

The connection between the client and Spider device must be open to IP traffic and use TCP port 443 (HTTPS). Firewalls and NAT devices should be configured to support this configuration. The TCP port can be changed by accessing **Interfaces > Network**.

Lantronix recommends using Fast Ethernet connections and a switched network environment because In a LAN, traffic affects the responsiveness of the Remote Console window.

Spider Power

The Spider device gets power from an external DC power supply (part number 520-0203-00).

Use the power-on reset to reboot the Spider device or reboot from the user interface, from the serial port, or by clicking the reset switch through the pinhole on the back of the body.

4: Installing the SpiderDuo Device

This chapter describes how to install the Lantronix SpiderDuo device. It contains the following sections:

For technical specifications of the SpiderDuo, see *Chapter 2: Overview*.

Package Contents

In addition to the SpiderDuo distributed KVM-over-IP module, the package contains the following items:

- Null modem DB9F to RJ45 serial cable (30.48 mm;120 in)
- AC Power Cables (1830 ± 30 mm;72 ± 1.2 in)
- Local KVM cable
- Computer Input cable
- Mounting kit (See *Appendix C: Mounting Bracket Kit*)
- *Quick Start Guide*
- External AC/DC Power Supply

Warning: ***The connectors on the SpiderDuo device are not regular video connectors. To avoid damage to the SpiderDuo device, do not connect cables of any kind other than the cables provided Lantronix. Use the Lantronix power supply only, part number 520-104-R.***

Note: *This product is intended to be supplied by a Listed Power Adapter or DC power source marked "L.P.S." (Limited Power Source), rated 5 VDC, min. 2.0 A, ambient temperature 0C minimum, 40C maximum. Please contact Lantronix for further assistance. When a Class I adapter is used, the power cord of the adapter should be connected to a socket with an earthing connection.*

Note: *The SpiderDuo device should be used with UL-listed Information Technology Equipment only.*

Installing the SpiderDuo

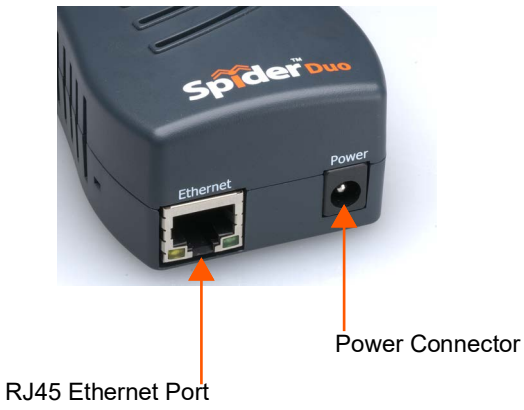
Consider the following factors when planning the installation of the SpiderDuo device.

- **USB Keyboard and Mouse Interfaces**—Provide better remote cursor tracking. Some older systems may not support USB devices or there may not be two USB ports available. In these cases, the PS/2-interface model may be required. You configure either interface type by using the software.
- **Serial Port**—Supports initial configuration of the device via a PC or laptop running a terminal emulator, e.g. HyperTerminal. Also supports management of the target host via Telnet or SSH - the target host console port can be connected to the Spider serial port, and remote users can telnet or SSH to the Spider and then connect directly to the target host console port, thus providing a backup connection in case the primary LAN connection to the target host is unavailable. The serial port can also connect to the Power Control Unit (PCU) for use as an AC power passthrough. For more information, see *PCU Power on page 38*.
- **Ethernet Port**—Connects to the LAN. The SpiderDuo device has one port only that connects to the LAN.
- **Local KVM Port**—Connects keyboard, video, and mouse to the local client.

Perform the following steps to install the SpiderDuo device and configure the initial network settings.

1. Plug the RJ45 cable into the SpiderDuo serial port.
2. Plug the DB9F end of the RJ45 cable into the COM port of a PC/laptop running a terminal emulator, for example HyperTerminal. The default serial port settings are: 9600 bits per second, 8 data bits, no parity, 1 stop bit, no flow control.
3. Plug an Ethernet cable connected to your network into the Ethernet port. The Link LED illuminates.
4. Plug the power adaptor into the SpiderDuo power connector.

Figure 4-1 SpiderDuo RJ45 Port and Power Connector



5. Plug the SpiderDuo video, USB, and PS/2 keyboard and mouse (if applicable) cables into the target computer. The blue LED SysOK lluminates and flashes to indicate that the SpiderDuo device is booting up. Bootup completes within approximately one minute. The SysOK LED stops flashing and remains illuminated. Connections for video, USB, and keyboard/mouse are integrated into the SpiderDuo device.

Figure 4-2 SpiderDuo Local KVM, USB, Computer Input and Serial Ports

Pinouts

Pin#	RS-232	PCU
1	RTS	--
2	--	V
3	TX	--
4	Ground	Sense
5	Ground	Ground
6	RX	--
7	--	Relay Driver
8	CTS	--

Table 4-3 SpiderDuo Indicator LEDs

Label	Color	Action
ID	**Amber**	On - Unit ID Selected Blinking -Thumb-drive Configuration Successful
SysOK	**Blue**	On - Powered up and OK Blinking - Booting
PCU	**Green**	*On - Power Unit Connected,* AC power is passed through

6. Upon bootup, the terminal window displays the login prompt as shown in *Figure 4-4*.

Figure 4-4 SpiderDuo Login Window

```
Welcome!
Choose a command for the following features:
-Initial IP configuration: "config".
-Change default sysadmin password: "password".
-Exit quick setup: "quit".
[172.18.0.100 SLSa38bffdc]>
```

7. To change the default IP auto-configuration settings, type **`config`** and press Enter. At the IP configuration prompt, follow the prompts as shown in *Figure 4-5*.

Figure 4-5 SpiderDuo Prompts

```
[172.18.0.100 SLSa38bffdc]> config
IP autoconfiguration (none/dhcp/bootp) [dhcp]: none
IP [172.18.0.100]:
NetMask [255.255.255.0]:
Gateway (0.0.0.0 for none): [172.18.0.100]:
LAN interface speed (auto/10/100/1000) [auto]:
LAN interface duplex mode (auto/half/full) [auto]:
Are the entered values correct? Enter y for Yes, n for No or c to Cancel: y

Configuring device ...
Done.
```

- To change the default IP configuration from DHCP to a static IP address, type **`none`** and press Enter.
  - Follow the remaining prompts to enter the IP address, subnet mask, default gateway, and LAN interface setting, pressing Enter after each entry. To accept the displayed setting, press Enter at each prompt to skip to the next option.
  - Press **`y`** to accept the changes. The system takes several seconds to update the internal protocol stack and display the updated information.

8. To change the sysadmin user password, type **`password`** at the login prompt and press Enter. At the prompt, type your password, and press Enter. Retype your password when prompted and press Enter again to confirm.
9. To leave the quick setup menu, type **`quit`** at the login prompt and press Enter.
10. Press **Enter**, to accept the changes. The system takes about 20 seconds to complete. Type **Enter** once again at the prompt to display the updated IP address.
11. Test the system installation (PC, local keyboard and mouse, video, and SpiderDuo) by completing the following:
    a. Turn off the power to the PC and SpiderDuo device.
    b. Reconnect all devices.
    c. Turn on the SpiderDuo device first, and wait for it to boot completely (the SysOK LED will be on steady).
    d. Turn on the PC.

Target Computer Setup

Setting up the target computer involves ensuring that the video resolution and refresh rates are correct for the taget computer monitor; that the mouse-to-cursor movement is sync'd properly; that the Telnet/SSH connections match the Spider device; and, that the cable connections are correct. Each of these items are discussed in more detail in the following:

- *Video Resolutions and Refresh Rates Configuration*
- *Mouse-to-Cursor Synchronization*
- *Telnet/SSH Connections to Serial Ports*
- *Cable Connections for KVM and USB*
- *Power Sequencing*

Video Resolutions and Refresh Rates Configuration

The SpiderDuo devices recognize video resolutions on the target computer up to a maximum of 1600 x 1200 at 60 Hz. For the complete list of supported video resolutions and refresh rates, see *Appendix B: Supported Resolutions and Refresh Rates*.

Note: *The other supported resolutions and refresh rates are recognized by the SpiderDuo devices, but could be difficult if the timing does not comply with the extended display identification data (EDID) standard that SpiderDuo supports.*

Perform the following steps to configure the video resolution and refresh rate.

- **Windows Server**

1. Select **Control Panel > Display > Settings**. Modify the screen resolution value as required.
2. Select **Control Panel > Display > Settings > Advanced > Monitor**. Modify the screen refresh rate. Because the server video card is driving the SpiderDuo device and not a monitor, a refresh rate higher than 60 Hz has no effect.

- **Linux Server**

1. Edit the Xfree86 file "XF86Config" to disable formats that are not supported or not VESA standard timing.
2. Reboot is required.

Notes:

- Background wallpaper and desktop appearances do not have any particular limitations.
- Microsoft Active Desktop and Linux virtual desktop are not supported. If bandwidth is a concern, plain backgrounds are preferred.

Mouse-to-Cursor Synchronization

Mouse-to-cursor synchronization can be an issue with digital KVM interfaces because PS/2 mice transmit incremental information about movement over a period of time rather than an absolute measurement.

The OS driver translates acceleration-to-distance based on the local screen resolution and applies linear or nonlinear acceleration mappings. When a remote client communicates with the target server, settings and screen resolutions on both sides of the connection must be taken into account to get natural mouse-to-cursor tracking.

Use the USB keyboard and mouse when supported by the target computer. Unlike the PS/2 interface, a USB mouse uses absolute coordinates rather than relative coordinates and does not present translation issues between the local and remote computers.

The PS/2 model sets the keyboard and mouse interface to Auto. When it first attempts to use the USB interface, and if it does not detect a USB interface, it falls back to PS/2.

There are no restrictions on the mouse settings of the client systems and no special care must be taken when setting mouse parameters of target servers for USB mice. The PS/2 interface performance (tracking) and synchronization can be optimized by removing any special acceleration or nonlinear ballistics.

Perform the following steps to configure the mouse-to-cursor synchronization.

- **Windows Server**

1. Select **Control Panel > Mouse > Pointer Options**.
2. Set the pointer speed to medium and disable **Enhanced pointer precision**.

- **Linux Server**

1. Set **Mouse Acceleration** to exactly 1 and threshold to exactly 1.

- **Solaris Server**

1. Set the mouse settings by using the CDE control panel to “1:1, no acceleration” or “xset m 1”.

Telnet/SSH Connections to Serial Ports

To use Telnet/SSH to access the target computer serial port, you must Telnet/SSH to the SpiderDuo serial port first and use `connect serial` CLI. This connects your SpiderDuo device to the target computer serial port. The serial port must be put in passthrough mode with the appropriate connection parameters and cabling, with Telnet and/or SSH access allowed. The default settings are 9600 bps, 8 data bits, 1 stop bit, no parity, and no flow control. The pinout of the included SpiderDuo cables match a standard DB9 COM port.

Cable Connections for KVM and USB

Connections for video, USB, and keyboard/mouse are integrated into the SpiderDuo device. Plug the SpiderDuo device directly into the appropriate ports on the host system. If using the serial port, cable it to the appropriate COM port on the server. Available extended-length cables are shown in *Table 4-6*.

Table 4-6 Extended Length Cables

Item	Part Number
USB connector; 1500 mm, (59 in.) VGA cable	500-199-R
PS/2 and USB connectors; 1500 mm, (59 in.) VGA cable	500-200-R

Power Sequencing

To ensure that the system (target computer, local KVM, and SpiderDuo device) function properly at power up, it is recommended that the following procedure be performed.

1. Ensure that the target computer and SpiderDuo are powered off.
2. Make connections for all devices.

3. Turn on the SpiderDuo first and wait for the SpiderDuo to boot up completely. The SysOK LED will be on steady.
4. Turn on the target computer.

Client Server Setup

Two mechanisms provide the monitoring of client servers that are connected through the Spider device: platform-dependent management and platform-independent management.

- Platform-dependent management—Spider View software is a standalone Windows 10 or later application that locates, manages, and accesses multiple Spider devices in an integrated view. Spider View application requires ActiveX controls enabled. Refer to the *Spider View User Guide* at https://www.lantronix.com/support/documentation.html for instructions on installation and operation of Spider View software.
- Platform-independent management—Each Spider device contains an embedded web server that delivers web pages, a KVM Remote Console program, and a terminal program. To access and manage the client server, a web browser running the latest version is required (Chrome, Edge, Firefox, Safari).

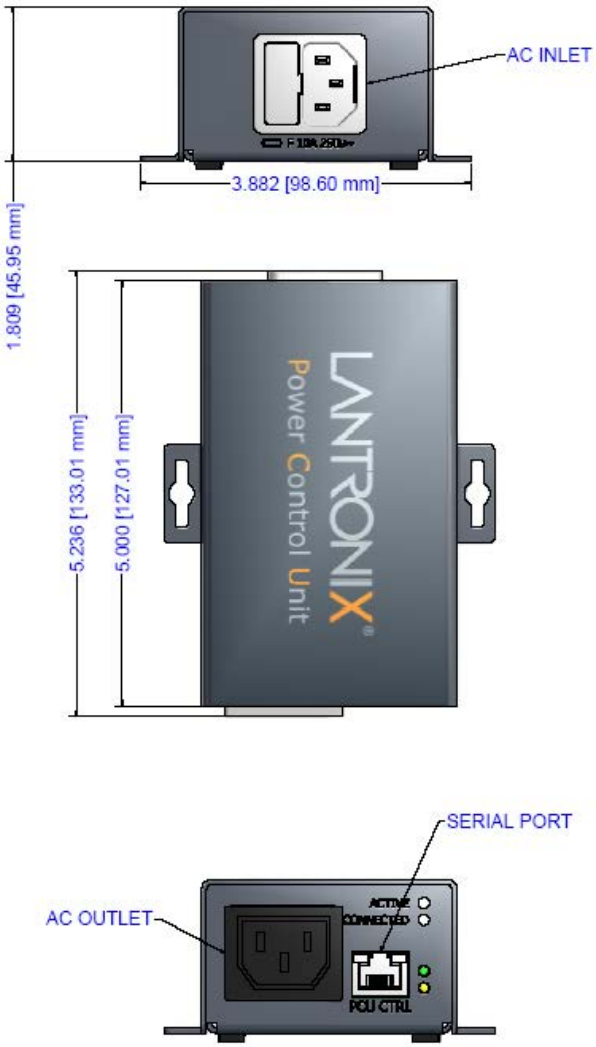
Network Environment

The connection between the client and SpiderDuo device must be open to IP traffic and use TCP port 443 (HTTPS). Firewalls and NAT devices should be configured to support this configuration. The TCP port can be changed by accessing **Interfaces > Network**.

PCU Power

To remotely control power to a PC and other equipment, an optional PCU is available (part number PCU100-01). The PCU manages power remotely to a target PC and other equipment. In addition, the user can restart or power-cycle the PC and other equipment. *Figure 4-7* shows the layout and dimensions of the PCU.

Figure 4-7 PCU Layout and Dimensions



Complete the following tasks to connect the PCU.

1. Connect the power output plug to a target PC or other equipment.
2. Connect the RJ45 cable from the PCU to the SpiderDuo serial port.
3. Connect the power input plug to AC power. Green LED = PCU ON (AC power pass- through), Blue LED = Sys OK.

Warning: ***AC power passes through by default if the RJ45 cable is disconnected from the PCU.***

The SpiderDuo device gets its power from an external DC supply. Replacement power supplies are available.

Note: *When the PCU is connected to the Spider Duo, the Configuration Login flow control must be set to "None"; see* *Serial Port Settings on page 49* *for more information.*

5: Web Browser Access

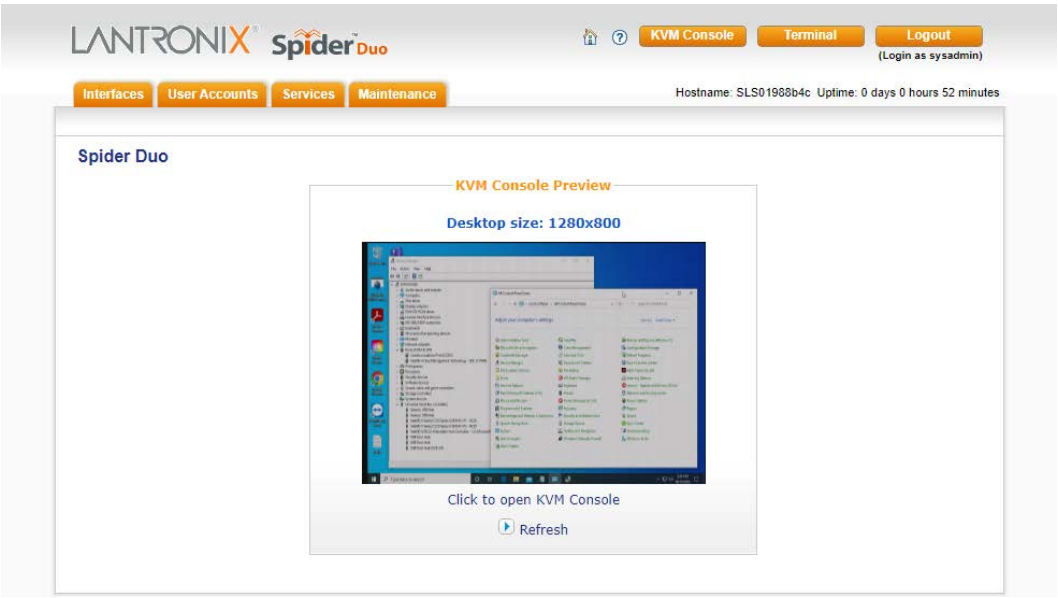
This chapter describes how to use the Lantronix Spider and SpiderDuo KVM-over-IP device to access and manage a target computer by using a Web browser or remote system.

Accessing the KVM Console

Perform the following steps to use a web browser.

1. Access the Spider or SpiderDuo device over the network by using a web browser by entering `https://<ipaddress>` (for a secure SSL connection). The browser must accept cookies for login.
2. Enter your user name (default is `sysadmin`) and password (default is `PASS`) at the prompt. The home page displays. From the home page the Remote **KVM Console** or Telnet **Terminal** session can be launched as shown in *Figure 5-1*.

Figure 5-1 Spider Device Home Page



The home page contains the following items:

- Snapshot of the target system video in the KVM Console Preview window in the center
- Session and host name information
- Tabs called Interfaces, User Accounts, Services, and Maintenance on the left
- Buttons including a **Logout** button on the right.

When you are logged in, you can make changes to the configuration and user database. You can set up the device for local or remote authentication for other users and define the permission level. As sysadmin, you can also make changes to the hardware settings, establish configuration parameters, and perform maintenance operations.

6: Remote System Control

This chapter describes the components of remote system control. It contains the following sections:

Overview

The Lantronix Spider and SpiderDuo devices control the target system by using a Remote Console. The Remote Console has settings that apply each time a user launches it. Other settings can be applied within the window itself. By scaling the window down in size, it is possible to have multiple Remote Console windows open, allowing interaction with multiple target systems.

Remote Console Window

The Remote Console window shows a real-time replica of the target system video (mimicking a monitor plugged directly into the remote computer). When the local computer window displays in the Remote Console window, mouse movements and keystrokes are transmitted to a remote computer. The title bar of the window shows the IP address of the Spider device or SpiderDuo (useful when multiple windows are open on the client system).

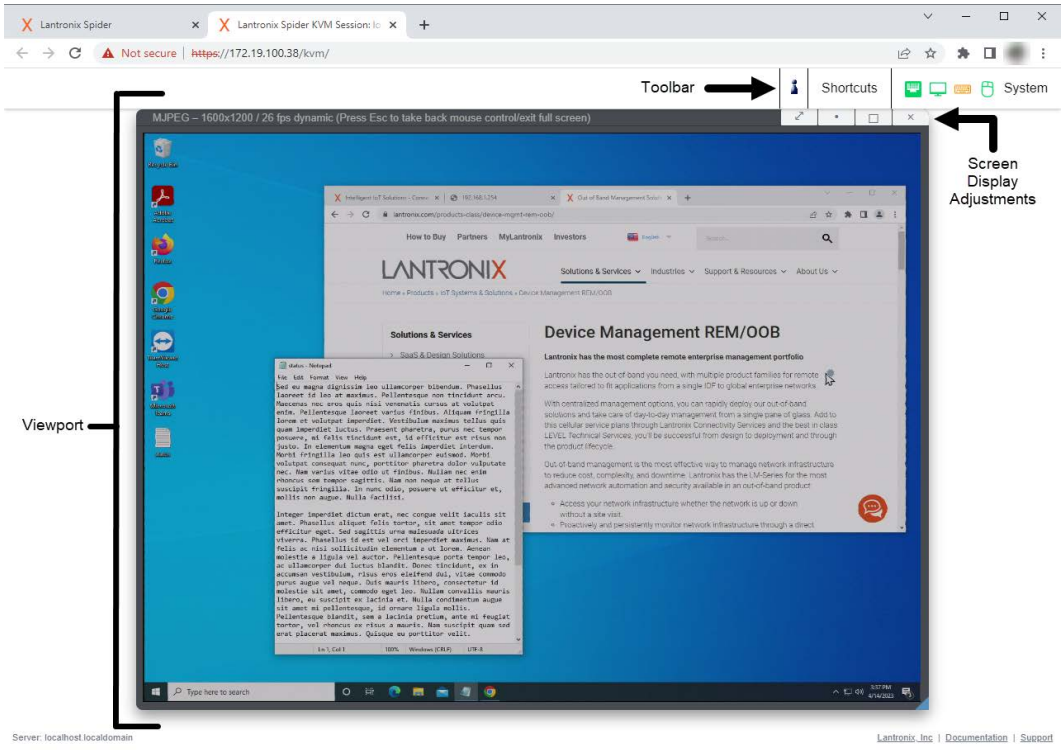
The Remote Console window can be minimized, maximized, or scaled in either direction. There are Main viewport and scroll bars, button keys, and a toolbar which are described in the following subsections.

To launch the Remote Console window, perform the following steps.

1. Click **KVM Console** to launch the Remote Console window. The Remote Console window can open in the foreground or in the background. If it launches in the background, click on the icon to bring the window to the front.
2. Or, launch the Remote Console by clicking the link below the preview image on the **KVM Console Preview** window.

   You can enable the Spider or SpiderDuo device to bypass the web page and take you directly to the remote system by clicking **Services > Security > Authentication Limitation > Enable Direct KVM Console Access without Authentication**. This capability is called Direct KVM.

Figure 6-1 Remote Console Window Components



Note: *Appearance and location of components described may vary depending on firmware version.*

Viewport

The full virtual screen of the target computer is mapped pixel for pixel to the console window main viewport

Toolbar

The top-right toolbar has a number of buttons for one-click access to functions, and a drop-down menu where other options may be reached. The icons vary depending on which keyboard interface is active.

- **Concurrent Access State**:

  One user is connected to the Remote Console

  Multiple users are connected to the Remove Console

  This user has exclusive access to the Remote Console. No other clients may access the target system until exclusive access is disabled.

  Another user has exclusive access to the Remote Console. No other clients may access the target system until exclusive access is disabled by that user, or until that user closes their Remote Console window.

- **Shortcuts**—Quick keyboard shortcuts that have been defined to send special key combinations directly to the target computer. See *KVM Console Virtual Keys on page 53* for more information.
- **System**—Displays the status of the connection, screen display, keyboard, and mouse. Click the button to view and modify KVM Console settings, display the virtual keyboard, or reset the keyboard and mouse connection.

Screen Display Adjustments

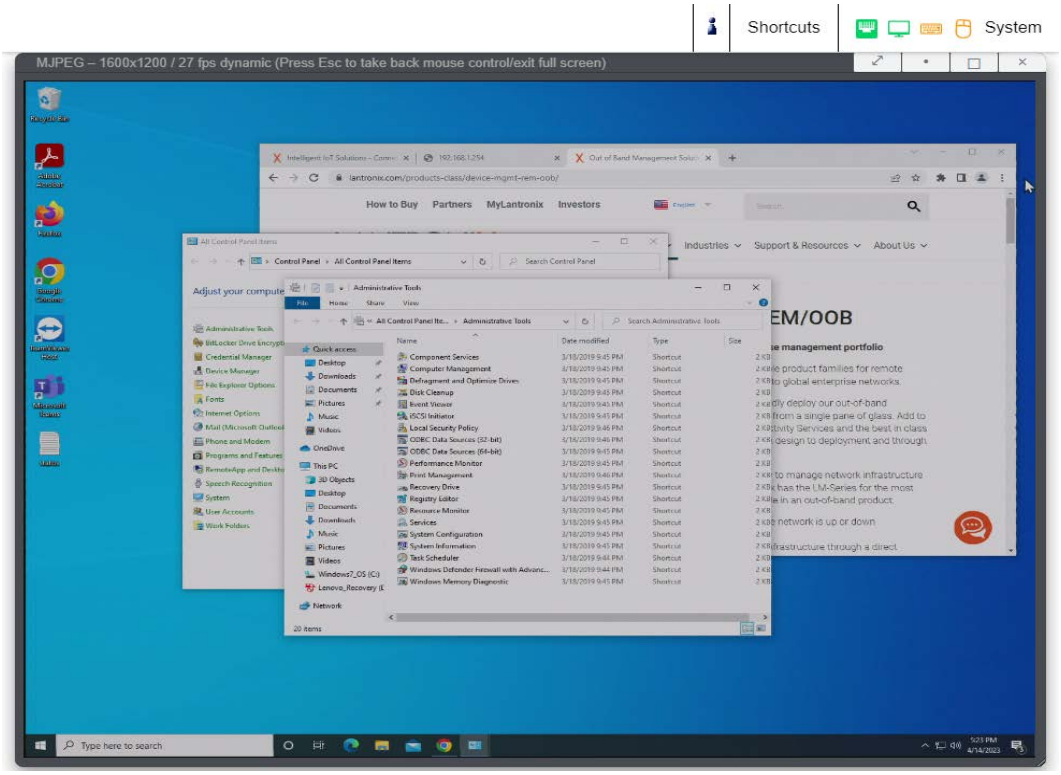
The Screen Display Adjustments toolbar contains buttons that can be used to enter full-screen mode, reset the remote console screen size, maximize the console screen size within the browser window, and close the console screen

Basic Remote Console Operation

When the Remote Console window is open, there are three key zones:

- Outside the Remote Console window (web browser tab), interaction is with the local computer's operating system or applications.
- Inside the Remote Console window's viewport, interaction is with the target computer.
- Inside the Remote Console window but outside the viewport, interaction is with the Remote Console control functions such as the toolbar or scroll bars.

Figure 6-2 Remote Console Window



Within the Remote Console viewport, interaction with the remote computer is generally the same as if there were a direct connection (with a minor lag due to network latency). Windows may be

opened, applications run, settings changed, maintenance functions performed, even system reboots performed. Powering down the target computer results in powering down the Spider device or SpiderDuo unless the redundant supply is used.

Auto Video Adjustment

The left side of the target computer screen must be aligned with the left side of the Remote Console viewport so that the tops align as well. If not, the local and remote cursors will always have a fixed offset of that amount, even if the USB interface is used.

Figure 6-3 Screen Display Adjustments Toolbar

Screen Display Adjustments

The following features facilitate Screen display changes:

- Full Screen Mode (Press and hold **Esc** to return to original size).
- Return viewport to original size.
- Maximize window within browser.
- Close window.

Telnet/SSH/Web Terminal

In addition to interacting with the target system using the KVM Console, the Spider device also allows serial communication with the target via SSH, Telnet, and the Terminal Console (Web Terminal). Telnet and SSH are network protocols that enable a tunnel from the client system to the Spider target device serial port. The Terminal Console is available from the “Terminal” button on the web interface. Once set up, the target may be accessed through the web interface via the Terminal Console window, or using a Telnet/SSH client to connect directly. The user at the client system can send and receive characters directly to the serial port.

Set up and Enable

To use Telnet, SSH, or the Terminal Console, the serial port must be put in passthrough mode with the appropriate connection parameters and cabling with Telnet and/or SSH access allowed. If desired, the TCP port numbers also may be changed from their defaults. A user attempting to connect via Telnet or SSH must also have the appropriate permissions; see *User Permissions on page 61*.

Passthrough Use

When using passthrough mode, the Spider device just acts as a conduit for the serial data traveling between the client system and whatever is connected to the serial port. This may be a COM port on the remote computer, or a serially controlled power strip, or anything else with an RS-232 port.

1. From the client system, use a Telnet or SSH utility to connect to the IP address of the Spider device, at the assigned Telnet or SSH TCP port number. Or, log in to the Spider web UI and click the Terminal button at the top of the page.

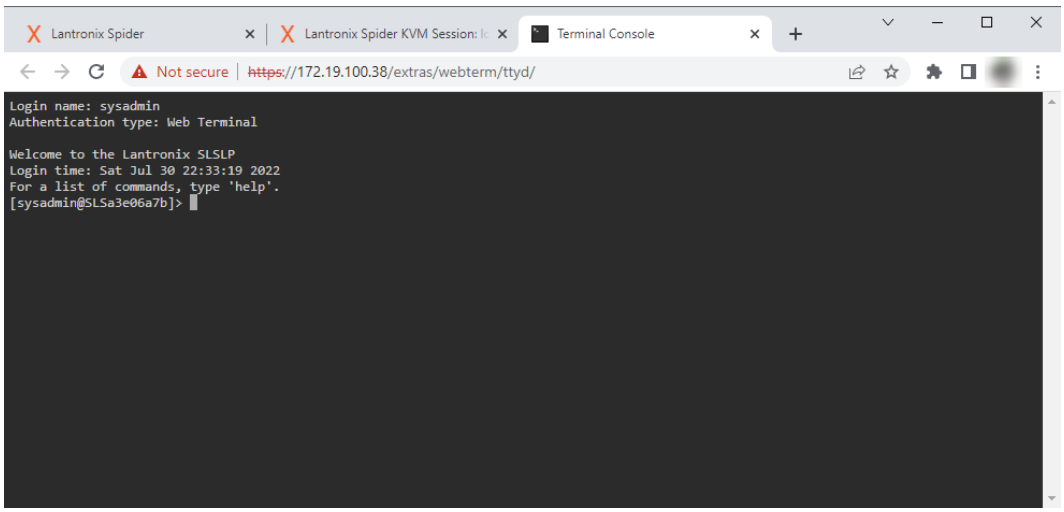
2. The Spider device will present **LOGIN** and **PASSWORD** prompts. Enter a valid user name and password. In the case of Telnet or SSH, the user must have permissions set to use Telnet or SSH.
3. The Spider device will reply with a Welcome and status, followed by a command line prompt. Selections are:
   - **`help`**—Displays a list of commands
   - **`admin version`**—Displays the current Spider firmware version number
   - **`connect serial`**—Enter passthrough to serial port mode
   - **`logout`**—Terminates the Telnet or SSH connection
4. Enter **`connect serial`** to open the connection to the serial port.
5. You are now connected and may interact with the attached serial console. Keystrokes are not locally echoed and must be echoed by the connected serial device.
6. Use the Terminal Console, SSH, or Telnet ability to send and receive serial data between the client and the serial port. The Spider device does not echo this data back to the client.
7. When complete, press **Esc**, then enter `exit` (i.e. the Escape key followed by the characters "`e`", "`x`", "**`i`**", "`t`") to return to the command line.
8. Enter `logout` to close the connection.

Terminal Console Use

When using the Terminal Console, the Spider device opens a window on the client system that provides direct access to the Spider CLI. This eliminates the need to have a Telnet or SSH utility running on the client system.

1. Click the **Terminal** button at the top of the Spider page. The Terminal Console window appears in a new browser tab as shown in *Figure 6-4*. Terminal Console and Remote KVM Console windows may be open concurrently.

Figure 6-4 Terminal Console Screen



7: Interfaces

This chapter describes the Interfaces tab including information about the pages for configuring network, serial port, KVM Console, Keyboard/Mouse, and Virtual Media settings. It contains the following sections:

Network Settings

The first link on the Interfaces tab is Network Settings. Do not forget that changing the settings while connected to the network can result in dropping the connection. This occurs when you click **Save**. Ensure that your new settings are correct when making changes from a remote site before you click **Save**.

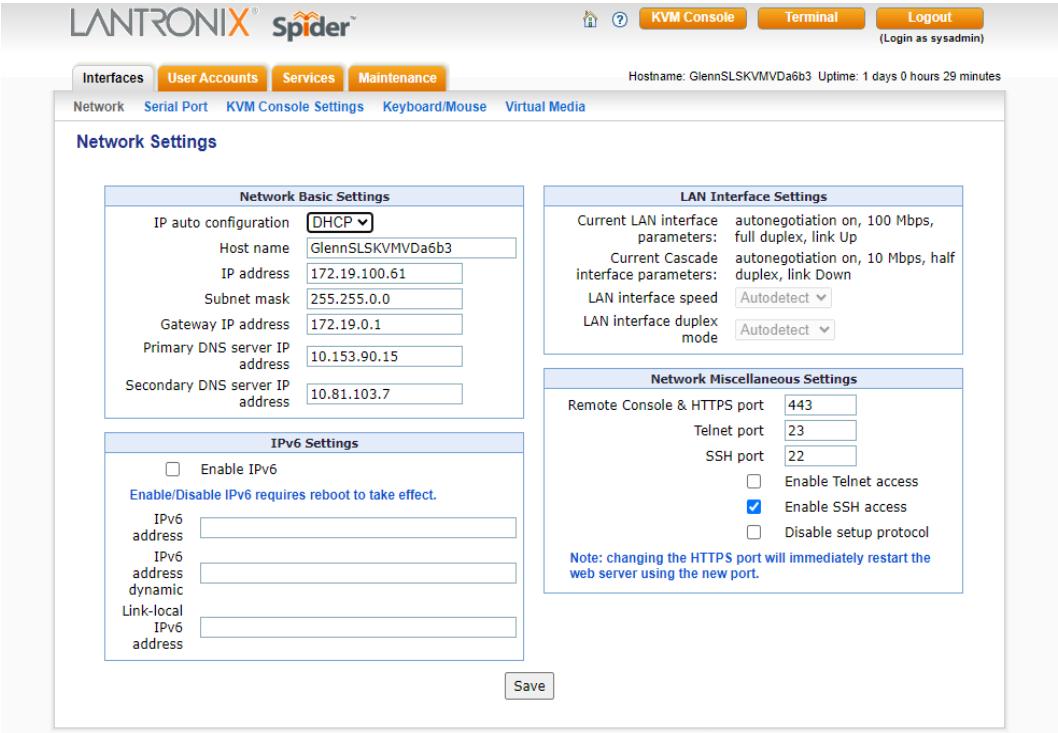
In Network Settings, there are four configuration areas:

- **Network Basic Settings**—Sets auto IP configuration, host name, IP address, subnet mask, gateway address, and primary and secondary DNS server addresses.
- **IPv6 Settings**—Enables IPv6.
- **LAN Interface Settings**—Sets LAN interface speed and duplex mode.
- **Network Miscellaneous Settings**—Enables ports and Telnet/SSH access.

To configure network settings, perform the following steps. (Alternately, the network settings can be modified via the Spider console port CLI.)

1. Click **Interfaces > Network.** *Figure 7-1* shows the page that displays.

Figure 7-1 Spider Network Settings Web Page



2. Modify the following fields.

Network Basic Settings

Field	Description
IP auto configuration	Select **DHCP** to fetch network settings from the appropriate type of server. Select **NONE** for a fixed IP address.
Host name	DHCP servers can register a name for this Spider device to assist in finding it, or you can configure it with a short host name or a fully qualified domain name.
IP address	If you are using a fixed IP address, enter it in the usual dot notation.
Subnet Mask	If you are using a fixed IP address, enter the subnet mask of the local network.
Gateway IP address (optional)	If the Spider device is to be accessible from outside the local subnet, enter the IP address of the router providing access.
Primary DNS Server IP Address (optional)	For name resolution, enter the IP address of the primary Domain Name Server. This is optional, but needed if names rather than static IP addresses are used for certain Spider device functions requiring network connections.
Secondary DNS Server IP Address (optional)	Enter the IP address of the Domain Name Server to be used if the Primary DNS Server cannot be reached.

LAN Interface Settings

Field	Description
Current LAN interface parameters	Displays current LAN interface settings.
Current Cascade interface paramenters	(Spider devices only) Displays current cascade interface settings.
LAN interface speed	Manual setup may be required for older equipment. With Autodetect on, the window displays the current state of the link. Note that the parameters of the second Ethernet port (Spider model only) are not configurable, they remain at Autodetect. Select the speed from the drop-down menu.
LAN interface duplex mode	Select the duplex mode from the drop-down menu.

IPv6 Settings

Field	Description
Enable IPv6	Select to enable IPv6.
IPv6 address	IPv6 address displays when enable IPv6 is selected,
IPv6 address dynamic	Assigned automatically by the system.
Link-local IPv6 address	Network address intended only for communications within one segment of a local network or a point-to-point link. Assigned automatically by the system.

Note: *When using link-local IPv6 addresses, the scope zone has to be included with the link-local address for communication; see RFC4007.*

To specify an IPv6 non-global address (link local address) without ambiguity, the intended scope zone should be specified as well. The scope zone for an IPv6 address is not encoded within the address itself, but is instead determined by the interface over which the packet is sent or received. The scope zone is attached to non-global IPv6 addresses using the '%' symbol [RFC6874].

The '%' symbol in a URL may not be supported by web browsers in directing to the web server; instead search results will be shown. This behavior depends on the underlying OS - Microsoft scope zones are in integers whereas GNU Linux scope zones are ASCII characters.

Example:

URL: https://[fe80::e65f:1ff:fe98:8b24%enp0s31f6]:443

```
curl -k -u sysadmin:pass https://
[fe80::e65f:1ff:fe98:8b24%enp0s31f6]:443/api/info?fields=meta

telnet fe80::e65f:1ff:fe98:8b24%enp0s31f6

ssh sysadmin@fe80::e65f:1ff:fe98:8b24%enp0s31f6
```

Network Miscellaneous Settings

Field	Description
Remote Console & HTTPS port	Port number at which the Spider device Remote Console server and HTTPS server are listening. The default is 443.
Telnet port	Port number at which the Spider device's Telnet server is listening. The default is 23.
SSH port	Port number at which the Spider device's SSH server is listening. The default is 22.
Enable Telnet access/ Enable SSH access	For security, by default Telnet is disabled and SSH is enabled. Check the appropriate box(es) and optionally set up the serial port for Telnet/SSH to use the Telnet console.
Disable Setup Protocol	The Spider View application and KVM Search use a special protocol to locate and set up Spider device IP addresses. As a security measure you may wish to disable this protocol when deploying Spider devices. If the protocol is disabled, the Spider device network will not find the Spider device.

3. Click **Save** to save settings.

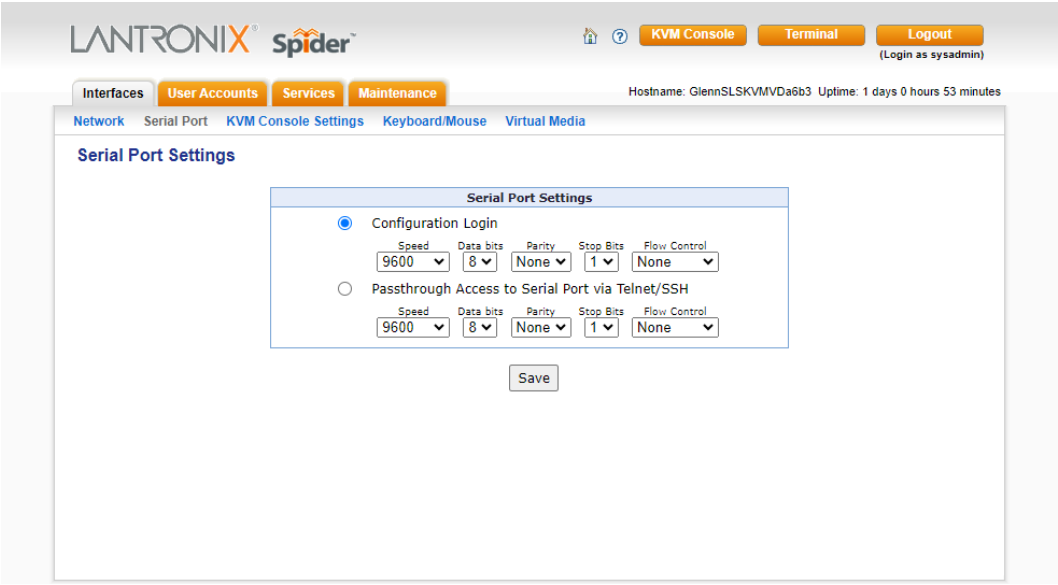
Serial Port Settings

After using the serial port to set up the network parameters, you can configure the serial port for other uses such as management of the target host via Telnet or SSH - the target host console port can be connected to the Spider serial port, and remote users can Telnet or SSH to the Spider and then connect directly to the target host console port, thus providing a backup connection in case the primary LAN connection to the target host is unavailable.

To configure the serial port, perform the following steps.

1. Click **Interfaces > Serial Port.** The Serial Port Settings page displays.

Figure 7-2 SpiderDuo Serial Port Settings Page



2. Modify the following fields.

Field	Description
Configuration Login	Select this option to use the serial port locally only to set up network parameters or reset the unit. Set the following parameters to match connected equipment: ◆ **Speed:** The speed with which the device port exchanges data with the attached serial device. From the drop-down list, select the baud rate. Most devices use 9600 for the administration port, so the device port defaults to this value. Check the equipment settings and documentation for the proper baud rate. ◆ **Data bits:** Number of data bits used to transmit a character. From the drop-down list, select the number of data bits. The default is **8** data bits. ◆ **Parity:** Parity checking is a rudimentary method of detecting simple, single-bit errors. From the drop-down list, select the parity. The default is **None**. ◆ **Stop Bits:** The number of stop bit(s) used to indicate that a byte of data has been transmitted. From the drop-down list, select the number of stop bits. The default is **1**. ◆ **Flow Control:** A method of preventing buffer overflow and loss of data. The available methods include None, software (Xon/Xoff), and hardware (RTS/CTS). The default is **None**. ***Note:*** *When connecting a PCU to the Spider Duo, Flow Control must be set to "None"*

Field	Description
Passthrough Access to Serial Port via Telnet/ SSH	The serial port may be used to connect to the target server's COM port for integrated access to command line functions or used to control a serial-interfaced peripheral. Telnet and SSH are network protocols that enable a tunnel from the client system over the network to the Spider device's serial port. Once the port is set up, it may be accessed through the web interface at the Terminal Console window, or using a Telnet/SSH client to connect directly. Set the following parameters to match connected equipment: ◆ **Speed:** The speed with which the device port exchanges data with the attached serial device. From the drop-down list, select the baud rate. Most devices use 9600 for the administration port, so the device port defaults to this value. Check the equipment settings and documentation for the proper baud rate. ◆ **Data bits:** Number of data bits used to transmit a character. From the drop-down list, select the number of data bits. The default is **8** data bits. ◆ **Parity:** Parity checking is a rudimentary method of detecting simple, single-bit errors. From the drop-down list, select the parity. The default is N**one**. ◆ **Stop Bits:** The number of stop bit(s) used to indicate that a byte of data has been transmitted. From the drop-down list, select the number of stop bits. The default is **1**. ◆ **Flow Control:** A method of preventing buffer overflow and loss of data. The available methods include None, software (Xon/Xoff), and hardware (RTS/CTS). The default is **None**.

3. Click **Save** to save settings.

KVM Console Settings

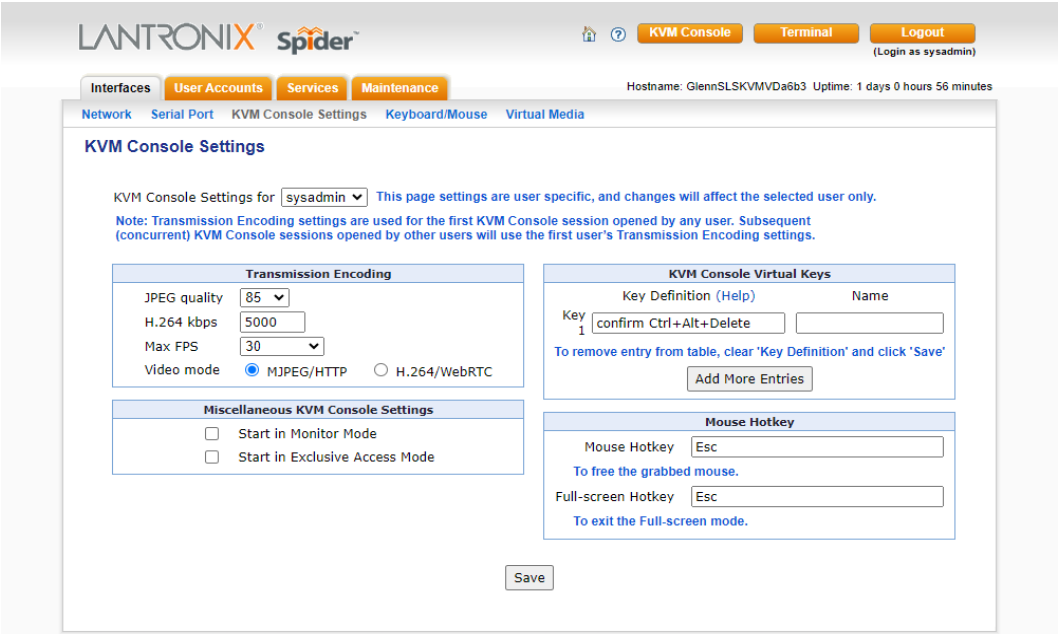
The Remote Console window into the target system has settings that may be changed for the way each individual user interacts with the Spider device. When a user is created by copying from an existing user, the Remote Console settings will be copied as well. You can change these settings on the **Interfaces > KVM Console Settings** page. Note that if you are using the Spider View application, these settings do not apply; see the *Spider View User Guide* for further information.

The way in which the Spider device transmits video data back to the client system can be tailored for the type of network connection. On a LAN where bandwidth is not an issue, compression is not required and the speed of updates can be maximized. For other connections, the optimum user interaction needs to trade off image quality and update speed to fit the size of the pipe. Because various users may be accessing the Spider device over different connections, these parameters are applied on a user-by-user basis. The default is set for maximum image quality and speed of updates, which results in high data rate and hence is suitable for LANs where bursts of up to 2 Mbytes/second are acceptable.

To modify the user console, perform the following steps.

1. Click **Interfaces > KVM Console**. The Remote Console Settings for User page displays.

Figure 7-3 User Remote Console Settings Page



2. Configure the following fields.

KVM Console Settings

Field	Description
KVM Console Settings for	Select the user from the drop-down menu. The settings on this page apply only to the selected user. When a user is created by copying from an existing user, the KVM Console Settings will be copied as well.

Transmission Encoding

Field	Description
JPEG quality	Select the level of compression to be applied to the remote console window. The default value is **100** (no compression).
H.264 kbps	Select the bitrate setting for H.264 video encoding, in kilobytes per second. The default setting is **5000** kbps.
Max FPS	Select the maximum refresh rate to be applied to the remote console window, in frames per second. The default setting is **30**.
Video mode	Use the radio buttons to select the video transfer mode. The default selection is **MJPEG/HTTP**. ***Note:*** *Spider API requires that the Video mode be set to MJPEG/HTTP. H.264/WebRTC is not supported with Spider API.*

Miscellaneous KVM Console Settings

Field	Description
Start in Monitor Mode	Results in the Remote Console window being view-only when launched for this user. This may be changed to interactive mode from within the Remote Console window, if the user has appropriate permission.
Start in Exclusive Access Mode	Upon any subsequent launch of the Remote Console applet by the selected user, terminates any other users' Remote Console windows and locks out any other users trying to access the Remote Console window. This may be changed from within the Remote Console window to allow shared access, if the user has appropriate permission.

Mouse Hotkey

Field	Description
Mouse Hotkey	When the Remote Console window is open, a key code that is not captured by the client system is needed for certain mouse functions. The default is **Esc**.
Full-screen Hotkey	Pressing and holding **Esc** will display the KVM console in Full-screen mode while maintaining the same aspect ratio. Press and hold **Esc** again to return to regular screen mode. The default is **Esc**.

KVM Console Virtual Keys

Field	Description
Key Definition	Button keys allow simulating keystrokes at the remote system that cannot be generated from the client keyboard. A flexible syntax allows for combinations of keys being clicked in combination or in sequence, with optional pauses and an optional confirmation-before-sending dialog box. One key is predefined, for **Ctrl+Alt+Delete** (with confirmation).The syntax to define a new button key is as follows: **<keycode>[+|-|>[*]<keycode>]*** Keycode is the key to send. Multiple key codes are concatenated with a + or a - sign. The + sign builds key combinations, all keys will be clicked until a - sign or the end of the combination is encountered. All clicked keys will be released in reversed sequence. The - sign builds single, separate key clicks and key releases. ***Note:*** *For a list of keys and further explanation, click the* ***(Help)*** *link within the KVM Console Virtual Keys settings box.* ***Note:*** *Virtual Keys appear in the Remote Console Window as Shortcuts. Adding or editing Virtual Keys requires that a new KVM Console session be opened for the updated keys to take effect.*
Name	Enter the name to appear on the button in the Remote Console window. Up to nine Button Keys may be defined for each user.

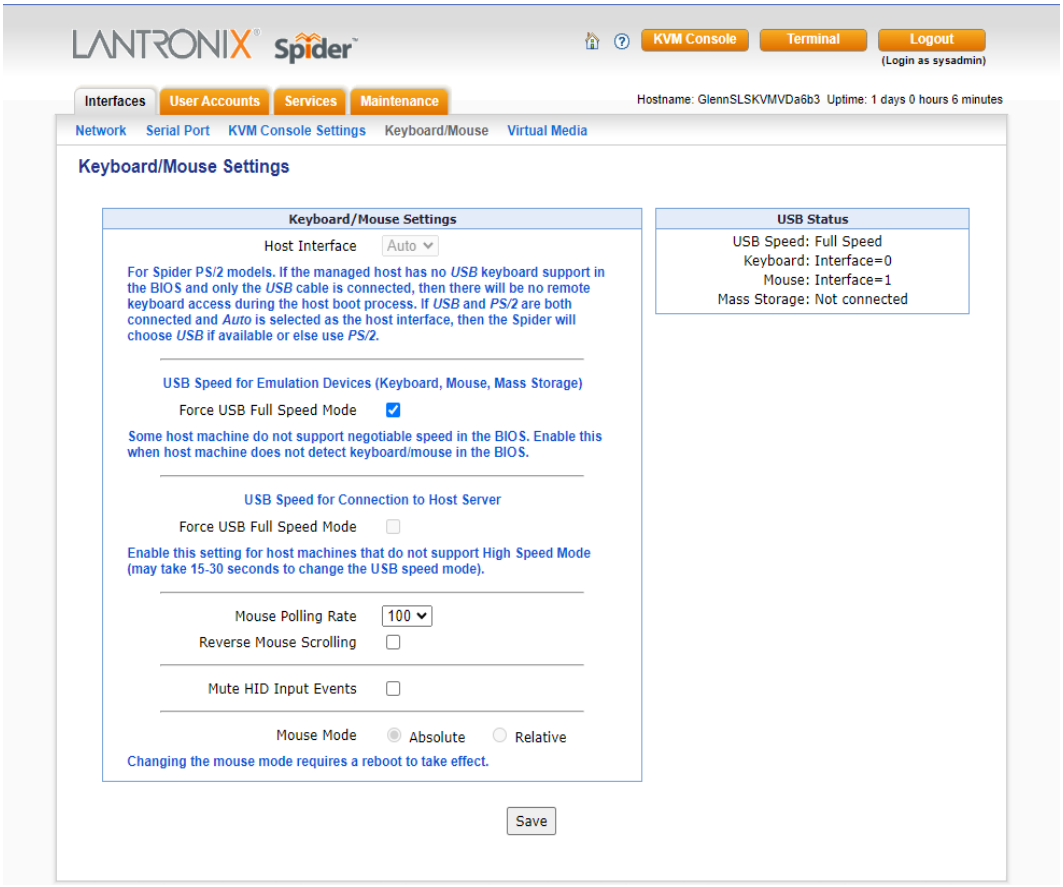
3. Click **Save** to save settings.

Keyboard/Mouse

To modify the keyboard and mouse settings, perform the following steps.

1. Click **Interfaces > Keyboard/Mouse**. The Keyboard/Mouse Settings page displays.

Figure 7-4 Keyboard/Mouse Settings



2. Modify the following fields.

Keyboard/Mouse Settings

Field	Description
Host Interface (PS/2 model only)	In general, the USB interface is preferred because it provides superior mouse tracking. The **Host Interface** drop-down provides three selections. In the default mode, **Auto**, the Spider device attempts to determine whether the attached computer supports a USB keyboard/mouse. If it does, that interface gets activated. If it does not, the Spider device falls back to PS/2. If you have a USB model Spider device and the attached computer does not support USB, the system will be view only. On the PS/2 model Spider device, select **PS/2** to force the PS/2 interface or **USB** to require USB. This selection has no effect on the USB model Spider device.

Field	Description
USB Speed for Emulation Devices	Some older systems do not support USB high-speed mode and may not recognize the keyboard/mouse. Check the **Force USB Full Speed Mode** option in this section to enable the Spider device to negotiate in USB full speed mode.
USB Speed for Connection to Host Server	Check the **Force USB Full Speed Mode** option in this section to enable the Spider device to negotiate with the connected host machine in USB full speed mode.
Mouse Polling Rate	Select the communication rate of the mouse, expressed in milliseconds. The default value is **100**.
Reverse Mouse Scrolling	Click the checkbox to enable reverse mouse scrolling. The default is unchecked, i.e. standard mouse scrolling.
Mute HID Input Events	Click the checkbox to enable indication of keyboard or mouse input events. The default value is unchecked, i.e. not muted.
Mouse Mode	In **Absolute Mode,** the input device transmits the exact coordinates (X,Y) where the cursor should be moved. This is how touchscreens or drawing tablets work. In **Relative Mode**, only the relative offset (dX,dY) to the current position is transmitted, which is unknown to the input device itself. This is a regular mouse. By default, Spider uses absolute positioning mode as the most convenient for the user and software. However, this is not always supported by the BIOS/UEFI. For such cases, support is provided for the relative mode of operation, which can be enabled in the config. When using relative mode, the browser will exclusively capture your mouse when you click on the stream window in Spider once. When you press Esc, the browser releases the mouse.

3. View the USB Status for USB Speed, Keyboard, Mouse, and Mass Storage.
4. Click **Save** to save settings.

Virtual Media

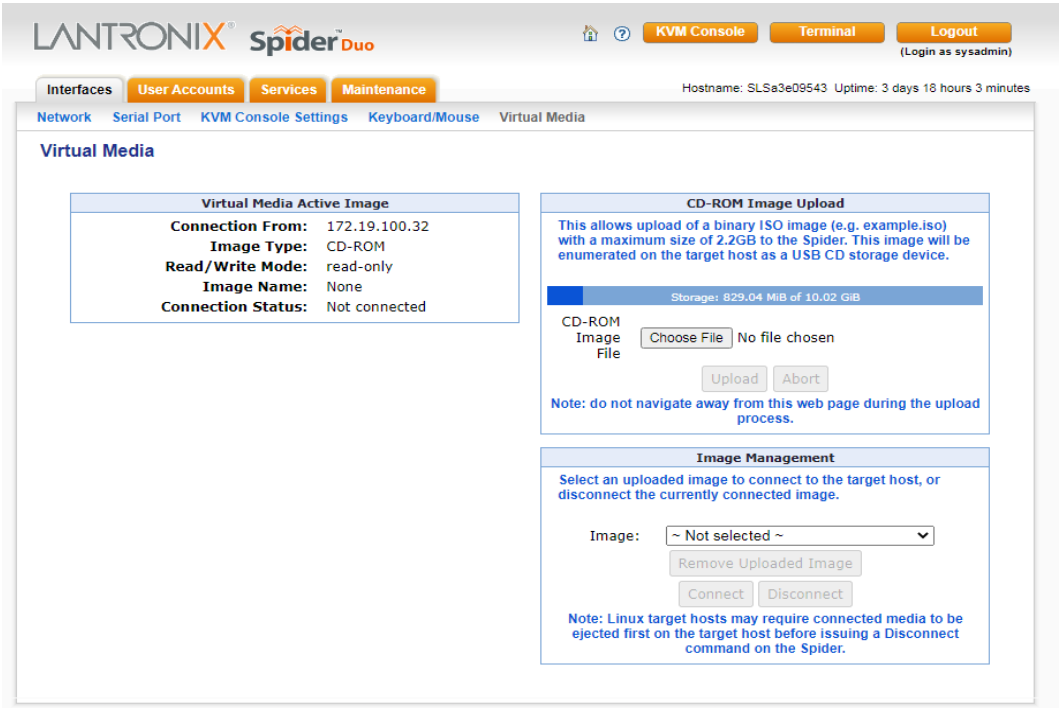
The Spider device provides a powerful capability called Virtual Media (or Virtual Disk). This feature enables users to remotely access and interact with virtual media, such as disk images or ISO files, as if they were physically connected to the target system. The virtual media support provided by Spider devices allows for seamless integration of virtual media into remote KVM sessions. This can allow system recovery in situations where local disks are down, and/or no primary network connection is available.

The Virtual Media feature allows the Spider Device to emulate a USB mass storage device to the attached target system via the Spider USB connection. When an ISO file is uploaded to the Spider device's Virtual Media and the Connection Status = Connected, the Spider device advertises the USB mass storage device to the target system as an attached USB external CD-ROM drive. The target system will mount the disk image, and the ISO file image will appear on a virtual drive as actual files on CD. From a remote KVM session, you will be able to read and install programs in the BIOS or operating system from those mounted files.

Virtual Media is not supported on all released Spider hardware. To check if your Spider supports Virtual Media, navigate to the **Maintenance > Device Status** page and check the Device Information section for Virtual Media = Supported. You can view the same information in the CLI using the `admin version` command.

To configure Virtual Media, click **Interfaces > Virtual Media**.

Figure 7-5 Virtual Media Page



Virtual Media Active Image

Field	Description
Virtual Media Active Image	The status of an uploaded and connected virtual image is displayed here.

CD-ROM Image Upload

In the **CD-ROM Image Upload** section, you can upload a disk image to the Spider device, which then appears to the attached computer as a USB CD storage device once it is connected. The file must be structured as a binary ISO image. The maximum image size is 2.2 GB.

To enable Spider Virtual Media emulation on the attached target system:

1. Ensure the Spider USB cable is connected to the target system.
2. In the **CD-ROM Image Upload** section, click **Choose File** to select the CD-ROM image file.
3. Click **Upload** to upload the image file. Click **Abort** to cancel the upload, or to discard our changes.
4. After the upload process has completed, in the **Image Management** section, select the ISO file from the pulldown menu, then click **Connect** to start the Spider Virtual Media emulation to the target system.

5. In the **Virtual Media Active Image** section, confirm the Image Name is correct, and the Connection Status is “Connected”. Check the "Virtual Media Active Image" section for the Spider Virtual Media Active State. Next check Target System File System to verify Spider Active Virtual Drive.

Image Management

An uploaded image file remains in the Spider device until the user deletes the image. The image must be disconnected before it can be deleted.

To disconnect/remove a Virtual Media ISO file from the attached target system:

1. In the **Image Management** section, click **Disconnect** to remove the Spider Virtual Media ISO file from the attached target system.
2. In the **Virtual Media Active Image** section, check that the Connection Status is “Not connected” and the Image File is “None”. On the same page, check the "Virtual Media Active Image" section for the Spider Virtual MediaState. Next check Target System File System to verify Spider ISO File has been removed.
3. Select the file from the **Image** pulldown, then click **Remove Uploaded Image** to delete the selected image file from the Spider device.

8: User Accounts

This chapter describes user accounts including local and remote authentication, management, and user groups and how to configure each. It contains the following sections:

Local vs. Remote Authentication

User names and groups may be administered on the Spider device to allow varying levels of access and control to different classes of users. To log in to the Spider device, a user must be authenticated by means of a password. This authentication may take place locally, where the user name and associated password are stored in the Spider device's configuration. The Spider device may query a centralized database using RADIUS or LDAP to determine if a given user may log in. In both of these cases, the user name must be defined on the Spider device as a local user where it has its permissions assigned.

Local User Management

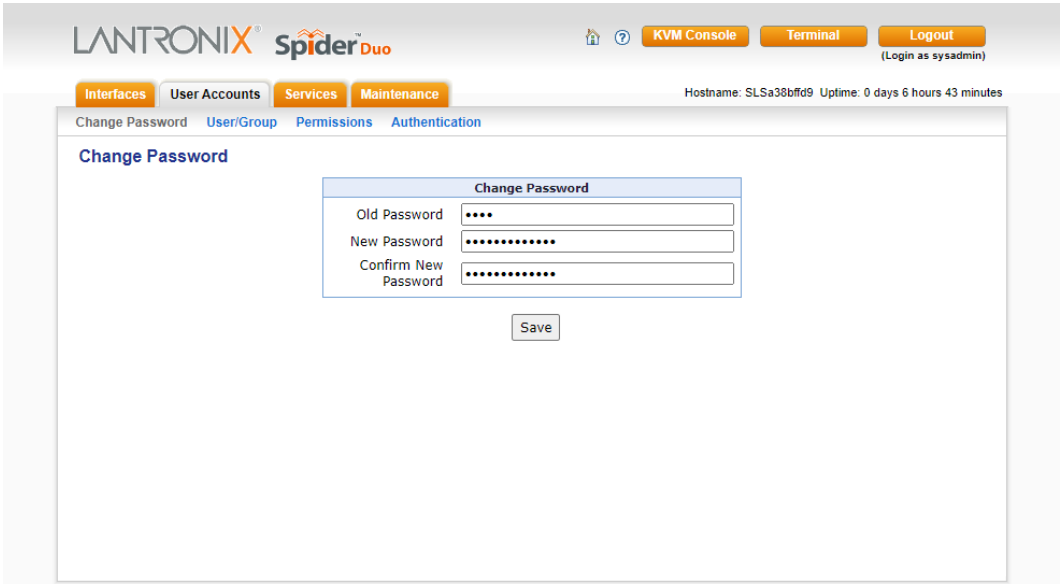
A newly assigned user has permissions inherited from an assigned group. All Local Users not associated with a group will inherit default settings.

Modifying Passwords

To change current user password, perform the following steps.

1. Click **User Accounts > Change Password.** The Change Password page displays.

Figure 8-1 Change Password Page



2. Enter the current password under **Old Password**.
3. Enter the new password under **New Password** and **Confirm New Password** (the password must contain a minimum of 4 characters; spaces are not allowed).

   When first logging in as sysadmin, for security purposes the password will need to be changed.
4. Click **Save** to save your settings.

User and Group Management

You must be logged in under a user name that has permissions for User/Group Management to access this page. The Spider device supports a maximum of 60 configured users. When defining a user, make sure the group to which the user will belong has already been created.

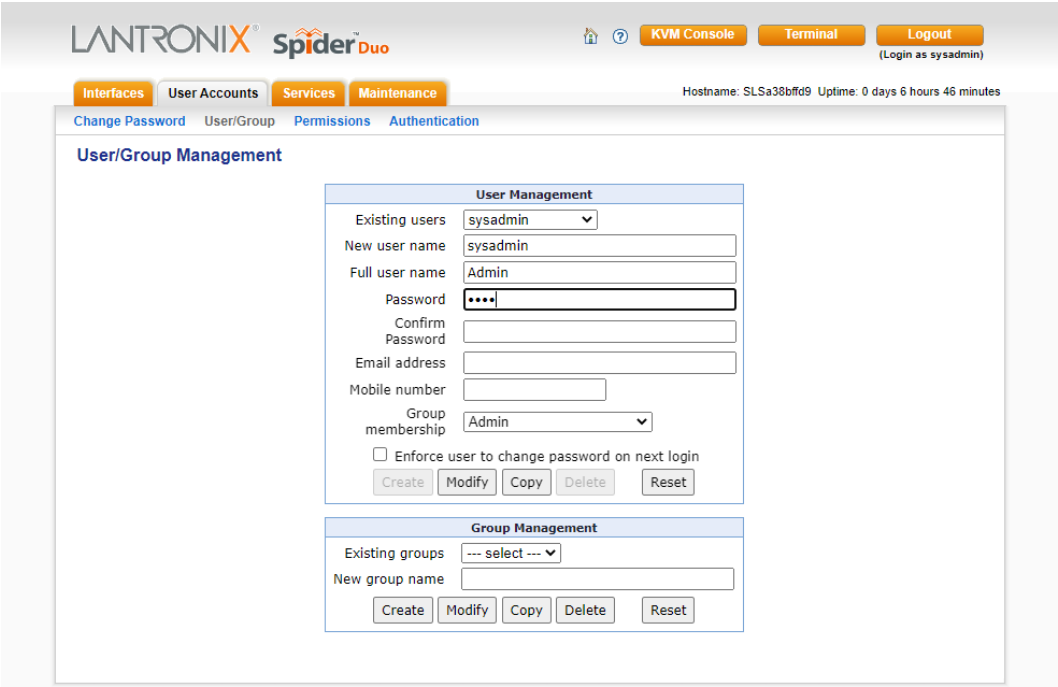
The following users and groups are available by default:

- Users:
  - **sysadmin**: The sysadmin user belongs to the **Admin** group.
  - **kvm_user**: The kvm_user user belongs to the **Admin** group.
- Groups:
  - **Admin**: By default, this group has full permissions enabled.
  - **None**: By default, this group has no permissions; permissions are set on a per-user basis; see *User Permissions on page 61*.
  - **Unknown**: By default, this group has no permissions; permissions for users in the Unknown group are set globally; see *User Permissions on page 61*.

To configure users and groups, perform the following steps.

1. Click **User Account > User/Group**. The User/Group Management page displays.

Figure 8-2 Configure User Page



User Management

To configure a user, perform the following steps.

1. Configure the following fields.

Field	Description
Existing users	To modify or copy an existing user, select that user from the drop-down menu.
New user name	Enter the new user's name. Minimum 1 character, maximum 32 characters. Valid characters are letters, numbers, period, dash, underscore; must start with a letter.
Full user name	Enter the full name of the configured user. Minimum 1 character.
Password	Enter the password for the user. Minimum 4 characters.
Confirm Password	Re-enter the password for the user.
Email address	(Optional) Enter the user's email address.
Mobile number	(Optional) Enter the user's mobile phone number.
Group Membership	Select the user's group from the drop-down menu. By default, new users are added to the Unknown user group; use the pulldown menu to select a new group.
Enforce user to change password on next login	Select checkbox to require the user to change the password upon initial login.

2. Do one of the following:
   a. Click **Create** to add the new user.
   b. Click **Modify** to change an existing user.
   c. Click **Copy** to create a new user based on the selected existing user.

d. Click **Delete** to delete an existing user.

e. Click **Reset** to restore original settings.

Group Management

To configure a user group, perform the following steps.

1. Configure the following fields.

Field	Description
Existing Groups	To copy or modify a group, select the group from the drop-down menu.
New Group Name	Enter the new group's name.

2. Do one of the following:

a. Click **Create** to add the new group.

b. Click **Modify** to change an existing group.

c. Click **Copy** to create a new group based on the selected existing group.

d. Click **Delete** to delete an existing group.

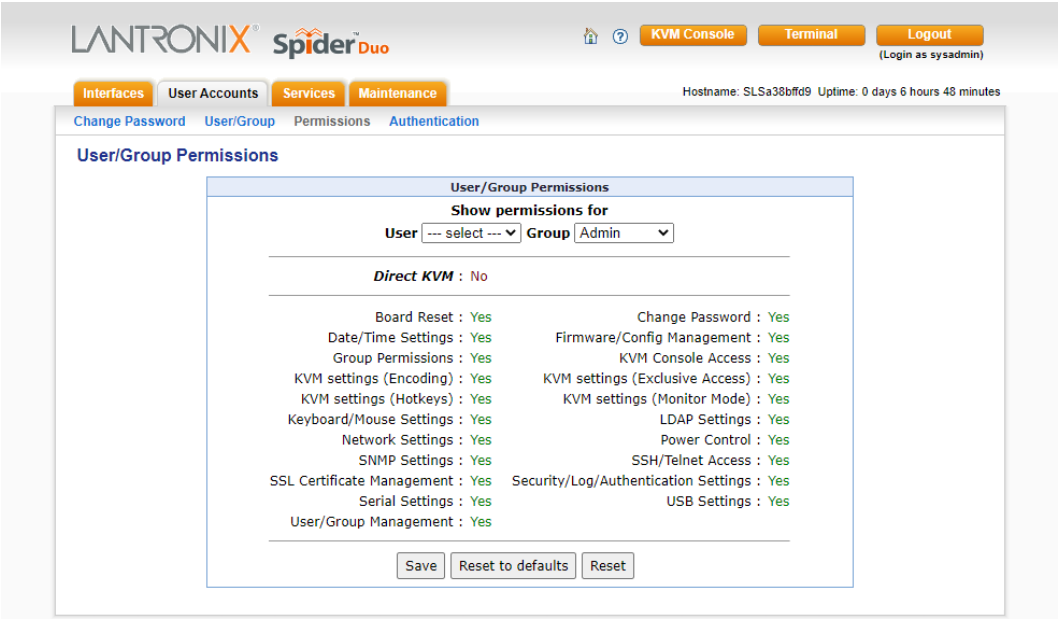
e. Click **Reset** to restore original settings.

User Permissions

To modify user permissions, perform the following steps.

1. Click **User Accounts > Permissions**. The User/Group Permissions page displays.

Figure 8-3 User Permissions Page



2. From the drop-down menu, select **Group** to configure:

3. If you created a user belonging to a group, and you want to change permissions for the group, select **Group**.
4. If you created a user who does not belong to any group, then select **User**.
5. From the **Direct KVM** drop-down menu, do one of the following:
   a. Select **Yes** to enable the user or group to access the Remote Console only. After a user is authenticated, it launches the KVM console program.
   b. Select **No** (default) to display the web page after logon.

Note: *Setting **Yes** may overwrite some selected permissions selected in step 4.*

6. Modify the displayed permissions as necessary for the selection.
7. Do one of the following:
   a. Click **Save** to save settings.
   b. Click **Reset to Defaults** to restore system defaults.
   c. Click **Reset** to restore original settings.

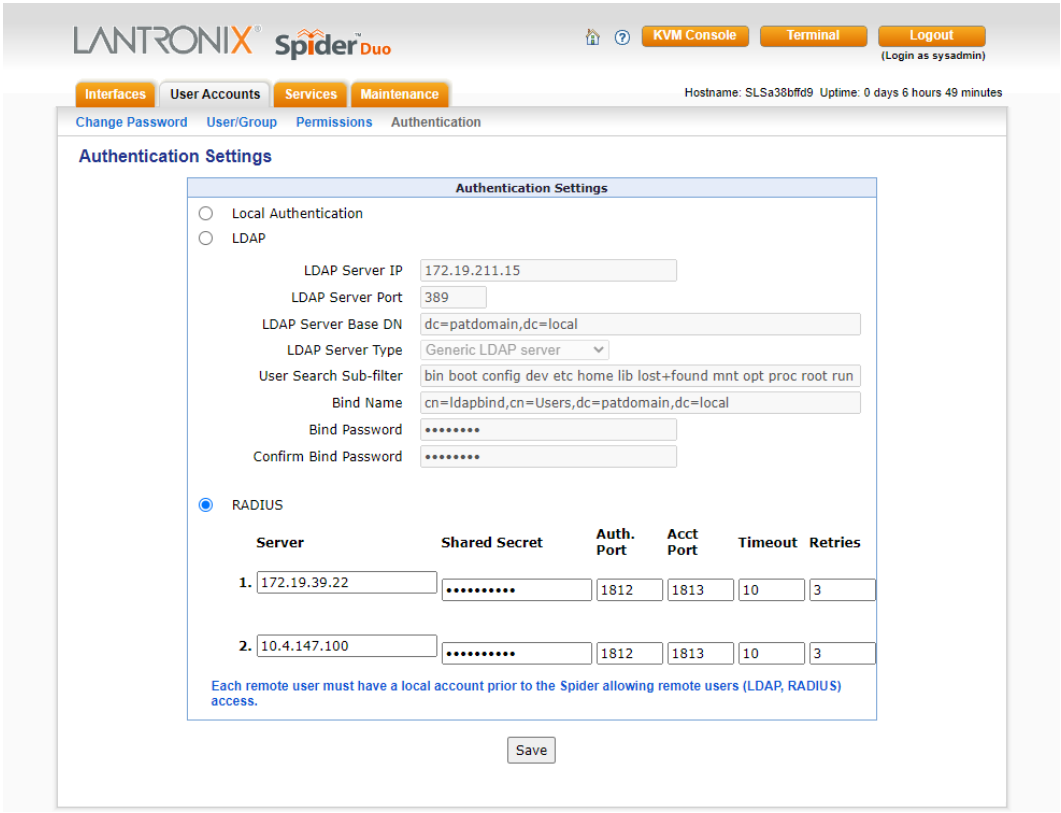
Remote Authentication

If the authentication settings have been set to Local Authentication (the default), the Spider device uses its own database to perform authentication. If one of the remote authentication protocols is selected, the Spider device communicates with a remote server to authenticate user passwords.

To configure authentication settings, perform the following steps.

1. Click **User Accounts > Authentication**. The Authentication Settings page displays.

Figure 8-4 Authentication Page



2. Modify the following field.

Field	Description
Local Authentication	When Local Authentication is selected, the Spider device will authenticate against its internal database of users and passwords, as described in Local User Management.

LDAP

When you select LDAP Authentication, the Spider device will communicate with a Microsoft Active Directory or generic LDAP server for user authentication. The user profile must be set up in the local database as described in Local User Management, but no password is stored locally. When a user attempts to log in, the Spider device contacts the specified LDAP server, which either approves or denies access.

Field	Description
LDAP Server IP	Enter the name or IP address of the LDAP server, reachable over the network by the Spider device, containing the user database. Be sure to configure a DNS server if a name rather than address is used.
LDAP Server Port	Enter the port number of the LDAP server.
LDAP Server Base DN	Specify the Distinguished Name (DN) where the directory tree starts in the user LDAP server.
LDAP Server Type	Select the type of the external LDAP server. Available selections are **Generic LDAP** and **Microsoft Active Directory**. If a Generic LDAP Server is selected, edit the LDAP scheme.

Field	Description
User Search Sub-filter	Select to restrict the search for users by adding an additional search filter to each query for a user.
Bind Name	The name for a non-anonymous bind to an LDAP server. This item has the same format as LDAP Base. One example is cn=administrator,cn=Users,dc=domain,dc=com.
Bind Password and Confirm Bind Password	Password for a non-anonymous bind. This entry is optional. Acceptable characters are **a-z**, **A-Z,** and **0-9**. The maximum length is 127 characters.

RADIUS

When RADIUS is selected, the Spider device communicates with a RADIUS server for user authentication; up to two RADIUS server entries can be created. To access a Spider device set up for RADIUS, log in with a name and password. The Spider device contacts the RADIUS server for authentication and, if approved, the Spider device uses the locally stored user profile. If there is no such profile, access via RADIUS will be refused.

Field	Description
Server	Enter the name or IP address of the RADIUS server, reachable over the network by the Spider device, containing the user database. Configure a DNS server if a name rather than an address is used.
Shared Secret	A shared secret is a text string that serves as a password between the RADIUS client and RADIUS server. In this case the Spider device acts as a RADIUS client. A shared secret is used to verify that RADIUS messages are sent by a RADIUS-enabled device that is configured with the same shared secret and to verify that the RADIUS message has not been modified in transit (message integrity). Enter a maximum of 128 alphanumeric characters and symbols such as an exclamation point (“!”) or an asterisk (“*”).
Authentication Port	The port the RADIUS server listens for authentication requests. The default value is **1812**.
Accounting Port	The port the RADIUS server listens for accounting requests. The default value is **1813**.
Timeout	Sets the request time-to-live in seconds. The time-to-live is the time to wait for the completion of the authentication request. If the request job is not completed within this interval of time it is cancelled. The default value is **1** second.
Retries	Sets the number of retries if a request could not be completed. The default value is **3** times.

Click **Save** to save settings.

9: Services

This chapter describes the Spider and SpiderDuo KVM-over-IP services. It contains the following sections:

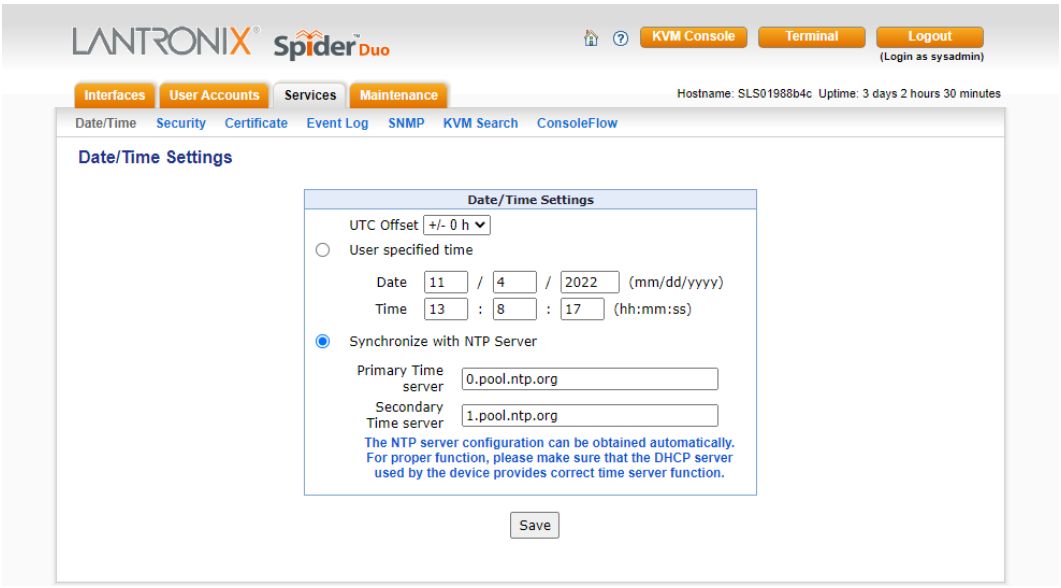
Date/Time

The Spider device contains an internal real time clock that maintains a basic date and time after being set. The clock, however, will reset if the unit loses power. If an accurate date and time are critical, the Spider device supports synchronization with Network Time Protocol servers. Internally, the date and time are only used to timestamp events in the log and for the inactivity timeout.

To configure the date and time settings, perform the following steps.

1. Click **Services > Date/Time**. The Date/Time Settings page displays.

Figure 9-1 Date/Time Settings Page



2. Modify the following fields.

Table 9-2 Date/Time Settings

Field	Description
UTC Offset	Time servers deliver time as Coordinated Universal Time (UTC, or Greenwich Mean Time). Select the appropriate offset in hours ± from the drop-down menu.
User Specified Time	Manually input the current date and time. The Spider device keeps time as long as power is applied. It has an internal calendar, but does not know about daylight savings time and requires resetting twice a year. The internal clock accuracy is ±30 ppm.
Synchronize with NTP Server	Enter a primary and secondary time server in the respective fields. Ensure NAT and firewalls are set up to allow the protocol to pass. Also, provide the Spider device with DNS server names. ***Note:*** *The Spider devices support setting the NTP server(s) via DHCP.*

3. Click **Save** to save settings.

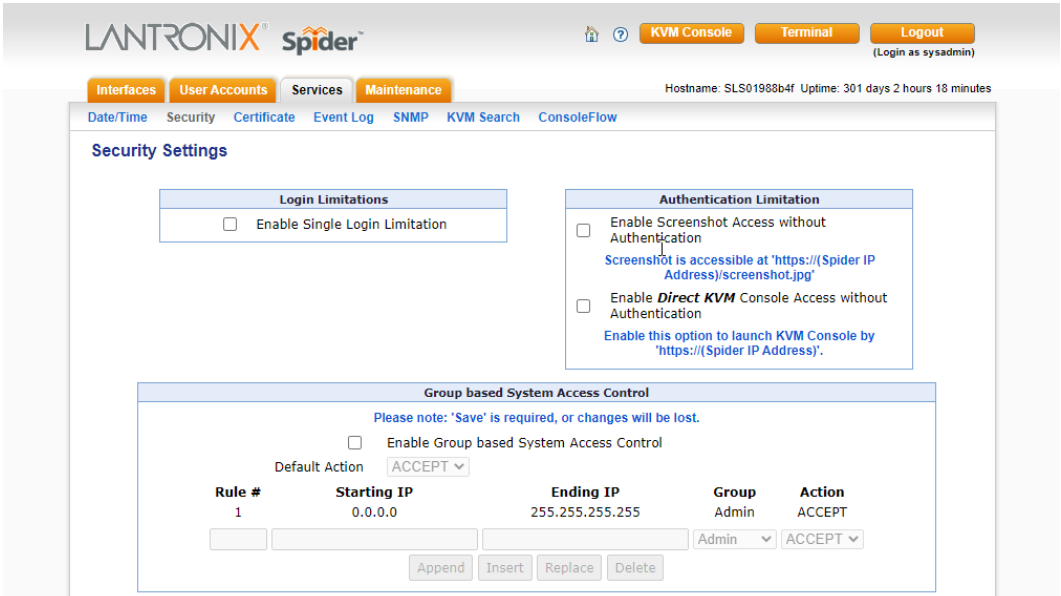
Security

General settings for security parameters such as encryption and access control are at **Services > Security**. Other areas with security implications include User Management/Permissions, Authentication, Network Settings, and the Event Log; see the appropriate sections for information on those areas.

To modify security settings, perform the following steps.

1. Click **Services > Security**. The **Security** page displays.

Figure 9-3 Security Settings Page



2. Modify the following fields.

Login Limitations

Field	Description
Enable Single Login Limitation	If this box is checked, each username may only have one logged in connection at a time. If unchecked, multiple instances of username logins are allowed.

Authentication Limitation

Field	Description

Enable Screenshot Access without Authentication	Select this option when you need to access the snapshot image without logging in to the Spider device. If enabled, the screenshot can be read directly with **`https://<Spider IP Address>/screenshot.jpg`**.
	If viewing from a web browser, the screenshot can be read directly with `https://<Spider IP Address>/screenshot.jpg, which redirects to https://<Spider IP Address>/share/screenshot.jpg`.
	If using a script or command line to retrieve screenshots, refer to your application's help sectionfor guidance on capturing images from secure websites; two examples are shown below:
	`% wget --no-check-certificate https://<Spider IP Address>/screenshot.jpg ; rm -f screenshot.jpg ; wget --no-check-certificate https://<Spider IP Address>/share/screenshot.jpg`
	`$ phantomjs --ignore-ssl-errors=true save_screenshot.js "https://<Spider IP Address>/screenshot.jpg"`

Enable Direct KVM Console Access without Authentication	Select this option to launch the Remote Console without authentication by entering the Spider device's IP address (https:/(Spider device IP address) in the browser's **Address** field. To launch Spider device web access type **`https:/(Spider IP Address)/home`** in the browser's Address field.

Group Based System Access Control

Field	Description
Enable Group Based System Access Control	When this box is checked, the rules for IP-based access are enforced. They are ignored when the box is not checked.
Default Action	If after evaluation of all rules a request for connection from a given IP address has not had either an **Accept** or **Drop** decision made, this selection can allow it to be either Accepted or Dropped. In other words, this drop-down defines the default action for IP addresses with no rules defined.

Field	Description
Rule creation and editing	Spider devices come from the factory with one rule defined as an example of the rule structure: Rule 1 allows all groups access from source IP 0.0.0.0 to 255.255.255.255. Additional rules may be entered in the edit boxes. ◆ **Rule Number**: Defines where in the evaluation sequence this rule is to be applied. ◆ **Starting** and **Ending IP Addresses**: Define the range over which the rule applies. ◆ **Group**: Defines which user group is affected by this rule. Built-in groups include **Admin**, **All**, and **Unknown** (no group assigned). As additional groups are defined in **User Management > Users > Group Management**, they will appear in the drop-down. A rule can apply to only one group at a time. ◆ **Action**: Chooses whether this is to be a **DROP** or **ACCEPT** rule. After a rule has been defined, it needs to go in the correct place in the list. ◆ **Append**: Puts the rule at the end of the list. The rule number changes to reflect the last position on the list. ◆ **Insert**: Puts the rule in the place on the list indicated by the rule number, renumbering and moving down the other rules to make room. ◆ **Replace**: Deletes the previous rule of that number and replaces it with the new rule. ◆ **Delete**: Deletes the rule of that number and moves the others up. Note that for a **Delete**, the fields other than the rule number do not need to be filled in.

3. Click **Save** to save settings.

Certificate

The Spider device uses the Transport Layer Security (TLS) protocol for any encrypted network traffic between itself and a connected client. During the connection establishment the Spider device has to expose its identity to a client using a cryptographic certificate. Upon leaving the factory this certificate and the underlying secret key is the same for all Spider devices and will not match the network configuration where it is installed. The certificate's underlying secret key is also used for securing the TLS handshake. Leaving the default certificate unmodified is all right in most circumstances and is necessary only if the network facility is vulnerable to man-in-the-middle attack.

It is possible to generate and install a new base64 x.509 certificate that is unique for a particular Spider device. The Spider device is able to generate a new cryptographic key and the associated Certificate Signing Request (CSR) that needs to be certified by a certification authority (CA).

To create and install an SSL certificate, perform the following steps.

1. Click **Services > Certificate**. The Certificate Signing Request page displays.

Note: *The completed form fields shown in Figure 9-4 are provided as an example.*

Figure 9-4 Certificate Signing Request Page

2. Modify the following fields.

Field	Description
Common name	The network name of the Spider device once it is installed in the user's network (usually the fully qualified domain name). It is identical to the name that is used to access the Spider device with a web browser without the prefix http://. In case the name given here and the actual network name differ, the browser will pop up a security warning when the Spider device is accessed using HTTPS.
Subject Alternative Name	Any subject alternative names (SANs) associated with the certificate.
Organizational unit	This field specifies to the department within an organization to which the Spider device belongs.
Organization	The name of the organization to which the Spider device belongs.
Locality/City	The city where the organization is located.
State/Province	The state or province where the organization is located.
Country (ISO code)	The country where the organization is located. This is the two-letter ISO code (e.g., US for the United States).
Email	The email address of a contact person responsible for the Spider device and its security.
Challenge password/ Confirm Challenge password	Certain certification authorities require a challenge password to authorize later changes on the certificate (e.g., revocation of the certificate). The minimal length of this password is four characters.
Key length (bits)	Select the key length from the drop-down menu.

3. Click **Create** to initiate the Certificate Signing Request generation; an example is shown in *Figure 9-5*. Download the CSR by clicking **Download**. The **Download** button displays when a certificate is created. Send the saved CSR to a CA for certification.

Figure 9-5 Certificate Signing Request (Created)

4. Click **Upload** to upload the certificate from the client computer to the Spider device. The Spider device now has its own certificate used for identifying itself to its clients.

Note: *Uploaded certificates must have a .crt extension; the Spider device must be rebooted for the new SSL certificate to take effect.*

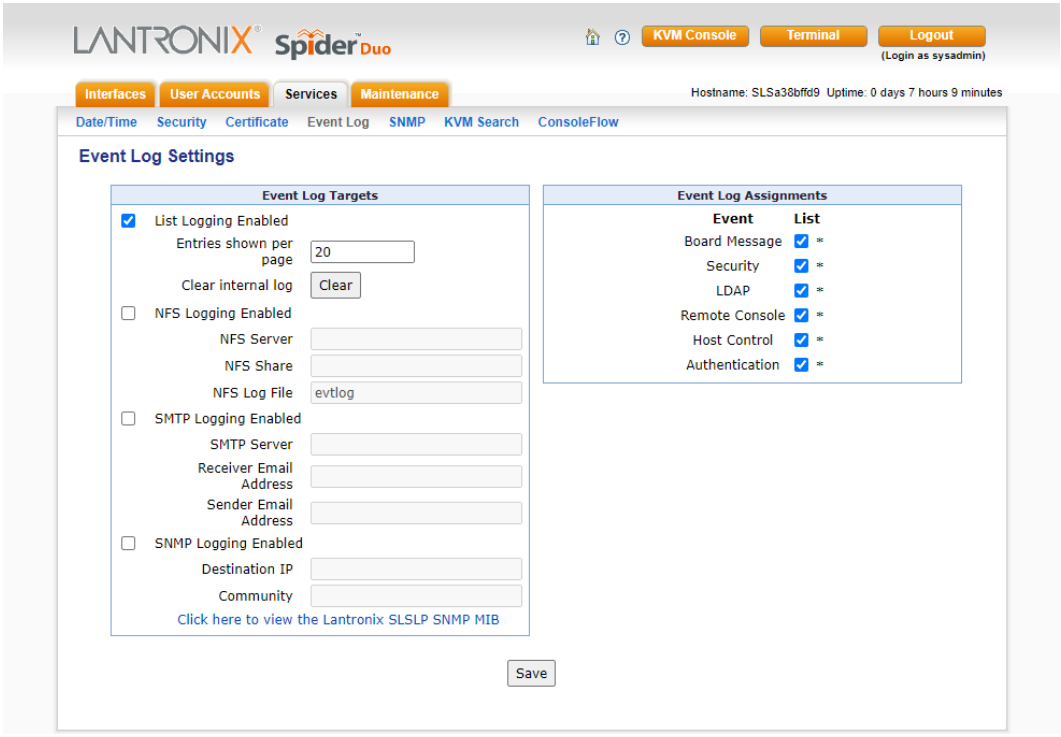
Event Log

The Event Log maintains a list of significant events locally. Alternatively it can use an NFS log file, SMTP email, or SNMP to distribute event information on the network. The Spider device monitors five classes of events with the logging of each enabled or disabled.

To configure event log settings, perform the following steps.

1. Click **Services > Event Log**. The **Event Log Settings** page displays.

Figure 9-6 Event Log Settings Page



2. Modify the following fields:

Event Log Targets

Field	Description
List Logging Enabled	Check this box to use the internal log list of the Spider device. The default value is 20; the maximum number of entries is 1,000. Every entry that exceeds this limit overrides the oldest one. The number of log entries shown on each page may be changed in the text box. The internal log list is cleared when power is removed from the Spider device, or when you click the **Clear** button.
NFS Logging Enabled	The Spider device can write log information to a file on an NFS server. Provide the name of the server, share, and file in the boxes. The NFS share will be mounted immediately, and an error message will result if it cannot be found.

Field	Description
SMTP Logging enabled	With this option, the Spider device is able to send emails to an address given by the email address. These emails contain the same description strings as the internal log file and the mail subject contains the event class. To use this log destination, specify an **SMTP Server**, the **Receiver Email Address**, and **Sender Email Address**. Enter the mail server and SMTP port as **<serverip>:<port>**.
SNMP Logging Enabled	If selected, the Spider device sends an SNMP trap to a specified destination IP address every time a log event occurs. Configure the **Destination IP** and **Community**. View the SNMP MIB implemented in the Spider device by clicking on the **Spider device SNMP MIB** link.

Event Log Assignments

Field	Description
Event Log Assignments	Select the event classes for monitoring, local logging, and exportation.

3. Click **Save** to save settings.

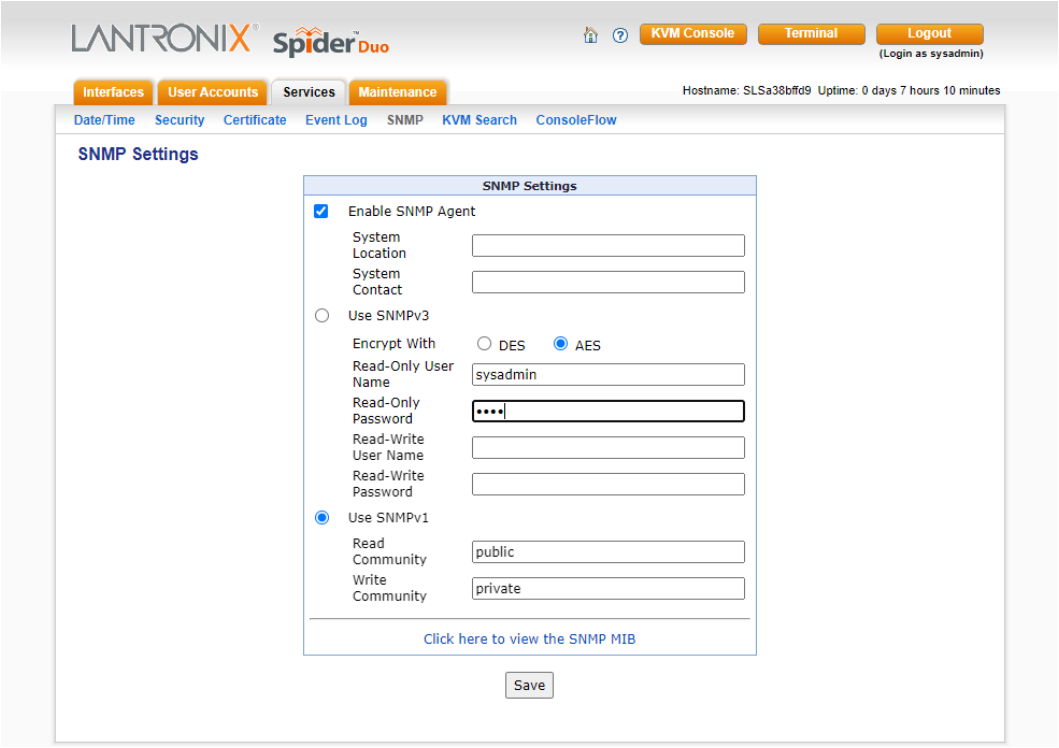
SNMP

The Spider device has an internal SNMP agent that has various objects accessible in its MIB. It also can generate traps based on events. The Spider device permits enabling or disabling the SNMP agent, input read and write communities, location information, contact information, and viewing the MIB.

To configure SNMP settings, perform the following steps.

1. Click **Services > SNMP**. The **SNMP Settings** page displays.

Figure 9-7 SNMP Settings Page



2. Modify the following fields.

Field	Description
Enable SNMP Agent	Click the checkbox to enable the Spider device SNMP agent, and enter the system location and the contact name for the system.
Use SNMPv3	Select to use SNMPv3 (rather than SNMPv1)and enter the following: ◆ **Encrypt With:** Select whether to tenable encryption with Data Encryption Standard (DES) or Advanced Encryption Standard (AES), ◆ **Read-Only User Name:** User ID for a user with read-only authority to use to access SNMP v3. ◆ **Read-Only Password**: Password for a user with read-only authority to use to access SNMP v3. Up to 64 characters. ◆ **Read-Write User Name**: Enter a user ID for users with read-write authority. Up to 20 characters. ◆ **Read-Write Password**: Enter a password for the user with read-write authority to use to access SNMP v3. Up to 64 characters.
Use SNMPv1	Select to use SNMPv1 (rather than SNMPv3) and enter the following: ◆ **Read Community:** Enter the SNMP read community name. The default is **public**. ◆ **Write Community:** Enter the SNMP write community name. The default is **private**.

3. Click **Save** to save settings.

KVM Search

The KVM Search option enables you to view the properties of other Spider devices on the network. The following items display:

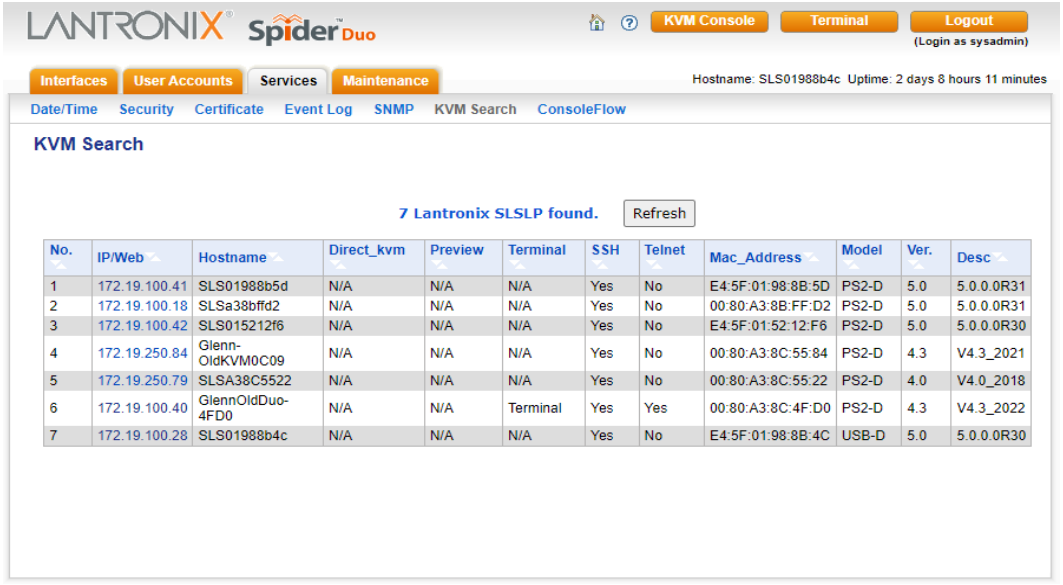
- IP address
- Hostname
- Direct KVM
- Preview
- Terminal
- SSH
- Telnet
- MAC Address
- Model
- Version
- Description

Note: *The information shown on the web interface represents a snapshot in time. To see the most recent data, click* ***Refresh****.*

To view a KVM search, perform the following steps.

1. Click **Services** > **KVM Search**. The search results display.

Figure 9-8 KVM Search Page



No.	IP/Web	Hostname	Direct_kvm	Preview	Terminal	SSH	Telnet	Mac_Address	Model	Ver.	Desc
1	172.19.100.41	SLS01988b5d	N/A	N/A	N/A	Yes	No	E4:5F:01:98:8B:5D	PS2-D	5.0	5.0.0.0R31
2	172.19.100.18	SLSa38bffd2	N/A	N/A	N/A	Yes	No	00:80:A3:8B:FF:D2	PS2-D	5.0	5.0.0.0R31
3	172.19.100.42	SLS015212f6	N/A	N/A	N/A	Yes	No	E4:5F:01:52:12:F6	PS2-D	5.0	5.0.0.0R30
4	172.19.250.84	Glenn-OldKVM0C09	N/A	N/A	N/A	Yes	No	00:80:A3:8C:55:84	PS2-D	4.3	V4.3_2021
5	172.19.250.79	SLSA38C5522	N/A	N/A	N/A	Yes	No	00:80:A3:8C:55:22	PS2-D	4.0	V4.0_2018
6	172.19.100.40	GlennOldDuo-4FD0	N/A	N/A	Terminal	Yes	Yes	00:80:A3:8C:4F:D0	PS2-D	4.3	V4.3_2022
7	172.19.100.28	SLS01988b4c	N/A	N/A	N/A	Yes	No	E4:5F:01:98:8B:4C	USB-D	5.0	5.0.0.0R30

ConsoleFlow

ConsoleFlow is a cloud or on-premise portal for the centralized management of multiple Lantronix Out-of-band management devices, including Spider devices. A browser based interface (including mobile phone app support) allows an administrator to view status, send commands, view logs and charts and update firmware. Each device can communicate with the cloud server or on-premise server, sending status updates, responding to commands sent by the server.

A Spider device requires a unique Device ID to communicate with the ConsoleFlow portal. The ID is viewable in the ConsoleFlow settings. If a device is not already pre-configured with the ID, the ID must be provisioned using Lantronix Provisioning Manager (LPM).

Changing the Spider device's timezone or making significant changes to the current date and time may cause issues with the ConsoleFlow client's ability to connect to or send updates to the ConsoleFlow server; restarting the client will resolve these issues.

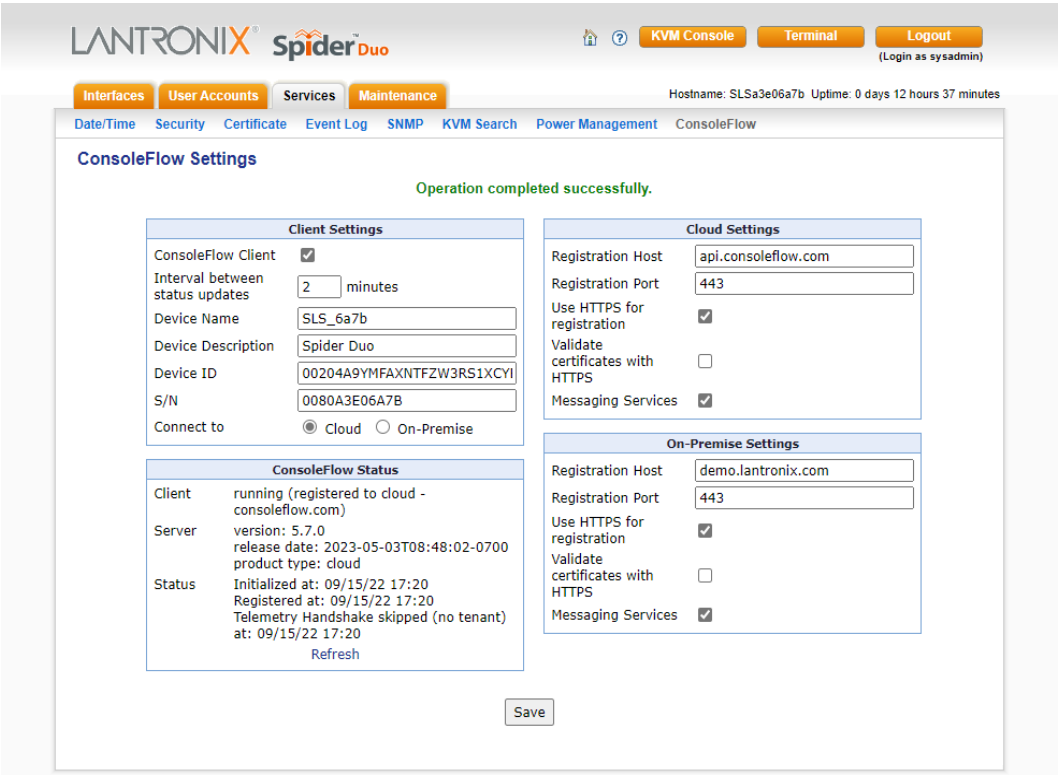
The ConsoleFlow client follows a sequence of steps to connect to the cloud or on-premise ConsoleFlow server, send status updates, check for firmware and configuration updates, and respond to commands from the server. This series of steps is the same each time the client starts - at boot, or if the client is enabled. Any changes to the ConsoleFlow Device ID, Registration settings or Messaging settings require the ConsoleFlow client to be disabled and re-enabled for the changes to take effect.

The ConsoleFlow Status section shows the Client, Server, and Status information for the device.

To configure ConsoleFlow settings, perform the following steps.

1. Click **Services > ConsoleFlow**. The **ConsoleFlow Settings** page displays.

Figure 9-9 ConsoleFlow Settings Page



2. Modify the following fields.

Client Settings

Field	Description
ConsoleFlow Client	Enables or disables the ConsoleFlow client. This option is **disabled** by default.
Interval between status updates	Number of minutes between status updates sent from the client to the server. Valid values are 1 - 60 minutes. The default is **2** minutes.
Device Name	The device name displayed in the ConsoleFlow server UI. Valid characters are alphanumeric characters, dash "-", and underscore"_". The default is the device type (SLS) with the last 4 characters of the device serial number appended
Device Description	Long description that is displayed in the ConsoleFlow server UI.
Device ID	The unique device identifier. The ID is 32 alphanumeric characters. The ID may be provisioned using Lantronix Provision Manager (LPM). Contact Lantronix Tech Support for more information on LPM.
S/N	View-only field. Displays the serial number.
Connect to	Allows you to choose Cloud or On-Premise server settings for the ConsoleFlow client. By default, **Cloud** is selected as the active connection.

Cloud Settings

Field	Description
Registration Host	Hostname of the server the client registers with. The **Host Name** should start with api.
Registration Port	The TCP port on the Registration Host. Defaults to **443**.
Use HTTPS for registration	If enabled, HTTPS (instead of HTTP) is used for registration. **Enabled** by default.
Validate certificates with HTTPS	If enabled, use a certificate authority to validate the HTTPS certificate. A certificate authority file can be uploaded on the *Certificate* page. **Disabled** by default.
Messaging Services	If enabled, messaging services are used for status updates and commands. **Enabled** by default.

On-Premise Settings

Field	Description
Registration Host	Hostname of the server the client registers with. The **Host Name** should start with api.
Registration Port	The TCP port on the Registration Host. Defaults to **443**.
Use HTTPS for registration	If enabled, HTTPS (instead of HTTP) is used for registration. **Enabled** by default.
Validate certificates with HTTPS	If enabled, use a certificate authority to validate the HTTPS certificate. A certificate authority file can be uploaded on the *Certificate* page. **Disabled** by default.
Messaging Services	If enabled, messaging services are used for status updates and commands. **Enabled** by default.

3. Click **Save** to save settings.

10: Maintenance

This chapter describes various maintenance activities of an administrator. These include viewing status, backing up and restoring configuration files, updating firmware, viewing the event log, and resetting the unit. It contains the following sections:

- *Device Status*
- *Configuration/Factory Defaults*
- *Update Firmware*
- *View Event Log*
- *Unit Reset*

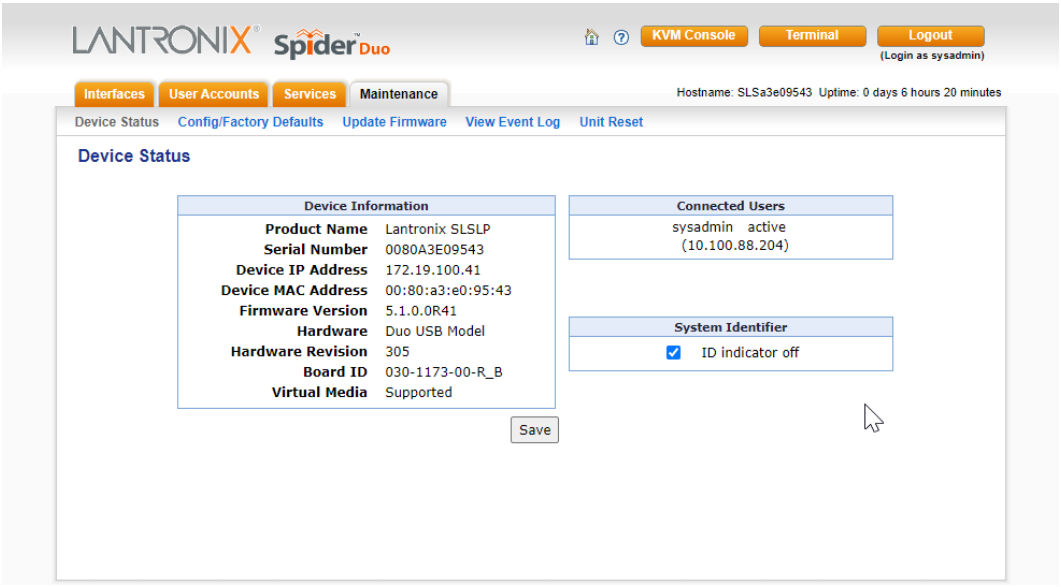
Device Status

The Device Status page contains a table with information about the Spider device's hardware and firmware. This information is useful if technical support is required.

To view device information, perform the following steps.

1. Click **Maintenance** > **Device Status**. The Device Status page displays.

Figure 10-1 Device Status Page



2. View or modify the following fields.

Table 10-2 Device Status Settings

Field	Description
Device Information	Displays the product name, serial number, device IP address, device MAC address, firmware version, SAM4s firmware version, hardware, hardware revision, board ID, and virtual media.

Table 10-2 Device Status Settings (continued)

Field	Description
Connected Users	Displays the user name and IP address of the active connection. It also displays whether the user is connected to the Remote Console, and if so, whether exclusive access mode is activated.
System Identifier	Check the box to turn the SysID LED indicator on and off. Each Spider device has an orange LED that can be lit by remote control. By default the LED is off, and when you clear the checkbox, the LED gets turned on.

3. Click **Save** to save settings.

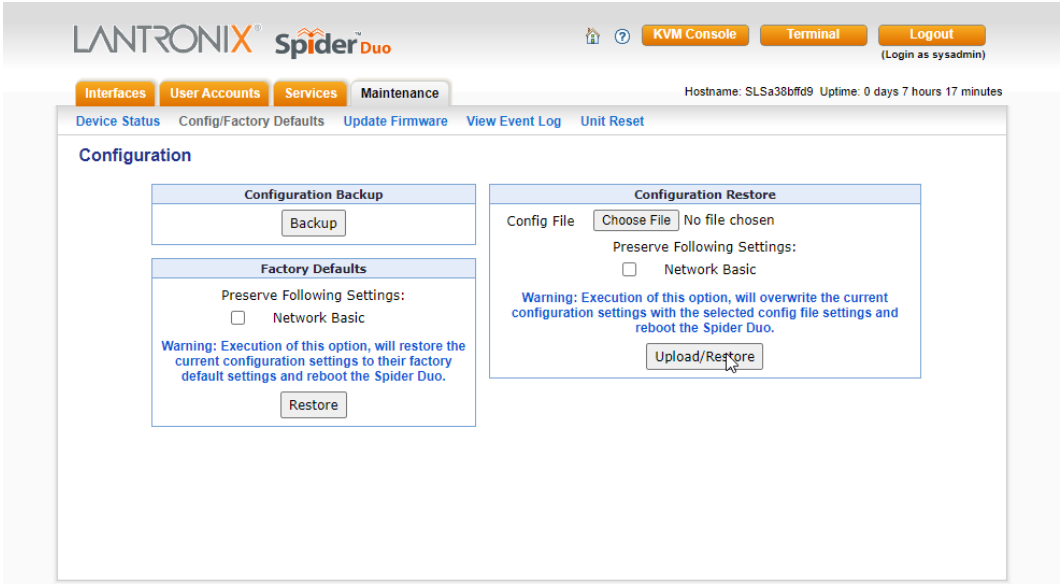
Configuration/Factory Defaults

In the Configuration page, you can specify the backup, preserve Network Basic settings, and restore the computer or Spider device configuration.

To view the configuration parameters, perform the following steps.

1. Click **Maintenance > Config/Factory Defaults**. The following page displays.

Figure 10-3 Configuration Page



2. Edit the following fields.

Field	Description
Configuration Backup	To back up all settings to a file on the client system, click the **Backup** button.

Field	Description
Configuration Restore	To return the Spider device settings to a previously saved configuration: ◆ Click the **Choose File** button. You can then browse to and select the saved configuration file. ◆ In the **Preserve Following Settings:** field, click the **Network Basic** checkbox to preserve the current network basic settings on the Network Settings page and import only the remaining settings from the configuration file. ◆ Click the **Upload/Restore** button. If you select this option, the Spider device reboots after you apply the update. ***Warning:*** ***Execution of this function overwrites the current configuration settings with the selected configuration file settings and reboots the device.***
Factory Defaults	To restore the factory defaults, click the **Network Basic** checkbox. Then click the Restore button. ***Warning:*** ***Execution of this option restores the current configuration settings to the factory default settings and reboots the device.*** ***Note:*** *The device can also be restored to its original factory settings via the physical reset switch. To access the reset switch, insert a pin or similar object through the pinhole on the underside of the device until the switch is depressed for 3 to 5 seconds. This will initiate a factory reset followed by a reboot of the device.*

Update Firmware

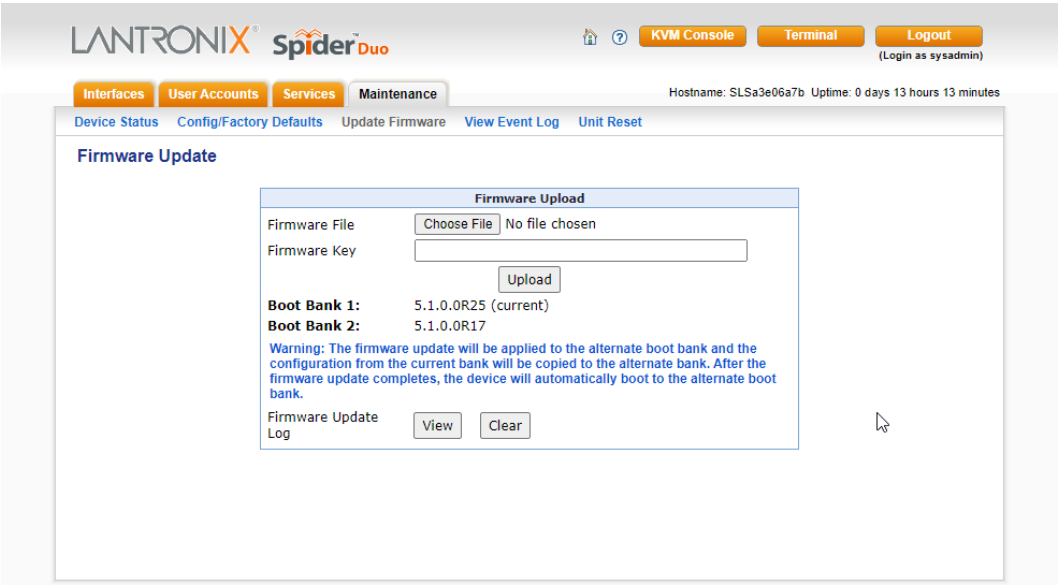
Many of the functions and features of the Spider device are implemented in firmware and capable of field upgrades. The latest firmware may be found at www.lantronix.com. The firmware file is approximately 200 Mbytes in size and has a .tgz suffix.

Upon updating firmware, the Spider device resets itself. After the reset, the login page displays (if not, manually return to the login page).

To update Spider device firmware, perform the following steps.

1. Download the firmware file to the client system local drive or an accessible network drive.
2. Click **Maintenance > Update Firmware**. The Firmware Update page displays.

Figure 10-4 Update Firmware Page



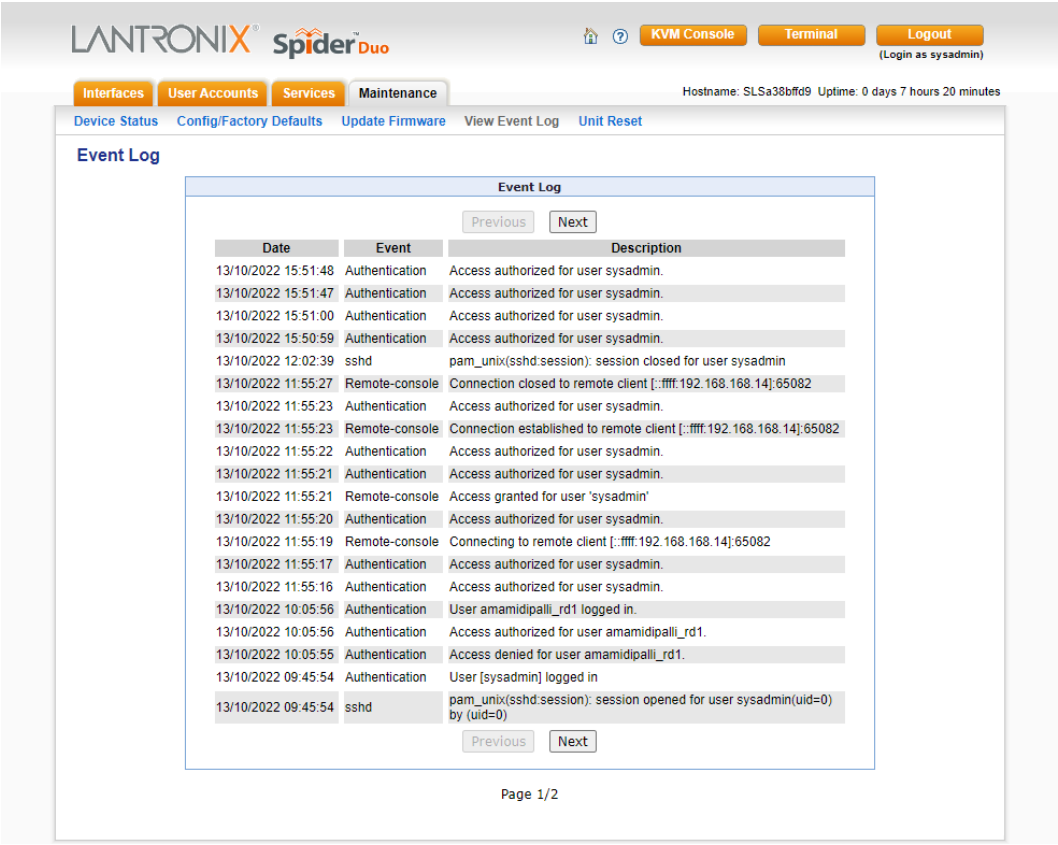
3. Click **Choose File**. In the pop-up window, navigate to and select the firmware file (decompressing the .tgz file is not necessary).
4. Enter the **Firmware Key** in the provided field.
5. Click **Upload** to copy the file into the Spider device's local memory. When uploaded correctly, the Firmware Upload window displays the version number of the new firmware. Click the **Update** button to replace the old with the new, or to cancel the operation, click the **Discard** button. Do not interrupt power to the Spider device during the update process.

View Event Log

To view the current event log, perform the following steps.

1. Click **Maintenance > Event Log**. The Event Log page displays.

Figure 10-5 Event Log Page



2. Navigate between logs by clicking **Prev** and **Next**.

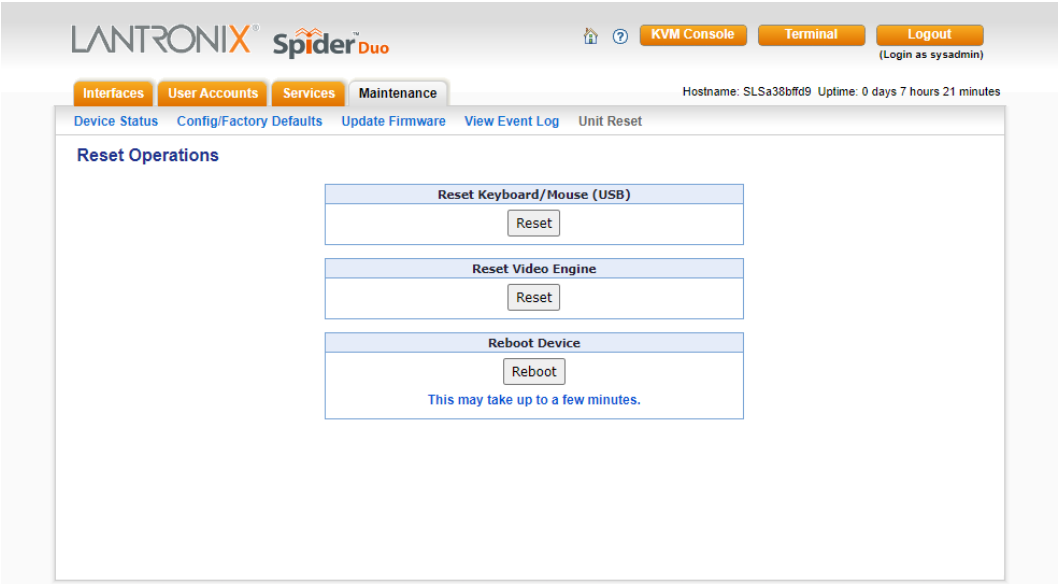
Unit Reset

In general, the Spider device requires a reset when implementing a firmware update. In the event of an abnormal operation, a number of subsystems may be reset without resetting the entire Spider device.

To reset the Spider device, perform the following steps.

1. Log into the Spider device as **`sysadmin`**.
2. Click **Maintenance > Unit Reset**. The following page displays.

Figure 10-6 Unit Reset Page



3. Click the **Reset** button for **Reset Keyboard/Mouse (USB)**, **Reset USB**, or **Reset Video Engine** to clear and reset the subsystem. Resetting subsystems does not terminate connected users.

Note: *Reset USB displays only on the SpiderDuo device.*

4. To perform a complete device reboot, click **Reboot Device**. A prompt requesting confirmation displays. Upon confirmation, all user connections are closed and the device performs a full reboot.

11: Command Reference

This chapter lists and describes the command line interface (CLI) syntax and contains the following sections:

Command Syntax

Commands have the following format: <action> <category> <parameter(s)> where <action> is set, show, connect, diag, admin, or logout. <category> is a group of related parameters you want to configure or view. Examples are device, group, user, and network. <parameter(s)> is one or more name-value pairs in one of the following formats:

- <parameter name> <aa | bb>—Specify one of the values (aa or bb) separated by a vertical line (|). The values are all lowercase and must be entered exactly as shown. Bold indicates a default value.
- <parameter name> <Value>—Specify an appropriate value, for example, a device group name. This User Guide shows parameter values in mixed case to indicate they are case sensitive. For example, if you saved a device group name in mixed case, you must enter it in mixed case; if you saved it in lowercase, you must enter it in lowercase.
- Square brackets [ ]—Indicate optional parameters.

Table 11-1 Action and Category

Action	Category
set	cflow | datetime | group | history | media | network | power | security | serial | user
show	cflow | datetime | group | history | logs | media | network | power | release | security | serial | sysconfig | user
connect	serial
diag	auth | internals | iperf | ping | ping6 | updatelogs
admin	config | firmware| reboot | reset | shutdown | sysinfo | version
logout	Terminates CLI session

Command Help

For general command help, type: **`help`**

For more information about a specific command, type **`help`** followed by the command, for example:

```
help set network
```

OR

type **`?`** after the command:

```
set network ?
```

Tips

Type enough characters to identify the action, category, or parameter name uniquely. For parameter values, type the entire value.

For example,

```
set network port 1 state static ipaddr 122.3.10.1 mask 255.255.0.0
```

can be shortened to

```
se net po 1 st static ip 122.3.10.1 ma 255.255.0.0.
```

Use the **Tab** key to automatically complete action, category, or parameter names. Type a partial name and press **Tab** to complete the name if only one is possible, or to display the possible names if more than one is possible.

Should you make a mistake while typing, backspace by pressing the **Backspace** key or the **Delete** key, depending on how you accessed the interface. Both keys work if you use VT100 emulation in your terminal access program when connecting to the console port. Use the **left** and **right arrow** keys to move within a command.

Use the **up** and **down arrows** to scroll through previously entered commands. If desired, select one and edit it. You can scroll through up to 100 previous commands entered in the session.

When the number of lines displayed by a command exceeds the size of the window (the default is 20), the "`Type more to see the next page`" message displays. To display the next page, type **`more`** and press **Enter**. You can override the number of lines (or disable the feature altogether) with the `set cli` command.

To clear an IP address, type **`0.0.0.0`**.

Admin Commands

admin config factorydefaults

Syntax

```
admin config factorydefaults
               [preserveconfig <Config Params to Preserve>]
```

Parameters

`<Config Params to Preserve>` is a comma separated list of current configuration parameters to retain after the config restore or factorydefaults: nt - Network Basic vp.

Description

Restores the Spider configuration and device database settings to factory defaults.

Note: *The unit reboots after this command. All current settings are lost.*

admin config restore

Syntax

```
admin config restore configname <Configuration Name>
                     location <local|default>
                     preserveconfig <Config Params to Preserve>
```

Parameters

`<Config Params to Preserve>` is a comma separated list of current configuration parameters to retain after the config restore or factorydefaults: nt - Network Basic vp.

Description

Restores a saved configuration.

Note: *A reboot automatically occurs after this command.*

admin config save

Syntax

```
admin config save
               [name <Configuration Name>]
               [location <local|default>]
```

Parameters

None

Description

Saves the current configuration.

Note: *Each time you use the admin config save command, the existing "config_save" file is overwritten.*

admin config show

Syntax

```
admin config show <local|default>
                  [sort <filename|date>]
```

Parameters

None

Description

Shows the current configuration.

admin firmware clearlog

Syntax

```
admin firmware clearlog
```

Description

Clears the firmware update log.

admin firmware show

Syntax

```
admin firmware show [viewlog <enable|disable>]
```

Description

Lists the current firmware revision, the boot bank status, and optionally displays the log containing details about firmware updates.

admin reboot

Syntax

```
admin reboot
```

Description

Immediately terminates all connections and reboots the device.

admin reset kmsoft

Syntax

```
admin reset kmsoft
```

Description

Software reset keyboard and mouse.

admin reset switchhard

Syntax

```
admin reset switchhard
```

Description

Hardware reset switch.

admin reset switchsoft

Syntax

```
admin reset switchsoft
```

Description

Software reset switch.

admin reset usb

Syntax

```
admin reset usb
```

Description

USB hub reset.

admin shutdown

Syntax

```
admin shutdown
```

Description

Immediately terminates all connections and prepares the SLS for power off.

admin sysinfo download

Syntax

```
admin sysinfo download <ZIP File Name> location <ftp|sftp|scp>
  host <IP Address or Name> login <User Login> [<parameters>]
```

Parameters

```
[path <Path to Save File>]
```

Description

Download locally saved sysinfo ZIP files.

admin sysinfo save

Syntax

```
admin sysinfo save <ZIP File Name> location <ftp|sftp|scp>
  host <IP Address or Name> login <User Login> [<parameters>]
```

Parameters

```
[path <Path to Save File>]
```

```
[comment <Comment Included in the System Info File>]
```

Description

Saves the current Spider system info to a selected location in ZIP format.

admin sysinfo show

Syntax

```
admin sysinfo show
```

Description

List locally saved sysinfo ZIP files.

admin version

Syntax

```
admin version
```

Description

Displays firmware version information.

ConsoleFlow Commands

set cflow client

Syntax

```
set cflow client <enable|disable>
```

Description

Configure interaction with ConsoleFlow management server. The communication with the server is disabled by default, and can be enabled.

set cflow statusinterval

Syntax

```
set cflow statusinterval <1-60 minutes>
```

Description

Set interval between status updates.

set cflow connection

Syntax

```
set cflow connection <cloud|onpremise> [<one or more parameters>]
```

Parameters

```
[host <FQDN>]
[port <TCP Port>]
[secureport <enable|disable>]
[validatecerts <enable|disable>]
[mqttstate <enable|disable>]
```

Description

Configure ConsoleFlow Cloud or On-Premise settings.

set cflow devicename

Syntax

```
set cflow devicename <Device Name> description <Device Description>
```

Description

Configure the device name and description used for registration.

set cflow id

Syntax

```
set cflow id
```

Description

Set the device ID.

set cflow key

Syntax

```
set cflow key
```

Description

Set the device key.

show cflow

Syntax

```
show cflow
```

Description

Show ConsoleFlow settings and status.

Date/Time Commands

set datetime

Syntax

```
set datetime <one parameter>
```

Parameters

```
date <MMDDYYhhmm[ss]>
utcoffset <offset string>
```

Notes:

- *MMDDYYhhmm[ss] can be:*
  - MM is 1-12
  - DD is 1-31
  - YY is 00-99
  - hh is 0-23
  - mm is 0-59
  - ss is 0-59
- *Offset string can be:*
  - -11h, -10h, -9h, -8h, -7h, -6h, -5h, -4h, -3h, -2h, -1h
  - +/-0h, +1h, +2h, +3h, +4h, +5h, +6h, +7h, +8h, +9h, +10h, +11h, +12h

Note: *Select only one offset as shown above.*

Description

Sets the date and time or UTC offset.

show datetime

Syntax

```
show datetime
```

Description

Shows the date/time and UTC offset.

Diagnostic Commands

diag auth

Syntax

```
diag auth <enable|disable>
```

Description

Enables or disables additional logging for user authentication.

Note: *Enable authentication diagnostics before configuring LDAP or RADIUS. This option does not persist through reboots.*

diag internals

Syntax

```
diag internals [detailed <enable|disable>]
```

Description

Displays debugging information for internal Spider processes.

diag iperf

Syntax

```
diag iperf mode <server|client> [host <iPerf Server IP Address or Name>]
[options <iPerf options>] [email <Email Address>
```

Description

Run an iPerf server or client to measure network throughput.

iPerf Options (enclose all options in quotes):

Set server port to listen on/connect to (default 5201):	`-p, --port n`
Format to report	`-f, --format [kmgtKMGT]`
Pause n seconds between reports	`-i, --interval n`
Bind to a host, an interface or multicast address	`-B, --bind <host>`
More detailed output	`-V, --verbose`
Output in JSON format	`-J, --json`
Options below are supported on client only:	
Set length of buffer to n (default 8 KB)	`-l, --length n[KMG]`
Use UDP rather than TCP	`-u, --udp`
TCP window size (socket buffer size)	`-q, --window n[KMG]`
Set TCP/SCTP maximum segment size (MTU)	`-M, --set-mss n`
Set TCP/SCTP no delay, disabling Nagle's Algorithm	`-N, --no-delay`
Set bandwith to n bits/sec (default 1Mbit/sec, unlimited for TCP)	`-b, --bitrate n[KMG]`
Number of bytes to transmit (instead of -t)	`-n, --bytes n[KMG]`
Time in seconds to transmit for (default 10 secs)	`-t, --time n`
Set the IPv6 flow label	`-L, --flowlabel n`
Use a 'zero copy' method of sending data	`-Z, --zerocopy`
Omit the first n seconds	`-O, --omit n`
Prefix every output line with this string	`-T, --title str`
# of blocks (packets) to transmit (instead of -t/-n)	`-k, --blockcount`
Set the IP type of service, 0-255. The usual prefixes for octal and hex can be used, i.e. 52, 064 and 0x34 all specify the same value	`-S, --tos n`
Set the IP dscp value, either 0-63 or symbolic	`--dscp n`

Note: *The output can optionally be emailed.*

Note: *The Spider2 uses iPerf version 3.X, which is incompatible with older versions (2.x).*

diag ping

Syntax

```
diag ping <IPV4 Address>
```
or
```
diag ping6 <IPV6 Address>
```

Description

Verifies if the Spider or SpiderDuo device can reach a host over the network.

diag updatelogs

Syntax

```
diag updatelogs
```

Description

Displays logs saved after the completion of the last firmware update.

History Commands

set history clear

Syntax

```
set history clear
```

Description

Clears the CLI command history.

show history

Syntax

```
show history
```

Description

Displays the 100 most recent CLI commands.

Log Commands

show logs

Syntax

```
show logs [<parameters>]
```

Parameters

```
[since <boot|YYYY-MM-DD HH:MM:SS|YYYY-MM-DD|Number of Minutes Ago>]
[level <info|warning|error>]
[download <scp|ftp|sftp> host <IP address or Name>
 login <User Login> file <Name of Log File>
 [path <Directory for Download>] [allsavedlogs]]
[savedlogs <list|all|tail|Saved Log File Name>]
```

Description

Displays system (journal) logs, with filtering options.

Note: *Without filtering the output will be very long; the use of a filter is recommended.*

Media Commands

Configures the SLS to present an image uploaded to the SLS (for example, a CDROM image) for system recovery or installation.

set media connect

Syntax

```
set media connect <Uploaded Media Filename>
```

Description

Connect the uploaded media to the target server.

set media disconnect

Syntax

```
set media disconnect
```

Description

Disconnects the media.

Note: *Linux target hosts may require connected media to be ejected first on the target host before a issuing a Disconnect command on the Spider.*

set media remove

Syntax

```
set media remove <Uploaded Media Filename>
```

Description

Remove an uploaded media file.

show media directory

Syntax

```
show media directory <Uploaded Media Filename>
```

Description

Display the top level directory of an uploaded media file.

show media status

Syntax

```
show media status
```

Description

Display virtual media status, including uploaded images.

Network Commands

set network basic

Syntax

```
set network basic <parameters>
```

Parameters

```
dns1 <IP Address>
dns2 <IP Address>
gateway <IP Address>
hostname <Host Name>
ipaddr <IP Address>
ipv6 <enable/disable>
ipv6addr <IPv6 Address/Prefix>
mask <Mask>
state <dhcp|static>
```

Note: *To clear IPV4 addresses, set ipv4 address to "0.0.0.0".To clear IPV6 address, set ipv6 address to "::" or "::/128".*

set network misc

Syntax

```
set network misc <parameters>
```

Parameters

```
httpsport <TCP Port>
telnet <enable/disable>
telnetport <TCP Port>
setupprotocol <enable/disable>
ssh <enable/disable>
sshport <TCP Port>
```

Description

Sets miscellaneous network parameters.

set network interface

```
set network interface <parameters>
```

Parameters

```
mode <auto|10mbit-half|100mbit-half|10mbit-full|100mbit-full|1000mbit-
full>
```

Description

Sets network interface modes.

show network all

Syntax

```
show network all
```

Description

Displays all network settings.

show network basic

Syntax

```
show network basic
```

Description

Displays basic network parameters.

show network misc

Syntax

```
show network misc
```

Description

Displays network miscellaneous parameters.

show network interface

Syntax

```
show network interface
```

Description

Displays network interfaces.

show network statistics

Syntax

```
show network statistics
```

Description

Displays network statistics.

Power Commands

set power

Syntax

```
set power state <on|off>
```

Description

Set PCU parameters.

show power

Syntax

```
show power
```

Description

Display Power Control Unit status and settings.

Release Commands

show release

Syntax

```
show release
```

Description

Displays current release notes.

Security Commands

set security

Syntax

```
set security <one or more parameters>
```

Parameters

```
[singlelogin <enable|disable>]
[screenshot <enable|disable>]
[directkvm <enable|disable>]
[system_access_control <enable|disable>]
[default_action <DROP|ACCEPT>]
```

Description

Sets security parameters.

set security system_access

Syntax

```
set security system_access delete rule_# <parameter>
set security system_access append option<1> <parameter<1> option<2>
<parameter<2>...
```

Parameters

```
rule_#              [Number]
starting_ip         {IP Address]
ending_ip           [IP Address]
group               [String]
action              [String]
```

Description

Security SYSTEM-ACCESS to append or delete an IP range entry. The append command requires all 4 options <starting_ip, ending_ip, group and action> to be completed.

show security

Syntax

```
show security
```

Description

Displays security parameters.

Serial Port Commands

connect serial

Syntax

```
connect serial
```

Description

Connects the Spider device to a device serial port.

Note: *To connect to a serial port, put the serial port in passthrough mode on the web interface. To disconnect from the device serial port, press* ***Esc****, then type* `exit` *(i.e. press the Escape key followed by the letters "e", "x", "i", "t").*

set serial mode

Syntax

```
set serial mode passthrough | config [<parameters>]
```

Parameters

```
[baud <1200-115200>]
[databits <7|8>]
[stopbits <1|2>]
[parity <none|odd|even>]
[flowcontrol <none|xon/xoff|rts/cts>]
```

Description

Set serial port parameters for each mode.

show serial

Syntax

```
show serial
```

Description

Displays serial port settings.

Sysconfig Commands

show sysconfig

Syntax

```
show sysconfig
```

Description

Display a report of parameters with firmware version, serial number, basic network settings, security settings, user/group information, and basic system settings.device.

User Commands

set user

Syntax

```
set user add|edit <User Login> [<parameters>]
```

Parameters

```
[email <Email Address>]
[fullname <Full Name>]
[group <Group Name|default|Admin|None>]
[mobile <Phone Number>]
```

Note: *The group 'default' (Unknown) and 'Admin' and are built-in groups. The group 'None' indicates that user is created without defining a group, and permissions will be assigned specifically to the user. A user will be assigned 'default' group by omitting group parameter when creating a new user.*

Description

Sets user login, email address, group, and mobile phone number.

set user delete

Syntax

```
set user delete <User Login>
```

Description

Deletes a user login.

set user password

Syntax

```
set user password <User Login>
```

Description

Sets user password.

show user name

Syntax

```
show user name [user <User Login>]
```

Description

```
Displays user names.
```

show user

Syntax

```
show user [index <Index Number>]
```

Description

Displays index numbers.

User Group Commands

set group

Syntax

```
set group add|edit <Group Name> [<parameters>]
```

Parameters

permissions <Permission List>

Description

Configures user groups. See *Group Permissions on page 102* for information about permissions.

set group delete

Syntax

```
set group delete <Group Name>
```

Description

Deletes user groups.

show group name

Syntax

```
show group [name <Group Name>]
```

Description

Displays group names.

show group index

Syntax

```
show group [index <Index Number>]
```

Description

Displays group indexes.

Note: *[Group of 'None (username)'] indicates that user was created without defining a group, and permissions will be assigned specifically to the user. In order to specify a group of this type "None", use '@username' as the name parameter.*

Group Permissions

For group permissions, each user is a member of a group, and has a set of permissions associated with the group. The group permissions are defined by permissions parameters.

A <Permission List> is a comma-separated list of user rights to be added to or removed from the group current permissions. Precede the two-letter acronym with a '-' to remove a user right. For example, 'nt,dt,-ka' adds Networking and Date/Time rights and removes KVM Console Access rights. See the following list:

- br: Board Reset
- dk: Direct KVM
- dt: Date/Time Settings
- fc: Firmware/Config Management
- gp: Group Permissions
- ka: KVM Console Access
- ke: KVM Settings(Encoding)
- kx: KVM Settings(Exclusive Access)
- kh: KVM Settings(Hotkeys)
- km: KVM Settings(Monitor Mode)
- ks: Keyboard/Mouse Settings
- ld: LDAP Settings
- ns: Network Settings
- pc: Change Password
- po: Power Control
- sn: SNMP Settings
- sa: SSH/Telnet Access
- sm: SSL Certificate Management
- sl: Security/Log/Authentication
- ss: Serial Settings
- us: USB Settings
- um: User/Group Management
- vu: Virtual Media

Appendix A: Troubleshooting

This section provides a list of possible solutions to common issues. If the issue persists, contact *Technical Support* for further assistance. If applicable, perform one or more of the following steps and include the outputs when reporting your issue:

- Create video/screenshot showing the issue
- From the CLI, run `admin sysinfo save` and save the output

No connection can be established to the Spider device.

Check cabling. Are both USB cables or all of the USB and PS/2 cables plugged in? Are both Pwr LEDs lit? Is the Ethernet cable plugged in, and the Link light lit? Is there Activity?

Have a look on your network. Verify your network configuration (IP address, router). Send a ping request to the Spider device to find out whether the Spider device is reachable via the network. Establish a direct connection between the Spider device and the client. If you use a firewall then check the appropriate port for accepting connections. The TCP port443 (for both HTTPS and RFB) has to be open (the server providing the firewall has to accept incoming TCP connections on these ports). You may restrict these connections to the IP addresses used by the Spider device and your client.

Login on the Spider device fails.

Verify both your user login and your password. By default, the user **sysadmin** has the password **PASS**. Ensure the web browser is configured to accept cookies.

The Remote Console window of the Spider device does not open.

A firewall may prevent access to the Remote Console (TCP port 443). If there is a proxy server between the Spider device and your host, then you may not be able to transfer the video data using RFB. Check the settings of the Spider device and choose a different server port used for RFB transfer.

The video quality is bad or the picture is grainy.

Verify a supported resolution/timing is being used (see *Appendix B: Supported Resolutions and Refresh Rates*). Alternately, from the web UI go to **Maintenance > Unit Reset** and click the Reset button under “Reset Video Engine”.

The keyboard and/or mouse is not behaving as expected.

Try the following:

- From the web UI go to **Maintenance > Unit Reset** and click the Reset button under “Reset Keyboard/Mouse”.
- Disconnect/reconnect the mouse and/or keyboard.
- Reboot or power cycle the device.
- From the CLI, reset the SAM4s controller by running `admin reset km`.
- For USB keyboard or mouse, check the connection from the target host to see if the keyboard or mouse is recognized - on Linux target hosts, collect the input from the `dmesg` command, and on Windows target hosts, check the Device Manager.

Special key combinations (e.g., ALT+F2, ALT+F3) are intercepted by the client system and not transmitted to the remote computer.

You have to define a Button Key. This can be done in the Remote Console settings. Alternatively, use the soft keyboard feature.

The Spider device web pages are not displayed correctly.

Check your browser's cache settings. Ensure the cache settings are not set to "do not check for newer pages". Otherwise the web pages may be loaded from your browser cache and not from the Spider device.

Every time I open a dialog box with some buttons, the mouse pointers are not synchronous anymore.

Disable the setting **Automatically move mouse pointer to the default button of dialog boxes** in the mouse settings of your operating system.

I forgot my password. How can I reset the Spider device to factory defaults?

To reset the device via the physical reset switch, see *Configuration/Factory Defaults on page 78*.

Cannot upload the signed SSL certificate in MacOS X.

If an "internal error" occurs while uploading the signed certificate either changes the extension of the file to .txt or adds a file helper using the web browser preferences for this type of file. Make sure that the encoding is set to "plain text" and the checkbox "use for outgoing" is set. As an alternative, you may also use a Mozilla based browser (Mozilla, Firefox).

If you cannot get into the BIOS of your system or you cannot boot your system using Virtual Media, try some of the following:

If you have a PS/2 model Spider device:

1. Under **Interfaces > Keyboard/Mouse**, set the **Host Interface** to PS/2
2. If your system only has USB and no PS/2, do the above and use a PS/2 to USB adapter

If the key used to enter BIOS setup or the boot menu on your PC is intercepted by your client OS, add a Virtual Key under **Interfaces > KVM Console Settings**.

When a Spider USB model (Duo or KVM) is connected to a Linux host, and the Linux host is rebooted, sometimes messages such as "device not accepting address XX", "Cannot reset (err = -22)", "Cannot disable (err = -22)" or "Cannot enable. Maybe the USB cable is bad?" are displayed on the Linux host.

These messages are benign, and are displayed when the Linux host does not properly handle the shutdown of the USB connection. These messages do not affect functionality; when the Linux host boots USB functionality should resume without any issues.

Appendix B: Supported Resolutions and Refresh Rates

The table below lists the supported resolution and refresh rates for video.

Table B-1 Supported Video Resolutions and Refresh Rates

Resolution (x,y)	Refresh Rates (Hz)
640x480	60
800x600	60, 75
1024x768	60, 75
1152x864	75
1280x800	60
1280x960	60
1280x1024	60, 75
1440x900	60
1600x1200	60

Appendix C: Mounting Bracket Kit

A versatile mounting bracket and screws are supplied to assist in easily installing and mounting a single Spider or SpiderDuo device into a server rack in various orientations (e.g., horizontal or vertical). The kit number is 083-015-R.

Figure C-1 Mounting Bracket and Screws

The kit includes:

- One (1) 4.0” x 1-3/4” x 1/4” bracket
- Two (2) 1/2” long, #10-32 stainless steel Phillips-head screws

  Once the mounting bracket is installed in the rack, the Spider or SpiderDuo device can be easily and securely attached to the elevated mounting posts and easily removed if necessary.

To install the mounting bracket and Spider device into a server rack, perform the following steps.

1. Mount the bracket with a Phillips screwdriver.

Figure C-2 Attaching the Mounting Bracket

2. Attach the Spider or SpiderDuo device to the bracket mounting posts.

Figure C-3 Attaching the Device to the Mounting Bracket

3. Connect the cables and the Spider or SpiderDuo device is ready to use!

Figure C-4 Connecting the Cables

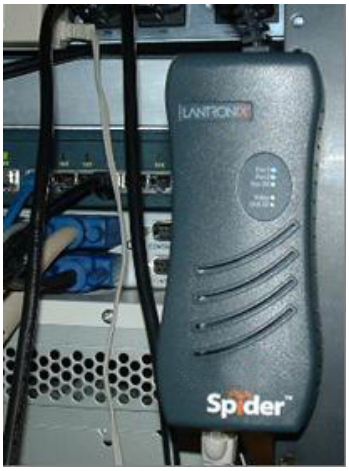


Table C-5 Lantronix Part Number

Lantronix Part Number	Description
083-015-R	Mounting Bracket Kit for Spider device

The bracket kit is included in the box with the Spider or SpiderDuo device that ship with v2.0 firmware and later. For earlier shipments, the mounting kit is sold separately. For additional information contact Lantronix Sales at 800-422-7055, or for technical questions contact Lantronix Technical Support at https://www.lantronix.com/technical-support.

Appendix D: PCU Safety Information

Please follow the safety precautions described below when installing and operating the PCU.

Cover

- Do not remove the cover of the PCU. There are no user-serviceable parts inside. Opening or removing the cover may expose you to dangerous voltage that could cause fire or electric shock.
- Refer all servicing to Lantronix.

Power Plug

- When disconnecting the power cable from the socket, pull on the plug, not the cord.
- Always connect the power cord to a properly wired and grounded power source. Do not use adapter plugs or remove the grounding prong from the cord.
- Only use a power cord with a voltage and current rating greater than the voltage and current rating marked on the unit.
- Install the unit near an AC outlet that is easily accessible.
- Always connect any equipment used with the product to properly wired and grounded power sources.
- To help protect the product from sudden, transient increases and decreases in electrical power, use a surge suppressor, line conditioner, or uninterruptible power supply (UPS) connected between the AC power source and PCU.
- Do not connect or disconnect this product during an electrical storm.

Input Supply

- Check nameplate ratings to assure there is no overloading of supply circuits that could affect overcurrent protection and supply wiring.

Warning: ***To avoid electrical shock always disconnect the AC power cords to the PCU before servicing.***

Grounding

- Maintain reliable grounding of this product.
- Pay particular attention to supply connections when connecting to power strips, rather than directly to the branch circuit.

Fuses

For protection against fire, replace the power-input-module fuse with the same type and rating.

Appendix E: Technical Support

If you are unable to resolve an issue using the information in this documentation, contact the following resources.

Technical Support

Check our online knowledge base or send a question to Technical Support at www.lantronix.com/technical-support.

When you report a problem, please provide the following information:

- Your name, and your company name, address, and phone number
- Lantronix model number
- Lantronix serial number
- Firmware version
- Description of the problem
- Target computer interface (PS/2 or USB) and video format
- Status of the unit when the problem occurred (please try to include information on user and network activity at the time of the problem)
- From the CLI, run `admin sysinfo save` and save the output

Appendix F: Compliance

The following meet the ISO/IEC Guide 17050-1, 17050-2 and EN 45014 compliances.

Manufacturer Name & Address

Lantronix, Inc.
48 Discovery, Suite 250, Irvine, CA 92618 USA

Declares that the following product:

Product Name: Lantronix® Spider™

Conforms to the following standards or other normative documents:

- UL 62368-1
- CE - IEC 62368-1
- FCC Part 15, Equipment Class A
- EN 55032:2015/A11: 2020
- EN 55035 2017/A11:2020
- EN61000-3-2: 2019/A1:2021
- EN61000-3-3: 2013/A2:2021

Warning: ***This is a class A product. In a domestic environment this product may cause radio interference in which case the user may be required to take adequate measures.***

Caution: ***Risk of explosion if battery is replaced by an incorrect type. Dispose of used batteries according to the instructions.***

RoHS Notice

All Lantronix products in the following families are China RoHS-compliant and free of the following hazardous substances and elements:

◆ Lead (Pb)	◆ Mercury (Hg)	◆ Polybrominated biphenyls (PBB)
◆ Cadmium (Cd)	◆ Hexavalent Chromium (Cr (VI))	◆ Polybrominated diphenyl ethers (PBDE)

Product Family Name	Toxic or hazardous Substances and Elements					
	Lead (Pb)	Mercury (Hg)	Cadmium (Cd)	Hexavalent Chromium (Cr (VI))	Polybrominated biphenyls (PBB)	Polybrominated diphenyl ethers (PBDE)
UDS1100 and 2100	0	0	0	0	0	0
EDS	0	0	0	0	0	0
MSS100	0	0	0	0	0	0
IntelliBox	0	0	0	0	0	0
XPress DR & XPress-DR+	0	0	0	0	0	0
SecureBox 1101 & 2101	0	0	0	0	0	0
WiBox	0	0	0	0	0	0
UBox	0	0	0	0	0	0
MatchPort	0	0	0	0	0	0
SLC	0	0	0	0	0	0
XPort	0	0	0	0	0	0
WiPort	0	0	0	0	0	0
SLB	0	0	0	0	0	0
SLP	0	0	0	0	0	0
SCS	0	0	0	0	0	0
Spider	0	0	0	0	0	0
DSC	0	0	0	0	0	0

O: toxic or hazardous substance contained in all of the homogeneous materials for this part is below the limit requirement in SJ/T11363-2006.

X: toxic or hazardous substance contained in at least one of the homogeneous materials used for this part is above the limit requirement in SJ/T11363-2006.

LANTRONIX®

CE

EU DECLARATION OF CONFORMITY

Manufacturer's Name:	LANTRONIX, INC.
Manufacturer's Address:	48 Discovery, Suite 250 Irvine, CA 92618 USA
Product Type:	KVM over IP Switch
Product Family:	SpiderDUO
Model name:	SLSLP400USB-02
Rated:	5.0 VDC
Intended use:	Commercial installations, indoor use

Manufacturer's Quality System:

TÜVRheinland

ISO 9001:2015 Certificate No. 74 300 4282 TUV Rheinland

Applicable EU Directives:

Low Voltage Directive (2014/35/EU)
- EN IEC 62368-1:2020/A11:2020

EMC Directive (2014/30/EU)
- EN 55032:2015/A11:2020
- EN 55035:2017/A11:2020
- EN IEC 61000-3-2:2019/A1: 2021
- EN 61000-3-3:2013/A2:2021

RoHS
1) 2011/65/EU Restriction of the use of Hazardous Substances in EEE (RoHS)
2) 2015/863/EU Change of Annex II from 2011/65/EU
3) Directive 2018/736/EU and 2018/741/EU
- EN 6300-2018

Statement of Conformity: The product specified above complies with applicable EU directive referenced, including the application of sound engineering practice.

Signature: _____ Date: November 8, 2022

Name: Fathi Hakam Title: VP of Engineering

CERT-00XXX rev A

LANTRONIX®

UK CA

UK DECLARATION OF CONFORMITY

Manufacturer's Name:	LANTRONIX, INC.
Manufacturer's Address:	48 Discovery, Suite 250 Irvine, CA 92618 USA
Product Type:	KVM over IP Switch
Product Family:	SpiderDUO
Model name:	SLSLP400USB-02
Rated:	5.0 VDC
Intended use:	Commercial installations, indoor use

Manufacturer's Quality System:

TÜVRheinland

ISO 9001:2015 Certificate No. 74 300 4282 TUV Rheinland

Applicable EU Directives:

Low Voltage Directive (2014/35/EU)
- EN IEC 62368-1:2020/A11:2020

EMC Directive (2014/30/EU)
- EN 55032:2015/A11:2020
- EN 55035:2017/A11:2020
- EN IEC 61000-3-2:2019/A1: 2021
- EN 61000-3-3:2013/A2:2021

RoHS
1) 2011/65/EU Restriction of the use of Hazardous Substances in EEE (RoHS)
2) 2015/863/EU Change of Annex II from 2011/65/EU
3) Directive 2018/736/EU and 2018/741/EU
- EN 6300-2018

Statement of Conformity: The product specified above complies with applicable EU directive referenced, including the application of sound engineering practice.

Signature: _____ Date: November 8, 2022

Name: Fathi Hakam Title: VP of Engineering

CERT-00XXX rev A