

LANTRONIX®

Spider™

# SecureLinx Spider™ and SpiderDuo™ User Guide



SecureLinx Spider (USB)



SecureLinx SpiderDuo (PS/2)

## Copyright and Trademark

© 2009 and 2010, Lantronix. All rights reserved. No part of the contents of this book may be transmitted or reproduced in any form or by any means without the written permission of Lantronix. Printed in the United States of America.

Ethernet is a trademark of XEROX Corporation. UNIX is a registered trademark of The Open Group. Windows 95, Windows 98, Windows 2000, Windows XP are trademarks of Microsoft Corp. Netscape is a trademark of Netscape Communications Corporation.

## LINUX GPL Compliance

Certain portions of source code for the software supporting the Spider family are licensed under the GNU General Public License (GPL) as published by the Free Software Foundation and may be redistributed and modified under the terms of the GNU GPL. A machine readable copy of the corresponding portions of GPL licensed source code is available at the cost of distribution.

Such source code is distributed WITHOUT ANY WARRANTY, INCLUDING ANY IMPLIED WARRANTY OF MERCHANTABILITY OR FITNESS FOR A PARTICULAR PURPOSE. See the GNU General Public License for more details.

A copy of the GNU General Public License is available on the Lantronix Web Site at <http://www.lantronix.com/> or by visiting <http://www.gnu.org/copyleft/gpl.html>. You can also obtain it by writing to the Free Software Foundation, Inc. 59 Temple Place, Suite 330, Boston, MA 02111-1307 USA.

## Warranty

For details on the Lantronix warranty replacement policy, go to [www.lantronix.com/support/warranty](http://www.lantronix.com/support/warranty).

## Contacts

### Lantronix Corporate Headquarters

167 Technology Drive  
Irvine, CA 92618, USA  
Toll Free: 800-526-8766  
Phone: 949-453-3990  
Fax: 949-450-7249

### Technical Support

Online: [www.lantronix.com/support](http://www.lantronix.com/support)  
Phone: (800) 422-7044  
(949) 453-7198

### Technical Support Europe, Middle East, Africa

Phone: +33 1 39 30 41 72  
Email: [mailto:eu\\_techsupp@lantronix.com](mailto:eu_techsupp@lantronix.com) or [mailto:eu\\_support@lantronix.com](mailto:eu_support@lantronix.com)

Firmware downloads, FAQs, and the most up-to-date documentation are available at [www.lantronix.com/support](http://www.lantronix.com/support)

### Sales Offices

For a current list of our domestic and international sales offices, go to the Lantronix web site at [www.lantronix.com/about/contact](http://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 cause 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 voids 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 [www.lantronix.com/support/documentation](http://www.lantronix.com/support/documentation).

## Revision History

| Date  | Rev. | Comments  |
|-------|------|---|
| 3/07  | A    | Initial Document  |
| 11/07 | 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. |
| 4/08  | C    | Added Direct KVM; KVM-only mode; Spider network web page; ability to preserve network settings for factory defaults; country code support; iGoogle gadget; instructions for using the mounting kit.                 |
| 5/09  | D    | Updated to firmware version 2.2, VIP access.  |
| 9/09  | E    | Updated and added SpiderDuo.  |
| 03/10 | F    | Updated to firmware version 3.01.   |

## Table of Contents

|   |           |
|---|-----------|
| Copyright and Trademark                           | 2         |
| LINUX GPL Compliance                              | 2         |
| Warranty  | 2         |
| Contacts  | 2         |
| Disclaimer and Revisions                          | 3         |
| Documentation Changes                             | 3         |
| Revision History                                  | 3         |
| <b>1: About This Guide</b>                        | <b>13</b> |
| Chapter and Appendix Summaries                    | 13        |
| Conventions                                       | 14        |
| Additional Documentation                          | 14        |
| <b>2: Overview</b>                                | <b>15</b> |
| Spider Overview                                   | 15        |
| Features  | 15        |
| Functionality                                     | 16        |
| System Configuration and Cables                   | 16        |
| Technical Specifications                          | 18        |
| SpiderDuo Overview                                | 19        |
| Features  | 19        |
| Functionality                                     | 19        |
| System Configuration and Cables                   | 20        |
| Technical Specifications                          | 22        |
| Product Information Label                         | 23        |
| <b>3: Installing the Spider</b>                   | <b>24</b> |
| Package Contents                                  | 24        |
| Installing the Spider                             | 24        |
| Detector Installation and IP Address Reset        | 27        |
| Target Computer Setup                             | 29        |
| Video Resolutions and Refresh Rates Configuration | 29        |
| Mouse-to-Cursor Synchronization                   | 30        |
| Telnet/SSH Connections to Serial Ports            | 30        |
| Cable Connections for KVM and USB                 | 31        |
| Device Failure or Cable Break in the Daisy Chain  | 31        |
| Client Server Setup                               | 31        |
| Network Environment                               | 31        |
| Spider Power                                      | 32        |
| <b>4: Installing the SpiderDuo</b>                | <b>33</b> |
| Package Contents                                  | 33        |
| Installing the SpiderDuo                          | 33        |
| Detector Installation and IP Address Reset        | 36        |

---

|   |           |
|---|-----------|
| Target Computer Setup                             | 38        |
| Video Resolutions and Refresh Rates Configuration | 38        |
| Mouse-to-Cursor Synchronization                   | 39        |
| Telnet/SSH Connections to Serial Ports            | 39        |
| Cable Connections for KVM and USB                 | 39        |
| Power Sequencing                                  | 40        |
| Client Server Setup                               | 40        |
| Network Environment                               | 40        |
| PCU Power   | 41        |
| <b>5: Web Browser Access</b>                      | <b>43</b> |
| Accessing the KVM Console                         | 43        |
| <b>6: Remote System Control</b>                   | <b>44</b> |
| Overview  | 44        |
| Remote Console Window                             | 44        |
| Main Viewport and Scroll Bars                     | 45        |
| Button Keys                                       | 45        |
| Toolbar   | 45        |
| Options   | 46        |
| Information Bar - Connection                      | 46        |
| Information Bar - Resolution                      | 46        |
| Information Bar - Network Traffic                 | 46        |
| Concurrent Access State                           | 46        |
| Monitor Only State                                | 46        |
| Exclusive Access                                  | 46        |
| Basic Remote Console Operation                    | 47        |
| Auto Video Adjustment                             | 48        |
| Screen Display Adjustments                        | 48        |
| Fast Sync and Intelligent Sync                    | 48        |
| Single and Double Mouse Modes                     | 48        |
| Local Cursor                                      | 48        |
| Optimizing Video                                  | 49        |
| Auto and Manual Video Adjustment                  | 49        |
| Clock and Phase                                   | 49        |
| Video Encoding                                    | 49        |
| Scaling Target Video to Client Resolution         | 50        |
| Keyboard Functions                                | 50        |
| Soft Keyboard                                     | 50        |
| Local Keyboard                                    | 50        |
| Hotkeys   | 50        |
| Other Remote Console Functions                    | 50        |
| Monitor Only                                      | 51        |
| Exclusive Access                                  | 51        |

---

|   |           |
|---|-----------|
| Screenshot to Clipboard _____                 | 51        |
| Refresh Video _____                           | 51        |
| Telnet/SSH _____                              | 51        |
| Set up and Enable _____                       | 51        |
| Passthrough Use _____                         | 51        |
| Telnet Console Use _____                      | 52        |
| <b>7: Interfaces _____</b>                    | <b>53</b> |
| Network Settings _____                        | 53        |
| Network Basic Settings _____                  | 54        |
| LAN Interface Settings _____                  | 55        |
| IPv6 Settings (Firmware v3.0 or higher) _____ | 55        |
| Miscellaneous Network Settings _____          | 55        |
| Serial Port Settings _____                    | 56        |
| KVM Console Settings _____                    | 57        |
| KVM Console Settings _____                    | 58        |
| Transmission Encoding _____                   | 59        |
| KVM Console Type _____                        | 59        |
| KVM Console Deployment _____                  | 59        |
| Miscellaneous KVM Console Settings _____      | 59        |
| Mouse Hotkey _____                            | 60        |
| KVM Console Virtual Keys _____                | 60        |
| Keyboard/Mouse _____                          | 60        |
| Keyboard/Mouse Settings _____                 | 61        |
| Keyboard Model _____                          | 62        |
| Key Release Timeout _____                     | 62        |
| Country Code _____                            | 62        |
| USB Mouse Type _____                          | 62        |
| Mouse Speed _____                             | 63        |
| Video _____                                   | 64        |
| Virtual Media _____                           | 65        |
| Virtual Media Active Image _____              | 66        |
| Drive Redirection _____                       | 66        |
| Virtual Media Options _____                   | 67        |
| Image on Windows Share _____                  | 67        |
| Floppy Image _____                            | 68        |
| Connecting to a Redirected Drive _____        | 69        |
| User Interface Settings _____                 | 71        |
| Configure VIP _____                           | 72        |
| <b>8: User Accounts _____</b>                 | <b>73</b> |
| Local vs. Remote Authentication _____         | 73        |
| Local User Management _____                   | 73        |
| Modifying Passwords _____                     | 73        |

---

|   |            |
|---|------------|
| User and Group Management _____                           | 74         |
| User Management _____                                     | 74         |
| Group Management _____                                    | 75         |
| User Permissions _____                                    | 75         |
| Remote Authentication _____                               | 76         |
| LDAP _____  | 77         |
| RADIUS _____  | 78         |
| <b>9: Services _____</b>                                  | <b>79</b>  |
| Date/Time _____   | 79         |
| Security _____  | 80         |
| HTTP Encryption _____                                     | 81         |
| Login Limitations _____                                   | 81         |
| KVM Encryption _____                                      | 82         |
| Group Based System Access Control _____                   | 82         |
| Authentication Limitation _____                           | 83         |
| Certificate _____   | 83         |
| Event Log _____   | 85         |
| Event Log Targets _____                                   | 85         |
| Event Log Assignments _____                               | 86         |
| SNMP _____  | 86         |
| KVM Search _____  | 88         |
| Power Management _____                                    | 89         |
| SpiderDuo Power Control Unit _____                        | 90         |
| Wake-On LAN _____   | 90         |
| Enable WOL _____  | 91         |
| Remove Entries, Reset to Defaults, or Reset _____         | 91         |
| <b>10: Maintenance _____</b>                              | <b>92</b>  |
| Device Status _____                                       | 92         |
| Configuration _____                                       | 93         |
| Update Firmware _____                                     | 94         |
| View Event Log _____                                      | 95         |
| Unit Reset _____  | 96         |
| iGoogle Gadgets _____                                     | 97         |
| <b>11: ManageLinx Integration and Configuration _____</b> | <b>100</b> |
| Upload a Bootstrap File With Spider _____                 | 100        |
| Upload a Bootstrap File With SpiderDuo _____              | 101        |
| <b>12: Command Reference _____</b>                        | <b>104</b> |
| Command Syntax _____                                      | 104        |
| Command Help _____  | 105        |
| Tips _____  | 105        |
| Configuration Commands _____                              | 105        |

---

|   |            |
|---|------------|
| Connect Commands                                  | 106        |
| VIP Commands                                      | 111        |
| User Group Commands                               | 113        |
| OEM Customization Commands                        | 116        |
| Power Commands                                    | 117        |
| Serial Port Commands                              | 117        |
| WOL (Wake on LAN) Commands                        | 118        |
| USB Host Disk Commands                            | 118        |
| Reboot Commands                                   | 119        |
| Diagnostic Commands                               | 119        |
| Group Permissions                                 | 119        |
| <b>A: Troubleshooting</b>                         | <b>121</b> |
| <b>B: Virtual Media Example</b>                   | <b>123</b> |
| Goal  | 123        |
| Step 1 – Prepare the VM Server                    | 123        |
| Step 2 – Enable Virtual Media                     | 124        |
| Step 3 – Use the Virtual Media                    | 126        |
| <b>C: Supported Resolutions and Refresh Rates</b> | <b>127</b> |
| <b>D: Mounting Bracket Kit</b>                    | <b>128</b> |
| <b>E: PCU Safety Information</b>                  | <b>130</b> |
| Cover   | 130        |
| Power Plug  | 130        |
| Input Supply                                      | 130        |
| Grounding   | 130        |
| Fuses   | 130        |
| <b>F: Technical Support</b>                       | <b>131</b> |
| Technical Support US                              | 131        |
| Technical Support Europe, Middle East, Africa     | 131        |
| <b>G: Compliance</b>                              | <b>132</b> |
| RoHS Notice                                       | 133        |

## List of Figures

|  |    |
|--|----|
| Figure 2-1 Spider System Configuration                               | 17 |
| Figure 2-2 Spider Cable Dimensions                                   | 17 |
| Figure 2-3 SpiderDuo System Configuration                            | 20 |
| Figure 2-4 SpiderDuo PS/2 Cable Dimensions                           | 21 |
| Figure 2-5 SpiderDuo USB Cable Dimensions                            | 21 |
| Figure 2-6 Spider Family Product Information Label                   | 23 |
| Figure 3-1 Spider RS-232 Serial Port and Pinouts                     | 25 |
| Figure 3-3 Spider Login Window                                       | 26 |
| Figure 3-4 Spider Prompts  | 26 |
| Figure 3-5 Spider RJ45 Ethernet and Cascade Ports                    | 27 |
| Figure 3-6 Lantronix Detector Window                                 | 27 |
| Figure 3-7 Detector Device List Window                               | 28 |
| Figure 3-8 Network Settings Window                                   | 28 |
| Figure 4-1 SpiderDuo RJ45 Port and Power Connector                   | 34 |
| Figure 4-2 SpiderDuo Local KVM, USB, Computer Input and Serial Ports | 34 |
| Figure 4-4 SpiderDuo Welcome Screen                                  | 35 |
| Figure 4-5 SpiderDuo Default IP Configuration Screen                 | 35 |
| Figure 4-6 Lantronix Detector Window                                 | 36 |
| Figure 4-7 Detector Device List Window                               | 37 |
| Figure 4-8 Network Settings Window                                   | 37 |
| Figure 4-10 PCU Layout and Dimensions                                | 41 |
| Figure 5-1 Spider Home Page  | 43 |
| Figure 6-1 Remote Console Window Components                          | 45 |
| Figure 6-2 Remote Console Window                                     | 47 |
| Figure 6-3 Remote Console Toolbar                                    | 47 |
| Figure 6-4 Login Screen  | 52 |
| Figure 7-1 Spider Network Settings Web Page                          | 54 |
| Figure 7-6 SpiderDuo Serial Port Settings Page                       | 56 |
| Figure 7-8 User Remote Console Settings Page                         | 58 |
| Figure 7-16 Keyboard/Mouse Settings                                  | 61 |
| Figure 7-23 Keyboard/Mouse Settings Page B                           | 64 |
| Figure 7-24 Miscellaneous Video Settings Page                        | 65 |
| Figure 7-25 Virtual Media Page                                       | 66 |
| Figure 7-30 Virtual Media Active Page                                | 68 |
| Figure 7-31 Virtual Media Active Image                               | 69 |
| Figure 7-32 Drive Redirection Window                                 | 70 |
| Figure 7-33 Drive Redirect Buttons                                   | 70 |
| Figure 7-34 Select Drive Redirect Window                             | 70 |
| Figure 7-35 Enable Write Support Window                              | 70 |
| Figure 7-36 Local Drive Browser Window                               | 71 |
| Figure 7-37 Drive Redirection Established Window                     | 71 |

---

|   |     |
|---|-----|
| Figure 7-38 User Interface Settings Page                | 71  |
| Figure 7-39 Configure VIP Page                          | 72  |
| Figure 7-40 Bootstrap Update Window                     | 72  |
| Figure 8-1 Change Password Page                         | 73  |
| Figure 8-2 Configure User Page                          | 74  |
| Figure 8-5 User Permissions Page                        | 76  |
| Figure 8-6 Authentication Page                          | 77  |
| Figure 9-1 Date/Time Settings Page                      | 79  |
| Figure 9-3 Security Settings Page                       | 81  |
| Figure 9-9 Certificate Signing Request Page             | 84  |
| Figure 9-11 Event Log Page                              | 85  |
| Figure 9-14 SNMP Settings Page                          | 87  |
| Figure 9-16 KVM Search Page                             | 89  |
| Figure 9-17 Power Management Page                       | 90  |
| Figure 10-1 Device Status Page                          | 92  |
| Figure 10-3 Configuration Page                          | 93  |
| Figure 10-5 Update Firmware Page                        | 95  |
| Figure 10-6 Event Log Page                              | 96  |
| Figure 10-7 Unit Reset Page                             | 97  |
| Figure 10-8 iGoogle Gadget Page                         | 99  |
| Figure 11-1 Spider VIP Page                             | 101 |
| Figure 11-2 Spider Bootstrap Update Screen              | 101 |
| Figure 11-3 SpiderDuo VIP Page                          | 102 |
| Figure 11-4 SpiderDuo Bootstrap Update Window           | 102 |
| Figure B - 1 Virtual Media                              | 123 |
| Figure B - 2 Windows Browser                            | 123 |
| Figure B - 3 Firewall Properties Window                 | 124 |
| Figure B - 4 Virtual Media Page                         | 125 |
| Figure B - 5 Virtual Media Active Image                 | 125 |
| Figure B - 6 Linux PC Window                            | 126 |
| Figure B - 7 Linux PC Window and USB CD                 | 126 |
| Figure D-1 Mounting Bracket and Screws                  | 128 |
| Figure D-2 Attaching the Mounting Bracket               | 128 |
| Figure D-3 Attaching the Device to the Mounting Bracket | 129 |
| Figure D-4 Connecting the Cables                        | 129 |

## List of Tables

|   |    |
|---|----|
| Table 1-1 Chapter/Appendix and Summary        | 13 |
| Table 1-2 Conventions Used in This Book       | 14 |
| Table 2-1 SpiderTechnical Specifications      | 18 |
| Table 2-2 SpiderDuo Technical Specifications  | 22 |
| Table 3-2 Spider LEDs                         | 26 |
| Table 4-3 SpiderDuo Indicator LEDs            | 34 |
| Table 4-9 Extended Length Cables              | 39 |
| Table 7-2 Network Basic Settings              | 54 |
| Table 7-3 LAN Interface Settings              | 55 |
| Table 7-4 IPv6 Settings                       | 55 |
| Table 7-5 Miscellaneous Network Settings      | 55 |
| Table 7-7 Serial Port Settings                | 56 |
| Table 7-9 KVM Console Settings                | 58 |
| Table 7-10 Transmission Encoding              | 59 |
| Table 7-11 KVM Console Type                   | 59 |
| Table 7-12 KVM Console Deployment             | 59 |
| Table 7-13 Miscellaneous KVM Console Settings | 59 |
| Table 7-14 Mouse Hotkey                       | 60 |
| Table 7-15 KVM Console Virtual Keys           | 60 |
| Table 7-17 Keyboard/Mouse Settings            | 61 |
| Table 7-18 Keyboard Model                     | 62 |
| Table 7-19 Key Release Timeout                | 62 |
| Table 7-20 Country Code                       | 62 |
| Table 7-21 USB Mouse Type                     | 62 |
| Table 7-22 Mouse Speed                        | 63 |
| Table 7-26 Virtual Media Active Image         | 66 |
| Table 7-27 Drive Redirection                  | 66 |
| Table 7-28 Virtual Media Options              | 67 |
| Table 7-29 Image on Windows Share             | 67 |
| Table 8-3 User Management                     | 74 |
| Table 8-4 Group Management                    | 75 |
| Table 8-7 Local Authentication                | 77 |
| Table 8-8 LDAP                                | 77 |
| Table 8-9 RADIUS                              | 78 |
| Table 9-2 Date/Time Settings                  | 80 |
| Table 9-4 HTTP Encryption                     | 81 |
| Table 9-5 Login Limitations                   | 81 |
| Table 9-6 KVM Encryption                      | 82 |
| Table 9-7 Group Based System Access Control   | 82 |
| Table 9-8 Authentication Limitation           | 83 |
| Table 9-10 SSL Server Certificate Management  | 84 |

|   |     |
|---|-----|
| Table 9-12 Event Log Targets _____                            | 85  |
| Table 9-13 Event Log Assignments _____                        | 86  |
| Table 9-15 SNMP Settings _____                                | 87  |
| Table 10-2 Device Status Settings _____                       | 92  |
| Table 10-4 Configuration Settings _____                       | 94  |
| Table 12-1 Action and Category _____                          | 104 |
| Table C-1 Supported Video Resolutions and Refresh Rates _____ | 127 |
| Table D-5 Lantronix Part Number and Description _____         | 129 |

# 1: About This Guide

This guide describes how to install, configure, use, and update the SecureLinx Spider and SpiderDuo 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:

- ◆ [Chapter and Appendix Summaries](#)
- ◆ [Conventions](#)
- ◆ [Additional Documentation](#)

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

## Chapter and Appendix Summaries

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

**Table 1-1** Chapter/Appendix and Summary

| Chapter/Appendix   | Summary  |
|--|--|
| <a href="#">2: Overview</a>                                  | Describes the Spider and SpiderDuo features and supported protocols.   |
| <a href="#">3: Installing the Spider</a>                     | Provides technical specifications; describes connection formats and power supplies.  |
| <a href="#">4: Installing the SpiderDuo</a>                  | Provides technical specifications; describes connection formats and power supplies.  |
| <a href="#">5: Web Browser Access</a>                        | Describes method to access the Web browser.  |
| <a href="#">6: Remote System Control</a>                     | Describes the remote system control.   |
| <a href="#">7: Interfaces</a>                                | Provides instructions for configuring network ports, firewall and routing settings, and date and time.   |
| <a href="#">8: User Accounts</a>                             | Provides instructions for configuring user accounts.   |
| <a href="#">9: Services</a>                                  | Provides instructions for configuring services, such as date and time, security settings, and certificates.  |
| <a href="#">10: Maintenance</a>                              | Provides instructions for upgrading firmware, viewing system logs and diagnostics, generating reports, and defining events. Includes information about web pages and commands used to shut down and reboot the Spider and SpiderDuo. |
| <a href="#">11: ManageLinx Integration and Configuration</a> | Provides instructions for configuring connections and viewing, updating, or disconnecting a connection.  |
| <a href="#">12: Command Reference</a>                        | Lists and describes all of the commands available on the Spider/SpiderDuo command line interface   |
| <a href="#">A: Troubleshooting</a>                           | Describes troubleshooting methods.   |

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

| Chapter/Appendix                                  | Summary   |
|---|---|
| <b>B: Virtual Media Example</b>                   | Gives examples of virtual media.  |
| <b>C: Supported Resolutions and Refresh Rates</b> | Lists the resolutions and refresh rates that are supported.                             |
| <b>D: Mounting Bracket Kit</b>                    | Describes how to mount the Spider/SpiderDuo in a rack.                                  |
| <b>E: PCU Safety Information</b>                  | Provides PCU safety information.  |
| <b>F: Technical Support</b>                       | Lists technical support telephone and fax numbers.                                      |
| <b>G: Compliance</b>                              | Provides information about the Spider and SpiderDuo 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  |
|-------------------------------------|--|
| <b>Bold text</b>                    | Default parameters.  |
| <b>Brackets [ ]</b>                 | Optional parameters.   |
| <b>Angle Brackets &lt; &gt;</b>     | Possible values for parameters.  |
| <b>Pipe  </b>                       | Choice of parameters.  |
| <b>Warning</b>                      | <b>Warning:</b> 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. |
| <b>Note</b>                         | <b>Note:</b> Notes contain helpful suggestions, information, or references to material not covered in the publication.   |
| <b>Caution</b>                      | <b>Caution:</b> You might do something that could result in faulty equipment operation, or loss of data.   |
| <b>Screen Font</b><br>(Courier New) | CLI terminal sessions and examples of CLI input.   |

## Additional Documentation

Visit the Lantronix web site at [www.lantronix.com/support/documentation](http://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.
- ◆ **SecureLinx Spider Quick Start Guide**—Provides an overview of using the Spider.
- ◆ **SecureLinx SpiderDuo Quick Start Guide**—Provides an overview of using the SpiderDuo.

## 2: Overview

SecureLinx Spider and SpiderDuo are distributed Keyboard, Video, and Mouse-over-IP (KVM)-over-IP devices 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 over a local or wide area network connection using a standard web browser.

Spider and/or SpiderDuo is an evolution of the traditional remote KVM switch 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 switches in several ways. Unlike rack mounted KVM-over-IP switches, the allocation of one Spider 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:

- ◆ [Spider Overview](#)
- ◆ [SpiderDuo Overview](#)
- ◆ [Product Information Label](#)

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

### Spider Overview

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

- ◆ [Features](#)
- ◆ [Functionality](#)
- ◆ [System Configuration and Cables](#)
- ◆ [Technical Specifications](#)

#### Features

The Spider is unique in that it is low-enough in power consumption to be powered from the attached server. The color-coded cable plugs for the keyboard, mouse, USB port and video are designed to plug directly into the target server. An optional external AC/DC power supply is available.

It uses Lantronix SwitchPort+ technology to incorporate two hardware-switched Ethernet ports, one for the primary network connection and the second for daisy-chaining Spiders, 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 comes in the following four models:

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

- ◆ One model with cable length of 58"
- ◆ 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
- ◆ Flexible 1-port design allows growth
- ◆ Guaranteed non-blocked access to remote servers that ensures lowest "cost-per-remote user"
- ◆ Browser-based, no client software or special licensing required
- ◆ Virtual Media support allows local drive (floppy, CD, hard drive, USB stick) sharing with a remote server or remote installation of an OS from an .ISO image
- ◆ 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 pass-through or remote dial-in access
- ◆ Ideal for distributed IT system environments such as small branch offices, campuses, test labs, and server hosting environments
- ◆ Server-powered design - no external power supply required
- ◆ Lantronix SwitchPort+ technology allows Spiders to be cascaded or share a host Ethernet connection

## Functionality

The Spider captures the video output from the attached computer, compresses and sends it over the network to a Java 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 also uses Java KVM coaxnsle 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.

**Note:** *The Spider supports up to 1600 x 1200 resolution at 60 Hz if its hardware revision is G22, G23, E21 or higher. If the Spider hardware is an earlier revision, it will only support resolutions up to 1280 x 1024 at 60 Hz. The hardware revision number can be found on the Product Information Label as shown in [Figure 2-6](#).*

## 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

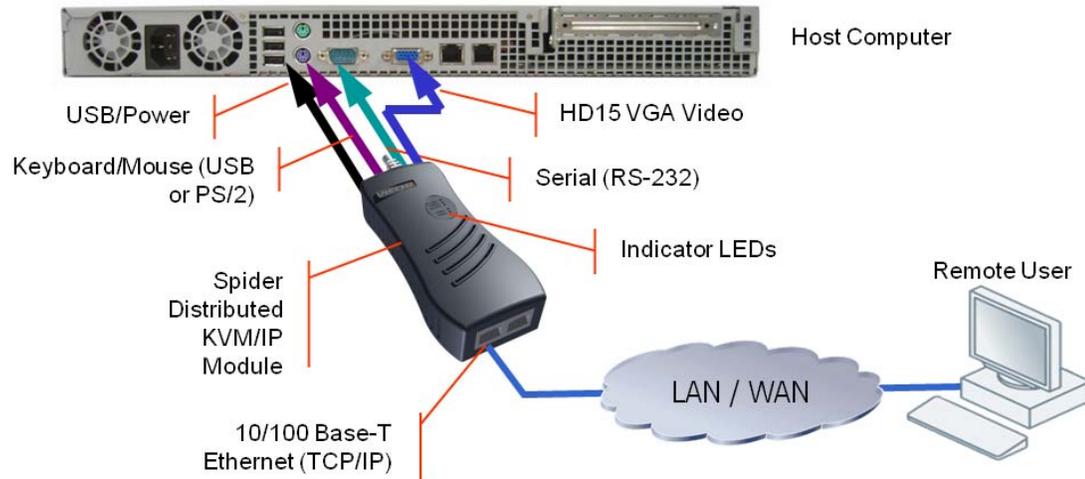
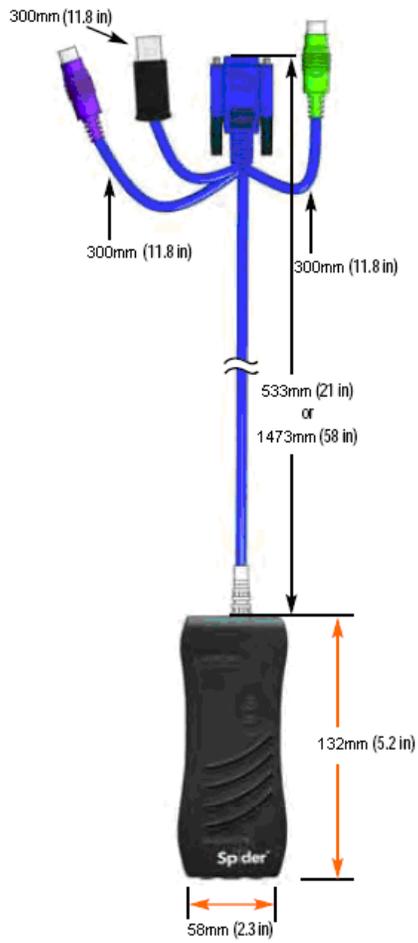


Figure 2-2 Spider Cable Dimensions



## Technical Specifications

Table 2-1 lists the components and general specifications.

Table 2-1 SpiderTechnical Specifications

| Component                  | Specification  |
|----------------------------|--|
| Security                   | <ul style="list-style-type: none"> <li>◆ IP Source Address Filtering</li> <li>◆ Remote Authentication: LDAP, RADIUS, Active Directory</li> <li>◆ User/Group management with permissions control</li> <li>◆ Configurable port numbers (HTTP, HTTPS, Telnet, SSH)</li> <li>◆ Selective disable of Telnet/SSH</li> <li>◆ Secure encryption of keyboard, mouse, and video data</li> <li>◆ AES used as cipher for SSH/SSL communications</li> </ul>   |
| Target Server Requirements | <ul style="list-style-type: none"> <li>◆ Multiple Operating Systems supported: Windows 98/2000/2003/XP/Vista, Unix, Linux, or MAC OSX 10</li> <li>◆ Power/keyboard/mouse: 2 USB ports; or 1 USB and 1 PS/2 keyboard and 1 PS/2 mouse connector</li> <li>◆ Video Interface: HD15 VGA video output</li> </ul> <p><i>Note: The Spider supports up to 1600 x 1200 resolution at 60 Hz if its hardware revision is G22, G23, E21 or higher. If the Spider hardware is an earlier revision, it will only support up to 1280 x 1024 resolution at 60 Hz. The hardware revision number can be found on the Product Information Label as shown in Figure 2-6.</i></p> |
| Client System Requirements | <ul style="list-style-type: none"> <li>◆ SUN Java Runtime Environment (JRE) 1.4 or later</li> </ul>  |
| Optional Items             | <ul style="list-style-type: none"> <li>◆ Replacement mounting bracket kit (see <a href="#">D: Mounting Bracket Kit</a>)</li> <li>◆ Optional DC power supply with international adapters (100-240VAC, 50-60 Hz; 5 VDC @ 1A; USB "Mini-B" Type jack)</li> </ul>  |
| Interfaces                 | <ul style="list-style-type: none"> <li>◆ Network: One 10/100Base-T Ethernet Port with activity indicators (RJ45)</li> <li>◆ Cascade: One 10/100Base-T Ethernet Port with activity indicators (RJ45)</li> <li>◆ Serial: RS-232, up to 115,200 bps</li> <li>◆ Keyboard/Mouse: PS/2 or USB</li> <li>◆ Video: HD15 VGA</li> </ul>  |
| Power Requirements         | <ul style="list-style-type: none"> <li>◆ Input: 5 VDC @ .8A max. (server powered)</li> <li>◆ Optional Auxiliary DC power supply available for redundancy</li> </ul>  |
| Environmental              | <ul style="list-style-type: none"> <li>◆ Operating: 0° to 45° C (32° to 115° F)</li> <li>◆ Storage: -20° to 70° C (-4° to 158° F)</li> <li>◆ Humidity: 0 to 95% RH (non-condensing)</li> <li>◆ Heat Dissipation: 4 Watts (14 BTU/hr)</li> </ul>  |
| Dimensions (H x W x D)     | <ul style="list-style-type: none"> <li>◆ 13.2 x 5.8 x 3.1 cm (5.2 x 2.3 x 1.2 in) (See <a href="#">Figure 2-2</a> for cable dimensions.)</li> </ul>  |

Table 2-1 SpiderTechnical Specifications (continued)

| Component       | Specification     |
|-----------------|-------------------|
| 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 reboots over the network. SpiderDuo allows complete local, plus remote management of the host machine anytime, from virtually anywhere.

It has one model with both PS/2 and USB keyboard and mouse interfaces (software selectable), and one model for USB-only systems. It has the following 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
- ◆ Flexible 1-port design allows growth
- ◆ Guaranteed non-blocked access to remote servers that ensures lowest “cost-per-remote user”
- ◆ Browser-based, no client software or special licensing required
- ◆ Virtual Media support allows local drive (floppy, CD, hard drive, USB stick) sharing with a remote server or remote installation of an OS from an .ISO image
- ◆ 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 pass-through or remote dial-in 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 Java 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 Java 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 2-3 shows an SpiderDuo system configuration, Figure 2-4 shows the PS/2 cable dimensions, and Figure 2-5 shows the USB cable dimensions.

Figure 2-3 SpiderDuo System Configuration

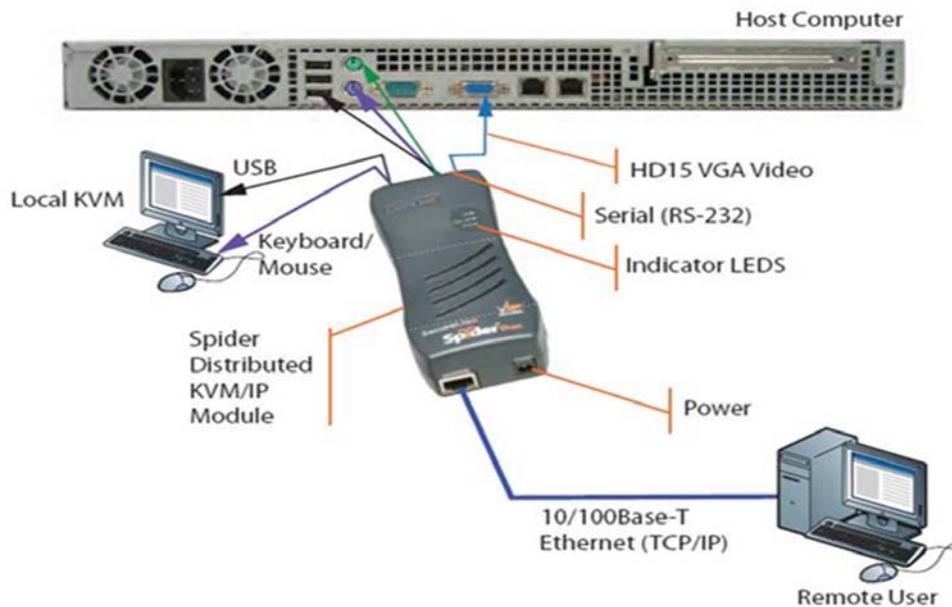


Figure 2-4 shows the PS/2 cable dimensions.

**Figure 2-4 SpiderDuo PS/2 Cable Dimensions**

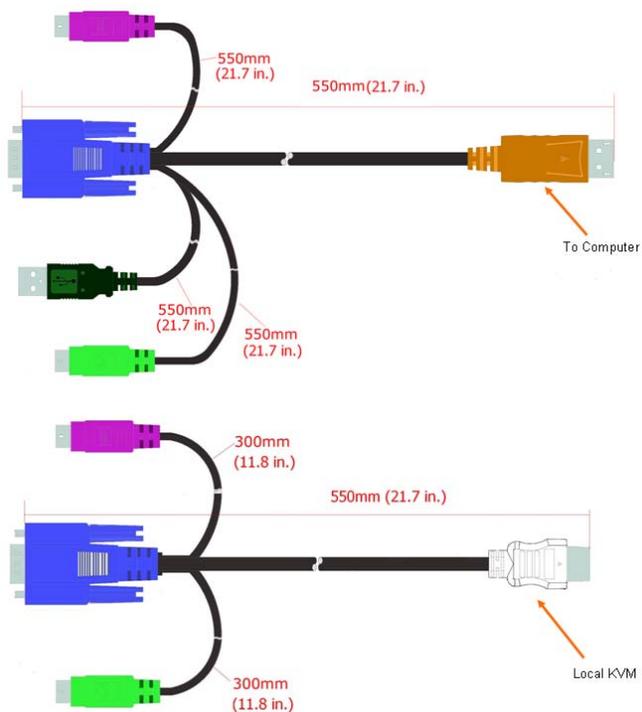
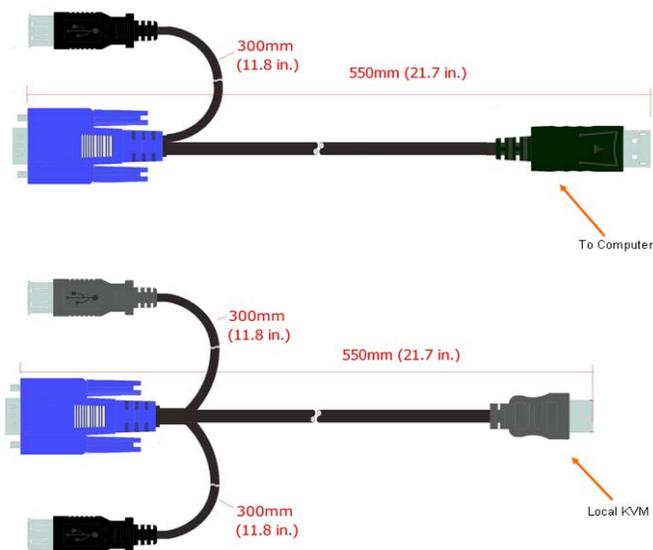


Figure 2-5 shows the USB cable dimension.

**Figure 2-5 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 2-2 lists the general components and the specifications.

Table 2-2 SpiderDuo Technical Specifications

| Component                         | Specification  |
|-----------------------------------|--|
| <b>Security</b>                   | <ul style="list-style-type: none"> <li>◆ Hardware based encryption of keyboard, mouse and video data</li> <li>◆ IP Source Address Filtering</li> <li>◆ Remote Authentication: LDAP, RADIUS, Active Directory</li> <li>◆ User/Group management with permissions control</li> <li>◆ Configurable port numbers (HTTP, HTTPS, Telnet, SSH)</li> <li>◆ Selective disable of Telnet/SSH</li> </ul> |
| <b>Target Server Requirements</b> | <ul style="list-style-type: none"> <li>◆ Multiple Operating Systems supported: Windows 98/2000/2003/XP/Vista, Unix, Linux, or MAC OSX 10</li> <li>◆ Power/keyboard/mouse: 2 USB ports; or 1 USB and 1 PS/2 keyboard and 1 PS/2 mouse connector</li> <li>◆ Video Interface: HD15 VGA video output (up to 1600 x 1200 at 60Hz)</li> </ul>  |
| <b>Client System Requirements</b> | <ul style="list-style-type: none"> <li>◆ Internet Explorer 6.0+, Netscape 5.0+, Mozilla FireFox 1.0+, Safari 2.0+</li> <li>◆ PIII Processor equivalent or better (recommended)</li> <li>◆ Sun Java 2 Runtime Environment</li> <li>◆ Telnet/SSH client for command line (CLI) access</li> </ul>   |
| <b>Optional Items</b>             | <ul style="list-style-type: none"> <li>◆ Replacement mounting bracket kit (See <a href="#">D: Mounting Bracket Kit.</a>)</li> <li>◆ PS/2 extended length cable: 1500mm, (59 in.) part number 500-199-R</li> <li>◆ USB extended length cable: 1500mm, (59 in.) part number 500-200-R</li> </ul>   |
| <b>Interfaces</b>                 | <ul style="list-style-type: none"> <li>◆ Network: 10/100Base-T Ethernet Port with activity indicators (RJ45)</li> <li>◆ Serial: RS-232, up to 115,200 bps for serial device pass-through, unit configuration or PCU controller</li> <li>◆ USB</li> <li>◆ Local KVM connector</li> <li>◆ Computer input connector</li> </ul>  |
| <b>Environmental</b>              | <ul style="list-style-type: none"> <li>◆ Operating: 0° to 45° C (32° to 115° F)</li> <li>◆ Storage: -20° to 70° C (-4° to 158° F)</li> <li>◆ Humidity: 0 to 95% RH (non-condensing)</li> <li>◆ Heat Dissipation: 4 Watts (14 BTU/hr)</li> </ul>  |
| <b>Power Requirements</b>         | <ul style="list-style-type: none"> <li>◆ Input 5VDC 2A Wall Adaptor, part number 520-104-R.</li> </ul>   |
| <b>Dimensions (H x W x D)</b>     | <ul style="list-style-type: none"> <li>◆ 13.2 x 5.8 x 3.6 cm (5.2 x 2.3 x 1.4 in) (See <a href="#">Figure 2-4</a> (PS/2) and <a href="#">Figure 2-5</a> (USB) for cable dimensions.)</li> </ul>  |

Table 2-2 SpiderDuo Technical Specifications (continued)

| Component       | Specification          |
|-----------------|------------------------|
| 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:

- ◆ Bar code
- ◆ Serial number
- ◆ Revision number
- ◆ Hardware address (also known as the Ethernet or MAC address)
- ◆ Manufacturing code

Figure 2-6 shows the Product Information Label.

Figure 2-6 Spider Family Product Information Label



## 3: Installing the Spider

This chapter describes how to install the Spider. It contains the following sections:

- ◆ [Package Contents](#)
- ◆ [Installing the Spider](#)
- ◆ [Detector Installation and IP Address Reset](#)
- ◆ [Target Computer Setup](#)
- ◆ [Client Server Setup](#)
- ◆ [Network Environment](#)
- ◆ [Spider Power](#)

For technical specifications of the Spider, see [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 [D: Mounting Bracket Kit](#))
- ◆ *Quick Start Guide*

**Note:** *An optional external AC/DC power supply is available.*

### Installing the Spider

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

- ◆ **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 Ports**—Performs the initial configuration to setup parameters and connects to a target COM port. It also allows remote users to Telnet or SSH to that port, eliminating the need for a separate box to perform serial command line management. The serial port can be used for PPP connections to the user interface so that remote users can use a modem or other serial interface. It can be the primary network connection or a backup connection in case the primary LAN connection is unavailable.
- ◆ **Optional Auxiliary DC Power Supply (Redundancy)**—Overcomes the loss of power when the attached server goes down by using the auxiliary DC power supply connected to an independent AC power source. The Spider will always have power regardless of the state of the server.
- ◆ **Ethernet Ports**—Connects to the LAN. The Spider 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 has its own IP address on the network. Because the Spider 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 in a chain. But, if the network switch that connects to the Spider 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 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 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 with its IP address or write it on the serial number label on the bottom.

Perform the following steps to install the Spider 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       | DTR (out) |
| 3       | TX (out)  |
| 4       | GND       |
| 5       | GND       |
| 6       | RX (in)   |
| 7       | DSR (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.
3. Plug the Spider video, USB, and PS/2 keyboard and mouse cables into the target computer. The Spider boots.

- The Pwr2 LED illuminates blue and the SysOK LED flashes green to indicate that the Spider is booting. Bootup should complete within one minute. The SysOK LED stops flashing and remains illuminated. If you use the external power supply to boot, Pwr1 illuminates blue. lists the LED labels, colors, and actions.

Table 3-2 Spider LEDs

| Label   | Color  | Action  |
|---------|--------|---|
| Pwr1    | Blue   | Indicates adequate power from USB1 (external power supply first). |
| Pwr2    | Blue   | Indicates adequate power from USB2 or PS/2.                       |
| SysOK   | Green  | Blinks upon bootup. Steady when up and healthy.                   |
| Video   | Green  | Indicates that video (VSync) transmitting from server.            |
| Unit ID | Orange | Indicates, when lit, to assist in finding unit.                   |

- When the bootup process completes, the terminal window displays the login prompt as shown in [Figure 3-3](#).

Figure 3-3 Spider Login Window

```

Welcome!
Choose a login for the following features:
-Initial IP configuration: "config".
-Reset device: "reset".
<none> login: config
IP autoconfiguration <none/dhcp/bootp> [dhcp]: none

```

- To change the default IP auto configuration from DHCP to a static IP address, type `config` and press Enter.
- At the IP autoconfiguration prompt, type `none` and press Enter.
- Follow the prompts to enter the IP address, subnet mask, default gateway, and LAN interface information as shown in [Figure 3-4](#).

Figure 3-4 Spider Prompts

```

IP [192.168.1.22]:
NetMask [255.255.255.0]:
Gateway <0.0.0.0 for none> [0.0.0.0]:
LAN interface speed <auto/10/100> [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.

```

- Type `y` and press Enter to accept the changes. The system takes several seconds to update the internal protocol stack and display the updated information. See [Detector Installation and IP Address Reset on page 27](#) for more information about using Detector.
- Plug an Ethernet cable connected to your network into the Ethernet port. The Lnk LED in the RJ45 illuminates. The RJ45 jack is shown in [Figure 3-5](#).

Figure 3-5 Spider RJ45 Ethernet and Cascade Ports



## Detector Installation and IP Address Reset

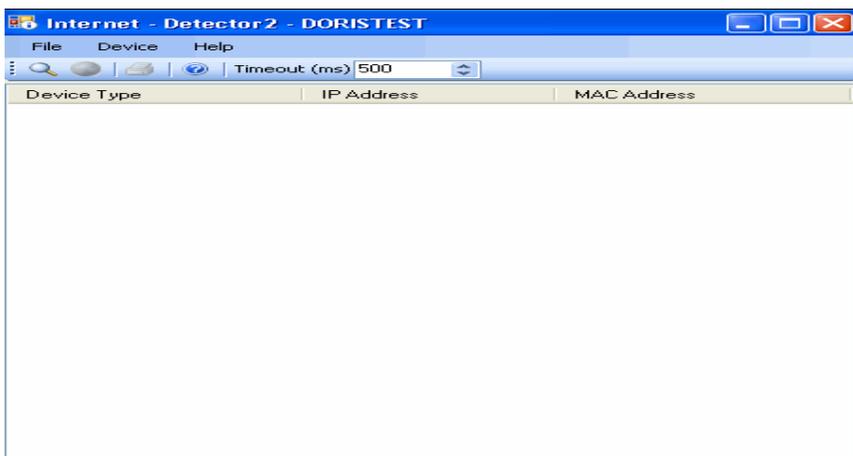
The initial IP address gets assigned during bootup of the Spider. To change it, use the Detector application. You can download Detector from Lantronix at <http://www.lantronix.com/support/downloads.html>.

**Note:** Lantronix recommends that you run Detector from its CD or copy it to your local hard drive and run it from there rather than from a shared network drive. Otherwise you may get a security exception. If you must run the program from a shared network drive, you need to change your security settings using the .NET Framework Configuration or “caspol” tool.

Perform the following steps to install Detector.

1. Double-click detector2.exe on its CD. If you see this error message: “The application failed to initialize properly (0xc0000135),” click **OK** to terminate the application and install .NET Framework. Go to Step 2.
2. Copy the .NET Framework application from the Spider CD or go to Microsoft and download the stand-alone executable file, **Dotnetfx.exe**. The file is at <http://www.microsoft.com/downloads/details.aspx?FamilyID=0856EACB-4362-4B0D-8EDD-AAB15C5E04F5&displaylang=en>.
3. Double-click detector2.exe again on its CD. Detector gets installed successfully.
4. Open the Detector software. The Lantronix Detector window opens as shown in Figure 3-6.

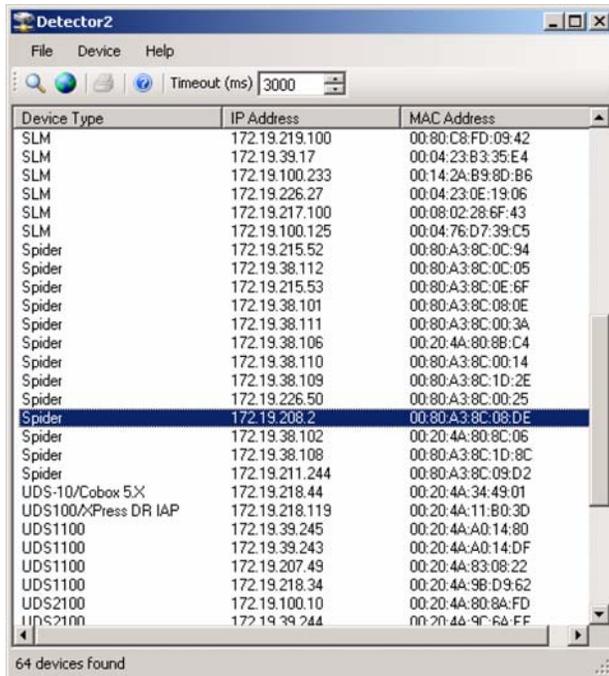
Figure 3-6 Lantronix Detector Window



5. Before searching for devices, go to the Timeout drop-down menu in the toolbar. Change the milliseconds for the search by clicking the number in the Timeout drop-down menu. The default is **3000**.

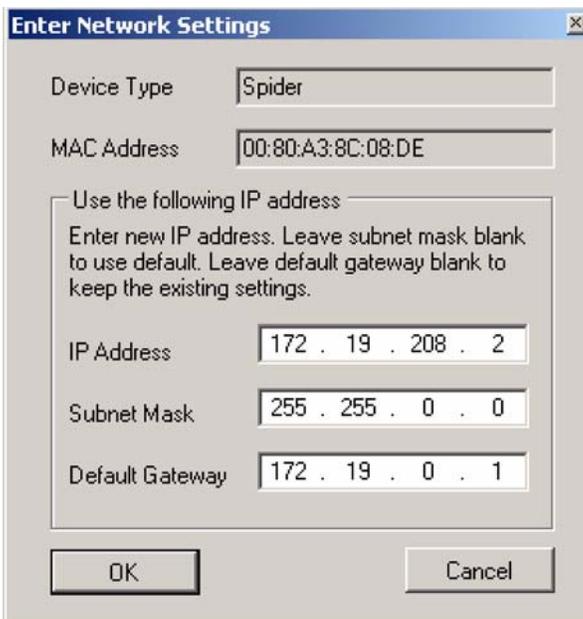
6. Click the **Search** icon . A list of Lantronix Ethernet devices on the network displays as shown in [Figure 3-7](#).

**Figure 3-7** Detector Device List Window



7. Click to highlight the device that you want and click the **Network Settings** icon  to change the IP address. The **Enter Network Settings** window displays the Device Type and MAC Address (Ethernet address) that identifies the device as shown in [Figure 3-8](#).

**Figure 3-8** Network Settings Window



8. Enter an unique and valid IP Address on your network and in the same subnet as your PC. There is no default.
9. Enter the subnet mask that is the network segment connected to the Spider. To accept the default, leave blank.
10. Enter the default gateway that is the router IP address for your network. To accept the default, leave blank.
11. Click **OK**. A message confirms the network configuration.
12. Click **OK**.
13. Confirm the IP address change by clicking the **Search icon** . Find the device in this list and verify the IP address. You can access the device by using its new IP address.

**Note:** On the *Interfaces Network page* of the web interface, make sure *Disable Setup Protocol* is not selected in the *Network Miscellaneous Settings* section.

## 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 sync'd properly; that the Telnet/SSH connections match the Spider; 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 recognizes video resolutions on the target computer up to a maximum of 1600 x 1200 at 60 Hz if its hardware revision G22, G23, E21 or higher. If the Spider hardware is an earlier revision, it will only support up to 1280 x 1024 resolution at 60 Hz. For the complete list of supported video resolutions and refresh rates, see [C: Supported Resolutions and Refresh Rates on page 127](#).

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

## Telnet/SSH Connections to Serial Ports

To Telnet/SSH to a target computer serial port, you must Telnet/SSH to the Spider serial port first and use `connect serial` CLI. This connects your Spider to the target computer serial port. 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. Do not use extension cables. Plug the Spider 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 to the target computer management LAN port, or to a main LAN port, or to an Spider chain. When connecting the Ethernet ports, straight through or crossover cables can be used, because the Spider 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 if using only one Ethernet interface.

Perform the following steps when daisy chaining Spider devices.

1. Plug the outside network cable into the left Ethernet port of the first Spider.
2. Connect the right Cascade port to the left port of the next Spider in the chain.
3. Repeat as necessary. The last Spider 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 Spider chain attaches. Then, connect the last Spider 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 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: platform-dependent management and platform-independent management.

- ◆ Platform-dependent management—Spider View is a standalone Windows XP or later application that locates, manages, and accesses multiple Spider devices in an integrated view. Spider View requires ActiveX controls enabled. Refer to the *Spider View User Guide* at <http://www.lantronix.com/support/documentation.html> for instructions on installation and operation of Spider View .
- ◆ Platform-independent management—Each Spider contains an embedded web server that delivers web pages, a Java KVM Remote Console program, and a terminal program. To access and manage the client server, a web browser is required. For example, use the latest version of Internet Explorer, Netscape, FireFox, and Safari. To run the Remote Console window and manage the target server, a Java plug-in (SUN JRE 1.4 or later) is required.

## Network Environment

The connection between the client and Spider must be open to IP traffic and use TCP ports 80 (HTTP) and 443 (HTTPS). Firewalls and NAT devices should be configured to support this configuration. The TCP ports can be changed by accessing **Interfaces > Network**.

When idle, minimal network traffic gets generated. Traffic bursts exceeding 10 Mbps can occur if images change rapidly on the host server and image quality gets set to the maximum. 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 consumes under 4 watts of power that it draws from the attached computer. It requires all cables to be plugged in to receive sufficient power.

Plug in both USB cables or a USB and a PS/2 cable. Pwr1 and Pwr2 LEDs indicate that power is available. Pwr1 indicates that power is available only on the first USB port. Pwr2 indicates that power is available on the second USB port or the PS/2 port. When both LEDs are lit, the Spider is powered and can boot.

The Spider can also get power from an external DC power supply. DC power supplies are available from Lantronix (part number 520-085-R). The DC power supply acts as a backup, because the Spider loses power when the attached computer goes down.

Use the power-on reset to reboot the Spider 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

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

- ◆ [Package Contents](#)
- ◆ [Installing the SpiderDuo](#)
- ◆ [Detector Installation and IP Address Reset](#)
- ◆ [Target Computer Setup](#)
- ◆ [Client Server Setup](#)
- ◆ [Network Environment](#)
- ◆ [PCU Power](#)

For technical specifications of the SpiderDuo, see [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 [D:Mounting Bracket Kit](#))
- ◆ *Quick Start Guide*
- ◆ CD-ROM containing documentation and utilities
- ◆ External AC/DC Power Supply
- ◆ Optional power control unit (PCU100-01)

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

### Installing the SpiderDuo

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

- ◆ **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 Ports**—Performs the initial configuration to setup parameters and connects to a target COM port. It also allows remote users to Telnet or SSH to that port, eliminating the need for a separate box to perform serial command line management. 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 41](#).

- ◆ Optional Auxiliary DC Power Supply (Redundancy)—Overcomes the loss of power when the attached server goes down by using the auxiliary DC power supply connected to an independent AC power source.
- ◆ Ethernet Ports—Connects to the LAN. The SpiderDuo 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 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 the power adaptor into the SpiderDuo power connector.

**Figure 4-1 SpiderDuo RJ45 Port and Power Connector**



4. Plug the SpiderDuo video, USB, and PS/2 keyboard and mouse (if applicable) cables into the target computer. The blue LED SysOK illuminates and flashes to indicate that the SpiderDuo 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.

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



**Table 4-3 SpiderDuo Indicator LEDs**

| Label | Color | Action  |
|-------|-------|---|
| ID    | Amber | On - Unit ID Selected<br>Blinking -Thumb-drive Configuration Successful |

Table 4-3 SpiderDuo Indicator LEDs (continued)

| Label | Color | Action   |
|-------|-------|--|
| SysOK | Blue  | On - Powered up and OK<br>Blinking - Booting           |
| PCU   | Green | On - Power Unit Connected , AC power is passed through |

- Upon bootup, the terminal window displays the **IP Configuration** screen. At the command prompt type **config** and press **Enter**.

Figure 4-4 SpiderDuo Welcome Screen

```
Welcome!
Choose a command for the following features:
-Initial IP configuration: "config".
-Reset device: "reset".
[172.19.205.165 spider]> _
```

- To change the default IP auto configuration from DHCP to a static IP address, at the **IP autoconfiguration** prompt type **none** and press **Enter**.

Figure 4-5 SpiderDuo Default IP Configuration Screen

```
IP autoconfiguration (none/dhcp/bootp) [none]: none
IP [172.19.205.165]: 172.19.208.30
NetMask [255.255.0.0]:
Gateway (0.0.0.0 for none) [172.19.0.1]:
LAN interface speed (auto/10/100) [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 ...
```

- Follow the prompts to enter the IP address, subnet mask, default gateway, and LAN interface information.
- Type **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.
- Plug an Ethernet cable connected to your network into the Ethernet port. The Link LED illuminates.

**Note:** To reboot or reset the SpiderDuo, press the reset switch through the pinhole on the bottom of the device. You can also use the user interface or serial port.

- Test the system installation (PC, local keyboard and mouse, video, and SpiderDuo) by completing the following:
  - Turn off the power to the PC and SpiderDuo.
  - Reconnect all devices.
  - Turn on the SpiderDuo first, and wait for it to boot completely (the SysOK LED will be on steady).
  - Turn on the PC.

## Detector Installation and IP Address Reset

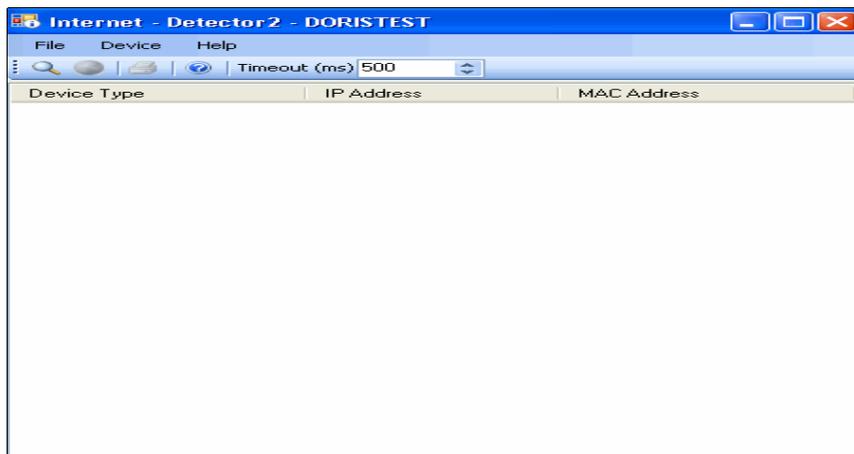
The initial IP address gets assigned during bootup of the SpiderDuo. To change it, use the Detector application. You can download Detector from Lantronix at <http://www.lantronix.com/support/downloads.html>.

**Note:** Lantronix recommends that you run Detector from its CD or copy it to your local hard drive and run it from there rather than from a shared network drive. Otherwise you may get a security exception. If you must run the program from a shared network drive, you need to change your security settings using the .NET Framework Configuration or “caspol” tool.

Perform the following steps to install Detector.

1. Double-click detector2.exe on its CD. If you see this error message: "The application failed to initialize properly (0xc0000135)," click **OK** to terminate the application and install .NET Framework. Go to Step 2.
2. Copy the .NET Framework application from the Spider CD or go to Microsoft and download the stand-alone executable file, **Dotnetfx.exe**. The file is at <http://www.microsoft.com/downloads/details.aspx?FamilyID=0856EACB-4362-4B0D-8EDD-AAB15C5E04F5&displaylang=en>.
3. Double-click detector2.exe again on its CD. Detector gets installed successfully.
4. Open the Detector software. The Lantronix Detector window opens as shown in [Figure 4-6](#).

**Figure 4-6** Lantronix Detector Window



5. Before searching for devices, go to the Timeout drop-down menu in the toolbar. Change the milliseconds for the search by clicking the number in the Timeout drop-down menu. The default is **3000**.
6. Click the **Search** icon . A list of Lantronix Ethernet devices on the network displays as shown in [Figure 4-7](#).

Figure 4-7 Detector Device List Window

| Device Type          | IP Address     | MAC Address       |
|----------------------|----------------|-------------------|
| SLM                  | 172.19.219.100 | 00:80:C8:FD:09:42 |
| SLM                  | 172.19.39.17   | 00:04:23:83:35:E4 |
| SLM                  | 172.19.100.233 | 00:14:2A:B9:8D:B6 |
| SLM                  | 172.19.226.27  | 00:04:23:0E:19:06 |
| SLM                  | 172.19.217.100 | 00:08:02:28:6F:43 |
| SLM                  | 172.19.100.125 | 00:04:76:D7:39:C5 |
| Spider               | 172.19.215.52  | 00:80:A3:8C:0C:94 |
| Spider               | 172.19.38.112  | 00:80:A3:8C:0C:05 |
| Spider               | 172.19.215.53  | 00:80:A3:8C:0E:6F |
| Spider               | 172.19.38.101  | 00:80:A3:8C:08:0E |
| Spider               | 172.19.38.111  | 00:80:A3:8C:00:3A |
| Spider               | 172.19.38.106  | 00:20:4A:80:88:C4 |
| Spider               | 172.19.38.110  | 00:80:A3:8C:00:14 |
| Spider               | 172.19.38.109  | 00:80:A3:8C:1D:2E |
| Spider               | 172.19.226.50  | 00:80:A3:8C:00:25 |
| Spider               | 172.19.208.2   | 00:80:A3:8C:08:DE |
| Spider               | 172.19.38.102  | 00:20:4A:80:8C:06 |
| Spider               | 172.19.38.108  | 00:80:A3:8C:1D:8C |
| Spider               | 172.19.211.244 | 00:80:A3:8C:09:D2 |
| UDS-10/Cobox 5X      | 172.19.218.44  | 00:20:4A:34:49:01 |
| UDS100/XPRESS DR IAP | 172.19.218.119 | 00:20:4A:11:80:3D |
| UDS1100              | 172.19.39.245  | 00:20:4A:A0:14:80 |
| UDS1100              | 172.19.39.243  | 00:20:4A:A0:14:DF |
| UDS1100              | 172.19.207.49  | 00:20:4A:83:08:22 |
| UDS1100              | 172.19.218.34  | 00:20:4A:9B:D9:62 |
| UDS2100              | 172.19.100.10  | 00:20:4A:80:8A:FD |
| UDS2100              | 172.19.39.244  | 00:20:4A:9C:FA:FF |

64 devices found

- Click to highlight the device that you want and click the **Network Settings** icon  to change the IP address. The **Enter Network Settings** window displays the Device Type and MAC Address (Ethernet address) that identify the device as shown in [Figure 4-8](#).

Figure 4-8 Network Settings Window

Enter Network Settings

Device Type: Spider

MAC Address: 00:80:A3:8C:08:DE

Use the following IP address

Enter new IP address. Leave subnet mask blank to use default. Leave default gateway blank to keep the existing settings.

IP Address: 172 . 19 . 208 . 2

Subnet Mask: 255 . 255 . 0 . 0

Default Gateway: 172 . 19 . 0 . 1

OK Cancel

- Enter an unique and valid IP Address on your network and in the same subnet as your PC. There is no default.
- Enter the subnet mask that is the network segment connected to the Spider. To accept the default, leave blank.

10. Enter the default gateway that is the router IP address for your network. To accept the default, leave blank.
11. Click **OK**. A message confirms the network configuration.
12. Click **OK**.
13. Confirm the IP address change by clicking the **Search icon** . Find the device in this list and verify the IP address. You can access the device by using its new IP address.

**Note:** On the *Interfaces Network page of the web interface*, make sure *Disable Setup Protocol* is not selected in the *Network Miscellaneous Settings section*.

## 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 sync'd properly; that the Telnet/SSH connections match the Spider; 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 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 [C: Supported Resolutions and Refresh Rates on page 127](#).

**Note:** *The other supported resolutions and refresh rates are recognized by the SpiderDuo, 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 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 Telnet/SSH to a target computer serial port, you must Telnet/SSH to the SpiderDuo serial port first and use `connect serial` CLI. This connects your SpiderDuo to the target computer serial port. 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. Plug the SpiderDuo 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 4-9](#).

**Table 4-9** *Extended Length Cables*

| Item                                       | Part Number |
|--|-------------|
| USB connector; 1500 mm, (59 in.) VGA cable | 500-199-R   |

**Table 4-9 Extended Length Cables**

|  |           |
|--|-----------|
| PS/2 and USB connectors; 1500 mm, (59 in.) VGA cable | 500-200-R |
|--|-----------|

## Power Sequencing

To ensure that the system (PC, local keyboard and mouse, and SpiderDuo) function properly at power up, it is recommended that the following procedure be performed.

1. Ensure that the PC 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 PC.

## Client Server Setup

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

- ◆ Platform-dependent management—Spider View is a standalone Windows XP or later application that locates, manages, and accesses multiple Spider devices in an integrated view. Spider View requires ActiveX controls enabled. Refer to the *Spider View User Guide* at <http://www.lantronix.com/support/documentation.html> for instructions on installation and operation of Spider View .
- ◆ Platform-independent management—Each Spider contains an embedded web server that delivers web pages, a Java KVM Remote Console program, and a terminal program. To access and manage the client server, the latest web browser is required. For example, Internet Explorer, Netscape, FireFox, and Safari. To run the Remote Console window and manage the target server, a Java plug-in (SUN JRE 1.4 or later) is required.

## Network Environment

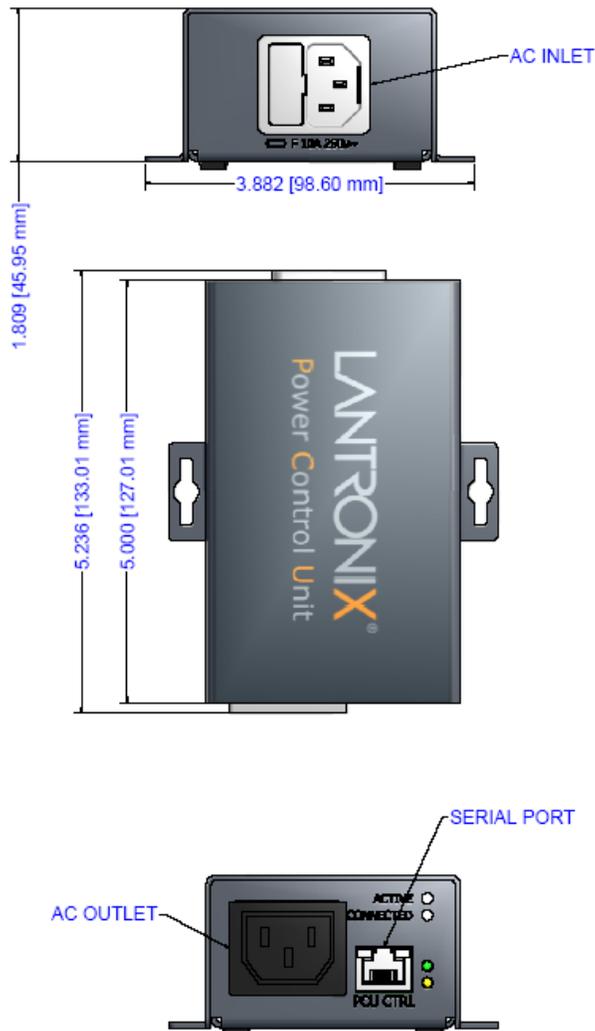
The connection between the client and SpiderDuo must be open to IP traffic and use TCP ports 80 (HTTP) and 443 (HTTPS). Firewalls and NAT devices should be configured to support this configuration. The TCP ports can be changed by accessing **Interfaces > Network**.

When idle, minimal network traffic gets generated. Traffic bursts exceeding 10 Mbps can occur if images change rapidly on the host server and image quality gets set to the maximum. Lantronix recommends using Fast Ethernet connections and a switched network environment because in a LAN, traffic affects the responsiveness of the Remote Console window.

## 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. shows the layout and dimensions of the PCU.

**Figure 4-10 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 gets its power from an external DC supply. Replacement power supplies are available.

## 5: Web Browser Access

This chapter describes how to use the SecureLinx Spider and SpiderDuo devices to access and manage a target computer by using a Web browser or remote system. It contains the following section:

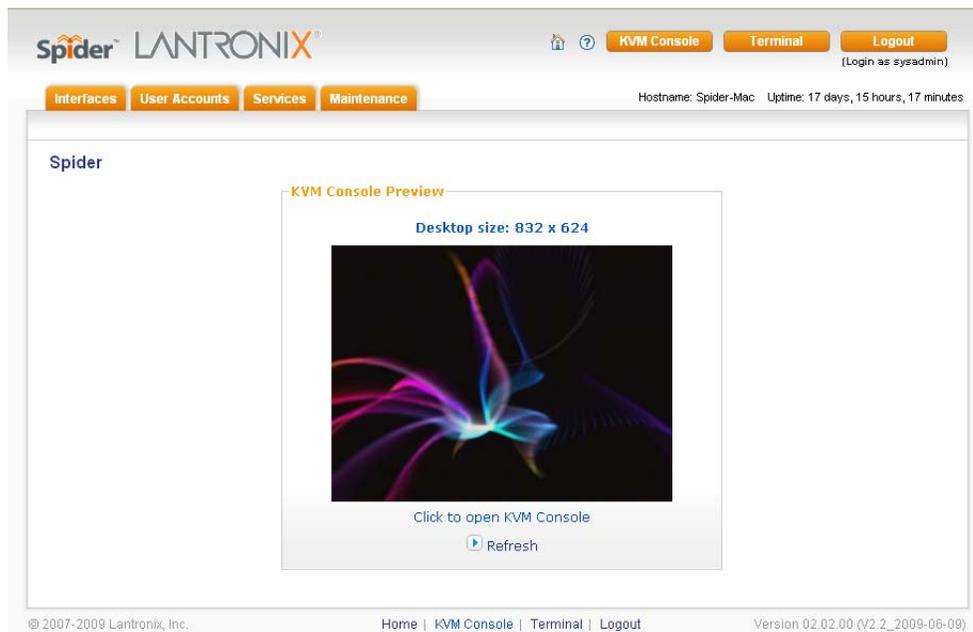
- ◆ [Accessing the KVM Console](#)

### Accessing the KVM Console

Perform the following steps to use a web browser.

1. Access the Spider or SpiderDuo over the network by using a web browser by entering `https://<ipaddress>` (for a secure SSL connection) or `http://<ipaddress>` (for an unsecure 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 Console or Telnet Console can be launched as shown in [Figure 5-1](#).

**Figure 5-1** Spider 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
- ◆ Remote Console Window
- ◆ Basic Remote Console Operation
- ◆ Optimizing Video
- ◆ Keyboard Functions
- ◆ Other Remote Console Functions
- ◆ Telnet/SSH

### Overview

The SecureLinux Spider and SpiderDuo 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 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 to bypass the web page and take you directly to the remote system by clicking **Services > Security > Authentication Limitation > Enable Direct KVM**. This capability is called Direct KVM.

Figure 6-1 Remote Console Window Components



## Main Viewport and Scroll Bars

When first launched, the full virtual screen of the target computer is mapped pixel-for-pixel to the console window main viewport. As a result, if the target is running at a resolution less than that of the client, the entire screen is visible in the Remote Console window. If the resolution is such that the screen does not fit, scroll bars are available in the Remote Console window to move the viewport around within the target's screen. The virtual screen size of the target may also be scaled down to match the Remote Console window.

## Button Keys

Along the top there are Button Keys that have been defined to send special key codes directly to the target computer.

## Toolbar

The top 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.

- ◆ Access Virtual Media—The leftmost diskette icon is used to activate the Virtual Media toolbar.
- ◆ Auto Adjust Video—This button activates the Auto Adjust Video function. When first opening the Remote Console window, it is recommended to click this button to ensure the Spider has locked on to the video format on the attached computer. Also, click this button if there is an offset from the proper horizontal or vertical start position relative to the target screen (black bars to the right, left, top, or bottom of the main viewport, or a distorted video).
- ◆ Screen Display Adjustments—These 3 buttons (A,S,R) facilitate changes to the Screen display

- ◆ Sync Mouse, Single/Double Cursor—These icons appear when the PS/2 mouse interface is active.

## Options

The drop-down menu provides access to a number of options and features.

### Information Bar - Connection

The left side of the information bar indicates whether the connection is encrypted (**Console (SSL)**) or unencrypted (**Console (Norm)**).

### Information Bar - Resolution

Displays the horizontal by vertical resolution of the target system's video.

### Information Bar - Network Traffic

Displays the approximate number of bytes per second incoming and outgoing to the window. An indication of the number of frames per second (fps) updated is also displayed. Incoming data is generally comprised of video updates. Outgoing data is generally comprised of keystrokes and mouse movements. When the target screen is not changing, **In** should be low or zero. If not, click the auto-adjust button. The amount of network traffic is a function of the detail in the captured screen, the rate at which the screen is changing, and the video encoding settings.

## Concurrent Access State



One user is connected to the Remote Console



Multiple users are connected to the Remote 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.

## Monitor Only State

The far right icon shows whether this client may interact or simply view the target computer. If Monitor Only is disabled, then the keyboard and mouse may interact with the target. If Monitor Only is enabled, the the client is view-only.

## Exclusive Access

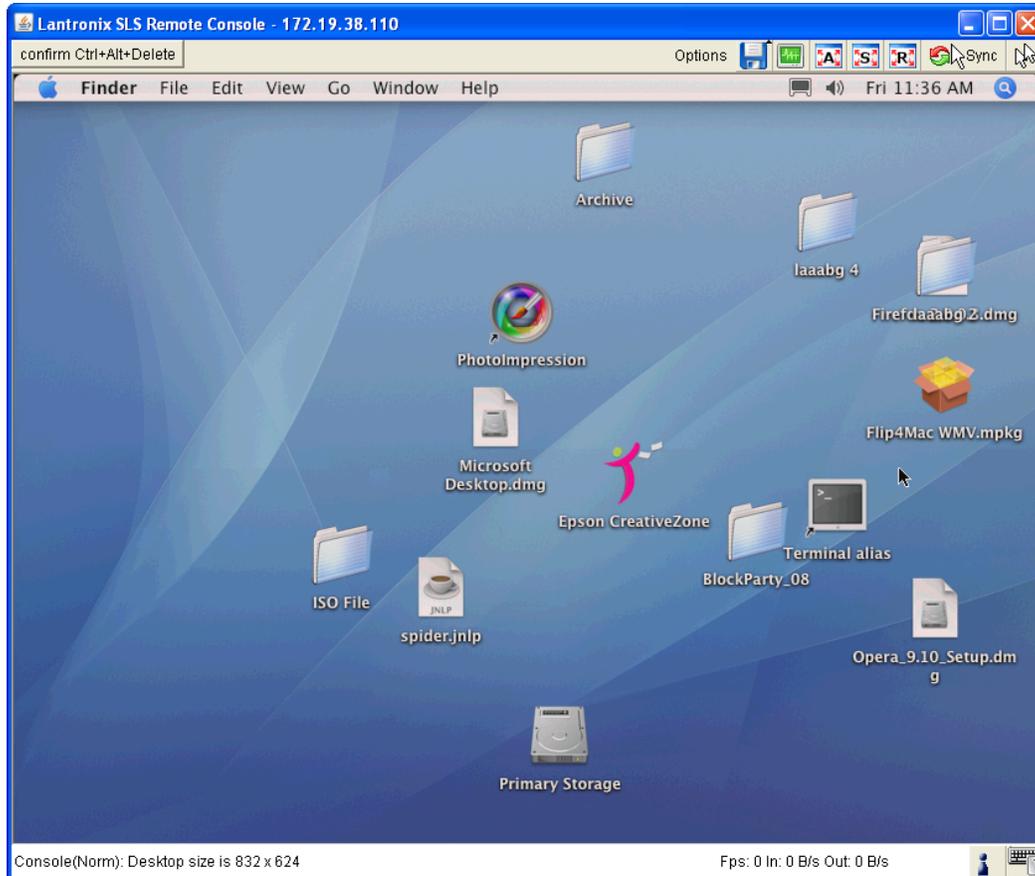
Only one user at a time may access the Spider or SpiderDuo.

## Basic Remote Console Operation

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

- ◆ Outside the Remote Console window, 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 or SpiderDuo unless the redundant supply is used.

**Figure 6-3 Remote Console Toolbar**



## 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. Clicking the **Auto Video Adjustment** one or more times typically cures any offset.

## Screen Display Adjustments

Three features are added to the toolbar to facilitate Screen display changes:

- ◆ **A**—Full Screen Mode (**Ctrl+F10**).
- ◆ **S**—Full Screen Stretch Mode (**Ctrl+F10** to return to regular mode).
- ◆ **R**—Full Screen Mode with Changing Client Monitor Resolution (**Ctrl+F10** to return to regular mode).

## Fast Sync and Intelligent Sync

The Spider uses two different algorithms for re-synchronizing local and remote cursors. Use the Fast Sync button on the toolbar to correct a fixed skew.

Intelligent Sync uses a different algorithm and is useful when the mouse settings have changed on the remote system or when Fast Sync does not work. It is accessed through the **Options > Mouse Handling** drop-down menu. The Sync button on the toolbar usually performs a Fast Sync, but will perform an Intelligent Sync if the video format has recently changed.

## Single and Double Mouse Modes

Continuous synchronization of local and remote cursors may not be feasible. The Spider provides a mode where only one cursor is visible when operating in the active Remote Console viewport. Click the **Single/Double** button on the toolbar to activate Single Mouse Mode. This is indicated by a single arrow in the **Single/Double** button. When in this mode, the Java KVM console “grabs” the local cursor after clicking within the viewport and will not release it until a “release-cursor” hot key sequence is given (**Alt+F12** by default). As there is only one cursor, and that one is confined to the active viewport, there is no issue with local to remote cursor tracking. There also is no local cursor; **Alt+F12** is required to free the cursor to move the focus from the active viewport. Clicking when the local cursor is within the viewport will re-grab the cursor. Single Mouse Mode may be exited by clicking on the **Single/Double** button.

If at some point the cursor seems to disappear, click **Alt+F12** or check the Single/Double Button as Single Mouse Mode may have been entered in error.

**Note:** *Single Mouse Mode requires Sun Java 1.4 or higher*

## Local Cursor

The Spider has an option to change the appearance of the local cursor when the focus is on the remote computer. Select **Options > Local Cursor** and select one of the following cursor options:

- ◆ **Default**—the local cursor maintains its appearance regardless of the focus location
- ◆ **Transparent**—the local cursor is invisible when the focus is on the remote computer. This is similar to Single Mouse Mode except the cursor is not “grabbed” and will reappear when moved outside of the active viewport.
- ◆ **The other selections** provide a change of appearance for a visual clue that the focus is on the remote computer; the cursor changes back when the focus is back at the client system (including those areas of the Remote Console window outside the main viewport.)

Selections made in the Local Cursor submenu are associated with the current user and will be saved for the next Remote Console session.

## Optimizing Video

The Spider and SpiderDuo can automatically make adjustments to video settings including clock and phase, and encoding to ensure that a picture displays quickly. You can also manually specify the settings.

### Auto and Manual Video Adjustment

The Spider automatically recognizes and adapts to many standard video resolutions and refresh rates. When it first enters the Remote Console window, it recognizes and locks onto the video in order to provide a picture as soon as possible.

Once the window displays, click the **Auto Video Adjustment** button once or twice to provide a greater degree of optimization. The Auto Adjustment process analyzes the timing of the incoming video horizontal and vertical sync signals then adjusts the digitizing hardware parameters. If there is slightly nonstandard timing, these parameters may be manually fine-tuned.

If it is necessary to adjust video hardware parameters, this may be done from **Options > Video Settings**. This brings up a window with a number of slider bars.

Adjust the brightness and contrast of the Remote Client window as presented by the Auto Adjustment. This is a hardware parameter and applies to all Spider users. Overall brightness and the contrast levels of each of the red, green, and blue primaries may be modified up or down. The Remote Console window immediately reflects the change. Once there is a satisfactory color-mapping, click **Save Changes** to retain those colors permanently for that video format. To discard the changes made, click **Undo Changes**. To return a particular setting or all settings to the original factory defaults, click **Reset this Mode** or **Reset All Modes**.

See [C: Supported Resolutions and Refresh Rates](#) for more information.

### Clock and Phase

The A/D converter uses these low-level settings in the digitization process. Adjustment should not be required unless advised by Lantronix Tech Support.

If the timing of the video signal is slightly off, the Auto Adjustment may not capture the frame at the right point. This will result in black bars along left, right, top, or bottom of the Remote Console viewport, and cutting off the opposite side of the captured image. The Offset sliders can be used to align the sides properly. Once there is correct alignment, click **Save Changes** to retain those settings permanently. To discard the changes made, click **Undo Changes**. To return a particular setting or all settings to the original factory defaults, click **Reset this Mode** or **Reset All**.

### Video Encoding

Various video encoding schemes have been defined to try to tailor the bandwidth usage to what is available. In addition to the predefined schemes, compression levels, and color depth can be manually adjusted. The default settings for each user are established in the **KVM Console Settings > KVM\_User > Transmission Encoding** web page.

To change the settings during a session, select **Options > Encoding > Predefined, Encoding > Compression, Encoding > Color Depth**, and **Encoding > Lossy** manual adjustments. These settings will be lost when the Remote Console window is closed; for nonvolatile changes use the **KVM Settings > User Console > Transmission Encoding** web page.

## Scaling Target Video to Client Resolution

In addition to the 1:1 pixel mapping mode, which is the default when the Remote Console window is first launched, scaling factors may be applied to the captured video in order to match various sizes of windows on the client. This scaling may be a fixed ratio or dynamically adjustable, as selected from the **Options > Scaling** selection. The default is 100 percent, although it may result in a viewport smaller than the virtual screen and is moved around with scroll bars. The optimal viewing percentages are 25 and 50.

## Keyboard Functions

The Spider and Spider Duo provide a number of useful functions for mapping or translating between the local keyboard/keycodes and the emulated keyboard presented to the target computer.

### Soft Keyboard

With remote control of a computer, it may be that the target system and client system are in different countries, using different languages. By using a Soft Keyboard, the local user can have the keycodes available to send to the target that are not on the local keyboard, without worrying about OS and application character set mappings.

Select **Options > Soft Keyboard > Mapping** to get a submenu listing the languages supported. Make the desired selection, and then verify it with **Show soft keyboard**.

Select **Options > Soft Keyboard > Show**. This provides an image of the currently selected Soft Keyboard. The Soft Keyboard sends single keystrokes as well as combinations of keys such as **Ctrl+C**. For a single keystroke, click on the button with the desired character. Single keys such as alphanumeric characters and punctuation are sent immediately. Special keys such as **Ctrl**, **Shift**, and **F1** to **F12** must be selected twice. The first click sends the signal “key is clicked.” The second click indicates the signal “key is released” to the remote system. After the first click the button will change its color to indicate that the key remains clicked, and that a code has not been sent. After the second click the button will appear as usual, showing that the keycode was sent.

Click the **Close** button on the title bar to close the soft keyboard.

### Local Keyboard

The Java Virtual Machine running the Remote Console applet on the client computer determines its keyboard language mapping automatically from the operating environment. There may be circumstances where it is unable to do so, such as when the keyboard mapping and OS language do not match. The **Options > Local Keyboard** selection allows manual designation of the language/layout of the keyboard on the client system.

### Hotkeys

Hotkeys provide an alternative method for sending keycode sequences defined in the section on Remote Console Button Keys. Click **Options > Hotkeys** and select the Button Key to be sent. If that Button Key has been defined with “Confirm”, a confirmation dialog box pops up before the keycode is sent.

## Other Remote Console Functions

Other remote console functions are described in this section. For example, monitor only specifications, exclusive access, capture of the screen to the clipboard and refreshing the video.

## Monitor Only

When **Options > Monitor Only** is checked, the keyboard and mouse are disabled for this Remote Console window. The Monitor Only state is shown in the lower right corner of the Remote Console status bar. The user must have the appropriate permissions to change this setting.

## Exclusive Access

When **Options > Exclusive Access** is checked, no other client may open a Remote Console window to this Spider. Any open Remote Console windows on other clients will be disconnected. The Exclusive Access state is shown in the lower right corner of the Remote Console status bar. The user must have the appropriate permissions to change this setting.

## Screenshot to Clipboard

**Options > Screenshot** captures a snapshot of the entire target system's virtual screen to the clipboard for pasting into other applications.

## Refresh Video

The entire Remote Console viewport area is redrawn when the Remote Console window is first opened, and when the **Auto Adjust Video** button is clicked. As the encoding settings and noise filter may sometimes result in visible compression artifacts, selecting **Options > Refresh Video** can be used to redraw the entire viewport area.

## Telnet/SSH

In addition to interacting with the target system using the KVM Console, the Spider also allows text communication with the target via the Telnet Console, also a Java program window. Telnet and SSH are network protocols that enable a tunnel from the client system to the Spider's serial port. Once set up, it may be accessed through the web interface at the Telnet Console window, or using a Telnet/SSH client to connect directly. Note that Telnet/SSH cannot be used to connect to the Spider itself in order to control it, as the Spider has an HTTP and not a command line interface.

The Telnet Console is a Java program and has the same Java Runtime Environment requirements as the Remote Console. When the Telnet Console window is open, the user at the client system can send and receive characters directly to the serial port.

## Set up and Enable

To use Telnet or SSH, 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.

## Passthrough Use

When using Telnet/SSH in passthrough mode, the Spider 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, at the assigned Telnet TCP port number.
2. The Spider will present **LOGIN** and **PASSWORD** prompts. Enter a valid user name and password. The user must have permissions set to use Telnet or SSH.

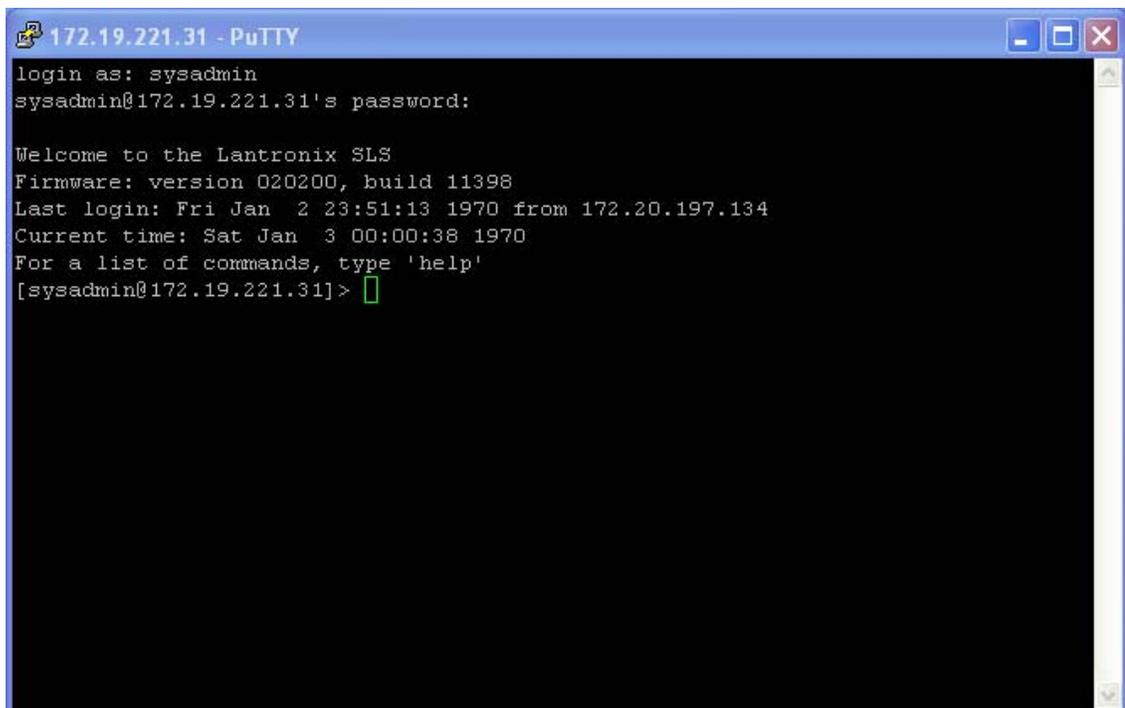
3. The Spider will reply with a Welcome and status, followed by a command line prompt. Selections are:
  - ◆ **Help**—Displays a list of commands
  - ◆ **Version**—Displays the current Spider firmware version number
  - ◆ **Connect Serial**—Enter passthrough to serial port mode
  - ◆ **Logout**—Terminates 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 SSH or Telnet ability to send and receive serial data between the client and the serial port. The Spider does not echo this data back to the client.
7. When complete, enter **Esc-Exit** to return to the command line.
8. Enter `logout` or `!` to close the connection.

## Telnet Console Use

When using the Telnet Console, the Spider opens a window on the client system that provides direct access to the Telnet/SSH command line. 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 user must have permissions set to use Telnet or SSH. The JRE will launch, and the Telnet Console window appears. Telnet Console and Remote KVM Console windows may be open concurrently.

**Figure 6-4** Login Screen



```
172.19.221.31 - PuTTY
login as: sysadmin
sysadmin@172.19.221.31's password:

Welcome to the Lantronix SLS
Firmware: version 020200, build 11398
Last login: Fri Jan 2 23:51:13 1970 from 172.20.197.134
Current time: Sat Jan 3 00:00:38 1970
For a list of commands, type 'help'
[sysadmin@172.19.221.31]>
```

## 7: Interfaces

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

- ◆ [Network Settings](#)
- ◆ [Serial Port Settings](#)
- ◆ [KVM Console Settings](#)
- ◆ [Keyboard/Mouse](#)
- ◆ [Video](#)
- ◆ [Virtual Media](#)
- ◆ [User Interface Settings](#)
- ◆ [Configure VIP](#)

### 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, Telnet/SSH access, proxy hose and port, and bandwidth limit.

To configure network settings, perform the following steps.

1. Click **Interfaces > Network**. [Figure 7-1](#) shows the page that displays.

**Note:** A small green square to the right of a field name indicates that the current value is the default.

Figure 7-1 Spider Network Settings Web Page

The screenshot displays the Spider Network Settings web page. At the top, there are navigation tabs for Interfaces, User Accounts, Services, and Maintenance. The main content area is titled "Network Settings" and is divided into several sections:

- Network Basic Settings:** Includes fields for IP auto configuration (DHCP), Host name (SLS4a8984ee), IP address (172.19.100.2), Subnet mask (255.255.0.0), Gateway IP address (172.19.0.1), Primary DNS server IP address (172.19.1.1), and Secondary DNS server IP address (172.19.1.2).
- IPv6 Settings:** Features an "Enable IPv6" checkbox and a "REBOOT" icon. A note states: "Enable/Disable IPv6 requires reboot to take effect." Below are fields for IPv6 address, IPv6 address dynamic, and Link-local IPv6 address.
- LAN Interface Settings:** Shows "Current LAN interface parameters: autonegotiation on, 100 Mbps, full duplex, link ok". It includes dropdown menus for "LAN interface speed" (Autodetect) and "LAN interface duplex mode" (Autodetect).
- Network Miscellaneous Settings:** Contains fields for Remote Console & HTTPS port (443), HTTP port (80), Telnet port (23), and SSH port (22). It also has a "Bandwidth Limit" field and several checkboxes for "Enable Telnet access", "Enable SSH access", "Disable setup protocol", and "Enable remote console proxy access".

At the bottom of the settings area, there are buttons for "Save", "Reset to defaults", and "Reset". A small green square icon indicates "Stored value is equal to the default." The footer of the page includes copyright information (© 2007-2009 Lantronix, Inc.), navigation links (Home, KVM Console, Terminal, Logout), and the version number (Version 03.00.01 (V3.01\_2010-02-01)).

2. Modify the following fields.

## Network Basic Settings

Table 7-2 Network Basic Settings

| Field   | Description   |
|---|---|
| <b>IP auto configuration</b>                    | Select <b>DHCP</b> or <b>BOOTP</b> to fetch network settings from the appropriate type of server. Select <b>NONE</b> for a fixed IP address.  |
| <b>Host name</b>                                | DHCP servers can register a name for this Spider to assist in finding it, or you can configure it with a short host name or a fully qualified domain name.  |
| <b>IP address</b>                               | If you are using a fixed IP address, enter it in the usual dot notation.  |
| <b>Subnet Mask</b>                              | If you are using a fixed IP address, enter the subnet mask of the local network.  |
| <b>Gateway IP address (optional)</b>            | If the Spider is to be accessible from outside the local subnet, enter the IP address of the router providing access.   |
| <b>Primary DNS Server IP Address (optional)</b> | 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 functions requiring network connections. |

Table 7-2 Network Basic Settings (continued)

| Field                                      | Description  |
|--|--|
| 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

Table 7-3 LAN Interface Settings

| Field                            | Description  |
|----------------------------------|--|
| Current LAN interface parameters | Displays current LAN interface settings.   |
| LAN interface speed              | Manual setup may be required for older equipment. With autonegotiation on, the window displays the current state of the link. Note that the parameters of the second Ethernet port are not configurable, they remain at autonegotiate. Select the speed from the drop-down menu. |
| LAN interface duplex mode        | Select the duplex mode from the drop-down menu.  |

## IPv6 Settings (Firmware v3.0 or higher)

Table 7-4 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. |

## Miscellaneous Network Settings

Table 7-5 Miscellaneous Network Settings

| Field                              | Description  |
|------------------------------------|--|
| Remote Console & HTTPS port        | Port number at which the Spider's Remote Console server and HTTPS server are listening. The default is 443.  |
| HTTP port                          | Port number at which the Spider's HTTP server is listening. The default is 80.   |
| TELNET port                        | Port number at which the Spider's Telnet server is listening. The default is 23.   |
| SSH port                           | Port number at which the Spider's SSH server is listening. The default is 22.  |
| Bandwidth Limit                    | The maximum network traffic generated through the Spider's primary Ethernet port, in kilobits. If left blank, there is no bandwidth limitation applied.  |
| Enable TELNET/SSH access           | For security, the default is having Telnet and SSH disabled. Check the appropriate box (es) and set up the serial port for Telnet/SSH to use the Telnet console.   |
| Disable Setup Protocol             | Spider View uses a special protocol to locate and set up Spider IP addresses. As a security measure you may wish to disable this protocol when deploying Spiders. If the protocol is disabled, Detector and the Spider network will not find the Spider. |
| Enable remote console proxy access | Enable the Java KVM console program to use a proxy server to connect to the Spider. If you must configure your web browser to use a proxy server, you will likely have to do the same on the Spider.   |

Table 7-5 Miscellaneous Network Settings (continued)

| Field      | Description                       |
|------------|-----------------------------------|
| Proxy host | Enter the proxy server's address. |
| Proxy port | Enter the proxy port number.      |

3. 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.

## Serial Port Settings

After using the serial port to set up the network parameters, you can use the serial port for something else. You can establish a PPP connection to use a modem (Spider only) or another serial connection to log into and operate the Spider. If you want to access a console port remotely through the Spider, SSH and Telnet passthrough is available.

To configure the serial port, perform the following steps.

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

Figure 7-6 SpiderDuo Serial Port Settings Page

The screenshot shows the 'Serial Port Settings' page in the SpiderDuo web interface. The page has a navigation bar with 'Interfaces', 'User Accounts', 'Services', and 'Maintenance'. The 'Serial Port' tab is active. The settings are organized into three sections:

- Configuration Login:** Radio button selected. Fields: Speed (9600), Data bits (8), Parity (None), Stop Bits (1), Flow Control (None).
- Modem:** Radio button unselected. Fields: Serial Line Speed (115200 bits/s), Modem Init String (ATZHO OK ATLOM0&K3X1 OK), Modem Server IP Address (192.168.3.1), Modem Client IP Address (192.168.3.2).
- Passthrough Access to Serial Port 1 via Telnet/SSH:** Radio button selected. Fields: Speed (9600), Data bits (8), Parity (None), Stop Bits (1), Flow Control (None).

At the bottom, there are buttons for 'Save', 'Reset to defaults', and 'Reset'. A legend indicates that a green square means 'Stored value is equal to the default.'

2. Modify the following fields.

Table 7-7 Serial Port Settings

| Field               | Description  |
|---------------------|--|
| Configuration Login | Select this option to use the serial port locally only to set up network parameters or reset the unit. |

Table 7-7 Serial Port Settings (continued)

| Field   | Description   |
|---|---|
| <b>Modem (Spider Only)</b>                                | <p>Connect to the Spider with a dial-up or ISDN connection, using PPP. Essentially, the Spider acts as an ISP that you dial in to. The client system will need to be set up accordingly, for example using the Windows Network Connection Wizard. Change the following parameters as necessary:</p> <ul style="list-style-type: none"> <li>◆ <b>Serial Line Speed:</b> Most modems support 115200 bps.</li> <li>◆ <b>Modem Init String:</b> The initialization string sent out to set up the modem. If you have a special modem or are going through a PBX requiring an access sequence, you may modify the string. Consult the modem's manual on the AT command syntax.</li> <li>◆ <b>Modem server IP addresses:</b> As part of the PPP handshake, IP addresses are assigned to the remote device.</li> <li>◆ <b>Modem client IP address:</b> IP address assigned to the Spider.</li> </ul>  |
| <b>Passthrough Access to serial port 1 via Telnet/SSH</b> | <p>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's serial port. Once the port is set up, it may be accessed through the web interface at the Telnet Console window, or using a Telnet/SSH client to connect directly.</p> <p>Set the following parameters to match connected equipment:</p> <ul style="list-style-type: none"> <li>◆ <b>Speed:</b> 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.</li> <li>◆ <b>Data bits:</b> Number of data bits used to transmit a character. From the drop-down list, select the number of data bits. The default is <b>8</b> data bits.</li> <li>◆ <b>Parity:</b> Parity checking is a rudimentary method of detecting simple, single-bit errors. From the drop-down list, select the parity. The default is <b>none</b>.</li> <li>◆ <b>Stop Bits:</b> 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 <b>1</b>.</li> <li>◆ <b>Flow Control:</b> 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 <b>none</b>.</li> </ul> |

3. 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.

## 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. 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 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 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 7-8** User Remote Console Settings Page

The screenshot shows the 'KVM Console Settings' page for user 'sysadmin'. The page is divided into several sections:

- Transmission Encoding:** Includes radio buttons for 'Automatic Detection' (selected), 'Pre-configured', and 'Manually'. Under 'Pre-configured', there are dropdown menus for 'Network speed' (LAN (high color)), 'Compression' (0 - none), and 'Color depth' (16 bit - high col.).
- KVM Console Type:** Includes radio buttons for 'Default Java VM' (selected) and 'Sun Microsystems Java Browser Plugin'. A note states: 'If your system doesn't have the Java Plugin, this option will download 11MB Plugin for extended KVM Console function.'
- KVM Console Deployment:** Includes radio buttons for 'Java Web Start' (selected) and 'Applet'.
- Miscellaneous KVM Console Settings:** Includes checkboxes for 'Start in Monitor Mode' and 'Start in Exclusive Access Mode', both of which are checked.
- KVM Console Virtual Keys:** A table with 8 rows. Each row has a 'Key Definition (Help)' field and a 'Name' field. Key 1 is 'confirm Ctrl+Alt+Delete', Key 2 is '7', Key 3 is '1', Key 4 is '8', Key 5 is '2', Key 6 is '5', Key 7 is '9', and Key 8 is '3'. The corresponding names are 'confirm Ctrl+Alt+Delete', 'Home', 'End', 'Up', 'Down', 'Select', 'Up 1 cat', and 'Down 1 cat'. A note below the table says: 'To remove entry from table, clear 'Key Definition' and click 'Save''. There is an 'Add More Entries' button.
- Mouse Hotkey:** Includes a 'Mouse Hotkey (Help)' field with 'Alt+F12' and a 'Full-screen Hotkey (Help)' field with 'Ctrl+F10'. A note states: 'Used for fast mouse synchronization (in Double Mouse mode) and to free the grabbed mouse (in Single Mouse mode). Full-screen mode with maintaining the same aspect ratio.'

At the bottom, there are buttons for 'Save', 'Reset to defaults', and 'Reset'. A small note indicates: 'Stored value is equal to the default.'

2. Configure the following fields.

## KVM Console Settings

**Table 7-9** KVM Console Settings

| Field                           | Description   |
|---------------------------------|---|
| <b>KVM Console Settings for</b> | 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

Table 7-10 Transmission Encoding

| Field               | Description  |
|---------------------|--|
| Automatic Detection | This option uses an algorithm to try to determine what sort of connection is being used, and sets up parameters to match. These settings may change from login to login depending on the state of the network at that point.   |
| Preconfigured       | Establishes a set of parameters optimized for each of a number of connection types. The default transmission encoding is LAN (high color), which is uncompressed with a 16 bit color depth. Other data networks may be chosen from the <b>Network speed</b> drop-down list, and the compression and color depth will be configured accordingly.  |
| Manual              | Allows the direct control of the compression factor and color depth. The simplest way to reduce bandwidth is to cut the color depth down to 8 bits; subtle color shades will be gone but the overall image is very usable. Dialing up the compression level also makes available even further reductions in color depth, all the way down to black and white (1 bit.) As compression level increases and/or color depth decreases, image quality and responsiveness to changes deteriorates but required bandwidth is reduced. |

## KVM Console Type

Table 7-11 KVM Console Type

| Field                                | Description  |
|--------------------------------------|--|
| Default Java VM                      | Select this option to use Java on the client system launching the applet. If no Java environment is installed, the console window will not launch. The default is enabled. |
| Sun Microsystems Java Browser Plugin | Force the system to use the platform-independent Sun version instead when launching the Remote Console applet.   |

## KVM Console Deployment

**Note:** Users have two ways to deploy the Remote Console program. Both provide the same functionality and differ only in deployment method. The default is Java Web Start. Applet deployment is available in case the user cannot connect via Java Web Start. This usually should not happen unless the user has a special proxy server or firewall that blocks Java Web Start.

Table 7-12 KVM Console Deployment

| Field          | Description   |
|----------------|---|
| Java Web Start | Select this option to use Java Web Start deployment method. |
| Applet         | Select this option to use the Applet deployment method.     |

## Miscellaneous KVM Console Settings

Table 7-13 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. |

Table 7-13 Miscellaneous KVM Console Settings

| Field                          | Description  |
|--------------------------------|--|
| 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

Table 7-14 Mouse Hotkey

| Field              | Description   |
|--------------------|---|
| Hotkey (Help)      | 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 <b>Alt+F12</b> . Change the key code if necessary.   |
| Full-screen Hotkey | Pressing <b>Ctrl+F10</b> will display the KVM console in Full-screen mode while maintaining the same aspect ratio. Press <b>Ctrl+F10</b> again to return to regular screen mode. The default is <b>Ctrl+F10</b> . Change the key code if necessary. |

## KVM Console Virtual Keys

Table 7-15 KVM Console Virtual Keys

| Field                 | Description   |
|-----------------------|---|
| Key Definition (Help) | <p>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.</p> <p>One key is predefined, for <b>Ctrl+Alt+Delete</b> (with confirmation.) The syntax to define a new Button Key is as follows:</p> <p><b>&lt;keycode&gt;[+ -]&gt;[*]&lt;keycode&gt;*</b></p> <p>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.</p> <p><b>Note:</b> For a list of keys and further explanation, click the <b>Help</b> link at the top of the <b>Key Definition</b> column.</p> |
| 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. 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.

## 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 7-16 Keyboard/Mouse Settings

The screenshot displays the LANTRONIX Spider Duo web interface. At the top, there are navigation tabs for 'Interfaces', 'User Accounts', 'Services', and 'Maintenance'. The main content area is titled 'Keyboard/Mouse Settings'. It features a 'Host Interface' dropdown menu set to 'Auto' and a note explaining that the system will choose USB if available, otherwise PS/2. Below this, there is a checkbox for 'Force USB Full Speed Mode'. The 'Keyboard Model' is set to 'Generic 104-Key PC'. The 'Key Release Timeout' is set to '50 msec'. The 'Country Code' is set to 'None'. The 'USB Mouse Type' is set to 'Other Operating Systems'. The 'Mouse Speed' is set to 'Auto'. At the bottom, there are 'Save', 'Reset to defaults', and 'Reset' buttons. A 'USB Status' box on the right shows 'USB Speed: High speed', 'Keyboard: Interface=0 Max PS=8', 'Mouse: Interface=1 Max PS=8', and 'Mass Storage: Not Connected'.

2. Modify the following fields.

## Keyboard/Mouse Settings

Table 7-17 Keyboard/Mouse Settings

| Field          | Description   |
|----------------|---|
| Host Interface | <p>In general, the USB interface is preferred because it provides superior mouse tracking. The <b>Host Interface</b> drop-down provides three selections.</p> <p>In the default mode, <b>Auto</b>, the Spider 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 falls back to PS/2. If you have a USB model Spider and the attached computer does not support USB, the system will be view only.</p> <p>On the PS/2 model Spider, select <b>PS/2</b> to force the PS/2 interface or <b>USB</b> to require USB. This selection has no effect on the USB model Spider.</p> |

Table 7-17 Keyboard/Mouse Settings

| Field                     | Description  |
|---------------------------|--|
| Force USB Full Speed Mode | Some older systems do not support USB high-speed mode and may not recognize the keyboard/mouse. Enable this option for Spider to negotiate in USB full speed mode. |

## Keyboard Model

Table 7-18 Keyboard Model

| Field                                | Description   |
|--------------------------------------|---|
| <PS/2 keyboard model drop-down menu> | <p>When operating in PS/2 interface mode, key codes from several layouts may be emulated.</p> <ul style="list-style-type: none"> <li>◆ <b>Generic 104-key PC</b> for the traditional layout.</li> <li>◆ <b>Generic 109-key PC</b> for keyboard with added Windows keys. (Use 109 for Japanese keyboard.)</li> <li>◆ <b>Apple Macintosh</b> for Mac layout.</li> </ul> |

## Key Release Timeout

Table 7-19 Key Release Timeout

| Field               | Description   |
|---------------------|---|
| Key release timeout | Network delays may sometimes result in duplicated keystrokes. Enable Key Release Timeout to fix this problem. |
| Timeout after       | Enter time, in msec.  |

## Country Code

Table 7-20 Country Code

| Field        | Description   |
|--------------|---|
| Country Code | Select the check box to enable the Spider to recognize the country code. <b>Enable</b> if the host machine requires the keyboard to send a country code to use a certain language. Most operating systems do not require this except Sun Solaris. |
| Country      | From the drop-down list, select the code of the desired country.  |

## USB Mouse Type

Table 7-21 USB Mouse Type

| Field                           | Description  |
|---------------------------------|--|
| <USB mouse type drop-down menu> | Different operating systems running on the target system require different mouse emulation protocols. One selection is available for newer versions of Windows and Mac OS/X, and another for <b>Other Operating Systems</b> (e.g., Linux). |

## Mouse Speed

Table 7-22 Mouse Speed

| Field       | Description  |
|-------------|--|
| Mouse speed | <p>Select the method of assigning mouse speed.</p> <ul style="list-style-type: none"> <li>◆ <b>Auto</b> mouse speed determines the speed and acceleration settings of the target system. It is the recommended setting for most applications.</li> <li>◆ <b>Fixed scaling</b> translates a one-pixel motion on the client system to a selectable number of pixels moved on the target system. As the 1 to n mapping is linear, this will only work when there is no compression acceleration or other special effects turned on at the target system.</li> </ul> |

3. View the USB Status for USB Speed, Keyboard, Mouse, and Mass Storage.
4. 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.

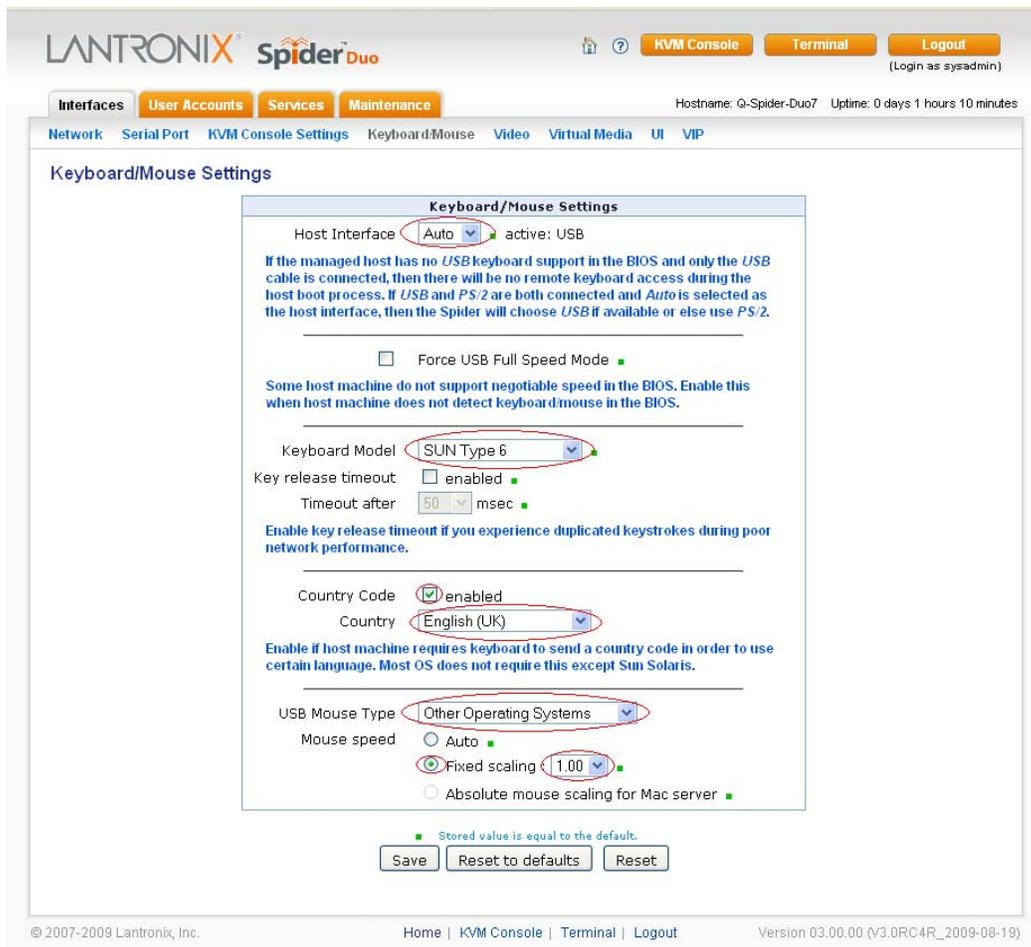
To configure the Spider USB model with a Sun Solaris operating system, perform the following steps.

1. Click **Interfaces > Keyboard/Mouse**. The Keyboard/Mouse Settings page displays.
2. On the **Keyboard/Mouse Settings** page configure the red outlined fields as shown.
3. The Sun Solaris operating system requires the keyboard to send a country code to use a certain language. At **Country Code** click **enabled** and use the **Country** drop-down list to select your language choice.

**Note:** Sun Solaris settings are for the Spider only.

4. Click **Save**.

Figure 7-23 Keyboard/Mouse Settings Page B



## Video

The Spider works by capturing and digitizing the analog video coming from the attached computer. This analog video may have more or less low-level electrical noise present, depending on the nature of the video card or embedded video controller.

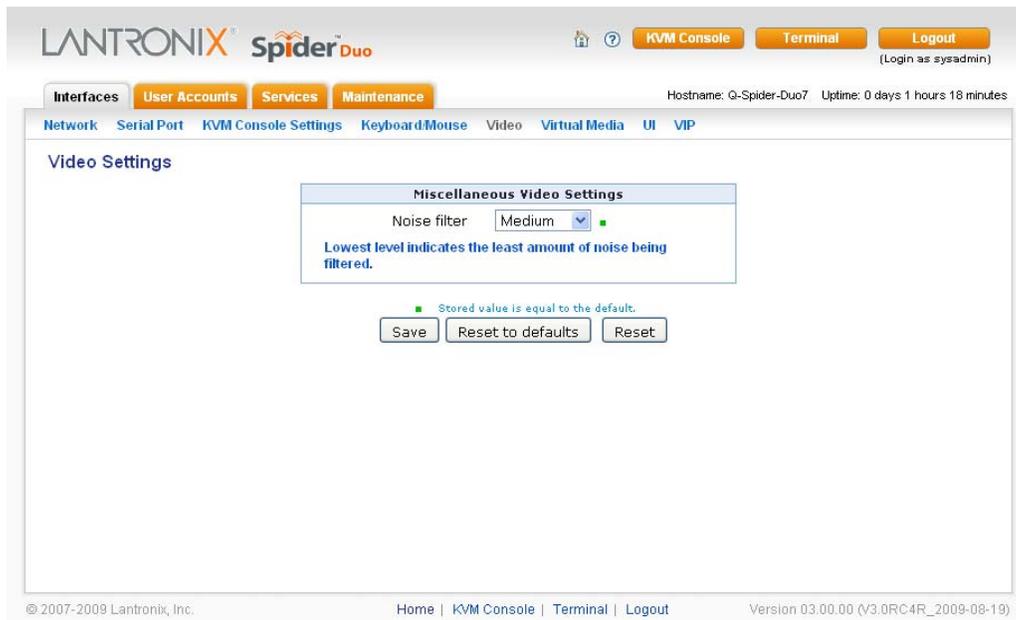
When viewed on a monitor, this noise (if random) is invisible as the display is being redrawn 60 to 100 times a second. Inside the Spider, however, the algorithm sees that noise as something changing on the screen, so that requires sending off an update to the client system.

This can result in a constant stream of data even when the image on the target computer's screen is not moving. In order to avoid this, at **Interface > Video > Miscellaneous Video Settings** the Spider has a selection for noise filter. The larger filter openings will filter out more of the noise, at the cost of potentially missing small incremental changes and seeing some compression artifacts (blocky-ness). Filter settings of **Medium** or **High** will work for most applications. Be sure to try the Remote Console Auto Adjust Video button a few times before deciding that a constant stream of data represents electrical noise requiring a larger filter setting.

To modify video settings, perform the followings steps.

1. Click **Interfaces > Video**. The Miscellaneous Video Settings page displays.

Figure 7-24 Miscellaneous Video Settings Page



2. Select the **Noise Filter** level from the drop-down menu.
3. 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.

## Virtual Media

The Spider provides a powerful capability called Virtual Media (or Virtual Disk). Using the USB port, the Spider can present either a local floppy disk image or a redirected remote CD-ROM image to the target computer. This can allow system recovery in conditions as bad as having local disks down and no primary network connection.

With Floppy Disk Image, the user can upload an image to the Spider's memory, which then emulates a locally attached floppy drive. With CD-ROM Image, a Windows or other SAMBA share can emulate a locally attached CD-ROM, for instance to update software.

Drive Redirection allows you to share (redirect) your local drive (floppy drives, hard disks, CD ROMs and other removable devices like USB sticks) with the remote system over a TCP network connection.

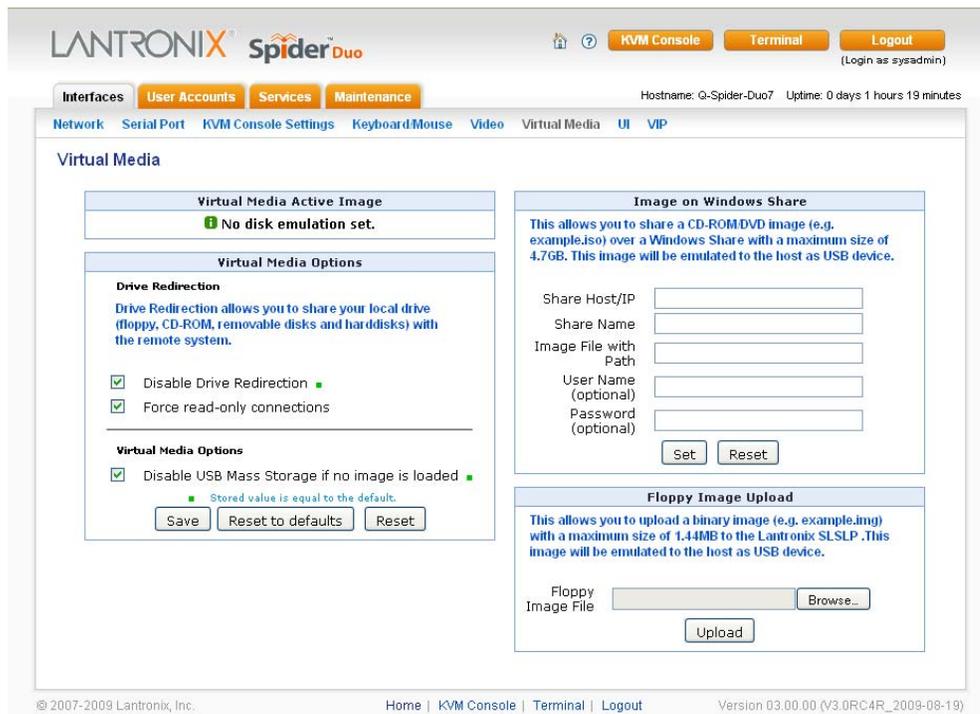
Thus, with Drive Redirection, you can use a virtual disk drive on the remote computer instead of an image file. It is also possible to enable a remote machine to write data to your local disc.

**Note:** Drive Redirection supports only Windows as the client computer since it redirects based on a drive letter.

To open the Virtual Media page, perform the following steps.

1. Click **Interfaces > Virtual Media**.

Figure 7-25 Virtual Media Page



To prepare for drive redirection, perform the following steps.

1. Enter the following fields.

## Virtual Media Active Image

Table 7-26 Virtual Media Active Image

| Field                      | Description  |
|----------------------------|--|
| Virtual Media Active Image | Once you set <b>Image on Windows Share</b> or <b>Floppy Image File</b> (on this web page), information about the currently assigned (active) image displays. |

## Drive Redirection

Table 7-27 Drive Redirection

| Field                       | Description   |
|-----------------------------|---|
| Disable Drive Redirection   | Drive Redirection is enabled by default. Select this checkbox to disable the ability to share the local drive with the remote system.   |
| Force read-only connections | Select to prevent the remote drive from writing to your local drive. Selected by default.<br><br><b>Warning:</b> Clearing the <b>Force read-only connections</b> check box may result in file system errors and data corruption because of drive caching when data is written back to the Redirected local drive. |

## Virtual Media Options

The operating system on the target computer must have a USB mass storage driver installed in order to use Virtual Media. As the BIOS on some systems does not always support mass storage emulation on the USB interface, the system default is to disable USB mass storage unless an image is loaded. This option may be unselected to use.

**Table 7-28** *Virtual Media Options*

| Field                              | Description   |
|------------------------------------|---|
| <b>Disable USB Mass Storage</b>    | Select the checkbox to disable USB mass storage if no image is loaded. Selected by default. Clear the check box if an image is loaded.  |
| <b>Force read-only connections</b> | Select to prevent the remote drive from writing to your local drive. Selected by default.<br><br><b>Warning:</b> <i>Clearing the Force read-only connections check box may result in file system errors and data corruption because of drive caching when data is written back to the Redirected local drive.</i> |

1. 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.

## Image on Windows Share

In this section of the page, you can enable the Spider to access a CD-ROM image up to 4.7 GB on a Windows shared folder via SAMBA. The Spider then makes that image accessible to the target computer by emulating a USB disk drive.

**Note:** *Windows 2003 and Windows Vista do not support this feature.*

Appropriate administrative permissions to access the host and file are needed, as well as the ability to see that computer over the network from the Spider.

The connection remains mounted until the current user logs out or the Spider is rebooted. Other client systems logging into the Spider will see the active image in all Virtual Media pages.

To share a CD-ROM image, perform the following steps.

1. Enter the following: fields.

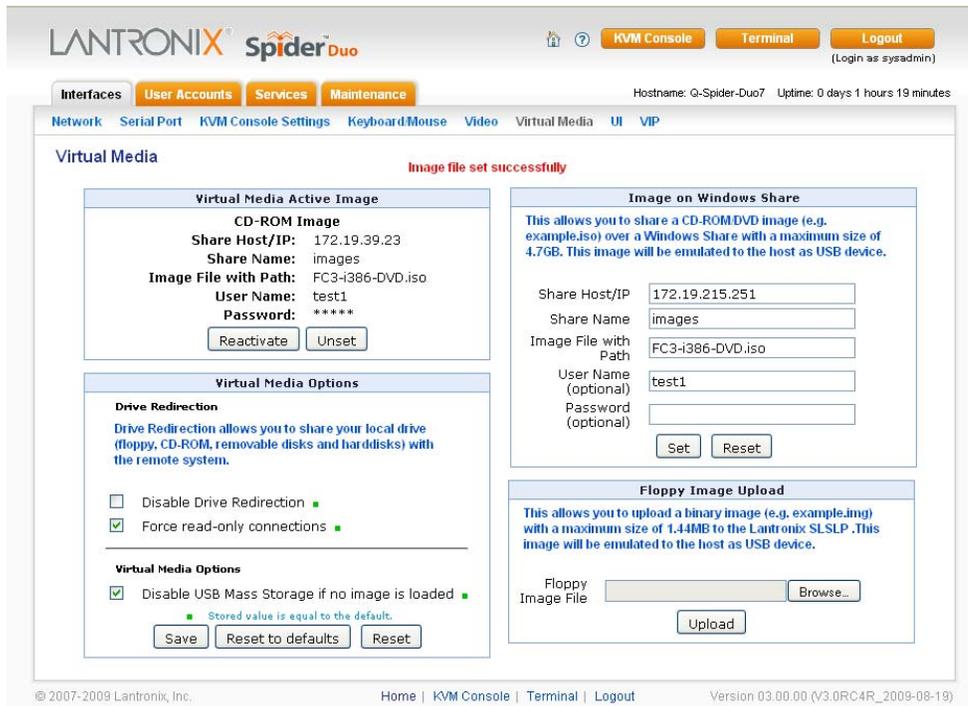
**Table 7-29** *Image on Windows Share*

| Field                       | Description   |
|-----------------------------|---|
| <b>Share Host/IP</b>        | IP address of the host of the Windows shared folder.  |
| <b>Share Name</b>           | Name of the host of the Windows shared folder.  |
| <b>Image File with Path</b> | Name and path to the CD-ROM image. The file must be structured as a CD-ROM image. The filename appears as the <b>Active Image</b> and the image is available to the target computer as a letter drive (e.g., <b>F:</b> ). |
| <b>User Name</b> (optional) | User name for accessing the host and file.  |
| <b>Password</b> (optional)  | Password for accessing the host and file.   |

2. Do one of the following:
  - a. To discard your changes, click **Reset**.

- b. To mount the image, click **Set**. Information about the image displays in the **Virtual Media Active Image** section of the page and the CD icon displays on the remote console.

Figure 7-30 Virtual Media Active Page



3. If desired, in the **Virtual Media Active Image** section:
- Click **Reactivate** if the remote console does not recognize the image.
  - Click **Unset** to remove the current image file. This option is available only when a user uploads a floppy image.
  - Click **Download** to save the image file.

## Floppy Image

In the **Floppy Image Upload** section, you can upload a floppy disk image to the Spider, which then appears to the attached computer as a physical floppy drive. The desired floppy image file will be uploaded from the client system or from a network drive accessible to the client system. The file must be structured as a floppy image. To make a floppy image, search for and use a utility such as `dd` or `rawwrite`. The maximum image size is 1.44 MB. For larger images, use the CD-ROM Image function.

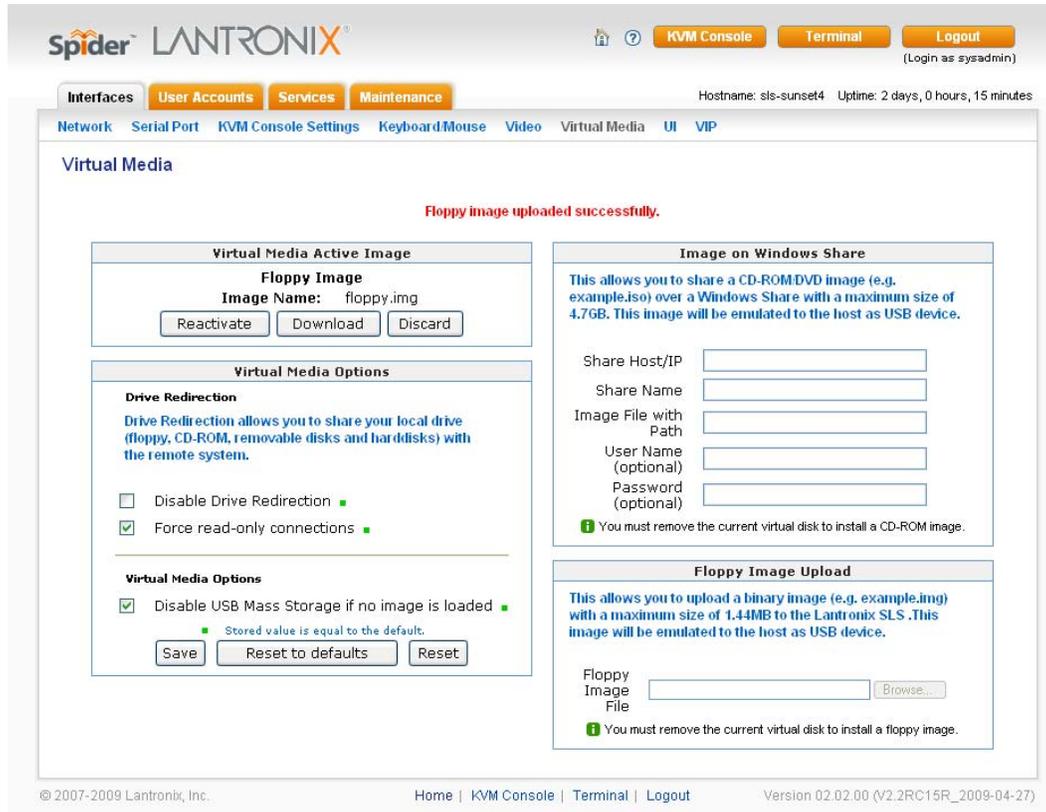
The image file remains in Spider until the current user logs out, or the Spider is rebooted. Other client systems logging into the Spider will also see the active image in all Virtual Media pages.

To upload a floppy image file, perform the following steps.

- In the **Floppy Image Upload** section (bottom right), click **Browse** to locate the floppy image file.
- Do one of the following:
  - Click **Reset** to discard your changes.

- b. Click **Upload** to load the image into Spider's memory. This floppy drive is accessible to the remote computer as a letter-name floppy drive (e.g., **B:**). Information about the image displays in the **Virtual Media Active Image** section of the page.

Figure 7-31 Virtual Media Active Image



3. If desired, in the **Virtual Media Active Image** section:
  - a. Click **Reactivate** if the remote machine does not recognize the image.
  - b. Click **Download** to save the image file.
  - c. Click **Discard** to remove the current image file.

## Connecting to a Redirected Drive

If Drive Redirection is enabled, you can connect to the drive. Depending on the combination of the type of drive and the Force read-only connections setting, different warnings display.

To connect to a redirected drive, perform the following steps.

1. Click the KVM Console button at the top of the Spider web page or click the console image that you see when you log in to the Spider. The Remote Console displays?
2. Click the disk icon  in the toolbar. Drive Redirection buttons display at the top left of the page.

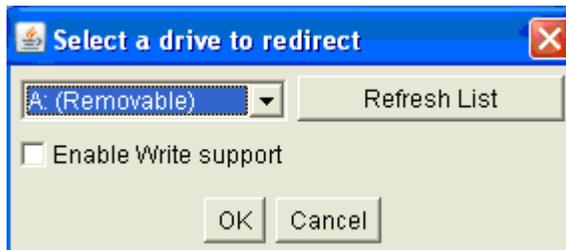
Figure 7-32 Drive Redirection Window



Figure 7-33 Drive Redirect Buttons

- Click the Connect Drive button at the top of the page. The Select a drive to redirect dialog box opens.

Figure 7-34 Select Drive Redirect Window

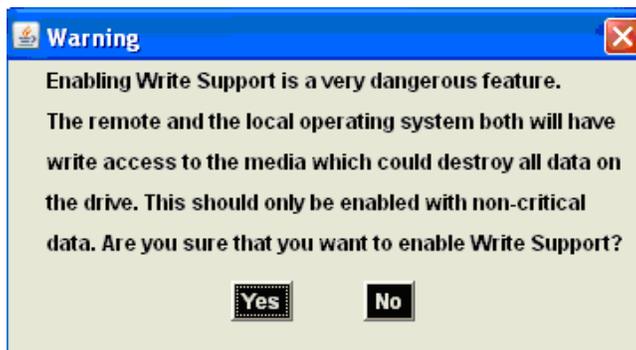


- From the drop-down list, select the drive you want to redirect.

**Note:** To refresh the list after adding or removing a drive, click the **Refresh List** button.

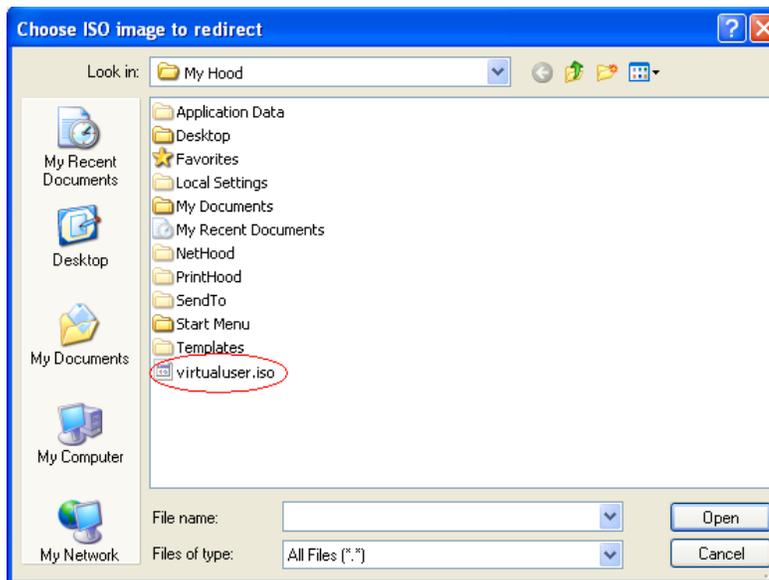
- If desired, select the **Enable Write support** check box.
- Click **OK**. Depending on your selections, the following events or warnings display:
- If you select **Enable Write support**, the following warning displays:

Figure 7-35 Enable Write Support Window



Because of the danger of destroying all data on the drive, click **Yes** only if you are certain of what you are doing. If you select the hard disk from the drop-down list, the following warning may display:

Figure 7-36 Local Drive Browser Window



8. Select the ISO image file to use as a local disk and press **Open**.

Figure 7-37 Drive Redirection Established Window



9. ISO Drive Redirection established displays at top of screen.

## User Interface Settings

The color of page tabs on the Spider can be changed. On the Interfaces page click **UI**. Select a style sheet from the drop-down list on the **User Interface Settings** page. Click **Save**.

Figure 7-38 User Interface Settings Page



## Configure VIP

To configure VIP, perform the following steps.

1. Click **Interfaces > VIP**. The current VIP settings display.
2. Enter new settings as needed.
3. Click **Save**.

**Figure 7-39** Configure VIP Page

The screenshot shows the 'Configure VIP' page in the Lantronix Spider Duo web interface. The page is divided into two main sections: 'VIP Settings' and 'Bootstrap Upload'. The 'VIP Settings' section includes a 'Conduit Enabled' checkbox (checked), a 'DSM IP Address' field (172.19.38.1), 'DSM Dna ID', 'Spider Dna ID', 'Tunnel User', 'Tunnel Port List' (22), 'Tunnel Port' (22), and 'Conduit Status' (Connected). The 'Bootstrap Upload' section features a 'Bootstrap File' input field with a 'Browse...' button, an 'Upload' button, and an 'Auto-Load from thumb drive' button. The page also includes a navigation menu at the top and a footer with copyright information.

**Note:** The **Bootstrap Upload** option allows for the upload of a bootstrap.xml file. You can also auto-load the file by clicking the **Auto-Load from thumb drive** button.

To upload a new bootstrap file, perform the following steps.

1. Click **Browse** to find and select the file.
2. Click **Upload**.
3. In the Bootstrap Update window, click **Update**.

**Figure 7-40** Bootstrap Update Window

The screenshot shows the 'Bootstrap Update' window. It displays the current settings: 'Current: 172.19.100.83 TUNb0892' and 'New: dna.dev.rmd:b5f69bf98 dna.dev.rmd:8ff849e47'. At the bottom, there are two buttons: 'Update' and 'Discard'.

## 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](#)
- ◆ [Local User Management](#)
- ◆ [User Permissions](#)
- ◆ [Remote Authentication](#)

### Local vs. Remote Authentication

User names and groups may be administered on the Spider to allow varying levels of access and control to different classes of users. To log in to the Spider, 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's memory. The Spider 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 where it has its permissions assigned.

### Local User Management

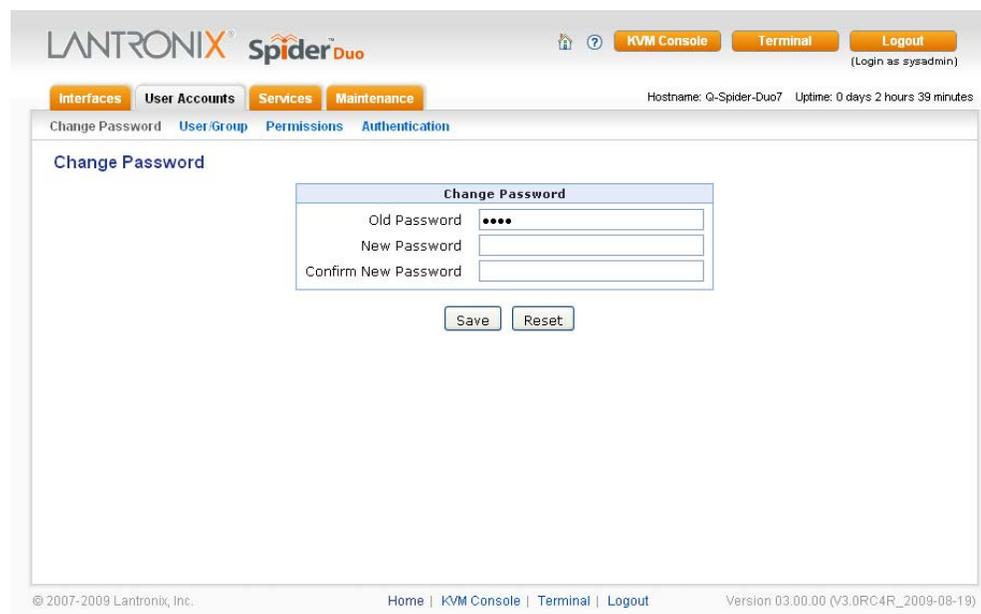
A newly assigned user has permissions inherited from an assigned group. All Local Users not associated with a group will inherit default settings.

### 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



The screenshot shows the Spider Duo web interface. At the top, there is a navigation bar with 'LANTRONIX Spider Duo' logo, a home icon, a help icon, and buttons for 'KVM Console', 'Terminal', and 'Logout (Login as sysadmin)'. Below this is a secondary navigation bar with 'Interfaces', 'User Accounts', 'Services', and 'Maintenance'. The 'User Accounts' section is active, showing sub-links for 'Change Password', 'User Group', 'Permissions', and 'Authentication'. The 'Change Password' page is displayed, featuring a form with three input fields: 'Old Password' (masked with dots), 'New Password', and 'Confirm New Password'. Below the form are 'Save' and 'Reset' buttons. The footer contains copyright information for Lantronix, Inc. (© 2007-2009), navigation links (Home, KVM Console, Terminal, Logout), and the version number (Version 03.00.00 (V3.0RC4R\_2009-08-19)).

2. Enter the current password under **Old Password**.

3. Enter the new password under **New Password** and **Confirm New Password**.
4. Click **Save** to save your settings, or click **Reset** to restore original 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 supports a maximum of 50 configured users. When defining a user, make sure the group to which the user will belong has already been created.

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.

**Table 8-3** User Management

| Field                   | Description  |
|-------------------------|--|
| <b>Existing users</b>   | To modify or copy an existing user, select that user from the drop-down menu and click <b>Lookup</b> . |
| <b>New user name</b>    | Enter the new user's name. Minimum 1 character.  |
| <b>Full user name</b>   | Enter the full name of the configured user. Minimum 1 character.                                       |
| <b>Password</b>         | Enter the password for the user. Minimum 4 characters.   |
| <b>Confirm Password</b> | Re-enter the password for the user.  |
| <b>Email address</b>    | (Optional) Enter the user's email address.   |
| <b>Mobile number</b>    | (Optional) Enter the user's mobile phone number.   |

Table 8-3 User Management

| Field   | Description  |
|---|--|
| Group Membership                              | Select the user's group from the drop-down menu.                               |
| 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.

Table 8-4 Group Management

| Field           | Description  |
|-----------------|--|
| Existing Groups | To copy or modify a group, select the group from the drop-down menu. Click <b>Lookup</b> . |
| New Group Name  | Enter the new group's name.  |

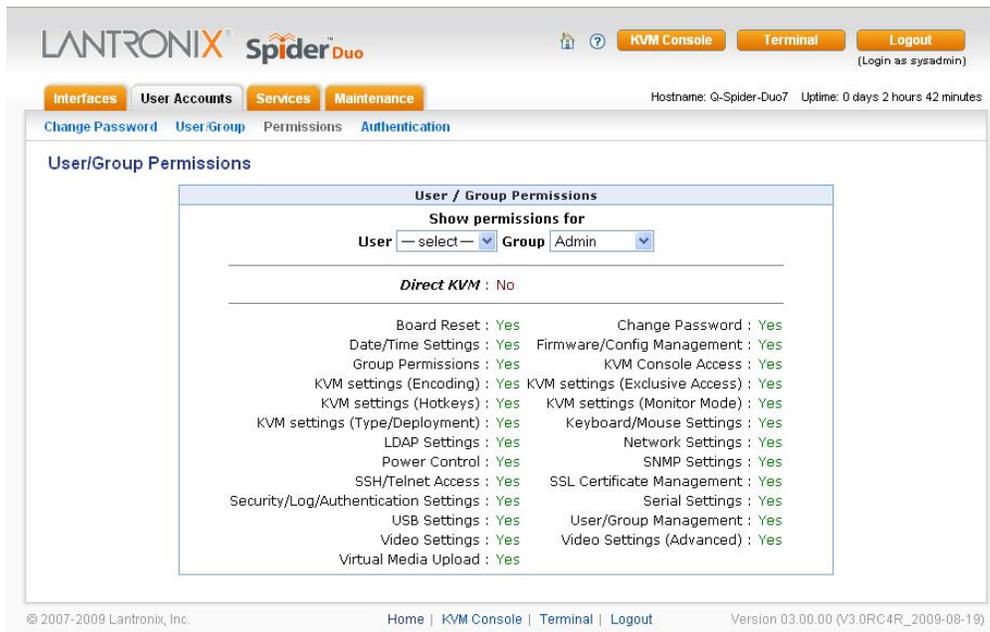
2. Do one of the following:
  - a. Click **Create** to add the new group.
  - b. Click **Modify** to change an existing group.
  - c. Click **Copy** to create a new group based on the selected existing group.
  - d. Click **Delete** to delete an existing group.
  - e. Click **Reset** to restore original settings.

## User Permissions

To modify user permissions, perform the following steps.

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

Figure 8-5 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 Java KVM console program.
    - b. Select **No** (default) to display the web page after login.
- 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 uses its own database to perform authentication. If one of the remote authentication protocols is selected, the Spider 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 8-6 Authentication Page

The screenshot shows the 'Authentication Settings' page in the Spider Duo web interface. The 'Local Authentication' radio button is selected. Below it, there are input fields for LDAP Server IP, LDAP Server Base DN, LDAP Server Type (set to 'Generic LDAP server'), User Search Sub-filter, Bind Name (set to 'sysadmin'), Bind Password, and Confirm Bind Password. The 'RADIUS' section is unselected and contains a table with columns: Server, Shared Secret, Auth. Port, Acc. Port, Timeout, and Retries. The table has one row with values: 1, Shared Secret, 1812, 1813, 1, and 3. Below the table is a button 'Add More Entries'. At the bottom of the form are buttons for 'Save', 'Reset to defaults', and 'Reset'. The footer of the page includes '© 2007-2009 Lantronix, Inc.', navigation links, and 'Version 03.00.00 (V3.0RC4R\_2009-08-19)'.

2. Modify the following field.

Table 8-7 Local Authentication

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

## LDAP

When you select LDAP Authentication, the Spider 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 contacts the specified LDAP server, which either approves or denies access.

Table 8-8 LDAP

| Field               | Description   |
|---------------------|---|
| LDAP Server IP      | Enter the name or IP address of the LDAP server, reachable over the network by the Spider, containing the user database. Be sure to configure a DNS server if a name rather than address is used. |
| 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 <b>Generic LDAP</b> and <b>Microsoft Active Directory</b> . If a Generic LDAP Server is selected, edit the LDAP scheme.     |

Table 8-8 LDAP (continued)

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

## RADIUS

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

Table 8-9 RADIUS

| Field                      | Description   |
|----------------------------|---|
| <b>Server</b>              | Enter the name or IP address of the RADIUS server, reachable over the network by the Spider, containing the user database. Configure a DNS server if a name rather than an address is used.   |
| <b>Shared Secret</b>       | A shared secret is a text string that serves as a password between the RADIUS client and RADIUS server. In this case the Spider 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).<br>Enter a maximum of 128 alphanumeric characters and symbols such as an exclamation point ("!") or an asterisk ("*"). |
| <b>Authentication Port</b> | The port the RADIUS server listens for authentication requests. The default value is <b>1812</b> .  |
| <b>Accounting Port</b>     | The port the RADIUS server listens for accounting requests. The default value is <b>1813</b> .  |
| <b>Timeout</b>             | 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 <b>1</b> second.  |
| <b>Retries</b>             | Sets the number of retries if a request could not be completed. The default value is <b>3</b> times.  |

1. 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.

# 9: Services

This chapter describes the Spider and SpiderDuo services. It contains the following sections:

- ◆ [Date/Time](#)
- ◆ [Security](#)
- ◆ [Certificate](#)
- ◆ [Event Log](#)
- ◆ [SNMP](#)
- ◆ [KVM Search](#)
- ◆ [Power Management](#)

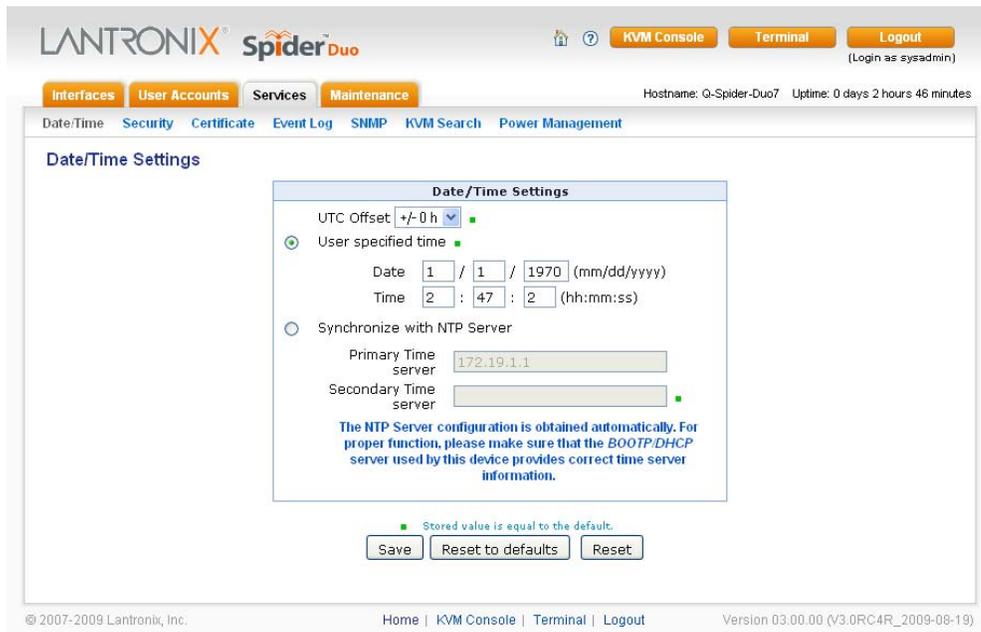
## Date/Time

The Spider 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 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   |
|------------------------------------|---|
| <b>UTC Offset</b>                  | Time servers deliver time as Coordinated Universal Time (UTC, or Greenwich Mean Time). Select the appropriate offset in hours $\pm$ from the drop-down menu.  |
| <b>User Specified Time</b>         | Manually input the current date and time. The Spider 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 $\pm 30$ ppm. |
| <b>Synchronize with NTP Server</b> | 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 with DNS server names.  |

3. 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.

## 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

The screenshot shows the Security Settings page for LANTRONIX Spider Duo. The page is divided into several sections:

- HTTP Encryption:** A checkbox for "Force HTTPS for Web access" is currently unchecked.
- Login Limitations:** A checkbox for "Enable Single Login Limitation" is currently unchecked.
- KVM Encryption:** Radio buttons for "KVM Encryption" are set to "Off".
- Authentication Limitation:** Two checkboxes are present: "Enable Screenshot Access without Authentication" (unchecked) and "Enable *Direct KVM* Console Access without Authentication" (unchecked). Below these are links for screenshot and KVM console access.
- Group based System Access Control:** A section with a note: "Please note: 'Save' is required, or changes will be lost." It includes a checkbox for "Enable Group based System Access Control" (unchecked) and a "Default Action" dropdown set to "ACCEPT". Below is a table with one rule:

| Rule # | Starting IP | Ending IP       | Group | Action |
|--------|-------------|-----------------|-------|--------|
| 1      | 0.0.0.0     | 255.255.255.255 | All   | ACCEPT |

Buttons for "Append", "Insert", "Replace", and "Delete" are located below the table. At the bottom, there are "Save", "Reset to defaults", and "Reset" buttons. A note indicates "Stored value is equal to the default." for the "ACCEPT" action.

2. Modify the following fields.

## HTTP Encryption

Table 9-4 HTTP Encryption

| Field                             | Description   |
|-----------------------------------|---|
| <b>Force HTTPS for Web Access</b> | Typically, the Spider listens on both HTTP and HTTPS ports for incoming connections. If this box is checked, access can only be made using SSL, and connection requests on the HTTP port will be ignored. See the section on Certificate for further information on how the Spider identifies itself using a cryptographic certificate. |

## Login Limitations

Table 9-5 Login Limitations

| Field                                 | Description  |
|---------------------------------------|--|
| <b>Enable Single Login Limitation</b> | 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. |

## KVM Encryption

Table 9-6 KVM Encryption

| Field          | Description   |
|----------------|---|
| KVM Encryption | In addition to the SSL encryption of the Spider's web pages, the keyboard, mouse, and video data may be encrypted. Select <b>Off</b> to use no encryption. Select <b>Try</b> for the Spider to attempt to make an encrypted connection but will back off to unencrypted if one cannot be established. Select <b>Force</b> for an encrypted connection to be made, or an error will be reported. |

## Group Based System Access Control

Table 9-7 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 <b>Accept</b> or <b>Drop</b> 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.   |
| Rule creation and editing                | <p>Spiders 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.</p> <ul style="list-style-type: none"> <li>◆ <b>Rule Number:</b> Defines where in the evaluation sequence this rule is to be applied.</li> <li>◆ <b>Starting and Ending IP Addresses:</b> Define the range over which the rule applies.</li> <li>◆ <b>Group:</b> Defines which user group is affected by this rule. Built-in groups include <b>Admin</b>, <b>All</b>, and <b>Unknown</b> (no group assigned). As additional groups are defined in <b>User Management→Users→Group Management</b>, they will appear in the drop-down. A rule can apply to only one group at a time.</li> <li>◆ <b>Action:</b> Chooses whether this is to be a <b>Drop</b> or <b>Accept</b> rule.</li> <li>◆ After a rule has been defined, it needs to go in the correct place in the list.</li> <li>◆ <b>Append:</b> Puts the rule at the end of the list. The rule number changes to reflect the last position on the list.</li> <li>◆ <b>Insert:</b> Puts the rule in the place on the list indicated by the rule number, renumbering and moving down the other rules to make room.</li> <li>◆ <b>Replace:</b> Deletes the previous rule of that number and replaces it with the new rule.</li> <li>◆ <b>Delete:</b> Deletes the rule of that number and moves the others up. Note that for a <b>Delete</b>, the fields other than the rule number do not need to be filled in.</li> </ul> |

## Authentication Limitation

Table 9-8 Authentication Limitation

| Field  | Description   |
|--|---|
| <b>Enable Screenshot Access without Authentication</b>         | Select this option when you need to access the snapshot image without logging in to the Spider. If enabled, the screenshot can be read directly with <code>http(s)://&lt;spiderIPaddress&gt;/screenshot.jpg</code> . One use of this unauthenticated screenshot is to read it from a Google gadget  |
| <b>Enable Direct KVM Console Access without Authentication</b> | Select this option to launch the Remote Console without authentication by entering the Spider's IP address ( <code>http(s)://(Spider IP address)</code> ) in the browser's <b>Address</b> field or type <code>javaws http(s)://(Spider IP address)</code> in the command line. To launch Spider web access type <code>http(s)://(Spider IP address)/home</code> in the browser's Address field. |

3. 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.

## Certificate

The Spider uses the Secure Socket Layer (SSL) protocol for any encrypted network traffic between itself and a connected client. During the connection establishment the Spider 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 Spiders and will not match the network configuration where it is installed. The certificate's underlying secret key is also used for securing the SSL 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. The Spider 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.

Figure 9-9 Certificate Signing Request Page

The screenshot shows the LANTRONIX Spider Duo web interface. At the top, there are navigation tabs for 'Interfaces', 'User Accounts', 'Services', and 'Maintenance'. Below these are sub-tabs for 'Date/Time', 'Security', 'Certificate', 'Event Log', 'SNMP', 'KVM Search', and 'Power Management'. The main content area is titled 'SSL Server Certificate Management' and contains a 'Certificate Signing Request (CSR)' form. The form has the following fields: 'Common name', 'Organizational unit', 'Organization', 'Locality/City', 'State/Province', 'Country (ISO code)', 'Email' (pre-filled with 'sysadmin'), 'Challenge password' (masked with dots), 'Confirm Challenge password', and 'Key length (bits)' (set to 1024). A 'Create' button is located at the bottom of the form. The footer of the page includes copyright information for Lantronix, Inc. and version details.

2. Modify the following fields.

Table 9-10 SSL Server Certificate Management

| Field   | Description   |
|---|---|
| <b>Common name</b>  | The network name of the Spider 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 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 is accessed using HTTPS. |
| <b>Organizational unit</b>                                    | This field specifies to the department within an organization to which the Spider belongs.  |
| <b>Organization</b>   | The name of the organization to which the Spider belongs.   |
| <b>Locality/City</b>  | The city where the organization is located.   |
| <b>State/Province</b>   | The state or province where the organization is located.  |
| <b>Country (ISO code)</b>                                     | The country where the organization is located. This is the two-letter ISO code (e.g., US for the United States).  |
| <b>Email</b>  | The email address of a contact person responsible for the Spider and its security.  |
| <b>Challenge password/<br/>Confirm Challenge<br/>password</b> | 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.   |
| <b>Key length (bits)</b>                                      | Select the key length from the drop-down menu.  |

3. Click **Create** to initiate the Certificate Signing Request generation. Download the CSR by clicking **Download**. The **Download** button displays when a certificate is created. Send the saved CSR to a CA for certification.
4. Click **Upload** to upload the certificate from the client computer to the Spider. The Spider now has its own certificate used for identifying itself to its clients.

## 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 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** page displays.

Figure 9-11 Event Log Page

The screenshot shows the 'Event Log Settings' page in the Spider Duo web interface. The page is divided into two main sections: 'Event Log Targets' and 'Event Log Assignments'.

**Event Log Targets:**

- List Logging Enabled. Below it, 'Entries shown per page' is set to 20. There is a 'Clear internal log' button and a 'Clear' button.
- NFS Logging Enabled. Below it are input fields for 'NFS Server', 'NFS Share', and 'NFS Log File' (containing 'evtlog').
- SMTP Logging Enabled. Below it are input fields for 'SMTP Server', 'Receiver Email Address', and 'Sender Email Address'.
- SNMP Logging Enabled. Below it are input fields for 'Destination IP' and 'Community'.

**Event Log Assignments:**

| Event          | List                                  |
|----------------|---------------------------------------|
| Board Message  | <input checked="" type="checkbox"/> * |
| Security       | <input checked="" type="checkbox"/> * |
| LDAP           | <input checked="" type="checkbox"/> * |
| Remote Console | <input checked="" type="checkbox"/> * |
| Host Control   | <input checked="" type="checkbox"/> * |
| Authentication | <input checked="" type="checkbox"/> * |

At the bottom of the page, there are 'Save', 'Reset to defaults', and 'Reset' buttons. A note indicates that a green square icon means 'Stored value is equal to the default.' The footer contains copyright information and version details.

2. Modify the following fields:

### Event Log Targets

Table 9-12 Event Log Targets

| Field                       | Description  |
|-----------------------------|--|
| <b>List Logging Enabled</b> | Check this box to use the internal log list of the Spider. 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, or when you click the <b>Clear</b> button. |
| <b>NFS Logging Enabled</b>  | The Spider 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.  |

Table 9-12 Event Log Targets

| Field                | Description  |
|----------------------|--|
| SMTP Logging enabled | With this option, the Spider 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 <b>SMTP Server</b> , the <b>Receiver Email Address</b> , and <b>Sender Email Address</b> . Enter the mail server and SMTP port as <code>&lt;serverip&gt;:&lt;port&gt;</code> . |
| SNMP Logging Enabled | If selected, the Spider sends an SNMP trap to a specified destination IP address every time a log event occurs. Configure the <b>Destination IP</b> and <b>Community</b> . View the SNMP MIB implemented in the Spider by clicking on the <b>Spider SNMP MIB</b> link.   |

## Event Log Assignments

Table 9-13 Event Log Assignments

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

3. 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.

## SNMP

The Spider has an internal SNMP agent that has various objects accessible in its MIB. It also can generate traps based on events. The Spider 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 9-14 SNMP Settings Page

The screenshot shows the LANTRONIX Spider Duo web interface. The main content area is titled 'SNMP Settings'. It contains a form with the following fields and options:

- Enable SNMP Agent
  - System Location: [text input]
  - System Contact: [text input]
- Use SNMPv3
  - DES Encryption:  Off  Force
  - Read-Only User Name: [text input with value 'sysadmin']
  - Read-Only Password: [password input with asterisks]
  - Read-Write User Name: [text input]
  - Read-Write Password: [password input]
- Use SNMPv1
  - Read Community: [text input with value 'public']
  - Write Community: [text input with value 'private']

At the bottom of the form, there is a link: 'Click here to view the SNMP MIB'. Below the form are three buttons: 'Save', 'Reset to defaults', and 'Reset'. A small green square icon indicates 'Stored value is equal to the default.' for several fields.

2. Modify the following fields.

Table 9-15 SNMP Settings

| Field             | Description   |
|-------------------|---|
| Enable SNMP Agent | Click the checkbox to enable the Spider 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: <ul style="list-style-type: none"> <li>◆ <b>DES Encryption:</b> Select whether to turn off or enable encryption with Data Encryption Standard (DES),</li> <li>◆ <b>Read Username:</b> User ID for a user with read-only authority to use to access SNMP v3.</li> <li>◆ <b>Read Password:</b> Password for a user with read-only authority to use to access SNMP v3. Up to 32 characters.</li> <li>◆ <b>Write Username:</b> Enter a user ID for users with read-write authority. Up to 32 characters.</li> <li>◆ <b>Write Password:</b> Enter a password for the user with read-write authority to use to access SNMP v3. Up to 20 characters.</li> </ul> |
| Use SNMPv1        | Select to use SNMPv1 (rather than SNMPv3) and enter the following: <ul style="list-style-type: none"> <li>◆ <b>Read Community:</b> Enter the SNMP read community name. The default is <b>public</b>.</li> <li>◆ <b>Write Community:</b> Enter the SNMP write community name. The default is <b>private</b>.</li> </ul>  |

3. 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.

## KVM Search

The KVM Search option enables you to view the properties of other Spiders 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 9-16 KVM Search Page

LANTRONIX SpiderDuo

KVM Console Terminal Logout (Login as sysadmin)

Interfaces User Accounts Services Maintenance

Hostname: steven-Vista Uptime: 3 days 16 hours 53 minutes

Date/Time Security Certificate Event Log SNMP KVM Search Power Management

### KVM Search

20 Lantronix SLSLP found.

| No. | IP/Web         | Hostname               | Direct KVM | Preview | Terminal | SSH | Telnet | MAC Address       | Model | Ver. | Descr.    |
|-----|----------------|------------------------|------------|---------|----------|-----|--------|-------------------|-------|------|-----------|
| 1   | 172.19.100.15  | steven-Vista           | N/A        | N/A     | N/A      | Yes | No     | 00:81:A3:8C:00:02 | PS2-D | 1.0  | Standard  |
| 2   | 172.19.100.127 | SLSa38c0001            | N/A        | N/A     | N/A      | Yes | No     | 00:81:A3:8C:00:01 | USB-D | 1.0  | Standard  |
| 3   | 172.19.238.75  |                        | N/A        | N/A     | N/A      | Yes | No     | 00:20:4A:80:8A:ED | PS2   | 2.2  | V2.2RC1_2 |
| 4   | 172.19.100.26  |                        | KVM        | Preview | Terminal | Yes | Yes    | 00:80:A3:8C:4F:64 | USB-D | 3.1  | V3.1RC1R_ |
| 5   | 172.19.215.52  | DaveSLS                | N/A        | N/A     | N/A      | Yes | Yes    | 00:80:A3:8C:0C:94 | USB   | 2.2  | V2.2RC1_2 |
| 6   | 172.19.208.2   | sls-sunset2-<br>proto1 | KVM        | Preview | Terminal | Yes | Yes    | 00:80:A3:8C:00:17 | PS2-D | 3.1  | V3.1RC1R_ |
| 7   | 172.19.208.5   | sls-sunset5            | N/A        | N/A     | N/A      | Yes | No     | 00:80:A3:8C:28:57 | USB   | 3.0  | V3.0RC7R_ |
| 8   | 172.19.100.1   |                        | N/A        | N/A     | N/A      | Yes | Yes    | 00:80:A3:8C:00:46 | PS2   | 3.0  | V3.01_201 |
| 9   | 172.19.38.102  | Spider-LinuxBrg        | KVM        | N/A     | N/A      | Yes | Yes    | 00:20:4A:80:8C:06 | PS2   | 3.0  | V3.01_201 |
| 10  | 172.19.208.6   | sls-sunset6            | N/A        | N/A     | N/A      | Yes | No     | 00:80:A3:8C:08:06 | PS2-D | 3.0  | V3.01_201 |
| 11  | 172.19.38.110  | Spider-Mac             | KVM        | Preview | N/A      | Yes | Yes    | 00:80:A3:8C:00:14 | USB   | 3.0  | V3.01_201 |
| 12  | 172.19.208.11  | sls-sunset11           | KVM        | Preview | N/A      | Yes | No     | 00:20:4A:80:8D:59 | USB-D | 3.1  | V3.1RC1R_ |
| 13  | 172.19.226.50  |                        | KVM        | N/A     | N/A      | Yes | Yes    | 00:80:A3:8C:00:25 | USB   | 2.2  | V2.2_2009 |
| 14  | 172.19.38.108  | SpiderG-108            | KVM        | Preview | N/A      | Yes | Yes    | 00:80:A3:8C:1D:8C | PS2   | 3.0  | V3.01_201 |
| 15  | 172.19.231.99  | avi-dsm                | KVM        | Preview | N/A      | Yes | Yes    | 00:80:A3:8C:01:61 | PS2   | 2.2  | V2.2RC1_2 |
| 16  | 172.19.208.12  | sls-sunset12           | KVM        | Preview | N/A      | Yes | No     | 00:20:4A:80:8D:B3 | PS2-D | 3.1  | V3.1RC1R_ |
| 17  | 172.19.208.4   | sls-sunset4            | N/A        | N/A     | N/A      | Yes | Yes    | 00:80:A3:8C:16:76 | PS2   | 3.0  | V3.0RC7R_ |
| 18  | 172.19.208.7   | sls-sunset7            | KVM        | Preview | Terminal | Yes | Yes    | 00:20:4A:80:8D:58 | USB-D | 3.1  | V3.1RC1R_ |
| 19  | 172.19.100.162 |                        | N/A        | N/A     | N/A      | Yes | No     | 00:20:4A:80:8D:9F | USB-D | 3.0  | V3.0_2009 |
| 20  | 172.19.100.2   | SLS4a8984ee            | KVM        | Preview | N/A      | Yes | No     | 00:20:4A:89:84:EE | PS2-D | 3.0  | V3.01_201 |

© 2007-2009 Lantronix, Inc. Home | KVM Console | Terminal | Logout Version 01.00.00 (Standard Edition)

## Power Management

The Power Management option enables you to manage the properties of the power system. It enables the monitoring of the Power Control Unit (PCU) that only applies to the SpiderDuo, and the sending of Wake-On-LAN (WOL) messages to a computer that has WOL enabled.

To view the Power Management page, perform the following steps.

1. Click **Services > Power Management**. The Power Management page displays.

Figure 9-17 Power Management Page

LANTRONIX Spider Duo

Interfaces User Accounts Services Maintenance

Hostname: steven-Vista Uptime: 3 days 17 hours 21 minutes

Date/Time Security Certificate Event Log SNMP KVM Search Power Management

### Power Management

Power pcu interface changed successfully.

**Power Outlet**

Power PCU Interface: Enabled

Enable/Disable Power PCU Interface requires reboot to take effect.

PCU Status: Disconnected

Power Status: Unknown

**Wake On LAN**

Send to the MAC address below

MAC Address  Password

Send to the following devices

| Device Name          | IP Address           | MAC Address          | Password             |
|----------------------|----------------------|----------------------|----------------------|
| <input type="text"/> | <input type="text"/> | <input type="text"/> | <input type="text"/> |

To remove entry from table, clear 'Device Name' and click 'Save'

Stored value is equal to the default.

© 2007-2009 Lantronix, Inc. Home | KVM Console | Terminal | Logout Version 01.00.00 (Standard Edition)

The Power Management web page contains two sections as displayed in Figure 9-17. The upper portion displays information about the SpiderDuo PCU. The PCU only applies to the SpiderDuo. The WOL applies to both the Spider and SpiderDuo devices.

## SpiderDuo Power Control Unit

The SpiderDuo Power Control Unit section of the web page contains the power and PCU status. You can also enable or disable the PCU which requires a reboot.

To enable the PCU, perform the following steps.

1. Click **Enable**. A warning displays requesting that you confirm.
2. Click **Confirm Enable**. The message that the enable was successful.
3. Reboot for the change to take effect.

## Wake-On LAN

Wake-On-LAN (WOL, sometimes WoL) is an Ethernet computer networking standard that allows a computer to be turned on or woken up remotely by a network message sent usually by a program executed on another computer on the network.

The WOL requests get generated and sent to a single machine or group of devices. If a single machine is selected (via the first radio button), the MAC address for the selected device must be supplied. If no password is needed, the password field maybe left blank.

If the second radio button is selected, the WOL message may be sent to any number of devices identified by a Device Name, IP Address (optional), or MAC address (entered into the respective text boxes). If no password is needed, this field should be left blank.

WOL support is implemented on the motherboard of a computer and the network interface and is not dependent on the operating system running on the hardware, although the operating system can sometimes control the WOL behavior. Refer to your motherboard and operating system user guide for configuration information.

### **Enable WOL**

To enable WOL, perform the following steps.

1. Enter the MAC address and password in the **Send to the MAC address below** field.

1. Click **Wake Up**.

Or

2. Enter the device name, IP address, MAC address, and password in the **Send to the following devices** field.

3. Click **Add More Entries** if required. Repeat Step 2 for each additional entry.

4. Click **Wake Up**.

### **Remove Entries, Reset to Defaults, or Reset**

To remove an entry from the **Send to the following devices** table, clear the **Device Name** field and click **Save**.

To reset to defaults, click **Reset to Defaults**.

To reset, click **Reset**.

# 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](#)
- ◆ [Update Firmware](#)
- ◆ [View Event Log](#)
- ◆ [Unit Reset](#)
- ◆ [iGoogle Gadgets](#)

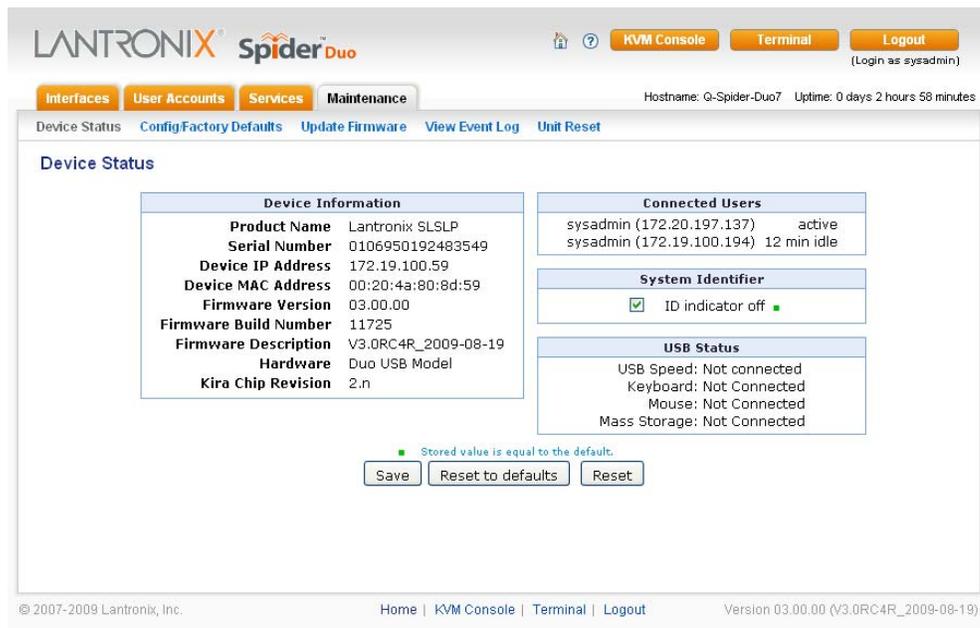
## Device Status

The Device Status page contains a table with information about the Spider'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, board ID, device IP address, device MAC address, firmware version, firmware build number, firmware description, hardware, and Kira chip revision. |

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 ID indicator on and off. Each Spider 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. |
| USB Status        | Displays the USB speed, keyboard, mouse, and mass storage status.   |

3. 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.

## Configuration

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

The screenshot shows the Lantronix Spider Duo Configuration Page. The page is titled "Configuration" and has a navigation bar with tabs for "Interfaces", "User Accounts", "Services", and "Maintenance". The "Maintenance" tab is selected. Below the navigation bar, there are links for "Device Status", "Config/Factory Defaults", "Update Firmware", "View Event Log", and "Unit Reset". The "Config/Factory Defaults" link is selected.

The main content area is divided into two sections: "Configuration Backup" and "Configuration Restore".

**Configuration Backup:** This section has two radio buttons. The first, "Backup and save to Spider", is selected. The second, "Backup and save to your computer", is unselected. A warning message states: "Warning: Execution of 'backup to spider' option, will overwrite the backup file if existed." Below the radio buttons are two buttons: "Backup" and "Restore".

**Configuration Restore:** This section has two radio buttons. The first, "Restore from config file on Spider", is selected. The second, "Upload and restore from config file saved on your computer", is unselected. Below the radio buttons is a "Config File" input field with a "Browse..." button. Below the input field are two checkboxes under the heading "Preserve Following Settings": "Network Basic" and "VIP". A warning message states: "Warning: Execution of this option, will overwrite the current configuration settings with the selected config file settings and reboot the stvn-spdr-Vista." Below the checkboxes is an "Upload" button.

The footer of the page includes copyright information: "© 2007-2009 Lantronix, Inc.", navigation links: "Home | KVM Console | Terminal | Logout", and version information: "Version 01.00.00 (Standard Edition)".

2. Edit the following fields.

**Table 10-4 Configuration Settings**

| Field                 | Description  |
|-----------------------|--|
| Configuration Backup  | <p>To back up all settings to a file on the client system, click the <b>Backup and save to your computer</b> radio button. To save to a Spider, click the <b>Backup and save to Spider</b> radio button. Then, click Backup.</p> <p><b>Warning:</b> <i>Execution of the Backup and save to Spider option overwrites the backup file.</i></p>   |
| Configuration Restore | <p>To return the Spider settings to a previously saved configuration:</p> <ul style="list-style-type: none"> <li>◆ Click the <b>Restore from Config File on Spider</b> radio button or <b>Upload and restore from config file saved on your computer</b> radio button. You can then browse to and select the saved configuration file.</li> <li>◆ In the <b>Preserve Following Settings:</b> field, click Network Basic or VIP. Click the <b>Network Basic</b> 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 <b>VIP</b> checkbox to preserve the VIP settings.</li> <li>◆ Click the <b>Upload</b> button. If you select this option, the Spider reboots after you apply the update.</li> </ul> <p><b>Warning:</b> <i>Execution of Upload function overwrites the current configuration settings with the selected configuration file settings and reboots the host.</i></p> |
| Factory Defaults      | <p>To preserve the factory defaults, click the Network Basic or VIP checkbox. Then click the Restore button.</p> <p><b>Warning:</b> <i>Execution of this option restores the current configuration settings to the factory default settings and reboots the host.</i></p>  |

## Update Firmware

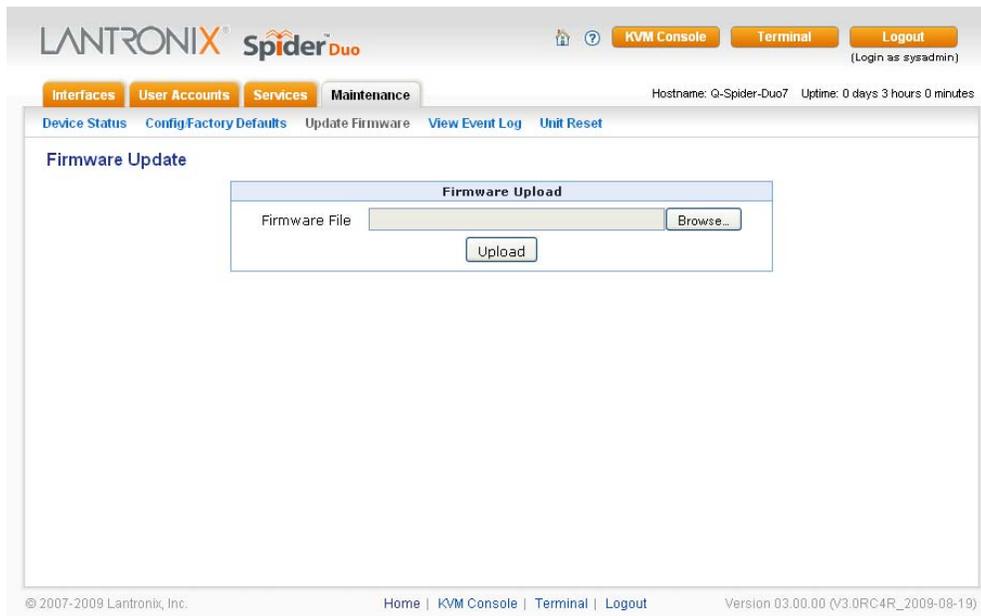
Many of the functions and features of the Spider are implemented in firmware and capable of field upgrades. The latest firmware may be found at [www.lantronix.com](http://www.lantronix.com). The firmware file, when uncompressed, is approximately 4 Mbytes in size and has a .bin suffix.

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

To update Spider 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 10-5 Update Firmware Page



3. Click **Browse**. In the pop-up window, navigate and locate the firmware file.
4. Click **Upload** to copy the file into the Spider'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 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 10-6 Event Log Page

The screenshot shows the LANTRONIX Spider Duo web interface. The top navigation bar includes 'KVM Console', 'Terminal', and 'Logout'. Below this, there are tabs for 'Interfaces', 'User Accounts', 'Services', and 'Maintenance'. The 'Maintenance' tab is active, and the 'Event Log' sub-tab is selected. The main content area displays the 'Event Log' page, which contains a table of system events. The table has three columns: 'Date', 'Event', and 'Description'. The events listed include Remote Console connections, Authentication for 'sysadmin', and Board Messages for device initialization. The footer of the page shows the copyright information for Lantronix, Inc. and the version number 03.00.00 (V3.0RC4R\_2009-08-19).

| Date                | Event          | Description  |
|---------------------|----------------|--|
| 01/01/1970 02:45:29 | Remote Console | Connection to client 172.19.100.194 closed.              |
| 01/01/1970 02:40:04 | Remote Console | Connection to client 172.19.100.194 established.         |
| 01/01/1970 02:39:45 | Authentication | User 'sysadmin' logged in from IP address 172.20.197.137 |
| 01/01/1970 02:39:44 | Authentication | User 'sysadmin' logged in from IP address 172.19.100.194 |
| 01/01/1970 02:03:23 | Authentication | User 'sysadmin' logged in from IP address 172.19.100.251 |
| 01/01/1970 01:03:02 | Remote Console | Connection to client 172.20.197.137 closed.              |
| 01/01/1970 01:01:57 | Remote Console | Connection to client 172.20.197.137 established.         |
| 01/01/1970 00:58:37 | Remote Console | Connection to client 172.20.197.137 closed.              |
| 01/01/1970 00:54:50 | Remote Console | Connection to client 172.20.197.137 established.         |
| 01/01/1970 00:50:57 | Authentication | User 'sysadmin' logged in from IP address 172.20.197.137 |
| 01/01/1970 00:10:03 | Authentication | User 'sysadmin' logged in from IP address 172.20.197.137 |
| 01/01/1970 00:08:45 | Remote Console | Connection to client 172.19.100.194 closed.              |
| 01/01/1970 00:06:27 | Remote Console | Connection to client 172.19.100.194 established.         |
| 01/01/1970 00:06:13 | Authentication | User 'sysadmin' logged in from IP address 172.19.100.194 |
| 01/01/1970 00:01:22 | Board Message  | Device successfully started.                             |
| 01/01/1970 00:01:21 | LDAP           | Initialized successfully.                                |
| 01/01/1970 00:01:22 | Board Message  | Device successfully started.                             |
| 01/01/1970 00:01:22 | Board Message  | Device successfully started.                             |
| 01/01/1970 00:01:21 | LDAP           | Initialized successfully.                                |
| 01/01/1970 02:54:25 | Authentication | User 'sysadmin' logged in from IP address 172.19.100.194 |

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

## Unit Reset

In general, the Spider 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.

To reset the Spider, perform the following steps.

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

Figure 10-7 Unit Reset Page



3. Click the **Reset** button for **Reset Keyboard/Mouse (PS/2)**, **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.*

4. To perform a complete reset, click **Reset Device**. A prompt requesting confirmation displays. A complete reset closes all user connections and performs a full reboot.

## iGoogle Gadgets

You can create an iGoogle gadget that enables you to view and access multiple Spiders on one web page. You access a snapshot of each of the Spider's Remote Console without logging in to the Spider.

Technically, the number of Spiders that can be viewed and accessed on one web page is unlimited. It is important to note that the more Spiders that are added, the slower the response time will be.

Anyone with a Google email account (gmail.com) can create an iGoogle gadget for viewing web pages. There are two types of iGoogle gadgets: public gadgets and private gadgets. When you submit a gadget's XML code to Google, it becomes part of the iGoogle public gadgets, which are listed for import on iGoogle web pages. When a gadget's XML code is stored on a private server, the gadget stays private and is usable only by users who are aware of its location.

To use iGoogle gadget to manage multiple Spiders, perform the following steps.

1. Click **Services > Security**.
2. In the Authentication Limitation section, select the **Enable Screenshot Access without Authentication** check box.

3. Edit a file similar to the example below and save it with extension "xml." This example assumes the file is saved as spider1.xml. The sample code displays a snapshot and refreshes the image every minute. Also, clicking the snapshot opens the remote console program or spider web page, depending on your settings.

```
<?xml version="1.0" encoding="UTF-8" ?>
<Module>
<ModulePrefs title="Spider Preview (Your Spider IP Address)"
height="240" scaling="false" />
<Content type="html">
<![CDATA[
<center>
<div>

</div>
<script>
var c = 0
var t
function updateSpiderSnapshot()
{
    document.getElementById('sp_img').src = "http://(your Spider IP
address)/screenshot.jpg?rnum=" + c;
    c = c + 1
    t = setTimeout("updateSpiderSnapshot()", 60000) // 60 sec
}
updateSpiderSnapshot();
</script>
]]>
</Content>
</Module>
```

4. Upload the edited xml file (spider1.xml) to a web server that is accessible over the Internet.
5. Enter the URL <http://www.google.com/ig>.
6. Log in to your iGoogle account.
7. Click **Add Stuff**.
8. Click **Add feed or gadget**.
9. Enter [http://\(your internet web server IP address\)/spider1.xml](http://(your internet web server IP address)/spider1.xml) and click **Add**.
10. In response to a Google pop-up a warning, click **OK**.
11. Click **Back to homepage**. You should see an iGoogle gadget similar to [Figure 10-8](#).

Figure 10-8 iGoogle Gadget Page



# 11: ManageLinx Integration and Configuration

This chapter describes uploading the ManageLinx VIP Access Bootstrap XML configuration file that enables the VIP Access functionality on the Spider and Spider Duo. The Spider family VIP Access feature provides secure remote access to virtually any computer via Lantronix provision ManageLinx System.

The Lantronix ManageLinx technology solves the access-through-firewall issue by using the existing network infrastructure to create a virtual device network (VDN). ManageLinx is a secure and totally transparent remote access solution.

VDN provides direct access to authorized equipment only, behind firewalls, from anywhere via the Internet. VDN technology creates a dedicated TCP/IP tunnel between any two private network-specific devices by using easily deployed hardware appliances. There is no client software to install. No changes are required to network software or applications at either end of the connection.

The VDN hardware consists of a publicly accessible Device Services Manager (DSM) and individual Device Services Controller (DSC) appliances in multiple locations. The secure encrypted tunnel is created between the two DSCs through the DSM. The DSM and DSC components enable the set up and management of individual VIP addresses and Routes. The Spider and SpiderDuo with the VIP Access feature enabled takes the place of a DSC and provides direct access to your equipment.

Once the Spider/SpiderDuo ManageLinx VIP Access Bootstrap XML file has been installed and VIP Access (Conduit) enabled, the Spider opens an encrypted secure Conduit connection to the ManageLinx DSM using the information in the bootstrap file. Once the Conduit has been established, the DSM allows other devices to open direct and secure KVM Console sessions (SSL only) through the ManageLinx DSM configured VIP Route Tunnel. Refer to the *ManageLinx Users Guide* for help on configuring the DSM.

This chapter contains the following sections:

- ◆ [Upload a Bootstrap File With Spider](#)
- ◆ [Upload a Bootstrap File With SpiderDuo](#)

## Upload a Bootstrap File With Spider

The Spider's Bootstrap file is created on the ManageLinx DSM and stored locally on a PC. The file contains all of the information about the DSM and the necessary credentials to establish a secure and encrypted Conduit/Tunnel connection with the DSM.

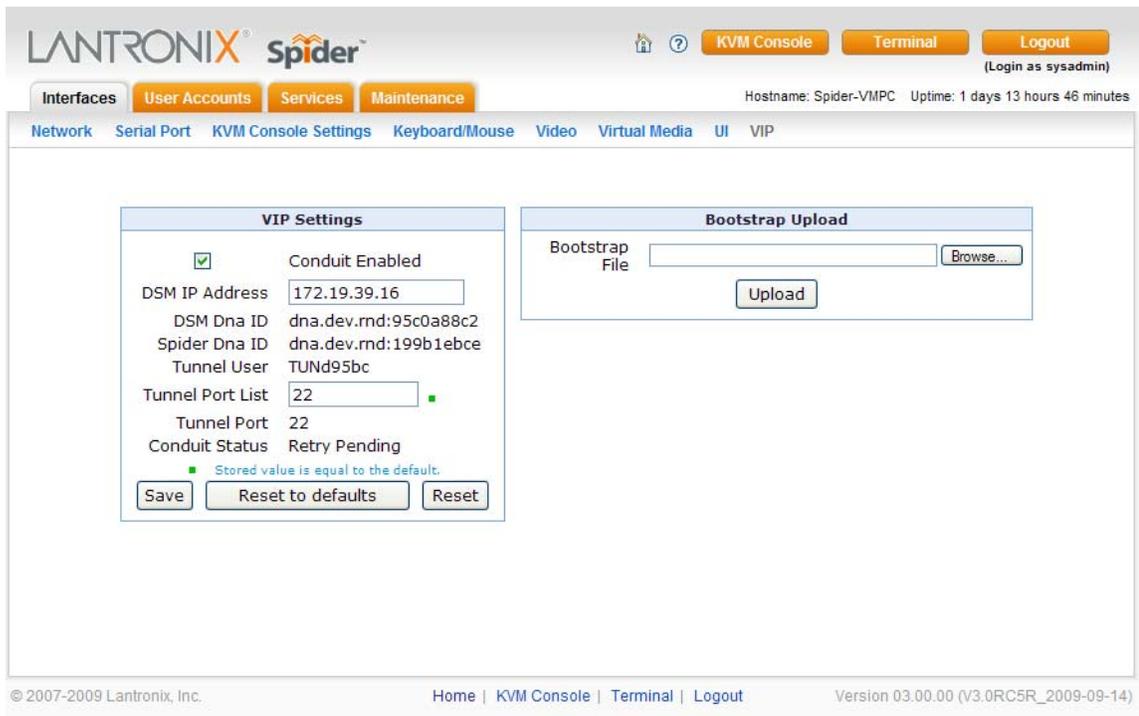
**Note:** Usable on ManageLinx v1.2 or greater.

To upload a bootstrap file, perform the following steps.

1. Access the Spider by using the Web Manager or Spider View.
2. Click **Interfaces > VIP**. [Figure 11-1](#) shows the page that displays.

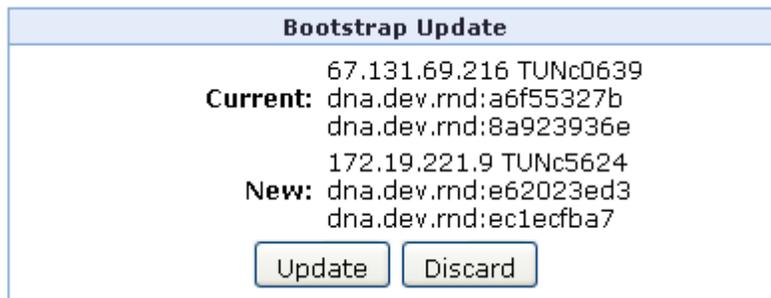
**Note:** Prior to uploading the Bootstrap XML file retrieved from the DSM, ensure that the Spider VIP Access feature is disabled. To disable VIP Access, uncheck the **Conduit Enabled** box and click **Save**.

Figure 11-1 Spider VIP Page



3. In the **Bootstrap Upload** section, click **Browse**.
4. Find the file to upload and click **Upload**.
5. At the Bootstrap Update window, click **Update**.

Figure 11-2 Spider Bootstrap Update Screen



6. After the upload completes, enable the VIP Access feature by checking the **Conduit Enabled** box and clicking **Save**. The Conduit Status will show Connected when the Spider/SpiderDuo has successfully established a Conduit session with the ManageLinX DSM.

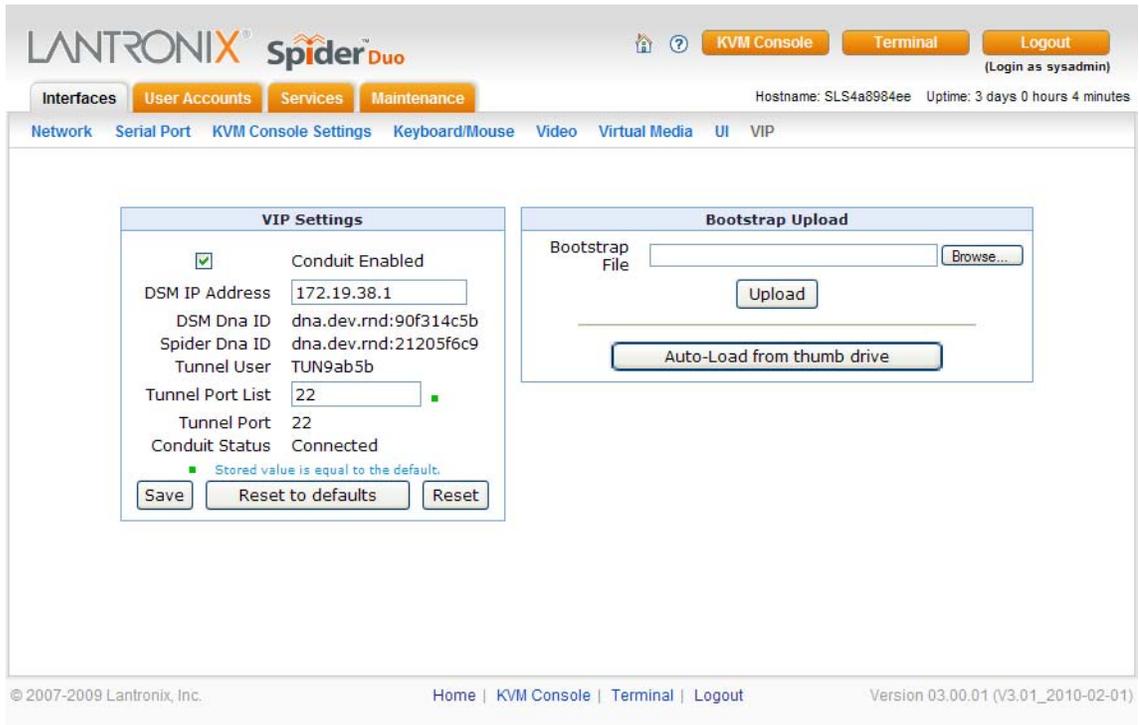
## Upload a Bootstrap File With SpiderDuo

The SpiderDuo supports using a USB Thumb Drive as an additional method of uploading the ManageLinX VIP Access Bootstrap XML file. To upload the ManageLinX VIP Access Bootstrap XML file, perform the following steps:

1. Copy the ManageLinX VIP Access Bootstrap XML file to your USB Thumb Drive (making sure no other files exist on the drive).

2. Remove and insert the USB Thumb Drive directly into the SpiderDuo USB port (on the Spider Duo, not the cable).
3. Using a PC with a Web Browser, access and login to the SpiderDuo with a username that has VIP configuration permissions, such as sysadmin.
4. Click the **Interfaces** tab, then the **VIP** link (see [Figure 11-3](#)).

**Figure 11-3 SpiderDuo VIP Page**



**Note:** Prior to uploading the Bootstrap XML file retrieved from the DSM, make sure the Spider VIP Access feature is disabled. To disable VIP Access uncheck the 'Conduit Enabled' box and clicking the 'Save' button

5. Click **Auto-Load from thumb drive**.
6. Click **Update** on the Bootstrap Update pop-up message box as shown in [Figure 11-4](#).
7. After the upload completes, enable the VIP Access feature by checking the **Conduit Enabled** box and clicking **Save**. The Conduit Status will show Connected when the SpiderDuo has successfully established a Conduit session with the ManageLinx DSM.

**Figure 11-4 SpiderDuo Bootstrap Update Window**



Accessing the Spider/SpiderDuo via its VIP Access tunnel requires HTTPS for connections. Non SSL Web connections (HTTP) are not supported. After the Conduit has been established, remote users can access the Spiders via a ManageLinx DSM defined VIP Route IP address that is on the remote user IP subnet (https://(VIP Route IP Address)).

## 12: Command Reference

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

- ◆ [Command Syntax](#)
- ◆ [Configuration Commands](#)
- ◆ [Connect Commands](#)
- ◆ [VIP Commands](#)
- ◆ [User Group Commands](#)
- ◆ [OEM Customization Commands](#)
- ◆ [Power Commands](#)
- ◆ [Serial Port Commands](#)
- ◆ [WOL \(Wake on LAN\) Commands](#)
- ◆ [USB Host Disk Commands](#)
- ◆ [Reboot Commands](#)
- ◆ [Diagnostic Commands](#)
- ◆ [Group Permissions](#)

### 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 12-1 Action and Category**

| Action         | Category  |
|----------------|---|
| <b>set</b>     | datetime   device   group   history   network   oem   power   security   serial   sshkey   user   vip             |
| <b>show</b>    | datetime   device   group   history   network   oem   power   security   serial   sshkey   sysconfig   user   vip |
| <b>connect</b> | serial   wakeonlan  |
| <b>diag</b>    | ping   ping6  |
| <b>usbhost</b> | disk  |

Table 12-1 Action and Category (continued)

| Action | Category                  |
|--------|---------------------------|
| admin  | config   reboot   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`.

## Configuration Commands

### admin config

#### 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 - VIP.

**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 show****Syntax**

```
admin config show
```

**Parameters**

None

**Description**

Shows the current configuration.

**admin config save****Syntax**

```
admin config save
```

**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 restore****Syntax**

```
admin config restore
```

**Parameters**

None

**Description**

Restores a saved configuration.

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

## Connect Commands

**connect serial****Syntax**

```
connect serial
```

**Description**

Connects the Spider to a device serial port.

**Note:** To connect to a serial port, put the serial port in passthrough mode on the web interface.

**ESC exit**

**Syntax**

ESC exit

**Description**

Available only when connected to a serial port.

## SSH Key Commands

**set sshkey delete**

**Syntax**

```
set sshkey delete keyuser <SSH Key User> keyhost <SSH Key Host>
```

**Description**

Deletes an imported SSH key.

**Examples**

To delete an imported SSH public key on host **slm-pipe** for the sysadmin user, enter the following CLI:

```
set sshkey delete keyuser sysadmin keyhost slm-pipe
```

**set sshkey import**

**Syntax**

```
set sshkey import <copypaste> format <openssl> keyuser <SSH Key User>
keyhost <SSH Key Host>
```

**Description**

Imports public SSH key (OpenSSH format)

**Examples**

To import a public key in OpenSSL format on host **slm-pipe** for the sysadmin user, enter the following CLI:

```
set sshkey import copypaste format openssl keyuser sysadmin keyhost
slm-pipe
```

**Note:** RSA keys must be 1024 bits

**show sshkey import**

**Syntax**

```
show sshkey import <one or more parameters>
```

### Parameters

```
[keyuser <SSH Key User>]
[keyhost <SSH Key IP Address or Name>]
[viewkey <enable|disable>]
```

### Description

Displays imported SSH keys.

### Examples

To display all imported SSH public keys with content of keys, enter the following CLI:

```
show sshkey viewkey enable
```

To displays an imported SSH public key on host **slm-pipe** for the sysadmin user, enter the following CLI:

```
show sshkey keyuser sysadmin keyhost slm-pipe
```

## 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.

## Network Commands

### **set network gateway**

**Note:** *The set network gateway command is deprecated with this release. See set network basic.*

### **set network**

#### 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|bootp|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

```

bwlimit <8-10000 kbit/s>
httpsports <TCP Port>
httpport <TCP Port>
proxy <enable/disable>
proxyhost <IP Address>
proxyport <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>
```

### 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 all****Syntax**

```
show network all
```

**Description**

Displays all network settings.

## Version Command

**admin version****Syntax**

```
admin version
```

**Description**

Displays firmware version information.

## Date/Time Command

### 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.

## VIP Commands

### set vip

#### Syntax

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

#### Parameters

```
[conduit <enable|disable>]
```

```
[dsmip <IP Address>]
```

```
[tunnelportlist <Tunneling port list>]
[configportlist <Configuration port list>]
[tunnelport] <Current tunneling TCP port>
[configport] <Current configuration TCP Port>
```

### Examples

To set a VIP tunnel port list to ports 22 and 30, enter the following CLI:

```
set vip tunnelingportlist 22,30
```

### Description

Configures VIP parameters to connect to DSM. It is recommended that you import the settings from a bootstrap file created on the DSM.

### show vip

#### Syntax

```
show vip
```

#### Description

Displays the VIP settings.

### show vip all

#### Syntax

```
show vip all
```

#### Description

Displays all VIP settings.

## 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' 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 119](#) 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.

## Security Commands

**set security****Syntax**

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

**Parameters**

```
[forcehttps <enable|disable>]  
[singlelogin <enable|disable>]  
[kvmencryption <off/try/force>]  
[screenshot <enable|disable>]  
[directkvm <enable|disable>]
```

**Description**

Sets security parameters.

**show security****Syntax**

```
show security
```

**Description**

Displays security parameters.

## Sysconfig Commands

**show sysconfig****Syntax**

```
show sysconfig
```

**Description**

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

## Device Commands

**set device****Syntax**

```
set device add | edit <Device Name> macaddress <MAC Address> [parameters]
```

**Parameters**

```
ipaddress <IP Address>
```

```
password <Password>
```

**Note:** MAC address must be in hex form: XX:XX:XX:XX:XX:XX.

**Description**

Configures devices.

**set device delete****Syntax**

```
set device delete <Device Name>
```

**Description**

Deletes a device.

**show device****Syntax**

```
show device
```

**Description**

Displays devices.

**show device all****Syntax**

```
show device all
```

**Description**

Displays all devices.

**show device name****Syntax**

```
show device name
```

**Description**

Displays device names.

## OEM Customization Commands

**set oem****Syntax**

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

**Parameters**

```
[product <Product Name>]
```

```
[company <Company Name>]
```

```
[copyright <Copyright>]
```

```
[url <URL>]
```

```
[title <Title>]
```

**Examples**

To set the product name as MyKVM and the company name as MyCompany, enter the following CLI:

```
set oem product MyKVM company MyCompany
```

**Description**

Sets product/company specific information on the web interface.

**show oem****Syntax**

```
show oem
```

**Description**

Displays OEM settings.

## Power Commands

**set power <parameters>**

### Syntax

```
set power <parameters>
```

### Parameters

```
[state <on/off>]
```

### Description

Sets PCU parameters.

**show power**

### Syntax

```
show power
```

### Description

Displays PCU status and settings.

## Serial Port Commands

**set serial mode**

### Syntax

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

### Parameters

```
[baud <300-115200>]
```

```
[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.

## WOL (Wake on LAN) Commands

### **connect wakeonlan device**

#### **Syntax**

```
connect wakeonlan device [Device Name]
```

#### **Description**

Sends a WOL packet to a specified device.

### **connect wakeonlan macaddr**

#### **Syntax**

```
connect wakeonlan macaddr [MAC Address] [password <Password>]
```

**Note:** MAC address must be in hex format: 'XX:XX:XX:XX:XX:XX'

#### **Description**

Sends a WOL packet to specified MAC address.

## USB Host Disk Commands

**Note:** The following USB Host Disk commands are available for the SpiderDuo only.

### **usbhost disk mount drive**

#### **Syntax**

```
usbhost disk mount drive
```

#### **Description**

Mounts a USB thumb drive to use as a storage device. The USB thumb drive must be formatted with an fat filesystem and drive must support USB high speed mode.

### **usbhost disk unmount drive**

#### **Syntax**

```
usbhost disk unmount drive
```

#### **Description**

Unmounts the USB thumb drive.

### **usbhost disk dir drive**

#### **Syntax**

```
usbhost disk dir drive
```

#### **Description**

Displays a directory listing of a USB thumb drive.

## **usbhost disk dump**

### **Syntax**

```
usbhost disk dump <Filename>
```

### **Description**

Dumps the first 256 lines or 1M bytes of the specified file content of a USB thumb drive.

## **Reboot Commands**

### **admin reboot**

#### **Syntax**

```
admin reboot
```

#### **Description**

Immediately terminates all connections and reboots the device.

## **Diagnostic Commands**

### **diag ping**

#### **Syntax**

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

#### **Description**

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

## **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 Resetdk
- ◆ 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)

- ◆ kt: KVM Settings(Type/Deployment)
- ◆ 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
- ◆ vs: Video Settings
- ◆ va: Video Settings(Advanced)
- ◆ vu: Virtual Media UpLoad

## A: Troubleshooting

### **No connection can be established to the Spider**

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 to find out whether the Spider is reachable via the network. Establish a direct connection between the Spider and the client. If you use a firewall then check the appropriate port for accepting connections. The TCP ports 80 (for HTTP) and 443 (for both HTTPS and RFB) have 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 and your client.

### **Login on the Spider 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 does not open.**

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

### **The video quality is bad or the picture is grainy.**

Enter the Remote Console and click the **Auto Adjust** button to adjust the Spider's video input parameters to the correct values.

### **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 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.

### **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.

### **The Remote Console does not open with Opera in Linux.**

Some versions of Opera do not grant enough permission if the signature of the applet cannot be verified. To solve the problem, add the lines `grantcodeBase "nn.pp.rc.RemoteConsoleApplet"`

{**permission java.lang.RuntimePermission "accessClassInPackage.sun.\*"**; to the java policy file of opera (e.g., /usr/share/opera/java/opera.policy).

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

Use the serial interface with a terminal emulator program set to 9600 or 115200, 8 bit characters, No parity, 1 Stop bit, and No flow control. Within 2 seconds of booting the Spider, press the **Esc** key a few times to get a =>prompt. Type **defaults** at the => prompt.

If you can't get the => prompt after several tries at 9600, try 115200. Earlier firmware sets the serial console port to 115200 by default.

### **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 Internet Explorer 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:

1. Under Interfaces:Keyboard/Mouse – Check the **Force USB Full Speed Mode** box.
2. Under Interfaces:Keyboard/Mouse – Set the **Host Interface** to PS/2
3. If your system only has USB and no PS/2, do the above and use a PS/2 to USB adapter

If you have a USB model Spider, in **Interfaces:Keyboard/Mouse**, check the **Force USB Full Speed Mode** box.

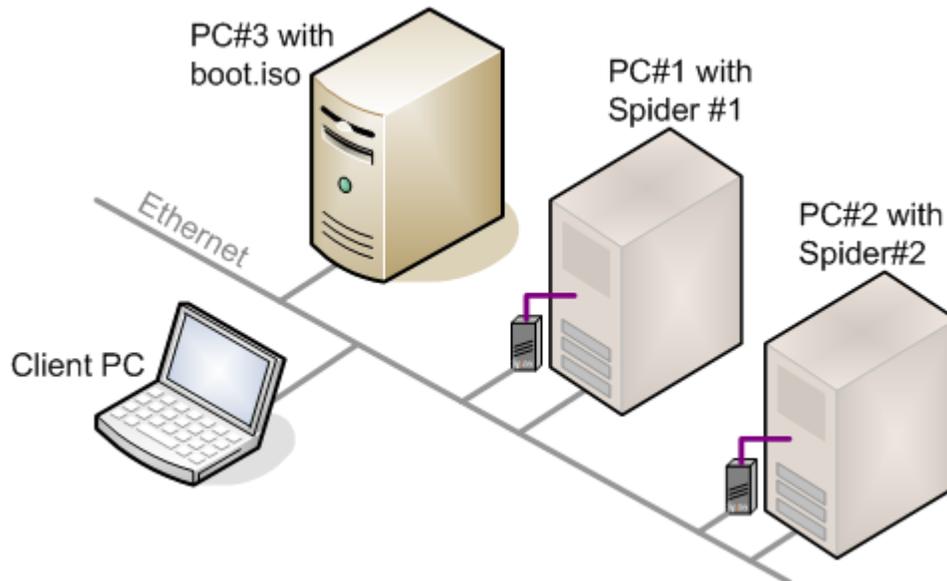
If the key used to enter BIOS setup or the boot menu on your PC is intercepted by your client OS, add a Virtual Key under Interfaces:KVM Console Settings.

## B: Virtual Media Example

### Goal

In this example, the goal is to put a rescue CD (a CD used to boot a PC when the hard-disk corruption prevents OS boot) on PC#3 so that the rescue CD can be used by any Spiders on the network.

Figure B - 1 Virtual Media

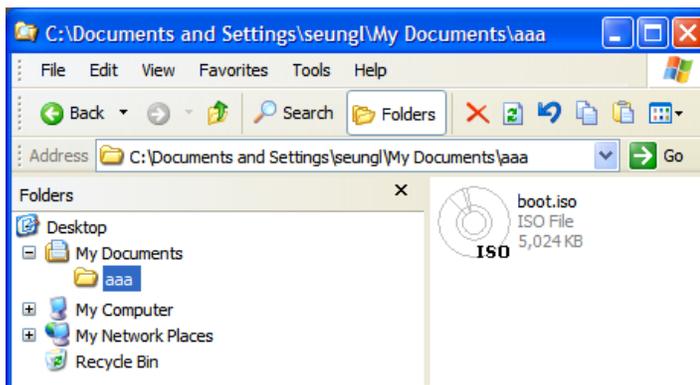


In this example, PC#2 cannot boot from its hard disk, so the user wants to use the rescue CD to boot the PC. We assume PC#2 can boot from external USB device.

### Step 1 – Prepare the VM Server

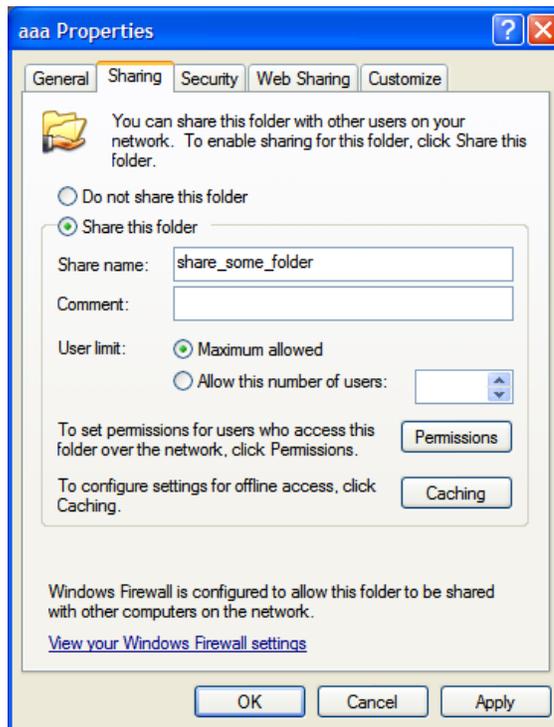
1. Use any CD-copy application to create an ISO image of the rescue CD, and call this ISO image file `boot.iso`.
2. On PC#3 (Windows XP in this example), put the ISO file in a Windows folder – file `boot.iso` in folder `aaa` as shown in the diagram below.

Figure B - 2 Windows Browser



- Right-click the folder `aaa` and select the “sharing” menu. The default name is the folder name but changed to `share_some_folder` as shown in the diagram below.

**Figure B - 3 Firewall Properties Window**



Now, the file `boot.iso` can be used from a Spider. The file can be left there permanently, and when a PC/server crashes and cannot boot, the combination of this file and the Spider will be used to boot the PC/server.

## Step 2 – Enable Virtual Media

In this example, PC#2 does not respond, and rebooting does not cure the problem. PC#2 has Spider#2 attached.

- On any PC (call this the client PC), bring up a browser, browse to Spider#2, and log in.

- Go to the Virtual Media page and complete the fields in the **Image on Windows Share** section of the page as shown in the diagram below.

Figure B - 4 Virtual Media Page

The screenshot shows the Lantronix Spider Duo web interface. The 'Virtual Media' section is active. The 'Image on Windows Share' section is highlighted, showing the following configuration:

- Share Host/IP: 172.19.215.251
- Share Name: images
- Image File with Path: FC3-386-DVD.iso
- User Name (optional): test1
- Password (optional): [empty]

Buttons for 'Set' and 'Reset' are visible below the input fields. The 'Virtual Media Active Image' section shows 'No disk emulation set.' The 'Virtual Media Options' section includes checkboxes for 'Disable Drive Redirection' (unchecked), 'Force read-only connections' (checked), and 'Disable USB Mass Storage if no image is loaded' (checked).

- Click **Set**, and see that the **Virtual Media Active Image** section now contains data as shown in the diagram below.

Figure B - 5 Virtual Media Active Image

The screenshot shows the Lantronix Spider Duo web interface after the 'Set' button was clicked. A red message 'Image file set successfully' is displayed at the top. The 'Virtual Media Active Image' section is now populated with the following data:

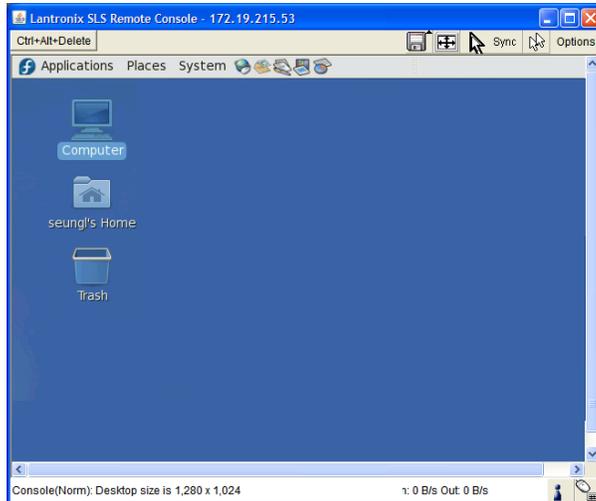
- CD-ROM Image
- Share Host/IP: 172.19.39.23
- Share Name: images
- Image File with Path: FC3-386-DVD.iso
- User Name: test1
- Password: \*\*\*\*\*

Buttons for 'Reactivate' and 'Unset' are visible below the input fields. The 'Image on Windows Share' section remains unchanged. The 'Virtual Media Options' section is also unchanged.

## Step 3 – Use the Virtual Media

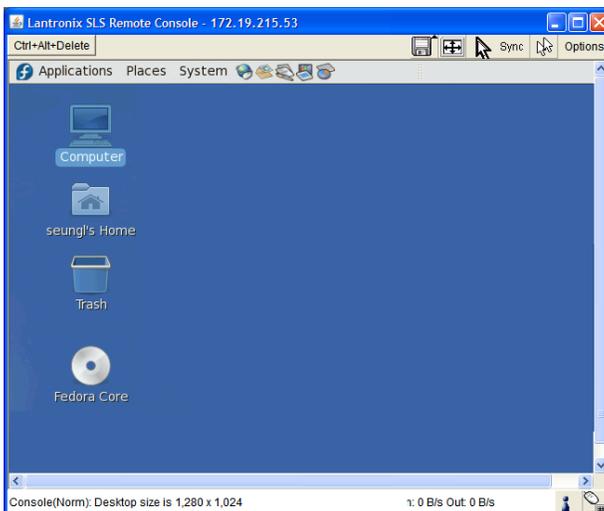
1. PC#2 shown in the diagram below is a Linux PC.

**Figure B - 6 Linux PC Window**



2. Once Step 1 is done, PC#2 will detect a new USB CD drive connected to its USB as shown in the diagram below. The CD is shown below as **Fedora Core** because that is the volume name of the rescue CD (`boot.iso` is the ISO image of this CD).

**Figure B - 7 Linux PC Window and USB CD**



3. You should be able to boot from the external USB device (`boot.iso`) on PC#2. Make sure that you set BIOS to boot from the USB device.

**Note:** Some systems may not support USB boot.

## C: Supported Resolutions and Refresh Rates

Table C-1 lists the supported resolution and refresh rates for video.

**Table C-1** Supported Video Resolutions and Refresh Rates

| Resolution (x,y) | Refresh Rates (Hz)     |
|------------------|------------------------|
| 640x340          | 70, 85                 |
| 640x400          | 56, 85                 |
| 640x480          | 60, 67, 72, 75, 85     |
| 720x400          | 70, 85                 |
| 800x600          | 56, 60, 70, 72, 75, 85 |
| 832x624          | 75                     |
| 1024x768         | 60, 70, 72, 75, 85     |
| 1152x864         | 75                     |
| 1152x870         | 75                     |
| 1152x900         | 66, 76                 |
| 1280x960         | 60                     |
| 1280x1024        | 60                     |
| 1600x1200        | 60                     |

**Note:** The 1600 x 1200 resolution and 60 Hz refresh rate is supported by the SpiderDuo without conditions. If a Spider hardware is revision G22, G23, E21 or higher, it will also support up to 1600 x 1200 at 60 Hz. If the Spider hardware is an earlier revision, it will only support up to 1280 x 1024 at 60 Hz. The hardware revision number can be located on the Spider Product Information Label shown in [Figure 2-6](#).

## D: Mounting Bracket Kit

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

**Figure D-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/SpiderDuo can be easily and securely attached to the elevated mounting posts and easily removed if necessary.

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

1. Mount the bracket with a Phillips screwdriver.

**Figure D-2** Attaching the Mounting Bracket



2. Attach the Spider/SpiderDuo to the bracket mounting posts.

**Figure D-3 Attaching the Device to the Mounting Bracket**



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

**Figure D-4 Connecting the Cables**



**Table D-5 Lantronix Part Number and Description**

| Lantronix<br>Part Number | Description                     |
|--------------------------|---------------------------------|
| 083-015-R                | Mounting Bracket Kit for Spider |

The bracket kit is included in the box with the Spider/SpiderDuo 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 <http://www.lantronix.com/support>.

## E: 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.

## ***F: Technical Support***

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

### **Technical Support US**

Check our online knowledge base or send a question to Technical Support at <http://www.lantronix.com/support>.

Phone: (800) 422-7044  
(949) 453-7198

### **Technical Support Europe, Middle East, Africa**

Phone: +33 1 39 30 41 72

Email: [mailto:eu\\_techsupp@lantronix.com](mailto:eu_techsupp@lantronix.com) or [mailto:eu\\_support@lantronix.com](mailto:eu_support@lantronix.com)

Firmware downloads, FAQs, and the most up-to-date documentation are available at <http://www.lantronix.com/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)

## G: Compliance

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

### Manufacturer Name & Address

Lantronix, Inc.,  
167 Technology, Irvine, CA 92618 USA

Declares that the following product:

### Product Name: SecureLinx Spider

Conforms to the following standards or other normative documents:

- ◆ UL/CUL (CSA-22.2 No. 60950-1-03 / UL-60950-1)
- ◆ CE - IEC 60950-1
- ◆ C-Tick
- ◆ FCC Part 15, Equipment Class A
- ◆ VCCI V-3/2006.04 Class A
- ◆ AS/NZS CISPR 22: 2006 Class A
- ◆ EN55022:1998 +A1:2000 +A2:2003 Class A
- ◆ EN61000-3-2: 2000 +A2: 2005 Class A
- ◆ EN61000-3-3: 1995 +A1: 2001
- ◆ EN55024: 1998 +A1:2001 +A2:2003
- ◆ Pb-free components

***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.*

## RoHS Notice

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

<sup>2</sup> Lead (Pb)                      <sup>2</sup> Mercury (Hg)                      <sup>2</sup> Polybrominated biphenyls (PBB)  
<sup>2</sup> Cadmium (Cd)                <sup>2</sup> Hexavalent Chromium (Cr (VI))                <sup>2</sup> 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.