

Catalog# 307183





INFORMATION



Electro Standards Laboratories 36 Western Industrial Drive Cranston, RI 02921 – USA Tel: 401.943.1164 Fax: 401.946.5790

WARRANTY AND LIMITATION OF LIABILITY

All equipment, software, and documentation is sold subject to the mutual agreement that it is warranted by the company to be free from defects of material and workmanship but the company shall not be liable for special, indirect or consequential damages of any kind under this contract or otherwise. The company's liability shall be limited exclusively to replacing or repairing without charge, at its factory or elsewhere at its discretion, any material or workmanship defects which become apparent within one year from the date on which the equipment was shipped, and the company shall have no liability of any kind arising from the installation and/or use of the apparatus by anyone. The buyer by the acceptance of the equipment will assume all liability of any damages which may result from its use or misuse by the buyer, his or its employees, or by others.

The warranties of the company do not cover, and the company makes no warranty with respect to any defect, failure, deficiency or error which is:

Not reported to the company within the applicable warranty period; or

Due to misapplication, modification, dis-assembly, abuse, improper installation by others, abnormal conditions of temperature, dirt, or corrosive matter; or

Due to operation, either intentional or otherwise, above rated capacities or in an otherwise improper manner.

The company believes that the information in this manual is accurate. The document has been carefully reviewed for technical accuracy. In the event that technical or typographic errors exist, the company reserves the right to make changes to subsequent editions of this document without prior notice to holders of this edition. The reader should consult the company if errors are suspected. In no event shall the company be liable for any damages arising out of or related to this document or the information contained in it.

There are no other warranties, expressed or implied including the implied warranties of merchantability and fitness for a particular purpose.

COPYRIGHT

Under the copyright laws, this publication may not be reproduced or transmitted in any form, electronic or mechanical, including photocopying, recording, storing in an information retrieval system, or translating, in whole or in part, without the prior consent of Electro Standards Laboratories.

© August 10, 2017 Electro Standards Laboratories. All rights reserved.

SOFTWARE RESTRICTIONS

IMPORTANT - READ CAREFULLY. By employing the Remote SSH Interface via the LAN access port on the switch and accessing its embedded software, you are agreeing to be bound by the terms of this agreement. This is a legal agreement between you (either an individual or an entity) and Electro Standards Laboratories ("ESL"). If you do not agree to all the terms of this agreement, promptly return the switch and the accompanying items (including all written materials and their containers) to the place you obtained them for a full refund.

- Copyright. The embedded SOFTWARE is owned by ESL or its suppliers and is protected by the United States copyright laws and international treaty provisions. Therefore, you must treat the embedded SOFTWARE like any other copyrighted material. You may not copy the written materials accompanying the embedded SOFTWARE.
- 2. **Other Restrictions.** You may not reverse engineer, decompile, or disassemble the embedded SOFTWARE.

THIS SOFTWARE IS PROVIDED "AS IS" AND ANY EXPRESSED OR IMPLIED WARRANTIES, INCLUDING BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE ARE DISCLAIMED. IN NO EVENT SHALL JCRAFT INC. OR ANY CONTRIBUTORS TO THIS SOFTWARE BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING BUT NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION) HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGE.

TABLE OF CONTENTS

INFORMATION1
WARRANTY AND LIMITATION OF LIABILITY1
COPYRIGHT1
SOFTWARE RESTRICTIONS
TABLE OF CONTENTS
TABLE INDEX5
TABLE OF FIGURES5
INTRODUCTION
INSTALLATION
POWER SUPPLY
OPERATION9
MANUAL CONTROL
REMOTE ETHERNET CONNECTIONS 12
VERIFY THE HARDWARE
10/100BASE-T LAN SETUP13
NETWORK SETUP13GETTING DEVICEINSTALLER13FINDING THE IP ADDRESS OF THE SWITCH13STATIC/DHCP IP ADDRESS CONFIGURATION13RESETTING THE REMOTE ETHERNET PORT14
REMOTE CONFIGURATION GUI15
SECURING THE SWITCH 15 ACCESSING THE REMOTE CONFIGURATION GUI 16 LOGGING INTO THE REMOTE CONFIGURATION GUI 16 IP Address/Network Configuration 17 HTTP Configuration and Authentication 18 Authentication Parameters for HTTP 19 Adding HTTP Users 20

Deleting HTTP Users	
SSH Users and Host Keys	21
Authorized SSH Users	22
Adding SSH Users	22
Changing SSH User Passwords	22
Deleting SSH Users	22
SAVING/RESTORING TO/FROM XML	23
Saving Settings to XML	23
Restoring Settings from XML	24
Restoring Factory Defaults from XML	
OTHER CONFIGURATION CHANGES	25
REMOTE SSH SESSION	26
SSH IN WINDOWS USING PUTTY	26
SSH IN LINUX/MAC OS X	
SSH SESSION	27
SSH Session using Port 22	27
SSH Session using Port 10001	
SSH Session using Port 10001 TROUBLESHOOTING	
SSH Session using Port 10001 TROUBLESHOOTING Swittching Issues	29 29
SSH Session using Port 10001 TROUBLESHOOTING Switching Issues Remote Connection Issues	29 29 29
SSH Session using Port 10001 TROUBLESHOOTING Switching Issues Remote Connection Issues Remote Login Issues	29 29 29 30
SSH Session using Port 10001 TROUBLESHOOTING Switching Issues Remote Connection Issues Remote Login Issues SPECIFICATIONS	29 29 29 30 31
SSH Session using Port 10001 TROUBLESHOOTING Switching Issues Remote Connection Issues Remote Login Issues SPECIFICATIONS CUSTOMER & TECHNICAL SUPPORT	
SSH Session using Port 10001 TROUBLESHOOTING SWITCHING ISSUES REMOTE CONNECTION ISSUES REMOTE LOGIN ISSUES SPECIFICATIONS CUSTOMER & TECHNICAL SUPPORT	
SSH Session using Port 10001 TROUBLESHOOTING Switching Issues Remote Connection Issues Remote Login Issues SPECIFICATIONS CUSTOMER & TECHNICAL SUPPORT CUSTOMER SUPPORT TECHNICAL SUPPORT	

TABLE INDEX

Table 1: Ethernet Remote Port Pinout	8
Table 2: Remote Control Commands	10

TABLE OF FIGURES

Figure 1: Model 7183 Rear Panel	7
Figure 2: Model 7183 Front Panel	9
Figure 3: Crossover Cable connection for no LAN	. 12
Figure 4: Connecting to a LAN with a 10/100Base-T cable	. 12
Figure 5: Finding the IP address in DeviceInstaller	. 13
Figure 7: Remote Configuration Login Prompt	. 16
Figure 8: Remote Configuration GUI Status Screen	. 16
Figure 9: IP Address/Network Configuration	. 17
Figure 10: HTTP Configuration	. 18
Figure 11: HTTP User Authentication	. 19
Figure 12: SSH Server: Host Keys	.21
Figure 13: SSH Server: Authorized Users	. 22
Figure 16: XML Export of Remote Configuration GUI Settings	.23
Figure 17: Restoring Settings from XML	.24
Figure 18: XML Import of Settings, Factory Defaults	.25
Figure 19: PuTTY Configuration using Port 22	.26
Figure 20: SSH Session Menu on Port 22	.27
Figure 21: Remote Control SSH tunnel session using Port 22	.27
Figure 22: Remote Control SSH tunnel session using Port 10001	. 28

INTRODUCTION

The PathWay® Model 7183 Dual Channel BJ80 BNC A/B/OFFLINE Switch with Secure Ethernet Remote allows the user the capability of sharing a single port interface device, connected to the "COMMON" port, among two other devices, connected to the "A" and "B" ports for each channel. Remote Control access can be accomplished using a Secure Ethernet 10/100BASE-T connection SSH Commands. The Model 7183 is enclosed in a 1U, full rack size, all metal black chassis designed to provide EMI/RFI shielding and fit in a standard 19" rack.



Features:

- The switch ports are transparent to all data.
- Both the center pin and the shell signals are switched via breakbefore-make electromechanical relays..
- Switch maintains last set position on power loss and continues to pass data.
- Switch powers up in last known position.
- Simultaneous Channel Control.
- Exclusive Ethernet Remote Control. No front panel control.
- Control of the switch position from a 10/100Base-T LAN Ethernet environment.
- Remote Control SSH Command Interface that allows the user to control switch position, lockout front panel operations, and obtain switch status.
- Remote allows query of switch position before selecting a new switch position.
- Front panel LED's display present position and power status.
- All BJ80 BNC ports are impedance matched to support 50 Ohm equipment.

INSTALLATION

This section describes the physical connections required to start operating the Model 7183.

Model 7183 Rear Panel



Figure 1: Model 7183 Rear Panel

The rear panel view of the switch is shown in the above figure. On the rear of the switch are the following ports:

- **POWER** Phoenix (F), External Power Supply Input connector.
- **REMOTE** RJ45 (F), 10/100BASE-T LAN access Ethernet Remote Control port.
- **RESET** Reset button for the 10/100Base-T LAN access Ethernet port.
- **COM** BJ80 BNC (F), the "COMMON" or shared device port fro each channel.
- A BJ80 BNC (F), the "A" device port for each channel.
- **B** BJ80 BNC (F), the "B" device port for each channel.

Power Supply

After all the proper connections have been made, plug the Model 7183 into a 100VAC/240VAC, 50Hz/60Hz wall receptacle using the supplied 12VDC, 500mA, UL listed and LPS approved, 2-prong US non-polarized NEMA 1-15P plug wall mount power supply, P/N 516682.

Option: Wide Range Power Module, (Cat. No. 517277), 100VAC/240VAC, 50Hz/60Hz, IEC 60320 C14 inlet, can be ordered for use in place of the standard NEMA 1-15P plug power module that is included with the unit. Ideal for international applications.

Upon power up the Model 7183 will process its power up routine. When the routine is done the front panel LED's will indicate the present position of the unit. At this point the unit is ready for operation.

SIGNAL NAME	PIN #	DIRECTION
TRANSMIT DATA A (XMT-A)	1	OUTPUT
TRANSMIT DATA B (XMT-B)	2	OUTPUT
RECEIVE DATA A (RCV-A)	3	INPUT
RECEIVE DATA B (RCV-B)	6	INPUT

Ethernet Remote Port Pinout

Table 1: Ethernet Remote Port Pinout

OPERATION

The Model 7183 can be operated either by the front panel or through its Remote port.



Figure 2: Model 7183 Front Panel

Manual Control

The front panel view of the Switch System is shown in the above figure. On the front of the switch are the following controls and indicators:

- **A, B, OFFLINE INDICATORS** Red LED's indicate the switch position as well as the power status.
 - The LED in the steady state indicates the position of the switch.
 - When first powering up, both LED's will light during the power up routine. During the power up routine, the LED's will flash sporadically. This will continue for approximately 12 seconds. Upon completion, the LED's will display the present position and be ready for operation.

Remote Control Commands

All commands are ASCII commands. For Control Commands, the command is created by pressing and holding the [CTRL] key and the designated character key simultaneously. For example, to create the CTRL-A command, simply press the [CTRL] and [A] keys on the keyboard simultaneously then release both.

When starting an SSH session, the user will be prompted to enter a username and password. The default username is "admin" and the default password for this user is "ESL02921".

Once the Model 7183 Remote SSH session has been initiated, commands from Table 2 can be entered. Do not press the enter key at the end of a command. All responses are terminated with a carriage return ('\r') followed by a new line feed ('\n').

A note to those programming their own systems to control this switch automatically: The ASCII Control Commands are represented as the decimal equivalent of the numerical position of that letter in the alphabet, which can then be translated to hex. For example, CTRL-A translates to '1' in decimal or 0x01 in hex, since A is the 1st letter of the alphabet. CTRL-V, on the other hand, translates to '22' in decimal, and 0x16 in hex, since it is the 22nd letter of the alphabet.

Command	Function	Response
CTRL A	Switch to the A position	Position: A
CTRL B,	Switch to the B position	Position: B
CTRL O	Switch to the OFFLINE position	Position: OFFLINE
CTRL P	Query position/status	Position:
CTRL I	Query MAC address	M7183 MAC Address: XX:XX:XX:XX:XX:XX
CTRL S	Query serial number	M7183, Serial Number: XXXXX
CTRL V	Query firmware version number	M7183, Firmware Version x.x, Compiled

Table 2: Remote	e Control	Commands
-----------------	-----------	----------

Error conditions not covered in Table 2:

 Issuing a command not found in Table 2 will respond with the error message: "Invalid Command." and no switching will occur.

Whenever a front panel pushbutton operation takes place, the new status will automatically be sent to the SSH session when logged in. When the unit sends automatic updates, they will be in the same format as the response for the CTRL-P command.

Switch Position on Power Down

If power to the Model 7183 is lost, the switch will maintain its present position and continue to pass data. Upon power restore, the unit will remain in the position it was in at power down.

REMOTE ETHERNET CONNECTIONS

Verify the Hardware

Verify that the switch is currently powered. If the user needs to directly connect to the switch rather than through a LAN, a 10/100BASE-T crossover cable will be necessary (ESL can provide this – p/n 984228-006). This cable allows direct connection of the switch's Remote LAN port to a computer with a Network Interface Card (NIC).

If no LAN is available, use a Crossover Cable

If no LAN connection is available, the user can use a crossover cable. Plug one end of the cable into the RJ45 Remote port on the rear of the switch and the other end into the computer NIC as in Figure 3.



Figure 3: Crossover Cable connection for no LAN

If connecting to a LAN use a 10/100Base-T Cable

Use a straight through 10/100BASE-T patchcord from the switch's LAN Remote port to a LAN connection, and likewise, reconnect the computer used to configure the system via a standard, straight through patchcord to the LAN as in Figure 4. ESL can provide this cable (p/n 984231-006).



Figure 4: Connecting to a LAN with a 10/100Base-T cable.

Electro Standards Laboratorie	es, Inc.	(401) 943-1164
www.electrostandards.com	- pg 12 -	Pub. 5847-01

10/100BASE-T LAN SETUP

Network Setup

The switch is configured from the factory to use DHCP to automatically get its IP address from a DHCP server on the local area network when connected to the network and powered up. Therefore, a DHCP server is needed on the local area network for the initial configuration. After that the switch can be configured to use a static IP address. To find the IP address of a switch that it has gotten from the DHCP server or to reconfigure the IP Address of the switch, use the Lantronix® DeviceInstaller application.

Getting DeviceInstaller

DeviceInstaller requires Microsoft's .NET Framework version 4.0 or higher. If you do not already have .NET Framework installed, you must first install it. The .NET Framework can be downloaded from Microsoft's website, either as a web install, or as a standalone installation. The latest version of DeviceInstaller can be downloaded from Lantronix's website.

Finding the IP Address of the Switch

After installing DeviceInstaller and opening it, the software will automatically search for devices on the network. Once found, the devices will be listed in the right pane (see Figure 5). Match the MAC address on the rear of the unit to the MAC address ("Hardware Address") shown in DeviceInstaller to correctly identify the desired unit and find the associated IP address.

E Lantronix DeviceInstaller 4.3.0.6						_ _ ×	
<u>Eile Edit View D</u> evice Iools <u>H</u> elp							
🔎 Search 🛛 🤤 Exclude 🛭 🗞 Assign IP							
E-	Туре	Name	Group	IP Address	Hardware Address	Status	
Yort Yort Yot Yot Wat Wat Wot 10.0038	Service Pro			10.0.0.38	00-80-A3-9B-E3-3A	Online	
🗹 Ready							

Figure 5: Finding the IP address in DeviceInstaller

Static/DHCP IP Address Configuration

The switch can be configured to use a static IP address or DHCP. This is done through the Remote Configuration GUI. See section "IP Address/Network Configuration" on page 17.

Electro Standards Laboratories, Inc. www.electrostandards.com - pg 13 -

Resetting the Remote Ethernet Port

The Remote Ethernet port can be reset by pressing the Reset button on the back of the unit.

REMOTE CONFIGURATION GUI

Securing the switch

Keeping the switch with the factory defaults is NOT secure. In order to secure the switch, the following security changes are required:

• Change the SSH username/password (section "Authorized SSH Users", page 22)

Accessing the Remote Configuration GUI

The Remote Configuration GUI can be accessed by typing http:// <The units IP address>

Logging into the Remote Configuration GUI

After you enter the units IP address into your browser and pressing enter. You will be prompted for the username and password. The default username is "admin" and the default password is "ESL02921".



Figure 6: Remote Configuration Login Prompt

When successfully logged in, the configuration status will be shown.

Status 쇼子 CLI	Device Status			[Log
CPM	Product Information	E.		
Diagnostics	Product Type:	Model 7183 Swite	th	
DNS	Firmware Version:	5.4.0.0R7		
Email	Build Date:	Mar 18 2016 (14:	56:21)	
ilesystem	Serial Number:	07163207T7CFC	J	
TP	Uptime:	0 days 00:14:13		
lost	Permanent Config:	Saved		
ITTP	Network Settings			
P Address Filter	Interface:	eth0		
Line	Link:	Auto 10/100 Mbp	s Auto Half/Full (100 Mbps Fu	ll)
LPD	MAC Address:	00:80:a3:bc:3f.be		
Modbus	Hostname:	<none></none>		
Network	IP Address:	10.0.0.117/8 (DH	CP)	
PPP	Default Gateway:	10.0.0.223 (DHC	²)	
Protocol Stack	Domain:	esidomain.local (DHCP)	
Query Port	Primary DNS:	10.0.0.10 (DHCP		
RSS	Secondary DNS:	8.8.8.8 (DHCP)		
SNMP	MTU:	1500		
SH	Line Settings			
SSL	M7183:	RS232, 9600, No	ne, 8, 1, None	
Syslog System	Tunneling	Connect Mode	Accept Mode	
[erminal	Tunnel 1:	Disabled	Waiting	

Figure 7: Remote Configuration GUI Status Screen

IP Address/Network Configuration

Configure the IP address by selecting "Network" in the left menu, then "Interface" and "Configuration" in the top center of the Network menu. Here, the DHCP and other IP address details can be changed, as well as the Domain and DNS servers. Note that the subnet is also entered in the IP address field, either in the form "<ip address>/<subnet bits>" or "<ip address> <subnet mask>", as shown in the context panel in the GUI on the right.

	Network 1	This page is used to configure the Network interface on the device. T
M		see the effect of these items after reboot, view the Status page.
ignostics	Interface Link	The following items require a rebor
IS		to take effect:
nail	Status Configuration	BOOTP Client On/Off
esystem		IP Address
P Network	(ethu) Interface Configuration	DHCP Client ID
st BOOTP Clien	t: 0 0n @ 0ff	If BOOTP or DHCP is turned on, any configured IP Address, Network
TP DHCP Client:		Mask, Gateway, Hostname, or
Address Filter		Domain will be ignored. BOOTP/DHCP will auto-discover
IP Address:	<none></none>	and eclipse those configuration
D Default Gate	way: <none></none>	If both BOOTP and DHCP are turne
dbus		on, DHCP will run, but not BOOTP.
twork Hostname:		When BOOTP or DHCP fails to
P Domain:		address will automatically be
otocol Stack		generated using AutoIP. This address will be within the
DHCP Client	ID:	169.254 x.x space.
S	Text O binary	IP Address may be entered alone
MP Primary DNS	<none></none>	mask:
H Secondary D	NS: <none></none>	192.168.1.1 (default mask) 192.168.1.1/24 (CDR)
L MTH.	4500	192.168.1.1 255.255.255.0 (explicit
slog MTU:	1500	mask) Hostoamo must hosis with a latte
stem		continue with letter, number, or
rminal		hyphen, and must end with a letter or number.
IP III		
nnel		

Figure 8: IP Address/Network Configuration

HTTP Configuration and Authentication

The settings for the HTTP server can be accessed by selecting "HTTP" in the left menu.

By selecting "Configuration" from the top center panel of the HTTP menu, the details of the server operation can be changed, including security requirements and timeouts. These settings should not need to be changed under a normal operating environment.

	Statisti	cs Cor	figuration Authentication	[Logoul This page displays and changes th current HTTP Configuration
liagnostics	HTTP Configu	Iratio	n	settings.
mail	State:	• Enat	oled O Disabled	1
ilesystem	Port:	80	7	
тр	Secure Port:	443]	
lost	Convert Destander	Root		
ПТР	Secure Protocols:	IN SSL	3 1 1LS1.0 1 1LS1.1	-
P Address Filter	Max Timeout:	10	seconds	
ine	Max Bytes:	40960		
PD	Logging State:	• Enat	oled O Disabled	
lodbus	Max Log Entries:	50		
letwork	Log Format:	%h %t'	"%r" %s %B "%(Beferer)i" "%{User-Agent!	
Protocol Stack	Authentication	30	minutes	<u>1</u>
uery Port	Timoodd			-
ISS				
NMP				
SH				
SL				
iyslog				
ystem				
erminal				
FTP				

Figure 9: HTTP Configuration

Authentication Parameters for HTTP

The "Authentication" option in the top center panel of the HTTP menu allows username and password changes. The URI in the "Current Configuration" listing at the bottom of the HTTP menu are "/". This pertains to the Remote Configuration GUI.

XPc	ort [®] Pro [®]		EVOLUTION OS"
Status <table-row></table-row>	Statistics HTTP Authentid UR: Realm: CauthType: SSU Username: Password: Submit	Configuration Authentication Cation Basic O Digest SSL/Basic O SSL/Digest	Legant The HTTP Server can be configured with many different authentication directives. The authentication is hieractival in that any URI can be given an authentication directive in order to override a parent URI authentication directive. The URI must begive with / to refer to the flexystem. The different AuthType values offer various levels of security. From the least to most secure: no authentication necessary Basic encides passwords using
LPD Modbus	Current Configurat	ion	Base64 Digest encodes passwords using MD5
PPP Protocol Stack Query Port	URI: Realm: AuthType: Users:	/ [<u>Delete</u>] config Digest admin [<u>Delete</u>]	SSL page can only be accessed over SSL (no password) SSL/Basic page can only be accessed over SSL (encodes passwords using
RSS SNMP SSH SSSH Syslog System Terminal TFTP TFTP Tunnel		,	Base(4) SSL0(gent) Base(2) Base(2) MDS) When changing the parameters of Digest or SSL0(gent) authentication, it is often best to ensure that the 4 does not attempt to use cached authentication information.
XML			Note that SSL by itself does not

Figure 10: HTTP User Authentication

When adding/changing the users/passwords, the options to note are the "URI", "AuthType", "Username", and "Password".

- URI: The URI for the desired GUI to make changes to should be entered. This is "/" for the Remote Control GUI Realm: This can be left blank to preserve the existing settings.
- AuthType: This should only be selected if making a change to the security. Leaving the AuthType unselected will leave the URI with the existing AuthType.
- Username: The new/existing username.
- Password: The new password.

Adding HTTP Users

Type the URI into the "URI" Text Field at the top of the panel. The AuthType should only be selected if making a change. Type the name of the new user in the "Username" Text Field, and the new user's password in the "Password" Text Field. Press the "Submit" button to complete the addition. See the section "Authentication Parameters for HTTP" and Figure 11 for more information.

Changing HTTP User Passwords

To change the password for a desired user, type the URI and Username associated with this user into the corresponding Text Fields. Type the new password into the "Password" Text Field and press the "Submit" button. This will override the existing user password. See the section "Authentication Parameters for HTTP" and Figure 11 for more information.

Deleting HTTP Users

To delete a user, find the username associated with the desired URI in the "Current Configuration". There will be a "[Delete]" hyperlink to the right of the name. Press the link to delete the user. See the section "Authentication Parameters for HTTP" and Figure 11 for more information.

SSH Users and Host Keys

The SSH Server provides settings for the host keys as well as the authorized users. The SSH menu can be accessed by selecting "SSH" from the left menu.

The Host Keys can be configured by selecting "SSH Server: Host Keys" from the panel in the top center of the SSH menu. On this screen, new keys can be created by selecting the desired options under the "Create New Keys" heading and pressing the "Submit" button below. There is also the option to upload existing key files if desired. If uploading an existing key, be sure this is done over a secure connection.

The unit is shipped with a 1024-bit RSA key by default.

XPc	ort°Pro			EVOLUTION OS"
Status 🖓 CLI CPM	SSH Server: Host I SSH Server: Author	Keys SSH Cli prized Users SSH Cli	ent: Known Hosts ent: Users	[Logout] The SSH Server Host Keys are used by all applications that play the role of an SSH Server. Specifically the Command Line Interface (CII)
Diagnostics DNS Email Filesystem	SSH Server: Hos Upload Keys	and Tunneling in Accept Mode. These keys can be created elsewhere and uploaded to the device or automatically generated on the device		
FTP	Private Key:		Browse	If uploading existing keys, take care
Host	Public Key:		Browse	to ensure the Private Key will not be
нттр				the data is uploaded over some kind
IP Address Filter	Submit	of secure private network.		
Line	odonik	RSA Host Keys to be at least 1024		
LPD	Create New Keys			bits in size.
Modbus	Key Type: O RSA O DSA			
Network	Bit Size: 0512 0768			
ррр	Submit			
Protocol Stack	oubline			_
Query Port	Current Configuratio			
RSS				
SNMP	Public RSA Key:	[View Key] [Dele	te Key]	-
SSH	Public DSA Key:	No DSA Key Cor	ntigured	
SSL				
Syslog				
System				
Terminal				
TETP				
Tunnel				
XML				

Figure 11: SSH Server: Host Keys

Authorized SSH Users

The "SSH Server: Authorized Users" option in the top center of the SSH menu allows changes to be made to the SSH users and passwords. Existing keys can also be uploaded if desired. If uploading an existing key, be sure this is done over a secure connection.

XPo	ort°Pro			EVOLUTION OS
Status 🕼				[Logout]
CLI	SSH Server: Host K	eys SSH Client:	Known Hosts	The SSH Server Authorized Users
СРМ	SSH Server: Author	rized Users SSH Client:	Users	are used by all applications that play the role of an SSH Server.
Diagnostics				Specifically the Command Line
DNS	SSH Server: Auth	norized Users		Accept Mode.
Email				Every user account must have a
Filesystem	Username:			Password.
FTP	Password:			optional and only necessary if
Host	Public RSA Key:		Browse	public key authentication is wanted. Using public key authentication will
нттр	Public DSA Key:		Browse	allow a connection to be made
IP Address Filter	Add/Edit			at that time.
Line				<u> </u>
LPD	Current Configuration	n		
Modbus	Una	adaptic (Dalate Hand)		-
Network	Deer:	Confirmed		-
PPP	Password:	No DCA Key Configured		-
Protocol Stack	Public DSA Kow	No DSA Key Configu	red	-
Query Port	Fublic DSA Ney.	No DOA Key Conligu	leu	
RSS				
SNMP				
SSH				
SSL				
Syslog				
System				
Terminal				
TFTP				
Tunnel				
XML				

Figure 12: SSH Server: Authorized Users

Adding SSH Users

To add a user, type the desired username and password into the appropriate fields. If uploading an RSA or DSA public key, this can be done as well. Press the "Add/Edit" button to complete.

Changing SSH User Passwords

Changing an SSH user password is done by entering the existing username into the "Username" Text Field, and then entering the new password into the "Password" Text Field. Public keys can also be added in this way. Pressing the "Add/Edit" button saves the changes.

Deleting SSH Users

Deleting SSH users can be done by finding the desired username under the "Current Configuration" section towards the bottom of the SSH menu, and pressing the "[Delete User]" hyperlink next to the name.

Saving/Restoring to/from XML

All Remote Configuration GUI settings can be saved or restored via XML files. The XML import/export can be accessed by selecting "XML" from the left menu.

Saving Settings to XML

Select "Export Configuration" from the panel at the top center of the XML menu. An array of checkboxes will appear below. Select the checkboxes for the desired settings groups to export.

Note that when selecting to export passwords (the "Export secrets" checkbox), this should only be done when being extremely mindful of security hazards since it can make passwords vulnerable if the XML file is recovered or intercepted in transit.

When the desired settings have been selected, choose to either "Export to browser" or "Export to local file". Exporting to a local file will export it to the Filesystem on the unit. This can be left on the unit for easy access in the future or it can be retrieved either by enabling FTP or TFTP.

← → 5 http://10.0.0.198/#XmlExportPage					¢ ★ ♠ ۵-۹
Lantronix Web Manager ×	an 17 - 18 Mar		And a second		The second s
and a second					
				NTRONIX	<u>^</u>
			E	VOLUTION OS"	
Status	₫ 			[Logout]	
cu	Export Configurat	ion Export Status	Import Configuration	This page is used for exporting the current system configuration in XML	
СРМ	VAL - Frances C	XML: Export Configuration		format as XCR records. The	
Diagnosti	XML: Export C			at a later time to restore the	
Email	Export to browse			configuration.	
Filesyster	Export to local fil			url' group must be exported with	
FTP	-	- L		export secrets enabled if it is to be used to later restore the	
Host	L Export secrets (u	Export secrets (use only with extreme caution) Comments configuration			
HTTP	Lines to Export: [C]	ear All] [Select All]		modified and imported to update the	
IP Addres	ss Filter 🗸 1 🖌 networ			configuration on this device or another.	
Line				The XML data can be exported to	
LPD	Groups to Export: [Jear Allj (Select All bu	t Networking)	the browser window or to a file on the filesystem.	
Modbus	🗹 arp	🗹 cli	Cp group	Caution: Only export secrets	
Network	✓ device	diagnostics	🗹 email	over a secure connection and make sure that the data goes only to	
Destand	ethernet: eth0	ftp server	Most Index	secure locations.	
Query Po	http	A http server	✓ icmp	Notice that by default, all Groups to Export are checked except	
RSS	interface: eth0	V in	V in filter	some pertaining to the network	
SNMP	V line	V Ind	M modbus	later "paste" the entire XML	
SSH		guery port	✓ rss	network connectivity. You may	
SSL	serial command			check or uncheck any group to include or omit that group from	
Syslog	mode	🗠 smtp	i≌ snmp	export.	
System	🗹 ssh	Ssh client	ssh server	Selection of Lines to Export fitters instances to be exported in the line.	
Terminal	I ssl	Syslog	✓ tcp	lpd, ppp, serial, tunnel, and terminal	
TETP	☑ teinet	✓ terminal	✓ tftp server	groups.	
Tunnel	✓ tunnel accept	✓ tunnel connect	tunnel disconnect		00000000000000000000000000000000000000
XML	✓ tunnel modem	🗹 tunnel packing	🗹 tunnel serial		
	I xml import contro				
	Export				~

Click the "Export" button at the bottom to complete the process.

Figure 13: XML Export of Remote Configuration GUI Settings

Restoring Settings from XML

Settings can be imported from XML to restore previously exported setting configurations. Select "Import Configuration" from the top center panel of the XML menu. Select whether to import from an "External file" or from the "Filesystem" (Figure 17).

Status 🕼		n ILogout
CLI	Export Configuration Export Status Import Configuration	This page is used for importing
CPM		system configuration from an XML
Diagnostics	XML: Import Configuration	Import Configuration from
DNS		External file picks up all the
Email	Import:	Import Configuration from
Filesystem	Configuration from External file	Filesystem picks up settings from the selected Groups, Lines and
FTP	O Configuration from Filesystem	Instances. Import Line(s) from
Host	Oliver(a) from visuals line Continues on the Eilenstein	single line Settings on the Filesystem copies lines settings
нттр	Uline(s) from single line Settings on the Filesystem	from an the input file containing only
IP Address Filter		selected Lines.
Line		When selecting a Whole Groups
LPD		to Import item, all instances of that oroup will be imported. Notice that
Modbus		by default, all groups are checked
Network		network configuration; this is so
PPP		that import will not break your
Protocol Stack		check or uncheck any group to
Query Port		include or omit that group from import.
RSS		Selection of Lines to Import
SNMP		filters instances to be imported in the line and one serial hungel and
SSH		terminal groups. This affects both
SSL		Whole Groups to Import and Text List selections.
Syslog		Use the Text List string to import
System		specific instances of a group. The textual format of this string in
Terminal		toritori format of bile energies.
TETP		<pre><gr:<1>;<g>;<1>;<i>;<i>;<i>;<i>;<i>;<i>;<i>;<i>;<i>;<i< td=""></i<></i></i></i></i></i></i></i></i></i></g></gr:<1></pre>
Tunnel		Each group name <g> is followed by a colon and the instance value</g>
XML		And each kg>:ki> value is
		group has no instance then only the
		group name <g> should be</g>

Figure 14: Restoring Settings from XML

Selecting an option will bring up a new screen. On this screen, the configuration file to import can be selected. It is also possible to use the array of checkboxes below to select only certain settings to import (Figure 18). After selecting the XML file to import and choosing which settings to import from that XML file, press the "Import" button at the bottom the GUI panel.

Restoring Factory Defaults from XML

To restore factory defaults for some or all of the settings, choose to Import from the Filesystem. For the filename in the next screen, type in "/factory_defaults.xml". If it is not desired to import all of the settings, choose which settings to include using the checkboxes below. Press the "Import" button at the bottom to proceed with the restoration.

Note that it is recommended not to import the "interface" settings group since this contains the IP address and other such configurations for the unit. This is different from the "ip" settings group, which contains protocol related items such as TTL values.

Status for				II onou
CLI	Export Configurat	tion Export Status	mport Configuration	This page is used for importing
CPM				system configuration from an XML file
Diagnostics	XML: Import C	onfiguration		Import Configuration from
DNS				External file picks up all the
Email	Import configuration	from the filesystem:	-	Import Configuration from
ilesystem	Filename factory_de	faults.xml]	Filesystem picks up settings from the selected Groups, Lines and
тр	Lines to Import: [C	lear All] [Select All]		Instances. Import Line(s) from
lost	Telever telever telever			Filesystem copies lines settings
ITTP	🗹 1 🗹 networ	k		from an the input file containing on one Line instance to all of the
P Address Filter	Whole Groups to Im	port: [Clear All] [Select	All but Networking]	selected Lines.
.ine	-			When selecting a Whole Groups
.PD	i arp	l⊻ cli	✓ cp group	group will be imported. Notice that
Aodbus	i device	diagnostics	⊻ email	by default, all groups are checked
letwork	d ethernet	✓ execute	≤ exit cli	network configuration; this is so
ppp	Iftp server	✓ host	i⊻ http	that import will not break your network connectivity. You may
Protocol Stack				check or uncheck any group to
Query Port	I nup server	C icmp		import.
RSS	in la	Ip inter		Selection of Lines to Import
SNMP	i≊ iba	i⊻ modbus	✓ ppp	filters instances to be imported in the line, lod, pop, serial, tunnel, and
SSH	duery port	🗹 rss	mode	terminal groups. This affects both
SSL	I smtn	✓ snmp	✓ ssh	Text List selections.
Syslog	Ssh client	Ssh server	✓ ssl	Use the Text List string to import
System	V syslag	V ten	V telnet	specific instances of a group. The textual format of this string is:
erminal	✓ terminal	tftp septer	✓ tunnel accent	
and a second	the contribution	up server		·····
FTP	tunnel connect	1 tunnol disconnect	N tunnol modom	Each arous same you is followed
IFTP Tunnel	tunnel connect	tunnel disconnect	tunnel modem	Each group name <g> is followed by a colon and the instance value</g>

Figure 15: XML Import of Settings, Factory Defaults

Other Configuration Changes

There are many other settings that can be changed or accessed through this Remote Configuration GUI. Please contact Electro Standards for any help required for these additional features (see "Customer & Technical Support" on page 32).

REMOTE SSH SESSION

SSH can be used to connect to and command the switch. Before connecting and starting an SSH session, first connect the switch in accordance with the section entitled "Remote Ethernet Connections" on page 12. Once the network settings and users have been configured, the unit is ready for SSH users to connect using an SSH client.

SSH in Windows using PuTTY

To start an SSH session in Windows, an SSH client is required, such as PuTTY. After downloading PuTTY from the internet, run the executable (no installation is required). The PuTTY GUI will prompt the user for connection information. Enter the Host Name or IP address, as well as the port number. Save the settings below if desired, and then press the "Open" button. Upon connecting, a prompt will display for the username and password.



Figure 16: PuTTY Configuration using Port 22

SSH in Linux/Mac OS X

SSH is commonly built into distributions of Linux and Mac OS X, or is readily available through a package manager or appropriate binary distribution. Often SSH sessions are accomplished through the terminal. For example, in Ubuntu and Mac OS X, SSH sessions can be started with the command:

```
ssh <username>@<ip address or host name>
```

For ports other than the standard port 22, adding the option "-p <port>" before the username will work.

SSH Session

There are two possible ports to access by default. The standard SSH port 22 is open for multiple connections. It presents a menu, where one of the options is the Remote Control SSH tunnel. The other SSH port is port 10001. This is the direct access to the Remote Control SSH tunnel. Only one open connection to the Remote Control SSH tunnel can exist at any given time.

SSH Session using Port 22

When a connection to port 22 is established, a menu will appear. The menu will allow the selection of the Remote Control SSH tunnel (Option 1), or the Remote Configuration CLI (Option 2), as well as an option to terminate (Option 3).

🚰 10.0.1.40 - PuTTY		 x
login as: admin admin@10.0.1.40's password:		^
1) M7377 3) Log out	2) Exit to CLI	
Selection =		
		-

Figure 17: SSH Session Menu on Port 22

Selecting Option 1 will redirect to the Remote Control SSH tunnel if it is open. Once established, the unit can be commanded using the Remote Control Commands in Table 2.

10.0.1.40 - PuTTY		- • ×	
login as: admin admin@10.0.1.40's password:			~
1) M7377 3) Log out	2) Exit to CLI		
Selection = 1			
Connected to line 1 (M7377).			
Escape sequence is <control>C</control>			
			-

Figure 18: Remote Control SSH tunnel session using Port 22

Electro Standards Laboratories, Inc. www.electrostandards.com - pg 27 -

(401) 943-1164 Pub. 5847-01 Selecting Option 2 will bring up the command line tool for configuring the Remote Connection. These are the same settings that are changed via the Remote Configuration GUI. It is highly recommended to make any configuration changes via the GUI.

SSH Session using Port 10001

When connecting to port 10001, there will be no menu or prompt. Once logged in, the unit will immediately be ready for command entry and status. See the Remote Control Commands in Table 2.



Figure 19: Remote Control SSH tunnel session using Port 10001

TROUBLESHOOTING

Described below are some common troubleshooting steps and solutions. If following the troubleshooting guide does not solve the problem, please contact Technical Support for further assistance.

Switching Issues

Commanding the unit remotely to switch does not cause the unit to switch.

- Check that the Remote Connection is still active. In SSH sessions, query the unit to see if a response is received.
- Consider disconnecting and attempting to reconnect to ensure that the Remote is still accessible.

Remote Connection Issues

An SSH session with the unit cannot be opened.

- Check that the physical connections are correct. See section "Remote Ethernet Connections" on page 12 for more information.
- Check that the IP address settings have been configured properly. See section "10/100BASE-T LAN Setup" on page 13 for more information.
- Ensure that the SSH port being used is correct. Note that the default port numbers are 22 and 10001.
- Check that no other users are currently connected to the switch remotely. If another Remote Control SSH tunnel or logged in GUI session is active, new connections will not be established.

An IP address is not being assigned or the unit is unreachable.

- By default, the unit is configured for DHCP. If the unit cannot obtain an IP address from a DHCP server within the first minutes after booting, the unit will assign itself an IP address via BOOTP.
- If this is the case, it will be necessary to use DeviceInstaller using the "Assign IP Address" feature to force the refresh by resetting it to DHCP (or any other desired setting).
- While the unit is already connected to a network with a DHCP server, power cycling the unit will solve the problem as well.
- Press the Reset button on the rear panel.
- If the problem persists, there may be other network issues. Make sure there are no MAC address filters on the DHCP server or any other part in the network that would prevent this unit from connecting. If such filters exist, they must either be

disabled, or this unit must be added to the whitelist. Please consult the system administrator for further assistance on this.

Remote Login Issues

The password is not being accepted.

- Check that the correct password is being typed.
- Note that passwords are case-sensitive.

The password has been lost/forgotten.

- If the password has never been changed, the default password should still be the valid password. By default, the username and password for SSH access are "admin" and "ESL02921", respectively.
- If the password has been changed from the default and the new password has been lost, the password can be restored to the default by resetting the Remote port and restoring the Remote Configuration GUI. See the "Restoring Factory Defaults from XML" on page 25.

SPECIFICATIONS

Size

Width: 19" (19" full rack size) [48.3 cm] Height: 1.75" (1U) [4.5 cm] Depth: 10.54" [26.8 cm] Weight: 5.4 lbs [2.5 kg]

Environment

Operation Temperature: 0°C to 50°C Storage Temperature: -40°C to 85°C Humidity: 10% to 90% without condensation

Power Requirements

DC Voltage: 12VDC DC Current: 200mA (peak), 90mA (nominal) DC Power: 2.4W (peak), 1.08W (nominal)

Signal Port Ratings

Max Power: 60W, 125VA Max Voltage: 220VDC, 250VAC Max Current: 2A

Signal Port Interfaces

(6) BJ80 BNC (F) Signal ports

Signal Port Channels

(2) Channels of BJ80 BNC A/B/COM ports Simultaneous Control

Signal Port Pins Switched

BJ80 BNC: Center and shell

Remote Port Interface

(1) RJ45 port
 SSH Operation (default ports: 22 or 10001)
 Password protection (default user/pass: admin/ESL02921)

Front Panel Control and Indicators

(3) Red LED's

Power Supply 516682

Input: 100-240VAC, 50/60Hz, 0.2A Output: 12VDC (regulated), 0.5A

CUSTOMER & TECHNICAL SUPPORT

Customer Support

For customer assistance, ordering assistance, or communications cables of any length or configuration, please contact Electro Standards Laboratories, (877) 943-1164 and ask for sales/customer support.

Technical Support

For technical support with unit operation, cable configuration, etc., please contact Electro Standards Laboratories, (877) 943-1164 and ask for technical support. Please have the unit model number and serial number available when you call.