



SX-590-1402
Cryptographic Officer Guidance Manual

Revision A
Date: 2020.10.26

© 2020 silex technology, Inc. All rights reserved.

silex technology and silex technology America SPECIFICALLY DISCLAIMS THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS OF THIS PRODUCT FOR A PARTICULAR PURPOSE. Silex shall not be liable for any errors contained in this manual or for any damages resulting from loss of use, data, profits, or any incidental or consequential damages arising from the use of silex products or services. The information contained in this documentation is subject to change without notice.

Information and descriptions contained herein are the property of silex technology. Such information and descriptions may not be copied, disseminated, or distributed without the express written consent of silex technology. This publication is subject to change without notice.

This product contains software programs licensed under GPL (GNU General Public License) and/or LGPL (GNU Lesser General Public License). Silex Technology, Inc. will provide the source code subject to GPL/LGPL software under terms and conditions of GPL/LGPL to individuals or groups at their own cost by distributing a media such CD-ROM, etc. for a period of at least 3 years after the date of purchase upon written request. Please send the request to the email address below.

Email address: silex_oss@silex.jp

* For the source code, please contact us at the above email address in either Japanese or English.

For details on license information of GPL and LGPL, see below website:

<http://www.silex.jp/products/license/index.html>

Trademarks

All company or product names referenced in this document may be trademarks or registered trademarks of their respective owners.

silex technology, Inc.
www.silexamerica.com

Contents

About This Reference Guide.....	9
Safety Precautions.....	9
Emissions Disclaimer.....	9
Chapter 1: Introduction.....	11
Approved Modes.....	12
PHYSICAL PORTS.....	15
Logical Ports.....	15
Configuration.....	18
Physical Protection.....	19
Secure Operation.....	20
Chapter 2 Installing the SD-330AC-1402 Hardware.....	21
Installing the SD-330AC-1402.....	21
Monitoring Serial Device Server Status.....	23
Chapter 3 Configuring the SX-590-1402.....	24
Basic Configuration Requirements.....	24
Configuration Service.....	25
Using a Web Browser to Configure the SX-590-1402.....	26
Using the Configuration Command Console.....	31
Chapter 4 Using the SX-590-1402 with Your Application.....	34
Customizing the SX-590-1402 User Interface.....	35
Raw TCP connection.....	36
RFC 2217 Remote Modem Control Support.....	36
ECable Connection.....	38
Print Server Emulation.....	39
Serial Data Port Status Console Switching.....	39
Access Point Mode.....	41
Wireless Standard.....	41
Channel.....	41
Channel Band Width.....	41
Supported Authentication/Encryption Mode.....	42
Bridge Mode.....	43
How to Enable the Bridge Mode.....	44
Chapter 5 Advanced Configuration.....	46
Serial Data Port Factory Default Settings.....	46
Restoring Factory Default Settings.....	47
Modifying TCP/IP Settings.....	47
Modifying the Cryptographic Officer Password.....	49
Chapter 6 Troubleshooting.....	50
Chapter 7 Product Specifications.....	52
Appendix A Console Commands.....	56

1. Introduction and command console access information.....	56
2. FIPS 140-2 Mode Configuration Commands.....	57
2.1 SHow FIPS1402.....	57
2.2 SET Link-Compatible Mode.....	57
2.3 SET App-Compatible Mode.....	57
2.4 SET RSA Ciphersuites.....	57
2.5 Zeroize Non Volatile R/W filesystem.....	58
2.6 Execute test.....	58
3. Network Commands.....	58
3.1 SET NW WIRED.....	58
3.2 SH NW.....	59
3.3 SET NW CHannel.....	60
3.4 SET NW MOde.....	60
3.5 SET NW RADio.....	60
3.6 SH NW RATE.....	60
3.7 SET NW RTS.....	61
3.8 SH NW SQ.....	61
3.9 SET NW SSid.....	61
3.10SET NW START.....	61
3.11SH NW MAC.....	62
3.12 SH NW WLLIST.....	62
4. Wireless Network Security Commands.....	63
4.1 SET NW AUTHtype.....	63
4.2 SET NW ENC.....	63
4.3 SET NW WPAPSK.....	64
4.4 SET NW ID.....	64
4.5 SET NW PKPASS.....	64
4.6 SET NW CACERT.....	64
4.7 SET NW CLCERT.....	65
4.8 SET NW CLKEY.....	65
5. Wireless to Ethernet Client Bridging Configuration.....	66
5.1 SET NW BRACCess.....	66
5.2 SET NW BRIDGE.....	66
5.3 SH NW BRIDGE.....	67
5.4 SH NW BRFILTER.....	67
5.5 SET NW BRFILTER.....	67
5.6 SET NW BRFILTERADDR.....	68
5.7SH NW BRFILTERADDR.....	68
6. Port Commands.....	69
6.1Serial Port Commands.....	69

6.1.1 SH PORT.....	69
6.1.2 SET PORT S1 CH.....	69
6.1.3 SET PORT S1 CONSTR.....	70
6.1.4 SH PORT S1 CONSTR.....	70
6.1.5 SET PORT S1 DTR.....	71
6.1.6 SET PORT S1 FLOW.....	71
6.1.7 CLEAR PORT S1 JOB.....	71
6.1.8 SET PORT S1 LATENCY.....	71
6.1.9 SET PORT S1 PARITY.....	72
6.1.10 SET PORT S1 SPeed.....	72
6.1.11 SH PORT S1 STATus.....	72
6.1.12 SET PORT S1 STOP.....	72
6.2 ECable Port Commands.....	73
6.2.1 SET PORT S1 ECABLE.....	73
6.2.2 SH PORT S1 ECABLE.....	73
6.2.3 SET PORT S1 ECADDR.....	73
6.2.4 SET PORT S1 ECCONN.....	74
6.2.5 SET PORT S1 ECENCRYPT.....	74
6.2.6 SET PORT S1 ECLPORT.....	74
6.2.7 SET PORT S1 ECNHOST.....	74
6.2.8 SET PORT S1 ECPORT.....	75
6.2.9 SET PORT S1 ECRADDR.....	75
6.2.10 SET PORT S1 ECRPORT.....	75
6.2.11 SET PORT S1 ECTMMSEC.....	75
6.2.12 SET PORT S1 ECUDP.....	76
7. Server Information Commands.....	77
7.1 SH SERIAL.....	77
7.2 SH SERVER.....	77
7.3 SH SERVER CO.....	78
7.4 SET SERVER DEscription.....	79
7.5 SH SERVER FWVER.....	79
7.6 SH SERVER MODEL.....	79
7.7SET SERVER NAme.....	79
7.8 SHow SERVER QUEue.....	80
7.9 SH SERVER STATistics.....	81
7.10 SH SNMP.....	81
7.11 SET SNMP CONtact.....	81
7.12 SET SNMP GETCOMM.....	81
7.13 SET SNMP LOCation.....	82
7.14 SET SNMP SETCOMM2.....	82
7.15SH VErSion.....	82
8. Service Commands.....	83
8.1 SH SERVI.....	83
8.2 SET SERVI <service name> BOT.....	83
8.3 SET SERVI <service name> EOT.....	83
8.4 SH SERVI STRings [string_num].....	84
8.5 SET SERVI <service name> Filter.....	84
8.6 SH SERVI FILters.....	84

8.7 SET SERVI <service name> FMS.....	84
8.8 SET SERVI <service name> FRS.....	85
8.9 SET SERVI <service name> IP.....	85
8.10 SET SERVI <service name> NAmE.....	85
8.11SET SERVI <service name> POrt.....	85
8.12 SET SERVI <service name> PRlarity.....	85
8.13 SH SERVI PRI [service_num].....	86
8.14 SET SERVI <service name> QUEue.....	86
8.15 SET SERVI <service name> RECeive.....	86
8.16 SET SERVI <service name> TCP.....	86
8.17 SH SERVI SUMMary [service_num].....	86
9. String Commands.....	87
9.1SET STRIng.....	87
9.2 CL STRIng.....	87
9.3 SH STRIng [string_num].....	88
9.4 SH FILters.....	89
10. TCP/IP Commands.....	90
10.1SH IP.....	90
10.2SET IP ACcess.....	90
10.3 SET IP MEmethod.....	91
10.4 SET IP ADdress.....	91
10.5 SET IP SUbnet.....	91
10.6 SET IP ROuter.....	91
10.7 SET IP BOot.....	92
10.8 SET IP KEepalive.....	92
10.9 SET IP HTTP.....	92
10.10 SET IP TFTP.....	92
10.11 SET IP NTP.....	93
10.12 SET IP TCP.....	93
10.13 SET IP LPD.....	93
10.14 SET IP TELnet.....	93
10.15SET IP SX_FLDP.....	94
10.16 SET IP PRObe.....	94
10.17 SET IP Tlmeout.....	95
10.18 SET IP FTlme.....	95
10.19 SET IP REtry.....	95
10.20 SET IP STATus.....	95
10.21 SET IP WIndow.....	96
10.22 SET IP BAnner.....	96

11. DNS Commands.....	97
11.1 SH DNS.....	97
11.2 SET DNS DOMain.....	97
11.3 SET DNS PRImary.....	97
11.4 SET DNS SEConDary.....	97
12. DHCP Server Commands.....	98
12.1 SET DHCPS.....	98
12.2 SH DHCPS.....	98
12.3 SET DHCPS Address.....	98
12.4 SET DHCPS SUBnet.....	98
12.5 SET DHCPS ROuter.....	98
12.6 SET DHCPS LEase.....	99
13. NTP Command.....	100
13.1SET NTP SERVER.....	100
13.2SH NTP DATE.....	100
14. GPIO Control.....	101
14.1 SET GPIO DIR.....	101
14.2 SH GPIO DIR.....	101
14.3 SET GPIO DIRM.....	102
14.4 SH GPIO DIRM.....	102
14.5 SH GPIO SPECial.....	102
14.6 SHow GPIO SPECM.....	103
14.7 SET GPIO DATA.....	104
14.8 SHow GPIO DATA.....	104
15. Firmware Update.....	106
15.1 SET LOAd XModem.....	106
16. Power Management.....	107
16.1 SET NW WLIF.....	107
16.2 SET POWER LEVEL.....	107
17. Other Commands.....	108
17.1 SET ADMIN.....	108
17.2 SET DEFAULT.....	108
17.3 EXIT.....	108
17.4 HEIp <command>.....	108
17.5 INIT.....	109
17.6 SET PAssword.....	109
17.7 SAVE.....	109
18. Compatibility with Other Models.....	110
18.1 SET NW DISCONN.....	110
18.2 SET RM SCAN LOW.....	110
18.3 SET RM THRESH LOW.....	110

Appendix B Firmware Update Procedures.....	111
Appendix C GNU/Linux Open Source and Programming.....	112
Appendix D Silex Contact Information.....	113

Figures

Figure 1 - SX-590-1402 Cryptographic Module.....	11
Figure 2 - SD-330AC-1402 Cryptographic Module.....	12

Tables

Table 1: Approved Cryptographic Algorithms.....	13
Table 2: Allowed Algorithms.....	14
Table 3: Non Approved Algorithms.....	14
Table 4: Physical Ports.....	15
Table 5: Link-Compatible Mode Interfaces.....	16
Table 6: App-Compatible Mode Interfaces.....	17
Table 7: App-Compatible Mode required configuration.....	18
Table 8: Ethernet Status Outputs.....	23
Table 9 - Mode and Wireless Status.....	23
Table 10: Serial Data Port Factory Default Settings.....	46
Table 11 TCP/IP Settings.....	48
Table 12 Product Specification.....	52
Table 13 Radio Performance Specifications.....	53

About This Reference Guide

Safety Precautions

- To prevent damage to the device's electronic circuit components, follow established ESD practices and procedures for handling static-sensitive devices. All ESD-sensitive components must be stored and shipped in ESD-conductive bags or bubble-wrap and labeled as such using the standardized ESD adhesive warning label.
- Ethernet electrical wiring must be at least 6 feet from bare power wiring or lightning rods and associated wires, and at least 6 inches from other types of wire (antenna wires, doorbell wires, wires from transformers to neon signs), steam or hot water pipes, and heating devices.
- Protectors and grounding wire placed by the service provider must not be connected to, removed, or modified by the customer.

Emissions Disclaimer

Regulatory compliance information can be found in by contacting silex technology, Inc. Final emission certification per FCC, CE and other agency requirements are the responsibility of the OEM using any printed circuit assemblies or other items in their final packaged product.

REVISION HISTORY

Rev. No.	Date	Revision by	Comments
A	TBD	Lee Aydelotte	Initial Release



Figure 2 - SD-330AC-1402 Cryptographic Module

Approved Modes

The SX-590-1402 has two approved modes of operation. In the Link-Compatible mode, the Wireless Port data link is encrypted. Security is only claimed for the Wireless data link between the SX-590-1402 and the Access Point to which it is connected. No security is claimed beyond the link to the Wireless Access Point.

In App-Compatible mode, in addition to the Wireless Port data link encryption provided by the Link-Compatible mode, the Application TLS service is available to provide TLS transport security on an end-to-end network connection to the Serial Data port.

The tables below indicates the cryptographic algorithms provided by the module. The additional algorithms listed on the certificates are tested but not used by the module.

CAVP Cert	Algorithm	Standard	Mode/ Method	Key Lengths, Curves, or Moduli	Use	Approved Modes Using the Algorithm
C1997	AES	FIPS 197 SP800-38A	ECB, CCM	128, 256 ²	Data Encryption / Decryption	Link-Compatible App-Compatible
	AES	FIPS 197 SP800-38A	CBC, GCM ³	128, 256	Data Encryption / Decryption	App-Compatible
	RSA	FIPS 186-4	PKCS #1.5, SHA-256	4096	Digital Signature Verification	Link-Compatible App-Compatible
	CVL	SP 800-56B	RSADP	2048	Key Unwrapping	App Compatible
	SHS	FIPS 180-4	SHA-1, SHA-256		Message Digest	Link-Compatible App-Compatible
	SHS	FIPS 180-4	SHA-384		Message Digest	App-Compatible
	HMAC	FIPS 198-1	HMAC-SHA-1, HMAC-SHA-256,	128 256	Message Authentication	Link-Compatible App-Compatible
	HMAC	FIPS 198-1	HMAC-SHA-384	384	Message Authentication	App-Compatible
C2191	DRBG	SP800-90A	CTR -AES	256	Deterministic Random Bit Generation	Link-Compatible App-Compatible
C2011, C2017	KDF	SP 800-108	HMAC-SHA-1 HMAC-SHA-256		Key Derivation	Link-Compatible App-Compatible
C2012	KDF-TLS	TLS 1.2 SP800-135 rev 1			Key Derivation	App-Compatible

Table 1: Approved Cryptographic Algorithms

The module also uses the following allowed algorithms

² The 256 key size is only used in the AES-ECB prerequisite required for AES-GCM-256; the module does not support AES-CCM-256.

³ AES GCM IV generation is performed in accordance with Scenario 1 of IG A.5 TLS 1.2 protocol IV generation. The application closes the TLS session after 2⁴¹ bytes have been transferred, so the IV will be incremented at most 2⁴¹ times (at 1 byte/TLS record worst case) which is less than the 2⁶⁴ limit.

Algorithm	Caveat	Use	Approved Modes Using the Algorithm
Hardware NDRNG		Seeds the DRBG with a minimum security strength of 112 bits	Link-Compatible App-Compatible
TLS v1.2 RSA key wrapping	allowed until 2023.12.31 per FIPS 140-2 IG D.9 RSA-based key wrapping/unwrapping algorithm that uses an RSA modulus that is 2048 bits long.	Key Wrapping	App-Compatible

Table 2: Allowed Algorithms

The module uses the following non-approved algorithms. These non-approved algorithms are only available in Non-Compatible mode, which is not an approved mode of operation.

Algorithm	Use
MD5	Wireless link establishment in Non-Compatible mode
RC4	Wireless link encryption in Non-Compatible mode
HMAC-MD5	Wireless link establishment in Non-Compatible mode
ECC DHE (non-compliant)	Key Agreement in Non-Compatible mode
ECDSA (non-compliant)	Key Generation for Key Agreement in Non-Compatible mode
RSA (non-compliant)	CA Public Key Chain Validation of peer in Non-Compatible mode
RSA key wrapping (non-compliant)	RSA key with non-approved key size (not 2048 bits)

Table 3: Non Approved Algorithms

PHYSICAL PORTS

The following physical ports are available on the SX-590-1402

Port Name	Sub-Port name	Description
System connector		High density connector with pins assigned for the sub-ports listed below.
	Power	Power (+5V and ground) connections
	Ethernet	Ethernet 10/100 wired network interface
	Serial Data port	Serial Port for data transfer
	Serial Configuration Port	Serial port for Configuration and status
	Serial System Console Port	Serial port for status
	Control button input	Control input, active low
	LED status output	Status outputs, active low and connected to LEDs on the SD-330AC-1402
Wireless		u.FL connector for antenna attachment

Table 4: Physical Ports

For installation and connection of the interface ports, refer to Chapter 2.

Logical Ports

The SX-590-1402 has logical interfaces for transfer of data and for configuration and control of the unit. These logical interfaces may share a physical port. The application firmware in the SX-590-1402 separates and routes the data to the appropriate internal firmware task associated with the logical interface. For network ports (Ethernet, Wireless) this separation is based on the TCP or UDP protocol port number. For the serial port, data or control/status mode is controlled by specific protocol strings, only one mode is active at a time.

The following table describes the logical interfaces of the unit when operating in the FIPS 140-2 approved link mode.

FIPS-140-2 Interface	Physical Interface	Logical Interface
Data Input	Serial Data Port	Plaintext data for transmission to network
	Ethernet	Plaintext data for bridging to wireless network
	Wireless	Ciphertext data for Serial or Ethernet port
Data Output	Serial Data Port	Plaintext data received from wireless network
	Ethernet	Plaintext data received from wireless network
	Wireless	Ciphertext data from Serial or Ethernet port

FIPS-140-2 Interface	Physical Interface	Logical Interface
Control Input	Ethernet	Plaintext Control data for Configuration Service received via Telnet
		Control data for Configuration Service received via HTTP
		Discovery Request via silex custom UDP port
	Wireless	Control data for Configuration Service received via Telnet
		Control data for Configuration Service received via HTTP
		Discovery Request via silex custom UDP port
	Control Button Input	Invoke configuration reset
	Serial Configuration Port	Control data for configuration service
	Serial System Console Port	Control data for configuration service
	Serial Data Port	Control sequence entry to invoke CLI status task
Status Output	Ethernet	Status response from Configuration Service via Telnet
		Status response from Configuration Service via HTTP
		Discovery request response
	Wireless	Status response from Configuration Service via Telnet
		Status response from Configuration Service via HTTP
		Discovery request response
	Serial Data Port	status from CLI status query
	Serial Configuration Port	status messages from Configuration Service
Serial System Console Port	status messages	
Power Interface	LED status output	Indicate operating mode, link status and unit error status
	Power input	

Table 5: Link-Compatible Mode Interfaces

Please note that in Link-Compatible mode, all application level data is considered plaintext. Only the wireless link is considered ciphertext due to the link encryption thereon. In App-Compatible mode, application level ciphertext transport is available on a limited number of ports.

The following table describes the logical interfaces of the unit when operating in the FIPS 140-2 approved App-Compatible mode.

FIPS-140-2 Interface	Physical Interface	Logical Interface
Data input	Serial Data Port	Plaintext data for transmission to network application.
	Ethernet	Ciphertext data from designated TCP socket *
	Wireless	Ciphertext data from designated TCP socket * Note: Only Ethernet or Wireless interface is active for a current session, determined by the existence (or not) of an Ethernet link during the module initialization

FIPS-140-2 Interface	Physical Interface	Logical Interface
		* Note: After 2 ⁴¹ bytes have been transferred on any one encrypted serial to network connection, the connection will be closed. This forces a new connection to be established with a new session key.
Data Output	Serial Data Port	Plaintext data received from wireless application
	Ethernet	Ciphertext data received from Serial data port to designated TCP socket
	Wireless	Ciphertext data received from Serial data port to designated TCP socket
Control Input	Ethernet	Control data for Configuration Service via HTTPS
		Discovery Request via silex custom UDP port
	Wireless	Control data for Configuration Service via HTTPS
		Discovery Request via silex custom UDP port
	Control Button Input	Invoke configuration reset
	Serial Configuration Port	Control data for Configuration Service
	Serial System Console Port	Control data for configuration service
Serial Data Port	Control sequence entry to invoke CLI status task	
Status Output	Ethernet	status data via HTTPS
		Discovery Request response
	Wireless	status data via HTTPS
		Discovery Request response
	Serial Data Port	status from CLI status query
	Serial Configuration Port	status messages from Configuration Service
	Serial System Console Port	status messages
LED status output	Indicate operating mode, link status and unit error status	
Power Interface	Power input	

Table 6: App-Compatible Mode Interfaces

When the module enters an error state, all Data Input and Data Output interfaces are disabled. If an error state is encountered, the LED status output will indicate the error by blinking in a pattern until the unit is reset. The unit will not send or receive any data until the reset is complete.

The SX-590-1402 performs cryptographic self tests during initialization after power up or a firmware induced reset. Until the self tests are complete, no data input or output interfaces are active. If the self test fails, the unit will enter an error state.

The Data Output interfaces are logically disconnected from the processes that perform key generation and zeroization. No plaintext key information is output through the Data Output interfaces or Status interfaces at any time.

Configuration

The Cryptographic Officer is responsible for configuring the unit for use in the target environment. See Chapter 3 for instructions on configuring the unit. The peripheral unit (usually a PC) being used to configure the SX-590-1402 must be directly connected to the unit via a crossover cable or local hub which is not connected to any LAN, WLAN or other larger network. This will enable manual transport and electronic entry of secret and private keys (RSA private key and WPA Pre-Shared Key) in a plaintext form. Even if RSA private keys are protected with a PEM passphrase when entered, they are still considered to be in plaintext form.

The SX-590-1402 has three operating mode settings: Link-Compatible, App-Compatible, and Non-Compatible. If Link-Compatible mode is not enabled, the unit operates in the Non-Compatible mode.

When the SX-590-1402 operates in a FIPS 140-2 approved mode, Wireless port link encryption is required. The wireless security configuration must be set as shown in the table below. Use with these parameters set to any value not in the table is not FIPS 140-2 compliant.

Item	Required Setting
Wireless Encryption Mode	WPA2 (AES-CCMP)
Wireless Authentication	PSK
Radio mode	Infrastructure

In App-Compatible mode, the following application parameters must be set as shown in the table below:

Item	Setting
NW BRIDGE	Disable
APPTLS TLSECC	Disable
APPTLS TLSRSA	Enable
APPTLS CACERT	Not Configured

Table 7: App-Compatible Mode required configuration

In App-Compatible mode, the transport protocols are limited to those using approved encryption. If the encryption option is used for the raw TCP port protocol, or the ECable protocol, App-Compatible mode must be enabled. In addition, the Ethernet port to Wireless port bridging option must be disabled in App-Compatible mode.

In App-Compatible mode, the Cryptographic Officer must load a 2048 bit RSA key pair. No other size is allowed in the approved mode of operation.

The compatible mode and Non-Compatible mode configurations are kept separate. No operations in Non-Compatible mode affect the compatible mode configuration (and vice-versa).

ECC DH Ephemeral Key Agreement cannot be used in the approved modes.

The SX-590-1402 implements a Non-Compatible mode which allows other security settings for interoperability in non FIPS 140 environments. However, use of the SX-590-1402 in the Non-Compatible mode is not FIPS 140-2 compliant.

In particular, the WPA2-WPA transition mode is NOT FIPS 140-2 compliant. Only networks exclusively using WPA2 (AES-CCMP) encryption comply.

Separate configurations are maintained for the compatible modes and the non-compatible mode. The current security settings for the device in the currently active mode may be observed by the Cryptographic Officer logging into the unit web server, or by logging in to the configuration console task. The Link-Compatible security parameters may be viewed and set by navigating to the network security page, or with the configuration console command SHOW NW. The application security parameters may be viewed by navigating to the web server TCP/IP page, or by using the configuration console SHOW IP and SHOW APPTLS commands. This should be done after configuration and before use to verify that the device is properly configured for the intended target environment.

The SX-590-1402 is validated at level 1, which means it has no physical security beyond the physical protection of the IC packages, and is presumed to be used in a secure environment. If the unit is to be left unused in an unsecured area, or is to be transported to a new location via unsupervised means, it is recommended that the Cryptographic Officer zeroize the device. This is done by configuring the unit for operation in Link-Compatible mode, restarting the unit if not already in the Link-Compatible mode, resetting the unit to its factory default settings, executing the configuration console command SET FIPS1402 ZERONV, and then resetting the unit. After zeroization the unit will need to be re-configured before communication in Link-Compatible mode is possible.

The compatible mode and non-compatible mode configurations are kept separate. No operations in non-compatible mode affect the compatible mode configuration (and vice-versa).

The default setting in compatible mode includes a known PSK value. The Cryptographic officer MUST configure the device with a different PSK value before operating the device. Operation of the device using the default PSK value is NOT FIPS 140-2 compliant. The Cryptographic Officer must be aware that all configuration program inputs are in plaintext for purposes of FIPS 140-2 compliance regardless of the transport encoding used. The only FIPS 140-2 cryptographic protection claimed for this module in the Link-Compatible mode is for the wireless link between the unit and an associated Access Point. For the App-Compatible mode, the protection claimed is for the TLS protected TCP sockets transferring data to and from the Serial Data Port.

The WPA2-PSK value must be entered by the Cryptographic officer on an isolated network with the machine containing Cryptographic Officer's web browser directly connected to the SX-590-1402 and not connected via a LAN. The WPA2-PSK value must be entered using the Configuration CLI. The same is true for entry of externally generated RSA private keys/public certificates.

The Cryptographic officer must zeroize the module when transitioning the device configuration from a FIPS-140-2 approved mode to a non-approved mode.

Physical Protection

There are no user serviceable parts inside the SX-590-1402 module. The Cryptographic Officer should zeroize the module before the SD-330AC-1402 enclosure or OEM product incorporating the SX-590-1402 is opened.

Secure Operation

The Cryptographic Officer and any users of the SX-590-1402 module must be familiar with the SX-590-1402 Cryptographic Security Policy and must follow its guidelines for proper operation.

Chapter 2

Installing the SD-330AC-1402 Hardware

The SX-590-1402 is intended to be incorporated into an OEM device. For non-silex technology products utilizing the SX-590-1402, refer to the OEM product installation guide. The information in this section is specific to the SD-330AC-1402 product from silex technology which incorporates the SX-590-1402.

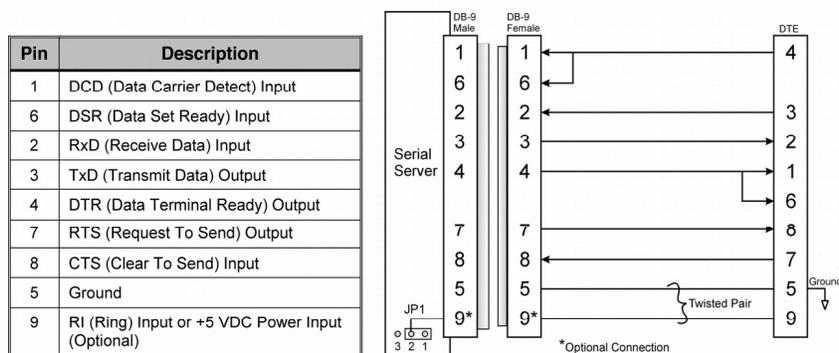
The SD-330AC-1402 is a silex technology product incorporating the SX-590-1402. The SD-330AC shipping kit includes a power adapter for supplying power to the SD-330AC-1402 power input jack. Note that +5V power can also be provided via pin 9 of the SD-330AC-1402 DB-9 connector for the Serial Data Port. The installer will need to provide the Ethernet and/or serial cable to connect your client device to the SD-330AC-1402.

Installing the SD-330AC-1402

Follow the steps below to install the SD-330AC-1402. The unit default settings should be sufficient for many serial connections; however, some of the configuration settings may have to be changed for your particular installation.

- . Before attempting to install the SD-330AC-1402, make sure you have installed and set up your client device as described in the documentation that came with the device.

- . Write down the 12-digit MAC (Media Access Code) address printed on the label located on the bottom of the SD-330AC-1402 (for example: 84253F6C0165). You may need this number in order to configure the Serial Device Server.
- . Connect the SD-330AC-1402 to your client device. If you are using serial RS-232, you may use standard PC cabling (you should normally use a null modem crossover cable). The 9-pin connector pin outs and cabling are as follows:



RS-232 connector pin outs and cabling

If you are connecting to the client device via Ethernet, you will need to use an Ethernet crossover cable to connect the client device to the SD-330AC-1402. Note in this case, you will need to configure the device via a PC connected to the SD-330AC-1402 Ethernet port before you can connect the client device.

- . Plug the SD-330AC-1402 power supply adapter into a suitable AC receptacle, and then plug the power supply cable into the SD-330AC-1402. Alternatively, you can use pin 9 on the 9-pin DB-9 connector to provide power to the Serial Device Server (1 amp @ +5V is required).

When power is applied the SD-330AC-1402 will run through a sequence of power-up diagnostics for a few seconds, then the Orange status led will be lit..

- The unit powers up configured for Serial Device Server operation, which provides for connection from the network to the client device connected to the Serial Data Port of the SD-330AC-1402.
- If the orange LED blinks continuously in a regular pattern, or all the LED blink in a patter, a problem exists. If this is the case, try powering the unit OFF and then ON again.

□. Connect the SD-330AC-1402 to the configuration host device you will use for configuration (usually a PC or laptop) directly using a category 5 (CAT5) Ethernet crossover cable. Alternatively, both the host device and SD-330AC-1402 can be connected to an Ethernet hub or switch, as long as no other devices are connected to the nub or switch.. Then cycle power on the device to ensure the unit uses the Ethernet port as the active port for configuration. The wireless networking will not be enabled in this case.

□. The SD-330AC-1402's IP address must be configured before a network connection is available. If the configuration host offers DHCP (Dynamic Host Configuration Protocol), the SD-330AC-1402 will automatically search for a DCHP server upon power up and obtain an IP address. If the configuration host does not offer DHCP, after a few attempts the SD-330AC-1402 will use a default fixed IP address of 169.254.111.111. The default IP parameters may be changed during the initial configuration.

Monitoring Serial Device Server Status

The LED status outputs indicate the operating mode and network (Ethernet and Wireless) port status as shown below.

The Ethernet port status is shown as follows:

SX-590-1402 LED status signal	SD-330AC-1402 LED	Light pattern	Status
GPIO1 GPIO5	RJ45 yellow RJ45 green	Yellow: OFF Yellow Green: OFF	The wired LAN cable is not connected.
		LED Yellow: OFF Green Green: ON	Wired LAN connected by 10BASE-T.
		LED Yellow: ON Green: ON	Wired LAN connected by 100BASE-TX.

Table 8: Ethernet Status Outputs

The SX-590-1402 displays status on 3 GPIO lines as shown in this section. When used in the SD-330AC-1402, the GPIO lines control the LEDs on the top of the enclosure as described.

SX-590-1402 LED status signal	SD-330AC-1402 LED	Light pattern	Status
GPIO8	Orange LED	Off	The unit is not powered
		On	The unit is powered and active
		Blinking*	Firmware update is in progress (Important: Do not power off the module during the update process)
GPIO7	Yellow LED	Off	No wireless link
		Blink	Associated with AP, IP address not acquired
		On	Associated with AP & IP address acquired
GPIO6	Green LED	Off	Non-Compatible mode
		ON	Link-Compatible mode
		Blink	App-Compatible mode
GPIO8 GPIO7 GPIO6	Orange LED Green LED Yellow LED	All blink alternating	Firmware detected error, unit must be reset

Table 9 - Mode and Wireless Status

Chapter 3

Configuring the SX-590-1402

This chapter describes the methods for configuring the basic settings of the SX-590-1402, including the IP address, serial port settings, and wireless security and TCP application security. The SX-590-1402 also has an extensive range of advanced configuration capabilities that are described in Chapter 5, Appendix B. The SX-590-1402 configuration must be done by a Cryptographic Officer with technical knowledge of TCP/IP networking and serial communications.

Basic Configuration Requirements

In order to use the SX-590-1402, the following basic parameters must be configured:

TCP/IP Settings:

- IP Address
- Subnet Mask
- Router Address

Note: The TCP/IP settings can be automatically configured using DHCP.

Wireless Configuration Settings:

- SSID
- Mode (Infrastructure or Access Point)
- Channel (required only if using Access Point)

Wireless Security Settings:

- Wireless Encryption Mode (WPA2, WPA*, WPA2-WPA*)
- Wireless Encryption Settings
- Wireless Authentication Mode (WPA-PSK, Open System*)

* NOTE: these settings are unavailable in Link-Compatible or App-Compatible mode of operation.

Serial Daa Port Settings (must match the settings of the attached client serial device, if any):

- Baud Rate (Speed)
- Parity
- Character Size
- Flow Control

In addition to the above parameters, the Serial Device Server allows you to configure numerous other capabilities. These other capabilities provide you with the unparalleled flexibility to use the Serial Device Server with a wide range of serial devices.

Configuration Service

There are two ways to configure the Serial Device Server:

- *Configuration Web GUI (HTTP/HTTPS).* You can use any standard web browser to access the SX-590-1402 internal web pages. These web pages provide an easy-to-use graphical interface for configuring the unit. In order to use the internal web pages, you must know the SX-590-1402 IP address. If you do not know the address, the silex technology SX-Finder Windows utility can be used to discover the unit, and then connect to the internal web server.
NOTE: HTTPS is not available on a unit set to the factory default values, as the application private key and public key for the unit will not have been configured yet.
- *Configuration Command Console.* The Configuration Command console provides a command line interface for advanced users to configure the SX-590-1402. It can be accessed by connecting a serial cable to the Serial Configuration Port, or it may be accessed via TELNET, or via the Configuration web GUI.

Configuring the SX-590-1402 using each of the above methods is described in the following sections of this chapter.

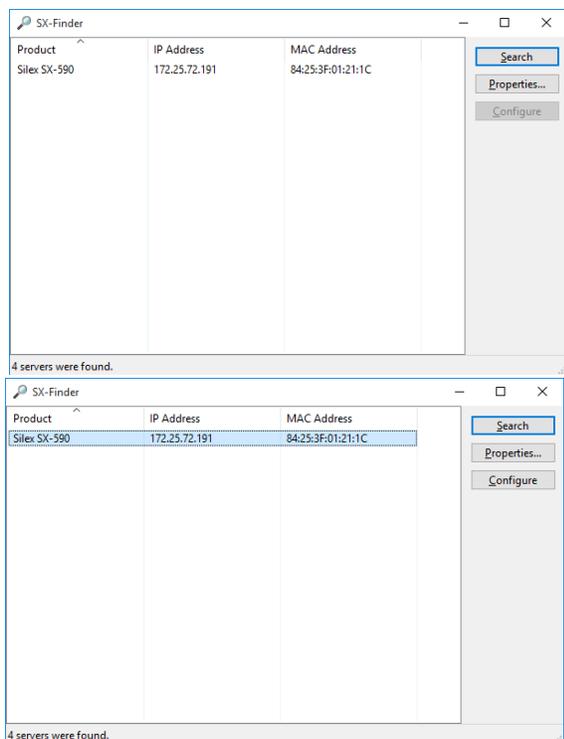
Using a Web Browser to Configure the SX-590-1402

If you do not know the IP address of the target SX-590, use the "SX-Finder" utility (SX-590 module discovery utility). The SX-Finder utility can be downloaded from our website (www.silexamerica.com/). Power on the SX-590 and then start SX-Finder, as shown below. If you know the IP address of the unit, you can go directly to the configuration step.

NOTE: The FIPS 140-2 operating mode and WPA2 PSK value must be configured using the Configuration Console CLI. This can be accessed via the web GUI via the 'Web Console' link in the web GUI. Refer to the Configuration Console section for details on the appropriate commands. The factory default is for the unit to operate in the approved Link-Compatible mode.

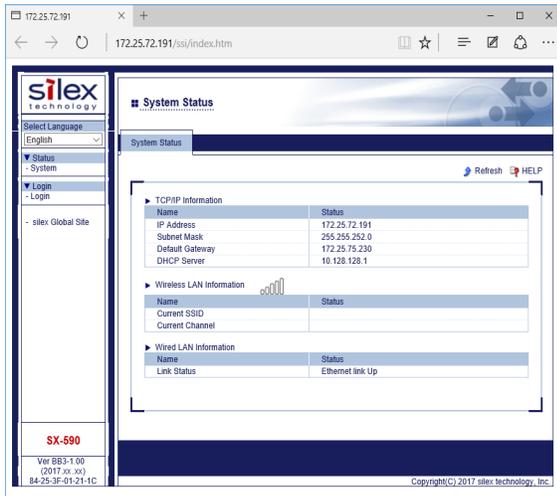
NOTE: If you intend to operate the unit in the Ethernet to Wireless bridge mode, this can only be configured using the Configuration Console CLI. This can be accessed via the 'Web Console' link in the Web GUI. Refer to the Configuration Console section for details on the appropriate commands.

IMPORTANT: You must click the *Submit* button when you have finished configuring an internal web page. If you do not do this, your changes will not be saved.

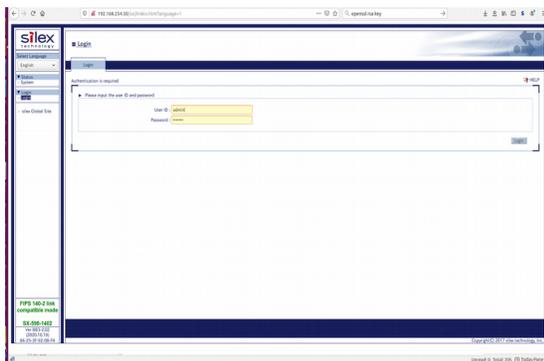


1. Power on the SX-590-1402 and then start SX-Finder. The available SX-590-1402 units will be displayed in the main window of SX-Finder.

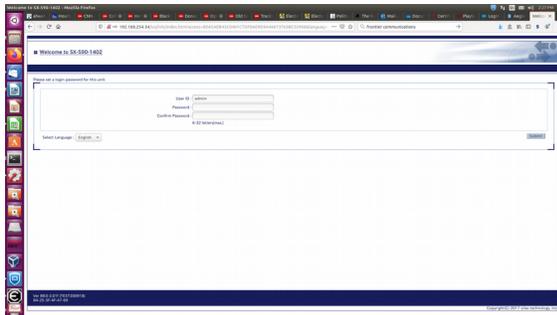
2. Select the SX-590 that you wish to configure and click the **Configure** button. The web browser will run and the internal web page for the unit will be displayed.



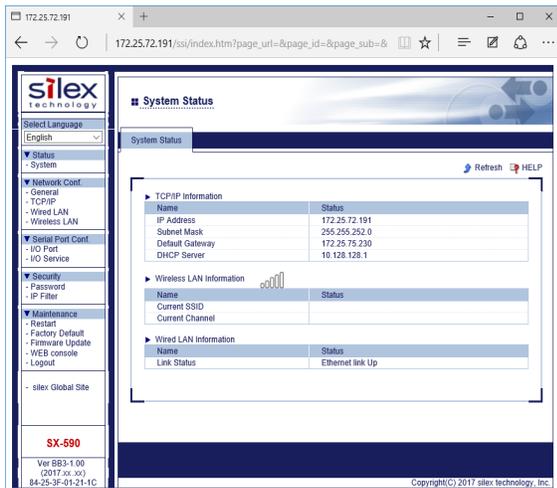
1. When you have connected to the SX-590, you will get the **System Status** page. Click **Login** on the left side of the screen.



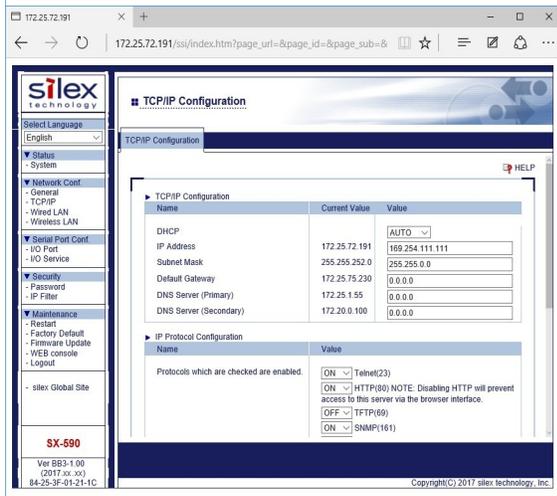
2. Enter the Cryptographic Officer user name and password in the fields provided. The default user name is **admin** and the default password is **access**. Press **Submit**.



3. If the password was set to the default value, the password change page will be displayed to change the value from the default password. The user ID may optionally also be changed at this time.



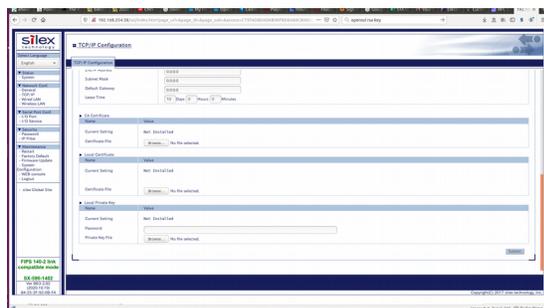
- You will return to the **System Status** page, but new options will be listed on the left side of the screen. Click on **TCP/IP**.



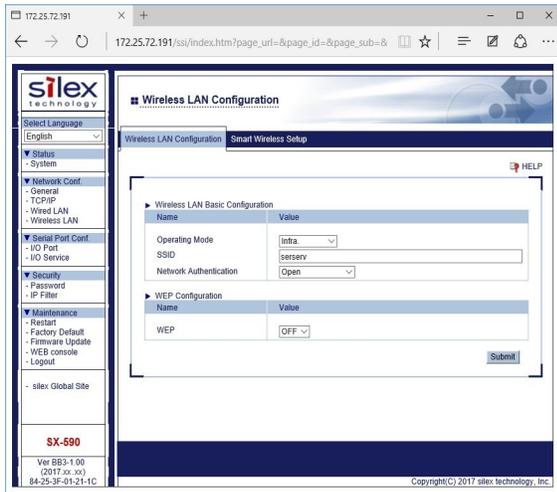
- If you used DHCP, verify that the IP address is correctly set. If you used the default 169.254.111.111 IP address, you should change it to a new valid IP address to prevent an address conflict with other units. If necessary, change the Subnet Mask and Gateway. It is generally not necessary to change the other parameters on this page (refer to Chapter 6 Advanced Configuration for advanced configuration information).

Click the **Submit** button at the bottom of the window (you may need to scroll) to save your changes.

NOTE: If you are using DHCP on your network, the SX-590-1402 should have acquired valid IP settings at this point and no further configuration is necessary. However, for some installations, a static IP address is preferred. If your DHCP server does not allow the SX-590-1402 to keep its assigned IP address permanently, then you must manually assign an IP address. In this case, use a static IP address outside the range reserved for DHCP (see your DHCP server documentation for details). To assign a static IP address, select **Set Permanent** as the **IP Address Resolution**.



- If you plan to use application TLS encryption, scroll down to the bottom of the TCP/IP page. Browse to enter the file names for the private key and local certificate with the public key that are to be used. Click **Submit** to download them into the unit.



- Click **Wireless LAN** on the left side of the screen to configure the 802.11a/b/g/n/ac wireless settings. The SX-590-1402 settings must be configured with the wireless configuration and security parameters required to allow the SX-590-1402 to communicate over the target wireless network (check with your network administrator if you do not know these parameters).

Select either **Infra.** (if you want to connect via an access point) or Access Point for wireless mode.

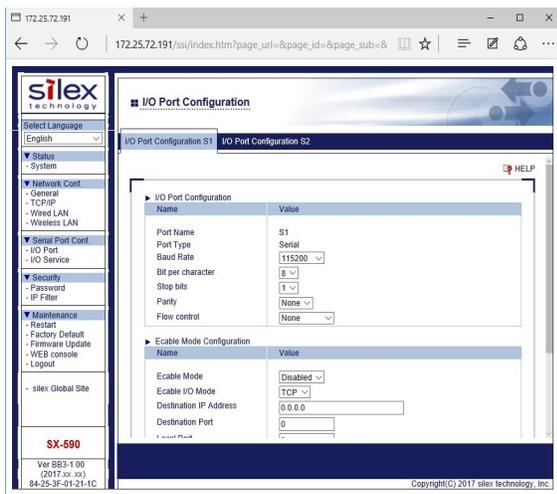
Enter the SSID for your network

If you use **Access Point**, select the RF channel (this is not required for **Infrastructure**).

Select the appropriate network authentication and encryption modes and enter the required settings (check with your network administrator for the proper settings if you do not know them).

NOTE: If the WPA2 PSK value is set to the factory default value (indicated by a red warning message in the menu pane on the left), you must enter a new valid 256 bit PSK value in order to be FIPS 140-2 compliant. The PSK value must be entered using the Configuration CLI.

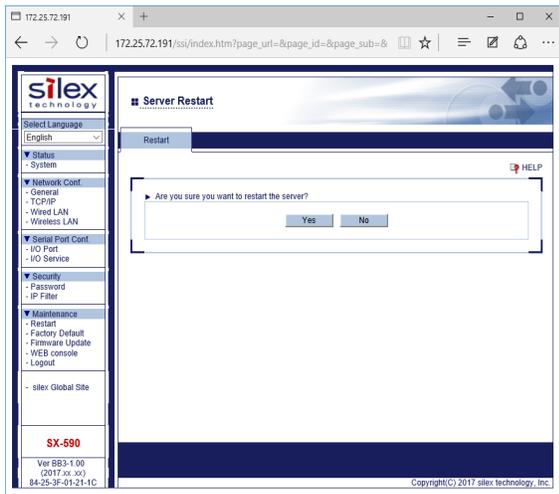
Click the **Submit** button at the bottom of the window (you may need to scroll) to save your changes.



- If connecting the client device via the Serial Data Port, click **I/O Port** on the left side of the screen and then click **I/O Port Configuration S1** to configure the Serial Data Port.

Configure the serial port settings so that they match the settings on your client device. For example, if your device is set for 9600bps, odd parity, and XON/XOFF flow control, you must change the settings on the SX-590 to these settings.

Click the Submit button at the bottom of the window (you may need to scroll) to save your changes.



9. When you have finished with all your configuration changes, you must restart the SX-590-1402 for these changes to take effect.

To restart the SX-590-1492, click **Restart** on the left side of the screen and click **Yes** in the page displayed.

This completes the basic device set up via the web GUI. Y

Using the Configuration Command Console

You may skip this section if you have completely configured the SX-590-1402 using the Configuration GUI Web Pages.

The Configuration Command Console is a command line (CLI) oriented method for configuring the SX-590-1402. It provides more comprehensive capabilities than the Internal Web Pages, but is not as easy to use. Advanced users may prefer to use this method because it is concise, fast, and powerful. This section describes the basic configuration of the unit. The full list of Configuration Console commands is found in appendix A

To use the Configuration Command Console:

1. The simplest way to access the Configuration Command Console is with a PC via a terminal emulator (for example, a Windows PC running the TeraTerm connected to the Serial Configuration port.

NOTE: The Serial Configuration Port is not accessible on the SD-330AC-1402.

The Configuration Command Console can also be accessed via the Configuration web GUI, by selecting the 'Web Console' link.

The Configuration Command Console can also be accessed via the network Telnet protocol, if the current mode of operation allows.

2. If connected via the Serial Configuration Port or via Telnet, enter the Cryptographic Officer user ID and password when prompted. This is not required when accessing the Configuration Command Console via the Configuration web GUI, as you have already logged in to the web GUI to allow access.
3. If the Cryptographic Officer password is set to the factory default value, you will be prompted to enter a new Cryptographic Officer password for the unit. Enter the new password, and finish with the <ENTER> key. .
4. When you see the *Local*> prompt, you can enter commands (note that this command may take up to 30 seconds to appear if you are using Serial Port 2). The SX-590 is set by default to use DHCP to obtain the IP address automatically, and use the configured fixed address if DHCP does not succeed . If you want to set the IP address manually, enter the following commands:

```
SET IP METHOD STATIC
SET IP ADDRESS aa.bb.cc.dd
SET IP SUBNET aa.bb.cc.dd
SET IP ROUTER aa.bb.cc.dd
```

Where *aa.bb.cc.dd* is the IP address of the SX-590. You can use the command SHOW IP to verify the IP address settings. If you want the unit to keep trying DHCP forever until it gets an address (never use the fixed fallback address), enter

```
SET IP METHOD DHCP
```

5. Enter the basic wireless settings as follows:

SET NW SSID <name> [where <name> is the SSID for your network]
SET NW MODE <mode> [where mode is INFRASTRUCTURE or AP*]
SET NW CHANNEL n [Only in AP mode]
* This options are not available in an approved mode of operation (Link-Compatible or App-Compatible).

6. Use the appropriate SET NW command to set wireless encryption mode and authentication type (check with your network administrator for the proper settings if you do not know them):

SET NW ENC <mode> [sets encryption mode, where <mode> is WPA*, WPA2, WPA2-WPA*]
SET NW AUTHTYPE <type> [sets authentication type, where <type> is OPEN*, PSK).
* These options are not available in an approved mode of operation (Link-Compatible or App-Compatible).

For WPA2-PSK or WPA-PSK, enter the command:

SET NW WPAPSK <psk> [sets pre-shared key for WPA2 or WPA, where <psk> is the key
NOTE: in approved modes of operation, this must be 64 hex digits reflecting a suitable randomly generated 256 bit value. Passphrases are not allowed
NOTE: If set to the default WPAPSK value, a new value must be entered to be FIPS 140-2 compliant]

Enter the following command to save the new wireless configurations

SAVE

7. To set the Serial Data Port, enter the following commands:

SET PORT S1 SPEED <baudrate> [where <baudrate> is 300 to 3000000]
SET PORT S1 PARITY <parity> [where <parity> is ODD, EVEN, or NONE]
SET PORT S1 SIZE <databits> [where <databits> is 7 or 8]
SET PORT S1 FLOW <flowcontrol> [where <flowcontrol> is NONE, XON/XOFF, or CTS,]

The console commands are summarized in Appendix A of this manual.

8. When you have finished entering commands, unless using the Configuration CLI, type:

```
INIT  
EXIT
```

If using the Configuration GUI, enter

```
SAVE
```

then click on the Restart link in the GUI menu pane.

These commands will save the configuration and restart the unit. You are now ready to use the SX-590-1402

IMPORTANT: The console command EXIT or SAVE must always be used in order to save the changes you made with the Configuration Command Console.

Chapter 4

Using the SX-590-1402 with Your Application

The Serial Device Server includes a number of capabilities that enable it to be used in a wide range of applications. These capabilities include:

1. Customizing the SX-590 User Interface
2. Raw TCP connection
3. RFC 2217 Remote Modem Control Support
4. ECable Connection
5. Print Server emulation

These methods are described in the following sections.

Customizing the SX-590-1402 User Interface

The SX-590 user interface can be customized to include your company's name or other information. The 3-character OEM code used in the SX-590 server name and service names can be changed from the default code **SDS** to a user-defined code. For example, by changing the OEM code to XYZ, the default server name **SDS000345** would become **XYZ000345**. To make these changes, enter the following commands using the Configuration Command console:

```
SET OEM code where code is the desired 3-character OEM code
SET DEFAULT [note that this resets the entire SX-590 configuration back to the factory defaults]
SET SERVER DESC description      where description is any string up to 32 characters in
length
                               [note that spaces are OK in the description and no quotation marks are necessary]
INIT [restarts the SX-590-1402 when the user exits the console]
EXIT [exits the console]
```

IMPORTANT:

This user interface customization must be done *before* making any other configuration changes, because the SET OEM command requires that the SX-590 be reset to the factory default configuration.

Raw TCP connection

You can communicate directly from your application program to the SX-590-1402 Serial Data Port using a raw TCP connection. This is done by opening a TCP port on the SX-590-1402 and then sending and receiving data to this port via a socket or equivalent API.

If you are using a raw TCP connection, the default TCP port number is either 9100 or 3001 for the Serial Data Port. The port number can be changed through the services option of the Configuration web GUI or the Configuration Console.

You can change the port number, if desired, by modifying one of the SX-590-1402 data services. To change the TCP port number:

1. Connect to the SX-590-1402 with a web browser (see Chapter 3 Configuring the SX-590-1402 for instructions on doing this);
2. After you have logged in, click **I/O Services** on the left side of the page.
3. Click on the service name that you want to change (any one of the services is OK, provided that you are not using the existing TCP port number of that service for a different application).
4. Change the **Raw TCP Port** to the desired number (must be greater than 1024).
5. Click **Submit** to save your change.

The TCP port number for the data service can also be changed via the Configuration Console commands, as defined in Appendix A.

You can test this connection by using the TELNET utility from the Windows Command Prompt (MS-DOS prompt), Mac OS X Terminal Utility, or UNIX/Linux command line as follows:

```
telnet ipaddress portnumber
```

Where *ipaddress* is the IP address of the SX-590-1492 and *portnumber* is the SX-590-1402 TCP port number. For example:

```
telnet 192.168.5.53 9100
```

NOTE: In App-Compatible mode, Telnet is not available and the encryption option for the data service must be used.

RFC 2217 Remote Modem Control Support

If you want to be able to access your device's modem control signals from your computer system, then the TCP port number is 9200 for the Serial Data Port. This socket provides RFC 2217 support, which is used by many host Serial Port Emulator programs.

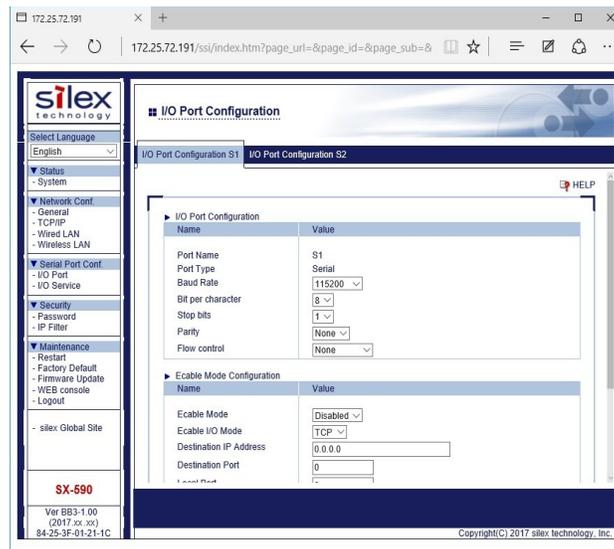
RFC 2217 allows you to access your device's modem control signals over the network. It is especially useful for migrating applications that use modem controls from a direct serial connection to a serial device server network connection. You can utilize RFC 2217 from the application program by connecting to TCP port 9200 from your application program.

NOTE: In App-Compatible mode, this option is not available as no TLS encryption is available for it.

ECable Connection

Normally, it is up a remote host to initiate a network connection to the SX-590-1402. For some applications, it is desirable for the SX-590-1402 r to initiate the connection to a remote host. The Serial Device Server supports this capability through its ECable feature.

To set ECable mode, use a web browser to access the Serial Device Server internal web pages (see chapter 3 for instructions on using the Configuration GUI web pages). After you have logged in, click I/O port on the left side of the screen.



You can now enable ECable mode and set the required parameters.

1. Select the S1 port.
2. Enable ECable mode by clicking the drop-down list.
3. Enter the address (Destination IP Address) of the computer or other device that will be communicating with the SX-590-1402)
4. Enter the TCP port number (Destination Port) used by the destination device for communicating with the SX-590-1402 (must be greater than 1024).
5. If desired, change the ECable Connection Attempt Time. This specifies the time interval between connection attempts. For example, by default the SX-59001402 will try once every 30 seconds to make a connection to the destination device; if it fails to make this connection, it will wait 30 seconds before attempting again. Changing this interval will reduce or increase the amount of network traffic.
6. It is also possible to use UDP instead of TCP for communicating to and from the SX-590. If you wish to use UDP, then in addition to the steps above:
 - a. Select UDP as ECable I/O Mode. Enter the UDP port number (Destination Port) used by the destination device to communicate with the SX-590-1402. This number must be a valid port on the destination device (check the documentation for that device to determine the valid port numbers). If the Destination Port number is zero, the SX-590-1402 will not send any data to the remote host.

- b. Enter the UDP port number (Local Port) used by the SX-590-1402 to communicate with the destination device. This number must be greater than 1024, but is otherwise arbitrary. If the local port number is zero, the SX-590-1402 will not receive any data for the Serial Data Port.

NOTE: In App-Compatible mode, the ECable encryption option must used. The UDP option is not available.

Print Server Emulation

You can use the SX-590 as a standard TCP/IP print server, which is very useful if you are connecting the SX-590 to a serial printer. The SX-590 supports the following standards:

- *lpr/lpd*. This is one of the most popular ways to print on a TCP/IP network. Check your computer's documentation to determine how to set up an lpr print queue. Usually this simply involves specifying the IP address of the Serial Device Server as the printer's address or host name. Some implementations require a queue name; this name is the name of any of the SX-590-1402 Serial Data services. To see the names of the SX-590-1402 Serial Data services, connect to the unit with a web browser (see chapter 3 for instructions on doing this); after you have logged in, click I/O Services on the left side of the page, or inquire via the Configuration Console CLI (see Appendix A).
- *Port 9100*. This method uses the Raw TCP service described above to set up a Windows Standard TCP/IP port. To use this capability on Windows with the *Add Printer Wizard*, specify that you want to use a **Local printer attached to this computer** (not a network printer), and then select **Create a new port**, specifying **Standard TCP/IP Port** as the type of port.

It is also possible to change the TCP port number from the default 9100 for compatibility with other printer manufacturer's software. To do this, refer to the instructions in the *Raw TCP Connection* section of this chapter.

NOTE: In App-Compatible mode, this option is not available as no TLS encryption is available for it.

Serial Data Port Status Console Switching

The SX-590-1402 allows the serial data port to dynamically switch to limited status console operation. In this state, data input on the Serial Data Port is sent to the limited status console task, and is not sent to the network. The only commands available from the limited status console are:

SH VER	Displays the system firmware version
SH NTP DATE	Shows the GMT+00 time setting of the unit.
EXIT	Return to normal data mode.

To switch the serial port to console mode, you must first define a console mode string. When the SX-590-1402 receives this string on the Serial Data Port, it will automatically enable the limited status console. To define the console mode string, use a web browser to access the SX-590-1402 Configuration GUI web pages. After you log in, click **I/O Port**, and then select S1. When you get the **I/O Port Settings** page,

enter any desired character string (for example, +++) as the **Console Mode String**. Click **Submit** to save your string, and then restart the SX-590-1402 to make the change take effect.

Alternatively, you can define the console mode string using the Configuration Console CLI as shown in the following example:

```
SET PORT S1 CONSTR ++++
```

Access Point Mode

In Access Point mode, the SX-590-1402 module will run as a host device in a wireless network.

Wireless Standard

Details	
IEEE 802.11 a/b/g/n/ac	

Channel

Details	
2.4 GHz band	US 1 ~ 11 ch JP/DE 1 ~ 13 ch
5 GHz band	JP/DE 36/40/44/48 ch (W52) US 36/40/44/48 ch (W52) 149/153/157/161/165 ch (W58)

- The SX-590-1402 module does not support detection of the radar wave which is required for DFS process. Therefore, when running in Access Point mode, the frequency bands (W53/W56) needed for DFS process are not supported.
- When automatic IP address configuration using DHCP is enabled, the AP function does not start until the SX-590-1402 module obtains an IP address.
- After IP address is configured using DHCP, the SX-590-1402 module continues to use that IP address unless the lease time expires.

Channel Band Width

The channel bandwidth changes depending on the operating status.

When 5GHz band channel is used, the SX-590-1402 module operates at 80MHz channel bandwidth. (The client devices can be connected when they are operating at 20MHz/40MHz/80MHz bandwidth.)

When 2.4GHz band channel is used, the SX-590-1402 module operates at 20MHz channel bandwidth. (The client devices can be connected when they are operating at 20MHz bandwidth.)

Supported Authentication/Encryption Mode

When running in the Access Point mode, the SX-590-1402 module supports the following authentication and encryption modes.

Authentication	Encryption
OPEN*	None
WPA-Personal*	AUTO/TKIP
WPA2-Personal	AES

- WEP encryption is not supported.
- WPA-Enterprise/ WPA2-Enterprise /802.1x are not supported.
- When TKIP is used for encryption, the SX-590 module will run in IEEE 802.11a or IEEE 802.11g. When AUTO is used, those client devices linked in TKIP will use IEEE 802.11a or IEEE 802.11g, and those linked in AES will use IEEE 802.11n or IEEE 802.11ac.
- *** In FIPS 140-2 approved compatible modes, only WPA2-PSK-AES is allowed.**

Bridge Mode

The Ethernet to Wireless Bridge Mode supports connecting an Ethernet enabled device to a wireless LAN network

NOTE:

When running in the Bridge Mode, there are the following restrictions:

- Access to the SX-590-1402 module is limited to those on a wired LAN port.
- It is not allowed to use devices with multiple MAC Addresses (e.g. devices with a load balancing feature, etc).
- No Serial Data Port access is allowed from the network

There are following restrictions for Bridge Mode.

- Only TCP/IP(IPv4, IPv6) communication is supported. Communication of other protocols is not supported.
- Bridge function is not available for following IPv6 packets.
 - Inverse Neighbor Advertisement (only one-way communication from wired LAN to wireless LAN is supported.)
 - Fragment Header (transfer as-is)
 - Authentication Header (transfer as-is)
 - Encapsulating Security Payload (transfer as-is)

How to Enable the Bridge Mode

To use the Bridge Mode, change the following three settings by using the Web page or Configuration console of the SX-590-1402 module.

- Bridge Mode
- IP Address
- Wireless LAN setting

By using the Web page:

1. Log into the Web page of the SX-590-1402 module. (For details on how to access the Web page, refer to **Chapter 3 Configuring the SX-590.**)

2. Click **General** from the left menu.

Select **Multi** for **Bridge Mode** in the page displayed.

If you want to limit the client to specific devices, select **ON** for **Device Filter** and set the MAC Address of the device to be connected to the wired LAN port for **Network Device Address**.

Click **Submit** to save the changes.

3. To configure the IP Address, click **TCP/IP** from the left menu.

When running in the Bridge Mode, communication with the SX-590-1402 module is limited Configuration and Status services via the wired Ethernet port. To access the SX-590-1402 module when running in Bridge Mode, a suitable IP Address must be configured.

Click **Submit** to save the changes.

4. To configure the wireless settings, click **Wireless LAN** from the left menu. Configure the SSID and authentication/encryption modes for your wireless network. Click **Submit** to save the changes.

5. Restart the SX-590-1402 module to take effect of the changes. To restart, click **Restart** from the left menu and click **Yes**.

By using the Configuration Console commands:

1. Access the Configuration Console of the SX-590-1402 module. (For details on how to access the Configuration Console, refer to **Chapter 3 Configuring the SX-590-1402.**)
2. To set the Bridge Mode, execute the commands below.

```
SET NW BRIDGE Mul           [Specify Mul to set the bridge mode]
SET NW BRFILTER <En/Dis>    [Enable/Disable device filter]
SET NW BRFILTERADDR <num> <mac addr> [Bridge MAC address
filter setting]
```

3. To configure the IP Address, execute the commands below.

```
SET IP METHOD <AUTO|DHCP|STATIC> [Set the method to
obtain IP Address]
SET IP ADDRESS <ip address>      [Set the IP Address]
SET IP SUBNET <subnet mask>     [Set the subnet mask]
SET IP Router <default gateway> [Set the default
gateway]
```

4. To configure the wireless settings, execute the commands below.

```
SET NW SSID <name>           [Set the SSID]
SET NW MODE INFRA           [Set the operating mode
(Infrastructure only)]
SET NW ENC <mode>           [Set the encryption mode]
SET NW AUTHTYPE <type>     [Set the authentication mode]
```

5. When finished, execute the commands below to terminate the command console.

```
INIT EXIT
```

After these commands are executed, the setting will be saved and the SX-590-1402 module will be restarted. When the restart is completed, the SX-590-1402 module will operate in the bridge mode configured.

Chapter 5 Advanced Configuration

The SX-590 module is equipped with a default configuration values that works for many applications. .

Serial Data Port Factory Default Settings

The table below displays the Serial Data Port configuration parameter descriptions and settings with the default settings indicated in a separate column.

Parameter	Description	Settings	Default Setting
Character	Bits per character	7, 8	8
Flow	Flow control	None, Xon, Xoff, CTS/RTS	None
Parity	Parity	None, Even, Odd	None
Speed	Baud rate of bits per second	300, 1200, 2400, 4800, 9600, 19200, 38400, 57600, 115200, 230400, 460800, 921600, 3000000	115200
Stop	Stop bits per character	1, 2	1
Ecable	ECable mode for TCP connections	Enable, Disable	Disable
Ecaddr	ECable destination IP address	Set by user	N/A
Econn	ECable connection attempt time	1-255 seconds	30 seconds
Ecport	ECable destination TCP port number	Set by user	N/A
Eclport	ECable destination local IP port number (required for E-Cable UDP mode only)	Set by user	N/A
Ectmmsec	Cable connection time resolution	Enable, Disable	Disable
Ecudp	ECable UDP mode	Enable, Disable	Disable

Table 10: Serial Data Port Factory Default Settings

Restoring Factory Default Settings

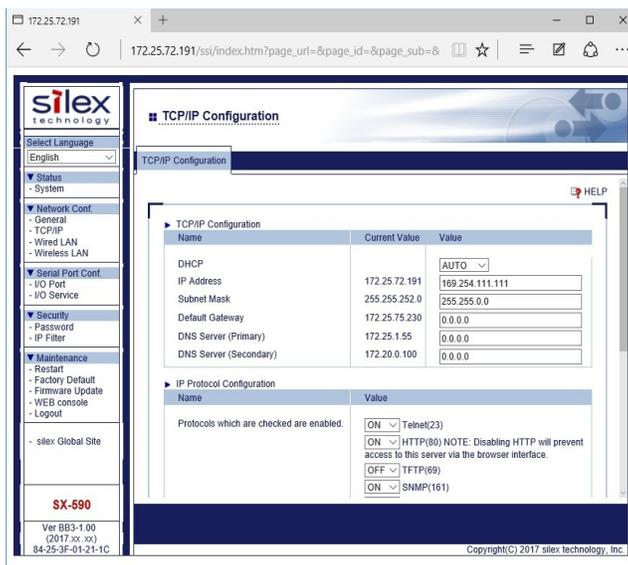
The factory default settings can be restored at any time. Both the Configuration web GUI and the Configuration Console CLI have commands for restoring the default values. In addition, holding the Control Button Input low (pressing the button on the SD-330AC-1402) for more than five seconds will reset the configuration to factory defaults, and then reset the unit. Holding the Control Button input low will also reset the Cryptographic Officer ID and password, if they have been forgotten.

Modifying TCP/IP Settings

You can modify the TCP/IP settings using the web browser interface or the Serial Device Server Serial Device Server's internal configuration console.

To modify TCP/IP settings:

1. You can configure the TCP/IP settings using the Web Page configuration. Simply log in using the Serial Device Server IP address and select **TCP/IP**.



- . Verify the settings, as defined in Table 11.

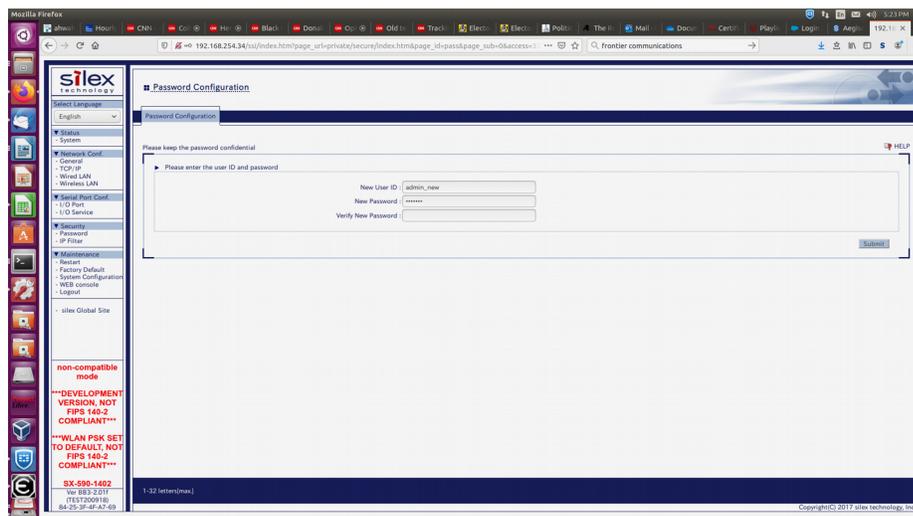
Table 11 TCP/IP Settings

Parameter	Setting
IP Address	To assign a static IP address, enter it in this field The IP address must follow the format XXX.XXX.XXX.XXX, where each XXX is a number between 0 and 255. The default IP address mask is 192.0.0.192.
Subnet Mask	To assign a static subnet mask, enter it in this field The subnet mask must follow the format XXX.XXX.XXX.XXX, where each XXX is a number between 0 and 255. The default subnet mask is 0.0.0.0. The server interprets a subnet mask of 0.0.0.0 or 255.255.255.255 as no subnet mask specified.
Default Gateway	Sets the default gateway, if your network is attached to other networks
DHCP	Sets an IP address configuration method by selecting from DHCP (obtaining from a DHCP server only), STATIC (assigning a static IP address manually) or AUTO (try to find a DHCP server first, use Static settings if DHCP fails). To assign an IP address using DHCP, a DHCP server must be running in your subnetwork.
DNS	Sets the Primary/Secondary DNS server address when it is necessary.

For the changes to become effective, click the **Submit** button, then reset the Serial Device Server.

Modifying the Cryptographic Officer Password

To change the Cryptographic Officer user ID or password, select the **Password** option on the menu.



Enter a the new password desired. Optionally, the user ID may be changed. If the user ID is changed, a new password must be entered. Click **Submit** to save the changes.

NOTE: Unlike many configuration changes, the new password (and ID if changed) take effect immediately. Any current Configuration session remains logged in, but new sessions will need to use the new credentials entered.

Chapter 6

Troubleshooting

If you have experience problems with the SX-590-2702, please check the following troubleshooting steps:

1. Make sure that you are getting power to the SX-590-1402. If it is not on, check the power supply connections, and if possible, try a different SX-590-1402 unit.
2. Make sure that you have a valid network connection.
 - a. Make sure that your network is operating properly (that is, other devices should be able to communicate using the same hub, switch, or access point that the SX-590-1402 is connected to).
 - b. If you are using the wired Ethernet port, the hub or switch to which it is connected should have a status LED lit. If it is not, make sure that the cable is properly connected, and if possible, try a different Ethernet cable.
 - c. If you are using a wireless connection, double check your wireless settings. The SSID and security parameters must exactly match the requirements of the access point in order for the SX-590-1402 to communicate on an infrastructure wireless network. .
 - d. Make sure that you have a valid IP address, subnet mask and router address (check with your network administrator to make sure that you have the correct information). r by using the PING command from a computer system connected to the network.
3. If you have a valid network connection and IP address, but you cannot communicate with your serial device, then:
 - a. Make sure that the settings of the serial port on your client device exactly match the settings of the Serial Data Port of the SX-590-1402. For example, if your device is set for 9600bps, 8-bit characters, no parity, and RTS/CTS flow control, the SX-590-1402 must also have these exact same settings.
 - b. Make sure that have a good cable connection between your serial device and the Serial Device Server. If possible, try a different cable.
 - c. Make sure that the cable pin outs are correct. In order to communicate properly, the transmit data line on the Serial Device Server must be connected to the receive data line on your serial device, and the receive data line on the Serial Device Server must be connected to the transmit data line on your serial device. Modem signals, if any, must

also be connected so that input signals are connected to output signals and vice-versa. Refer to the cable diagrams in Chapter 2 of this manual.

If none of the above steps solves your problem, then contact your local silex technology office or representative for assistance.

Chapter 7 Product Specifications

Table 12 Product Specification

Component	Specifications
Model	SX-590 module
Dimensions	55 x 30 x 9.25 mm (2.17 x 1.18 x 0.36 inches)
Processor	NXP MCIMX6Y1CVM05AA
RAM Memory	128 Mbytes DDR3
Operating Voltage	5 VDC
Processor Speed	528 MHz at full power
Radio/Baseband	Qualcomm 9377
Ethernet	10/100 Mbps Ethernet MAC+PHY
Interfaces Supported	Serial: 3 x UART (RS-232 w/ external transceivers); one port is dedicated as a console port USB 2.0 (480MHz) OTG x 1 USB 2.0 (480MHz) Host x 1 Serial Peripheral Interface (up to 45MHz)

Table 13 Radio Performance Specifications

Parameter	Specifications
Radio Emission Type	IEEE 802.11 a, b, g, n, ac, e, h, i
Operating Frequency	2.412 GHz - 2.472 GHz (11b, 11g, 11ng) 5.180 GHz - 5.825 GHz (11a, 11na, 11ac)
Data Modulation Type	IEEE802.11b : DSSS(CCK,DQPSK,DBPSK) IEEE802.11g/ng : DSSS-OFDM (64QAM,16QAM,QPSK,BPSK) IEEE802.11a/na : OFDM(64QAM,16QAM,QPSK,BPSK) IEEE802.11ac : OFDM(256QAM,64QAM,16QAM,QPSK,BPSK)
Channel Number	(US) 2.4GHz : 1-11ch 5GHz : (W52) 36, 40, 44, 48ch (W53) 52, 56, 60, 64ch (W56) 100, 104, 108, 112, 116, 132, 136, 140ch (W58) 149, 153, 157, 161, 165ch (JP/DE) 2.4GHz : 1-13ch 5GHz : (W52) 36, 40, 44, 48ch (W53) 52, 56, 60, 64ch (W56) 100, 104, 108, 112, 116, 120, 124, 128, 132, 136, 140ch <i>* Channels 52-64 and 100-140 can be used only when running in Infrastructure(station) mode.</i>
Data Rate	IEEE802.11a 6M / 9M / 12M / 18M / 24M / 36M / 48M / 54M (Auto-sensing) IEEE802.11b 1M / 2M / 5.5M / 11M (Auto-sensing) IEEE802.11g 6M / 9M / 12M / 18M / 24M / 36M / 48M / 54M (Auto-sensing) IEEE802.11n 20MHz : 6.5M / 7.2M / 13M / 14.4M / 19.5M / 21.7M / 26M / 28.9M / 39M / 43.3M / 52M / 57.8M / 58.5M / 65M / 72.2M (Auto-sensing) 40MHz(5GHz only) : 13.5M / 15M / 27M / 30M / 40.5M / 45M / 54M / 60M / 81M / 90M / 108M / 120M / 121.5M / 135M / 150M (Auto-sensing) IEEE802.11ac 20MHz (5GHz only): 6.5M / 7.2M / 13M / 14.4M / 19.5M / 21.7M / 26M / 28.9M / 39M / 43.3M / 52M / 57.8M / 58.5M / 65M / 72.2M / 78M / 86.7M (Auto-sensing) 40MHz(5GHz only): 13.5M / 15M / 27M / 30M / 40.5M / 45M / 54M / 60M / 81M / 90M / 108M / 120M / 121.5M / 135M / 150M / 162M / 180M / 200M (Auto-sensing) 80MHz(5GHz only): 29.3M / 32.5M / 58.5M / 65M / 87.8M / 97.5M / 117M / 130M / 175.5M / 195M / 234M / 260M / 263.3M / 292.5M / 325M / 351M / 390M / 433.3M (Auto-sensing)
Security	WPA-PSK/WPA2-PSK

Channel Number	(US) 2.4GHz : 1-11ch
Media Access Protocol	Carrier Sense Multiple Access with Collision Avoidance (CSMA/CA) with ACK architecture, 32 bits MAC-layer.
Antenna Connector Type	2 U.FL connectors
Operating Voltage	3.3 VDC
Bus Interface	SDIO

Appendix A

Console Commands

1. Introduction and command console access information

The Silex technology SX-590-1402 embedded servers support a sophisticated command-line oriented console for configuration and management. The console includes some features that are not available through other configuration methods. The console can be accessed via TELNET, the Serial Configuration Port, or through the console page on the Configuration web server. The general configuration procedure is the same regardless of which method is used, unless specifically noted.

In the descriptions below, the capitalized portions of commands indicates the minimum portion of the command token that must be entered for the command to be recognized.

The console accepts multiple commands for some functions. The following can be used interchangeably:

SEt, DEFine, CHange	Set a value
DEL, CLear, PURge	Remove a value

2. FIPS 140-2 Mode Configuration Commands

These commands are used to set the basic operating mode of the device, and to perform test and zeroization functions.

2.1 SHow FIPS1402

Show the current configuration status.

```
SH FIPS1402
```

The response shows the current active mode, and the configured mode for the next device restart:

```
FIPS 140-2 Link mode  configured  not active
FIPS 140-2 App mode  not configured  not active
```

```
TLS RSA ciphersuites Disabled
```

2.2 SET Link-Compatible Mode

Set the mode of operation after reset to the FIPS 140-2 approved Link-Compatible mode. This is the factory default setting.

```
SET FIPS1402 LINK ENable
```

Set the mode of operation after reset to the FIPS 140-2 non-approved non-compatible mode

```
SET FIPS1402 LINK DISable
```

2.3 SET App-Compatible Mode

Sets the App-Compatible mode state for operation after the next device reset. To be enabled, Link-Compatible mode must be active, and the application client private key and public certificate must have been configured. .

```
SET FIPS1402 APP [ENable | DISable ]
```

2.4 SET RSA Ciphersuites

Configures the flag indicating whether TLS RSA ciphersuites are allowed. These cannot be used in a FIPS 140-2 approved mode after Dec. 31, 2023. The default setting is disabled.

```
SET FIPS1402 TLSRSA [ENable | DISable ]
```

2.5 Zeroize Non Volatile R/W filesystem

This command overwrites free space on the non-volatile r/w partition with random data. This should be done after a SET DEFAULT operation has reset settings to their factory default, in order to overwrite any old discarded values.

```
SET FIPS1402 ZERONV
```

2.6 Execute test

This command executes a test function. The test executed depends upon the argument given. Available tests are dependent on the specific build. Tests 0 and 1 are always present.

```
SET FIPS1402 TEST <num>
```

<num> = 0 displays a list of the supported tests.

<num> = 1 executes the unit cryptographic self tests

3. Network Commands

This group of commands configures network parameters.

3.1 SET NW WIRED

Sets the wired LAN link mode.

```
SET NW WIRED <mode>
```

<mode>:

AUTO : Auto

FD100BASE : 100Base FULL

100BASE : 100Base Half

FD10BASE : 10Base FULL

10BASE : 10Base Half

3.2 SH NW

Display summary network information.

sample output:

```
Local> SH NW
```

```
WiFi Mode = INFRASTRUCTURE
```

```
WiFi SSID: SQRT
```

```
Current rate = 40.5 Mbps
```

```
Regulatory Domain = JP
```

```
WiFi FW Ver = Host 4.5.20.020 sx 1.0.0, TFW 1.0.0.4_0
```

```
Authentication type= PSK
```

```
Dynamic WPA2 Keys are in use
```

```
AP MAC Address = 3F 80 92 01 31 65
```

```
Signal Quality = Excellent (100%)
```

```
Connected to SSID SQRT on channel 36
```

3.3 SET NW CHannel

Sets a wireless channel to use for Access Point mode.

```
SET NW CHannel n
```

The default channel number is 11.

NOTE: The actual channels available depends on the radio installed in the unit and the current mode of operation.

This value is used in Access Point mode. It is ignored in *Infrastructure* mode. SH NW CHannel displays the currently configured channel number

3.4 SET NW MOde

Sets wireless LAN mode

```
SET NW MOde [Infrastructure | AP]
```

The default mode is *Infrastructure*.

SH NW MODE will display the current wireless mode.

3.5 SET NW RADio

Sets the wireless LAN Radio Mode

```
SET NW RADio [802.11a-n-ac | 802.11b-g-n | 802.11a-b-g-n-ac]
```

The radio can be configured to use all frequencies, or only the 2.4GHz frequencies (802.11b-g-n) or only the 5GHz frequencies (802.11a-n-ac). The default value is 802.11a-b-g-n-ac.

Note. This command is not supported in access point mode. SH NW RADio will display the currently configured radio mode.

3.6 SH NW RATE

Shows the current wireless

link rate. SH NW RATE

```
Current rate = 72 Mbps
```

This is an instantaneous value subject to change.

3.7 SET NW RTS

Sets WLAN RTS threshold

```
SET NW RTS      n
                n = 0-1500 (default = 0)
```

This sets the packet size at which the 802.11 RTS handshake is used for transmission. If the value is set to zero, the 802.11 RTS handshake is disabled.

SH NW RTS will display the currently configured value.

3.8 SH NW SQ

Displays the current signal quality seen on a wireless

network link. sample output:

```
Local> SH NW SQ
```

```
Signal Quality  = 97
Signal Strength = -57
Noise Level     = -96
```

The Signal Quality value is a scaled value from 0 to 100 indicating the relative strength of the wireless link. The Signal Strength values is the current RSSI value computed for the connection.

When communication is lost from the connected AP, it takes approximately 1.5 sec to confirm that AP does not exist any longer. Therefore, the Signal Quality will become '0' in 1.5 sec.

3.9 SET NW SSid

Sets the target wireless LAN SSID

```
SET NW SSid    <name>
<name> is user defined (default = serserv)
```

3.10 SET NW START

Sets a period of time to wait for a wired LAN link before wireless LAN is started in Infrastructure mode.

```
SET NW STARTdelay n
                n = 1-255 (default = 3)
```

SH NW STARTdelay will display the currently configured value.

3.11 SH NW MAC

Shows the MAC address of wired LAN and wireless

LAN. sample output:

```
Local> SH NW MAC
```

```
WLAN MAC address: 84:25:3F:00:00:00
```

```
Ethernet MAC address: 84:25:3F:00:00:01
```

3.12 SH NW WLLIST

Display wireless LAN networks visible to the module. Only access points which are broadcasting their SSID will be displayed. 'Hidden' access points will not be visible.

```
Local> SH NW WLLIST
```

```
"OFFICE-2F"      00:80:92:01:02:03 -40  1  11ng  AP      WPA2-PSK AES
"MeetingRoom1"  00:80:92:04:05:06 -82 13 11ng  AP      WPA-EAP  TKIP
"Suzuki"        00:80:92:07:08:09 -53  6  11ng  Ad-Hoc  OPEN     NONE
"DiningHall"    00:80:92:0A:0B:0C -63 11 11g   AP      WPA2-PSK TKIP/AES
```

4. Wireless Network Security Commands

This group of commands configures wireless network security parameters.

4.1 SET NW AUTHtype

Sets WLAN Authentication type

```
SET NW AUTHtype [OPEN | PSK]
```

The default setting is Open System.
Access Point mode can use only OPEN and PSK.

NOTE: In FIPS 140-2 approved mode (link or App-Compatible mode), only PSK is a valid option.

SH NW AUTHtype will show the currently configured value.

4.2 SET NW ENC

Sets the wireless LAN Encryption Mode.

```
SET NW ENC [DISable | WPA | WPA2 | WPA2-WPA]
```

Supported modes are DISable (none) WPA (TKIP) and WPA2 (AES). WPA2-WPA mode supports either AES or TKIP encryption in WPA systems.

NOTE: Only WPA2 is allowed in FIPS140-2 compliant modes.
The default setting is WPA2.

SH NW ENC will show the currently configured encryption mode.

4.3 SET NW WPAPSK

Sets the WPA PSK pass phrase or hex key.

```
SET NW WPAPSK <key>
```

This value is only used if the authentication mode is WPA-PSK. The argument to this command is either a pass phrase of 8-63 characters, or exactly 64 hex characters representing the 256 bit PSK value.

NOTE: In FIPS 140-2 approved operation (link or App-Compatible mode), the PSK value must be 64 hex characters.

4.4 SET NW ID

Sets Authentication User ID.

```
SET NW ID <user id>
```

The default user ID is “anonymous”.

SH NW ID will show the currently configured value.

4.5 SET NW PKPASS

Sets the password for a private key password file to be loaded into the unit.

```
SET NW PKPASS <passphrase>  
(default = null string)
```

NOTE: This value must be set before the key file is loaded, even if the private key file to be loaded is not encrypted.

4.6 SET NW CACERT

Updates the CA certificate file using XModem protocol. If the command is executed, XMODEM download of the file commences.

```
SET NW CACERT
```

4.7 SET NW CLCERT

Updates the client certificate file using XModem protocol. If the command is executed, XMODEM download of the file commences.

```
SET NW CLCERT
```

4.8 SET NW CLKEY

Updates the secret key file of client certificate using XModem protocol. If the command is executed, XMODEM download of the file commences.

```
SET NW CLKEY
```

5. Wireless to Ethernet Client Bridging Configuration

5.1 SET NW BRACCess

Enables or disables access to the configuration via the wired Ethernet interface in bridge mode.

```
SET NW BRACC [ENable | DISable]
```

The default setting is enabled.

If enabled, the attached client device can access the configuration functions, such as the console, the telnet or web interface, via the Ethernet interface when bridging is enabled. If disabled, this access is not available.

5.2 SET NW BRIDGE

Sets the Bridge Mode.

```
SET NW BRIDGE [MULti | DISable]
```

To use Bridge Mode, set **MULti**.

When the Bridge Mode is not used, set **DISable**. The default value is disabled.

5.3 SH NW BRIDGE

Displays information about the current bridge configuration.

```
Local> SH NW BRIDGE  
Bridge mode is disabled.
```

5.4 SH NW BRFILTER

Shows the current setting for bridge connection filter.

```
Local> SH NW BRFILTER  
Bridge Device Filter Disabled.
```

5.5 SET NW BRFILTER

Enables or disable the bridge connection filter.

```
SET NW BRFILTER [ENable | DISable]
```

5.6 SET NW BRFILTERADDR

Registers the address of devices not to be connected to wireless LAN when the device filter is set to Enable.

```
SET NW BRFILTERADDR <NUM> <MAC address>
```

<NUM>: Specify the index (0-15).

Up to 16 addresses can be registered.

When the device filter is set to Disable:

- All devices will be connected to wireless LAN when they are connected to wired LAN port of Evaluation Daughtercard via HUB.
- IEEE802.11X device authentication cannot be used.

<MAC address> may be in the format aa:bb:cc:dd:ee:ff or aa-bb-cc-dd-ee-ff.

When 00-00-00-00-00-00 is set, the filter is disabled.

5.7 SH NW BRFILTERADDR

Shows the addresses of registered devices.

```
Local> SH NW BRFILTERADDR
```

```
aa-bb-cc-dd-ee-ff  
aa-bb-cc-dd-ee-ff
```

"aa-bb-cc-dd-ee-ff" is the address of registered device.

Up to 16 addresses can be displayed. Only the registered addresses will be displayed. For those not registered, 00-00-00-00-00-00 will be displayed.

6. Port Commands

6.1 Serial Port Commands

In the following commands, S1 is the Serial Data Port. S2 is the Serial Configuration Port, and can only have its baud rate configured.

6.1.1 SH PORT

Shows Port parameters.

sample output:

```
Local> SH PORT
```

Port	Q-Size	Type	Attributes
*S1	0	serial	115200 N 8 1 XON/XOFF RS232
S2	0	serial	Console Mode

6.1.2 SET PORT S1 CH

Sets the size of a character on the serial port.

```
SET PORT S1 CHarsize [7 | 8]  
(default = 8)
```

6.1.3 SET PORT S1 CONSTR

This command sets the console mode string for the unit. If the serial port is in Trap mode, then if the string defined by this command is seen in the serial port input stream, then the serial port will connect to the limited status task. In this mode, data from the Serial Data Port is sent to an the limited status console, and output from the status task is sent to the Serial Data port. . If no string is defined, then this feature is disabled. The maximum length of the string is 31 bytes.

If non printing characters are desired in the string, then the value should be prefixed with “\x” and each byte should be defined with two hex characters. The binary equivalent of the two hex characters will be used when scanning the input for a match.

The value given does not take effect until the unit is reset. The default value of this string is NULL.

```
SET PORT S1 CONSTR
```

This version of the command clears the string definition.

```
SET PORT S1 CONSTR +++
```

This version of the commands sets the console mode string to “+++”.

```
SET PORT S1 CONSTR \x1B1B
```

The version of the command sets the console mode string to be two successive escape characters.

6.1.4 SH PORT S1 CONSTR

Show the current value of the console mode string for the unit.

If non printing characters are contained in the string, the string will be displayed prefixed with “\x” and each byte will be displayed as two hex characters. If nothing is displayed, the console mode string is not currently defined.

```
Local> SET PORT S1 CONSTR  
+++
```

```
Local> SET PORT S1 CONSTR  
\x1B1B
```

6.1.5 SET PORT S1 DTR

Set the DTR mode on serial port 1.

```
SET PORT S1 DTR [CONN | HI | LOW]
```

The SX-590-1402 GPIO2 signal drives the DTR0 signal for the Serial Data port. This command configures how the pin is to be driven.

If set to CONN, the pin will be set high if there is an active network link, and low if the network link is done.

If set to HI, the DTR signal will be set high.

If set to LOW, the DTR signal will be set low.

6.1.6 SET PORT S1 FLOW

Set serial port flow control to NONE, XON/XOFF, or CTS.

```
SET PORT S1 FLOW [ NOne | XOn-xoff | CTS ]  
(default = None)
```

6.1.7 CLEAR PORT S1 JOB

This command aborts the currently active job on the port specified.

```
CL PORT S1 JOB
```

If the remote host is still connected, any further data received will be discarded.

6.1.8 SET PORT S1 LATENCY

Sets the Serial Data port latency value in milliseconds.

```
SET PORT S1 LAT <ms>  
(default = 25ms)
```

If non-zero, when characters are received on the Serial Data port, the driver waits this many milliseconds more to see if additional characters will be received before sending the data to the network.

SH PORT S1 LATency will display the currently configured value.

6.1.9 SET PORT S1 PARITY

Set Serial Data port parity to NONE, EVEN, ODD.

```
SET PORT S1 Parity <parity>
    (Default = None)
```

6.1.10 SET PORT S1 SPeed

Sets the Serial Data port baud rate.

```
SET PORT S1 SPEED <baudrate>
    (default = 115200)
```

Options for <baudrate> are 300, 600, 1200, 2400, 4800, 9600, 19200, 38400, 57600, 115200, 230400, 460800, 921600 and 3000000.

6.1.11 SH PORT S1 STATus

Shows status information about the Serial Data port.

```
Local> SH PORT S1 STAT
```

```
Port S1 status = On-
line Serial Device
```

```
3 bytes transmitted, 0 bytes received
0 framing errors, 0 parity errors, 0 overrun errors, 0 buffer overruns, 0 breaks
```

6.1.12 SET PORT S1 STOP

Sets serialstop bits per character.

```
SET PORT S1 STOP [1 | 2]
    (default = 1)
```

6.2 ECable Port Commands

For products that support the Silex E-Cable application, which provides automatic connection between the port and a remote host, the following commands are available.

6.2.1 SET PORT S1 ECABLE

Enable or disable E-Cable operation.

```
SET PORT S1 ECABLE [ENable | DISable]
    (default = DISabled)
```

6.2.2 SH PORT S1 ECABLE

Show the current E-Cable settings.

```
Local> SH PORT S1 ECABLE

E-Cable mode TCP
E-Cable destination 192.168.5.28:3000
Attempt connection every 5 seconds
E-Cable TCP connection is Down
```

6.2.3 SET PORT S1 ECADDR

Set primary E-Cable destination IP address.

```
SET PORT S1 ECADDR <dest-addr>
    (default = 0.0.0.0)
```

This is the primary network address of the target host for data received on the I/O port. The address may be entered as an IP address, or, if DNS is enabled on TCP mode, as a symbolic host address.

If set to zero, no data will be sent.

6.2.4 SET PORT S1 ECCONN

This parameter applies only in TCP mode. If the TCP connection is broken, or cannot be established, this parameter defines the time to wait before attempting to re-establish the connection. The time units depend on the ECTMMSEC parameter below. The valid range is 1-255.

```
SET PORT S1 ECCONN n
      (default = 30)
```

6.2.5 SET PORT S1 ECENCRYPT

This parameter applies only in TCP mode. If enabled, data transfer on the TCP connection will be encrypted using a TLS channel. If disabled, the data is transferred in plain text. The unit client application private key and public certificate must be configured to enable this option.

NOTE: In App-Compatible mode, this parameter is forced to be enabled, and the TCP connection must be encrypted.

```
SET PORT S1 ECLPORT n
      (default = n)
```

6.2.6 SET PORT S1 ECLPORT

This parameter applies only in UDP mode. This is the port number of the local UDP port on the server to which remote hosts can send data intended for the I/O port. Only data from hosts whose IP address is configured as the primary or one of the optional secondary addresses will be accepted and passed to the I/O port - unless the primary and all secondary addresses are zero, in which case data from any host will be accepted. A port number of zero will disable reception.

```
SET PORT S1 ECLPORT n
      (default = n)
```

6.2.7 SET PORT S1 ECNHOST

This parameter applies only in UDP mode. This value sets the maximum number of remote hosts to which data can be sent, and from which data will be accepted. If the value is changed, all currently configured secondary host information will be erased. The valid range is 1-255.

```
SET PORT S1 ECNHOST n
      (default = 1)
```

6.2.8 SET PORT S1 ECPORT

Set primary E-Cable port address. Along with the primary IP address, this defines the remote destination for data received on the I/O port. If zero, no data will be sent.

```
SET PORT S1 ECPORT n
    (default = 0)
```

6.2.9 SET PORT S1 ECRADDR

This parameter applies only in UDP mode. This sets the primary or a secondary E-Cable destination IP address. This is the network address of the target host for data received on the I/O port. If zero, no data will be sent. If the index value is zero, the primary address is set (same as the ECADDR parameter). If not zero, the valid range is 1:(n-1), where n is the ECHNOST value configured. If n is one only the primary address can be set.

```
SET PORT S1 ECRADDR index a.b.c.d
    (default = 0.0.0.0)
```

6.2.10 SET PORT S1 ECRPORT

This parameter applies only in UDP mode. This sets the primary or a secondary E-Cable destination port number. Along with the corresponding network address this defines the destination for data received on the I/O port. If zero, no data will be sent. If the index value is zero, the primary port is set (same as the ECPORT parameter). If not zero, the valid range is 1:(n-1), where n is the ECHNOST value configured. If n is one only the primary port can be set.

```
SET PORT S1 ECRPORT index n
    (default = 0)
```

6.2.11 SET PORT S1 ECTMMSEC

This parameter applies only in TCP mode. This determines the units for the connection timer set with the ECCONN parameter. If enabled, the timer is in units of 10 milliseconds (20-2550 msec). If disabled, the timer is in units of seconds (1-255 seconds).

```
SET PORT S1 ECTMMSEC [ENable | DISable]
    (default = DISable)
```

6.2.12 SET PORT S1 ECUDP

Enable or disable E-Cable UDP operation. If disabled, TCP is used for network I/O. If enabled UDP is used.

NOTE: In App-Compatible mode, this parameter is forced disabled, and encrypted TCP communication must be used.

```
SET PORT S1 ECUDP [ENable | DISable]  
    (default = DISabled)
```

7. Server Information Commands

7.1 SH SERIAL

Displays the serial number of the

unit. sample output:

```
Serial number is 9047595
```

7.2 SH SERVER

Shows Server parameters.

```
Local> SH SERVer
```

```
Silex SX-590 Serial # 74033
```

```
Address: 84-25-3F-01-21-31 Name: SDS012131 Number: 0
```

```
Identification: Network Serial Server
```

```
Enabled Characteristics:
```

```
Ethernet link Up
```

7.3 SH SERVER CO

Shows Server network statistics.

sample output:

```
Local > SH SERVER CO

Seconds Since Zeroed:      434          Frames Sent, 1 Collision:    N/A
Bytes Received:           72950         Frames Sent, 2+ Collision:  N/A
Bytes Sent:               18726         Send Failures:              0
Frames Received:          752          Send Failure Reasons:      N/A
Frames Sent:              181          Receive Failures:          503
Multicast Bytes Rcv'd:    N/A          Receive Failure Reasons:   N/A
Multicast Bytes Sent:     N/A          Unrecognized Destination:  N/A
Multicast Frames Rcv'd:   N/A          Data Overrun:              N/A
Multicast Frames Sent:    N/A          User Buffer Unavailable:    N/A
Frames Sent, Deferred:    N/A          System Buffer Unavailable:  N/A
```

7.4 SET SERVER Description

Sets the server description string.

```
SET SERVER Description <description-string>
```

7.5 SH SERVER FWVER

Shows the firmware version string.

```
Local> SH SERVER
```

```
FWVER BB3-1.00 (2017.08.08)
```

This command shows just the firmware version string, without the additional information shown by SH VERSION.

7.6 SH SERVER MODEL

Shows Server model

```
name. Local> SH SERVER
```

```
MODEL SX-590-1402
```

This shows the server model name, without the other information displayed by SH SERVER.

7.7 SET SERVER NAME

Sets server node name.

```
Local> SET SERVERNAME <name>  
(default = "SDS_XXXXXX", where XXXXXX are the last 6 hex digits of the  
MAC address)
```

7.8 SHoW SERVER QUEue

Displays the I/O job queue for the Serial Data port.

```
Local> SH SERVER QUE
```

```
Port S1 status = On-line  
#   Type      Source
```

```
The queue is empty
```

7.9 SH SERVER STATistics

Shows information about print jobs received.

```
Local> SH SERVER STA

LPD Statistics:
Currently 0 jobs are waiting for the peripheral
0 connections have been made
0 data files have been printed
0 data bytes have been printed
0 control files have been received
0 print job commands have been received
```

7.10 SH SNMP

Shows the state of the SNMP protocol enable. This protocol is not supported on the SX-590-1402, so this is always disabled.

sample output:

```
Local> SH SNMP

SNMP is Disabled
```

7.11 SET SNMP CONTACT

Set system contact string. This is unused on the SX-590-1402.

```
SET SNMP CONTACT <string>
      (default = null string)
```

7.12 SET SNMP GETCOMM

Get Community Name. This is unused on the SX-590-1402.

```
SET SNMP GETCOMM <string>
      (default = "public")
```

7.13 SET SNMP LOCation

Set the system location string. This is unused on the SX-590-1402

```
SET SNMP LOCation <string>
    (default = null string)
```

7.14 SET SNMP SETCOMM2

Set Community Name. This is unused on the SX-590-1402

```
SET SNMP SETCOMM2 <string>
    (default = "public")
```

7.15 SH VErSion

Shows the units firmware version.

```
Local> SH VER
```

```
Silex SX-590
Firmware Ver. BB3-1.00 (2017.08.08)
Boot Ver. 1.2
64Mbit Flash
```

```
Protocols supported:
```

```
TCP/IP
DHCP
```

8. Service Commands

Logical I/O services are associated with the Serial Data port. I/O is routed through the service, which may perform modifications on the data stream based on its settings.

8.1 SH SERVI

Show service configuration.

```
Local> SH SERVI
```

#	Service	Port	FIL	BOT	EOT	DEL	OPT	PROT
* 1	SDS1E86B0_S1_A	S1	0	1	1	0	B	IP
2	SDS1E86B0_S1_B	S1	0	1	1	0	B	IP

The '*' indicates the default service for the Serial Data port.

8.2 SET SERVI <service name> BOT

Set beginning of transmission (BOT) string index for service.

```
SET SERVI <service name> BOT nn
```

The string indicated will be sent to the Serial Data port at the beginning of a connection to the service indicated. The default is the null string.

8.3 SET SERVI <service name> EOT

Set end of transmission (EOT) string index for service.

```
SET SERVI <service name> EOT nn
```

The string indicated will be sent to the Serial Data port at the end of a connection to the service indicated. The default is the null string.

8.4 SH SERVI STRings [string_num]

Defines the BOT and EOT strings used in services. If string_num is provided then the specific string definition and expansion is displayed. If string_num is not provided, then all string definitions (but not their expansions) are displayed.

sample output:

```
Local> SH SERVI STR 10  
10: \FF\04\FF\05\FF\06\FF\08
```

8.5 SET SERVI <service name> Filter

Set filter index for service.

```
SET SERVI <service name> Filter nn
```

SH FILTER shows the available filters on the unit.

8.6 SH SERVI FILTERS

Shows filter settings.

```
Local> SH SERVI FIL  
  
# Service Name Filter  
1 SDS1E86B0_S1_A 0: No Filter  
2 SDS1E86B0_S1_B 0: No Filter
```

8.7 SET SERVI <service name> FMS

Set filter 1 (text replacement filter) match string index. If the index is zero, the default string of <LF> (line feed) is used.

```
SET SERVI <service name> FMS nn  
(default = 0)
```

8.8 SET SERVI <service name> FRS

Set filter 1 (text replacement filter) replace string index. If the index is zero, the default string of <CRLF> (carriage return-line feed) is used.

```
SET SERVI <service name> FRS nn
    (default = 0)
```

8.9 SET SERVI <service name> IP

Enable or disable all IP based jobs (lpd, raw tcp, etc.) on the service.

```
SET SERVI <service name> IP [ENable | DISable]
    (default = enabled for service 1 and 2, disabled for all others)
```

8.10 SET SERVI <service name> NAmE

Change the service name.

```
SET SERVI <service name> NAmE <newname>
```

8.11 SET SERVI <service name> PORT

Set the output port associated with a service. Since there is only one serial data port on the SX-590-1402, this command does nothing.

```
SET SERVI <service name> PORT <portname>
    (default = "S1")
```

8.12 SET SERVI <service name> PRIority

Set priority for service if multiple service try to transmit data at the same time. Higher priority services are serviced first.

```
SET SERVI <service name> PRIority nn
    (default = 10)
```

8.13 SH SERVI PRI [service_num]

This shows the priority of a specific service. If service_num is not provided, the priority of all services is listed.

8.14 SET SERVI <service name> QUEue

If enabled, and if a raw TCP port is defined, the server will queue jobs sent to that port. If disabled, jobs will be rejected if the server is currently busy with another job.

```
SET SERVI <service name> QUEUE [ENable | DISable]
      (default = disabled)
```

8.15 SET SERVI <service name> RECeive

Set receive only mode for a service. This option is rarely required, but some host applications do not operate properly if data is received back from the serial client device.

```
SET SERVI <service name> RECeive [ENable | DISable]
      (default = disabled)
```

8.16 SET SERVI <service name> TCP

Set the raw TCP port for the service. If port number is zero, raw TCP is disabled on that service.

```
SET SERVI <service name> TCP nn
      (default = 9100 for service 1, 3001 for service 2)
```

8.17 SH SERVI SUMmary [service_num]

Shows the basic parameters for a specific service. If service_num is not provided, parameters for all services are displayed.

Note: The command SH SERVI is equivalent to SHOW SERVI SUM

9. String Commands

These commands configure strings used with services and service filters.

9.1 SET STRing

Set service string table entry.

```
SET STRing <string_num> "value"
```

Hex values can be entered as two hex digits in the string with the prefix '\'. One string can reference another string with two binary characters. The first is \FF, and the second is the string index of the referenced string.

Note: Strings 1-11 cannot be set or changed.

9.2 CL STRing

Clears the service string table entry.

```
CL STRing <string_num>
```

9.3 SH STRing [string_num]

Defines the BOT and EOT strings used in services. If string_num is provided then the specific string definition and expansion is displayed. If string_num is not provided, then all string definitions (but not their expansions) are displayed.

sample output:

```
Local> SH STR
```

```
1:
2: \1BE
3: \04
4: \1B%-12345X
5: @PJL
6: ENTER LANGUAGE=
7: PCL\0A
8: POSTSCRIPT\0A
9: \FF\04\FF\05\FF\06\FF\07
10: \FF\04\FF\05\FF\06\FF\08
11: \0C
```

9.4 SH FILTERS

Shows the available filters which can be used to modify a job

stream. sample output:

```
Local> SH FIL
#      Filter
0      No Filter
1      Text Substitution
3      Text to PostScript
4      PostScript Tagged Binary
```

10. TCP/IP Commands

10.1 SH IP

Display TCP/IP settings.

```
Local> SH IP
```

```
IP is enabled
Boot method    DHCP
IP address     192.168.5.40      (192.168.5.235)
Subnet Mask    255.255.255.0    (255.255.255.0)
IP gateway     192.168.5.1      (0.0.0.0)
Boot tries     3
Timeout        1 min
Keepalive      1 min

Service                Port  TCP port
SDS1E86B0_S1_A         S1    9100
SDS1E86B0_S1_B         S1    3001
```

10.2 SET IP ACcess

Allow or disallow access to a block of remote addresses.

```
SET IP ACcess [ENable | DISable | ALL] aa.bb.cc.dd ee.ff.gg.hh
```

This command modifies the IP access list. If ALL is selected, the access list is cleared and all hosts are allowed access.

If ENable is selected, then an entry for the range given by the two IP addresses is added to the list. Only hosts with an IP address within the range of one of the entries in the access list are allowed to connect to the unit.

If DISable is selected, if the two addresses match the range values of an entry in the access list, that entry is removed and hosts in that range will no longer be allowed access to the unit, unless another entry allows it.

SH IP ACcess or SH IP RANge will display the current access list settings.

10.3 SET IP Method

Set method of getting IP address.

```
SET IP Method    [AUTO | DHCP | STATIC]
                (default = AUTO)
```

DHCP will wait to acquire an address via DHCP.

STATIC will bring the IP stack up immediately with the configured IP static address.

AUTO will attempt to get an address via DHCP, but if it fails it will use the configured static IP address.

10.4 SET IP Address

Set server IP address.

```
SET IP Address aa.bb.cc.dd
```

If the IP address acquisition method is static, this command sets the IP address to be used.

This is also the fall back address for Auto mode, if a DHCP address is not received.

The default address is 169.254.111.111.

10.5 SET IP Subnet

Set the IP subnet mask.

```
SET IP Subnet    aa.bb.cc.dd
                (default = 0.0.0.0)
```

10.6 SET IP Router

Set the default router address.

```
SET IP Router    aa.bb.cc.dd
                (default = 0.0.0.0)
```

SET IP Gateway is an optional command which performs the same function.

10.7 SET IP B0ot

Number of times to try DHCP to acquire an address.

```
SET IP B0ot n
      (default = 3)
```

In Auto mode, the DHCP client will attempt the number of times specified to acquire an IP address. If it does not succeed after that number of times, the module will initialize with the fallback static IP address (SET IP ADDRESS) configured.

10.8 SET IP KEepalive

Set interval at which gratuitous ARP packets are sent in minutes.

```
SET IP KEepalive n
      (default = 5 min)
```

10.9 SET IP HTTP

Enable or disable the HTTP protocol.

NOTE: In App-Compatible mode, HTTP is forced to be disabled. Only HTTPS is allowed.

```
SET IP HTTP [ENable | DISable]
      (default = enable)
```

10.10 SET IP TFTP

Enable or disable the TFTP protocol.

NOTE: TFTP is not supported on the SX-590-1402, so this command is ignored.

```
SET IP TFTP [ENable | DISable]
      (default = disable)
```

10.11 SET IP NTP

Enable or disable the NTP protocol.

```
SET IP NTP      [ENable | DISable]
                (default = enable)
```

10.12 SET IP TCP

Enable or disable the raw TCP (9100) protocol.

```
SET IP TCP      [ENable | DISable]
                (default = enable)
```

10.13 SET IP LPD

Enable or disable the LPD protocol.

NOTE: In App-Compatible mode, LPD is always disabled regardless of this setting.

```
SET IP LPD      [ENable | DISable]
                (default = enable)
```

10.14 SET IP TELnet

Enable or disable the TELNET protocol.

NOTE: In App-Compatible mode, TELNET is always disabled regardless of this setting.

```
SET IP TELnet  [ENable | DISable]
                (default = enable)
```

10.15 SET IP SX_FLDP

Enable or disable the Silex proprietary production test protocol.

NOTE: This protocol can only be enabled in non-compatible mode. In Link-Compatible or App-Compatible mode, the protocol will be disabled, regardless of this setting.

```
SET IP SX_FLDP    [ENable | DISable]
                 (default = ENable)
```

10.16 SET IP PROBe

Enable or disable TCP connection probes (TCP Keepalive packets).

```
SET IP PROBe    [ENable | DISable]
                (default = disable)
```

10.17 SET IP TImeout

Set TCP Inactivity timeout.

```
SET IP TImeout  n
    (default = 1 minute)
```

This command sets inactivity timeout for IP to I/O port transfers via raw TCP, RFC2217, or LPD. If no data is received within the time specified, the connection will be closed and the port released to accept new connections.

If fast timeout (SET IP FTIme) is enabled, the value given is in seconds, otherwise it is defined in minutes.

10.18 SET IP FTIme

If enabled, the IP timeout is measured in seconds. If disable, the IP timeout is in minutes.

```
SET IP FTIme  [ENable | DISable]
    (default = disable)
```

10.19 SET IP REtry

Enable or disable LPD retry on incomplete job.

```
SET IP REtry  [ENable | DISable]
    (default = disable)
```

10.20 SET IP STATus

Sets user defined IP status string.

```
SET IP STATus <status-string>
```

This command defines an arbitrary string. If defined, the string will be appended to LPD status request responses.

SH IP STATus will display the current status string.

10.21 SET IP WInDow

Set TCP maximum window size in bytes.

```
SET IP WInDow    nn
                (default = 10240)
```

SH IP WInDow will display the currently configured value.

10.22 SET IP BAnner

Enable or disable printing of job banner on LPD jobs.

```
SET IP BAnner [ENable | DISable]
                (default = disable)
```

11. DNS Commands

These settings configure the DNS server settings, if not acquired via DHCP.

11.1 SH DNS

Display current DNS configuration settings.

```
Local> SH DNS
```

```
DNS is Enabled
```

```
Domain name:
```

```
Primary DNS server: 0.0.0.0
```

```
Secondary DNS server: 0.0.0.0
```

11.2 SET DNS DOMain

Set the desired DNS domain string.

```
SET DNS DOMain <domain-name>
```

11.3 SET DNS PRImary

Set the IP address for the primary DNS server to reference.

```
SET DNS PRImary aa.bb.cc.dd
```

11.4 SET DNS SECondary

Set the IP address for the secondary DNS server to reference.

```
SET DNS SECondary aa.bb.cc.dd
```

12. DHCP Server Commands

These settings are used to configure the SX-590-1402 DHCP server, if used when the server Wireless port is set for AP operation.

12.1 SET DHCPS

Enables or Disables the DHCP server function.

```
SET DHCPS [ENable | DISable]
```

The default value is disabled.

12.2 SH DHCPS

Displays information about the current DHCP server configuration.

```
Local> SH DHCPS
```

```
DHCP Server is Disabled
```

12.3 SET DHCPS Address

Set the range of IP address for lease.

```
SET DHCPS Address aa.bb.cc.dd ee.ff.gg.hh
```

12.4 SET DHCPS SUBnet

Set the IP subnet mask for lease.

```
SET DHCPS SUBnet aa.bb.cc.dd
```

12.5 SET DHCPS ROuter

Set the default router address for lease.

```
SET DHCPS ROuter aa.bb.cc.dd
```

12.6 SET DHCPS LEase

Set the lease time of IP address.

```
SET DHCPS LEase    dd hh:mm
```

13. NTP Command

13.1 SET NTP SERVER

Sets the information of NTP server to retrieve time information from.

```
SET NTP SERVER <server>  
(default = pool.ntp.org)
```

Up to 48 characters can be used to specify the NTP server. When <server> is not specified, the default value is applied.
SH NTP SERVER command will display the current setting.

13.2 SH NTP DATE

Shows the current system time in GMT+00.

```
SH NTP DATE
```

14. GPIO Control

The SX-590 has 11 GPIO signals available, numbered 0-10. GPIO0-GPIO8 have defined functions on the SX-590-1402, and that function cannot be changed. GPIO9 and GPIO10 can be configured with the commands herein. Refer to the product functional specification for details of the defined GPIO definitions.

14.1 SET GPIO DIR

Set a single GPIO direction control.

```
SET GPIO DIR [IN | OUT] <gpio-number>
```

This command sets an individual GPIO pin to be an input or an output pin. This setting is ignored for pins set for special function mode, the special function determines the pin direction.

NOTE: the direction bit configuration is not changed by a configuration reset to default.

14.2 SH GPIO DIR

Display GPIO direction configuration.

```
Local> SH GPIO DIR
```

```
GPIO Direction
-----
0 [SPCL]
1 [SPCL]
2 [SPCL]
3 [SPCL]
4 [SPCL]
5 [SPCL]
6 [SPCL]
7 [SPCL]
8 [SPCL]
9 [OUT]
10 [OUT]
```

14.3 SET GPIO DIRM

Sets all direction control bits.

```
SET GPIO DIRM <bit-mask>
```

<bit-mask> is an 11 bit mask expressed as 3 hex digits. This value should be in the range 000-7FF. The mask is encoded as follows:

10	9	8	7	6	5	4	3	2	1	0
GPIO10	GPIO9	GPIO8	GPIO7	GPIO6	GPIO5	GPIO4	GPIO3	GPIO2	GPIO1	GPIO0

A value of 1 sets the corresponding GPIO line to be an output. A value of 0 sets the GPIO line to be an input. For example, a hex value of 80 sets GPIO7 as an output, all other GPIO signals are inputs. The direction is not affected for any bits configured for a special function.

NOTE: the direction bit configuration is not changed by a configuration reset to default.

14.4 SH GPIO DIRM

Shows all direction control bits.

```
Local> SH GPIO DIRM
```

```
GPIO direction mask=7fc
```

14.5 SH GPIO SPECial

Shows the current setting of the GPIO special function configuration.

```
Local> SH GPIO SPECial
```

```
GPIO Special Functions
```

```
GPIO #0 is special
GPIO #1 is special
GPIO #2 is special
GPIO #3 is special
GPIO #4 is special
GPIO #5 is special
GPIO #6 is special
GPIO #7 is special
GPIO #8 is special
GPIO #9 is normal
GPIO #10 is normal
```

14.6 SHow GPIO SPECM

Shows GPIO special functions control bits as a mask value.

```
Local> SH GPIO SPECM
```

```
GPIO special function mask = 1FF
```

14.7 SET GPIO DATA

Sets all data out control bits.

```
SET GPIO DATA <bit-mask>
```

<bit-mask> is an 11 bit mask expressed as 3 hex digits. This value should be in the range 000-7FF. The mask is encoded as follows:

10	9	8	7	6	5	4	3	2	1	0
GPIO10	GPIO9	GPIO8	GPIO7	GPIO6	GPIO5	GPIO4	GPIO3	GPIO2	GPIO1	GPIO0

Each GPIO output bit is set to the corresponding value in the mask. If a GPIO signal is set as an input, the value is set but has no effect. If a GPIO signal is set for a special function, the bit value given is ignored. For example, a hex value of 80 sets the GPIO7 to a 1 (high), all other GPIO signals to 0 (low), except those set as special functions.

NOTE: the default output bit value on power up or reset is 0 for all GPIO signals.

14.8 SHOW GPIO DATA

Shows the current state of the GPIO signals.

```
Local> SH GPIO DATA
```

```
GPIO Data In
- - - - -
GPIO #0 [1]
GPIO #1 [0]
```

```
GPIO Data Out
- - - - -
GPIO #2 [0]
GPIO #3 [0]

GPIO #4 [0]
GPIO #5 [0]

GPIO #6 [0]
GPIO #7 [0]

GPIO #8 [0]
GPIO #9 [0]
```

GPIO #10 [0]

15. Firmware Update

These commands set up the unit for performing an update of the server firmware.

15.1 SET LOAd XModem

Initiate firmware update via the serial console using the XModem protocol. The server will reset after the firmware update is completed.

```
SET LOAd XModem
```

16. Power Management

16.1 SET NW WLIF

Sets the radio network interface enable.

```
SET NW WLIF [UP | DOWN]
```

UP puts the radio state in a normal operating mode. DOWN disables the radio so it produces no RF output and does not receive any data.

Note: This function is volatile, and the radio is enabled if the module is reset.

16.2 SET POWER LEVEL

Sets the server power profile.

```
SET POWER LEVEL nn
```

nn = 0 for High power and 1 for Low power.

In High power mode, the radio runs in maximum performance mode. In Low power mode, the radio runs in power save mode.

The SHow POWER command will display the currently configured power level.

17. Other Commands

17.1 SET ADMIN

Sets the server Cryptographic Officer user ID and password.

```
SET ADMIN <user id> <password>
      (default = "admin" "access")
```

17.2 SET DEFAULT

Set parameters to factory defaults.

NOTE: They Cryptographic Officer ID and password are not reset by this command.

```
SET DEFAULT
```

17.3 EXIT

This command exits the current configuration console session.

```
EXIT
```

17.4 HElp <command>

This is for getting help on the console commands. You can just type help, or type help and then a command to display instructions on specific commands.

Sample output:

```
Local> HE
```

```
EXIT/^D          Exit program
HElp            Information on available commands
INitialize      Reset          unit
CLear/PURge/DElete  Remove configuration item
```

SAVE	Save configuration to NV memory
SET/DEFine/CHange	Modify unit parameters
SHow	Display unit parameters
Zero	Zero statistical counts

Type 'HElp <cmd>' for more information

17.5 INIT

This command instructs the server to do a reset when the next "EXIT" command is executed.

INIT

17.6 SET PAssword

Sets the server Cryptographic Officer password. This does not change the user ID.

```
SET PAssword <password>
      (default = "access")
```

17.7 SAVE

This command saves the current configuration to non-volatile memory. Without this command, the configuration is not saved unless an "EXIT" command is performed.

SAVE

18. Compatibility with Other Models

Following commands are installed to assure compatibility with other silex technology models, however, even if the commands are executed, they do not affect the SX-590-1402 module.

18.1 SET NW DISCONN

This sets the time to retry within a wireless module when connection is disconnected from Access Point. As the wireless module of the SX-590 does not have a function to retry connection within the module, this setting does not work.

18.2 SET RM SCAN LOW

This setting works when custom loaming is enabled. As the SX-590 does not have loaming scan threshold of custom loaming, this setting does not work.

18.3 SET RM THRESH LOW

This setting works when custom loaming is enabled. As the SX-590 does not have loaming scan threshold of custom loaming, only loaming threshold works.

Appendix B

Firmware Update Procedures

Occasionally it may be necessary to update the SX-590-1402 to take advantage of new features or to fix specific problems. The only way to perform this update is with the Configuration GUI web page of the SX-590-1402. You can open the web page using a common web browser.

Firmware update is only allowed in one of the FIPS 140-2 approved modes (Link-Compatible or App-Compatible mode).

To update the firmware using the Configuration GUI web page:

1. Obtain the firmware update file from silex technology or your local silex technology representative. The file must be digitally signed by silex, and must be one of the approved versions listed in the current Security Policy document. Place the update file into a directory on your computer.
2. Access the Configuration GUI Web page of the SX-590-1402 via the browser of your choice. See Chapter 3 for how to do this.
3. In the Web page, click **Firmware Update** on the left menu. In the **Firmware Update** page, click **Browse** to specify the firmware update file that you have downloaded into your computer.
4. Check the correct file name is displayed in **New firmware** field and click **Update**.
5. Wait for the programming to complete and the unit to reset. Verify the Configuration GUI web page shows the expected firmware version.

Appendix C

GNU/Linux Open Source and Programming

The software embedded in this SX-590-1402 module includes the Linux operating system. Linux and certain other software programs used in the SX-590-1402 are licensed under GNU GPL compatible Free Software Licenses. In compliance with these licenses, you can obtain the relevant source code at no charge by contacting silex technology.

Appendix D

Silex Contact Information

Silex Technology America, Inc.

www.silexamerica.com

Technical Support: support@silexamerica.com

Sales: sales@silexamerica.com

Tel: (657-218-5199 9:00 to 5:00 Pacific Time

Tel: (866) 765-8761 toll-free

Fax: (801) 748-0730

Silex Technology Europe GmbH

www.silexeurope.com

Tel: +49(0)2154-88967-0

Email: contact@silexeurope.com

Silex Technology China, Inc.

www.silex.com.cn

Tel: +86 10 6440 3958

Email: contact@silex.com.cn

Corporate Headquarters

Silex Technology, Inc.

www.silex.jp

Tel: +81-774-98-3781

Email: support@silex.jp



Silex Technology America, Inc.

www.silexamerica.com