IT Resource Guide

for

Codonics®
Safe Label System®

(Software Release v2.3.0)

Codonics® Safe Label System®
SLS 500i® Point of Care Station (PCS)

Legal Notice

This document and the designs, specifications and engineering information disclosed hereon are the property of Codonics, Inc., and are not to be disseminated or reproduced without express written consent from Codonics, Inc.

TABLE OF CONTENTS

1. Overview

This document contains network and security information to assist users with the deployment of the Codonics® Safe Label System® AT (Administration Tool) and SLS 500i® Point of Care Station (PCS) with software release v2.3.0.

2. System Description

Summary: Codonics Safe Label System SLS 500i Point of Care Station (PCS) is an award-winning, FDA-approved Class II medical device that improves the safety and accuracy of medication management and labeling compliance anywhere medications are prepared. The SLS utilizes barcode technology to read information from a drug container and electronically identifies it against the pharmacy's hospital-approved drug database to reduce medication errors.

The Codonics Safe Label System (SLS) reads a drug identification barcode on an originating drug vial or ampoule and prints a color label for applying to a syringe or other secondary drug dispensing container.

The Codonics Safe Label System (SLS) and SLS Software provides a simple computer-based bar code scanning and printing system to provide on-demand, preparation specific vial and ampoule identification to automatically verify drug identity from NDC and other drug vial UDI Barcodes. At the Point of Care, SLS 500i (PCS) is part of approved medication preparation and secondary container (syringe, IV bags, etc) labeling for safe identification of prepared medications and other items in use in connection with patient care and during surgical procedures. Drug information from an original drug container can be easily verified against the hospital-approved drug database that includes preparation conditions and best practice guidelines stored locally in the device. The drug database, also called a "formulary", includes additional information about the color, graphic patterns and specific text information to be printed on the label for the scanned and prepared medication.

Codonics Safe Label System (SLS) is generally placed in, however not limited to, the peri-operative environment to identify syringes prepared for anesthesiology use during surgery. Additional uses include producing labels for IVs and other artifacts used during a surgical procedure. SLS can also be used to print "non-surgical environment" color and text labels as required. As a prescription Class 2 device, typical users of this system are trained professionals, including but not limited to physicians, nurses and technicians. The main purpose of the SLS is to improve the safety, accuracy, consistency and compliancy of medications in the course of preparation and labeling.

3. System Components

The Codonics Safe Label System has three major components:

1. SLS 500i PCS device (SLS)

2. Management software which includes the SLS Administration Tool (AT)

3. Monitoring software which includes the SLS Email Notifier (EN)

The following information describes these components.

3.1 SLS 500i PCS

The SLS 500i PCS is a standalone drug labeling device that uses embedded hardware and software manufactured and supported by Codonics. The SLS device contains a color inkjet label printer, embedded computer, embedded flash memory storage, LCD display, touch-screen interface, speaker for announcing drug information, Ethernet and optional Wi-Fi interface, and a USB port for updates or retrieving log files.

The SLS is an embedded device that requires no customer supplied software or hardware. They are typically installed in or near drug preparation areas such as operating rooms, PACU's, ICU's or pharmacies.

The SLS can be connected to a LAN network via Ethernet or Wi-Fi. Connecting SLS units to a network will simplify device monitoring and installation of updates from the Administration Tool (see section "System Networking" for more information on SLS network capabilities.)

The SLS can also be operated via air-gap (aka. "sneaker-net") without a network connection. When used in an air-gap configuration, formulary and configuration updates from the AT must be transferred manually to each SLS device using a site-supplied, unencrypted FAT or FAT32 formatted USB drive.

Security patches and software updates are tested, approved and released by Codonics. Codonics has a policy to monitor security related vulnerabilities in the SLS and release updates as required. Updates and patches are distributed in a proprietary, digitally-signed file format called "packages" to ensure the integrity of the software. Information about updates to SLS will be posted on the Codonics website.

The SLS uses an embedded SQL database for storage of drug information, configuration information and log files. Only the embedded software on the SLS has access rights to the database.

3.1.1   SLS 500i PCS Hardware

Hardware Minimum Requirements				
Component Name	**Processor**	**RAM**	**HDD**	**RAID**
SLS 500i PCS Serial Numbers Starting with: 142C	Intel Atom (embedded)	2 GB (embedded)	32 GB Solid State Drive Minimum (embedded)	N/A

Hardware Minimum Requirements				
Component Name	**Processor**	**RAM**	**HDD**	**RAID**
SLS 500i PCS Serial Numbers Starting with: 140C, 141C	Intel Atom (embedded)	1 GB (embedded)	4 GB Compact Flash (embedded)	N/A

3.1.2   SLS 500i PCS Software

Software		
Application Name	**Version #**	**Description**
SLS Embedded Application	2.3.0	Codonics Software version for the SLS 500i PCS device.
SLS Operating System	Linux Kernel 4.4.0-24	Linux has been optimized and hardened for the SLS device.
Java	OpenJDK JRE 7u101-2.6.6-0ubuntu0.14.04.1	Java is used to run some internal processes of the embedded application.
SQLite	3.6.14.2	An embedded open source SQL database is included in the SLS application for storage of drug data and log files.

3.1.3   SLS 500i PCS Virtualization

SLS 500i PCS software is embedded and cannot be virtualized.

3.2   SLS Software Security

The SLS 500i uses a Linux based operating system with custom developed software that is enhanced to reduce security vulnerabilities using the following techniques:

1. Disable unnecessary Linux user accounts including the "root" login and optionally the service shell login functions of the device.

2. Remove unnecessary Linux software.

3. Block incoming network connection requests on unused ports (refer to Appendix B).

4. Encrypt all network access credentials stored on the device (e.g. certificates, user names, passwords, keys).

5. Encrypt all incoming network communications using 128-bit SSL based on the SSH-2 protocol (RFC 4251).

6. Cryptographically sign important internal data to detect unintended modification.

7. Install only software and data updates with proper digital signatures on the device.

8. Disable standard boot functions to prevent unauthorized software installation.

9. Permit operation with or without a network (e.g. air gap, sneaker-net).

P/N: 900-653-007.01

3.3   AT (Administration Tool)

The AT is a Windows® based Java® application used to create and maintain the drug formulary and configuration files required by SLS devices. The AT can be installed in two configurations: AT Stand-alone and AT Server. The specific configuration is selectable at installation time. The AT application is the same for both configurations (Stand-alone and Server) but uses a different set of startup parameters. When the AT is run as a service (AT Server configuration), an executable wrapper is used to launch the application.

In addition to managing the formulary and configuration files for the SLS, the AT allows remote monitoring and updating of SLS 500i PCS devices when they are connected to a network.

> **The AT application only requires the customer to supply a Microsoft Windows based computer as described later is this section. All other software modules required for the operation of the AT are included and automatically installed when the AT is installed. No additional 3rd party software packages such as databases need to be supplied by the customer.**

3.3.1   AT Stand-alone

The initial release of the Safe Label System included only one configuration of the AT. That configuration is now called "AT Stand-alone." The AT Stand-alone application is available for every SLS software release since version 1.2.0. It is designed to run on a Windows based computer and appear to the user as a single application. AT Stand-alone utilizes a web browser on the host system (Internet Explorer 11 recommended) to provide the user interface for the application.

3.3.2   AT Server

A second configuration of the AT, called "AT Server", is included with SLS software release version 1.9.0 and later. AT Server provides the same functionality as AT Stand-alone, but uses a client/server model that allows installation on one computer that provides access to users from other computers on the network using a web browser (Internet Explorer 11 recommended).

Notes: 1. Both the AT Stand-alone and AT Server of the same software version can be installed and used, but the user should be aware of concurrent data access restrictions as documented in section 3.3.3 (AT Data).

2. The AT Server locks access to the AT data directory when service is running. This prevents concurrent access to AT data regardless if a user is logged into the AT Server.

3. The default AT Server configuration enables both HTTP (TCP port 8080) and

HTTPS (TCP port 8443) client connections. The default HTTPS configuration includes a self-signed SSL certificate provided by Codonics. For maximum security, the site administrator should provide their own certificate. This can be a self-signed certificate which has been added to the list of trusted root certificates on a domain, or a certificate signed by a trusted certificate authority (such as Verisign or Thawte). Contact Codonics for information on configuring SSL certificates.

3.3.3   AT Data

Both the AT Stand-alone and AT Server utilize a single directory tree structure that contains all SLS data for a given instance of the drug formulary. The SLS drug formulary and configuration files contained in the data directory are the same for both configurations. This allows the data directory to be used by different AT installations of the same software version. The AT uses file locking to restrict access so only one running instance of the AT can access the data directory at a time.

3.3.4   AT Miscellaneous Information

The AT is typically installed and run on PC equipment running Windows 7 or newer that is owned and operated by the medical institution (See minimum hardware requirements below). The AT does not require any web browser add-ons such as Flash/Shockwave/Active-X.

Security patches to the Windows operating system hosting the AT are the responsibility of the site administrators. Updates to the AT application are tested, approved and released by Codonics. Codonics has a policy to monitor security related vulnerabilities in the AT and release updates as required. Information about updates to the AT will be posted on the Codonics website.

The AT uses an embedded SQL database for storage of drug information, configuration information and log files.

3.3.5   AT Stand-alone Hardware

Hardware Minimum Requirements				
Component Name	**Processor**	**RAM**	**HDD**	**RAID**
Administration Tool PC	Intel 2.66 GHz Core 2 Duo	4 GB	5 GB free space minimum, 30 GB recommended	Optional, configured by site

3.3.6   AT Server Hardware

Hardware Minimum Requirements				
Component Name	**Processor**	**RAM**	**HDD**	**RAID**
Administration Tool PC / Server	Intel Quad Core (i5, i7 or Xeon) with 2 cores allocated to AT	8 GB	5 GB free space minimum, 30 GB recommended	Optional, configured by site

P/N: 900-653-007.01

3.3.7   AT Stand-alone/Server Hardware (when AT is virtualized)

Hardware Minimum Requirements				
Component Name	**Processor**	**RAM**	**HDD**	**RAID**
Administration Tool PC	Intel Quad Core (i7 or Xeon) with 2 cores allocated to AT	8 GB with 4 GB allocated to VM	5 GB free space minimum, 30 GB recommended	Optional, configured by site

See section 0 on AT Virtualization below for information on virtualized environments.

Note: The above specified hardware requirements for a virtualized AT environment (includes the Stand-alone AT and AT server) are sufficient to run the EN in addition to the AT.

3.3.8   AT Stand-alone/Server

Software		
Application Name	**Version #**	**Description**
Windows	7, 8.x, 2008, 2012R2, 2016	Approved operating systems to run the AT. (Supplied by user)
Internet Explorer	8-11	A web browser is required for the AT to operate. Windows Internet Explorer 11 is recommended. (Supplied by user)
Java	JRE 1.6.0-35 (32-bit)	The AT includes an embedded copy of Java that is only accessible by the AT. It can co-exist with other Java versions on the same PC. The locally installed version is not registered with the system as a visible resource. **NOTE: The AT has known problems working with newer versions of Java and Codonics recommends that users do not attempt to change the embedded version of Java. See additional notes below related to Java security.**
Derby	10.7.1.1	An embedded open source SQL database is included in the AT application for storage of drug information and log files.

P/N: 900-653-007.01

3.3.9   AT Virtualization

The AT allows virtualization. Codonics will make reasonable attempts to assist with virtualization issues, but the customer is responsible for ensuring proper operation in a virtual environment.

Software		
Application Name	**Version #**	**Description**
VMware ESXi (recommended)	N/A	The AT runs with an approved Windows OS under VMware ESXi.
Citrix XenServer	N/A	The AT runs with an approved Windows OS under Citrix XenServer.

3.3.10   AT Java Security

The SLS Administration Tool (AT) requires Java JRE 1.6.0-35 (32-bit) that is bundled with the AT software and automatically installed. However, the bundled JRE 1.6.0-35 runtime is not registered on the system as a resource that is visible to other applications or users. No other Java versions are required on the system that runs the AT. If you choose to install another version of Java (e.g. a newer version), that is OK but it will not be used by the AT.

Codonics recognizes that the older Java JRE 1.6.0-35 (32 bit) has some security issues. The vulnerabilities of JRE 1.6.0-35 are relevant only when it is registered on the system and used by other applications such as browsers that run Java applets. The AT does not use JRE 1.6.0-35 in a manner that exposes known vulnerabilities.

P/N: 900-653-007.01

3.4   EN (Email Notifier)

The Email Notifier (EN) is a Windows® based Java® application used to send email status messages related to SLS devices. The messages can contain information on either the status of the SLS device such as "out of media", or information about events such as "drug not found".   The EN can also be configured to send messages to groups of email users. The EN can only report on SLS devices that are accessible on the local network.

The EN is typically run as a system process on a Windows 7 or other Windows PC owned and operated by the medical institution. The EN can also be run manually from a command prompt. Security patches to the Windows operating system hosting the EN are the responsibility of the site administrators. Updates to the EN application are tested, approved and released by Codonics. Codonics has a policy to monitor security related vulnerabilities in the EN and release updates as required.

> **The EN application only requires the customer to supply a Microsoft Windows based computer as described later is this section. All other software modules required for the operation of the EN are included and automatically installed when the EN is installed. No additional 3rd party software packages such as databases need to be supplied by the customer.**

3.4.1   EN Hardware

Hardware Minimum Requirements				
Component Name	**Processor**	**RAM**	**HDD**	**RAID**
Email Notifier PC	Intel 2.66 GHz Core 2 Duo	4 GB	1 GB free space for application	Optional, Configured by site

EN Hardware (when EN is virtualized)

Hardware Minimum Requirements				
Component Name	**Processor**	**RAM**	**HDD**	**RAID**
Email Notifier PC	Intel Quad Core (i5, i7 or Xeon) with 2 cores allocated to EN	8 GB	1 GB free space for application (see note)	Optional, Configured by site

See section 3.4.3 on EN Virtualization below for more information on virtualized environments.

Note: The above specified hardware requirements for the EN virtual environment are sufficient to run the AT Stand-alone or AT Server in addition to the EN. However, the free space on the hard drive (HDD) should be increased to 5GB when running both applications.

P/N: 900-653-007.01

3.4.2   EN Software

Software		
Application Name	**Version #**	**Description**
Windows	Windows 7 or newer	Approved operating systems to run the EN.
Java	JRE 1.6.0-35 (32-bit)	Java is required by the EN. The EN includes an embedded copy a local copy of Java that is only accessible by the EN. It can co-exist with other Java versions on the same PC. **NOTE: See AT note on using other versions of Java.**

3.4.3   EN Virtualization

The EN allows virtualization, but Codonics does not explicitly support any particular virtual environment. Codonics will make reasonable attempts to assist with virtualization issues, but the customer is responsible for ensuring proper operation in a virtual environment.

Software		
Application Name	**Version #**	**Description**
Citrix XenServer	N/A	The EN runs with an approved Windows OS under Citrix XenServer.
VMware ESXi	N/A	The EN runs with an approved Windows OS under VMware ESXi.

3.4.4   EN Java Security

The SLS Email Notifier (EN) requires Java JRE 1.6.0-35 (32-bit) that is bundled with the EN software and automatically installed. The EN uses JRE 1.6.0-35 in a similar manner to the AT and has similar security considerations. Refer to section 3.3.10, AT Java Security for more information.

4. System Accessories

The following accessories are optional components of the Codonics Safe Label System.

4.1 SLS Accessories

4.1.1 SLS Hand Scanner

An optional external barcode hand scanner (Codonics part number: SLS500-HSCN) is available that connects to the SLS with a 6-foot USB cord and allows scanning of drug containers without bringing the containers to the built-in scanner of the SLS. The scanner is manufactured by Motorola (Model DS4208-HC). The hand scanner is enabled by a Codonics issued Feature Key installed on the SLS and by clearing (un-checking) the "Disable Wired Hand Scanner" setting in the AT Configuration Safety menu.

Codonics ships the hand scanner pre-programmed to operate with the SLS. In the event any scanner settings are changed, they can be reprogrammed using the procedure described in Codonics Tech Brief (part number 901-249-005). When the hand scanner is connected to the SLS, both the built-in scanner and hand scanner can be used to read barcodes.

4.1.2 SLS Wi-Fi Adapter

An optional Wi-Fi adapter is available that plugs into a USB port on the bottom of the SLS (Codonics part number: SLS500-WIFI.) The Wi-Fi adapter is enabled by a Codonics issued Feature Key installed on the SLS. When the Wi-Fi adapter is enabled, both the built-in Ethernet port and Wi-Fi can be configured and used concurrently. However, the most common configuration is for only one network interface to be active at a time. See section 8, System Networking for more details.

4.2 AT Accessories

4.2.1 AT Hand Scanner

A barcode hand scanner is required for learning and verifying drug containers on the AT. Codonics supplies a barcode scanner in the AT Accessory Kit, Codonics part number: AT-ACC-KIT-2. The Codonics supplied scanner is either the Motorola (DS4208-HC) or Zebra (DS4308-HC). The hand scanner settings must be programmed by the site to ensure proper operation with the AT. The programming procedure is described in Codonics Tech Brief (part number 901-260-002) provided with the scanner.

Other third party USB connected scanners configurable as an HID device, with AIM code support and all of the appropriate symbologies enabled may be used. Hand scanners from Zebra (formerly Motorola), Honeywell, Code and Datalogic have been used successfully with the AT. Codonics does not guarantee the operation of any specific third party hand scanner other than the recommended scanners shipped by Codonics (part numbers: AT-AAC-KIT or AT-ACC-KIT-2).

4.3   EN Accessories

The EN has no accessories.

P/N: 900-653-007.01

5. System Workflow

Each component of the Safe Label System has a unique workflow. The section describes the workflow of individual components after they are set up and operational.

5.1 SLS

A user logs in using the SLS touch-screen display or a barcode on a user badge printed by the system. Once logged in, the user can scan barcodes on drug containers (vials, ampoules, etc.) using the SLS barcode reader or optional USB hand scanner and provide any additional information, such as dilutions and diluents, required to prepare the drug using the touch-screen display. The SLS prints a label designed for application to a syringe or other secondary drug container using an embedded color printer.

The SLS stores information about the drug being prepared including user information and preparation date and time in internal logs files. All user interactions with the SLS including logins, logouts, drugs prepared, cancelled preparations and other user inputs are permanently logged by the SLS. The AT can retrieve log files from the SLS over the network or the user can make a copy of the log files onto a customer supplied, unencrypted FAT or FAT32 formatted USB drive connected to the SLS. Data analytic tools are available from Codonics to extract user and drug related information.

5.2 AT

A user logs in to the AT application (Stand-alone or Server) to access the application. Drug information is imported into an MDD (Master Drug Database) from trusted sources such as an internal pharmacy drug list in CSV format or a third party drug database such as Lexicomp. The user can also enter drug information manually.

Once the MDD is populated, the user selects a set of drugs, known as the "formulary", that will be accepted by the SLS. Other information required by the SLS such as dilutions, diluents, label color, label pattern, expiration time and warning messages are added by the user to complete the formulary. The user then approves the final formulary and builds a file package to be deployed to SLS devices over the network or via USB flash drive.

The user can also control certain operational aspects of the SLS by modifying configuration settings with the AT and deploying a configuration package to SLS devices similar to the way formulary packages are distributed. All AT data is stored in a configurable directory that is accessible by the system hosting the AT (see section 3.3.3 AT Data).   The site is responsible for backing up this directory (see section 10 System Backup).

5.3 EN

The EN can be configured to start automatically as a system process on the computer system hosting the EN application or the user can run the application at a command prompt. No other user interaction is required after the EN is running.

P/N: 900-653-007.01

6. System PII and User Accounts

6.1 SLS

SLS user accounts are initially created using the touch-screen display and stored locally on the device. User accounts contain limited PII (Personally Identifiable Information) that includes the user name (up to 38 characters), user initials (up to 3 characters, required for printing compliant drug labels), an alpha-numeric user ID (up to 16 characters) and a PIN security code (up to 10-digits). The PIN security code is encrypted using SHA-1 hashing for local storage on the SLS device.

When a user account is created, the SLS prints a user badge label with a barcode to simplify future logins by scanning the barcode on the SLS device. An account created on one SLS is automatically created on other SLS devices when the user badge is used for login. Users that do not login with the user badge will need to create an account on each SLS device with touch-screen display. All user accounts have the same permission level.

There are no default user accounts built into current SLS software, although older software releases (lower than 1.8.0) included a default user account with user ID "1111".

There are no user accessible methods to remove or change user accounts once created. Codonics Technical Support can provide information to customers for removing user accounts upon request. The SLS does not use LDAP or Active Directory. All user account activity related to creation, login and logout is logged and stored in files within the SLS system.

The SLS supports an auto-logout function with a configurable timeout that can be enabled using the configuration settings of the AT. There is no policy to enforce changing of SLS passwords at regular intervals.

6.2 AT

The AT relies primarily on login security of the Windows operating system hosting the AT application. One default login account with a default password is built-in to the AT application software. The password can be changed by the user after installation. Beginning with AT software version 1.8.0, a strong login password can be required as a configuration setting in the AT. The default login username cannot be changed. The AT password is encrypted using SHA-1 hashing and stored locally in the AT database. The AT login does not use LDAP or Active Directory. Beginning with version 1.9.0, the AT provides an auto-logout function (user configurable with a default of 30 minutes). There is no policy to enforce changing the AT password at regular intervals.

Notes: No PII (Personally Identifiable Information) other than the default AT login account is utilized or stored by the AT. When the AT is used to manage SLS devices on a network, the AT processes and stores PII information received from the SLS and SLS log files including the SLS user login name, user ID and user initials.

6.3   EN

The EN does not require user accounts or passwords. Access depends solely on login security of the Windows operating system. The SMTP functions of the EN may require login and password information. This information is contained in text configuration files set up by the site. The EN uses a special SSH read-only password to retrieve status information from SLS device. The SSH password is set in a text configuration file.

Notes: The EN stores PII (Personally Identifiable Information) in the form of email addresses required to deliver notification messages. The EN processes PII information received from SLS devices on the network including the SLS user login name, user ID and user initials.

6.4   SSH

All network communications between the AT or EN, and the SLS are handled by SSH and SCP protocols using 128-bit SSL encryption based on the SSH-2 protocol (RFC 4251) with AES-128-ctr ciphers for communications and diffie-hellman-group1-sha1 for key exchange. Two passwords for SSH/SCP are assigned to the AT and SLS that can be changed by the site. The first password, called the "Read-only password", is for retrieving SLS status information.   The other password, called the "Read-write password", is for updates transferred from the AT to the SLS over the network.   SSH passwords for the AT and SLS are encrypted using SHA-512 hashing and stored locally on the respective applications or devices. The EN only uses the Read-only password to retrieve status information from the SLS. The EN does not require the Read-write password. The Read-only password is set by the site administrator in the EN text configuration file.

P/N: 900-653-007.01

7. System PHI

7.1 SLS

As shipped from the factory, the SLS does not receive, store, process or transmit PHI (Protected Healthcare Information). The SLS does not support PHI in the U.S. market.

Note: In some non-U.S. markets, the SLS can optionally be configured to receive PHI for printing on labels. This requires a Codonics issued Feature Key that must be installed on each SLS unit and integration with third party equipment that is configured to send PHI data to the SLS using a proprietary SLS communication protocol. All PHI received by the SLS is transient. No PHI information is electronically logged or stored to any non-volatile memory on the SLS or transferred to any other device. The only record of PHI produced by SLS is in hardcopy form on ink jet printed labels.

7.2 AT

The AT does not receive, store, process or transmit PHI.

7.3 EN

The EN does not receive, store, process or transmit PHI.

P/N: 900-653-007.01

8. System Networking

8.1 SLS

The SLS 500i PCS is designed to operate with or without a network connection. It can be connected to an Ethernet network using a CAT-5 or higher straight-through RJ-45 network patch cable. The Ethernet speed is automatically negotiated by the SLS.

Note: SLS devices starting with 140C and 141C support 10 and 100mb/sec speeds.
    SLS devices starting with 142C support 10, 100 and 1000mb/sec speeds.

Optionally (if so ordered), a Wi-Fi adapter is available (Codonics part number: SLS500-WIFI). The Wi-Fi adapter can be added to SLS units at a later date. The SLS requires a Codonics issued Feature Key installed locally on the SLS to enable the Wi-Fi interface.

Several different Wi-Fi adapters have been shipped by Codonics for use on the SLS. Generally, new adapters are added when the previous adapter is no longer available. The table below shows the various adapters and the software releases that support those adapters.

SLS 500i PCS Wi-Fi Adapters

SLS 500i PCS Wi-Fi Adapters		
Adapter Name	**Support Begins in Software Version**	**Description**
Asus USB-N13 Rev A1	v1.3.0	802.11 b/g (2.4 GHz only)
EnGenius EUB9706	v1.4.0	802.11 b/g (2.4 GHz only)
Elecom W300NU2E	v1.6.1	802.11 b/g (2.4 GHz only) Note: For use in Japan only
Edimax EW-7811UTC	v1.8.2	802.11 b/g/n (2.4 GHz) and 802.11 a/n/ac (5.0 GHz)

Notes: 1. New SLS software releases maintain support for all previous Wi-Fi adapters.

2. SLS units with the Asus USB-N13 Rev A1, EnGenius EUB9706 and Elecom W300NU2E adapters enable 802.11 b/g only even though the hardware in these adapters can support 802.11 b/g/n. Future SLS software releases will continue to configure these adapters for 802.11 b/g only to ensure the installed base of SLS units will not encounter Wi-Fi related problems that may be caused by enabling the "n" protocol when installing new SLS software releases.

3. SLS units with the Edimax EW-7811UTC adapter enable all Wi-Fi protocols supported by the adapter hardware including 802.11 b/g/n @ 2.4 GHz and 802.11 a/n/ac @ 5.0 GHz.

4. SLS units with existing Wi-Fi devices can be upgraded to newer adapters by installing the appropriate software on the unit and replacing the existing Wi-Fi adapter with a newer adapter. Upgrading Wi-Fi adapters is not required when installing new SLS software as new software releases support previous adapters. Wi-Fi Feature Keys on the SLS will work with any adapter.

SLS Wi-Fi adapters support WEP, WPA or WPA2 encryption and can be configured for EAP-TLS or PEAPv0 certificate based authentication.

All network communications between Codonics supplied software applications (AT and EN) and the SLS are encrypted using 128-bit SSH (see section 6 "System PII and User Accounts" for more information on SSH and encryption).

The SLS uses an internal firewall to block incoming connection requests to network ports that are not used. A list of network ports used by the SLS is included in the Appendix B of this document.

P/N: 900-653-007.01

8.2   AT

The AT is designed to operate with or without a network connection to SLS units. Network services are provided by the Windows computer hosting the AT. The AT includes a user interface called the Device Manager that allows users to interact with SLS devices on the network. The Device Manager must be configured with a Device List of IP addresses or hostnames of each SLS device to be managed. Once configured, the AT polls each SLS device at regular intervals to retrieve status information. SSH is used to retrieve status information from SLS devices. The AT uses an SSH password called the "Read-only password" that is set in the Security menu of the AT to retrieve SLS status information. The AT can also transfer formulary updates, configuration updates and software updates to SLS devices when initiated by the AT user. All updates transferred to the SLS are in a digitally-signed, proprietary file format called "packages" to prevent unauthorized updates from being installed on SLS devices. SSH is used to transfer packages to SLS devices. This SSH password is called the "Read-write password" and is set in the Security menu of the AT. A list of network ports used by the AT is included in the Appendix B of this document.

P/N: 900-653-007.01

8.3 EN

The EN requires a network connection. Network services are provided by the Windows computer hosting the EN. The EN must be configured with a Device List of IP addresses or hostnames of the SLS systems. Once configured the EN polls SLS devices at regular intervals to retrieve status information and generates email notifications based on the status and rules configured in the EN. The EN uses SSH to retrieve status information from the SLS devices. The SSH password is set in an EN configuration file. This is the same password as the AT/SLS "Read-only" password. The EN does not transfer information to SLS devices. The EN must be configured with SMTP server information to send email messages to users at the site. A list of network ports used by the EN is included in the Appendix B of this document.

8.4 Third-Party Device Integration

The SSH/SCP network interface provided by the SLS and used by the AT and EN is also designed to be used by third party devices to achieve integration with the SLS device. This interface is called the SLS SNET interface. Examples of such devices are automated drug dispensing systems ("smart carts") and anesthesia information management systems ("AIMS"). There are two common types of integration leveraged by these devices:

1. **Common Login**: When a user logs in to the third party device, that device sends a message over SSH to the SLS device, causing the same user to be logged in on the SLS. For example, a user logs in to their smart cart application and is then automatically logged in to the SLS that is associated with that cart.

2. **Common Scanner**: When a user scans a drug container on the SLS in order to generate the proper label, the SLS sends the barcode scan information from the container to the third party device, alerting it to the fact that a particular drug is being prepared by the user. For example, a user scans a propofol vial on the SLS, causing the proper label to be printed. In addition, the barcode scan information from that vial is sent to the smart cart, which then decrements its inventory count for propofol.

3. **Patient Case:** When a user starts a patient case on the third party device, that device sends a Start-Case message over SSH to the SLS device, causing the SLS to display information about the patient and print the patient information on labels. The patient case will remain open on the SLS until closed by a message from the third party device or the SLS user logs out of the unit. For example, a user opens a case for patient name "John Smith" having ID "12345678" on a third party device and sends a Start-Case message to the SLS causing the SLS to display the patient name and ID and print John Smith and 12345678 on drug labels produced by the system. When the SLS receives a Stop-Case message from the third party device or the SLS user logs out, it ceases using the patient information and no electronic record of the patient information in maintained by the SLS.

The network communication required for these integration points is depicted in the diagram in Appendix A. The TCP Port that is used to communicate barcode scan information to the third party device is configured and controlled by the third party device. In addition, the third party device must provide configuration settings for indicating the specific SLS device it is talking to (i.e. IP address, Port, SSH 'read-write' password). No additional configuration of the SLS device is required to enable third party device integration.

9. System Logs

9.1 SLS

The SLS stores events related to drugs being prepared including user account information, along with date and time of the events in internal logs files. All user interactions with the SLS including logins, logouts, drugs prepared, cancelled preparations and other user inputs are permanently logged by the SLS. The AT can retrieve log files from the SLS over the network or the user can make a copy of the log files onto a customer supplied, unencrypted FAT or FAT32 formatted USB drive connected to the SLS.

The SLS stores an encrypted backup copy of SLS information including the system log files on a special removable USB drive supplied with the SLS device called a "SmartDrive."

Notes: 1. No PHI information is logged or stored by the SLS. PII information is stored in system log files (see section on System PII and User Accounts).

2. Contact Codonics Technical Support for assistance extracting user and drug related information from SLS log files.

9.2 AT

The AT does not provide any log files intended for user interpretation. Several internal system logs are maintained for Codonics diagnostic purposes.

Note: No PHI or PII information (other than the default AT login) is logged or stored by the AT.

9.3 EN

The EN does not provide any log files intended for user interpretation. Several internal system logs are maintained for Codonics diagnostic purposes.

Note: No PHI or PII information is logged or stored by the EN.

P/N: 900-653-007.01

10. System Backup

10.1 SLS

The SLS stores an encrypted backup copy of the formulary, configuration information, user accounts, Feature Keys and system log files on a removable USB drive supplied with the SLS device called a "SmartDrive". The SmartDrive is intended to simplify swapping of SLS devices when service is required by transferring all relevant data to the new device. Most information on the SmartDrive is encrypted and cannot be interpreted by users.

Log files can be copied off the SLS to an end-user supplied USB drive from the USB port of the SLS device. Users can also retrieve SLS log files over a network from the Device Manager menu of the AT. Log files copied off the SLS are not encrypted and are typically used for data analysis. Contact Codonics for assistance in processing information in the log files. Besides log files, other data input into the SLS such as formulary and configuration information is supplied from external sources and is considered static data that does not require backup by the SLS.

10.2 AT

The AT utilizes a single directory tree that contains all data for a given instance of the drug database. Some sites may use multiple directories when supporting multiple formularies. It is the responsibility of the site to perform regular backups of these directories. Beginning with AT release 1.7.0, a backup copy can be configured to maintain on local or remotely mounted (shared) drives at user defined intervals. The default configuration will create a backup copy when the formulary is promoted.

10.3 EN

The EN configuration data is stored in a single directory tree. It contains all data for the operation of the EN. It is the responsibility of the site to perform regular backups of this directory. The EN does not perform any automatic backups or maintain extra copies of the data.

　　　　　　　　　　　　　　　　　　　　P/N: 900-653-007.01

11. System Specifications

11.1 SLS 500i PCS

System:	Integrated touch screen computer, 2D barcode scanner, color ink jet printer, audio speaker, Ethernet interface and provision for optional Wi-Fi network interface and/or hand scanner.
Ink Cartridges:	One three-color cartridge (CMY)
SmartDrive:	USB flash drive for storing configuration data, formulary database, log files
Readable Barcodes:	Code 39, Code 32, Code 128, Data Matrix, EAN-8, EAN-13, EAN-128, GS1-128, GS1 DataBar Family, Interleaved 2 of 5, ISBT-128, ITF-14, QR Code, UPC-A, UPC-E, UPC-E1.
Writable Barcodes:	A primary Data Matrix barcode is printed on labels produced by the SLS. An auxiliary UPC-A, EAN-13, Code 128 and Codabar (NW7 in Japan) barcode can optionally be printed on the label that contains either the drug container ID (e.g. NDC) or the patient ID when PHI is enabled.
Network Interfaces:	Ethernet (RJ-45), included standard Wi-Fi (USB-2 adapter), optional, available from Codonics
Network Speeds:	Ethernet, full duplex: 10/100/1000 Base-T (SLS serial numbers 142C) 10/100 Base-T (SLS serial numbers 140C, 141C) Wi-Fi (See section 8.1 for Wi-Fi details)
Network Protocols:	SSH (Secure Shell) and SCP (Secure Copy) Used to access SLS from Codonics-authorized applications/devices

Dimensions:	Height:	16.50 in. (41.9 cm)
	Width:	10.43 in. (26.5 cm)
	Depth:	15.67 in. (39.8 cm)

Weight:	14.5 lbs (6.6 kg)
Power:	Universal Input:100-240 VAC, 50/60 Hz 0.3 A @ 90 VAC (27 W)

Environmental:	Operating Altitude:	700 to 1060hPa (0.7 to 1.05 atm)
	Temperature:	15–30°C (59–86°F)
	Humidity:	20%–80% non-condensing

Shipping and Storage:	Altitude:	500 to 1060hPa (0.5 to 1.05 atm)
	Temperature (Hardware):	-22.2–51°C (-8–123.8°F)
	Temperature (Ink and Labels):	1–43°C (34–110°F)
	Humidity (Hardware):	5%–85% non-condensing
	Humidity (Ink and Labels):	5%–80% non-condensing

Medical Compliance FDA cleared to market per 510(k) K101439, Class II MDD CE, GMP/QSR, and Regulatory: ISO13485: 2003, Safety IEC/EN 60601-1 and EMC/EMI
EN 55011(A) and EN 60601-1-2 for Healthcare facilities

FDA Classification: Class 2 equipment, Product Code BSZ, Anesthesiology Device

IEC 60601-1 Classification: Class I equipment, type ordinary IXPO continuous with intermittent loading.

Appendix A – Network Diagram (Full System)
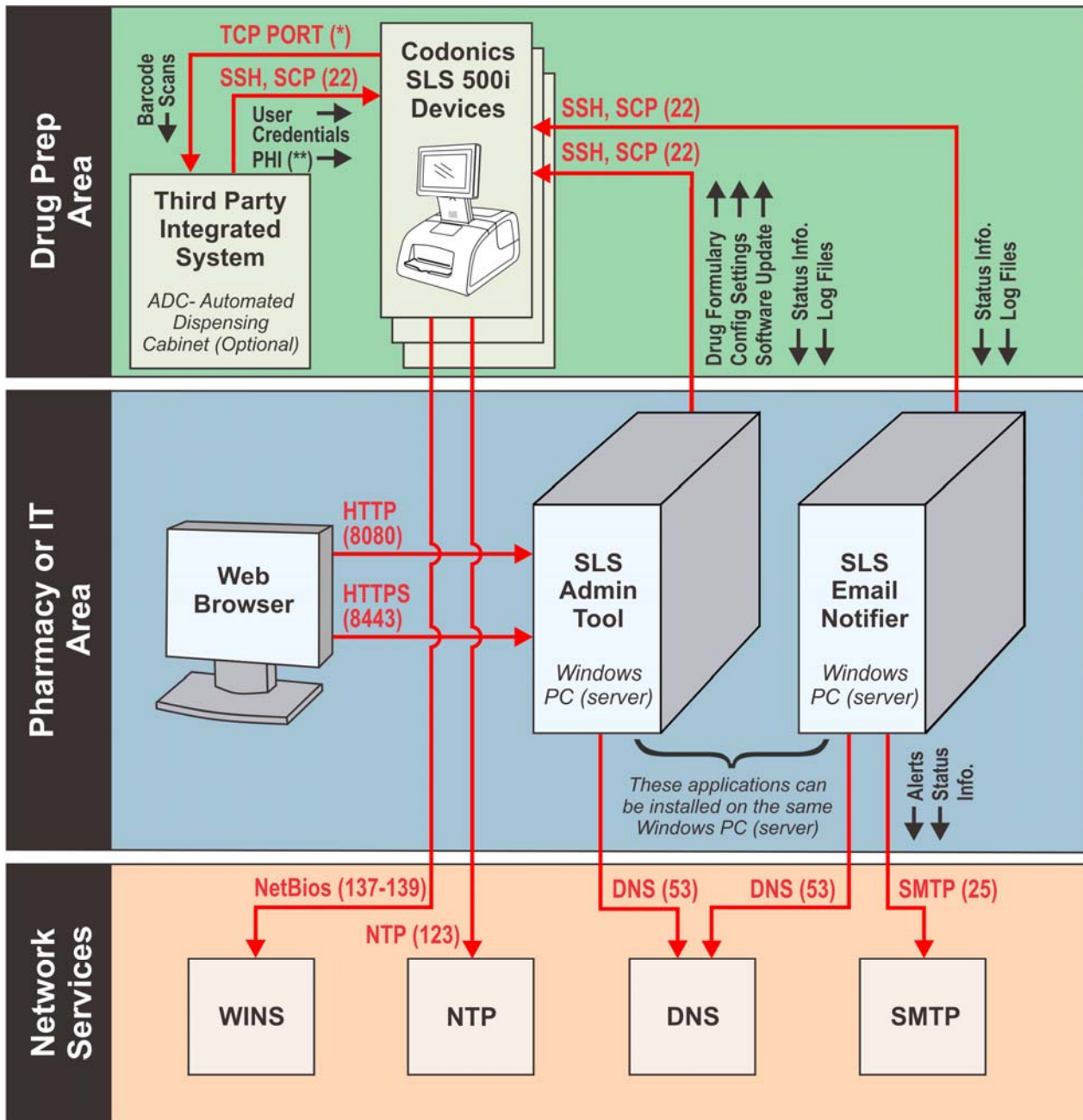
* TCP port number is configurable by ADC

** PHI transfers are optional, use encryption and require support by ADC

Appendix B – Network Ports and Protocols

SLS Network Ports

The SLS uses an internal firewall to restrict network connections. All incoming network connections are blocked except as documented below. All network connections use IPv4.

ICMP: Enabled

TCP and UDP:

Target Port	TCP	UDP	Direction	Description	Notes
22	X		In	Secure Shell (SSH). The SLS accepts incoming SSH connections from the AT (Administration Tool) or EN (Email Notifier). SSH/SCP is used to transfer software, configuration and formulary updates to the 500i. It is also used to query the 500i status and retrieve log files.	(1) The SSH passwords are site configurable using the Administration Tool (AT). (2) The SSH port number can be changed using the AT.
123		X	Out	Network Time Protocol (NTP)	Sets the internal time on SLS units.
137		X	In and Out	NetBIOS Name Service. The SLS uses NetBIOS services to assign each SLS a unique, static hostname. This simplifies setting up the Administration Tool (AT) and Email Notifier (EN) on networks that dynamically assign IP addresses to 500i devices.	Ports 137-139 are only opened when the "Enable Device Name" option is set in the System Configuration Section of the AT.
138		X	In and Out	NetBIOS Datagram Service.	
139	X		In and Out	NetBIOS Session Service.	

P/N: 900-653-007.01

SLS Administration Tool and Email Notifier Network Ports

The SLS AT (Administration Tool) and EN (Email Notifier) are designed to run on customer supplied Windows® computer systems. The information in this section only describes the network services used by the AT and EN.

TCP and UDP:

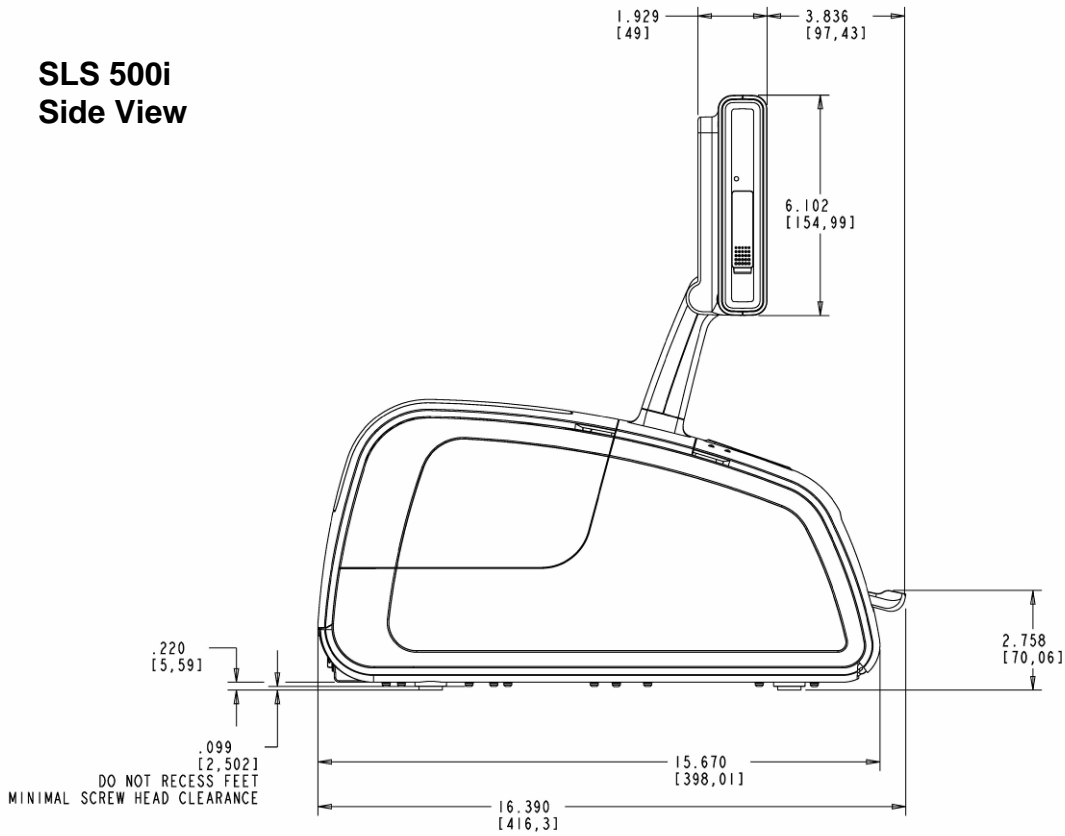| Target Port	T C P	U D P	Direction	Description	Notes
22	X		Out	Secure Shell (SSH). The AT (Administration Tool) and EN (Email Notifier) can optionally communicate with SLS devices on the network using SSH. The AT and EN initiate all SSH requests to SLS devices. SSH/SCP is used to transfer software, configuration and formulary updates to the 500i. It is also used to query the 500i status and retrieve log files.	(1) The SSH passwords are site configurable using the AT. (2) The SSH port number can be changed using the AT.
25	X		Out	Simple Mail Transport Protocol (SMTP). SMTP is used by the EN. The EN is an optional SLS utility that can send email messages to users when certain trigger events occur on the 500i.	SMTP is only used by the EN and not the AT.
53		X	Out	Domain Name Service (DNS). DNS is used by the AT and EN to resolve IP addresses of 500i devices that are referenced by hostname instead of IP addresses.	Most Windows computer systems running the AT or EN have DNS enabled by default.
8080	X		In	Hypertext Transport Protocol (HTTP)	This port is used to receive incoming browser requests when the AT is installed in Server mode.
8443	X		In	Secure Hypertext Transport Protocol (HTTPS)	This port is used to receive incoming browser requests when the AT is installed in Server mode. HTTPS connections will display a certificate warning on the user's browser unless the AT Server is configured with a proper SSL certificate issued by the site.

Target Port	T C P	U D P	Direction	Description	Notes
Random	X		In and Out	Hypertext Transport Protocol (HTTP). The AT is implemented as a client-server model with both the client and server running on the same computer. The AT installs a local application on the host computer and utilizes the default browser on the same computer to provide the user interface. The HTTP port used to communicate between the browser and AT application is selected at random using a port above 1024.	This port is only used internally on the host computer. When installed in stand-alone mode, the AT is configured to only communicate with a web browser on the local system and will not communicate with browsers on other computers.

P/N: 900-653-007.01

Appendix C – Mechanical Drawings

The following drawings provide basic SLS 500i mechanical information. A full set of mechanical drawings can be requested from Codonics (Tech Brief Part Number: 901-408-001).

**SLS 500i
Side View**

**SLS 500i
Bottom View**

P/N: 900-653-007.01