IT Resource Guide for Codonics® Safe Label System®

(Software Release v2.6.x)

Codonics® Safe Label System®
SLS 550i® and SLS 500i® Point of Care Station (PCS)

Legal Notice

TABLE OF CONTENTS

1. Overview

This document contains network and software security information related to the Codonics® Safe Label System® with software release 2.6.x. The purpose of the document is to assist IT staff and users with the deployment of the Safe Label System in healthcare environments.

2. System Description

The Safe Label System ("SLS") is an FDA-cleared Class II medical device (510K K101439), that improves the safety and accuracy of medication preparation and labeling compliance anywhere medications are prepared.

The Safe Label System consists of three main components:

SLS PCS. The SLS Point-of-Care Stations ("SLS PCS") are embedded devices used by anesthesia providers in operating rooms and other anesthetizing locations to label drugs that are prepared into secondary containers such as syringes and IV bags. The current shipping SLS PCS model is the SLS 550i®. The SLS 500i® is the previous model that is still supported but no longer in production. The SLS software release described in this document will work on all SLS PCS models.

SLS AT. The SLS Administration Tool ("SLS AT") is a Windows® based application installed and run on a hospital supplied server or computer. It is a required component of Safe Label System. The SLS AT is accessed by pharmacy using a web browser to maintain and update the drug formulary and safety configuration settings of the SLS PCS devices.

SLS EN. The SLS Email Notifier ("SLS EN") is a Windows® based application installed and run on a hospital supplied server or computer. It is an optional application that monitors the hardware status and user events of the SLS PCS devices connected to the hospital network and generates emails to specified users or groups with notifications that require attention.

The SLS workflow is designed for safe, efficient preparation and labeling of drugs. SLS PCS devices are typically installed on the hospital network and configured with a drug formulary and safety settings sent from the SLS AT. Users scan the NDC barcode on a drug vial or ampoule using an SLS PCS built-in barcode reader to print a compliant, color-coded drug identification label that is affixed to a syringe or IV bag. For safety, the recommended workflow is: Scan one vial; print one label; prepare one syringe; label one syringe.

3. System Details

This section provides technical details of the three major SLS components.

3.1 SLS PCS (Models SLS 550i and SLS 500i)

The SLS Point-of-Care Station ("SLS PCS") is a standalone drug labeling device that uses embedded hardware and software manufactured by Codonics. The SLS PCS contains a color inkjet label printer, embedded computer, flash memory storage, LCD display, touch screen interface, speaker for announcing drug information, Ethernet, optional Wi-Fi interface and USB ports for software updates, performing some maintenance functions and expansion (expansion on SLS 550i models only).

The SLS PCS is an embedded device that does not require any customer supplied software or hardware. The devices are typically installed on drug dispensing carts or near drug preparation areas in operating rooms, PACU's, ICU's or pharmacies.

The SLS PCS devices can be connected to a LAN network via Ethernet or Wi-Fi. Wi-Fi connections require the installation of an optional Wi-Fi module and Feature Key that are available from Codonics. Connecting SLS PCS 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 PCS 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 SLS AT must be transferred manually to each SLS PCS device using a site-supplied, unencrypted FAT or FAT32 formatted USB drive.

The SLS PCS uses an embedded SQL database for storage of drug formulary information, configuration information and log files. Only the embedded software on the SLS can access the database.

Software updates for the SLS system including the SLS PCS, SLS AT and SLS EN are tested, approved and released by Codonics according to the following policy.

Codonics performs ongoing monitoring of the SLS solution for software vulnerabilities and schedules regular software updates with security patches at least once per calendar year. If a significant software vulnerability is discovered between scheduled releases, Codonics will assess the risk posed and release documentation addressing the specific concerns including instructions to mitigate the vulnerability or a software update as required. Software updates are distributed in a proprietary, digitally-signed file format called "packages" to ensure the integrity of the software. Information about the availability of important software updates to SLS will be posted on the Codonics website.

3.1.1 SLS PCS Hardware

The following is a summary of the major hardware components of SLS PCS models.

SLS PCS Hardware Information				
Component Name	**Processor**	**RAM**	**Storage Capacity**	**SW Support**
SLS 550i Serial Numbers Starting with: 143C, 144C	Intel Atom (embedded)	2 GB (embedded)	32 GB Minimum Solid State Drive (embedded)	2.6.x (current)
SLS 500i Serial Numbers Starting with: 142C	Intel Atom (embedded)	2 GB (embedded)	32 GB Solid State Drive (embedded)	2.6.x (current)
SLS 500i Serial Numbers Starting with: 140C, 141C	Intel Atom (embedded)	1 GB (embedded)	4 GB Compact Flash (embedded)	2.6.x (current)

3.1.2 SLS PCS Software

The following is a summary of the versions of major software components used by the SLS PCS.

SLS PCS Software Information		
Application Name	**Version #**	**Description**
SLS PCS Embedded Application	2.6.x	Codonics designation of the software version installed on the SLS PCS device.
SLS PCS Operating System	Linux Kernel 4.15.0-122 based on Ubuntu 18.04	The embedded version of Linux has been optimized and hardened for the SLS PCS.
Java	OpenJDK 8u272-b10	Java is used to run some internal processes of the embedded SLS PCS application. No internal software components, including Java, are accessible to users.
SQLite	3.28.0	An embedded open source SQL database is included in the device for storage of drug data and log files.

3.1.3 SLS PCS Virtualization

The SLS PCS application and operating system are embedded in the PCS device and cannot be virtualized.

3.1.4 SLS PCS Software Security

The SLS PCS uses a custom Linux based operating system and application software designed 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 for information on SLS network ports).
4. Encrypt all network access credentials stored on the device (e.g. certificates, passwords, security 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). The SLS components, software and data are entirely hosted on-premises.

3.2 SLS AT (Administration Tool)

The SLS AT is a Windows® based Java® application used to create and maintain the drug formulary and configuration files required by SLS PCS devices. Additionally, the SLS AT allows remote monitoring and updating of software on SLS PCS devices when they are connected to a network.

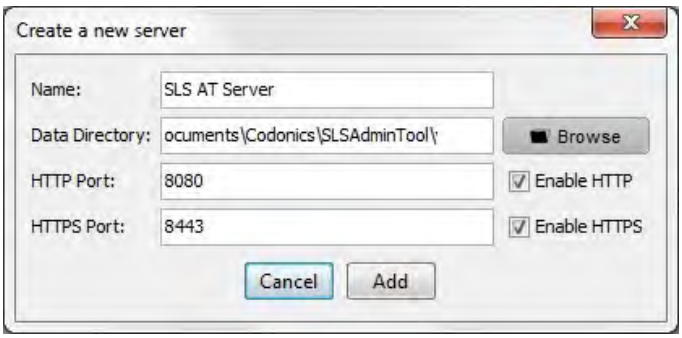
3.2.1 SLS AT Installation

The SLS AT application is installed in a server configuration that allows users access from a web browser on the same network. A list of compatible browsers is provided further down in this section.

The SLS AT application and data are entirely hosted on-premises. The application runs as a service on the site supplied Windows® system.

Notes:

1. Beginning with SLS software release 2.5.0, the SLS AT can only be installed in a web server configuration. The standalone version of the AT is no longer supported.
2. One instance of the SLS AT is typically installed at a site. In circumstances where multiple copies of the AT need to be installed, please contact Codonics Technical Support for assistance.
3. The SLS AT will lock access to the data directory when the application is running. This prevents concurrent access to data in the data directory, regardless of whether a user is currently logged into the AT.
4. The default SLS AT configuration enables both HTTP (TCP port 8080) and HTTPS (TCP port 8443) for client browser connections. The default HTTPS configuration includes a self-signed SSL certificate provided by Codonics. For maximum security, the site administrator should install 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). Request document TSi-SLS-0036.01 from Codonics Technical Support for more information about configuring SSL certificates for the SLS AT.
5. The HTTP and HTTPS protocols can be enabled or disabled using the SLS AT Server Manager menu and the following dialog box:



The SLS AT (Administration Tool) application only requires the customer to supply a Microsoft® Windows® based computer that meets the software and hardware requirements described later is this section. All other software modules required by the SLS AT are included and automatically installed when the SLS AT is installed. No additional 3rd party software packages such as databases need to be supplied by the customer.

3.2.2 SLS AT Data Information

The SLS AT utilizes a single directory tree that contains all data files for one instance of the drug formulary and associated configuration information. The structure of individual data files is generally unique to a specific software version of the SLS AT. A data migration tool is supplied with major releases of the SLS AT software to convert data files when moving to newer versions.

The SLS AT uses file locking to restrict access so that only one running instance of the AT can access the data directory at a time. The SLS AT application and the data directory should be located on the same drive.

3.2.3 SLS AT Hardware Requirements

Minimum Configuration		Recommended Configuration	
Processor	Xeon X5660 @ 2.80 GHz, Core i7-2600 @ 3.40 GHz or faster.	**Processor**	Xeon W-2135 @ 3.70 GHz, Core i7-7700 @ 3.60 GHz or faster.
RAM	6 GB	**RAM**	8 GB
Application Disk Space	10 GB	**Application Disk Space**	30 GB

Notes:

1. For best performance, use a locally attached SSD or high-speed RAID for hosting the SLS AT data directory.
2. When running more than one instance of the SLS AT on the same hosting system, increase the system RAM by at least 3 GB for each additional instance.
3. The hardware configurations shown are sufficient for running the SLS EN on the same system hosting the SLS AT.

3.2.4 SLS AT Hardware Requirements for Upgrades

Customers that are running previous versions of the SLS AT or SLS EN in a server configuration can use the following guidelines to determine if the existing system is sufficient to run new versions of SLS AT and SLS EN.

1. The existing processor should have at least four cores.
2. The Passmark Single Thread Rating of the processor should be at least 1250 to meet minimum performance criteria. The recommended Single Thread Rating is at least 2500 for best performance. The Passmark rating of most processors is available at:

   https://www.cpubenchmark.net/cpu_list.php
3. Follow the RAM and Disk Space recommendations in the previous section.
4. Follow the Windows operating system recommendations in the upcoming sections.

3.2.5 SLS AT Virtualization

The SLS AT allows virtualization, but Codonics does not explicitly support any particular virtual environment. Codonics will make reasonable efforts to assist customers with set up and operational questions regarding virtualization, but the customer is responsible for ensuring the proper operation of the SLS AT and the virtual environment.

Any set of hardware requirements shown in section 3.2.3, "SLS AT Hardware Requirements", are sufficient for running a virtualized SLS AT with the following additional considerations:

1. At least two CPU cores should be allocated to the VM.
2. When running more than one instance of the SLS AT on the same virtual machine, allocate one more CPU core (total of three) to the VM and increase the system RAM by at least 3 GB for each additional instance.

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

3.2.6 SLS AT Software

The following is a summary of the versions of major software components used by the SLS AT.

SLS AT Software Information		
Application Name	**Version #**	**Description**
SLS AT Application	2.6.x	Codonics software version.
Windows	10, 8.1, 2012R2, 2016, 2019 64-bit version required.	Approved operating systems to run the SLS AT. The operating system and computer hardware for running the SLS AT are supplied by site.
Internet Explorer Edge (old version) Edge (new version) Chrome Firefox (see note) Safari (see note)	11 44 88 (or higher) 88 (or higher) 85 (or higher) 13 (or higher)	A web browser is required for the SLS AT to operate. Internet Explorer, Edge (both old and new versions) and Chrome are recommended. Note: Firefox and Safari will generally work but have some known issues.
Java	OpenJDK 8u272-b10	The SLS AT includes an embedded copy of Java that is only accessible by the application. It can co-exist with other Java versions on the same PC. The version installed by the SLS AT is not registered with the system as a visible resource.
Derby	10.14.2.0	An embedded open source SQL database is included with the SLS AT application for storage of drug information and log files.

3.2.7 SLS AT Java Information

The SLS AT is designed and tested with the version of Java that is bundled with the SLS AT software and automatically installed. The bundled Java runtime is not registered on the system as a resource and is not visible or accessible to other applications running on the same system.

Other versions of Java can be installed on the same system hosting the SLS AT for other purposes, but they will not be used by the SLS AT.

No attempts should be made to change the Java version that is automatically installed with the SLS AT and SLS EN. The Safe Label System is an FDA cleared medical device that is verified and validated as a complete system with specific versions of software components such as Java. Codonics includes updates to Java as required when new SLS software versions are released.

The SLS AT includes the latest security patches for Java at the time of release. Java vulnerabilities that may be found in the future are typically relevant only when Java is registered on the system and used by other applications (such as browsers that run Java applets). The version of Java embedded in the SLS AT is only accessed by the AT and not used as a general-purpose Java runtime by other applications. This significantly mitigates the risk of Java vulnerabilities found after the SLS AT software is released.

3.2.8 SLS AT Miscellaneous Information

The SLS AT is installed and run on computer equipment provided by the medical institution (refer to section 3.2.3, SLS AT Hardware Requirements).

Web browsers accessing the SLS AT do not require any add-ons such as Flash, Shockwave, Active-X or Java.

The SLS AT uses an embedded SQL database for storage of drug information, configuration information and log files. The database is not accessible to other applications.

Security patches to the Windows system hosting the SLS AT are the responsibility of the site administrators and can be installed as necessary. Updates to the SLS AT application and supporting software components are tested, approved and released by Codonics.

3.3 SLS EN (Email Notifier)

The SLS EN is a Windows® based Java® application that is site configurable to periodically send users email messages related to SLS PCS devices. The messages can contain information on either the status of devices such as "Out of media", or information about user events such as "Drug not found" when a vial is scanned by a user that is not in the drug formulary. Messages can be sent to individual users or groups of email users. The SLS EN can only report information retrieved from SLS PCS devices that are connected to the same network as the system hosting the EN application.

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

The SLS EN (Email Notifier) application only requires the customer to supply a Microsoft® Windows® based computer that meets the software and hardware requirements described later is this section. All other software modules required by the SLS EN are included and automatically installed when the SLS EN is installed. No additional 3rd party software packages such as databases need to be supplied by the customer.

3.3.1 SLS EN Hardware Requirements

The SLS EN hardware requirements are the same as the SLS AT. The SLS EN can be installed on the same system running the SLS AT. Refer to section 3.2.3, "SLS AT Hardware Requirements" for details.

3.3.2 SLS EN Virtualization

The SLS EN allows virtualization, but Codonics does not explicitly support any particular virtual environment. The virtualization information for the SLS AT also applies to the SLS EN. Refer to section 3.2.5, SLS AT Virtualization for details.

3.3.3 SLS EN Software

The following is a summary of the versions of major software components used by the SLS AT.

SLS EN Software Information		
Application Name	**Version #**	**Description**
SLS EN Application	2.6.x	Codonics software version.
Windows	10, 8.1, 2012R2, 2016, 2019 64-bit version required.	Approved operating systems to run the SLS EN. The operating system and computer hardware for running the SLS EN are supplied by site.
Java	OpenJDK 8u272-b10	The SLS EN includes an embedded copy of Java that is only accessible by the application. It can co-exist with other Java versions on the same PC. The version install by the SLS EN is not registered with the system as a visible resource. **Note: The SLS EN has only been validated with the version of Java bundled with the application. Codonics recommends that users do not attempt to change the embedded version of Java.**

3.3.4 SLS EN Java Information

The SLS EN is designed and tested with a version of Java that is bundled with the SLS EN software. Java is automatically installed with the SLS EN application. The Java information for the SLS AT is the same as the Java information for the SLS EN. Refer to section 0, SLS AT Java Information for more information about how Java is managed.

4. System Accessories

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

4.1 SLS PCS Accessories

4.1.1 SLS PCS Hand Scanner

An optional external barcode hand scanner (Codonics Part Number: SLS500-HSCN) connects to the SLS PCS 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 hand scanner is enabled by a Codonics-issued Feature Key installed on the SLS PCS and by clearing (un-checking) the "Disable Wired Hand Scanner" setting in the SLS AT Configuration Safety menu.

Codonics ships the hand scanner pre-programmed to operate with the SLS PCS. If scanner settings are changed, they can be reprogrammed using the procedure described in Codonics Tech Brief (Codonics Part Number 901-260-003). When the hand scanner is connected to the SLS PCS, both the built-in scanner and hand scanner can be used to read barcodes.

4.1.2 SLS PCS Wi-Fi Adapter

An optional Wi-Fi adapter is available from Codonics that plugs into a USB port on the bottom of the SLS PCS (Codonics Part Number: SLS500-WIFI.) The Wi-Fi adapter is enabled by a Codonics-issued Feature Key installed on the SLS PCS. 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 SLS AT Accessories

4.2.1 SLS AT Hand Scanner

A barcode hand scanner is required for learning and verifying drug containers with the SLS AT. Codonics supplies a barcode scanner in the SLS AT Accessory Kit (Codonics Part Number: AT-ACC-KIT-2). The hand scanner settings must be programmed by the site to ensure proper operation with the SLS AT. The programming procedure is described in Codonics Tech Brief provided with the scanner (Codonics Part Number 901-249-006).

Other third-party USB barcode scanners configured as a HID device, with AIM code support and appropriate barcode symbologies enabled can be used. Hand scanners from Zebra (formerly Motorola), Honeywell, Code and Datalogic have been used successfully with the SLS AT. Codonics does not guarantee the operation of any third-party hand scanner other than the Codonics supplied scanner (Codonics Part Number: AT-ACC-KIT-2).

4.3 SLS EN Accessories

The SLS EN has no accessories.

5. System Workflow

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

5.1 SLS PCS

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

The SLS PCS 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 PCS including logins, logouts, drugs prepared, cancelled preparations and other user inputs are permanently logged by the SLS PCS. The SLS AT can retrieve log files from the SLS PCS devices 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 PCS. Data analytic tools are available from Codonics to extract user and drug related information.

5.2 SLS AT

The user, typically a pharmacist, connects to the SLS AT application with a web browser and logs in. 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 PCS. Other drug information 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 PCS devices over the network or via USB flash drive.

The user can also control certain operational aspects of SLS PCS devices by modifying configuration settings with the SLS AT and deploying a configuration package to the devices similar to the way formulary packages are distributed. All SLS AT data is stored in a configurable directory location (see section 3.2.2, SLS AT Data Information for more details). The site is responsible for backing up the data directory (see section 10, System Backup).

5.3 SLS EN

The SLS 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. Once the EN is set up and configured, no further user interaction is required.

6. System PII and User Accounts

6.1 SLS PCS

SLS PCS user accounts are initially created using the touch screen display and stored locally on the device. User accounts can optionally be created on the SLS AT using a licensed feature called SLS Centralized User Management, and installed on SLS PCS devices over the network or via a USB drive as part of the configuration package settings. There are no default user accounts built into current SLS software.

User accounts contain limited PII (Personally Identifiable Information) that includes the user name (up to 38 characters), user initials (up to 3 characters), an alpha-numeric user ID (up to 16 characters) and a PIN security code (up to 10-digits). The PIN security code is encrypted for local storage on SLS PCS devices using SHA-1 hashing on software releases 2.5.x and earlier, and PBKDF2 hashing beginning with 2.6.0.

The SLS PCS can print a user badge label with a barcode to simplify future logins by scanning the barcode on the SLS PCS device. An account created on one SLS PCS is automatically created on other SLS PCS devices when the barcode on the user badge is scanned for login. Users that do not login with the user badge will need to create an account on each SLS PCS device using the touch screen display or with the SLS Centralized User Management feature. All SLS PCS user accounts have the same permission level.

There is no method for normal users of the SLS PCS to remove user accounts once created. Codonics Technical Support can provide information to customers for removing user accounts. User accounts created with the SLS Centralized User Management feature can also be removed with that feature.

The SLS PCS does not use LDAP or Active Directory for managing user accounts on the devices. All user account activity related to creation, login and logout is logged and stored locally on the SLS PCS devices.

The SLS PCS supports an auto-logout function with a configurable timeout that can be enabled using the configuration settings of the SLS AT. There is no policy to enforce changing of SLS PCS PIN codes at regular intervals, but accounts created with the SLS Centralized User Management feature can be configured and require the user to enter a PIN code the first time the account is used.

6.2 SLS AT

The SLS AT supports three types of user authentication for login: (1) Windows Active Directory, (2) Secure LDAP (aka LDAPS), and (3) a single built-in login account with a site configurable password. When the SLS AT is initially installed, the built-in login account is active. Once logged into the built-in account, the login AT can be configured to use an alternate login authentication method such as Active Directory or LDAPS.

The SLS AT built-in login account can be configured after the initial login to require a strong password. The built-in login username cannot be changed. The built-in account

password is encrypted for local storage in the SLS AT database using SHA-1 hashing on software releases 2.5.x and earlier, and PBKDF2 hashing beginning with 2.6.0. An auto-logout function is configurable on the SLS AT with a default setting of 30 minutes. There is no policy to enforce changing the built-in SLS AT password at regular intervals.

Active Directory and LDAPS support on the SLS AT restricts user logins to only those users who are a member of a specified Security Group on the hospital domain. The Security Group is a configurable setting on the SLS AT.

Notes: 1. The SLS AT logs the username of successful and unsuccessful user login attempts.

2. When the SLS AT is used to manage SLS PCS devices on a network, the SLS AT can receive and store PII information received from the SLS PCS devices including the SLS PCS user IDs and user initials.

6.3 SLS EN

The SLS EN does not require configuration of user accounts or passwords. Access to the SLS EN application and associated files depends solely on the login security of the Windows operating system hosting the SLS EN application.

The SMTP functions of the EN may require login and password information depending on the configuration of the email server at the customer site. This information is contained in text configuration files set up on the hosting system by the site. The EN uses a special SSH read-only password to retrieve status information from SLS PCS devices. The SSH password is also set in a text configuration file on the hosting system.

Notes: 1. The EN stores some PII in the form of email addresses required to deliver notification messages through the customer site email server.

2. The EN processes some PII information received from SLS PCS devices on the network including the SLS PCS user IDs and user initials.

6.4 SSH

All network communications between the SLS AT or SLS EN applications and the SLS PCS devices 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 SLS AT and SLS PCS devices that can be changed by the site. The first password, called the “Read-only password”, is for retrieving SLS PCS device status information. The other password, called the “Read-write password”, is for updates transferred from the SLS AT to the SLS PCS over the network. SSH passwords for the SLS AT and SLS PCS are encrypted using SHA-512 hashing and stored locally on the respective applications or devices. The SLS EN only uses the Read-only password to retrieve status information from the SLS PCS. The SLS EN does not require the Read-write password. The Read-only password is set by the site administrator in a text configuration file on the Windows system hosting the SLS EN application.

7. System PHI

No SLS components require or use PHI (Protected Healthcare Information).

7.1 SLS PCS

The SLS PCS devices do not receive, store, process or transmit PHI.

7.2 SLS AT

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

7.3 SLS EN

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

8. System Networking

8.1 SLS PCS

The SLS 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.

Notes: 1. SLS PCS devices having serial numbers that start with 140C and 141C support 10 and 100 Mb/sec speeds.

2. SLS PCS devices having serial numbers that start with 142C, 143C and 144C support 10, 100 and 1000 Mb/sec speeds.

A Wi-Fi adapter is optionally available from Codonics (Part Number: SLS500-WIFI). The Wi-Fi adapter can be added to SLS PCS units at a later date. Each SLS PCS with Wi-Fi requires a Codonics-issued Feature Key installed on the device to enable the Wi-Fi interface.

Several different Wi-Fi adapters have been shipped by Codonics for use on the SLS PCS. The table below shows the various adapters and the SLS PCS software releases that first supported those adapters.

SLS PCS Wi-Fi Adapters

SLS 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)
DLink DWA-140 (HW v B2)	v2.4.2	802.11 b/g (2.4 GHz only)
TP-Link AC600 Mini, Archer-T2U TP-Link AC600 Nano, Archer-T2U	v2.6.0	802.11 b/g/n (2.4 GHz) and 802.11 a/n/ac (5.0 GHz)

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

2. SLS PCS units with the Asus USB-N13 (Rev A1), EnGenius EUB9706, Elecom W300NU2E and DLink DWA-140 (HW v B2) 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 PCS 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. This adapter uses a subset of the 5.0 GHz channels supported by 802.11ac. The supported 5.0 GHz channels are 36, 40, 44, 48, 149, 153, 157, 161 and 165. Most Wi-Fi access points properly handle this subset of channels. If there is a problem, Codonics Technical Support can provide instructions to change the SLS PCS to use 802.11n instead of 802.11ac to properly negotiate the 5.0 GHz channels with the access point.

4. SLS PCS units with existing Wi-Fi adapters can be upgraded to newer adapters by installing the appropriate software release 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 PCS software as new software releases support previous adapters. Wi-Fi Feature Keys install on the SLS PCS devices will work with any adapter.

The SLS PCS 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 (SLS AT and SLS EN) and the SLS PCS devices 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 PCS devices is included in the Appendix B of this document.

8.2 SLS AT

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

8.3 SLS EN

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

8.4 Third-Party Device Integration

The SSH/SCP network interface on SLS PCS devices that is used by the SLS AT and SLS EN is also designed to be used by third-party devices to achieve integration with SLS PCS devices. This interface is called the SLS SNET interface. Examples of devices that have interfaces with SLS PCS devices include automated drug dispensing systems ("smart carts"). The SNET interface provides several functions including:

1. **Common Login**: When a user logs in to the third-party device, that device sends a message over SSH to the SLS PCS device, causing the same user to be logged in on the SLS PCS.
2. **Common Scanner**: When a user scans a drug container on an SLS PCS device to generate a label, the SLS PCS sends information about the barcode that was scanned including extra information from the SLS PCS formulary and how the user prepared the drug over the network via SNET to the third-party device, alerting it to the fact that a particular drug is being prepared by the user. This information is commonly used by the drug cart to decrement inventory levels.
3. **Other Functions:** The SLS SNET interface can support other integration functions that are designed for specific OEM applications. Contact Codonics Technical Support or the SLS Sales team for more information.

The network communications required for SNET integrations is depicted in the network diagram shown in Appendix A.

9. System Logs

9.1 SLS PCS

The SLS PCS 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 PCS including logins, logouts, drugs prepared, cancelled drug preparations and other user inputs are permanently logged by the SLS PCS. The SLS AT can retrieve log files from the SLS PCS devices 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 PCS.

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

Notes: 1. No PHI information is received, logged or stored by the SLS PCS. Some PII information is stored in system log files (see section 6 on "System PII and User Accounts").

2. A software tool called the SLS Data Analytics Tool is available to help process information in the SLS PCS log files. Contact Codonics Technical Support for assistance with downloading and processing the SLS log files.

9.2 SLS AT

The SLS 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 limited PII information (SLS AT login information and information downloaded from SLS PCS log files) is logged or stored by the SLS AT.

9.3 SLS EN

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

Note: No PHI and limited PII (downloaded from SLS PCS log files) is logged or stored by the SLS EN.

10. System Backup

10.1 SLS PCS

The SLS PCS 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 PCS device called a "SmartDrive". SmartDrives are supplied only by Codonics. The SmartDrive is intended to simplify swapping of SLS PCS devices when service is required by transferring all relevant data to the new device. Most of the information on the SmartDrive is encrypted and cannot be interpreted by users.

Log files can be copied off the SLS PCS to a user-supplied USB drive from the USB port of the SLS PCS device. Users can also retrieve SLS log files over the network from the Device Manager menu of the SLS AT. Log files copied off the SLS PCS devices 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 PCS such as formulary and configuration information are supplied from external sources such as the SLS AT and are considered static data that do not require backup by the SLS PCS as the original files reside on another system.

10.2 SLS AT

The SLS 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. The SLS AT also includes a configurable option to make a backup copy of important data in the data directory on a local or remotely mounted (shared) drives at user defined intervals. The default configuration will create a backup copy whenever the drug formulary is promoted.

10.3 SLS EN

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

11. Remote Access, Cloud and SaaS

The Safe Label System does not include any built-in software or hardware capabilities that provide remote access, remote administration, Cloud or SaaS services.

All hardware, software and data associated with the SLS System are hosted entirely on-premises at the hospital facilities. No data is transmitted to Codonics, third-parties, the Internet or outside of the hospital network by the SLS System.

Codonics has experience with several remote access solutions and will work with customers if requested, to set up a remote access solution on an as-needed basis to help with system installation, training, upgrades or problem resolution.

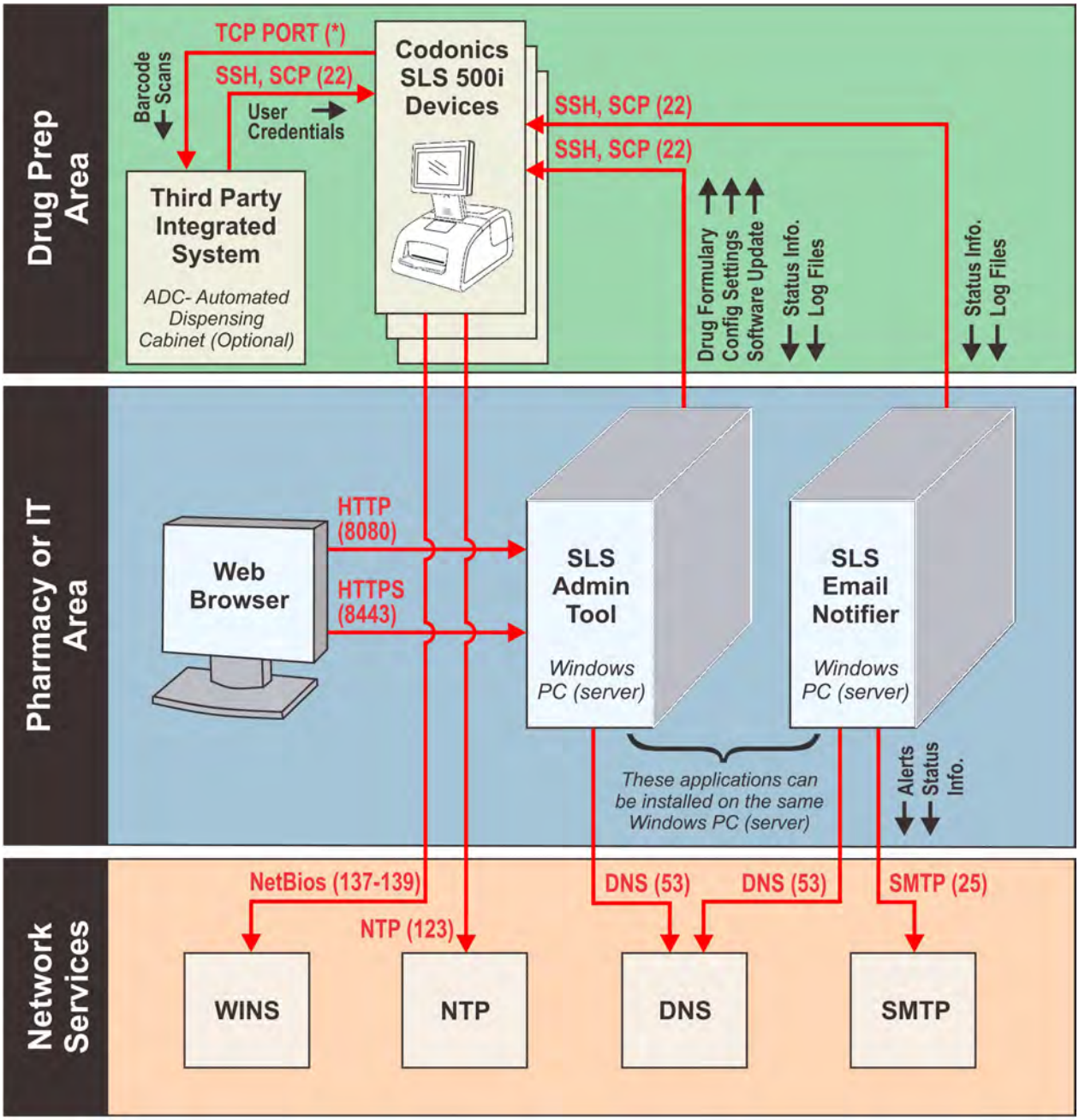
12. System Specifications

12.1 SLS 500i/550i 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:	Custom USB flash drive that is specific to SLS PCS devices for storing configuration data, formulary database, log files.
Readable Barcodes:	Code 128, GS1-128, Data Matrix, UPC-A, UPC-E, EAN-13, EAN-8, GS1 DataBar Family, Interleaved 2 of 5, ITF-14, Code 39, Code 32, ISBT 128, QR Code.
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 the drug container ID (e.g. NDC).
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 no. 142C, 143C, 144C); 10/100 Base-T (SLS serial no. 140C, 141C). Wi-Fi (See section 8.1 for Wi-Fi network speed details).
Network Protocols:	SSH (Secure Shell) and SCP (Secure Copy). Note: Required when accessing SLS from authorized apps/devices.
Dimensions:	H: 16.50 in. (41.9 cm) W: 10.43 in. (26.5 cm) D: 15.67 in. (39.8 cm)
Weight:	14.5 lbs (6.6 kg) without media. 15.7 lbs (7.1 kg) with media.
Electrical:	Universal Input: 100-240 VAC, 50/60 Hz, 27 W (0.3 A @ 90 VAC). Note: Add 10 W to power when connecting external USB devices.
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:	Full medical device compliance including Class 2 FDA 510(k) K101439 and Class I MDR 2017/745/EU (CE), GMP/QSR, ISO 13485: 2016/NS-EN ISO 13485:2016, Electrical Safety IEC 60601-1 Ed. 3.1 and EMC/EMI: FCC Class A and IEC 60601-1-2: Ed. 4 for Professional 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)



Appendix B – Network Ports and Protocols

SLS PCS Network Ports

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

SLS AT and SLS EN 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.

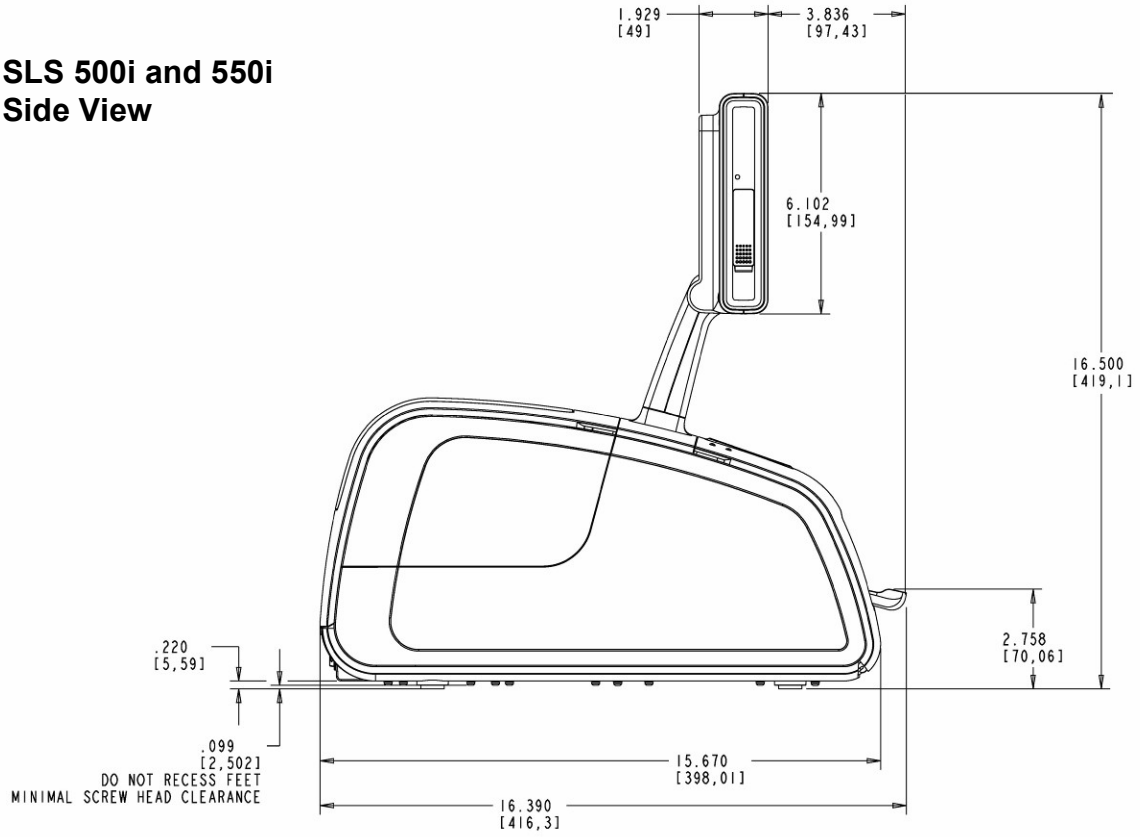
TCP and UDP:

Target Port	TCP	UDP	Direction	Description	Notes
22	X		Out	Secure Shell (SSH). The SLS AT and SLS EN can optionally communicate with SLS PCS devices on the network using SSH/SCP. The SLS AT and SLS EN initiate all SSH requests to SLS PCS devices. SCP is used to transfer software, configuration and formulary updates to the SLS. SSH is used to query the SLS PCS 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 SLS EN. The SLS EN is an optional application that can send email messages to users when certain trigger events occur on the SLS PCS devices.	SMTP is only used by the SLS EN and not the SLS AT.
53		X	Out	Domain Name Service (DNS). DNS is used by the SLS AT and SLS EN to resolve IP addresses of SLS PCS devices that are referenced by hostname instead of IP addresses.	Most Windows computer systems hosting the SLS AT and SLS EN have DNS enabled by default.
8080	X		In	Hypertext Transport Protocol (HTTP)	This port is used to receive incoming browser requests when the SLS AT. HTTP can be disabled using the SLS AT Server Manager menu.
8443	X		In	Secure Hypertext Transport Protocol (HTTPS)	This port is used to receive incoming browser requests when the SLS AT. HTTPS connections will display a certificate warning on the user's browser unless the SLS AT Server is configured with a proper SSL certificate issued by the site.

Appendix C – Mechanical Drawings

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

SLS 500i and 550i
Side View



SLS 500i and 550i
Bottom View