



IT Resource Guide for Codonics[®] Safe Label System[®] (Software Release 3.0.x)



**Codonics[®] Safe Label System[®]
SLS 550i[®] Point of Care Station (SLS PCS)**

PRODUCT CONTACT INFORMATION

Company Headquarters

Codonics Inc.
17991 Englewood Drive
Middleburg Hts., OH 44130
USA

Phone: 440.243.1198
800.444.1198
Fax: 440.243.1334
Email: info@codonics.com
Hours: 8:30 AM-5:30 PM ET, Mon-Fri (Closed official U.S. holidays)

Technical Support

Phone: 440.243.1198
800.444.1198
Fax: 440.243.1334 (Attn: SLS Tech Support -or- your support contact person)
Email: support@codonics.com for new support requests -or-
the email address of the support person you are working with.
Hours: 8:30 AM-5:30 PM ET, Mon-Fri (Closed official U.S. holidays)
After-hours, existing SLS customers can leave a message for a return call.

Sales

Phone: 440.243.1198
800.444.1198
Fax: 440.243.1334 (Attn: SLS Sales -or- your sales contact)
Email: info@codonics.com
Hours: 8:30 AM-5:30 PM ET, Mon-Fri (Closed official U.S. holidays)

Product Notices

Important information about the SLS product including software updates and cybersecurity notices can be found at: www.codonics.com/notices .

Legal Notice

This document and the designs, specifications and information disclosed herein 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	5
2. System Description	5
3. System Details	7
3.1 SLS PCS (Model SLS 550i)	7
3.2 SLS AT (Administration Tool)	10
3.3 SLS EN (Email Notifier)	14
4. System Accessories	16
4.1 SLS WAVE Scanner	16
4.2 SLS PCS Accessories	16
4.3 SLS AT Accessories	17
4.4 SLS EN Accessories	17
5. System Workflow	18
5.1 SLS PCS	18
5.2 SLS AT	18
5.3 SLS EN	19
6. System PII and User Accounts	20
6.1 SLS PCS	20
6.2 SLS AT	20
6.3 SLS EN	21
6.4 SSH	21
7. System PHI	22
7.1 SLS PCS	22
7.2 SLS AT	22
7.3 SLS EN	22
8. System Networking	23
8.1 SLS PCS	23
8.2 SLS AT	25
8.3 SLS EN	26
8.4 Third-Party Device Integration	27
9. System Logs	28
9.1 SLS PCS	28
9.2 SLS AT	28
9.3 SLS EN	29
10. System Backup	30
10.1 SLS PCS	30
10.2 SLS AT	30
10.3 SLS EN	30
11. Remote Access, Cloud and SaaS	31
12. System Specifications	32
12.1 SLS 550i PCS	32
Appendix A – Network Diagram (Full System)	33

Codonics Safe Label System: IT Resource Guide

Appendix B – Network Ports and Protocols.....34
Appendix C – Mechanical Drawings.....36
Appendix D – Confidential Addendum Request Procedure.....37
Appendix E – Security Recommendation and Best Practices38
Appendix F – SLS Software Update Policy and Process.....51

1. Overview

This document contains network and software security information related to the Codonics® Safe Label System® with Software Release 3.0.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.

Note: SLS Software Release 3.0.0 and higher no longer supports some older SLS 500i devices. The serial numbers of the unsupported SLS PCS devices start with 140C and 141C. Customers with these older SLS PCS 500i models should contact Codonics Sales Department (800.444.1198, 8:30 AM-5:30 PM ET, Mon-Fri) for upgrade options.

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 typically accessed by pharmacy using a web browser to maintain 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 that runs as a background service without a UI (see section 3.3 for more details). The SLS EN is installed and run on a hospital supplied server or computer. It can also be run on the same system hosting the SLS AT. the SLS EN 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 receive drug formulary and safety settings from the SLS AT over the network. 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.

SLS Security Note

Refer to “Appendix E - Security Recommendations and Best Practices” for details on configuring SLS components for improved network security.

3. System Details

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

3.1 SLS PCS (Model SLS 550i)

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, barcode scanner, Ethernet, optional WiFi interface and USB ports.

The SLS PCS does not require the addition of 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 WiFi. WiFi connections require the installation of an optional WiFi module and Feature Key that are available from Codonics. Connecting SLS PCS units to a network will simplify device monitoring and installation of formulary and software updates from the SLS AT (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 settings 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 Safe Label System
Software Security Update Policy**

Codonics performs ongoing monitoring of the Safe Label System (“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 and cybersecurity notices will be posted on the Codonics website at: www.codonics.com/notices.

3.1.1 SLS PCS Hardware

The following is a summary of the major hardware components of SLS PCS models supported by Software Release 3.0.x.

SLS PCS Hardware Information				
Component Name	Processor	RAM	Storage Capacity	SW Support
SLS 500i Serial Numbers Starting with: 142C	Intel Atom (embedded)	2 GB (embedded)	32 GB Solid State Drive (embedded)	3.0.x (current)
SLS 550i Serial Numbers Starting with: 143C, 144C	Intel Atom (embedded)	2 GB (embedded)	32 GB Minimum Solid State Drive (embedded)	3.0.x (current)

3.1.2 SLS PCS Software

For security reasons, some details about the internal software components used in the SLS PCS are only made available under NDA (Non-Disclosure Agreement). Refer to Appendix D in this document for more information.

3.1.3 SLS PCS Virtualization

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

3.1.4 SLS PCS Software Security

The SLS PCS uses a custom operating system (SLS OS 3) and application software designed to reduce security vulnerabilities using the following techniques:

1. Disable unnecessary user, administrative accounts and login functions of the device.
2. Remove or disable unnecessary software from the device.
3. Block incoming network connection requests on unused ports (refer to Appendix B for more 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 between SLS devices 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).

3.1.5 SLS PCS Touchscreen Keyboard

The SLS PCS uses a touchscreen keyboard for entry of some data fields. The touchscreen keyboard includes the most common characters required for typical data entry fields.

USB Keyboard Connection to SLS PCS

If a character is required that is not a part of the SLS PCS touchscreen keyboard (e.g. colon, semi-colon), a standard USB keyboard can be temporarily connected to the SLS PCS USB port on the left side of the touchscreen. The touchscreen keyboard will also work while the USB keyboard is connected to the SLS PCS.

Touchscreen Keyboard (Alphabetic):



Touchscreen Keyboard (Special Characters):



Touchscreen Keyboard (Numbers):



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 customer premises. The application runs as a service on a site supplied Windows® computer system or server.

Notes:

1. 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.
2. The SLS AT will lock access to the local 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.

SLS AT Security Note

Refer to “Appendix E - Security Recommendations and Best Practices” for details on configuring SLS components for improved network security.

SLS AT Additional Hardware and Software Requirements

The SLS AT (Administration Tool) application only requires the customer to supply a Microsoft® Windows® based server or computer that meets the software and hardware requirements described later in 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 or Java 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	30 GB	Application Disk Space	100 GB

Notes:

1. For best performance, use a locally attached SSD or high-speed RAID for hosting the SLS AT data directory.
2. A processor with at least four cores is recommended in hosting systems.
3. 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.
4. The hardware configurations shown are sufficient for running the SLS EN (Email Notifier) 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 version 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 using common virtual environments such as VMware ESXi and Citrix XenServer. 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 in the virtual environment.

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 to the VM and increase the system RAM by at least 3 GB for each additional instance.
3. When running the SLS EN on the same virtual machine as the SLS AT, allocate one more CPU core to the VM and increase the system RAM by at least 3 GB.
4. Virtualization of the SLS AT or SLS EN using Cloud based systems is not recommended.

3.2.6 SLS AT Software

For security reasons, some details about the internal software components used in the SLS AT are only made available under NDA (Non-Disclosure Agreement). Refer to Appendix D in this document for more information.

SLS AT Software Information		
Application Name	Version #	Description
SLS AT Application	3.0.x	Codonics software version.
Windows OS (Supported)	10 2016, 2019, 2022 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	11	A web browser is required for the SLS AT to operate. Internet Explorer, Edge (both old and new versions) and Chrome are recommended. Notes: Firefox works but has some known issues. Safari is not supported or recommended.
Edge (old version)	44	
Edge (new version)	105 (or higher)	
Chrome	105 (or higher)	
Firefox (see notes)	105 (or higher)	
Safari (see notes)	Not Supported	

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. The correct version of Java is automatically installed with the SLS AT. The bundled Java runtime used by the SLS AT is not registered on the hosting system as a public 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 the version of Java bundled in 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 registered on the system as a general-purpose Java runtime for use by other applications. This significantly mitigates the risk of Java vulnerabilities found after the SLS AT software is released. Codonics monitors security vulnerabilities to the SLS software and manages them as described in our Software Security Update Policy in section 3.1.

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 and anti-virus or malware protection for the Windows system hosting the SLS AT are the responsibility of the site administrators and can be installed as necessary. The SLS AT is compatible with most anti-virus and malware applications.

Updates to the SLS AT application and supporting software components are tested, approved and released by Codonics. No other changes to the installed SLS AT software should be made.

3.3 SLS EN (Email Notifier)

The SLS EN is a Windows® based Java® application that is site configurable to periodically send users email status messages related to SLS PCS devices using the customer’s email server. The SLS EN has no UI and runs in the background as a service. All administrative interactions with the SLS EN are done with a CLI interface using a CMD prompt on the hosting Windows system. The application can be started manually with a CLI command from CMD prompt or set up to automatically start using a Windows start up script.

The email messages produced by SLS EN contain information about the status of SLS PCS 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 users. The SLS EN can only report information retrieved from SLS PCS devices that are network accessible by the system hosting the EN application.

The SLS EN is typically run as a system process on a Windows system owned by the customer. 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.

SLS EN Additional Hardware and Software Requirements

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 in this section. The SLS EN runs in the background as a service and has no UI. All administrative interactions with the SLS EN is performed through CLI commands using a CMD prompt on the hosting system. 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 or Java 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

For security reasons, some details about of the internal software components used in the SLS EN are only made available under NDA (Non-Disclosure Agreement). Refer to Appendix D in this document for more information.

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 3.2.7, 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 WAVE Scanner

The SLS WAVE® (Codonics Part Number: SLS-WAVE) is an optional “hands-free” barcode scanner that connects via USB-2 to the local AIMS/EHR system in the operating room to record the NDC* (U.S. National Drug Code) number of the drug being administered to the patient. Several common AIMS systems including Epic, support the SLS WAVE scanner. The SLS WAVE is optimized for reading barcodes on syringe labels produced by the SLS PCS and transmitting that data to the AIMS/EHR system. The scanner connects to the AIMS computer using a USB cable (included) and special drug cart mounting hardware (included) to allow hands-free scanning of syringes by the anesthesia provider. The syringe label produced by the SLS PCS is configured to include a barcode with the NDC number of the drug used to fill the syringe. An anesthesia provider “waves” the syringe label barcode in front of the SLS WAVE scanner to send the NDC number to the AIM. The SLS WAVE does not require the installation of any special software, external power supplies or network connections.

() In other countries, the container ID and not the NDC is passed to the AIMS/EHR when the syringe is scanned at administration.*

4.2 SLS PCS Accessories

4.2.1 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.

4.2.2 SLS PCS WiFi Adapter

An optional WiFi adapter is available from Codonics that plugs into a USB port on the bottom of the SLS PCS (Codonics Part Number: SLS500-WIFI.) The WiFi adapter is enabled by a Codonics-issued Feature Key installed on the SLS PCS. When the WiFi adapter is enabled, both the built-in Ethernet port and WiFi 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.

4.3 SLS AT Accessories

4.3.1 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 AIMS 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).

4.4 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 print 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 also 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 for presentation in a user-friendly form.

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 SLS AT 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 an optional PIN security code (up to 10-digits). The PIN security code is encrypted using PBKDF2 hashing.

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 PBKDF2 hashing.

An auto-logout function is configurable on the SLS AT with a default setting of 30 minutes. There is no policy or setting available 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 WiFi adapter is optionally available from Codonics (Part Number: SLS500-WIFI). The WiFi adapter can be added to SLS PCS units at a later date. Each SLS PCS with WiFi requires a Codonics-issued Feature Key installed on the device to enable the WiFi interface.

Several different WiFi 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 WiFi Adapters

SLS PCS WiFi 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 GHz) *See Note 2
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 GHz)

Notes: 1. SLS PCS Software Release 3.0.x supports all previous WiFi adapters.

2. The Edimax EW-7811UTC adapter uses a subset of the 5 GHz channels supported by 802.11ac. The supported 5 GHz channels are in the UNII-1 and UNII-3 bands that include channels 36, 40, 44, 48, 149, 153, 157, 161 and 165. Most WiFi access points properly handle this subset of channels. If there is a problem, Codonics Technical Support can provide instructions to use 802.11n instead of 802.11ac to

properly negotiate the 5 GHz channels with the access point. Refer to section “SLS PCS 802.11ac (WiFi 5) Support” below for more information.

3. SLS PCS devices with existing WiFi adapters can be upgraded to newer adapters by installing the appropriate software release on the unit and replacing the existing WiFi adapter with a supported newer adapter. Upgrading WiFi adapters is not required when installing new SLS PCS software as new software releases support previous adapters. WiFi Feature Keys installed on the SLS PCS devices will work with any supported WiFi adapter.

4. 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 WiFi related problems that may be caused by enabling the “n” protocol when installing new SLS software releases.

SLS PCS 802.11ac (WiFi 5) Support

The 5 GHz WiFi channels supported by SLS PCS WiFi adapters can vary from the channels in the IEEE 802.11ac specification. The following tables show the 5 GHz channels defined by the IEEE and those channels actually supported by each SLS PCS WiFi adapter with 802.11ac capabilities. Channels highlighted in yellow are those supported by the adapters.

5 GHz 802.11ac (WiFi 5) Spectrum U.S.																											
US Band	Bandwidth	UNII-1				UNII-2a				UNII-2e (Extended)						UNII-3		ISM									
		20 MHz	36	40	44	48	52	56	60	64	100	104	108	112	116	120	124	128	132	136	140	144	149	153	157	161	165
		40 MHz	38		46		54		62		102		110		118		126		134		142		151		159		
		80 MHz	42				58				106				122				138				155				
		160 MHz	50								114																
		Freq (MHz)	5180-5240				5260-5320				5500-5560				5580-5640				5660-5720				5745-5825				
		Max Power	23 dBm (200 mW)								30 dBm (1 W)								14 dBm (25 mW)								
Note 1	DFS (Dynamic Frequency Selection)																										
Note 2	Ch 144, 142, 138 added after 802.11ac was ratified. Some devices don't support them.																										
Note 3													Weather Radar														

Edimax AC600 EW7811UTC (Configured for 802.11ac [WiFi 5] mode)																											
US Band	Bandwidth	UNII-1				UNII-2a				UNII-2e (Extended)						UNII-3		ISM									
		20 MHz	36	40	44	48	52	56	60	64	100	104	108	112	116	120	124	128	132	136	140	144	149	153	157	161	165
		40 MHz	38		46		54		62		102		110		118		126		134		142		151		159		
		80 MHz	42				58				106				122				138				155				
		160 MHz	50								114								138								
													Yellow = 5 GHz Channel Supported by Adapter														

SLS Adapter		Edimax AC600 EW7811UTC (Configured for 802.11n [WiFi 4] mode)																								
Bandwidth	US Band	UNII-1				UNII-2a				UNII-2e (Extended)						UNII-3				ISM						
	20 MHz	36	40	44	48	52	56	60	64	100	104	108	112	116	120	124	128	132	136	140	144	149	153	157	161	165
	40 MHz	38		46		54		62		102		110		118		126		134		142		151		159		
	80 MHz	42				58				106				122				138				155				
	160 MHz	50								114								Yellow = 5 GHz Channel Supported by Adapter								

SLS Adapter		TP-Link AC600 Archer-T2U (802.11ac [WiFi 5])																								
Bandwidth	US Band	UNII-1				UNII-2a				UNII-2e (Extended)						UNII-3				ISM						
	20 MHz	36	40	44	48	52	56	60	64	100	104	108	112	116	120	124	128	132	136	140	144	149	153	157	161	165
	40 MHz	38		46		54		62		102		110		118		126		134		142		151		159		
	80 MHz	42				58				106				122				138				155				
	160 MHz	50								114								Yellow = 5 GHz Channel Supported by Adapter								

Additional SLS PCS WiFi Information

The SLS PCS WiFi adapters support WEP, WPA or WPA2 encryption and can be configured for EAP-TLS or PEAPv0 password and 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 encryption and SSH passwords).

The SLS PCS 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.

Windows 10 and 11 have some limitations related to formatting USB flash drives with FAT32 filesystems. Windows CMD and Powershell include “format” commands that accept the /FS:FAT32 option to write a FAT32 filesystem to the drive. The /Q option specifies quick format mode to substantially speed up the process. If a flash drive is 32GB or less, it can be formatted by Windows for FAT32. If the flash drive is over 32GB and has a partition larger than 32GB, formatting as FAT32 can sometimes cause an error resulting in a corrupt filesystem. It is recommended that partitions over 32GB be deleted and a new partition of 32GB or less be created using “Create and format hard disk partitions” in the Windows Control Panel before formatting as FAT32. For more information, contact Codonics Technical Support and request document TSi-SLS-0064.

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.

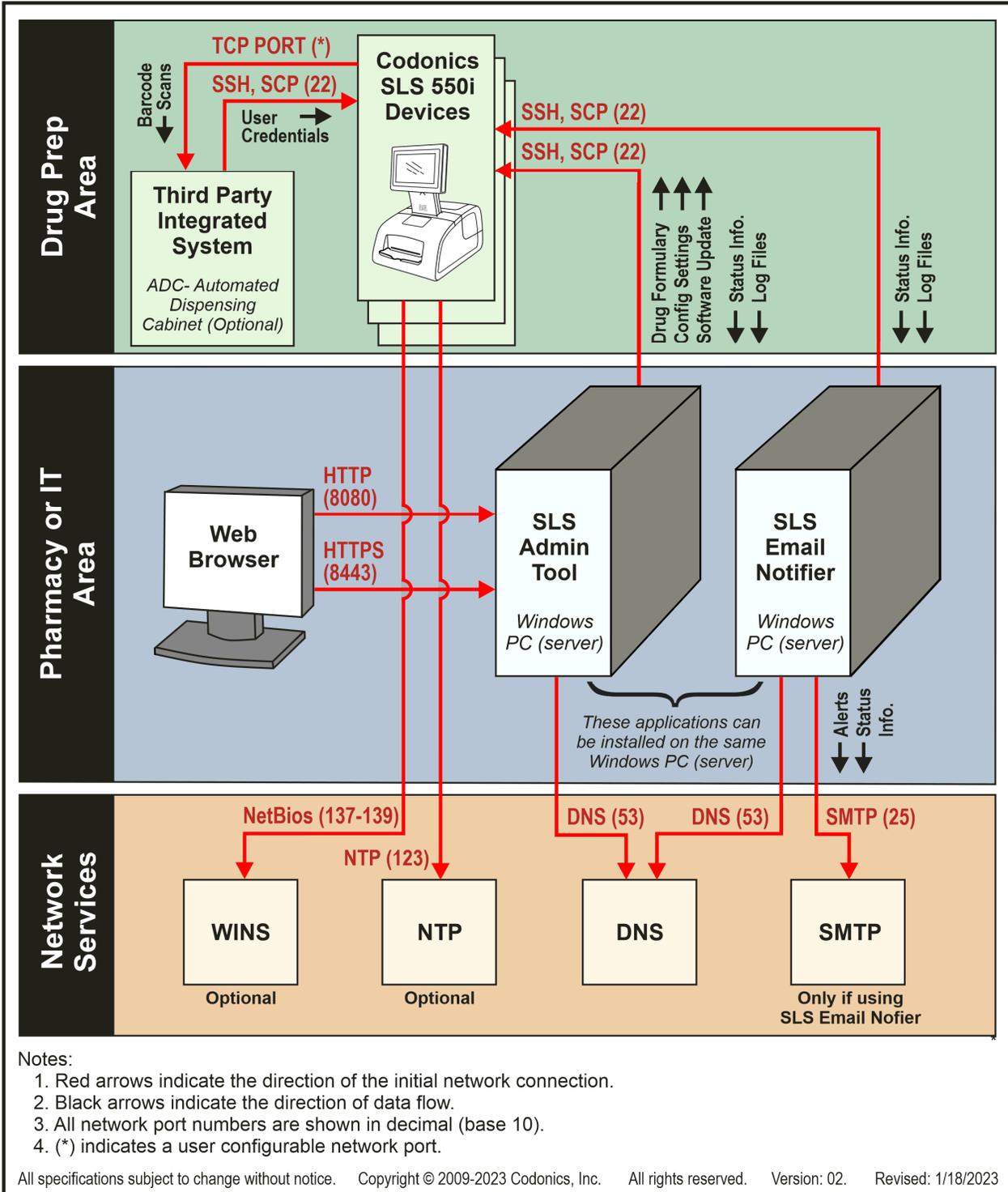
Codonics has experience with several remote access solutions and will work with customers if requested, to set up a remote access solution on an as-needed basis to help with system installation, training, upgrades or problem resolution.

12. System Specifications

12.1 SLS 550i PCS

System:	Integrated touch screen computer, 2D barcode scanner, color ink jet printer, audio speaker, Ethernet interface and provision for optional WiFi 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. WiFi (USB-2 adapter), optional, available from Codonics.
Network Speeds:	Ethernet, full-duplex: 10/100/1000 Base-T. WiFi (See section 8.1 for WiFi 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, 30 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	T C P	U D P	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 SLS EN (Email Notifier) are designed to run on customer supplied Windows® computer systems/servers. The information in this section only describes the network services used by the SLS AT and SLS EN, and not other software installed on the servers.

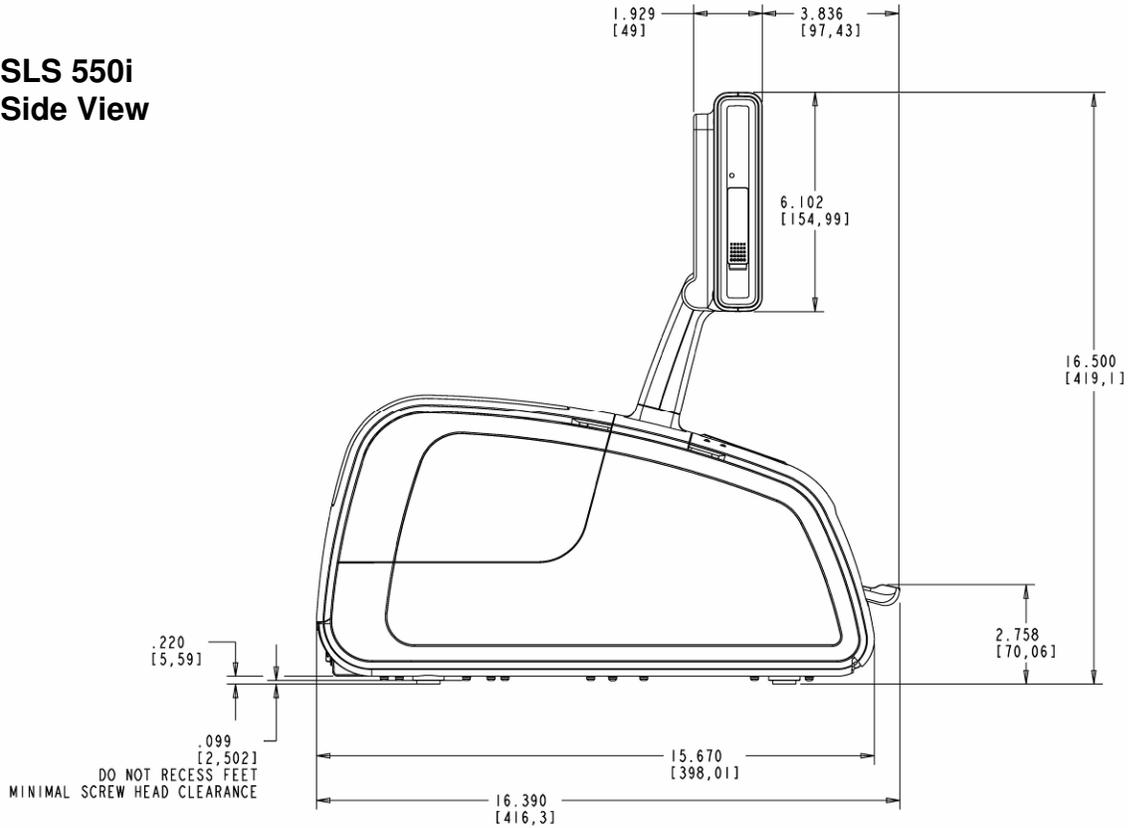
TCP and UDP:

Target Port	T C P	U D P	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.

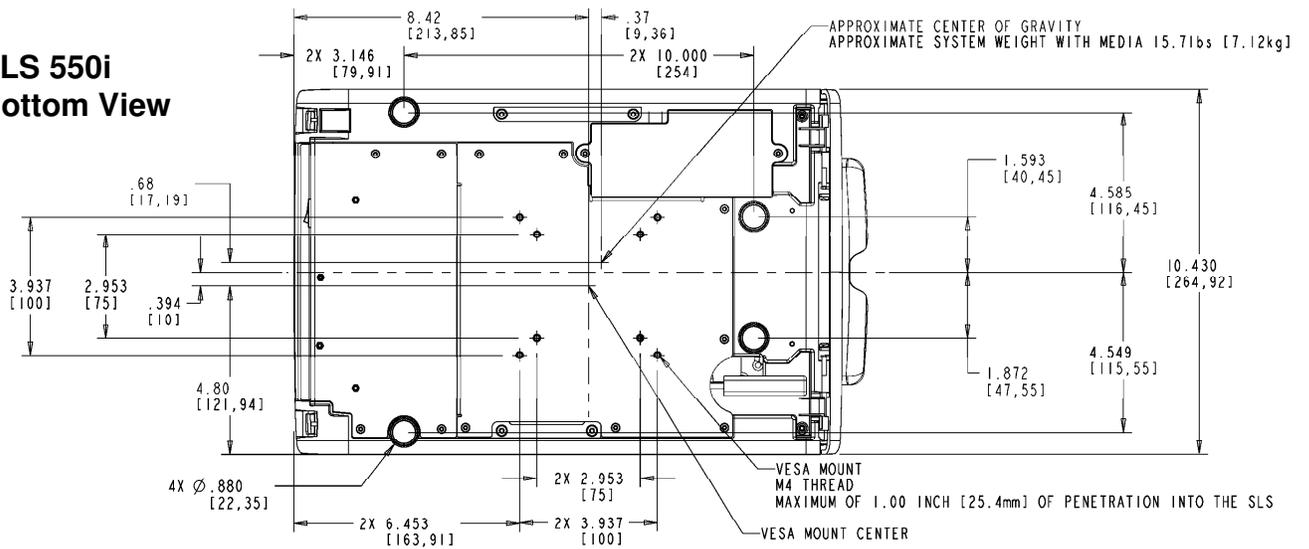
Appendix C – Mechanical Drawings

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 550i
Side View**



**SLS 550i
Bottom View**



Appendix D – Confidential Addendum Request Procedure

Some information related to the design, architecture and software of the Safe Label System is confidential and only provided under Non-Disclosure Agreement (NDA). A separate document called the Confidential Addendum to the IT Resource Guide for Codonics Safe Label System is available with this information.

Use the following instructions to request the Confidential Addendum:

1. Contact Codonics Technical Support.
 - Email: support@codonics.com
 - Phone: 800.444.1198 Fax: 440.243.1334 (mark with attention: Tech Support)
 - Hours: 8:30 AM-5:30 PM ET, Mon-Fri (Closed official U.S. Holidays).
2. Request Document Number: 900-880-001, Confidential Addendum to the IT Resource Guide for Codonics Safe Label System, Software Release 3.0.x.
3. Codonics will send back instructions with the NDA form.
4. Fill in and sign the NDA form.
5. Return the completed NDA form to Codonics using the instructions provided with the form.
6. Codonics will send the Confidential Addendum.

Disclaimer: Codonics reserves the right to release the Confidential Addendum on a case-by-case basis. The information contained in the Confidential Addendum is limited to that which Codonics chooses to release to assist customers with evaluating, purchasing or installing the Safe Label System.

Appendix E – Security Recommendation and Best Practices

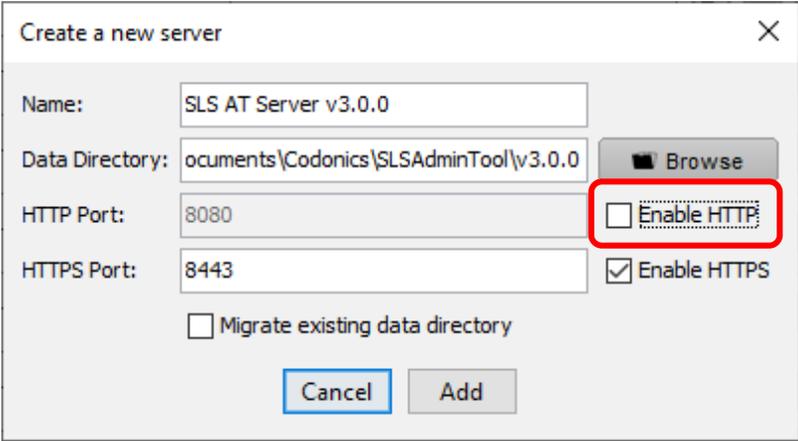
This section contains information to improve the overall network security of SLS components connected to a customer’s LAN network.

1. SLS Administration Tool (SLS AT) Server Setup Changes

a. Disable HTTP.

- i. Open AT Server Manager.
- ii. Click Add.
- iii. Uncheck “Enable HTTP”.

The default SLS AT configuration enables both HTTP (TCP port 8080) and HTTPS (TCP port 8443) for client browser connections. Refer to the SLS AT Server Manager menu and use the following dialog box to uncheck the Enable HTTP setting. Restart the SLS AT Server after changing this setting.



The screenshot shows a dialog box titled "Create a new server" with a close button (X) in the top right corner. It contains the following fields and controls:

- Name:** SLS AT Server v3.0.0
- Data Directory:** documents\Codonics\SLSAdminTool\v3.0.0, with a "Browse" button to its right.
- HTTP Port:** 8080
- HTTPS Port:** 8443
- Enable HTTP:** An unchecked checkbox, which is highlighted with a red rectangular box.
- Enable HTTPS:** A checked checkbox.
- Migrate existing data directory:** An unchecked checkbox.
- Buttons:** "Cancel" and "Add" buttons at the bottom.

b. Install a site-provided SSL certificate for HTTPS.

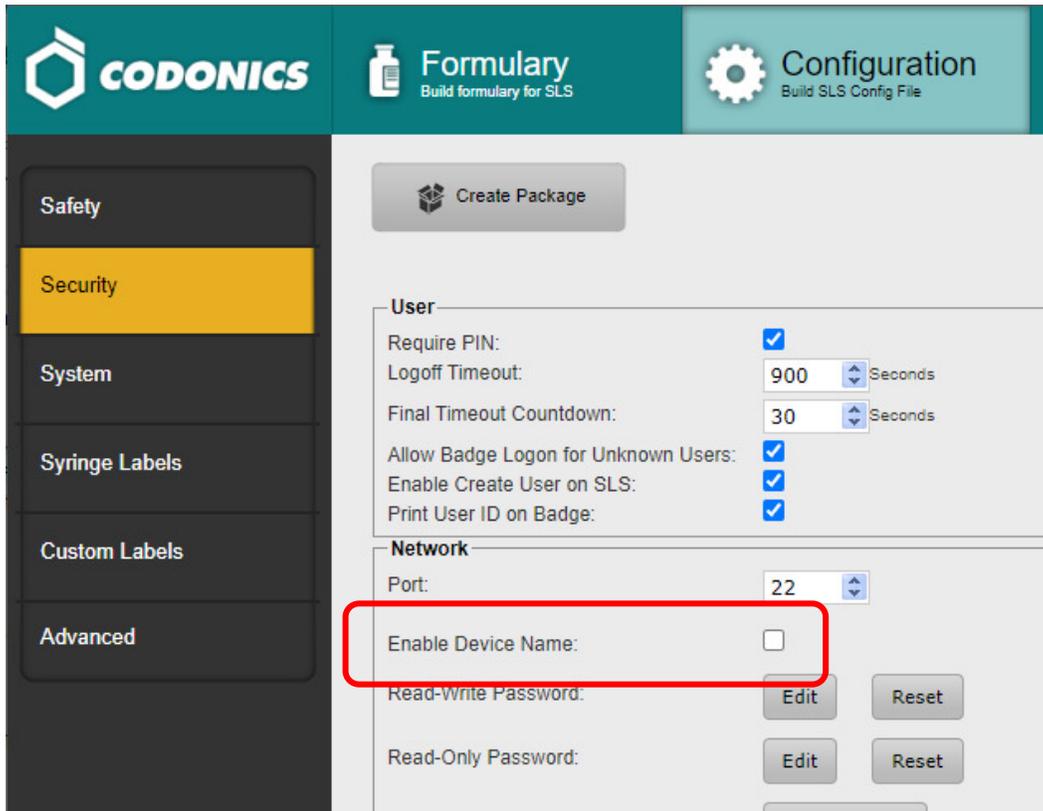
The default HTTPS configuration includes a self-signed SSL certificate provided by Codonics. The site administrator should install their own certificate. This can be a self-signed certificate which has been added to the list of trusted root certificates on a domain, or a certificate signed by a trusted 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.

2. SLS AT Configuration Changes

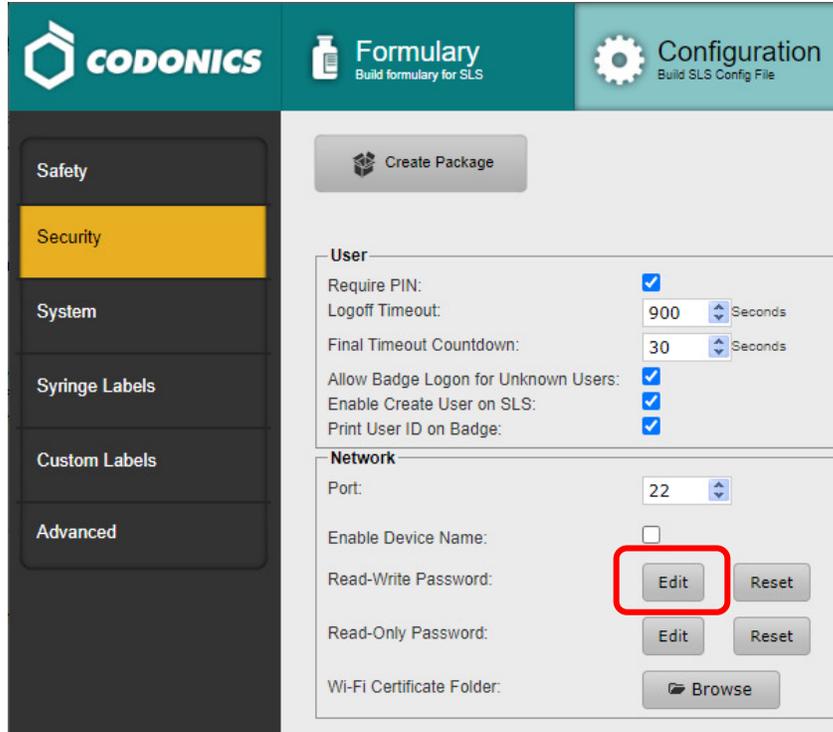
a. Disable NetBIOS (“Device Name” in AT config package security settings).

- i. Log in to the Administration Tool.
- ii. Navigate to the Configuration Page.
- iii. Select the “Security” tab on the left side.

- iv. Uncheck “Enable Device Name” under the “Network” section.



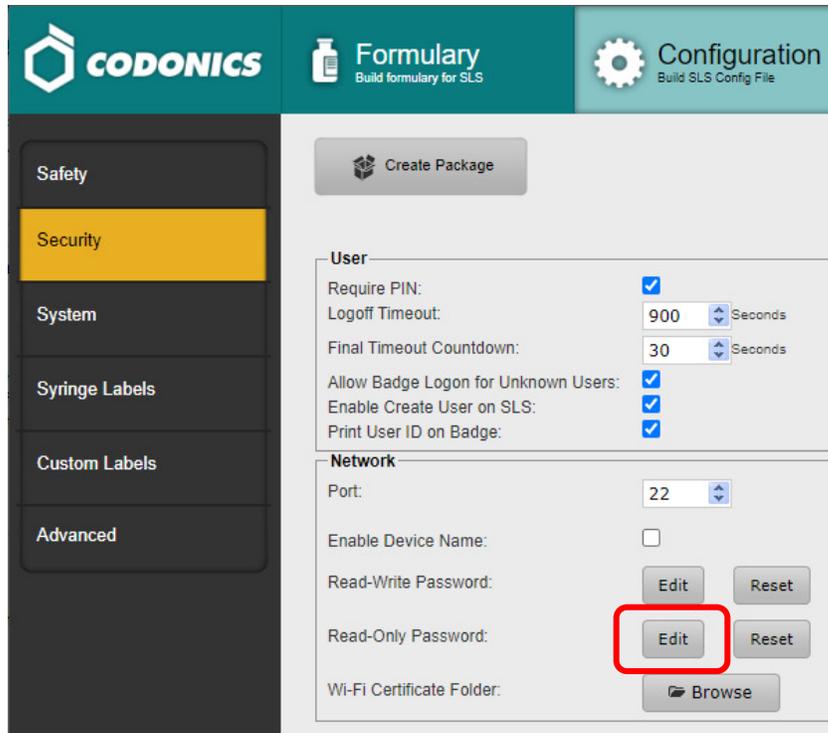
- b. Change from default password for both SNET (SSH) accounts (net-admin and net-readonly) to site assigned passwords.
 - i. Log in to the Administration Tool.
 - ii. Navigate to the Configuration page.
 - iii. Select the “Security” tab on the left side.
 - iv. Click “Edit” for the Read-Write Password.



- v. Enter the new password and a hint, then click Save.



- vi. Click "Edit" for the Read-Only Password.



vii. Enter the new password and a hint, then click Save.

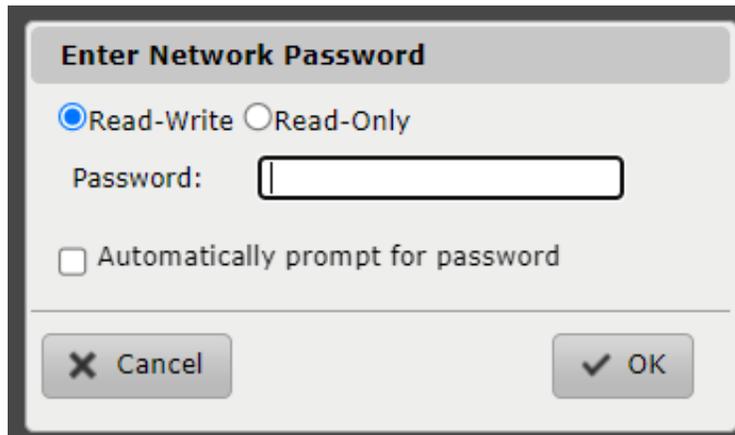


viii. Create a Configuration package with the setting(s) enabled and install on SLS(s) for any of the above changes.

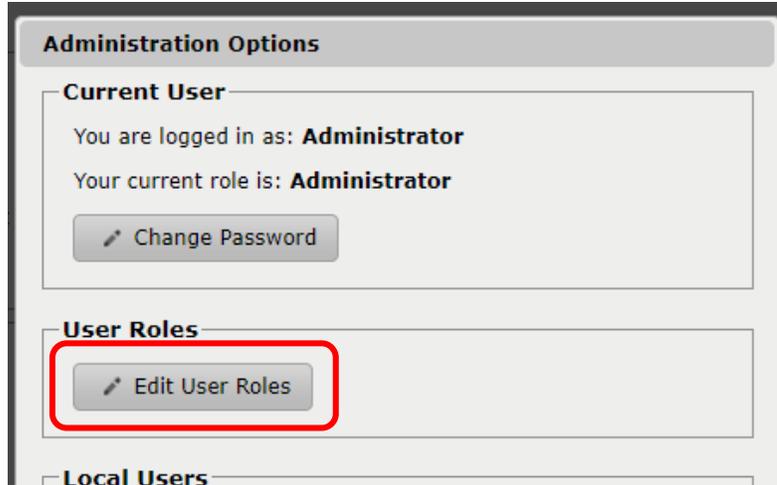
3. SLS AT Device Management Changes
 - i. Navigate to the Devices page.
 - ii. Click “Enter Network Password”.



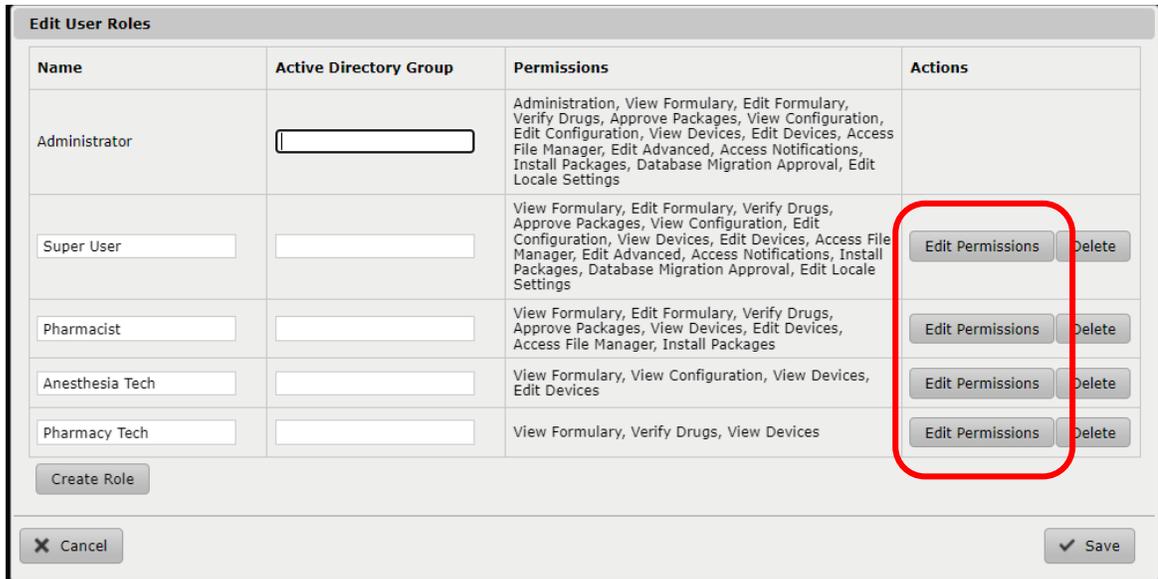
- iii. Enter the changed password(s) to maintain a connection to SLS units in your device list.



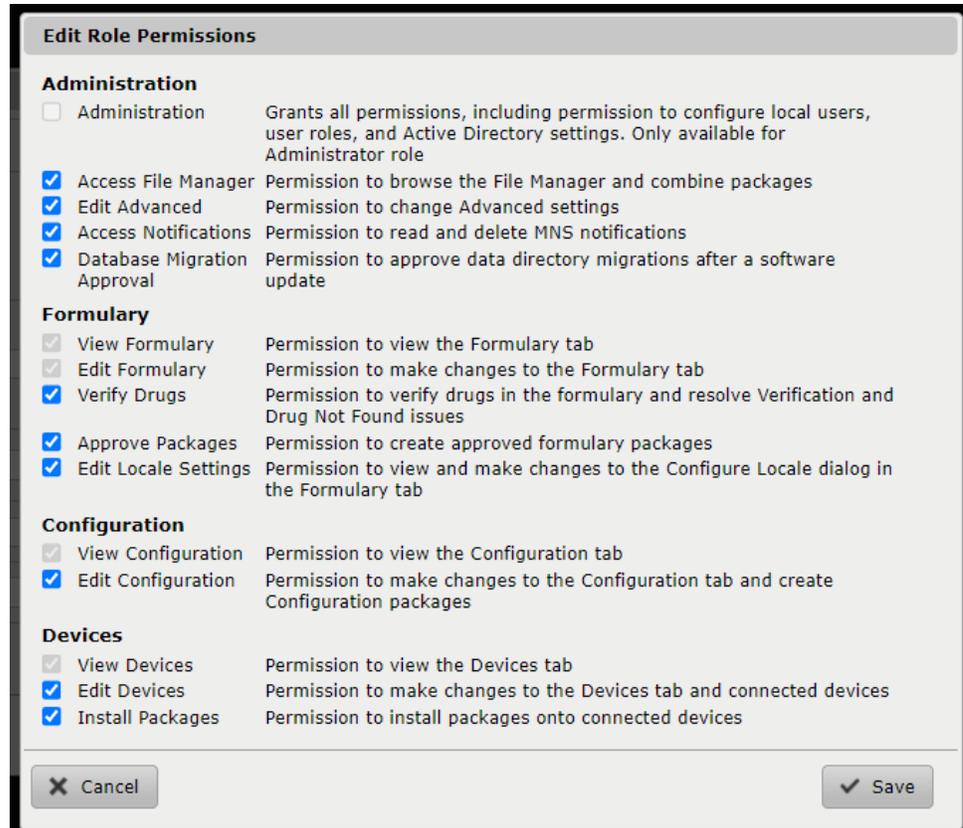
4. SLS AT Administrator Capabilities
 - a. Implement AT User Roles to limit user access (principle of least privilege).
 - i. Log in to the Administration Tool as the Administrator user.
 - ii. Click the “Administrator” link in the upper right of the AT.
 - iii. Click “Edit User Roles”.



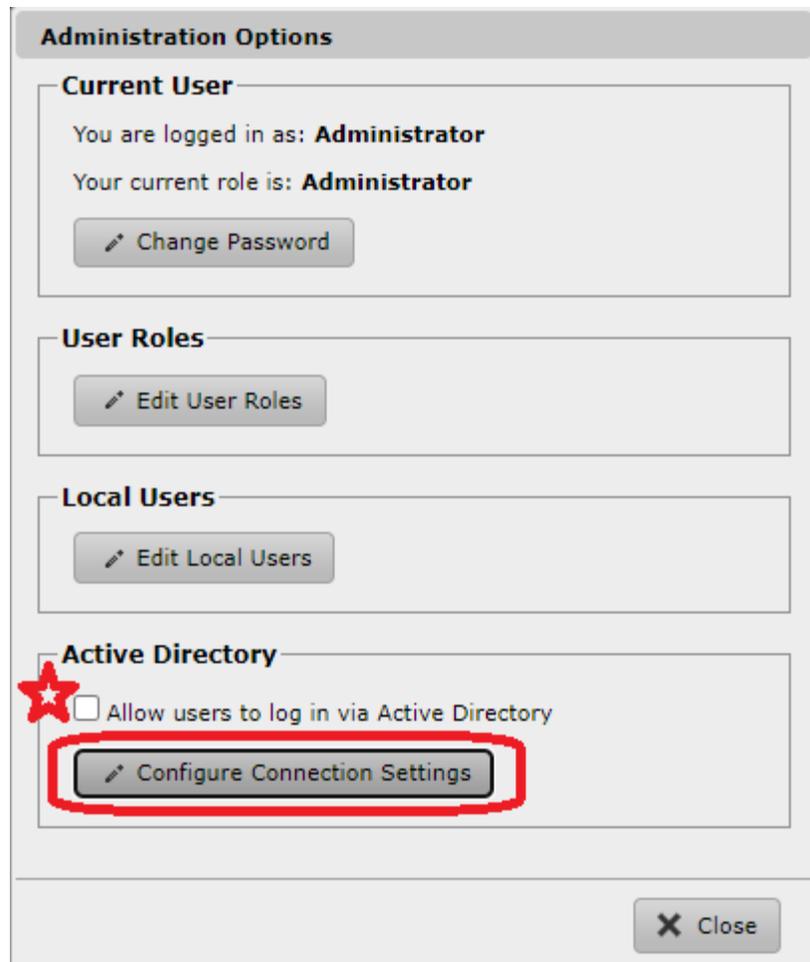
iv. Click “Edit Permissions” for the group you wish to edit permissions.



v. Check/Uncheck the permissions you wish to change.



- b. Use SSL for Active Directory AT login, if available.
 - i. Log in to the Administration Tool as the Administrator user.
 - ii. Click the “Administrator” link in the upper right of the AT.
 - iii. Check the box “Allow users to log in via Active Directory”.
 - iv. Click “Configure Connection Settings” under the Active Directory section.



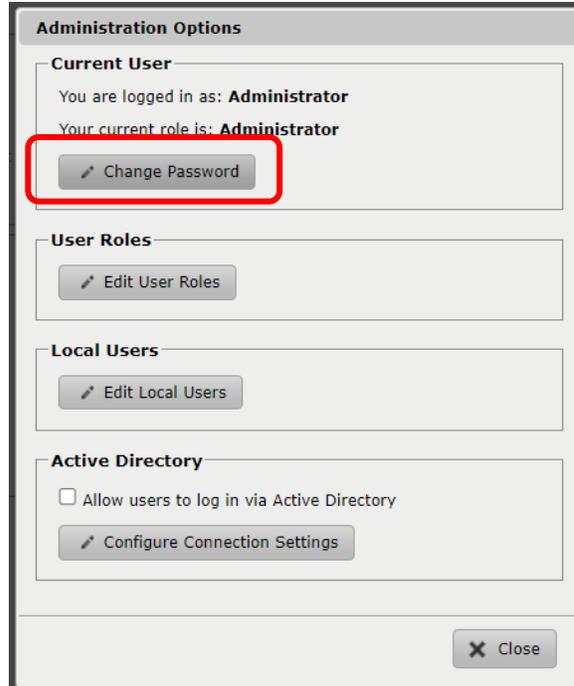
- v. Enter the AD settings into the “Configure Active Directory Settings” dialog. Check “Use SSL” and change the Port setting to the appropriate SSL port (636 is typical).

Configure Active Directory Settings	
Server Address	<input type="text"/>
Port	<input type="text"/>
Use SSL	<input type="checkbox"/> 
Authentication Method	UPN (e.g. JDoe@n1.hospital.org) ▼
Domain	<input type="text"/>
Search Base	<input type="text"/>
Group Search Base	<input type="text"/>

Buttons:

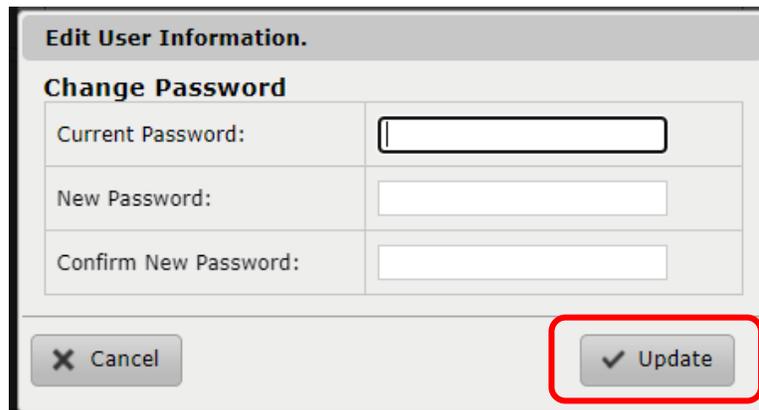
- c. Use an anti-virus or other endpoint security package on the Windows® system hosting the SLS AT.
- d. Keep current with Windows security updates on the system hosting the SLS AT.
- e. Change from default password for local AT Administrator account.
 - i. Log in to the Administration Tool as the Administrator user.
 - ii. Click the “Administrator” link in the upper right of the AT.
 - iii. Click “Change Password” for the current user in the “Administrator Options” dialog.

Codonics Safe Label System: IT Resource Guide



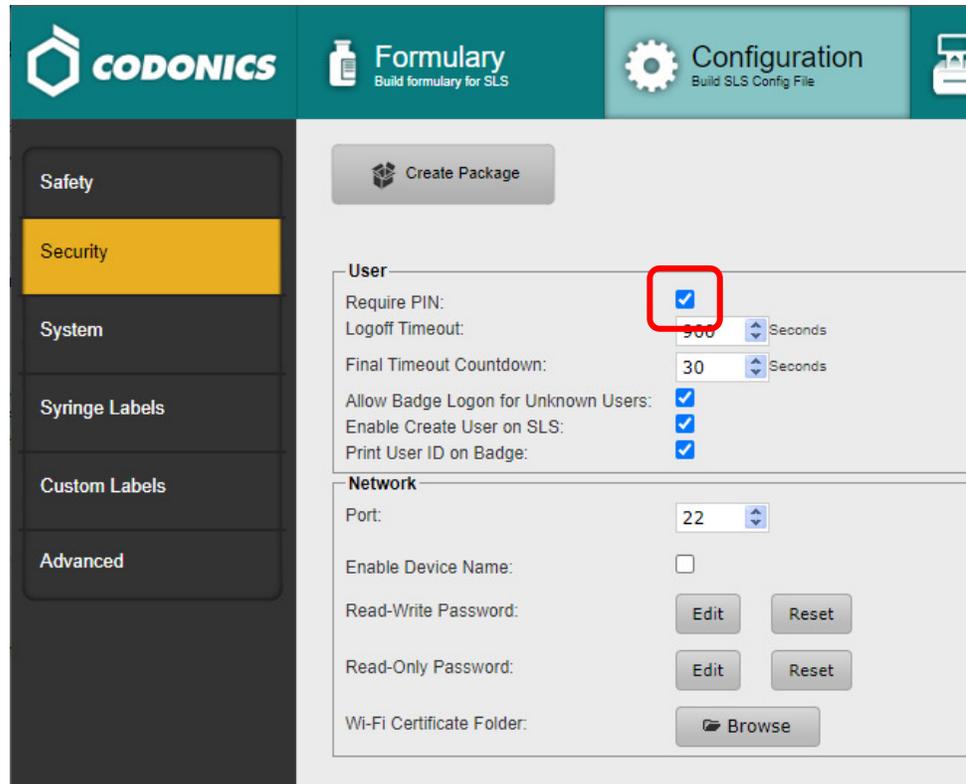
The image shows a dialog box titled "Administration Options". It contains four sections: "Current User", "User Roles", "Local Users", and "Active Directory". The "Current User" section shows "You are logged in as: Administrator" and "Your current role is: Administrator". A red box highlights the "Change Password" button. The "User Roles" section has an "Edit User Roles" button. The "Local Users" section has an "Edit Local Users" button. The "Active Directory" section has a checkbox for "Allow users to log in via Active Directory" and a "Configure Connection Settings" button. A "Close" button is at the bottom right.

- iv. Enter the current password, and the new password, then click “Update”.

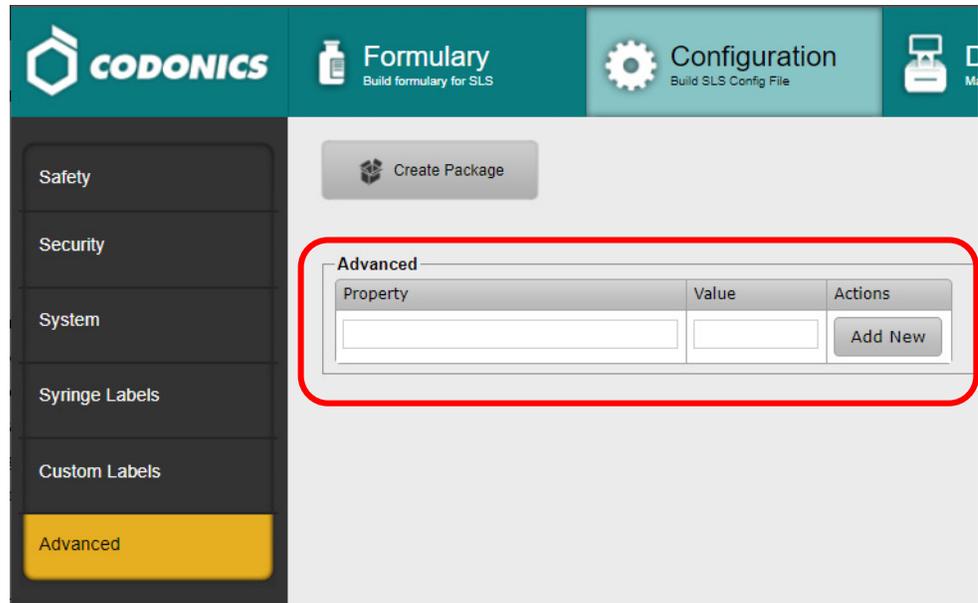


The image shows a dialog box titled "Edit User Information." with a sub-section "Change Password". It contains three input fields: "Current Password:", "New Password:", and "Confirm New Password:". A red box highlights the "Update" button at the bottom right. A "Cancel" button is at the bottom left.

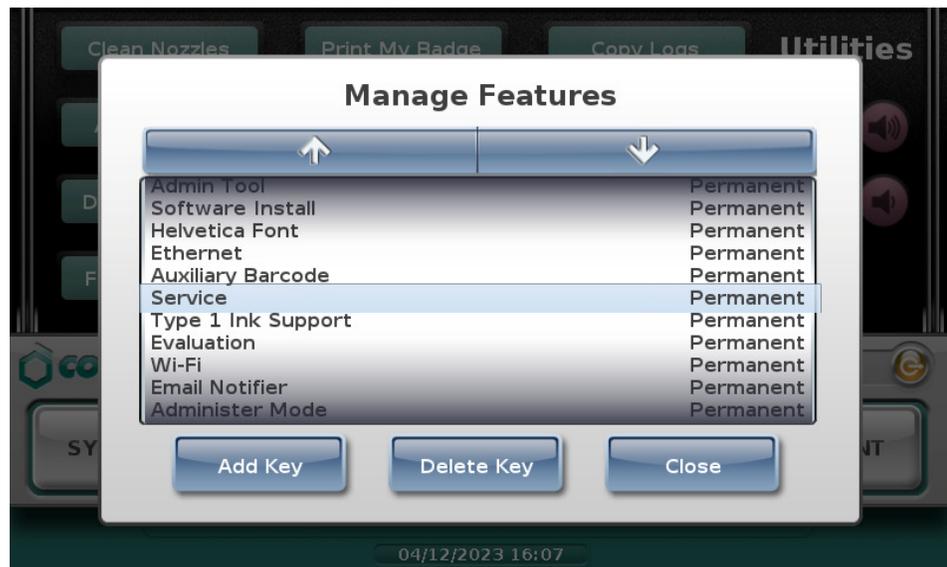
5. SLS Point of Care Stations, Model 500i, 550i (SLS PCS) Changes via the SLS AT
 - a. Require PIN for SLS login.
 - i. Log in to the Administration Tool.
 - ii. Navigate to the Configuration Page.
 - iii. Select the “Security” tab on the left side.
 - iv. Check the “Require PIN” option (this is checked by default).



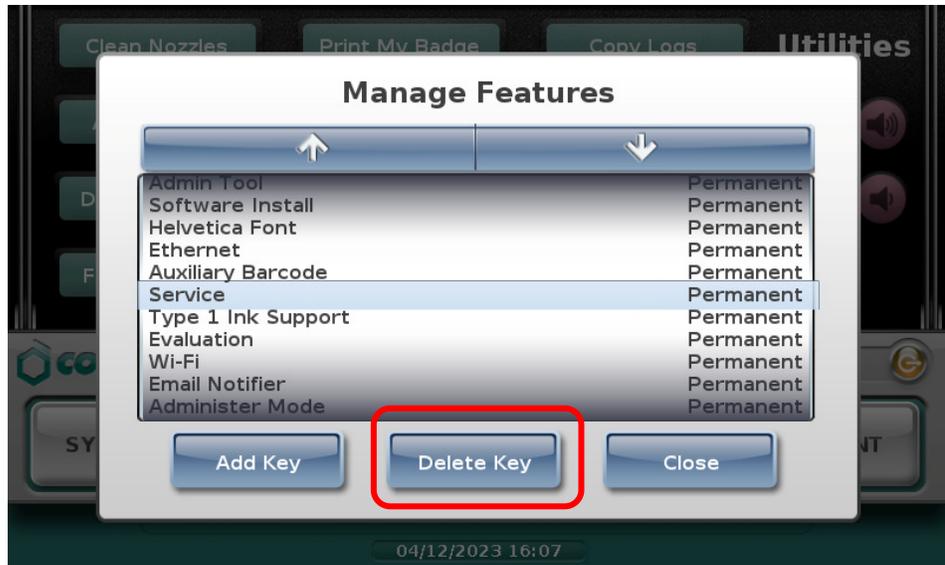
- v. Create an install a Configuration package with the setting enabled.
- b. If using Wi-Fi, choose EAP-TLS or PEAP for Wi-Fi network authentication if possible.
- 6. Other options for improved security, but are generally more difficult to implement:
 - a. Disable Diffie-Hellman SSH key exchange (requires Engineering to provide code for Advanced Configuration).
 - i. Log in to the Administration Tool.
 - ii. Navigate to the Configuration Page.
 - iii. Select the “Advanced” tab on the left side.
 - iv. Enter the property and value provided by Codonics Engineering.



- v. Create an install a Configuration package with the setting.
- b. Disable Service Shell.
 - i. Log in to the SLS unit.
 - ii. Click the wrench icon to open the Utilities Menu.
 - iii. Click “Manage Features”.
 - iv. Scroll to select the “Service” key.



- v. Delete the “Service” key.



Appendix F – SLS Software Update Policy and Process

The Codonics Safe Label System (“SLS”) is an FDA listed class 2 medical device. SLS components include the SLS Administration Tool (“SLS AT”)- a Windows® application for managing the SLS drug formulary and configuration settings, SLS Point of Care Stations (“SLS PCS”)- models SLS 500i and SLS 550i, SLS Email Notifier (“SLS EN”)- an optional SLS software application to generate email notifications regarding system status, and the SLS Data Analytics Tool (“SLS DAT”)- an optional software package that allows for analysis of SLS drugs prepared by the SLS system.

Each of the SLS components incorporate upgradeable software as a part of their design. Codonics, as the manufacturer of these medical devices, is the only authorized source of software updates to ensure continued safe and effective operation of the devices. This section describes the process for customers to receive and install SLS software updates.

SLS Software Update Policy

Codonics currently provides SLS software updates free of charge to the original SLS purchaser or current Codonics authorized medical establishment that owns the SLS system. Codonics currently provides phone, email and video conference technical support free of charge to SLS customers for the installation of software updates during normal Codonics business hours. Onsite support or support requests deemed unusual or outside normal support services will be reviewed and quoted on a case-by-case basis at Codonics’ discretion.

Codonics performs ongoing monitoring of the SLS solution for software vulnerabilities and other product improvements. Regular software updates that include cyber-security patches are released at least once per calendar year. If a significant software vulnerability is discovered between scheduled releases, Codonics will assess the risk posed and release either documentation addressing the specific concerns including instructions to mitigate the vulnerability or a software update as required.

Customer Notification of Software Updates

Customers can receive notification of SLS software updates the following ways:

1. By checking www.codonics.com/notices for current information about the Safe Label System. Information about SLS software updates can be found under “AT/SLS Software Release Notes”.

Note: Users can lookup SLS product lifecycle information that includes the support status of current and previous software versions using the same URL. The information is in the document “SLS Product Lifecycle Status”.

2. By enabling the SLS AT Message Notification Service (“MNS”) that periodically checks a Codonics server for SLS product information including software updates and displays the notifications in the SLS AT application.
3. By contacting Codonics Technical Support (see contact information at beginning of this document.)

4. By receiving a pro-active email or phone call from Codonics that an urgent issue has been identified that requires customer action.

Distribution of Software Updates

Customers must contact Codonics Technical Support to receive software updates (see contact information at the beginning of this document.) Software updates are typically distributed in three files: one for the SLS AT (includes the SLS EN), a second for SLS PCS and a third for the SLS Data Analytics Tool that is optional and allows for analysis of SLS drug preparation data at the site. These files can be downloaded by the customer from a Codonics server using a link provided by Codonics or shipped to the customer on a USB drive. The SLS AT and SLS PCS devices cannot automatically download or install software updates. User interaction is required.

Installation of Software Updates

Codonics recommends that all SLS software updates be performed with the assistance of Codonics Technical Support. This will ensure proper migration of existing drug formularies, device configuration settings and minimize downtime of the SLS system. Codonics has a designated upgrade coordination staff that work with customers to ensure hardware requirements are met for the software updates and data migration issues are properly handled prior to deploying software updates onto SLS devices. Software updates can take from a few days to a few weeks to perform depending on the number of devices being updated, the number of formularies to migrate, the number of software versions being advanced by the software update and whether an upgrade is required for the Windows computer running the SLS AT and/or SLS EN.

Software Updates of non-SLS Components

The customer is responsible for all updates to non-SLS components used by the SLS system. This includes the Windows® Operating System on the server hosting the SLS AT and/or SLS EN, and any anti-virus or anti-malware software on the Windows system.

SLS Software Update Compatibility Issues

SLS PCS- Codonics provides a minimum of five (5) years of software updates for new SLS PCS devices from the date of original shipment from the Codonics factory. Some older SLS PCS devices may not support current software updates. Generally, the SLS AT and SLS PCS devices must be at the same software version to operate properly. SLS PCS devices that are not compatible with the software version distributed in the software update will not operate with other components in the SLS system that have been updated. Contact Codonics sales staff for more information regarding replacement of older SLS PCS devices.

SLS AT and SLS EN- The minimum hardware and operating system requirements for the customer supplied Windows Server hosting the SLS AT and SLS EN change periodically. SLS software updates may require an upgrade of the Windows Server hardware or Windows Operating System to ensure proper operation of the SLS AT and SLS EN.

Disclaimer: Codonics reserves the right to change the Safe Label System Software Update Policy and Process at any time.