Administration Tool Server & Server Manager

Technical Brief

Overview

- Version 1.9.0 and newer software for Codonics Safe Label System® (SLS) includes support for installing the Administration Tool (AT) as a server. Version 2.5.0 and newer includes support for the AT Server Manager.
- The AT Server application provides all the same capabilities as the existing AT Stand-alone application. As of 2.5.0, this application is no longer supported.
- AT Server uses a web browser without the need to install software on a local PC. The web-based access allows it to be used from many different locations, not just a single PC.

Recommended - Requirements for AT Server:

Processor: Xeon W-2135 @ 3.70GHz, Core i7-7700 @ 3.60GHz or faster. Four (4) cores.

RAM: 8 GB free space for application.

Application Disk Space: 30 GB total at install.

Minimum - Requirements for AT Server:

Processor: Xeon X5660 @ 2.80 GHz, Core i7-2600 @ 3.40GHz or faster. Four (4) cores.

RAM: 6 GB free space for application.

Application Disk Space: 10 GB total.

Additional Information for AT Server:

Computer OS: Windows® 10, Windows Server 2012R2, 2016 and 2019. 64-bit required.

Concurrent access: Not supported

Notes:

- For best performance hosting the SLS AT data directory, use a locally attached SSD or high speed RAID.
- When running the SLS AT on a VM, allocate at least two CPU cores to the VM.
- 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.
- Both configurations shown are sufficient for running the SLS Email Notifier (EN) on the same system hosting the SLS AT.

Recommended requirements for AT Client:

Browser support: Internet Explorer IE 11 or newer, Edge, Chrome

Screen Resolution: Minimum 1440 x 900; use default browser fonts

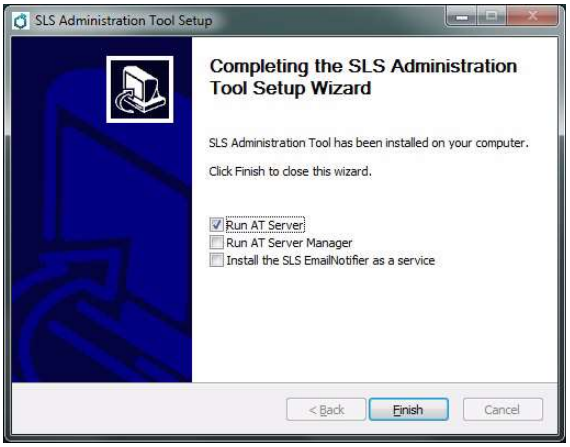
Computer OS: Windows 10 or newer

Applications: Excel 2003 or greater to open reports

AT Server

Installation

- To run the AT Server, follow the instructions in the SLS AT User's Manual for AT installation except, at the end of the process, select Run AT Server and Finish.



SLS Administration Tool Setup

Completing the SLS Administration Tool Setup Wizard

SLS Administration Tool has been installed on your computer.

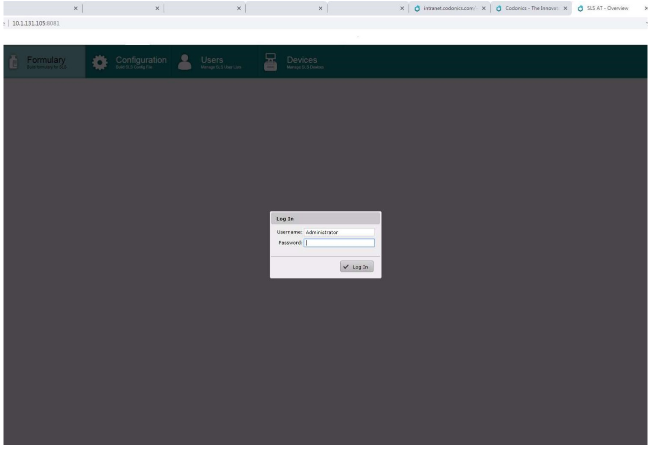
Click Finish to close this wizard.

☑ Run AT Server
☐ Run AT Server Manager
☐ Install the SLS EmailNotifier as a service

Note: Before starting installation, you should make sure there is a recent backup of the AT Data Directory. Contact Codonics Technical Support if help is required for creating a backup.

WARNING: All instances of the AT must be closed before migrating data either during installation or later using the migration utility. In addition, AT services running an AT Server being migrated from one version of the AT Server to another version (e.g., 2.5.0 to 2.6.0) have to be stopped. Refer to Technical Brief 901-253-018 for further instructions on formulary migration.

- The AT Server will start and the Login screen will appear.



10.1.131.105:8081

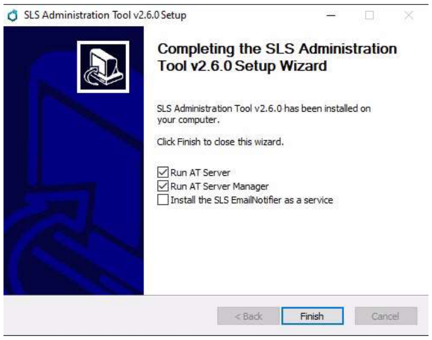
Log In

Username: Administrator

Password:

AT Server Manager

- If you would like to run the AT Server and setup multiple ATs as servers (e.g., for different formularies), at the end of the AT installation process check both the Run AT Server and Run AT Server Manager. When you click Finish, the AT Server Manager will automatically start..



Completing the SLS Administration Tool v2.6.0 Setup Wizard

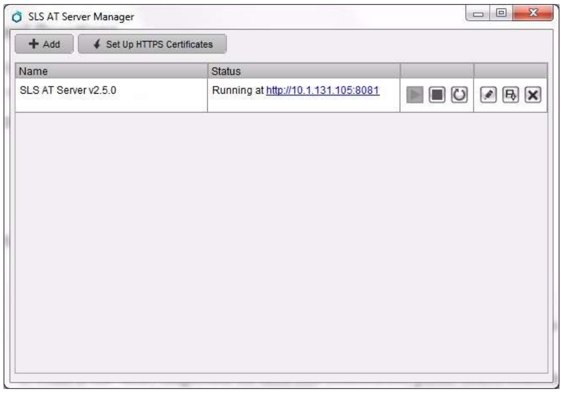
SLS Administration Tool v2.6.0 has been installed on your computer.

Click Finish to close this wizard.

☑ Run AT Server
☑ Run AT Server Manager
☐ Install the SLS EmailNotifier as a service

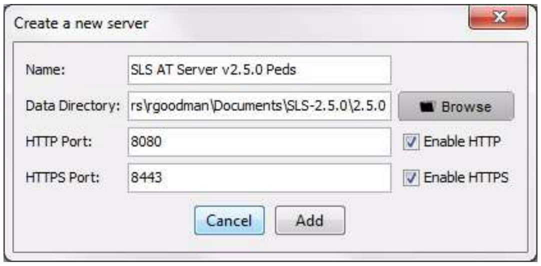
> **Note:** The default AT Data Directory location will be used when installing the AT. To change the default location, refer to editing the Data Directory path in the Additional Actions in the AT Server Manager section.

> **Note:** Previous versions (e.g., 2.3.0, 2.4.0) of an AT service will be added automatically to the AT Server Manager. The Name will be ATServer. Contact Codonics Technical Support with any questions.



Name	Status
SLS AT Server v2.5.0	Running at http://10.1.131.105:8081

- You can add additional AT servers by selecting +Add. A new dialog box (i.e., Create a new server) will open allowing you to edit the information shown (i.e. Name, Data Directory path, HTTP and HTTPS Port). After entering the information, select Add.



Name: SLS AT Server v2.5.0 Peds

Data Directory: rs\rgoodman\Documents\SLS-2.5.0\2.5.0

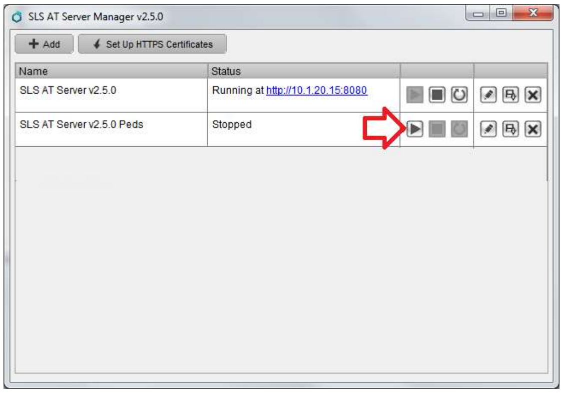
HTTP Port: 8080 ☑ Enable HTTP

HTTPS Port: 8443 ☑ Enable HTTPS

> **Note:** If a port is already in use by another non-AT service, the added AT service will not start-up and a warning will be displayed indicating that the port is already in use.

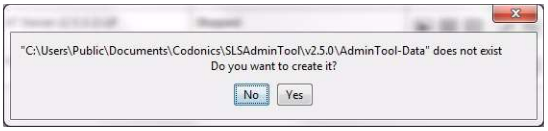
> **Note:** The default HTTP Port is 8080. If the default port is already in use by an existing AT service when installing 2.5.0, the server manager will automatically increment the port by 1 until an available port is found. For example, if a user is upgrading from 2.4.0 to 2.5.0 and has a service on their system using port 8080 already, when installing 2.5.0 the new service will be installed at port 8081. To change the default, see Additional Actions in the AT Server Manager section.

- The new AT Server (i.e., SLS AT Server v2.5.0 Peds) will appear in the SLS AT Server Manager. Click the start arrow.

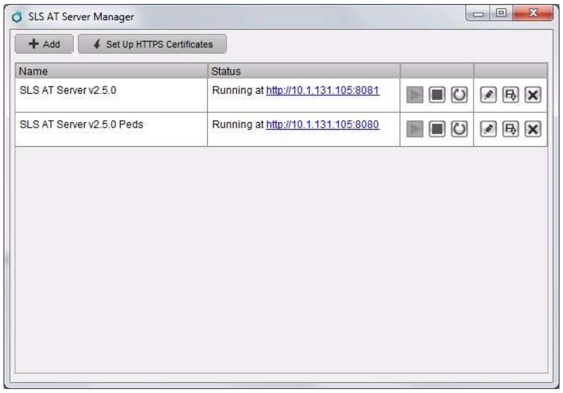


Name	Status
SLS AT Server v2.5.0	Running at http://10.1.20.15:8080
SLS AT Server v2.5.0 Peds	Stopped

- You will be asked if you want to create a new Data Directory in the location defined previously. Click Yes.

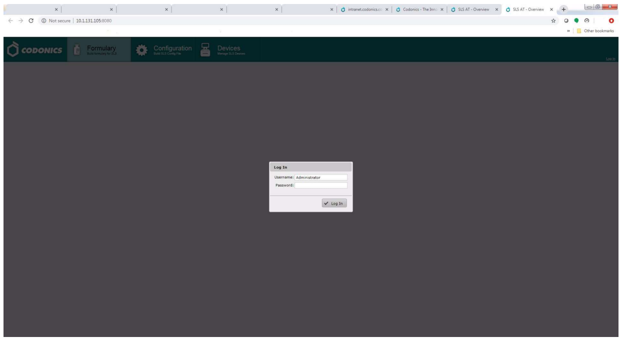

"C:\Users\Public\Documents\Codonics\SLSAdminTool\v2.5.0\AdminTool-Data" does not exist
Do you want to create it?

- A new Data Directory is created, the additional AT Server (i.e., SLS AT Server 2.5.0 Peds) will start running and will be displayed in the SLS AT Server Manager.



Name	Status
SLS AT Server v2.5.0	Running at http://10.1.131.105:8081
SLS AT Server v2.5.0 Peds	Running at http://10.1.131.105:8080

- Clicking on the IP address link in the Status field, will automatically open up a browser window that will display the AT and the Login Screen.

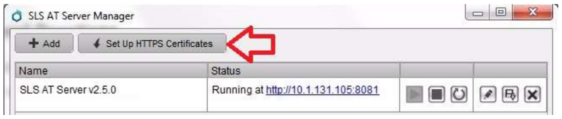

Not secure | 10.1.131.105:8080
Log In
Username: Administrator
Password:

Support for HTTPS Certificates

- HTTPS capability is provided for secure encrypted data transfer over the network.

> **Note:** The default HTTPS Port is 8443. If the default port is already in use by an existing AT service when installing 2.5.0, the server manager will automatically increment the port by 1 until an available port is found. For example, if a user is upgrading from 2.4.0 to 2.5.0 and has a service on their system using port 8443 already, when installing 2.5.0 the new service will be installed at port 8444. To change the default, see Additional Actions in the AT Server Manager section.

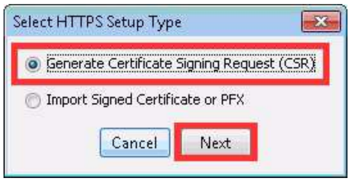
- If you want to add HTTPS Certificates, select Set Up HTTPS certificates as shown.



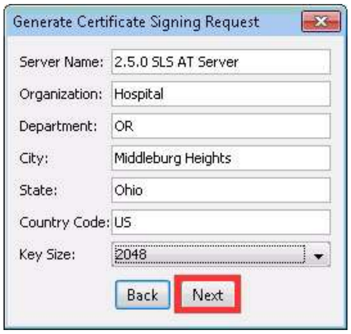
Name	Status
SLS AT Server v2.5.0	Running at http://10.1.131.105:8081

Generate Certificate Signing Request (CSR)

- A new dialog box will be displayed and allow you to setup CSR certificates. Click on Generate Certificate Signing Request (CSR). Select Next.


Select HTTPS Setup Type
● Generate Certificate Signing Request (CSR)
○ Import Signed Certificate or PFX

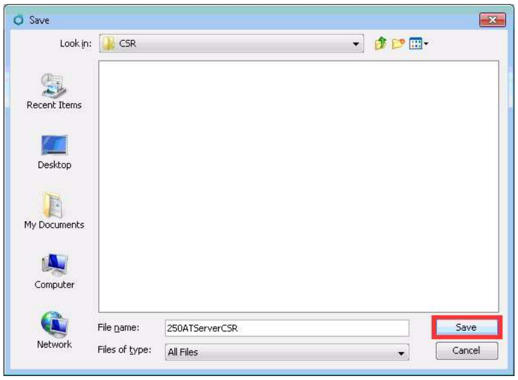
- A new dialog will be displayed to Generate a CSR. Fill in the information and select Next.


Generate Certificate Signing Request

Server Name: 2.5.0 SLS AT Server
Organization: Hospital
Department: OR
City: Middleburg Heights
State: Ohio
Country Code: US
Key Size: 2048

> **Note:** The Key Size has a dropdown with options of 2048, 3072 and 4096.

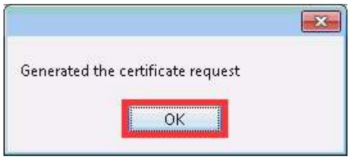
- Save the CSR.



File name: 250ATServerCSR

Files of type: All Files

- You are informed the CSR is being generated and again when it is generated. Select OK.



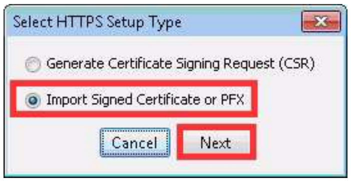
Generated the certificate request

- You will now have a .csr file located where you indicated it would be saved. You can now use it to generate signed certificates that can be imported into the AT Server Manager using the following workflow.

Warning: Generating a new CSR or importing certificates will invalidate existing certificates that are setup. Whenever the AT Server Manager changes (e.g., upgrades), you will need to update the certificate.You only need to set-up one certificate for the AT Server Manager; not one certificate per service.

Import Signed Certificate or PFX

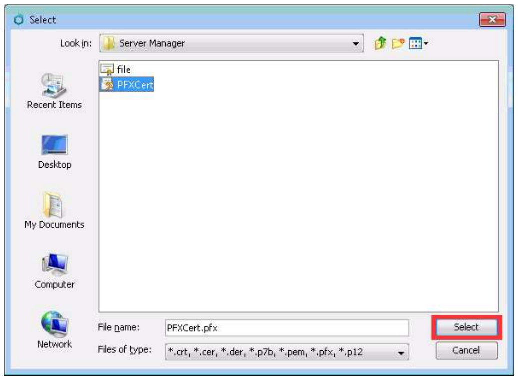
- Select Import Signed Certificate or PFX and then Next.



○ Generate Certificate Signing Request (CSR)

● Import Signed Certificate or PFX

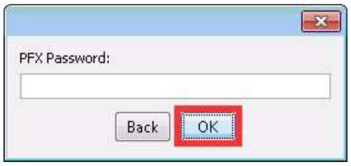
- You should now browse to and select the file that will be imported. The file should be of the following formats: .crt,. cer, .der, .p7b, .pem, .pfx or .p12. These options are also defaulted in the Files of Type filter.



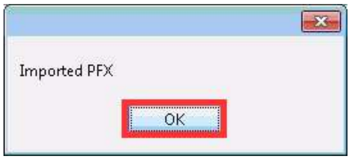
File name: PFXCert.pfx

Files of type: *.crt, *.cer, *.der, *.p7b, *.pem, *.pfx, *.p12

Note: If the certificate is a .pfx or .p12, a password is required and you will be prompted to enter the password. Select OK.



- You are informed the certificate is being imported and again when it is imported.



Imported PFX

- The AT Server Manager now has the certificate imported. In order for the changes to take effect, you will need to restart the AT Services.

Note: HTTPS certificates added to the AT Server Manager will secure new AT services as of 2.5.0. If you start additional 2.5.0 AT services after the initial install, the certificates will cover the new AT services. However, if there were previous services running, for example with 2.4.0 AT, separate HTTPS certificates will need to be created and installed for the 2.4.0 AT. Contact Codonics Technical Support for assistance.

Setting up HTTPS for a local computer

If you are using Chrome or Internet Explorer (IE) browsers:

1. Copy the file codonics.crt to the computer that will be accessing the AT Server.
2. Double-click the certificate and click Install Certificate...

3. Follow the wizard and browse to install the certificate to Trusted Root Certification Authorities.

4. Open Chrome or IE browsers and navigate to the HTTPS address for the server.

5. Verify that no warning is displayed to the user and the address bar will indicate HTTPS://IP_Address:port.

6. Refer to the Operation section of this Technical Brief for AT Server operation.

If you are using FireFox browser:

> **Note:** By default FireFox does not accept self-signed certificates. The following steps define how to setup FireFox with self-signed certificates:

1. Follow steps 1 through 3 in the Chrome setup instructions above. After completing step 3 in the Chrome instructions, open the Firefox browser.

2. Navigate to about:config.

3. Search for security.enterprise_roots.enabled.

4. Double-click the setting to set the value to true.

5. Open the Firefox browser and navigate to the HTTPS address for the server.

6. Verify that no warning is displayed to the user and the address bar will indicate HTTPS://IP_Address:port.

7. Refer to the Operation section of this Technical Brief for AT Server operation.

If you are using Safari browser:

> **Note:** By default Safari does not accept self-signed certificates. The following steps define how to setup Safari with self-signed certificates:

1. Follow steps 1 through 3 in the Chrome setup instructions above.

2. After completing step 3 in Chrome instructions, install the certificate to System on the Mac system.

3. Open Keychain Access.

4. Double-click the certificate to open it.

5. Expand the Trust section.

6. Set Secure Sockets Layer (SSL) to Always Trust for this certificate.

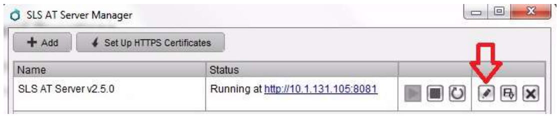
7. Open the Safari browser and navigate to the HTTPS address for the server.

8. Verify that no warning is displayed to the user and the address bar will indicate HTTPS://IP_Address:port.

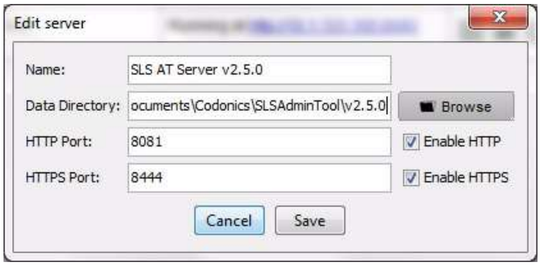
9. Refer to the Operation section of this Technical Brief for AT Server operation.

Additional Actions in the AT Server Manager

- If you need to edit an existing server, select the edit icon and a dialog box will open allowing you to edit the information shown (i.e. Name, Data Directory path, HTTP and HTTPS Port).



Name	Status
SLS AT Server v2.5.0	Running at http://10.1.131.105:8081



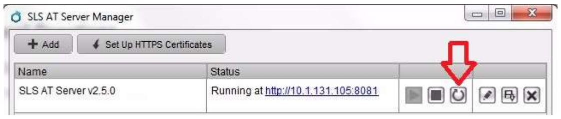
Name: SLS AT Server v2.5.0

Data Directory: ocuments\Codonics\SLSAdminTool\v2.5.0

HTTP Port: 8081 ☑ Enable HTTP

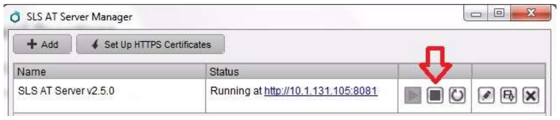
HTTPS Port: 8444 ☑ Enable HTTPS

- Once you make edits, you need to restart the service by selecting the circular arrow shown for the new values to take effect.



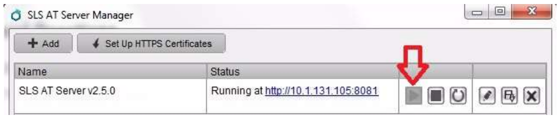
Name	Status
SLS AT Server v2.5.0	Running at http://10.1.131.105:8081

- To stop the service, select the square icon as shown.



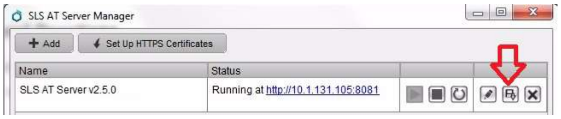
Name	Status
SLS AT Server v2.5.0	Running at http://10.1.131.105:8081

- To start the service, select the arrow icon as shown.

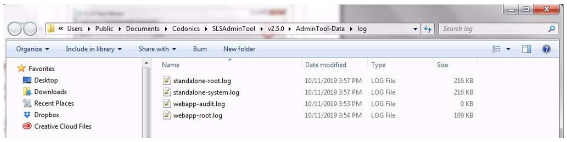


Name	Status
SLS AT Server v2.5.0	Running at http://10.1.131.105:8081

- To open the location where the AT logs are stored, select the disk icon as shown. After selecting the icon, a window will open as shown below displaying the AT logs which can then be opened for review or zipped up and stored locally on a PC or USB drive for further analysis.

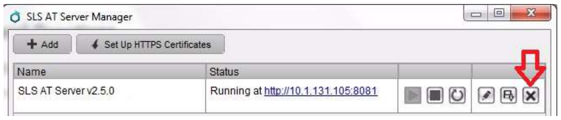


Name	Status
SLS AT Server v2.5.0	Running at http://10.1.131.105:8081



Name	Date modified	Type	Size
standalone-root.log	10/11/2019 3:57 PM	LOG File	216 KB
standalone-system.log	10/11/2019 3:57 PM	LOG File	216 KB
webapp-audit.log	10/11/2019 3:53 PM	LOG File	0 KB
webapp-root.log	10/11/2019 3:54 PM	LOG File	109 KB

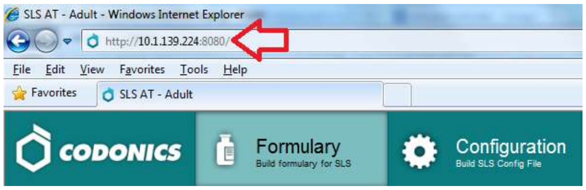
- To delete the AT service, select the X icon as shown.



Name	Status
SLS AT Server v2.5.0	Running at http://10.1.131.105:8081

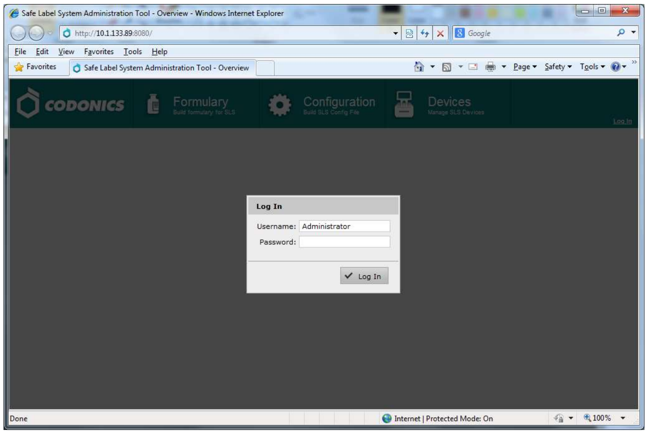
Operation

- To use the AT Server from any computer on the same network as the server, open a browser window (e.g., Internet Explorer, Chrome, FireFox) and enter the IP address of the host followed by the port where the formulary is located (e.g., http://10.1.139.224:8080/).



> **Note:** Refreshing the web page (e.g., pressing F5 on the keyboard) will automatically logout the user and restart the service.

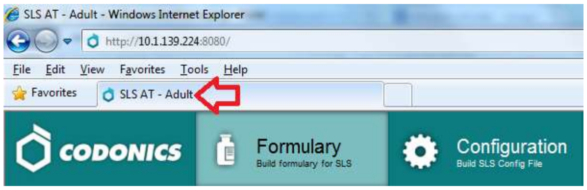
- The AT Server will start up and the Log In screen will appear. Sign in with the same password used for the AT Stand-alone.



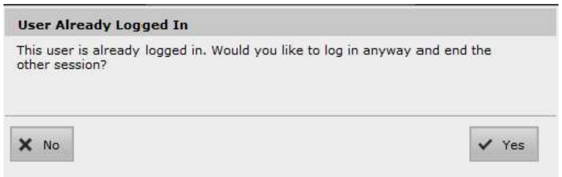
Username: Administrator
Password:

> **Note:** When starting the AT Server, you will not receive a prompt to choose a data directory as you did with the AT Stand-alone.

- The formulary name that the AT Server is running is displayed in the browser tab.

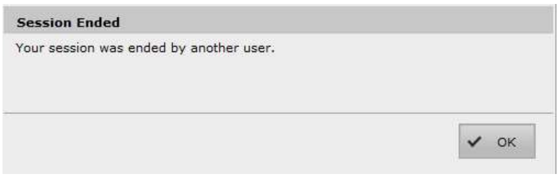


- If another user tries to log into an AT Server that is already logged into, the new user will receive a warning:


User Already Logged In

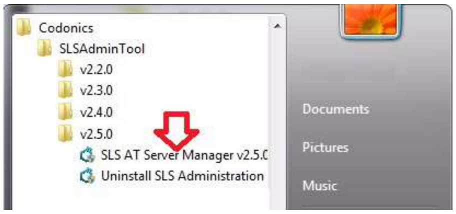
This user is already logged in. Would you like to log in anyway and end the other session?

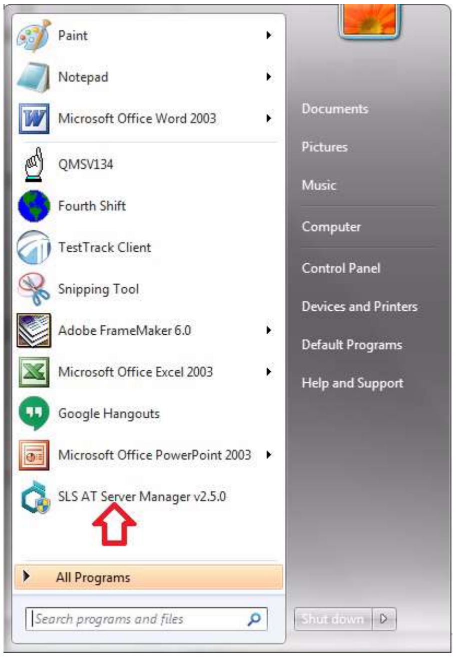
- The new user can click Yes which will log out the existing user who will receive a message:


Session Ended

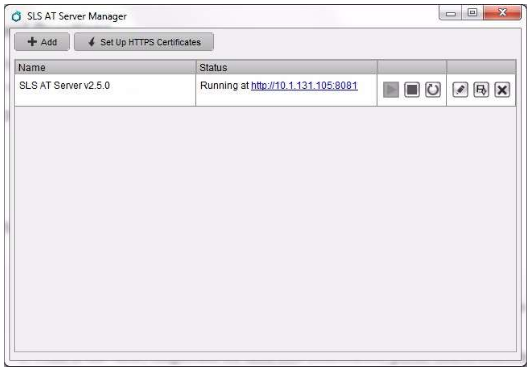
Your session was ended by another user.

- If you are using the AT Server locally on a PC and don't recall what the IP address is, click on the Windows start icon. The AT Server Manager will be located in the Codonics Application or pinned to the Windows start menu as shown below.





- Click on the SLS AT Server Manager which will open the AT Server Manager dialog and provide a link to the IP address and port where the AT is running. Click on the link to open and run the AT.

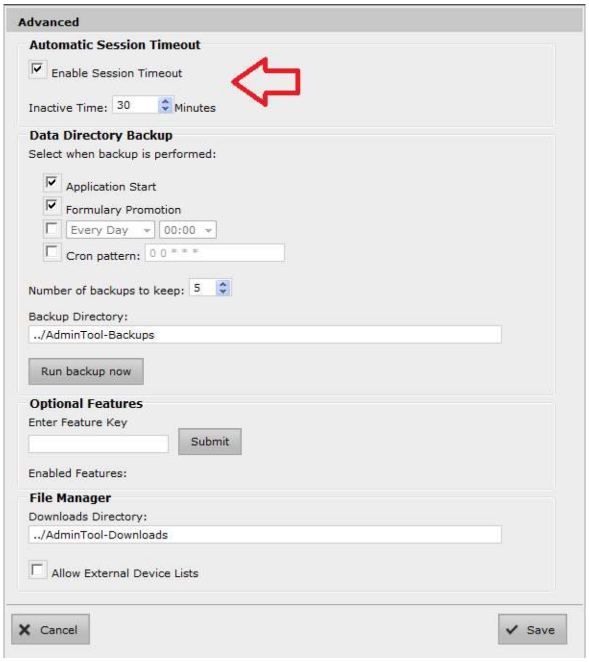


Name	Status
SLS AT Server v2.5.0	Running at http://10.1.131.105:8081

> **Note:** If the AT service is stopped, follow the instructions in the section Additional Actions in the AT Server Manager to start the AT again. A link will be provided to the AT's IP address and port. Click on the link.

AT Timeout Configuration

- When Automatic Session Timeout is enabled, the AT Server will automatically log out a logged in user after a predefined period of AT inactivity. To configure the AT Server's Automatic Session Timeout, click on the Advanced link in the upper right corner of the AT and the Advanced dialog will be displayed. The Automatic Session Timeout is enabled by default and set to 30 minutes of Inactive Time. The maximum Inactive Time is 480 minutes (i.e., 8 hours).



☑ Enable Session Timeout

Inactive Time: 30 Minutes

Select when backup is performed:

☑ Application Start

☑ Formulary Promotion

☐ Every Day 00:00

☐ Cron pattern: 0 0 * * *

Number of backups to keep: 5

Backup Directory: ../AdminTool-Backups

Enter Feature Key

Enabled Features:

Downloads Directory: ../AdminTool-Downloads

☐ Allow External Device Lists

Technical Support

If problems occur during operation, contact Codonics Technical Support at any time.

Phone:	+1.440.243.1198
Email:	support@codonics.com
Website:	www.codonics.com

Get it all with just one call
800.444.1198

All registered and unregistered trademarks are the property of their respective owners. Specifications subject to change without notice.

Patents: www.codonics.com/ip/patents.

CODONICS®
We bring the future into focus

17991 Englewood Drive
Middleburg Heights, OH
44130 USA
+1.440.243.1198
+1.440.243.1334 Fax
Email info@codonics.com
www.codonics.com

Codonics Trading Co, Ltd.
317 Xianxia Rd. Building B
Unit 1412
Changning Dist., Shanghai
P.R. China, 200051
86-21-62787701
86-21-62787719 Fax

Codonics Limited KK
AQUACITY 9F,
4-16-23, Shibaura
Minato-ku, Tokyo,
108-0023 JAPAN
81-3-5730-2297
81-3-5730-2295 Fax