Baxter

Welch Allyn Connex
Central Station & Server

Administrator's Guide

Welch Allyn assumes no responsibility for any injury to anyone, or for any illegal or improper use of the product, that may result from failure to use this product in accordance with the instructions, cautions, warnings, or statement of intended use published in this manual.

For information about this product, see hillrom.com/en/about-us/contact-us/contact-technical-support.

⚠ **CAUTION** Changes or modifications not expressly approved by Welch Allyn could void the purchaser's authority to operate the equipment.

REF 80018210 Ver. R, Revision date: 2022-12

This manual applies to # 901066 Monitoring Station

🏭

Welch Allyn, Inc.
4341 State Street Road
Skaneateles Falls, NY 13153 USA

baxter.com

Welch Allyn, Inc. is a subsidiary of Baxter International Inc.

1 Introduction 1
About this manual 1
Scope 1
Symbols used in this manual 1
Definitions 2
Technical support services 2
Partners in Care service agreements 3
Connex components general maintenance 3
2 Safety, warnings and cautions 5
Safety 5
Warnings and Cautions 5
General safety considerations 7
Electrostatic discharge (ESD) 7
3 Overview and System Hardware 9
Overview 9
4 Central Station Startup 11
Different startup 11
Networked environment (Client / Server) considerations 11
Warm Spare station considerations 11
Stand-alone central station considerations 11
Standard central station startup 12
Warm Spare station startup 12
5 Connex Server Startup 15
Confirm Connex Server operational state 15
Confirm communication with central stations 17
Confirm communication with EMR 18
Configure the Connex Central Station 20
Client/Server configurations 20
Standalone Connex Central Station configurations 20
6 Network, Printer, Time & Date config. 21
Connex CS Shell versus Windows Shell 21
Network Changes 22
Add a Customer Supplied Printer 23
Install print driver from an executable.EXE file 23
Install print driver from a media with an .INF file 23
If the desired printer is found using search: 23
If the printer was not found using search: 24
Change Date, Time, and Time zone 24
7 Backup & Restore 25
Backup users and configuration 25
Nightly System Backup 27
Backup Corepoint configuration - create a NIX file 28
Backup Corepoint HL7 License 31
Restore Patients and Users 32
Restore Settings 33
Creating a User list 34
8 Location Management 35
Add a Station 35
Add a Master bed list 38
Create a New Unit 39
Add a New Room and Bed 40
When complete... 45
Add a Covered area 46
9 Promoting a Warm Spare 49
Monitor the Data Sync Service 51
10 Activating a License 53
Open the license activation tool 53
Automatic license activation 54
Manual license activation 55

11 License Pool Configuration 57
Configure the License pool 57
Automatically assign per covered area licenses 58
Manually assign per covered area licenses 58
Assign Per Care Unit Licenses 59
When Complete... 59
12 Localize Station settings 61
Vital Signs settings 61
Patient Management settings 62
To change Display and Sound settings: 64
Configure alarm hold off 66
Configure patient rest mode 67
Configure continuous vital signs outbound 70
Configure units of measure 71
Configure auto discharge settings 73
ADT auto discharge settings 74
Auto discharge settings for confirmed patients 75
Late ADT settings 77
13 Managing Device assignments 79
Add a new device 79
Changing device assignments 81
14 Managing Views 85
Create a View 85
View Customizations for Mapped by patient location 90
15 Customizing Reports 93
Configure a custom facility logo 93
16 Time Synchronization 95
Setting up an authoritative time server, on Connex server 95
Configuring client sync with an authoritative time server 96
17 Connex Database Restore 97
Before you begin... 97
Overview 97
Preparation - Stop services, tasks and CS Application 97
Restore the database from backup 98
Deprovision the Restored Database 103
Reinstall the database on the central stations 103
Restart the Data Sync Service and Wait for Completion of the Initial Sync Operation 105
Restart Services, Scheduled Tasks, and Open the CS Application 105
Special circumstances... 105
18 Configure NRS 107
Change Server Ports 108
Assign Host for DCP 108
Assign Hosts for DCP Network Rendezvous 109
Adding an ordinal for Service Monitor 110
When all NRS settings are complete... 111
NRS conflicts with existing VM deployments 111
NRS conflicts with multiple stand-alone Connex CS deployments 111
19 Configure Device connectivity 113
DNS Name support at device 113
DHCP Option 43 / 60 support at device 113
Network Rendezvous Service (NRS) IP at device 113
Vitals Management (VM) IP at device 114
UDP Broadcast 114
Roles and users 114
Roles 114
Users 115
20 High Availability 117

About application redundancy ... 117
About data redundancy ... 117
Configuring High Availability ... 117
Changes for Network Rendezvous Service (NRS) ... 117
Changes for Corepoint Integration Engine (CIE) ... 118
Load balancer considerations ... 118
Troubleshooting ... 118
A Troubleshooting ... 119
General ... 119
Central Station Computer Startup ... 119
Device & System Connectivity problems ... 120
High Availability issues ... 122
B Moving from Test to Production ... 125
Assumptions ... 125
Preparation ... 125
Create a database restore point ... 126
Clearing test data from the WADB database ... 127
Configure HL7 connections, if required ... 130
Confirm Connex server operation, client-server only ... 131
Synchronize central stations, client-server only ... 131
Restart after synchronization is complete ... 133
Finalizing the Environment ... 133
Troubleshooting test to production issues ... 134
C ProView ... 135
Intended use ... 135
Installation and setup ... 135
Create roles and users ... 136
Create the ProView role ... 136
Create the VitalTestApp role ... 136
Create the ProView user ... 136
Create the VitalTestApp user ... 137
Create the BioMed user ... 137
Using ProView for data review ... 137
Logging in ... 137
Display the patient list ... 137
Search the patient list ... 138
Display the vitals test list ... 138
Using a vitals test record to test EMR connectivity ... 139
Create a vitals test record ... 139
Reference ... 140
Uninstall ProView ... 140
Update the server IP address ... 140
Patient states ... 141
D HL7 parameter labels and units of measurement ... 143
Units of Measure – Continuous Measurement Configuration (Unconfirmed) ... 144
Units of Measure – Vitals Outbound Configuration ... 145
Sample continuous ORU message ... 146
Continuous Measurement Configuration Labels ... 146
Sample Episodic ORU message ... 147
Episodic Measurement Configuration Labels ... 148
Connex CS Code Sets ... 152
PID-8 – Administrative Sex Code Set ... 152
PV1-2 – Patient Class Code Set ... 153
OBX-8 – Alarm Code Code Set ... 153
E HL7 interface test plan ... 155
Sample test plan ... 155
F Server Authentication and Encryption ... 157
Introduction ... 157

Enable Encrypted Device Connections ... 157
Enable Server Authentication From Devices ... 157
Episodic Device Connections (TLS) ... 158
Continuous Device Connections (DTLS) ... 159
Apply Certificate Authentication ... 159
Disable Server Authentication From Devices ... 160
Remove a server authentication certificate ... 160
Corepoint Certificates ... 160
Reinstall and Rebind Corepoint Security Certificates ... 160
G Configure Clinician Authentication ... 161
Multiple Security Providers ... 161
View Clinician Authentication settings ... 162
Configure for use with Connex Database ... 163
Configure Clinician Identifier for Connex CS Database ... 163
Configure Group Membership for Connex CS Database ... 164
Configure EMR Identifier for Connex CS Database ... 164
When changes are complete ... 164
Configure for use with Active Directory ... 165
Configure Clinician identifier with Active Directory ... 166
Configure Group membership with Active Directory ... 166
Configure EMR identifier with Active Directory ... 167
Add a Custom active directory identifier ... 167
When changes are complete ... 168
Configure for use with Imprivata OneSign ... 168
Add a provider for Imprivata ... 168
Order the security providers ... 169
Delete a security provider ... 170
H Connex database restore and reinstallation ... 171
Connex database restore ... 171
Stop Services, Scheduled Tasks, and close the CS Application ... 172
Restore the database from backup ... 172
De-provision the Restored Database ... 174
Reinstall the database on the central stations ... 175
Restart the Data Sync Service and Wait for Completion of the Initial Sync Operation ... 177
Restart Services, Scheduled Tasks, and Open the CS Application. ... 177
Special circumstances ... 177
Connex database reinstallation ... 178
I Network change and configuration ... 181
Network IP change overview ... 181
Client Server deployment ... 182
If the IP address of the Connex server changes ... 182
EMR-side changes ... 182
Connex server-side changes ... 182
Update the SERVER NRS configuration ... 183
Update additional Server settings for ECS and EGS ... 184
Each central station client-side changes ... 185
Update Central Station license service ... 185
If the IP address of the Connex Central Station changes ... 185
If the IP Address of the EMR Server Changes ... 186
If the IP Address of the Third Party Alarm Server changes ... 187
If the Corepoint IP address Changes ... 188
Standalone deployment ... 189
If the IP address of the standalone central station system changes ... 189
Update the NRS configuration ... 189
Update additional settings for ECS... 190
If the IP address of the Third Party Alarm Server Changes ... 191
J Anti-virus Software Exclusion Folders ... 193
Exclusion Overview ... 193
Connex CS Exclusions ... 193
Corepoint Exclusions ... 193

1 Introduction

About this manual

This manual provides information to configure, maintain and support Connex Central Station and Connex Server.

Before making changes to the Connex Central Station or server, read sections of this manual that pertain to your use of the product or planned activity.

Scope

Procedures documented within this manual are intended to be performed by trained Welch Allyn support personnel, authorized and trained biomedical engineers, or authorized and trained information technology professionals. Familiarity with Microsoft Window Operating Systems, SQL Databases, and networking is assumed including:

- File system directory navigation
- Editing application and system files
- Basic CLI commands
- MS Visual Studio
- Database modify and restore
- Basic network diagnostic commands

Contact Hillrom Technical Support at hillrom.com/en/about-us/contact-us/contact-technical-support/ for additional assistance as needed.

Symbols used in this manual

⚠ **WARNING** Warning statements identify conditions or practices that could result in personal injury.

⚠ **CAUTION** Caution statements identify conditions or practices that could result in damage to the equipment or property.

NOTE Notes provide additional important information. The content of the note may not be contained elsewhere in the document.

Definitions

ADT	Admit, Discharge, Transfer, a type of message notification of a change in status within the facility's record keeping system and/or the EMR application
AGS	Alarm Gateway Service, a licensable feature which provides alarm messages in a data stream to a 3rd party system.
CPU	Central Processing Unit, a desktop computer (PC) in the case of a central station, or a server computer in the case of a hardware Connex Server.
Component	A major subassembly of the central station or network (e.g. CPU, Video Display, Printer, Ethernet Switch, etc.).
DNS	Domain Name System (Server or Service), a system on the network which translates domain names to IP addresses
DHCP	Dynamic Host Configuration Protocol, a protocol for assigning dynamic IP addresses on the network.
DHCP Option 43/60	A location method for devices to locate a Connex Server using the facility's DHCP service. The facility's DHCP services provide a forwarding service to a system running NRS. Configure the DHCP server to support option 609 lookup or fixed Vendor Class Identifier "welchallyn-nrs". The corresponding option 43 value is an encapsulated list of up to 3 Connex Server IP addresses.
EMR	Electronic Medical Record, the record system maintained by the facility with patient information and data, including vital signs.
HIS	Hospital Information System, the network in use by the facility that supports network communication with various systems and devices, including Connex CS central station, Connex server, and devices.
Installation	The on-site process for installing the hardware, network infrastructure, and system configuration at the customer's location of business.
LAN	Local Area Network, a network of computers connected together in a local environment. Typical communication includes standard Ethernet protocols.
NRS	Network Rendezvous Service, a service that runs on the central station and Connex server that provides a location service to direct devices to the proper system upon connection to the network.
POST	Power On Self Test - An integrity check within the CPU and/or device to ensure that all expected components are present and working (e.g. memory tests).
Upgrade	On-site service activity to enhance or add functionality to a device or system. An upgrade can be accomplished with changes to hardware, software, configuration, or combinations of all three.
UPS	Uninterruptable Power Supply, a unit which provides battery back-up power for connected devices.

Technical support services

Hill-Rom offers the following technical support services:

- Telephone support
- Remote diagnostics
- Service agreements (Partners in Care)
- EMR Integration professional services
- Service training

For information on any of these services, go to hillrom.com/en/about-us/contact-us/contact-technical-support/.

Partners in Care service agreements

While product warranties provide basic assurance of Welch Allyn hardware and software quality, they may not include the full range of services and support you need. Welch Allyn offers premium service and support through our Partners in Care program. Whether you service your own devices and require a minimum of support or rely on us to service your device, Welch Allyn provides a program that will meet your needs. For more information visit our web site at hillrom.com/en/about-us/contact-us/contact-technical-support/ or call your sales representative.

Connex components general maintenance

General preventive maintenance consists of basic cleaning of equipment, inspection, and verification of the equipment and system operation. Only a trained biomedical engineer should perform these tasks.

Perform general preventative maintenance according to the following recommended schedules:

Service Activity	Frequency	Component	Action
Inspection	Bi-annually	Central Station Computer	• Visually inspect all cables, connectors, and indicators. • Perform alarm test and confirm proper operation of audio speakers.
		Display	• Visually inspect all cables, connectors, and indicators. • Inspect display quality and settings, such as brightness and contrast.
		Keyboard	• Visually inspect keys and cables. • Test function of keys.
		Mouse	• Visually inspect cables and connectors. • Test functions of rollers and control buttons.
		Printer	• Run the on-board print quality tests. • Visually inspect display LEDs, connectors, cable, and controls.

Service Activity	Frequency	Component	Action
Cleaning and maintenance	Annually	Central Station Computer	• Power down the computer. • Open the computer case and clean dust build up.
		Display	• General cleaning.
		Keyboard	• Remove and dust or debris build up. • General cleaning.
		Mouse	• Remove and dust or debris build up. • General cleaning.
		Printer	• Clean external cooling vents. • Refer to the Mfg. printer directions for use for additional cleaning and maintenance information.

NOTE Use only approved cleaning solutions according to your facility's guidelines and the manufacturer's recommendations.

Service Activity	Frequency	Component	Action
Component Replacement	Annually	Keyboard	• Replace to meet performance recommendations.
		Mouse	• Replace to meet performance recommendations.
	2 to 3 years	Display	• Replace to meet performance recommendations.

NOTE Actual performance of system components may vary depending on usage.

2 Safety, warnings and cautions

Safety

All persons performing activities to configure, maintain and support Connex CS central station and/or server must read and understand all safety information presented within this manual before beginning repairs.

Warnings and Cautions

WARNING It is strongly recommended that the central station computer and display are installed with a redundant power source, such as an uninterrupted power supply (UPS) capable of supporting at least 600 watts. The facility is responsible to provide 100 percent reliable power to the central station. The central station will only work with reliable AC power.

WARNING It is strongly recommended that any hardware server intended to be used as a Connex server be installed with a redundant power source, such as an uninterrupted power supply (UPS) capable of supporting at least 500 watts. The facility is responsible to provide 100 percent reliable power to the central station. A hardware Connex server will only work with reliable AC power.

WARNING When performing service and repair procedures, follow the instructions exactly as presented in this manual. Failure to do so could damage the system, invalidate the product warranty, and lead to serious personal injury

WARNING For maximum system performance and availability, the central station computer and server hardware must be replaced on a recommended preventative maintenance interval. See the service documentation for recommended intervals.

WARNING Do not change central station components or configuration, such as removing or adding a printer or substituting hardware, without approval by Welch Allyn. Such changes could degrade system performance and affect patient monitoring.

WARNING Do not install additional software on the central station PC without prior approval by Welch Allyn. Such changes could degrade system performance and affect patient monitoring.

WARNING Devices connected to the central station must be certified for overall system compliance according to the IEC 60601-1 safety standard. The interconnection of any device with the central station must comply with IEC 60601-1-1. If in doubt about network connectors or devices, please consult your facility's Biomedical Engineering department or Hillrom Technical Support

⚠ **CAUTION** The system many not function properly if components have been dropped or damaged. Protect system components from severe impact or shock. Do not use the system if you notice any signs of damage.

⚠ **CAUTION** Do not operate the system in the presence of magnetic resonance imaging (MRI) or hyperbaric chambers.

⚠ **CAUTION** No component-level repair of circuit boards and subassemblies is supported. Use only the support procedures documented in this manual.

⚠ **CAUTION** Changes to the network interfaces on a live network will cause outages, and should be planned with the facility. Additional changes may also be required on each central station if the IP address of the server that supports them is changed. Refer to the ***Connex CS Software Install Guide*** for additional information.

⚠ **CAUTION** The anti-virus system on your computer may attempt to block certain files that are necessary to successfully install and run the software. To address this issue, refer to the exclusion lists in "Anti-virus Software Exclusion Folders" on page 193 for the appropriate exclusion information.

⚠ **CAUTION** Customer networks used to support continuous monitoring functions as part of Connex CS shall be configured and maintained by information technology professionals.

⚠ **CAUTION** Connex CS shall be serviced by Welch Allyn trained service personnel.

⚠ **CAUTION** Connex CS components shall be replaceable by Welch Allyn service personnel, authorized customer biomedical engineers, or authorized information technology professionals.

General safety considerations

- If the system detects a recoverable problem, it displays an exception message on-screen. Contact Hillrom Technical Support for additional information.
- If the system detects an unrecoverable problem, it displays an error message. For more information see "Troubleshooting" on page 119.
- To ensure patient safety, use only accessories recommended or supplied by Welch Allyn. (See the accessories list on the user documentation or hillrom.com.) Always use accessories according to your facility's standards and according to the manufacturer's recommendations and instructions. Always follow the manufacturer's directions for use.
- Welch Allyn recommends that only Welch Allyn service personnel or an authorized repair center perform warranty service. Performing unauthorized service on a device that is within warranty may void the warranty.

Electrostatic discharge (ESD)

CAUTION
SENSITIVE ELECTRONIC DEVICES
DO NOT SHIP OR STORE NEAR STRONG ELECTROSTATIC, ELECTROMAGNETIC, MAGNETIC OR RADIOACTIVE FIELDS.

ATTENTION
OBSERVE PRECAUTIONS FOR HANDLING
ELECTROSTATIC SENSITIVE DEVICES

⚠ **CAUTION** Electrostatic discharge (ESD) can damage or destroy electronic components. Handle static-sensitive components only at static-safe workstation.

⚠ **CAUTION** Assume that all electrical and electronic components of the monitor are static-sensitive.

Electrostatic discharge is a sudden current flowing from a charged object to another object or to ground. Electrostatic charges can accumulate on common items such as foam drinking cups, cellophane tape, synthetic clothing, untreated foam packaging material, and untreated plastic bags and work folders, to name only a few.

Electronic components and assemblies, if not properly protected against ESD, can be permanently damaged or destroyed when near or in contact with electrostatically charged objects. When you handle components or assemblies that are not in protective bags and you are not sure whether they are static-sensitive, assume that they are static-sensitive and handle them accordingly.

- Perform all service procedures requiring disassembly of computers (e.g. installing a replacement hard disk drive) in a static-protected environment. Always use techniques and equipment designed to protect personnel and equipment from electrostatic discharge.
- Remove static-sensitive components and assemblies from their static-shielding bags only at static-safe workstations - ensuring that the person performing these activities is at the same ground potential as the device being serviced.
- Use of a properly grounded table and grounded floor mat, including the wearing of a grounded wrist strap (with a resistor of at least 1 megohm in series) or other grounding device is recommended.
- Any assembly or subassembly that has an exposed circuit board should be treated as a static sensitive device.

- Avoid touching the contacts or components on circuit board assemblies. Handle by the edges of the board whenever practical
- Remove or insert static-sensitive components and assemblies only with system power turned off.
- Insert and seal static-sensitive components and assemblies into their original static-shielding bags before removing them from static-protected areas.

3 Overview and System Hardware

Overview

The Connex Central Monitoring Station is intended to be use by clinicians for the central monitoring of neonatal, pediatric, and adult patients in health care facilities.

In addition to the central monitoring of patient data, alarms and alerts, the Connex software can include optional modules to provide extended recording of patient data, including full disclosure.

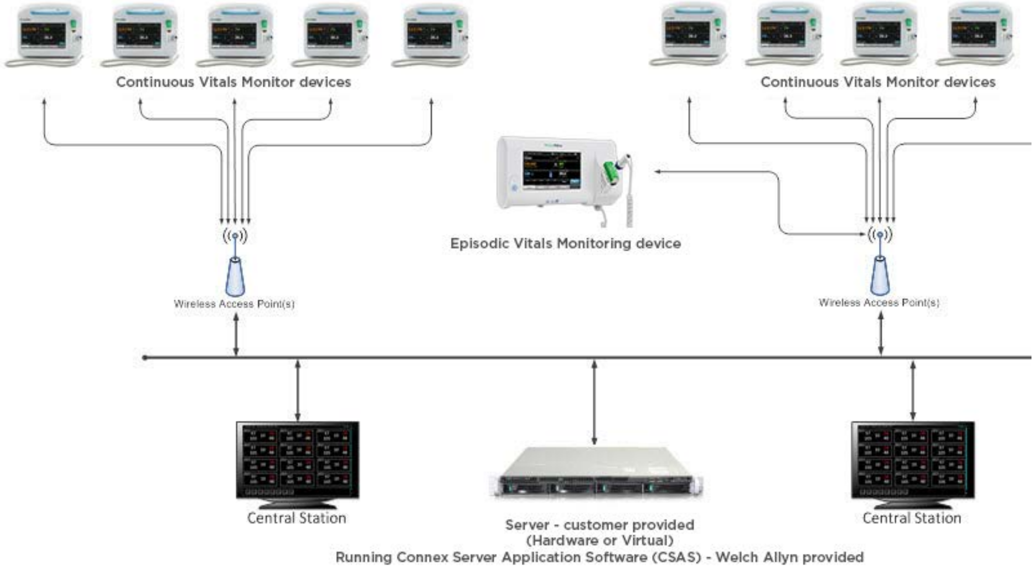
The Connex CS system consists of the Connex Server Application Software running on a customer supplied Microsoft server and SQL server. See the Technical Systems Requirements documentation for MS Server and MS SQL server for version specifics. A Connex Central Station with Connex Software, which receives and displays information from connected vitals monitoring devices, is optional for use with continuous monitoring. The Connex Central Station includes all of the software needed to provide a single, central display of all continuously monitored patients vitals data (both continuous parameters and episodic data are available). The central station also monitors connected continuous devices for proper operation, and displays an alarm if a continuous monitor stops working or is improperly disconnected.

Multiple central stations may be installed in a shared environment with a Connex server providing a central data repository for all information. In addition, the Connex server may also be used to support integration with the facilities HIS to share patient information and data.

A high-level topology with multiple central stations and a Connex server is shown in“Figure 3-1: Connex CS System with multiple Central Stations conceptual model” below. Although all devices are shown with wireless communication, a wired-networking model may also be used.

NOTE All screenshots and filepaths in this document are for example only. Your setup may be different.

Figure 3-1: Connex CS System with multiple Central Stations conceptual model


Continuous Vitals Monitor devices
Continuous Vitals Monitor devices
Episodic Vitals Monitoring device
Wireless Access Point(s)
Wireless Access Point(s)
Central Station
Central Station
Server - customer provided
(Hardware or Virtual)
Running Connex Server Application Software (CSAS) - Welch Allyn provided

4 Central Station Startup

Different startup

The computer may be configured as a networked central station with a shared Connex server, a warm spare station, or a stand-alone central station. The station behavior at startup differs based on the configuration.

Networked environment (Client / Server) considerations

In the networked environment, where there is a Connex server, it is preferred that the Connex server be started first. The Connex server hosts the main database that all central stations attempt to synchronize with on startup, using the Welch Allyn Connex Data Synchronization Service. A central station configured as part of a network (client-server) model will startup with the central station application and run by itself, but may take much longer during the startup process if the Connex server is unreachable. The central station may also be running in a degraded mode until the Connex server is brought online (e.g ADT services may not be available).

Warm Spare station considerations

A system configured for Warm Spare operation is licensed and configured to contact and synchronize its local database with that of the Connex server. The Warm Spare does not perform any other functions than to maintain a state of readiness to be put into place as a replacement central station when needed. Refer to "Standard central station startup" on page 12 below startup behavior of a Warm Spare station.

A Warm Spare is part of a network environment, with a closet sever as well. It is preferred that the Connex server be started first. Central stations, including a warm spare should be started after the Connex server is running.

Stand-alone central station considerations

In the stand-alone central station, all required services are self contained within the CPU. Thus, there are no other systems to consider in terms of startup order. Stand-alone stations do not have communication ability with the facility's EMR application.

Standard central station startup

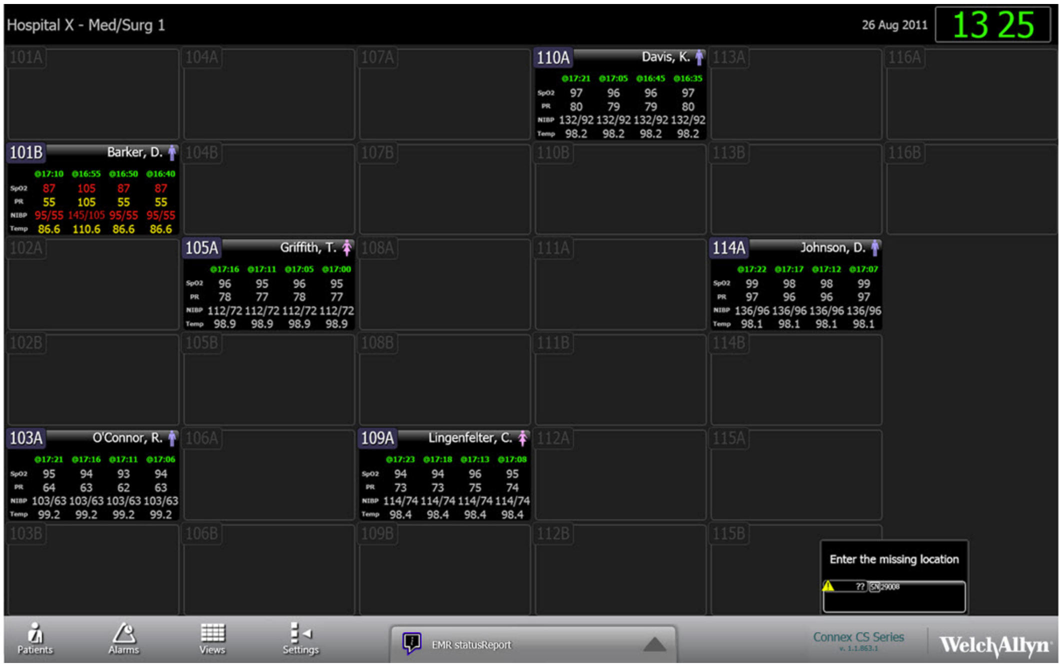
1. If properly configured, the central station should automatically startup with the Connex CS application running.

2. Upon successful start-up of the Connex CS application, the main screen is displayed. See "Figure 4-1: Connex Central Station main screen example - 36 tile grid - custom tile layout display configuration".

3. Some additional configuration may be required on site. Refer to other chapters in this manual for additional information subjects related to configuration and localization.

4. Refer to Appendix A "Troubleshooting" on page 119 if problems are encountered with starting up the central station CPU.

Figure 4-1: Connex Central Station main screen example - 36 tile grid - custom tile layout display configuration



Hospital X - Med/Surg 1

26 Aug 2011 13 25

101B Barker, D.

	@17:10	@16:55	@16:50	@16:40
SpO2	87	105	87	87
PR	55	105	55	55
NIBP	95/55	145/105	95/55	95/55
Temp	86.6	110.6	86.6	86.6

110A Davis, K.

	@17:21	@17:05	@16:45	@16:35
SpO2	97	96	96	97
PR	80	79	79	80
NIBP	132/92	132/92	132/92	132/92
Temp	98.2	98.2	98.2	98.2

105A Griffith, T.

	@17:16	@17:11	@17:05	@17:00
SpO2	96	95	96	95
PR	78	77	78	77
NIBP	112/72	112/72	112/72	112/72
Temp	98.9	98.9	98.9	98.9

114A Johnson, D.

	@17:22	@17:17	@17:12	@17:07
SpO2	99	98	98	99
PR	97	96	96	97
NIBP	136/96	136/96	136/96	136/96
Temp	98.1	98.1	98.1	98.1

103A O'Connor, R.

	@17:21	@17:16	@17:11	@17:06
SpO2	95	94	93	94
PR	64	63	62	63
NIBP	103/63	103/63	103/63	103/63
Temp	99.2	99.2	99.2	99.2

109A Lingenfelter, C.

	@17:23	@17:18	@17:13	@17:08
SpO2	94	94	96	95
PR	73	73	75	74
NIBP	114/74	114/74	114/74	114/74
Temp	98.4	98.4	98.4	98.4

Enter the missing location

?? SN 29008

EMR statusReport

Warm Spare station startup

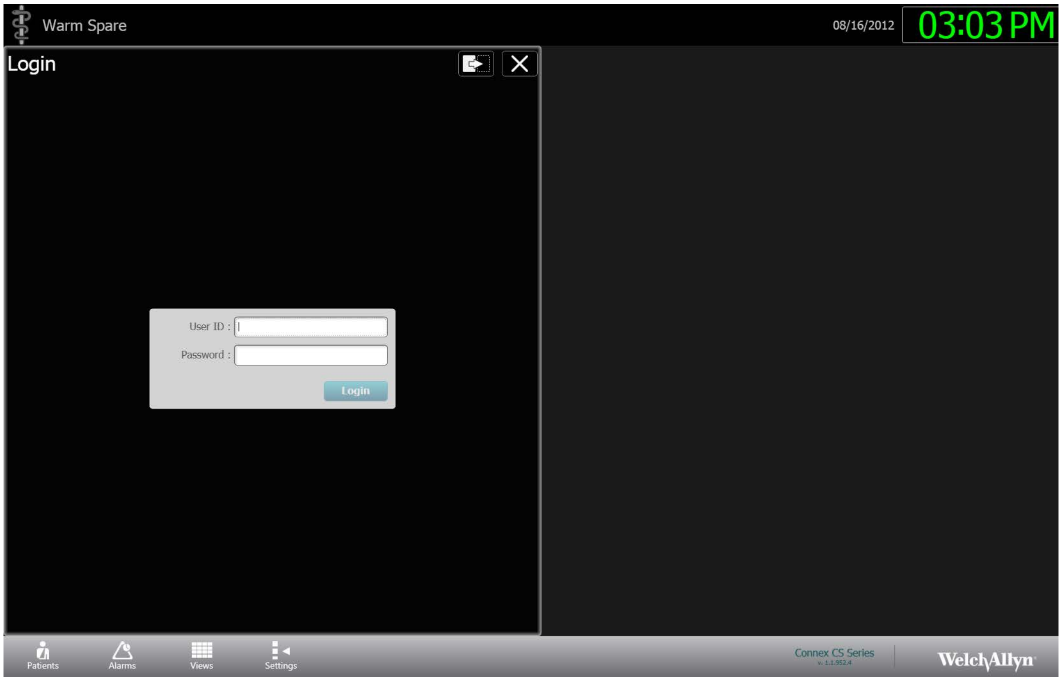
If the station is configured as a Warm Spare:

1. Upon successful start-up of the Connex CS application, the Warm Spare screen is displayed. An example is shown in "Figure 4-2: Warm Spare main screen example" on page 13.

2. With the exception of print drivers installation, typically no additional configuration is required beyond this point.

   a. Print drivers may be required to work with customer supplied printers. Refer to "Network, Printer, Time & Date config." on page 21 for additional information on installing print drivers.

Figure 4-2: Warm Spare main screen example



3. Refer to Appendix A "Troubleshooting" on page 119 if problems are encountered with starting up the central station CPU.

5 Connex Server Startup

Confirm Connex Server operational state

1. Login to the server with the Administrator account user name and password.

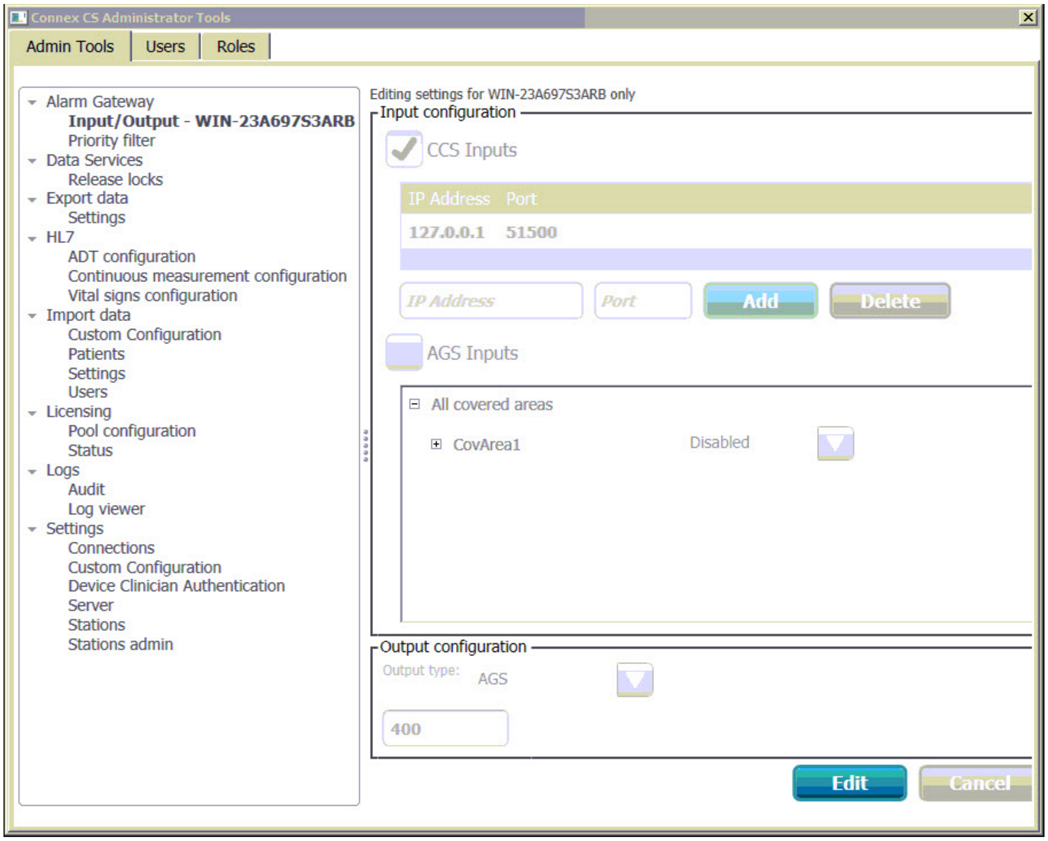
2. Upon success, the desktop screen is displayed.

3. On the desktop, double-click on Cx . The Connex CS Admin Tools function launches.

    a. If the icon is not present, go to **Start > All Programs** > **Welch Allyn** > **Connex** > **Admin Tools Launcher** > **(version number)** to locate the program. Right-click on **Welch Allyn Admin Tools Launcher** and select **Send to** > **Desktop (create shortcut)** to send a shortcut to the desktop.

4. The Connex CS Administrator Tools is similar to the **Settings** > **Advanced settings** (if needed) > **Admin tools** tab window on the Connex Central Station. An example is shown below.

Figure 5-1: Administrator Tools startup window



Editing settings for WIN-23A697S3ARB only

Input configuration

☑ CCS Inputs

IP Address	Port
127.0.0.1	51500

IP Address Port

□ AGS Inputs

⊟ All covered areas

⊞ CovArea1 Disabled

Output configuration

Output type: AGS

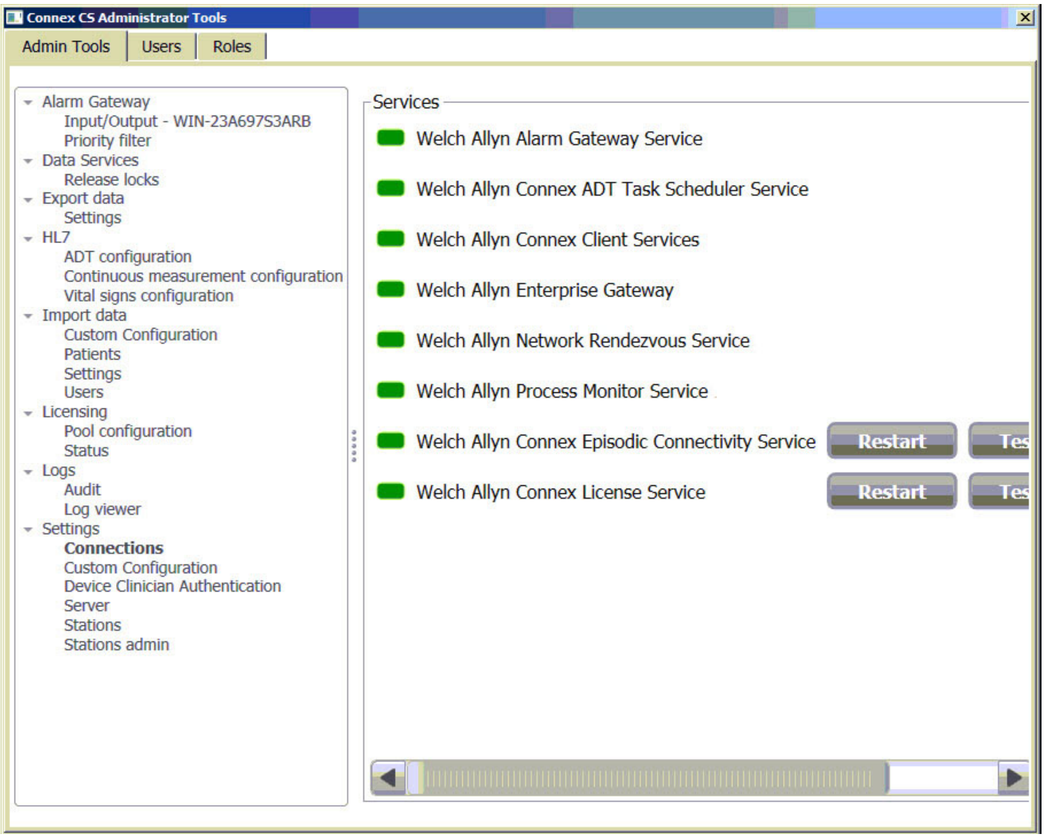
400

5. On the Admin Tools tab, navigate to **Settings** > **Connections**. The Services windows displays the state of all of the core services running which make up the Connex Server application. An example is shown below in Figure 5-2.

6. A **green** state means that the service is currently running normally.

7. A **red** state means that the service is not running in a normal state or has stopped.

Figure 5-2: Administrator Tools setting connections window



🟩 Welch Allyn Alarm Gateway Service

🟩 Welch Allyn Connex ADT Task Scheduler Service

🟩 Welch Allyn Connex Client Services

🟩 Welch Allyn Enterprise Gateway

🟩 Welch Allyn Network Rendezvous Service

🟩 Welch Allyn Process Monitor Service

🟩 Welch Allyn Connex Episodic Connectivity Service

🟩 Welch Allyn Connex License Service

8. If more than one service needs to be restarted, it is recommended all services be restarted in a specific sequence.

To restart multiple services:

a. Proceed by clicking on the **Restart** button associated with each service in the following sequence:

- Client Services
- License Service
- Enterprise Gateway service
- Episodic Connectivity Service
- Alarm Gateway Service
- ADT Task Scheduler Service
- Network Rendezvous Service
- Process Monitor Service.

b. The Services present in the working window depend on the features and licenses purchased.

NOTE Some Services may not be present on previous versions of Connex CS.

c. If one or more services cannot be restarted successfully, refer to "Troubleshooting" on page 119 for additional information.

Confirm communication with central stations

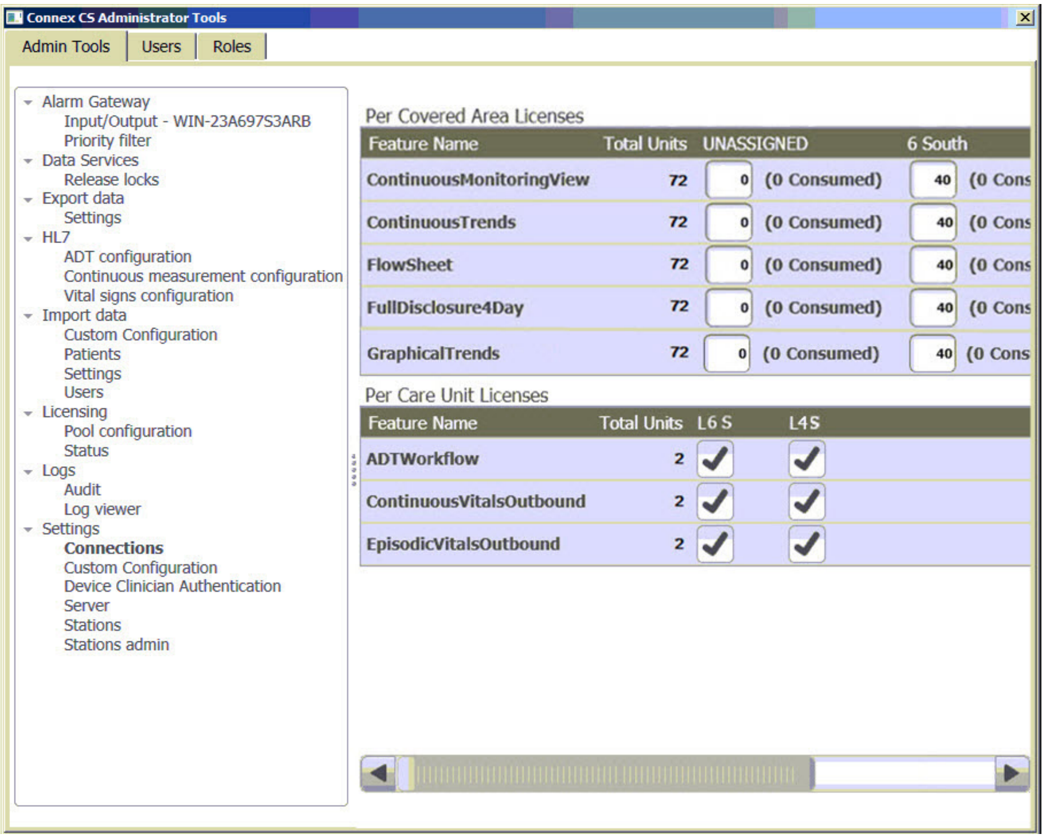
1. Ensure that all central stations have been installed and are reachable on the network.

2. Open a command tool and ping each host by it's assigned IP address. Refer to the ***Connex CS Customer Project Req. Form, Appendix B1*** as needed.

3. On the server, open the Administration Tools again.

4. On the Admin tools tab, navigate to **Licensing** > **Pool Configuration** to view the Covered Area central stations and their respective licensing allocations. An example is shown below.

Figure 5-3: Administrator Tools license pool configuration window



Per Covered Area Licenses

Feature Name	Total Units	UNASSIGNED		6 South	
ContinuousMonitoringView	72	0	(0 Consumed)	40	(0 Cons
ContinuousTrends	72	0	(0 Consumed)	40	(0 Cons
FlowSheet	72	0	(0 Consumed)	40	(0 Cons
FullDisclosure4Day	72	0	(0 Consumed)	40	(0 Cons
GraphicalTrends	72	0	(0 Consumed)	40	(0 Cons

Per Care Unit Licenses

Feature Name	Total Units	L6 S	L4S
ADTWorkflow	2	☑	☑
ContinuousVitalsOutbound	2	☑	☑
EpisodicVitalsOutbound	2	☑	☑

5. Confirm that all central stations installed on the network have a column present with the Covered Area name displaying in the Per Covered Area Licenses window.

   a. In the above example, there are two Covered Areas shown, 6 South and 4 South.

   b. Licenses are allocated to both Covered Areas but with differing quantities.

Confirm communication with EMR

If the server is configured for interface with the facility's EMR application, via HL7 messaging, perform these checks. Refer to the ***Connex CS Customer Project Req. Form*** for configuration settings of HL7 messaging options for both ADT inbound and ORU outbound workflows.

To launch the Corepoint Integration Engine Monitor:

1. Go to **Start** > **Corepoint Health** > **Monitor** to start the Monitor within a browser window.
2. Login with user name and password.

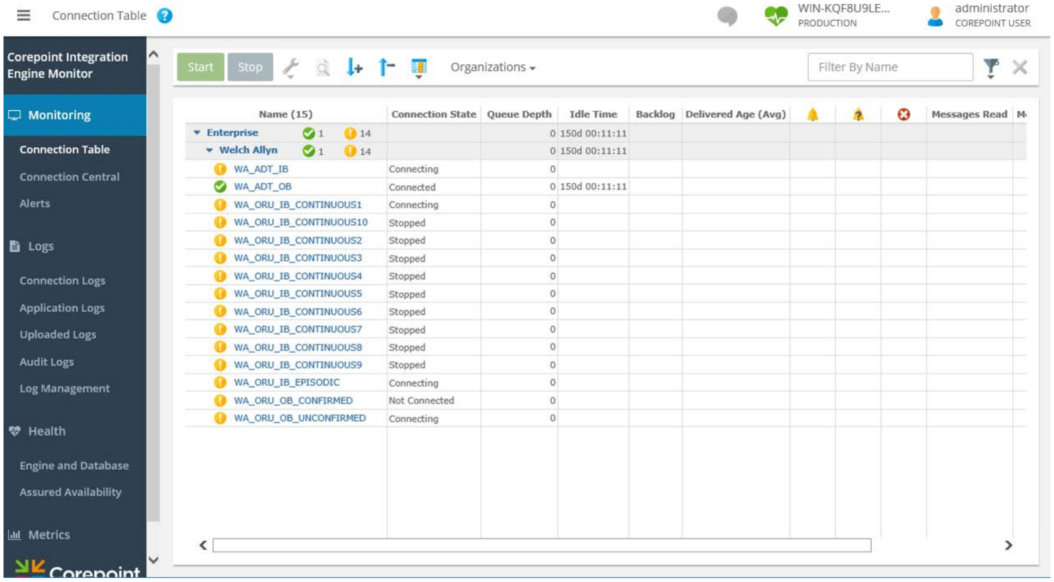
NOTE User names and passwords are case-sensitive.

Profile	User name	Password
View Only	View	ViewOnly
Manager	Manager	ManageHL7

NOTE These user names and passwords are the defaults for each profile.

3. Click on **Connections** tab near the top left of the window to view current connection states. An example is shown below.

Figure 5-4: Corepoint administration console connections initial view



Name (15)	Connection State	Queue Depth	Idle Time	Backlog	Delivered Age (Avg)	🔔	🔔	⊗	Messages Read	M
Enterprise ✓ 1 ! 14		0	150d 00:11:11							
Welch Allyn ✓ 1 ! 14		0	150d 00:11:11							
! WA_ADT_IB	Connecting	0								
✓ WA_ADT_OB	Connected	0	150d 00:11:11							
! WA_ORU_IB_CONTINUOUS1	Connecting	0								
! WA_ORU_IB_CONTINUOUS10	Stopped	0								
! WA_ORU_IB_CONTINUOUS2	Stopped	0								
! WA_ORU_IB_CONTINUOUS3	Stopped	0								
! WA_ORU_IB_CONTINUOUS4	Stopped	0								
! WA_ORU_IB_CONTINUOUS5	Stopped	0								
! WA_ORU_IB_CONTINUOUS6	Stopped	0								
! WA_ORU_IB_CONTINUOUS7	Stopped	0								
! WA_ORU_IB_CONTINUOUS8	Stopped	0								
! WA_ORU_IB_CONTINUOUS9	Stopped	0								
! WA_ORU_IB_EPISODIC	Connecting	0								
! WA_ORU_OB_CONFIRMED	Not Connected	0								
! WA_ORU_OB_UNCONFIRMED	Connecting	0								

4. Some simple view changes may provide a simpler way to view connection data.
   a. The typical view displays connections in terms of grouping. As the application is only being used with Connex, the grouping view contains additional information which is not needed.
   b. Click **Organizations** and select the option for **Flat View**.

c. Click on ▦ in the upper right corner to customize the columns to view. A drop down menu appears.

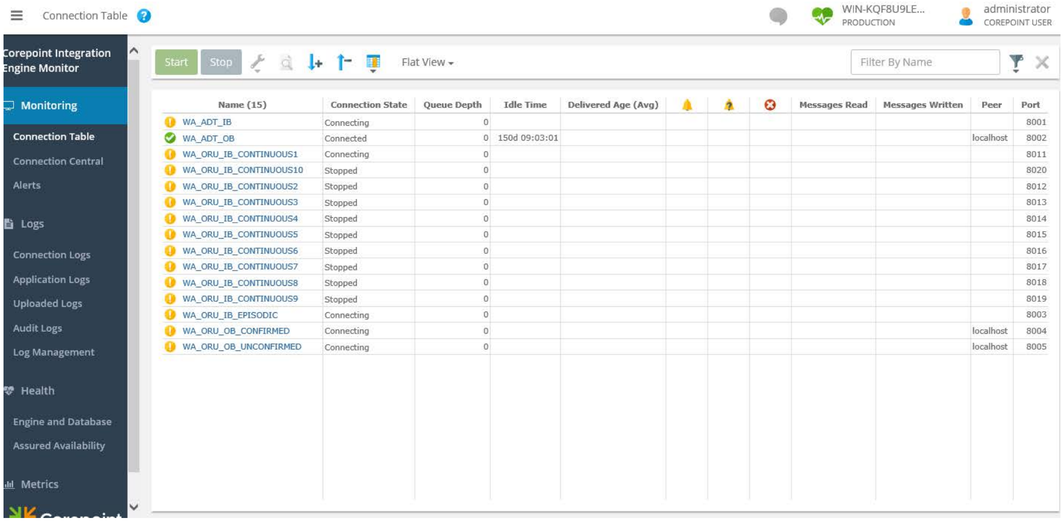
d. Items selected for view have a next to them are selected for inclusion in the view.

e. Use the drop down menu and select Backlog to remove.

f. An updated view example is shown in Figure 5-5 below.

g. The next time the administration console is accessed, it will retain the last know view.

Figure 5-5: Corepoint administration console connections updated view



Name (15)	Connection State	Queue Depth	Idle Time	Delivered Age (Avg)	🔔	🔔	⊗	Messages Read	Messages Written	Peer	Port
WA_ADT_IB	Connecting	0									8001
WA_ADT_OB	Connected	0	150d 09:03:01							localhost	8002
WA_ORU_IB_CONTINUOUS1	Connecting	0									8011
WA_ORU_IB_CONTINUOUS10	Stopped	0									8020
WA_ORU_IB_CONTINUOUS2	Stopped	0									8012
WA_ORU_IB_CONTINUOUS3	Stopped	0									8013
WA_ORU_IB_CONTINUOUS4	Stopped	0									8014
WA_ORU_IB_CONTINUOUS5	Stopped	0									8015
WA_ORU_IB_CONTINUOUS6	Stopped	0									8016
WA_ORU_IB_CONTINUOUS7	Stopped	0									8017
WA_ORU_IB_CONTINUOUS8	Stopped	0									8018
WA_ORU_IB_CONTINUOUS9	Stopped	0									8019
WA_ORU_IB_EPISODIC	Connecting	0									8003
WA_ORU_OB_CONFIRMED	Connecting	0								localhost	8004
WA_ORU_OB_UNCONFIRMED	Connecting	0								localhost	8005

5. Observe the items in the first column, Connection Name.

6. Connection names are related to the functions they serve. A typical list of connections which connect to the facility's EMR application (external to Connex CS) is described in "Table 5-1: External EMR facing connection names and functions, typical".

Table 5-1: External EMR facing connection names and functions, typical

WA_ADT_IB	Inbound ADT between facility HIS and Corepoint (External)
WA_ORU_OB_UNCONFIRMED	Outbound ORU unconfirmed data between Corepoint and facility HIS (External)
WA_ORU_OB_CONFIRMED	Outbound ORU confirmed data between Corepoint and facility HIS (External)

NOTE Connections names may appear differently on your system from those shown in the examples, as interfaces are customized based on facility needs and options purchased.Refer to the ***Connex CS HL7 Interface Guide*** for additional information.

7. A number of internal connections to the Corepoint application are also observed on the connections page. A typical list of connections which connect to other systems and processes in the Connex CS application (internal to Connex CS) is described in "Table 5-2: Internal Welch Allyn facing connection names and functions".

Table 5-2: Internal Welch Allyn facing connection names and functions

WA_ADT_OB	Outbound ADT data between Corepoint and Connex server (Internal)
WA_ORU_IB_CONTINUOUS1	Inbound Continuous ORU data between Central Station 1 and Connex (Internal)
WA_ORU_IB_CONTINUOUS2	Inbound Continuous ORU data between Central Station 2 and Connex (Internal)
WA_ORU_IB_EPISODIC	Inbound Episodic ORU data between Connex server and Corepoint (Internal)

8. In the above example shown in “Figure 5-5 Corepoint administration console connections updated view”, the connections for WA_ADT_IB and the WA_ADT_OB are both green or connected. This is the minimum state that should be present for ADT connections.

   a. The WA_ADT_IB connection may be shown in yellow if an interface between Corepoint and the facility HIS has not been established.

Configure the Connex Central Station

Client/Server configurations

1. Launch Connex Server Application on the Central Station.

   All new central stations begin as a warm spare. If the station is to be designated as a warm spare, no further configuration is necessary; continue to the next section.

2. Assign the station to the host CPU

   For new Connex CS system installations, station names unassigned station names should exist in CS as a result of the Connex Server Software installation and configuration.

   a. From the Warm Spare tab on the settings screen, select the desired station to assign and click **Assign Station**.

   b. Click **Yes** to confirm. Click **OK** to reboot.

3. Create views (tiles)

   a. Re-launch Connex CS

   b. Work with the customer to create and manage customized tile layout or views. Refer to *Software Install Guide, Section B "Create a View"* for detailed instructions.

Standalone Connex Central Station configurations

To configure a standalone Connex Central Station refer to *Software Install Guide* beginning with *Section B "Configuration Details."* These instructions, used together with the pre-populated CRD, will guide you in how to create a station name, master bed list, assign the warm spare to a the logical station name, and all other activities you will need to complete the standalone Connex Central Station configuration. The software install guide will refer to the CRD as needed.

NOTE A standalone Connex Central Station PC takes the role of both server and central station. Be aware that when instructions use an IP address to point to the Server, this will be the local PC's address with all standalone configurations.

6 Network, Printer, Time & Date config.

Connex CS Shell versus Windows Shell

The Connex Central Station is intended and designed to support automatic startup of the Connex CS application when the CPU starts. To support this, the system is configured to operate in the Connex CS Shell mode. This shell mode blocks general users access to Windows functions, such as the Windows key, Ctrl+Alt+Delete, and Alt+Tab.

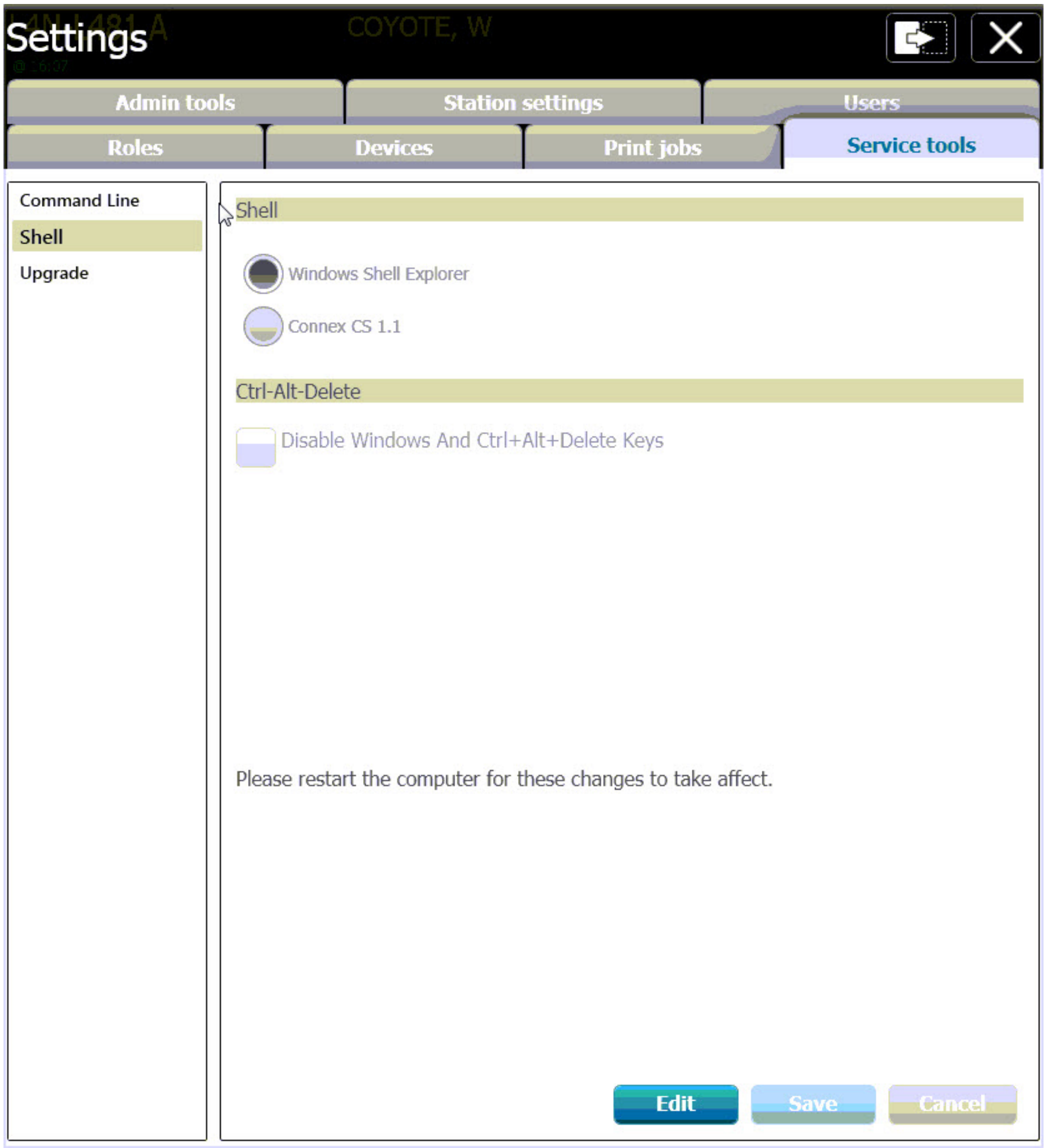
Windows functions are accessible from a command line tool built into the Settings tools, and described within this chapter.

NOTE It is recommended to make network changes, such as IP address settings, with the system configured for Windows shell.

To change the shell mode:

1. On the navigation area, click on **Settings > Advanced settings**. The login screen appears.
2. Login using your User ID and Password information. Upon success the Settings window appears.
3. Click on the **Service Tools** tab.
4. Click on **Shell**. The shell mode window appears. Select **Edit** to make changes. An example is shown below in "Figure 6-1: Shell mode configuration screen example" on page 22.
5. Select the **desired shell** by clicking on the corresponding **radio button**.
6. It is also desirable to **deselect** the check box next to **Disable Windows and Ctrl+Alt+Delete keys** if the system will be operating in **Windows shell** for configuration or maintenance activities.
7. Click **Save** when done. A confirmation window appears.
   - Select **Yes** to save changes and reboot now.
   - Select **No** to save changes without reboot.
   - Select **Cancel** to continue without saving changes.
8. Upon restart, the system starts with a normal PC Windows desktop display after login.
9. When all work in the Windows shell is complete, revert the system back to Connex CS shell prior to clinical usage.

Figure 6-1: Shell mode configuration screen example



Shell

● Windows Shell Explorer

○ Connex CS 1.1

Ctrl-Alt-Delete

□ Disable Windows And Ctrl+Alt+Delete Keys

Please restart the computer for these changes to take affect.

Network Changes

The change in the IP Address of one or more systems involved in Connex CS network will cause many components to break. This requires updating the specific configurations in the system used by such components. See Section J for more information.

Due to complexity of these level of changes, these scenarios are best managed by trained Welch Allyn staff, and may require planning for down-time. Please consult with your Welch Allyn Project Manager or Technical Support for additional information.

Add a Customer Supplied Printer

It may be necessary to add a printer on-site, especially in the case of using a customer provided or shared network printer.

It is the facility responsibility to provide a driver for the printer.

Consult with the facility IT staff to identify the network printer and obtain a driver compatible with Windows 7 - 64 bit. Refer to the ***Connex CS Customer Project Req. Form*** for network information.

To install a printer on the central station:

1. Ensure the printer is turned on and accessible on the network.
2. Open a command line interface window and ping the printer by the IP address to confirm that it is reachable.
3. Install the print driver provided by the facility.
   a. Use the Connex server internal CD/DVD ROM drive for optical media.
   b. Use one of the USB ports on the front panel for USB flash drive media.

Install print driver from an executable.EXE file

1. If the customer has provided CD/DVD media which will automatically run, follow the steps and prompts as provided.
2. If the customer has provided media with an .exe file type, double click on the file to start the installer. Follow the steps and prompts as provided.

Install print driver from a media with an .INF file

Use the Windows functions to Add a printer:

1. Click **Start > Control Panel > View devices and printers**.
2. Click on **Add a printer**.
3. Select **Add a network, wireless, or Bluetooth printer**.
4. Windows begins a search for known printers.

If the desired printer is found using search:

1. Select **Stop** when the printer appears in the search window.
2. Click on the printer, and then select **Next**.
3. Change the name of the printer as desired and select Next.
4. For printer sharing, select an option and then select Next.
5. Select **Print a test page**. and then select **Finish**.
6. Confirm that a test print was printed by the printer.
7. The printer appears in the Control Panel Printers and Faxes window.

If the printer was not found using search:

1. Click **The printer that I want isn't listed**.
2. Select the radio button next to **Add a printer using a TCP/IP address or hostname**, and then select **Next**.
3. Leave Device type as **Autodetect**.
4. Enter the **IP address** of the printer.
5. Ignore the Port name, and select **Next**.
6. Select the printer manufacturer and model from the menus.
7. If the printer is not listed, select **Have Disk**, and browse to the location of the .INF driver file. Select **OK** when ready.
8. Click on the **printer**, and then select **Next**.
9. Change the name of the printer as desired and select **Next**.
10. For printer sharing, select an option and then select **Next**.
11. Select **Print a test page**. and then select **Finish**.
12. Confirm that a test print was printed by the printer.
13. The printer appears in the Control Panel Printers and Faxes window.
14. If more than one printer is installed, choose a printer to set as the default.

Change Date, Time, and Time zone

It may become necessary to adjust the date and time to local settings. Use standard Windows control functions to adjust the date, time, and time zone settings as necessary.

⚠ **CAUTION** Date, time, and time zone settings must be set identical on the Central Station, Connex server, and attached devices. If time, date, and time zone settings are not the same, devices may not be able to communicate with the Central Station or Connex server.

1. For a standalone Central Station, the Internet Time tab will be available.
   a. Click on **Internet time > Change settings**.
   b. Click on **Synchronize** with an Internet time server.
   c. Use the drop down list to select **time.nist.gov**.
   d. Click **Update now** and confirm that the time is updated.
2. Click **OK**, and apply all changes when finished.
3. For a network that includes a Central Station, and Connex server, refer to "Time Synchronization" on page 95 for additional information as needed.

7 Backup & Restore

Backup users and configuration

The Administration tool tab has functionality to backup and restore configuration information for the system and users. Tasks may be completed at any Connex Central Station or the Connex server, and only needs to be done once for the entire network of central stations and Connex server.

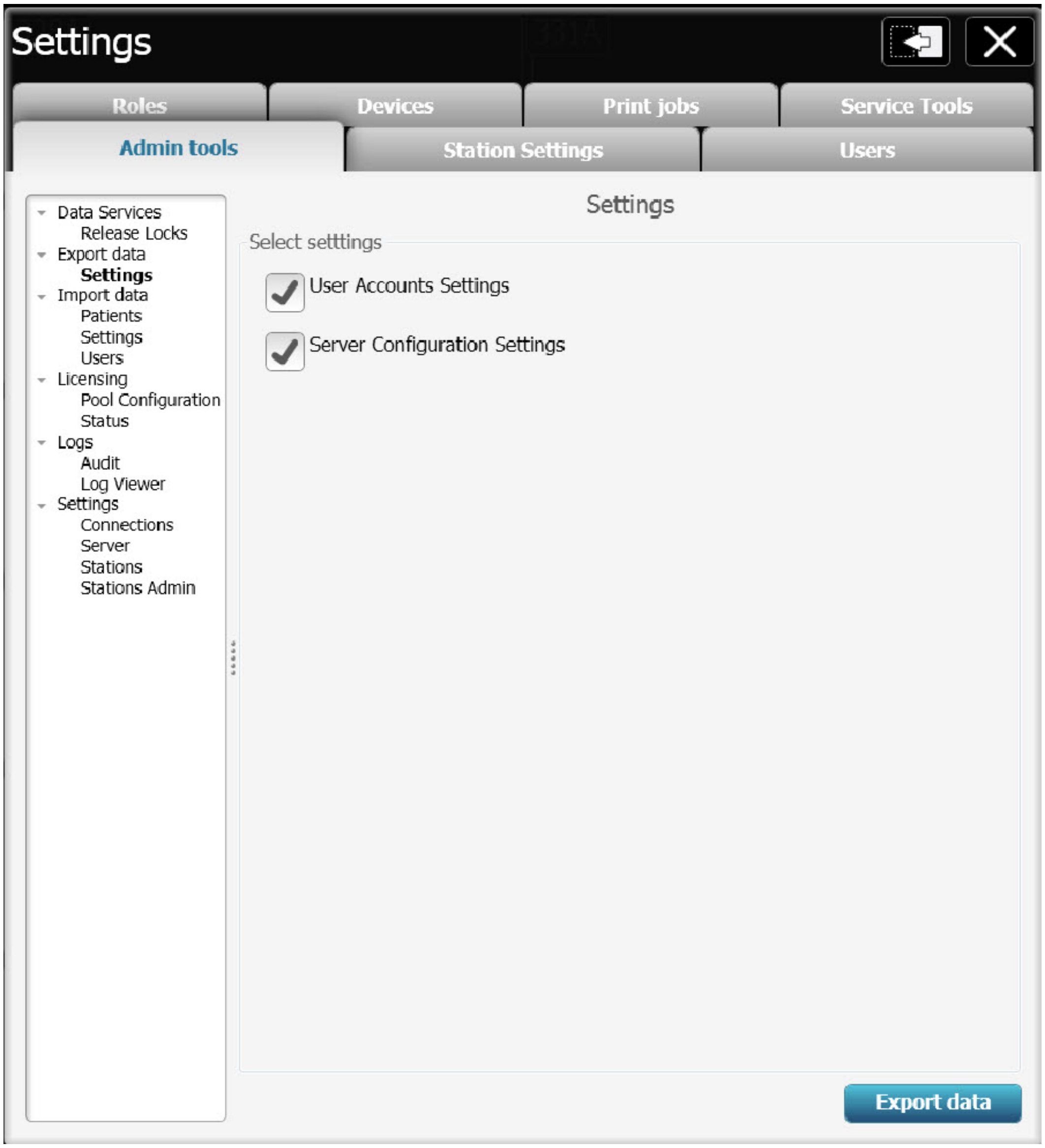
NOTE The export data and settings functions described in this section create an output of a single XML file, where all information is combined. In some situations it may also be desirable to create separate export (backup) files User Account Settings and Server Configuration Settings.

1. To make a local backup of Connex CS users and configuration information:
2. On the navigation area, click on **Settings**. The login screen appears.
3. Login using your administration account User ID and Password information. Upon success the Settings window appears.
4. Select the **Admin tools tab** > **Export data** > **Settings**. The Settings window appears. An example is shown in "Figure 7-1: Export data settings users and configuration window" on page 26.

Select **User Account Settings** and/ or **Server Configuration Settings** per desired.

NOTE If both Users and Configurations are selected, the output will be combined in to a single XML file. In some situations it may also be desirable to create separate export (backup) files User Account Settings and Server Configuration Settings.

Figure 7-1: Export data settings users and configuration window



Settings

Select setttings

☑ User Accounts Settings

☑ Server Configuration Settings

1. Select **Export data**.
2. Navigate to the USB flash drive. Choose a folder location for the backup.
3. Choose a file name for the saved file. By default, the file will be called WAConfigurationSettings.xml, but should be changed to the following format for consistency:
    - **System S/N . Backup type. Country or State . Facility Name . Covered Area . Date**
    - An example – CN01087.config&users.NY.CrouseHospital.AllHosts.2012.08.09.xml
4. Also save a local copy on the system at the following location:
    - **C:\ProgramData\Welchallyn\@Config.Backup**.

NOTE ProgramData is typically a hidden file. You may need to type location by hand into the folder location bar using the keyboard.

NOTE The folder **@Config.Backup** may not exist if this is a new installation. Create this folder as necessary.

5. Upon success, click **OK**.

Nightly System Backup

By default, all Connex CS system computers are configured to backup their database to a local source (same host) at approximately 12:00 am (midnight).

The Connex Data Backup runs on stand-alone Central Stations and Servers.

For stand-alone Central Stations, database backups can be found at the following location in the file system:

C:\Program Files\Microsoft SQL Server\MSSQL10_50.SQLExpress\MSSQL\Backup, where MSSQL10_50.SQLxxx is the main SQL version installed.

For Connex server, database backups can be found at the following location in the file system:

C:\Program Files\Microsoft SQL Server\MSSQL10_50.SQLSTANDARD\MSSQL\Backup, where MSSQL10_50.SQLxxx is the main SQL version installed.

Backup Corepoint configuration - create a NIX file

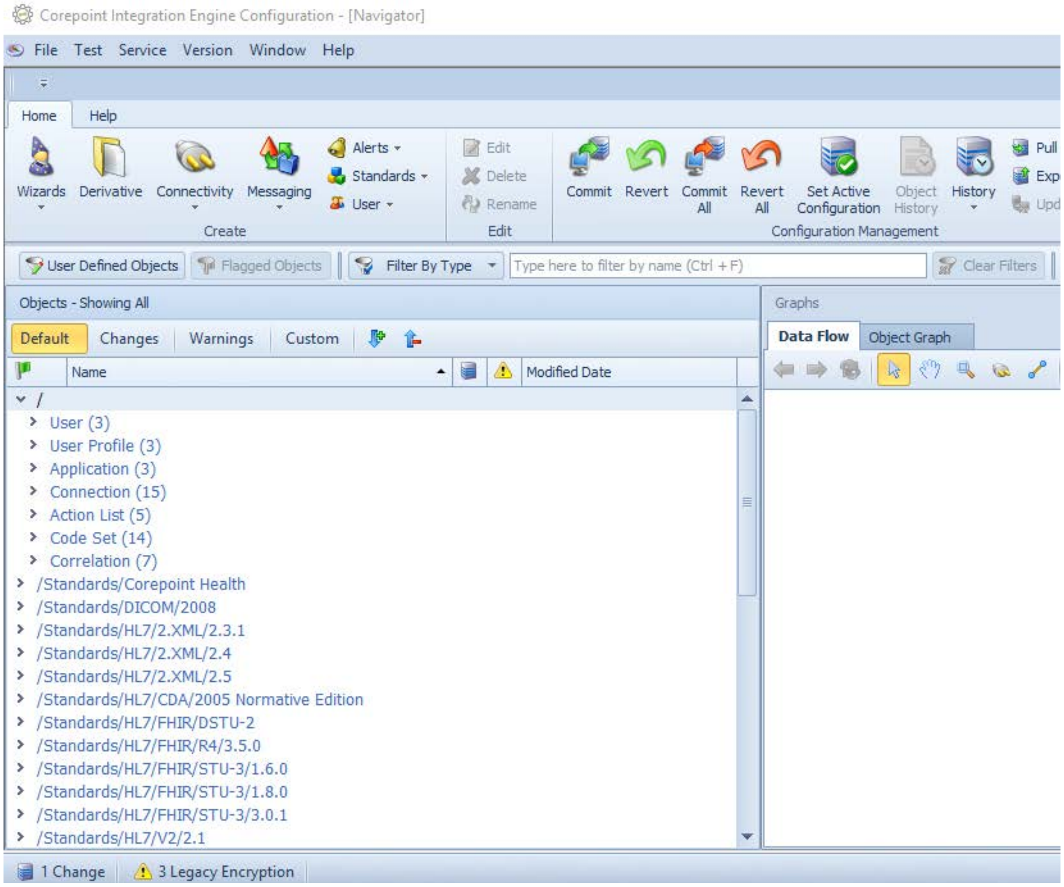
Create a backup of the current Corepoint configuration, which may be needed if replacing the system hardware in the event of failure.

NOTE These steps only apply if the Closet Service is licensed and configured to support HL7 interfaces, including ADT and/or ORU connections

1. On the Connex server, go to **Start** > **Corepoint Health** > **Configuration** to launch the configuration tool.

2. Login as Manager. The Corepoint Integration Engine Configuration tool appears.

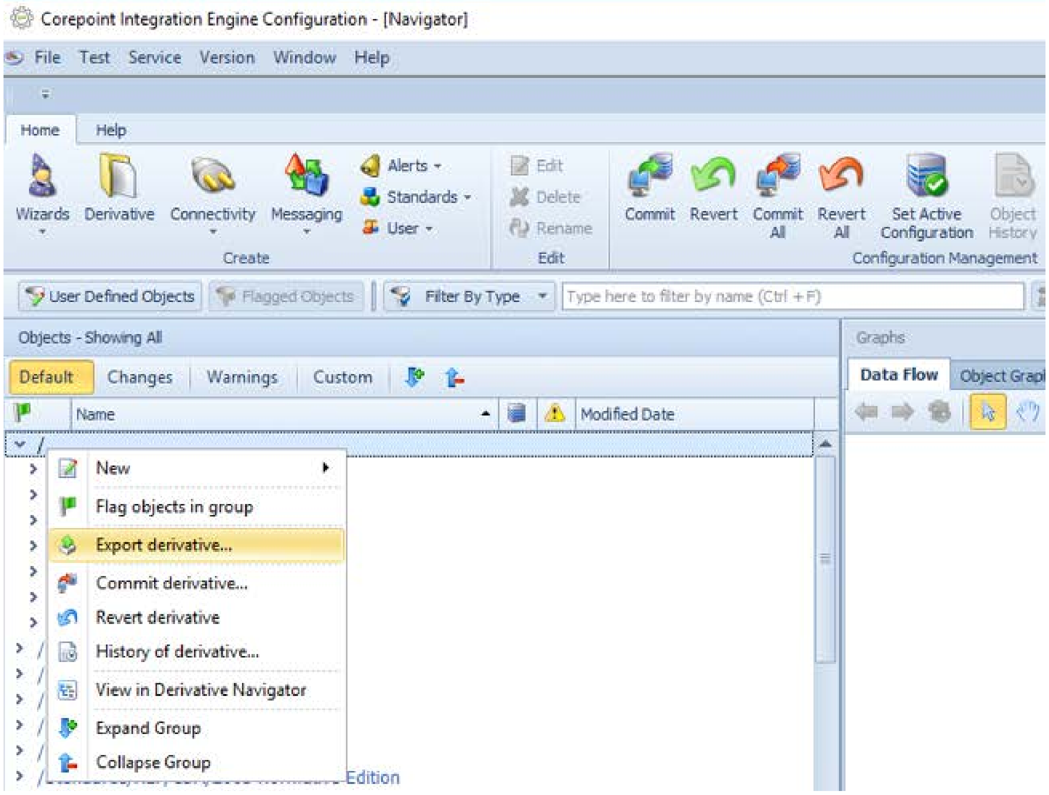
Figure 7-2: CIE configuration tool main display with navigator window example



3. In the navigator window, locate the **Objects** area on the left side of the window.

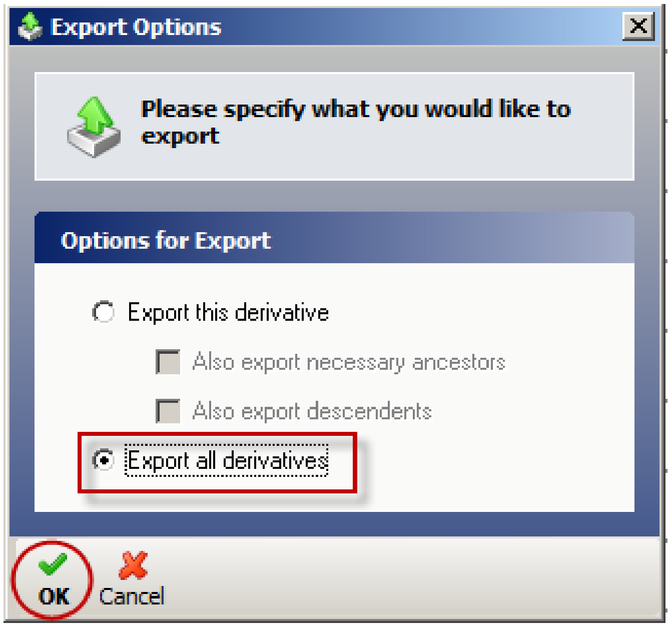
4. Right-click on the **root directory** /. An example is shown below.

Figure 7-3: Right-click on the root to open


Corepoint Integration Engine Configuration - [Navigator]
File Test Service Version Window Help
Home Help
Wizards Derivative Connectivity Messaging Alerts Standards User
Create
Edit Delete Rename
Edit
Commit Revert Commit All Revert All Set Active Configuration Object History
Configuration Management
User Defined Objects Flagged Objects Filter By Type Type here to filter by name (Ctrl + F)
Objects - Showing All
Default Changes Warnings Custom
Name Modified Date
Graphs
Data Flow Object Graph
New
Flag objects in group
Export derivative...
Commit derivative...
Revert derivative
History of derivative...
View in Derivative Navigator
Expand Group
Collapse Group
Edition

5. Click on **Export**. The export options window appears.

Figure 7-4: Corepoint export options window



Please specify what you would like to export

○ Export this derivative

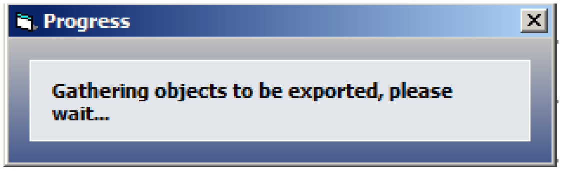
□ Also export necessary ancestors

□ Also export descendents

● Export all derivatives

6. Click on the option for **Export all derivatives**. Then click **OK**. The progress window appears momentarily.

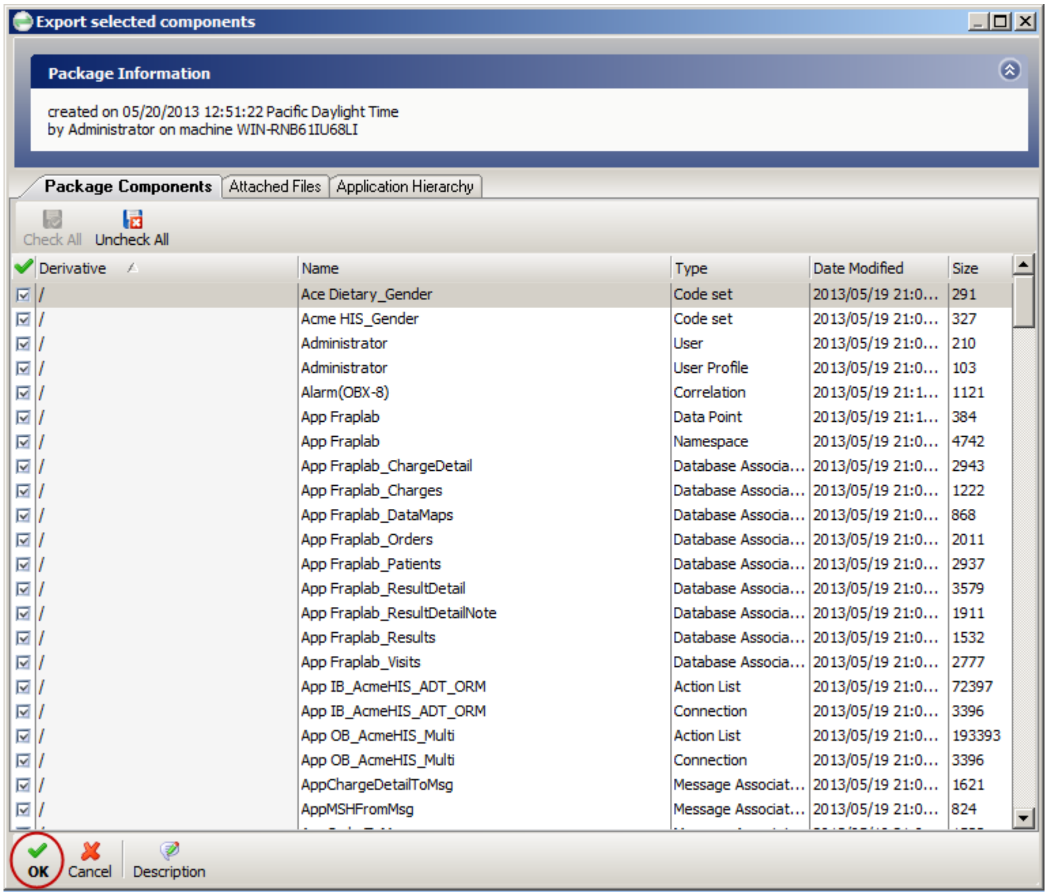
Figure 7-5: Corepoint export files being prepared



Gathering objects to be exported, please wait...

7. After a short while, the export selected components window appears.

Figure 7-6: Corepoint export select components window example

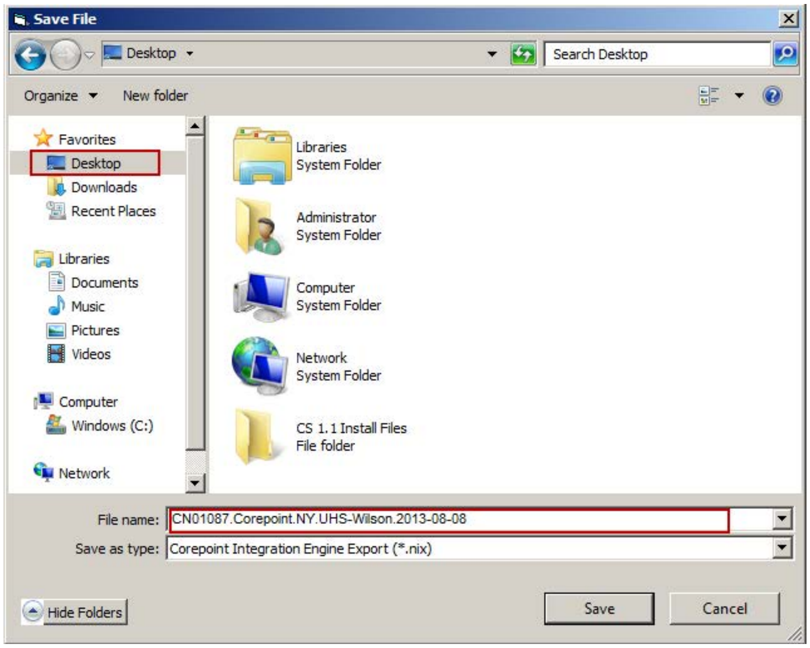


created on 05/20/2013 12:51:22 Pacific Daylight Time
by Administrator on machine WIN-RNB61IU68LI

✓	Derivative	Name	Type	Date Modified	Size
☑	/	Ace Dietary_Gender	Code set	2013/05/19 21:0...	291
☑	/	Acme HIS_Gender	Code set	2013/05/19 21:0...	327
☑	/	Administrator	User	2013/05/19 21:0...	210
☑	/	Administrator	User Profile	2013/05/19 21:0...	103
☑	/	Alarm(OBX-8)	Correlation	2013/05/19 21:1...	1121
☑	/	App Fraplab	Data Point	2013/05/19 21:1...	384
☑	/	App Fraplab	Namespace	2013/05/19 21:0...	4742
☑	/	App Fraplab_ChargeDetail	Database Associa...	2013/05/19 21:0...	2943
☑	/	App Fraplab_Charges	Database Associa...	2013/05/19 21:0...	1222
☑	/	App Fraplab_DataMaps	Database Associa...	2013/05/19 21:0...	868
☑	/	App Fraplab_Orders	Database Associa...	2013/05/19 21:0...	2011
☑	/	App Fraplab_Patients	Database Associa...	2013/05/19 21:0...	2937
☑	/	App Fraplab_ResultDetail	Database Associa...	2013/05/19 21:0...	3579
☑	/	App Fraplab_ResultDetailNote	Database Associa...	2013/05/19 21:0...	1911
☑	/	App Fraplab_Results	Database Associa...	2013/05/19 21:0...	1532
☑	/	App Fraplab_Visits	Database Associa...	2013/05/19 21:0...	2777
☑	/	App IB_AcmeHIS_ADT_ORM	Action List	2013/05/19 21:0...	72397
☑	/	App IB_AcmeHIS_ADT_ORM	Connection	2013/05/19 21:0...	3396
☑	/	App OB_AcmeHIS_Multi	Action List	2013/05/19 21:0...	193393
☑	/	App OB_AcmeHIS_Multi	Connection	2013/05/19 21:0...	3396
☑	/	AppChargeDetailToMsg	Message Associat...	2013/05/19 21:0...	1621
☑	/	AppMSHFromMsg	Message Associat...	2013/05/19 21:0...	824

8. Leave all settings in the above window at **default**, with **all items selected**. Click **OK** to proceed. The save file window appears.

Figure 7-7: Save file window example



File name: CN01087.Corepoint.NY.UHS-Wilson.2013-08-08

Save as type: Corepoint Integration Engine Export (*.nix)

9. Click on **Desktop** to place the backup file directly on the desktop, making the backup easy to locate if needed later.

10. Type a **File name** for the backup.

11. Choose a file name for the saved file. Follow the recommended naming schema below to maintain consistency:

    - **Network S/N.Corepoint.Country or State.Facility Name.Date**
    - An example – CN01087.Corepoint.NY.UHS-Wilson.2013.08.08

12. Also save a local copy on the system at the following location:

    - **C:\ProgramData\Welchallyn\@Config.Backup**.

NOTE **ProgramData** is typically a hidden file. You may need to type location by hand into the folder location bar using the keyboard.

NOTE The folder **@Config.Backup** may not exist if this is a new installation. Create this folder as necessary.

13. Leave the type of file at default, as displayed in the above example (*.nix). Click Save when ready.

14. **Confirm** the presence of the file as displayed on the desktop.

Backup Corepoint HL7 License

1. Open a Windows Explorer window.

2. Navigate to **C:\Program Files (x86)\Corepoint Health\Corepoint Integration Engine\License**.

3. Make a copy of the license file **CorepointEngine.lic** and place it in backup folder on the Desktop.

Restore Patients and Users

The Administration tool tab has functionality to backup and restore configuration information for the system and users. Tasks may be completed at any Connex Central Station or the Connex server, and only needs to be done once for the entire network of central stations and Connex server.

NOTE The import patients settings and users functions described in this section restore functions from input files previously saved or created off-line. Use care to select the proper file for import functions (restore).

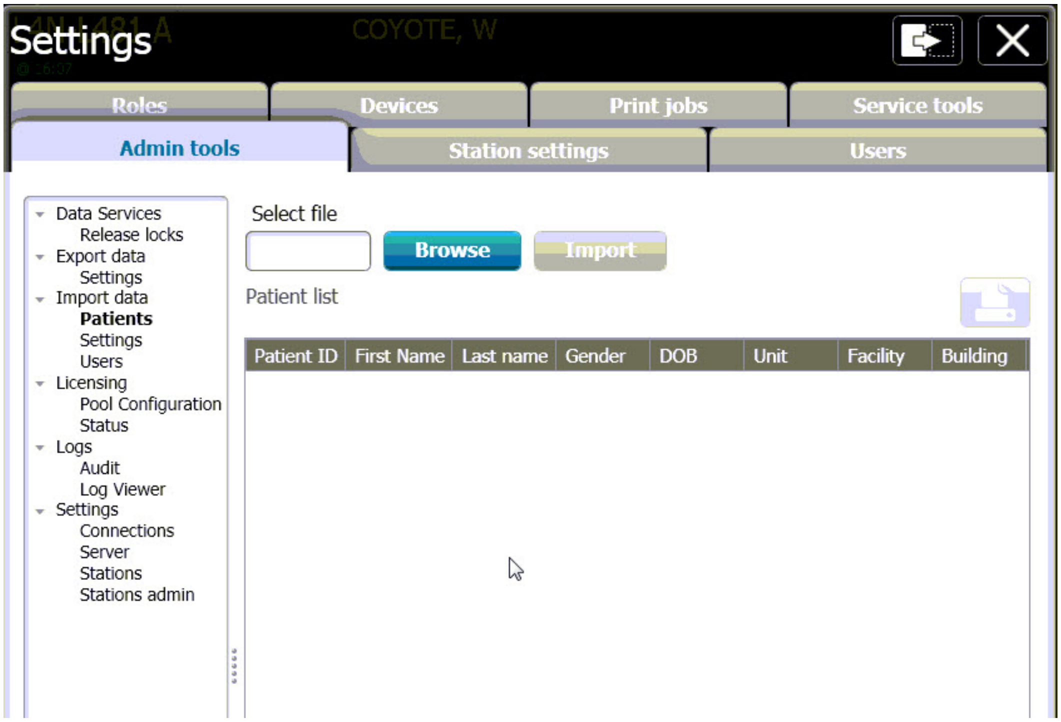
CAUTION Importing of patients is not used for standard clinical workflow, but is described herein and may be used for exercise during testing or demonstration purposes.

1. To restore Connex CS patients or users:
2. On the navigation area, click on **Settings**. The login screen appears.
3. Login using your account User ID and Password information. Upon success the Settings window appears.
4. Select the **Admin tools tab** > **Import data** > **Patients** or **Users**. The select file window appears. Select **Browse** and navigate to the import source file location. An example is shown below in "Figure 7-8: Import data Patients list window example" on page 33.

   NOTE Users list import functions support CSV type files only.

5. See "Creating a User list" on page 34 for additional information as needed.
6. See "Creating a User list" on page 34 for additional information as needed.
7. Select the file, and select **Open**.
8. The selected file name appears in the Import data window Select file area. Select **Import**, and **confirm** the select.
9. **Restart** for changes to take affect.

Figure 7-8: Import data Patients list window example



Restore Settings

The Administration tool tab has functionality to backup and restore configuration information for the system. Tasks may be completed at any Connex Central Station or the Connex server, and only needs to be done once for the entire network of central stations and Connex server.

To restore Connex CS settings:

1. Insert a USB flash drive into one of the USB ports on the CPU front panel.
2. On the navigation area, click on **Settings**. The login screen appears.
3. Login using your account User ID and Password information. Upon success the Settings window appears.
4. Select the **Admin tools tab** > **Import data** > **Settings**. The select file window appears. Select **Browse** and navigate to the import source file location.

NOTE Settings list import functions support XML type files only.

5. Select the file, and select **Open**.
6. The selected file name appears in the Import data window Select file area. Select **Import**, and **confirm** the select.
7. **Restart** for changes to take affect.

Creating a User list

A user list may be created off-line using standard office productivity software (e.g. Microsoft Office Excel) and saved in a comma separated variable format for importing a larger list of users.

Import users from a CSV format requires the following columns of data:

- SettingsGroup – Specifies group for user roles.
- Suffix – Specifies suffix for user roles, includes “Jr.”, “Sr.”.
- Title – Specifies user title, includes “Dr.”, “Mr.”, “Mrs.”, “Miss”.
- UserName – Specifies user name uniquely identified throughout the application.
- ClinicianNumber – Specifies clinician number.
- FirstName – Specifies first name of user.
- MiddleName – Specifies middle name of user.
- LastName – Specifies last name of user.
- IsActive – Specifies whether user is active or not.
- PasswordChangeRequired – Specifies whether user needs to change password while logging in for the first time.
- Clinician – Specifies whether user has “Clinician” role or not.

The following text block example below describes the format required within the first line, which is also a required line at the top of the CSV file.

```
SettingsGroup,Suffix,Title,UserName,ClinicianNumber,FirstName,MiddleName,LastName,IsActive,PasswordChangeRequired,Clinician
Physician,Jr.,Dr.,andersoa,00105602,Thomas,A,Anderson,TRUE,TRUE,TRUE
Clinician,,,greenes,00105623,Sally,,Greene,TRUE,TRUE,TRUE
Biomed,,,jamesont,0020041,Timothy,,Jameson,TRUE,TRUE,TRUE
Nurse Manager,,,duckworm,00100921,Marsha,,Duckworth,TRUE,TRUE,TRUE
```

NOTE It is important to confirm that the CSV file is precise. The first line must be exactly as specified. Review the user data to ensure that it reads exactly as expected, including leading zeros.

8 Location Management

Connex CS applications are structured around a flexible hierarchy used to establish a logical location for assignment for patients within the system. The following definitions describe some of the functions and relationship of each within the hierarchy.

Item	Description
Station	A logical system that can be used to service a covered area
Master Bed List	A complete list of all available beds to be managed by Connex. In a stand-alone system, all beds are known to the single central station. In a multi-system environment, all beds are known to the server.
Covered Area	A grouping of beds from the master list that can be covered or monitored by a Connex CS central station. Each central station is configured to support a single covered area.
Warm Spare	An installation of Connex CS application software that has not yet been configured or assigned to a station.
Host	A physical computer (PC) on which the Connex Central Station application software is installed.

⚠ **CAUTION** Making changes to settings in Location Management may cause interruptions in patient monitoring. Do not change Location Management settings without contacting Hillrom Technical Support. These steps are informational only, and included to support your understanding of the current system configuration.

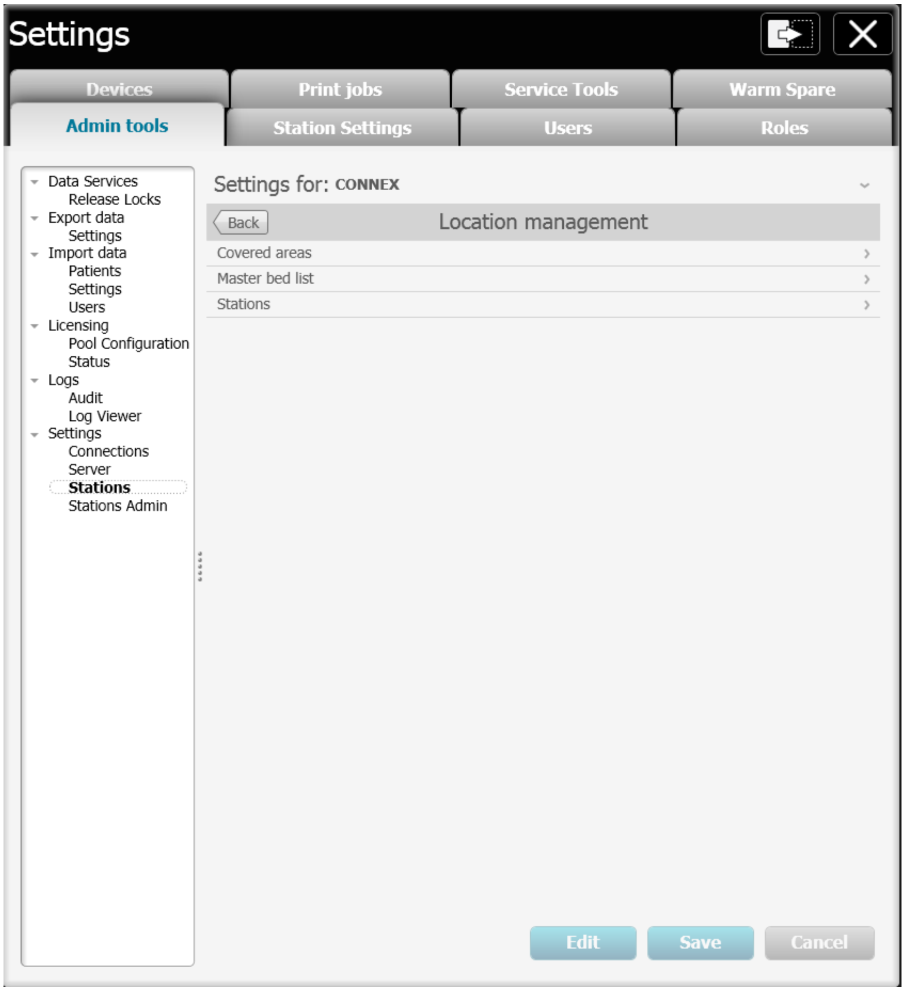
Add a Station

Though generally not the case, stations can exist and be configured without being applied to a host computer.

To add a station:

1. On the navigation area, click on **Settings**. The login screen appears.
2. Login using your assigned administrative level account User ID and Password information. Upon success the Settings window appears.
3. Select the **Admin tools** tab. From the left side menu, select **Stations**, nested under Settings.
4. Select **Location management**. The Location management window appears. An example is shown below in "Figure 8-1: Location management window example" on page 36.

Figure 8-1: Location management window example

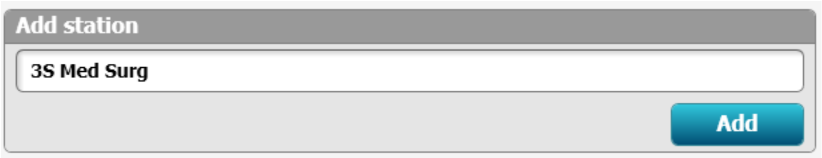


5. Click on **Stations**. The Stations window appears.

6. To add a station, first click on **Edit** near the bottom of the window.

7. To add a new station, click in the **Add station field** and **type** a name for the station. Refer to the ***Connex CS Customer Project Req. Form, Appendix B2*** as needed to determine the proper entry for the station.

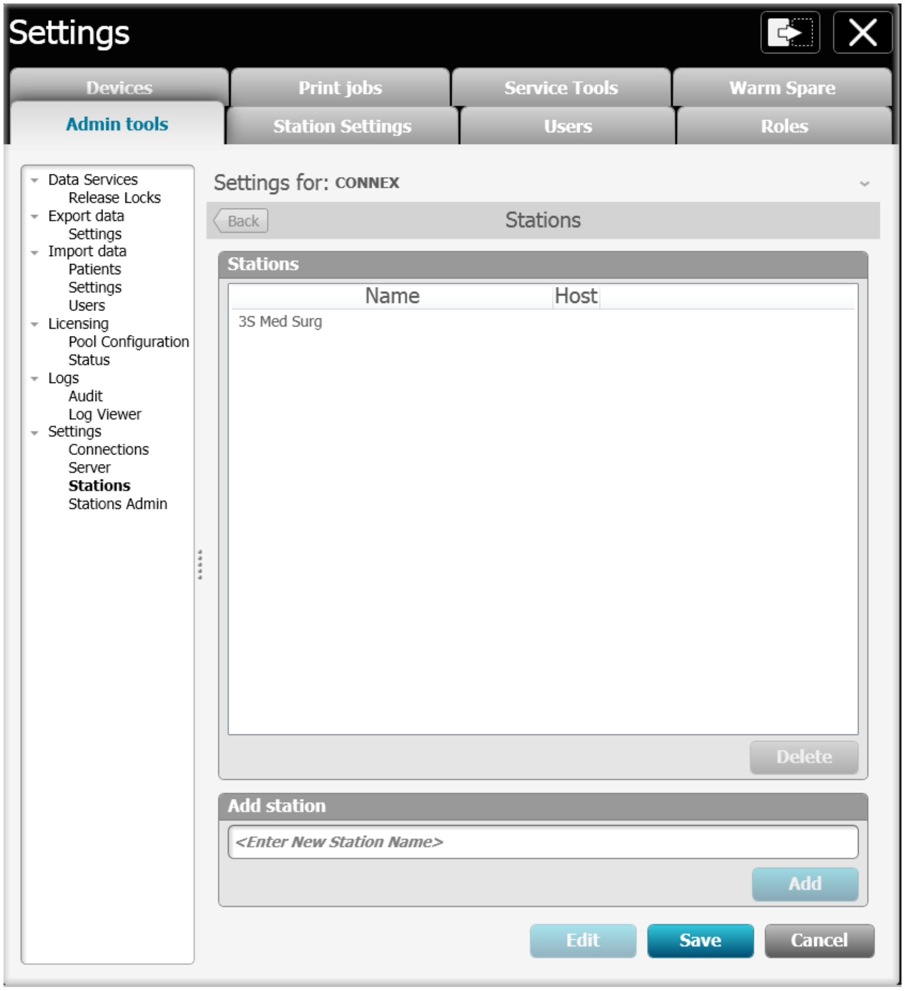
Figure 8-2: Add Station window



3S Med Surg

8. Click **Add** when finished. The station name now appears in the Stations window by name. An example is shown below in "Figure 8-3: Newly added station example" on page 37.

Figure 8-3: Newly added station example



Settings for: CONNEX

Stations

Stations

Name	Host
3S Med Surg	

Add station

<Enter New Station Name>

9. Click **Save** when finished.

10. Click on the **Back** button in the window header.

Add a Master bed list

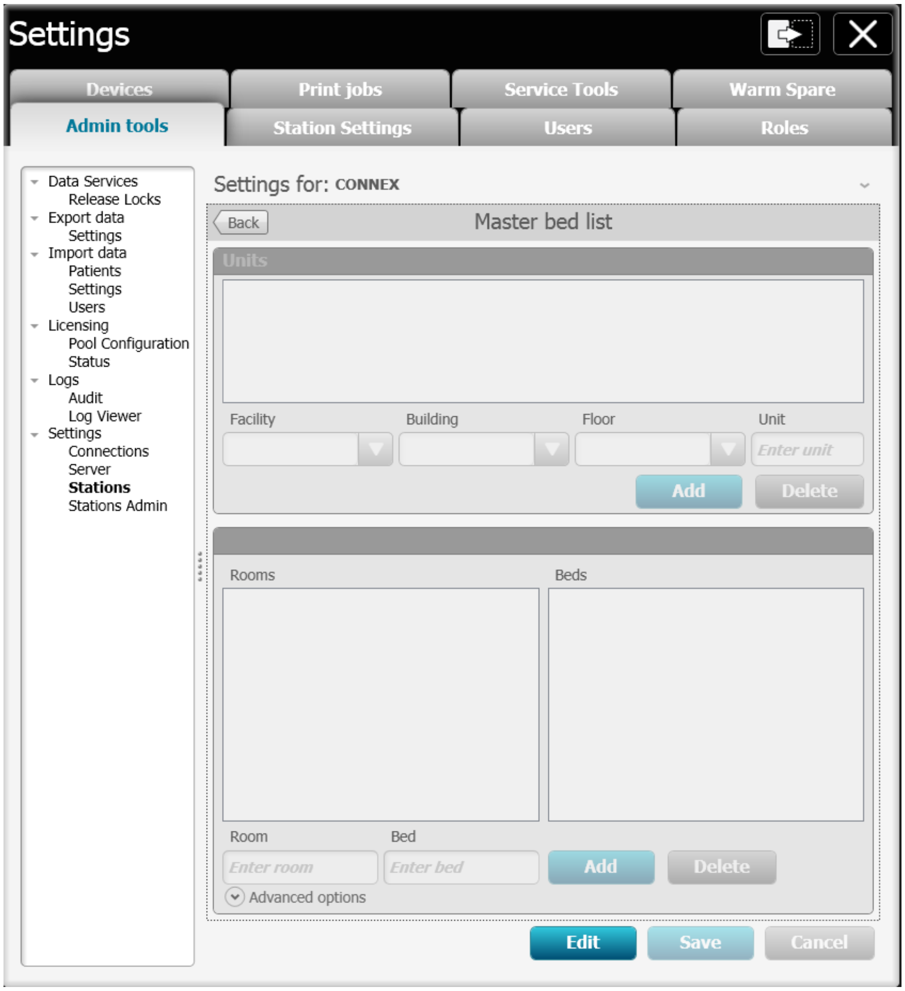
Within the master bed list exists another hierarchy structure for rooms and beds. All locations with Connex CS are defined by their names for Facility, Building, Floor, Unit, Room and Bed.

⚠ **CAUTION** Any time changes are made to the Master Bed List, Covered Area, or Licensing, the affected Central Station should be restarted prior to clinical usage.

To add a master bed list:

1. From the **Settings** > **Advanced settings** (if required) > **Admin tools** > **Stations** > **Location management** menu, click on **Master bed list**. The Master bed list window appears. An example is shown below in Figure 8-4.

Figure 8-4: Master bed list default window example



2. Observe that there are two sub-windows within the Master bed list main window.

3. Click on **Edit** near the bottom of the window.

4. Create a new Master bed list if there are no Units present.

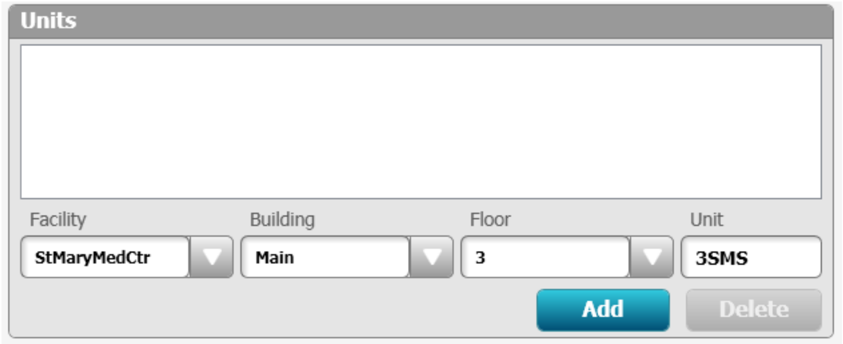
⚠ **CAUTION** Fields in the Master bed list control which units, rooms, and beds appear on the Central Station and associated patient monitors. In a networked environment with more than one Central Station, the Master bed list controls this information for all systems. Always refer to the ***Connex CS Customer Project Req. Form*** when entering information in these fields.

⚠ **CAUTION** If the system is configured with an ADT interface to the facility's EMR application, location fields for **Facility, Building, Floor,** and **Unit** must match exactly with the ADT messages. Use a dash "-" to denote a null field if the facility's ADT feed does not send specific data. **Data mis-matches in these location fields will result in no patients appearing in the Connex CS application Patient List.**

Create a New Unit

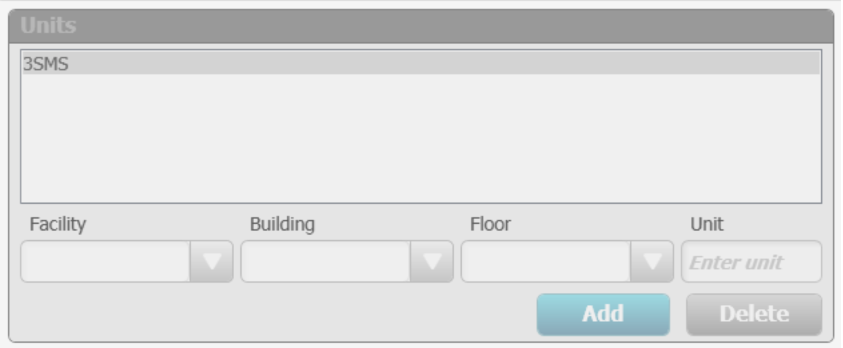
1. In the Units window, click in the **Facility** field and enter the facility name.
2. Continue for the **Building**, **Floor**, and **Unit** fields. An example is shown below in "Figure 8-5: Facility, Building, Floor and Unit entry field examples".
3. When finished, click **Add**. A new entry for the Unit appears in the Units window. See "Figure 8-6: Newly created Unit example".

Figure 8-5: Facility, Building, Floor and Unit entry field examples



Facility: StMaryMedCtr
Building: Main
Floor: 3
Unit: 3SMS

Figure 8-6: Newly created Unit example



3SMS

Enter unit

Add a New Room and Bed

In the Units window, click on the newly created Unit name, 3SMS in the above example. The Unit name appears in the header for the lower Room and Bed windows.

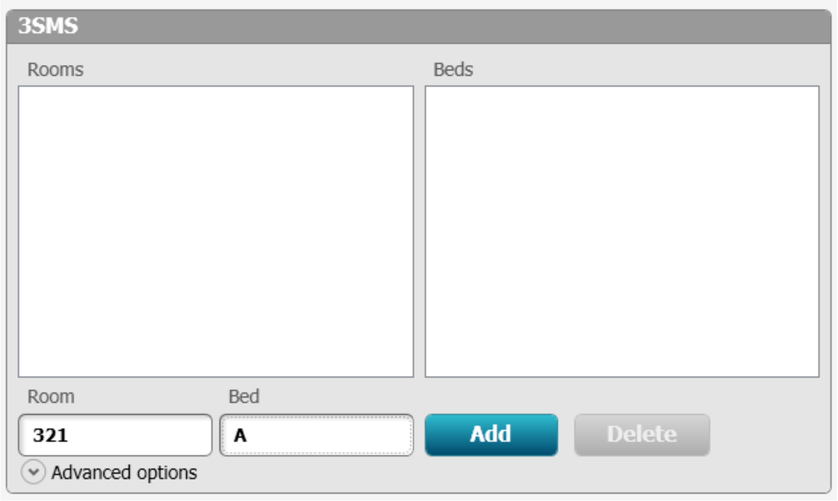
There are a number of different methods that can be used to add a room and bed including:

- Add a single room and bed.
- Add a range of rooms and beds.
- Change room and bed values.
- Copy rooms and beds info from a CSV file.

To add a single room and bed:

1. In the Master bed list window, click **Edit** to make changes.
2. Click in the **Room** field and enter a Room number.
3. Click in the **Bed** field and enter a Bed name. See Figure 8-7 for an example.

Figure 8-7: Single Room and Bed entry fields example



Room: 321

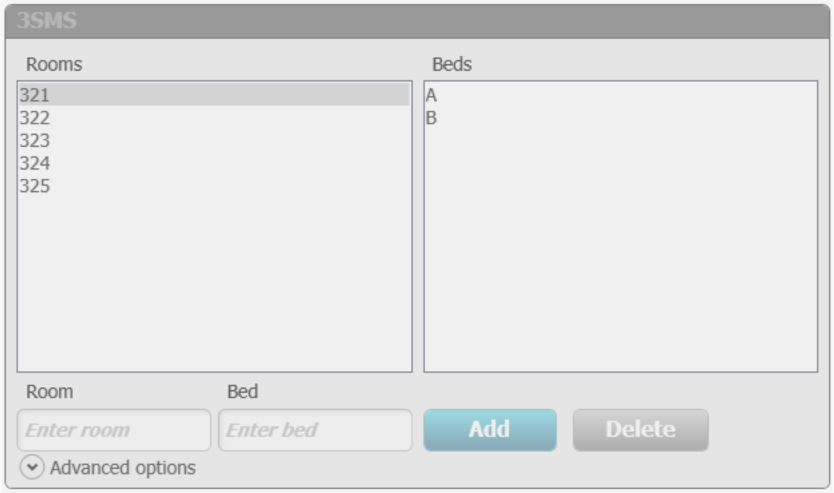
Bed: A

4. Click **Add**. Then new room and bed information appear in the respective fields.
5. Repeat steps 1 through 3 to additional rooms and beds. See Figure 8-8 for an example.

NOTE Rooms and beds will be displayed in descending order for the Unit, not the order in which they were entered.

6. Click **Save** when finished.

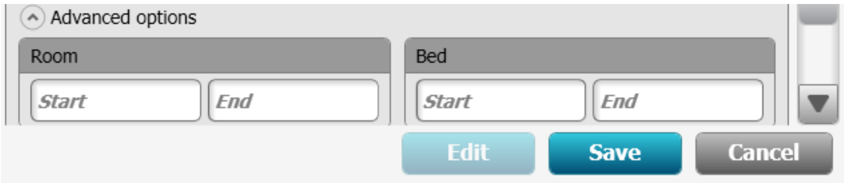
Figure 8-8: Newly added Room and Bed examples



To Add a Range of Rooms and Beds

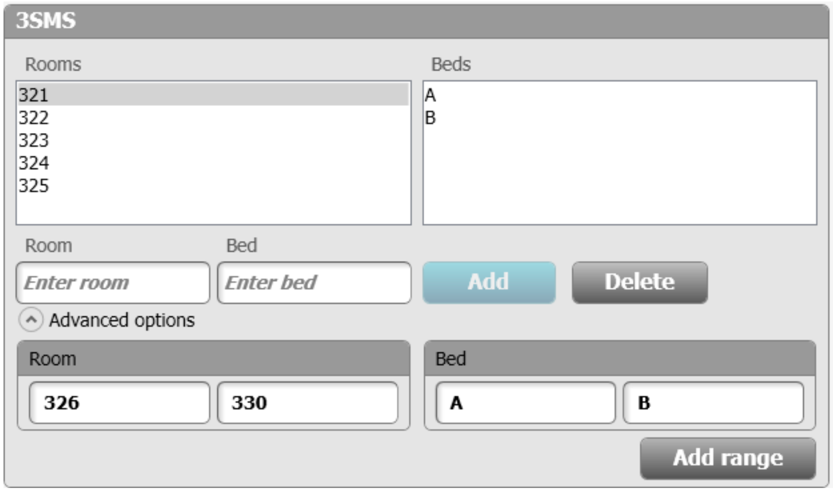
1. In the Master bed list window, click **Edit** to make changes.
2. Click on the **expander to the left of Advanced options**. Two additional windows appear. An example is shown in Figure 8-9.

Figure 8-9: Advanced options default



3. Click in the **Room *Start*** field to enter the first room number of a range.
4. Click in the **Room *End*** field to enter the last room number of a range.
5. Click in the **Bed *Start*** field to enter the first bed name of the range.
6. Click in the **Bed *End*** field to enter the last bed name of the range. An example is shown in Figure 8-10.

Figure 8-10: Advanced options default



Rooms: 321, 322, 323, 324, 325

Beds: A, B

Room		Bed	
326	330	A	B

7. Click **Add range** when finished. The new range of beds and rooms appears in the list.

NOTE Ranges of beds and rooms must be continuous. The Add range function may be used as many times as needed. Single rooms and beds may be specified by using the same start and end value (i.e. Room 318 - 318).

8. Click **Save** when finished.

To change Room or Bed values:

1. In the Master bed list window, click **Edit** to make changes.

NOTE When making changes to rooms and beds ensure that the bed is not currently in use or assigned to a patient.

2. If corrections are needed to a room value, click on the room to be changed and then click **Delete**.
3. A pop-up window appears asking to confirm the removal. Click **Yes** to confirm the removal, or **No** to cancel.
4. Re-enter the room and bed information as needed.

NOTE Removal of a room with more than one bed will also all remove all associated beds.

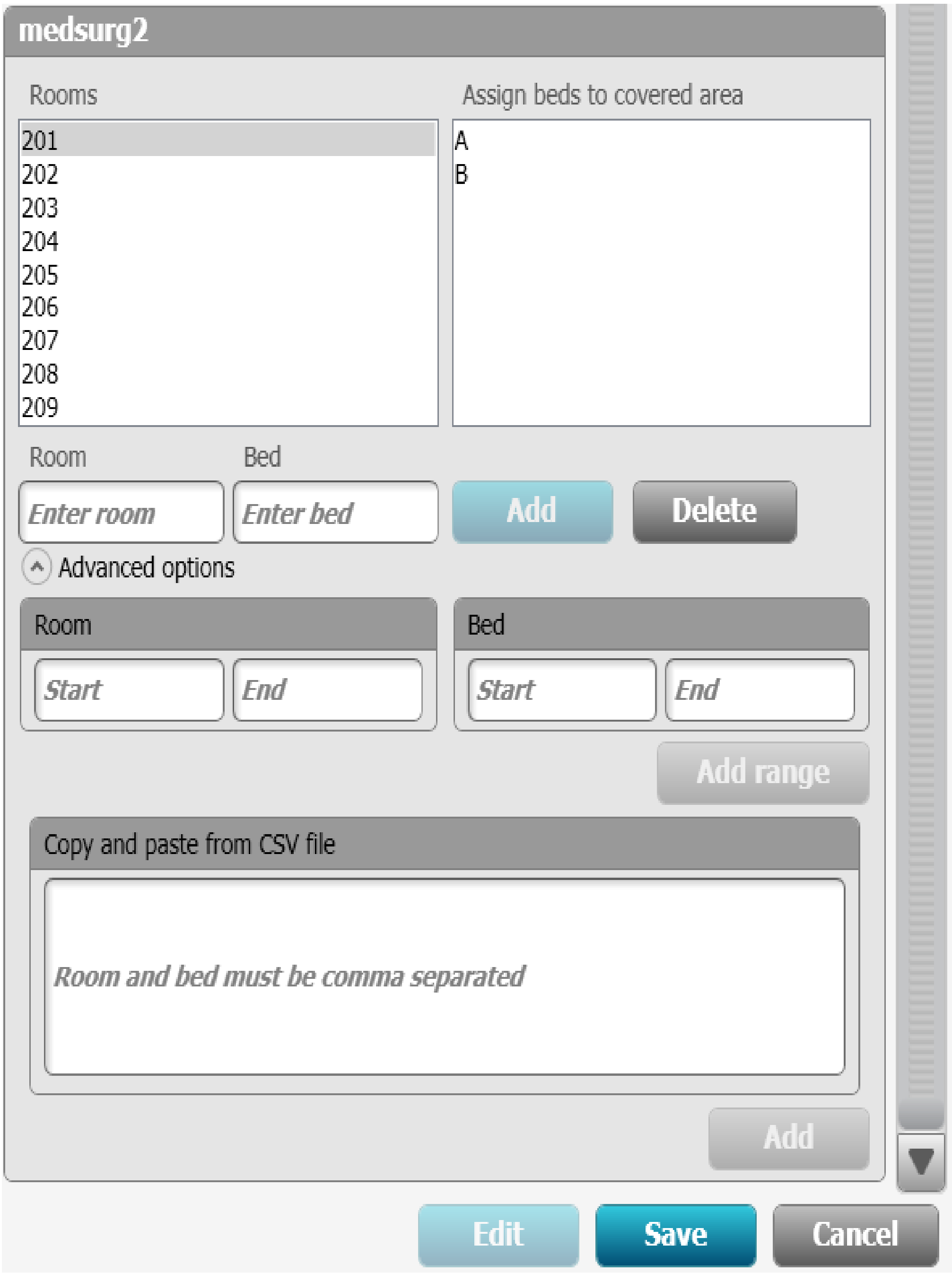
5. If corrections are needed to a single bed value, click on the room and bed to be changed and then click **Delete**.
6. A pop-up window appears asking to confirm the removal. Click **Yes** to confirm the removal, or **No** to cancel.
7. Re-enter room and bed information as needed.

To copy from a CSV file to add rooms and beds

Thisfeature is available beginning in Connex CS v1.2 and higher.

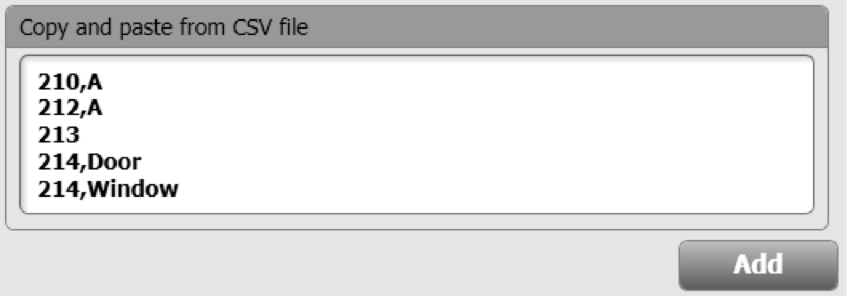
1. In the Master bed list window, click **Edit** to make changes.
2. Click on the **expander to the left of Advanced options**.
3. Continue to scroll down to the bottom of the window.The **Copy and paste from a CSV file window** is viewable. An example is shown in "Figure 8-11: CSV entry fields available in advanced options"

Figure 8-11: CSV entry fields available in advanced options



4. Click on the gray text within the CSV file window.
5. Copy and paste room and bed information from a CSV file into the window. An example is shown in “Figure 8-12: Copy and paste from CSV file window with data example”.
    a. Alternately type room and bed info directly into the window.
    b. Text should be of the format **room,bed** with no spaces.
    c. Type **room info only** as in the case of a single bed room with bed name.
    d. The use of the comma in the room or bed file name is not allowed.

Figure 8-12: Copy and paste from CSV file window with data example



Copy and paste from CSV file

```
210,A
212,A
213
214,Door
214,Window
```

6. Click **Add** to add the rooms and beds to the unit.
7. Click **Save** when finished.

When complete...

1. Confirm that all information listed in the Master bed list is complete, and matches the information contained in the ***Connex CS Customer Project Req. Form***.
2. Click **Save** when finished.
3. Click on the **Back** button in the window header. The Location management menu appears.

⚠ **CAUTION** Any time changes are made to the Master Bed List, Covered Area, or Licensing, the affected Central Station should be restarted prior to clinical usage.

Add a Covered area

The Covered area window contains configuration tools that bind all of the previously entered location information together with a station. The process described in this section includes:

- Add a new covered area
- Assign default location
- Assign bed to the covered area
- Assign a station to the covered area.

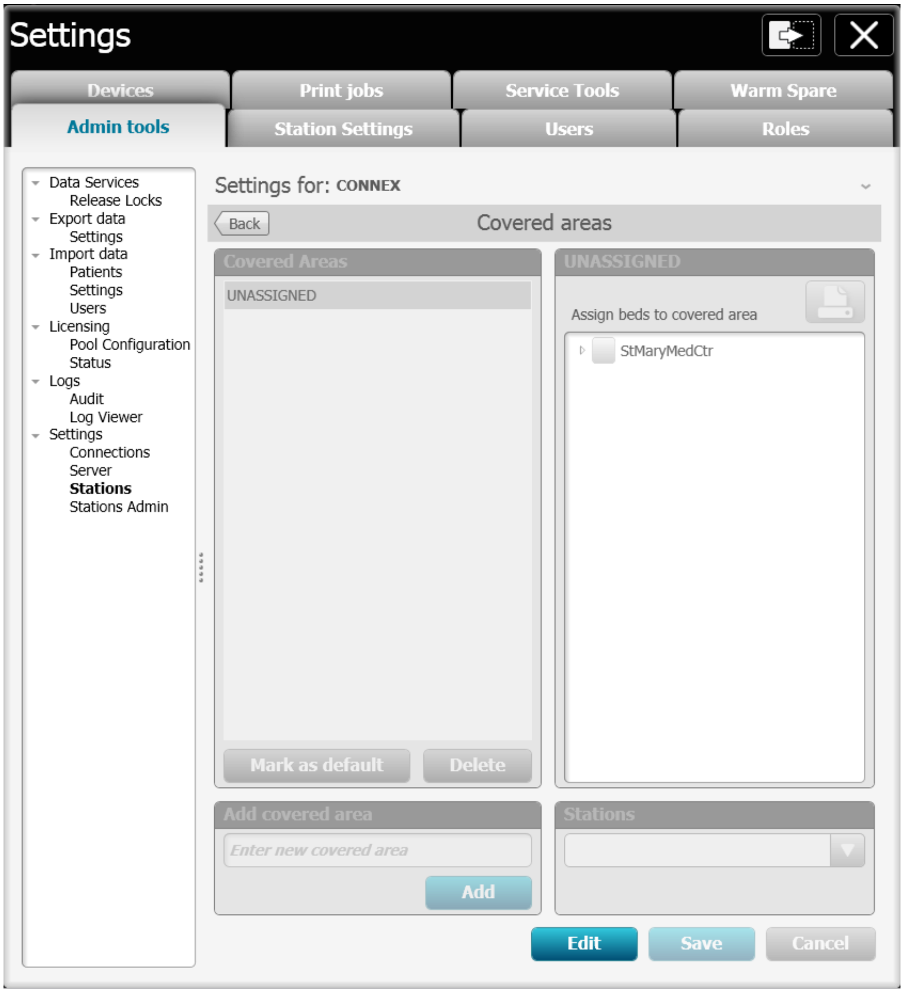
The binding of a covered area and specific bed locations to a specific station name together completes the configuration of location management settings prior to deploying to a host.

⚠ **CAUTION** Any time changes are made to the Master Bed List, Covered Area, or Licensing, the affected Central Station should be restarted prior to clinical usage.

To get started:

1. From the **Settings** > **Advanced settings** (if required)> **Admin tools** > **Stations** > **Location management** menu, click on **Covered Areas**. The Covered areas window appears. An example is show below in "Figure 8-13: Master bed list default window example".

Figure 8-13: Master bed list default window example



2. Observe that there are four sub-windows within the Covered areas main window.

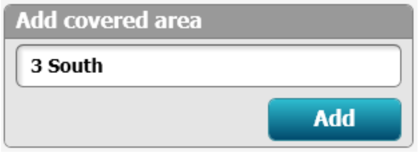
3. Click on **Edit** near the bottom of the window.

4. Create a new covered area if there are none present.

CAUTION The covered area name will appear in the upper left corner of the Connex CS display screen. Always refer to the ***Connex CS Customer Project Req. Form*** when entering information in these fields.

5. Click in the ***Enter new covered area*** field and enter the covered area name. An example is shown in "Figure 8-14: Add covered area example".

Figure 8-14: Add covered area example



Add covered area

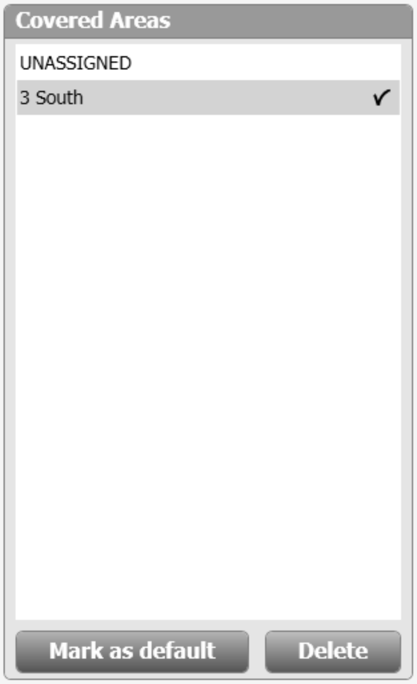
3 South

6. Click **Add** when finished. The newly create covered area appears above in the Covered areas window by name.

7. Click on the new covered area, 3 South in this example, and click on **Mark as default** if this is the default system for the network. See "Figure 8-15: Covered areas window example" for an example.

NOTE The default covered area provides a setting for all new devices to connect to the network for the first time, prior to being assigned to a location. There can be only one default covered area for a network. For a stand-alone central station, where there is only a single covered area, always mark the covered area as default.

Figure 8-15: Covered areas window example



Covered Areas

UNASSIGNED

3 South ✓

8. Observe the hierarchy within the **Assign beds to covered area window** to the right, click on the **expander** arrow next to the previously configured facility name.

9. Keep expanding all layers until the previously configured rooms and beds are viewable.

10. Note that the hierarchy is displayed in the following order with values previously entered in the Master bed list:

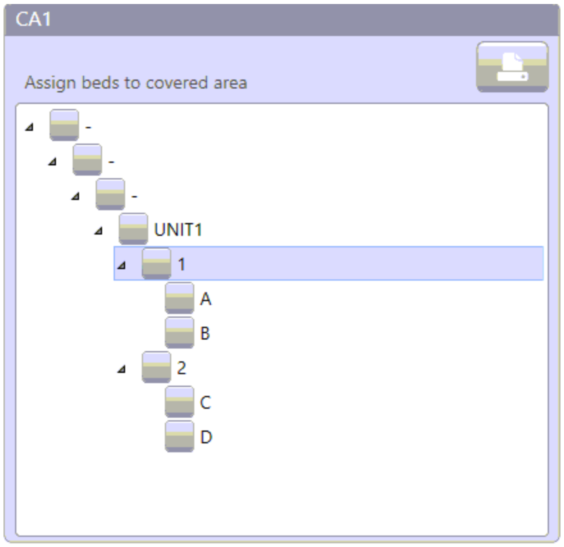
    Facility > Building > Floor > Unit > Room > Bed

11. If the covered area will be on a stand-alone central station, simple click on the Facility to select all items underneath. A check mark appears in the box next to each selected location in the hierarchy. An example is shown in "Figure 8-16: Assign beds to covered area window example".

12. If the covered area is part of a network where multiple stations will be present, select only the unit and/or rooms and beds to be assigned only to covered area chosen.

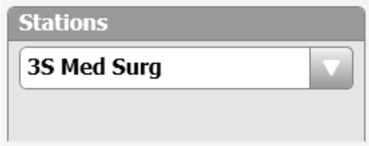
NOTE Refer to the ***Connex CS Customer Project Req. Form*** as needed for additional information about specific units, bed and rooms per covered area.

Figure 8-16: Assign beds to covered area window example



13. In the Stations sub-window, use the drop-down menu to select a station name previously created. An example is shown in "Figure 8-17 Add covered area example".

Figure 8-17 Add covered area example



14. Confirm that all information listed in the Covered area is complete, and matches the information contained in the ***Connex CS Customer Project Req. Form***.

15. Click **Save** when finished.

16. Click on the **Back** button in the window header. The Location management menu appears.

9 Promoting a Warm Spare

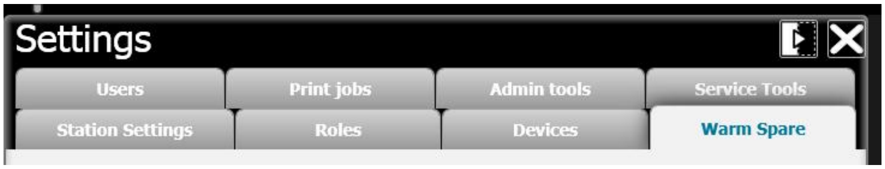
NOTE Make sure that you verify the warm spare has the static IP address it will use permanently as a Central Station.

Following are the steps to assign the current host PC to station.

1. Select the “Warm Spare” tab. An example is shown in “Figure 9-1: Warm Spare tab example”.

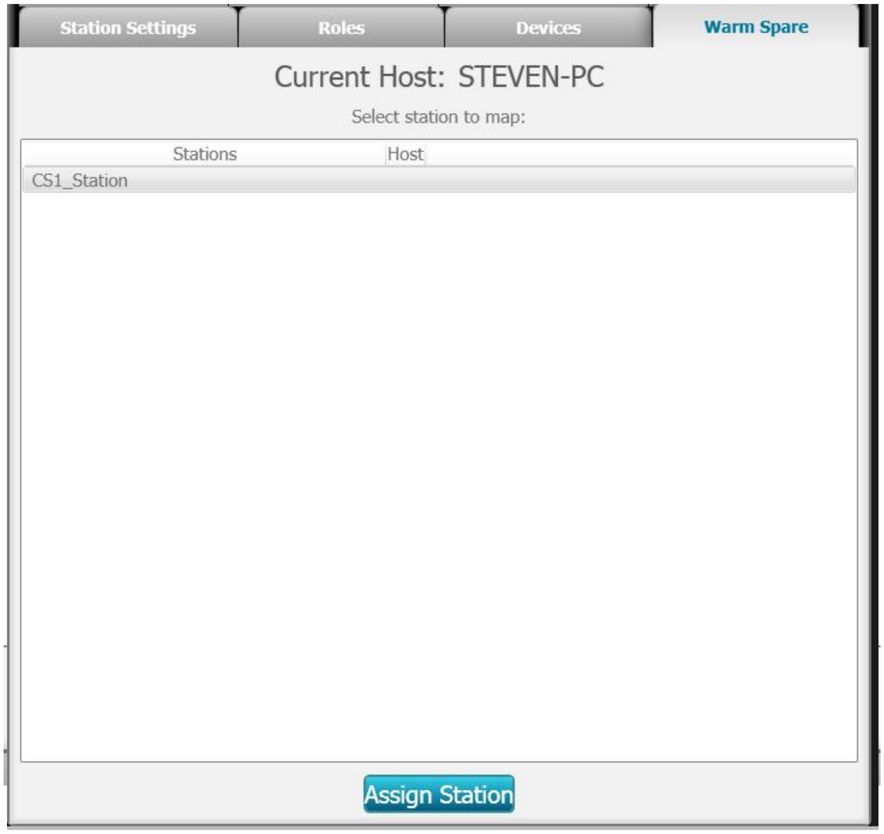
NOTE The warm spare tab will only be available if the current host pc is NOT assigned to a station.

Figure 9-1: Warm Spare tab example



2. Select the desired station to assign to. In the example shown in “Figure 9-2: Select host for warm spare assignment example”, the station is “CS1_Station”.

Figure 9-2: Select host for warm spare assignment example



Current Host: STEVEN-PC

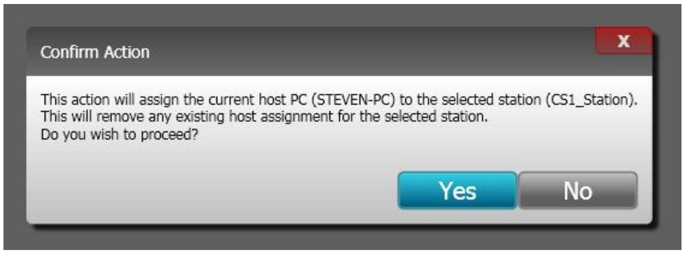
Select station to map:

Stations	Host
CS1_Station	

3. Click the “Assign Station” button to assign this host pc to the selected station. The Confirm Action window appears.

4. Click “Yes” to confirm the action. An example is shown in “Figure 9-3: Confirm warm spare assignment example”.

Figure 9-3: Confirm warm spare assignment example

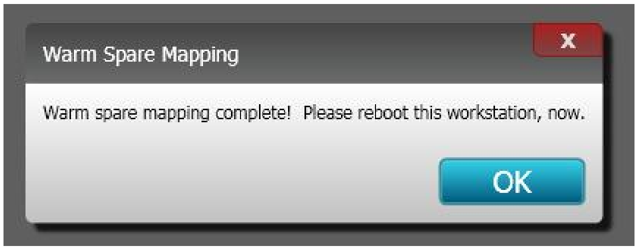


This action will assign the current host PC (STEVEN-PC) to the selected station (CS1_Station).
This will remove any existing host assignment for the selected station.
Do you wish to proceed?

5. Yes confirmation acknowledges the warm spare mapping as complete, and prompts to reboot the Connex Central Station now.

6. Click **OK** to acknowledge the message. An example is shown in “Figure 9-4: Mapping complete OK to reboot example”.

Figure 9-4: Mapping complete OK to reboot example



Warm Spare Mapping

Warm spare mapping complete! Please reboot this workstation, now.

7. The Connex Central Station application shuts down and the computer completes a reboot process automatically.
8. After the OS loads, the Connex CS application automatically starts on the Connex Central Station and is now servicing the assigned station, CS1_Station in this example.

Monitor the Data Sync Service

If the newly created station is part of a connected environment, it is best to wait for the data sync service to complete an initial sync operation before using the new station.

This is particularly true when a large volume of data must be exchanged with the server. If the newly created central station is part of a mature environment, there may be a large volume of data to synchronize. The application will function more effectively after completion of the initial sync operation.

10 Activating a License

It may become necessary to install a new license once a system has been deployed in the field. Typically this is a result of the purchase of an upgrade which includes installing new features or changes to existing licensing (e.g. increasing full disclosure from 1 day to 4 days).

On a stand-alone Central Station, the license server is local to that system only, and updates are applied locally.

In the client server model, the Connex server acts as the license server for all systems on the network. Client Central Stations do require a license to communicate with the license server. Depending upon features being updated, license activation may be required on both the Connex server and a client Central Station(s).

Depending on the type of licensing changes, it may be necessary to update all computers.

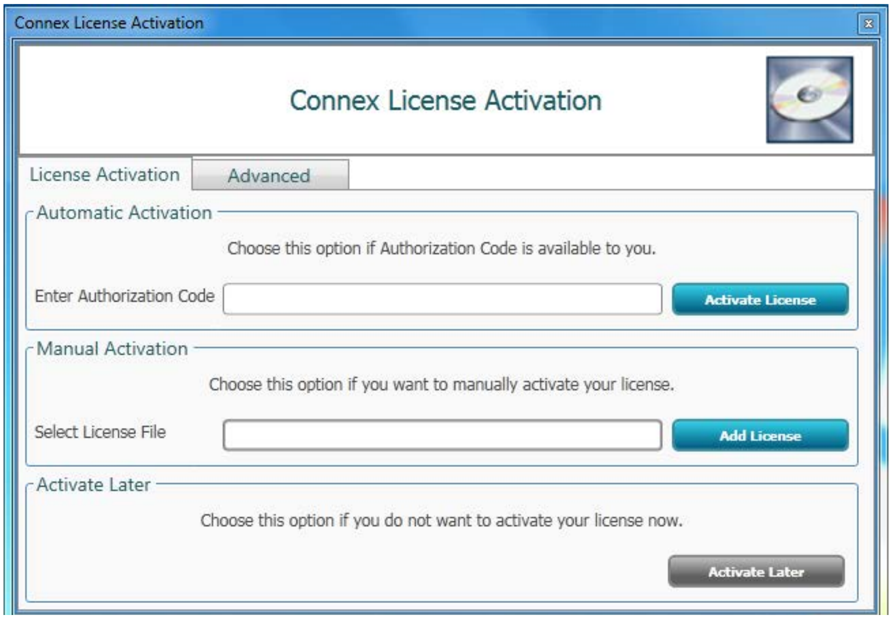
Open the license activation tool

1. From a central station, navigate to **Settings > Advanced Settings** (if necessary). The login screen appears.
    a. Login using your administration account User ID and Password information. Upon success the Settings window appears.
    b. Select the **Service tools** tab and click anywhere within the CLI window.
    c. Type explorer <Enter> to open a MS Windows Explorer window.
    d. Navigate to the following location:

       `C:\Program Files (x86)\Welch Allyn\Connex\License Activation\x.x`, where x.x is the system version number.

    e. Double-click on the **LicenseActivationTool** application. The Connex License Activation tool opens. An example is shown in "Figure 10-1: Connex license activation tool example" below.
2. From the server desktop, navigate to **Start** > **All Programs** > **Welch Allyn** > **Connex** > **License Activation** > **(version number)** and click on the entry for **Welch Allyn Connex Activation License Tool**. The Connex License Activation tool open. An example is shown in "Figure 10-1: Connex license activation tool example" below.

Figure 10-1: Connex license activation tool example



Choose this option if Authorization Code is available to you.

Choose this option if you want to manually activate your license.

Choose this option if you do not want to activate your license now.

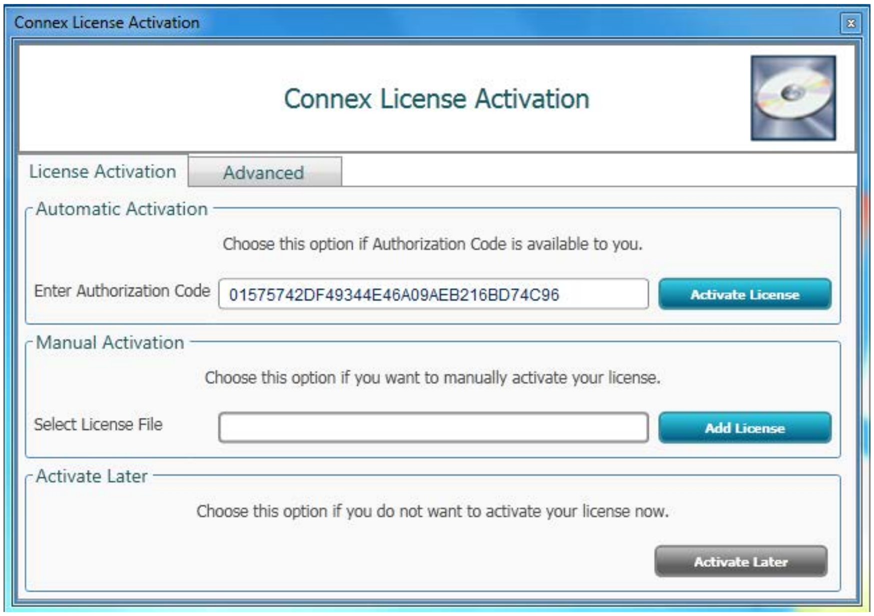
Automatic license activation

Use of automatic license activation requires that the central station or server you are attempting to update licensing on has internet access. Refer to "Manual license activation" on page 55 if the host does not have internet access.

To use automatic license activation:

1. From the License Activation tab, manually type or paste the activation code you were provided into the **Enter Authorization Code** field. An example key is shown below in "Figure 10-2: Enter an authorization code example".

Figure 10-2: Enter an authorization code example



Choose this option if Authorization Code is available to you.

Enter Authorization Code: 01575742DF49344E46A09AEB216BD74C96

Choose this option if you want to manually activate your license.

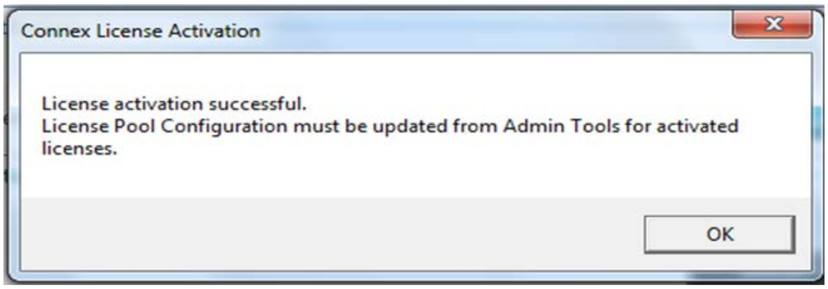
Choose this option if you do not want to activate your license now.

2. Click **Activate License** when ready.

3. A confirmation window appears indicating the status of the license activation, either success or failure. Click **OK** in the confirmation window. The license activation tool closes automatically. An example is shown below in "Figure 10-3: License activation successful message example".

Note Contact Hillrom Technical Support if there were problems activating the license.

Figure 10-3: License activation successful message example



License activation successful.
License Pool Configuration must be updated from Admin Tools for activated licenses.

4. Upon completion, reboot the affected system where the license was activated (system acting as the license server).

5. Refer to "License Pool Configuration" on page 57 to allocate updated licenses for each Central Station or network as necessary.

Manual license activation

Manual license activation may be required if the Connex server or Central Station does not have internet access to the Welch Allyn License Server.

1. On the Connex CS License Activation tool, click on the **Advanced** tab.

2. **Copy** the system information from field "**Your Machine Finger Print is:**". See "Figure 10-4: Connex license activation tool with machine fingerprint example" on page 56 below.

3. **Contact** Hillrom Technical Support to provide the **machine finger print**.

4. After a short while, Hillrom Technical Support will provide a license file via email.

5. Copy the license file contained in the email onto a USB flash drive, and then onto the system to be updated.

Note For a networked environment, multiple license files may be required as in the case of a Connex server and Central Station or Warm Spare station.

6. Return to the License Activation tab.

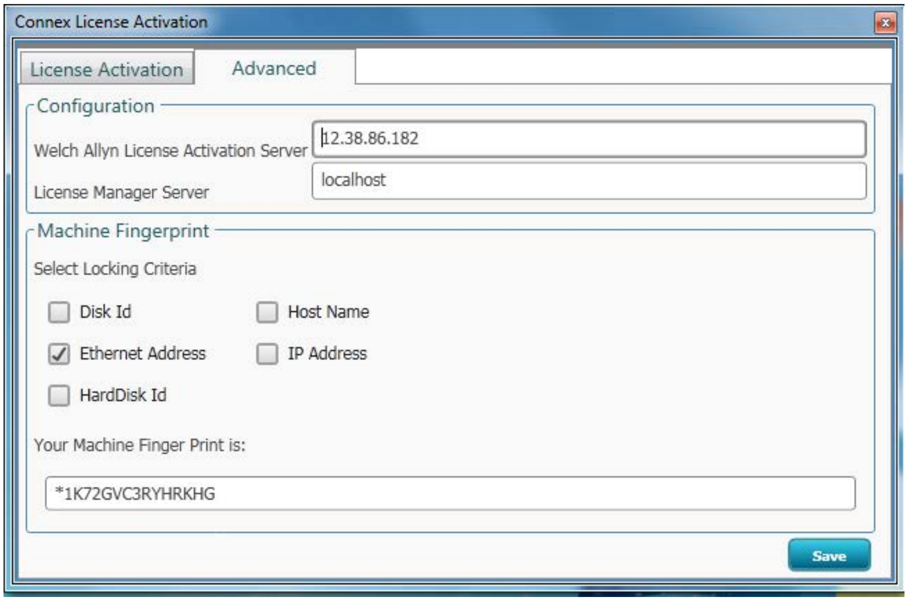
7. Click on **Add License**. The Open file navigator window appears.

8. Navigate to the location of the newly copied license file from step 5 above, click on the license file, and click **Open**.

9. Upon success the system displays a license install success screen.

10. Close the License Activation Tool window when complete.

Figure 10-4: Connex license activation tool with machine fingerprint example



Configuration

Welch Allyn License Activation Server: 12.38.86.182

License Manager Server: localhost

Machine Fingerprint

Select Locking Criteria

□ Disk Id
□ Host Name
☑ Ethernet Address
□ IP Address
□ HardDisk Id

Your Machine Finger Print is:

*1K72GVC3RYHRKHG

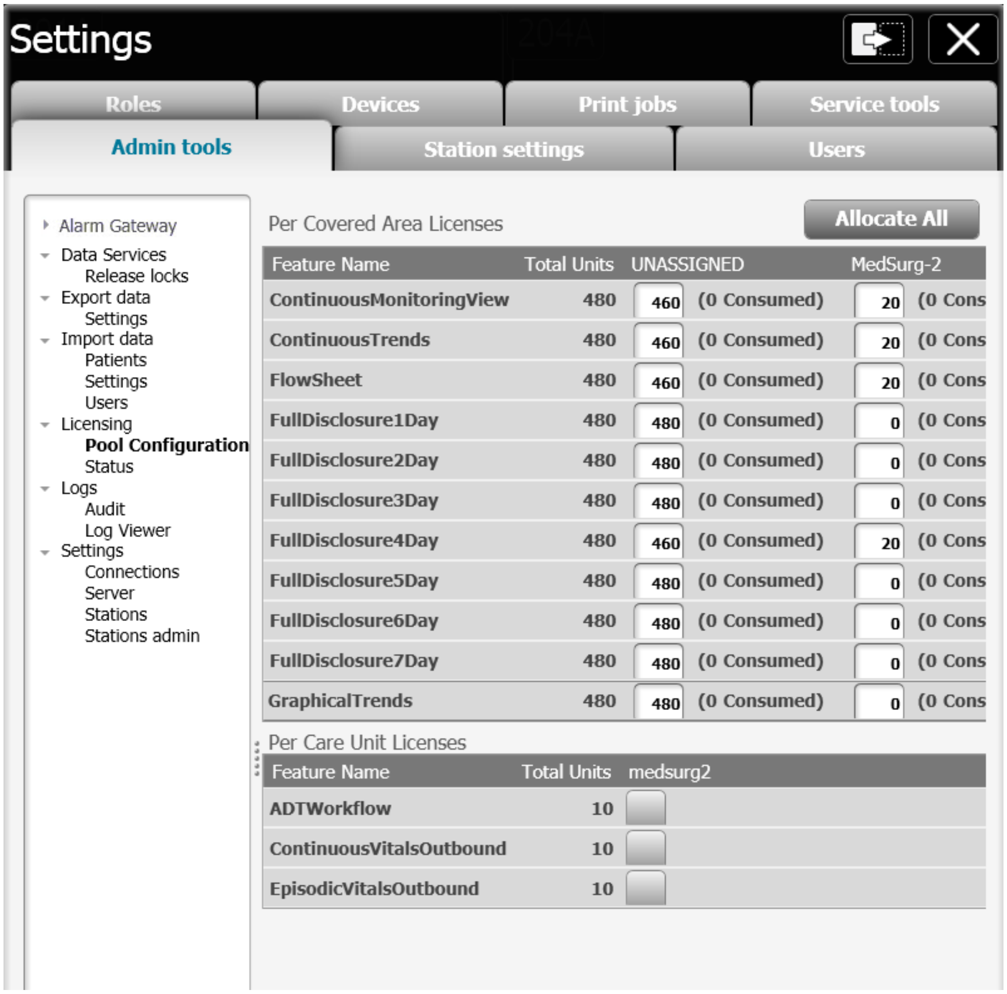
11 License Pool Configuration

Configure the License pool

Licenses for Connex CS are distributed from Welch Allyn as a pool model for an entire network and assigned as needed during configuration.

1. From the **Settings** > **Advanced settings** (if required) > **Admin tools,** click on **Pool Configuration** nested under Licensing. The Pool Configuration window appears. An example is show below in “Figure 11-1: License Pool Configuration window example”.

Figure 11-1: License Pool Configuration window example



Per Covered Area Licenses

Feature Name	Total Units	UNASSIGNED		MedSurg-2	
ContinuousMonitoringView	480	460	(0 Consumed)	20	(0 Cons
ContinuousTrends	480	460	(0 Consumed)	20	(0 Cons
FlowSheet	480	460	(0 Consumed)	20	(0 Cons
FullDisclosure1Day	480	480	(0 Consumed)	0	(0 Cons
FullDisclosure2Day	480	480	(0 Consumed)	0	(0 Cons
FullDisclosure3Day	480	480	(0 Consumed)	0	(0 Cons
FullDisclosure4Day	480	460	(0 Consumed)	20	(0 Cons
FullDisclosure5Day	480	480	(0 Consumed)	0	(0 Cons
FullDisclosure6Day	480	480	(0 Consumed)	0	(0 Cons
FullDisclosure7Day	480	480	(0 Consumed)	0	(0 Cons
GraphicalTrends	480	480	(0 Consumed)	0	(0 Cons

Per Care Unit Licenses

Feature Name	Total Units	medsurg2
ADTWorkflow	10	☐
ContinuousVitalsOutbound	10	☐
EpisodicVitalsOutbound	10	☐

2. Observe that there are two sub-windows within the Pool Configuration main window.

3. Each licensable feature is shown as a separate row.

4. The values contained in the **Total Units** column for each row correspond with the quantity of licenses purchased for that feature.

5. In the example above, 480 units corresponds with the maximum support for a network. Each central station can monitor up to 48 patients, and there are 10 central stations per network. (48 x 10 = 480).

6. By default, all new licenses are unassigned, and must be assigned to a unit for proper operation.

7. Click on **Edit** near the bottom of the window.

Automatically assign per covered area licenses

If the network is configured with only a single covered area, the **Allocate button** appears as available.

1. Click on **Allocate All** button to assign all available licenses from the Total Units to the single covered area. See "Figure 11-1: License Pool Configuration window example" on page 57 for an example.

2. The UNASSIGNED license pool automatically decreases as licenses are assigned to the covered area.

Note The Allocate All function limits the quantity of licenses for any one feature to no more than 48 per covered area by design.

Manually assign per covered area licenses

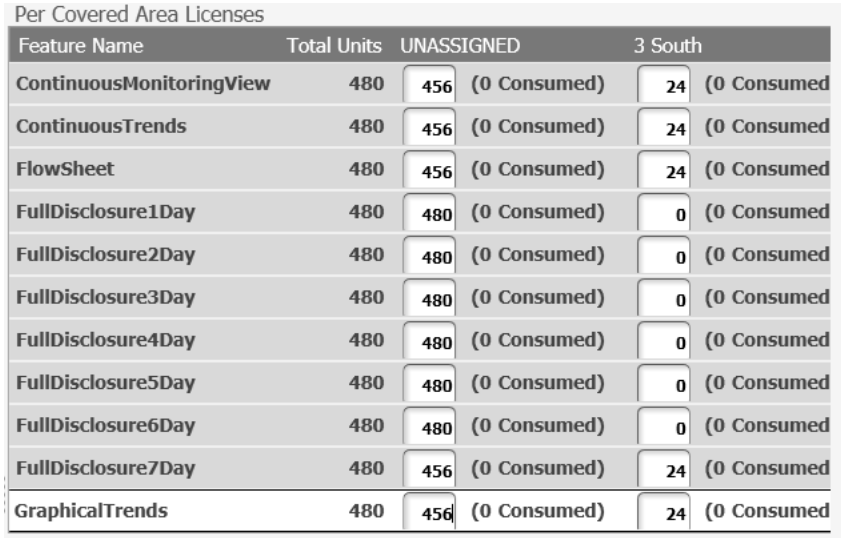
Licenses must be manually assigned when more than 1 covered area is configured on the network. The **Allocate All** button appears as unavailable as well.

1. Identify the column associated with the Covered Area name for the central station.

2. Double click in a field for the Unit, and **enter a quantity** of licenses to be allocated for each feature. Refer to the ***Connex CS Customer Project Req Form, Appendix B2*** as needed for additional information.

3. A common licensing model involves assigning licenses for ContinuousMonitoringView, ContinousTrends, FlowSheet, GraphicalTrend, and one of the FullDisclosure features. See "Figure 11-2: Per Covered Area Licenses assignment example" on page 59 below.

Figure 11-2: Per Covered Area Licenses assignment example



Per Covered Area Licenses

Feature Name	Total Units	UNASSIGNED		3 South	
ContinuousMonitoringView	480	456	(0 Consumed)	24	(0 Consumed
ContinuousTrends	480	456	(0 Consumed)	24	(0 Consumed
FlowSheet	480	456	(0 Consumed)	24	(0 Consumed
FullDisclosure1Day	480	480	(0 Consumed)	0	(0 Consumed
FullDisclosure2Day	480	480	(0 Consumed)	0	(0 Consumed
FullDisclosure3Day	480	480	(0 Consumed)	0	(0 Consumed
FullDisclosure4Day	480	480	(0 Consumed)	0	(0 Consumed
FullDisclosure5Day	480	480	(0 Consumed)	0	(0 Consumed
FullDisclosure6Day	480	480	(0 Consumed)	0	(0 Consumed
FullDisclosure7Day	480	456	(0 Consumed)	24	(0 Consumed
GraphicalTrends	480	456	(0 Consumed)	24	(0 Consumed

4. Licenses are automatically removed from the UNASSIGNED column.

5. Repeat steps 1 through 4 for each Covered Area on the network.

Assign Per Care Unit Licenses

Per Care Unit Licenses are **only used for HL7 interfaces** with the customer's EMR, and are deployed as one per unit, on or off. Always refer to the ***Connex CS Customer Project Req. Form*** when configuring Per Care Unit Licenses.

1. Identify the column associated with the Unit name for the central station.

2. Click in the box for the Unit, to enable a license for each feature. Refer to the ***Connex CS Customer Project Req Form, Appendix B2*** as needed.

3. If there are more that one Unit on the network, repeat steps 1through 2 for each Unit.

When Complete...

1. Confirm that all information listed in the Licensing Pool configuration is complete, and matches the information contained in the ***Connex CS Customer Project Req Form, Appendix B2***.

2. Click **Save** when finished.

12 Localize Station settings

Additional configuration may be needed to meet the clinical desired settings, again using the Settings menu and tool structure.

Global settings and defaults, applied to all Central Stations, are controlled in **Admin tools** > **Settings** > **Stations**.

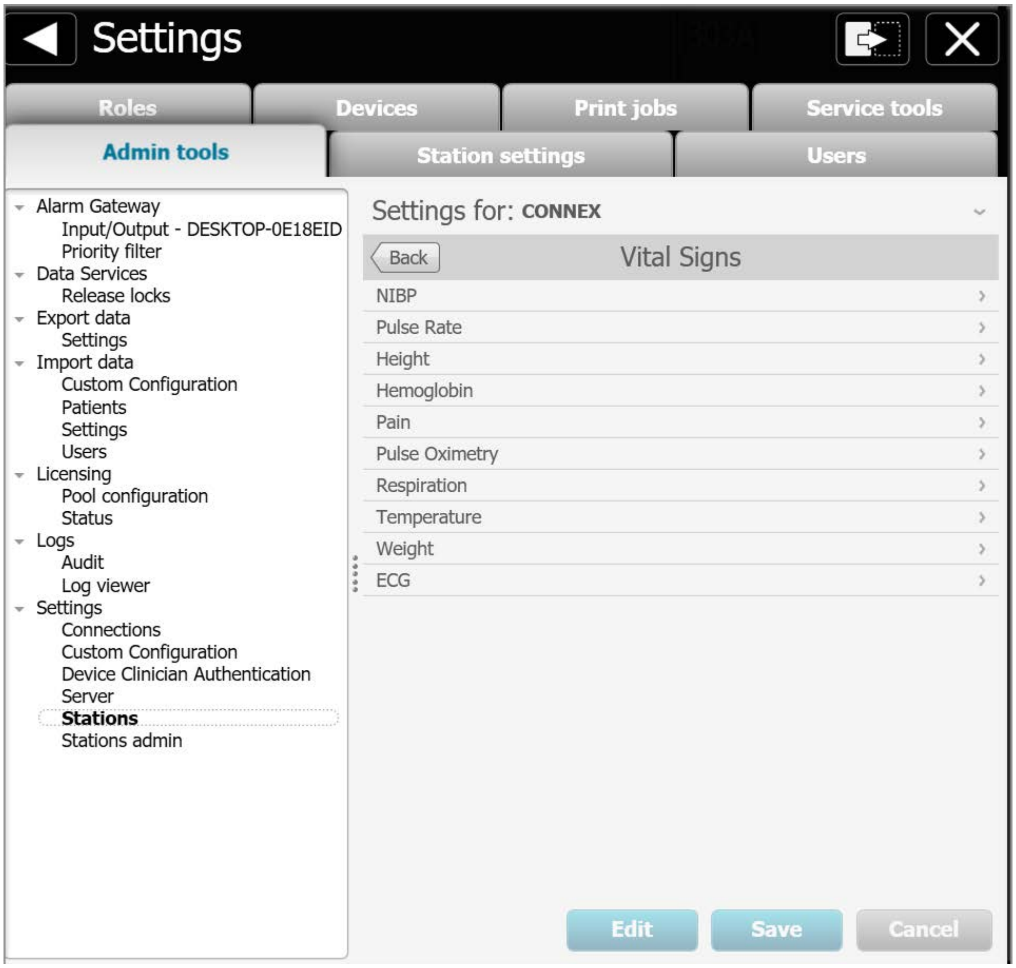
Vital Signs settings

To change Vital Signs settings:

1. From the **Settings** > **Advanced settings** (if required) > **Admin tools** > **Settings** menu, click on **Stations**. The Station Settings window appears.
2. Select **Vital Signs** to display a list of support episodic parameters made available to all clinicians. An example is show below in "Figure 12-1: Vital Signs General Parameters configuration window example" on page 62.
3. By default, all parameters are enabled. To change settings, select the desired vital sign, make changes to the available measurements list, and select **Save** when finished.
4. Select the **Back** button to return to the previous menu.
5. By default, all Vital Signs modifiers are enabled and available at Connex CS. If changes for Vital Signs modifiers are requested, such as disabling modifiers, select each desired parameter and navigate to the appropriate screen menus, make changes and save as desired.
6. Use the **Back** button to navigate back to **Station Settings** when complete.

NOTE When adjusting Central Station parameters, you will need to adjust the corresponding device parameter(s) on each connected device.

Figure 12-1: Vital Signs General Parameters configuration window example



Patient Management settings

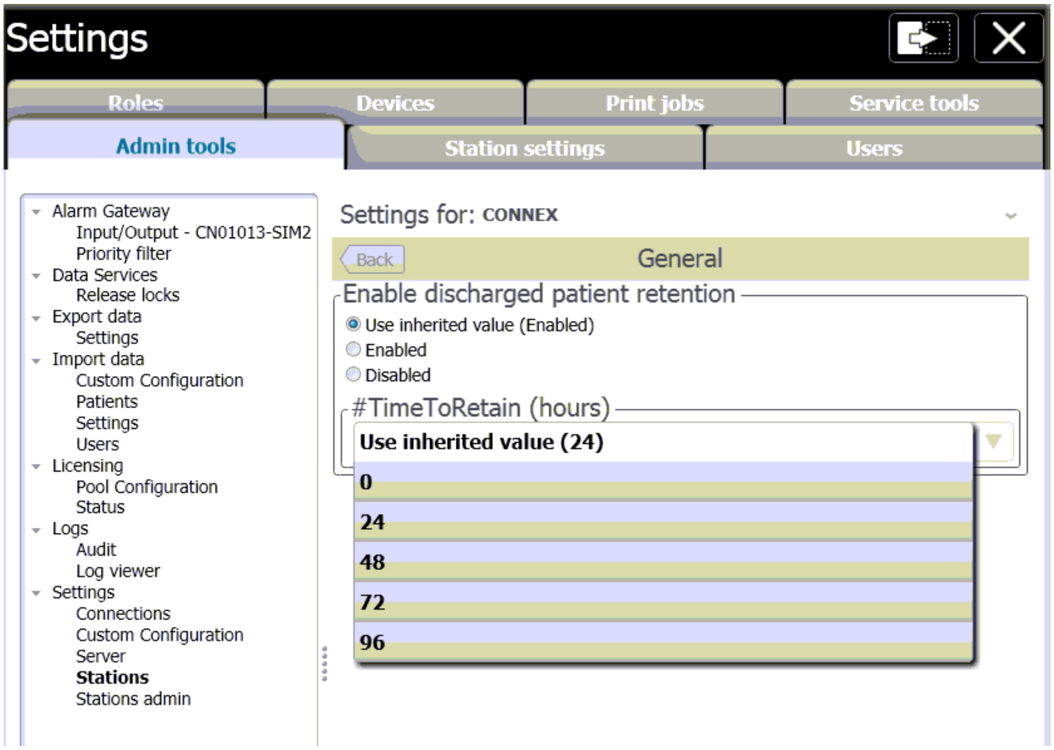
Two main functions are controlled in this area including:

- Duration of discharge patients appearing in the patient list.
- Patient tags enabled and customer descriptions.

To change how long a discharged patient stays in the Patient List:

1. From the **Settings** > **Advanced settings** (if required) > **Admin tools** > **Settings** menu, click on **Stations**. The Station Settings window appears.
2. Select **Patient management.**
3. Select the **General** setting to control how long a discharged patient is retained in the patient list. The default value is 24 hours, and can be changed using the drop down menu choices. An example is shown in "Figure 12-2: General Patient management configuration window example" on page 63.

Figure 12-2: General Patient management configuration window example



Settings for: CONNEX

Enable discharged patient retention

● Use inherited value (Enabled)

○ Enabled

○ Disabled

#TimeToRetain (hours)

Use inherited value (24)

0

24

48

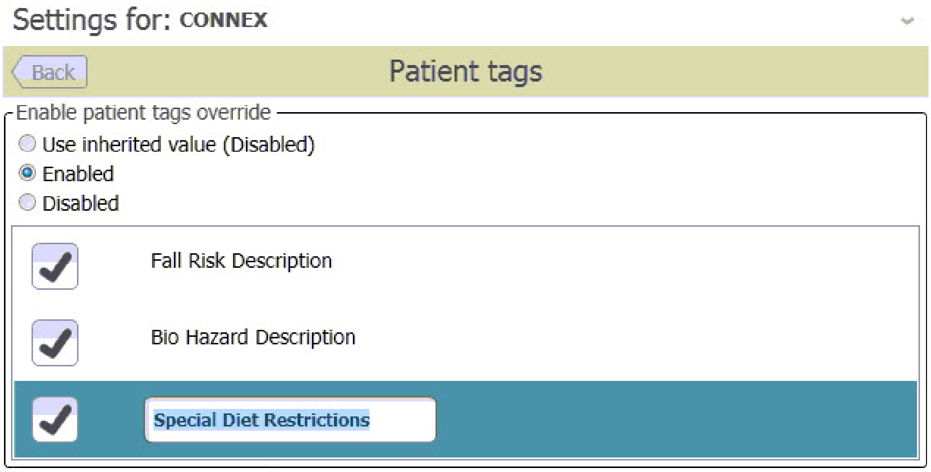
72

96

To change Patient tag settings:

1. Use the Back button, and select **Patient tags** to control settings for Fall Risk, Bio Hazard, and Diet symbols. All three tags are enabled by default.
2. To make changes, first select **Edit** and then **Enabled** to allow override of the default Patient tag values.
3. To hide a tag from view, un-check it.
4. Additionally, on-screen helper text can be modified for a tag value by double-clicking on the text field and typing in a new string. An example is shown in "Figure 12-3: General Patient management Patient tag configuration window example" on page 64.

Figure 12-3: General Patient management Patient tag configuration window example



Settings for: CONNEX

Patient tags

Enable patient tags override

○ Use inherited value (Disabled)

● Enabled

○ Disabled

☑ Fall Risk Description

☑ Bio Hazard Description

☑ Special Diet Restrictions

5. Select **Save** when finished, and **Back** to return to the Station Settings menu.

To change Display and Sound settings:

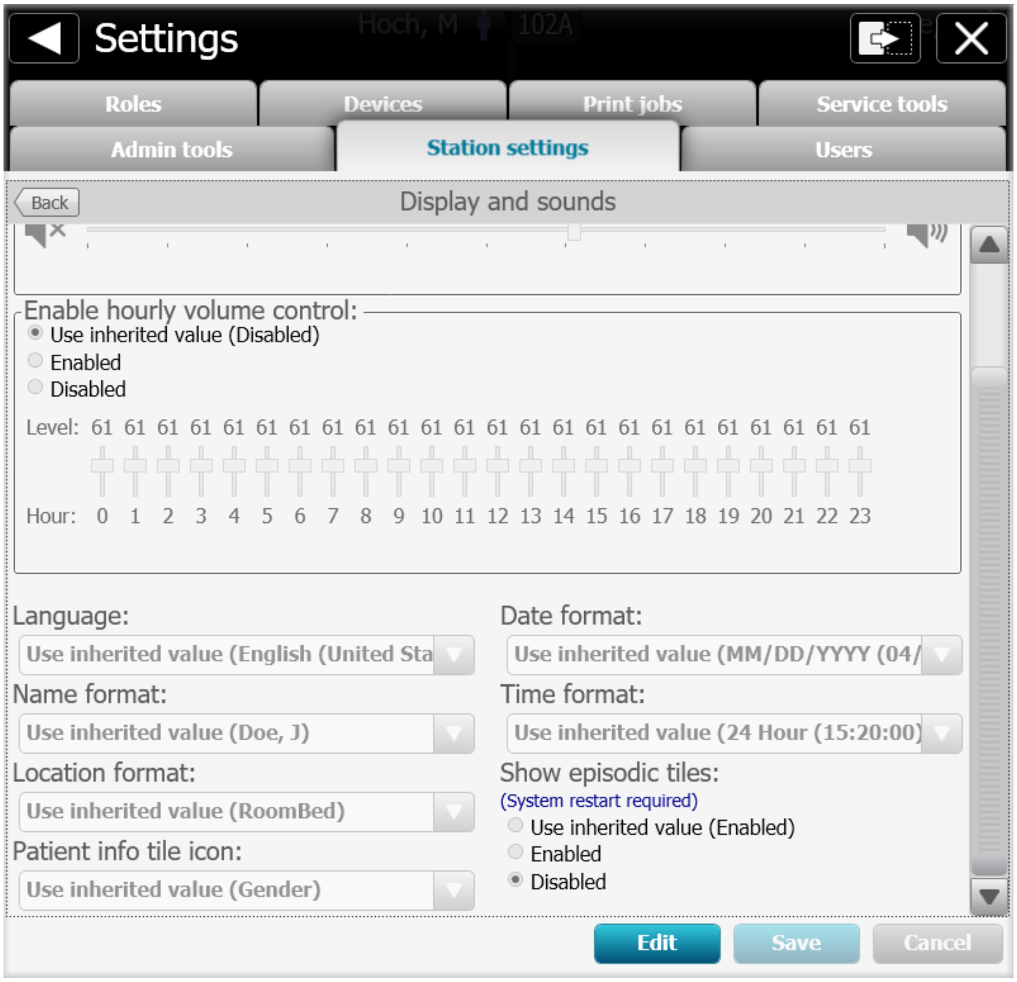
1. From the **Settings** > **Advanced settings** (if required) > **Admin tools** > **Settings** menu, click on **Stations**. The Station Settings window appears.

2. Select **Display and sounds**. By default, the controls are all disabled.

3. Select the **Edit** and **Enabled** button to make changes for manual volume override and hourly volume control settings if desired.

4. Changes can also be made for **Language**, **Name format**, **Location format**, **Date format**, **Time format**, and **Disable/Enable Display of Episodic Tests** in this window, using the various drop-down menus and radio buttons for each. An example is shown below in "Figure 12-4: Display and sounds configuration window example" on page 65.

Figure 12-4: Display and sounds configuration window example



Enable hourly volume control:

● Use inherited value (Disabled)

○ Enabled

○ Disabled

Level:	61	61	61	61	61	61	61	61	61	61	61	61	61	61	61	61	61	61	61	61	61	61	61	61
Hour:	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23

Language: Use inherited value (English (United Sta

Date format: Use inherited value (MM/DD/YYYY (04/

Name format: Use inherited value (Doe, J)

Time format: Use inherited value (24 Hour (15:20:00)

Location format: Use inherited value (RoomBed)

Show episodic tiles:
(System restart required)

○ Use inherited value (Enabled)

○ Enabled

● Disabled

Patient info tile icon: Use inherited value (Gender)

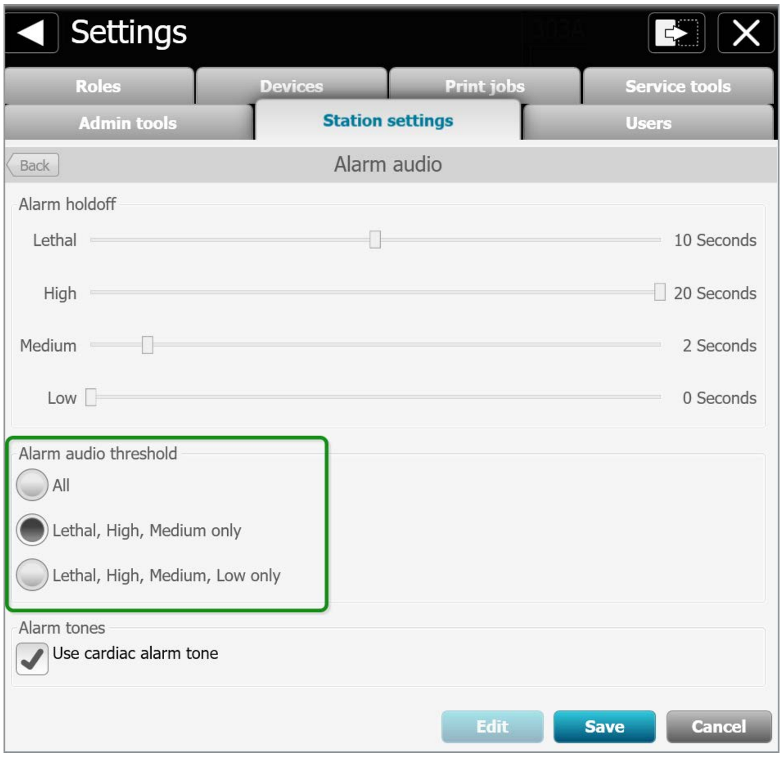
Configure alarm hold off

By default, all alarms are set to zero seconds of hold off, meaning they will be displayed and annunciated by alarm sound immediately upon occurrence. Hold off settings are configurable on a per level basis from zero to twenty seconds.

To configure Alarm hold off:

1. From the **Settings** > **Advanced settings** (if required) > **Stations Settings** tab, click on **Alarm audio**. The alarm hold off configuration window appears.
2. Select **Edit** to make changes.
3. Click and drag the desired slider for each alarm type Lethal, High, Medium, and Low as desired. An example is shown in "Figure 12-5: Alarm audio configuration window example".
4. The Alarm Audio threshold area allows you to set the alarm audio threshold. When an option is selected, only the indicated alarms are audible. All visual alarm notifications still occur.
    a. Select **All** to allow all alarms to sound.
    b. Select **Lethal, High, Medium only** to mute Low and Very Low alarms.
    c. Select **Lethal, High, Medium, Low only** to mute Very Low alarms.
5. This area allows you to set the alarm audio threshold. Select **Use cardiac alarm tone** to enable an alternate alarm tone for ECG LTA alarms.
6. Click **Save** when finished, and click **Back** to return to the main Station Settings tab.

Figure 12-5: Alarm audio configuration window example



Alarm audio

Alarm holdoff

Lethal 10 Seconds

High 20 Seconds

Medium 2 Seconds

Low 0 Seconds

Alarm audio threshold

○ All

● Lethal, High, Medium only

○ Lethal, High, Medium, Low only

Alarm tones

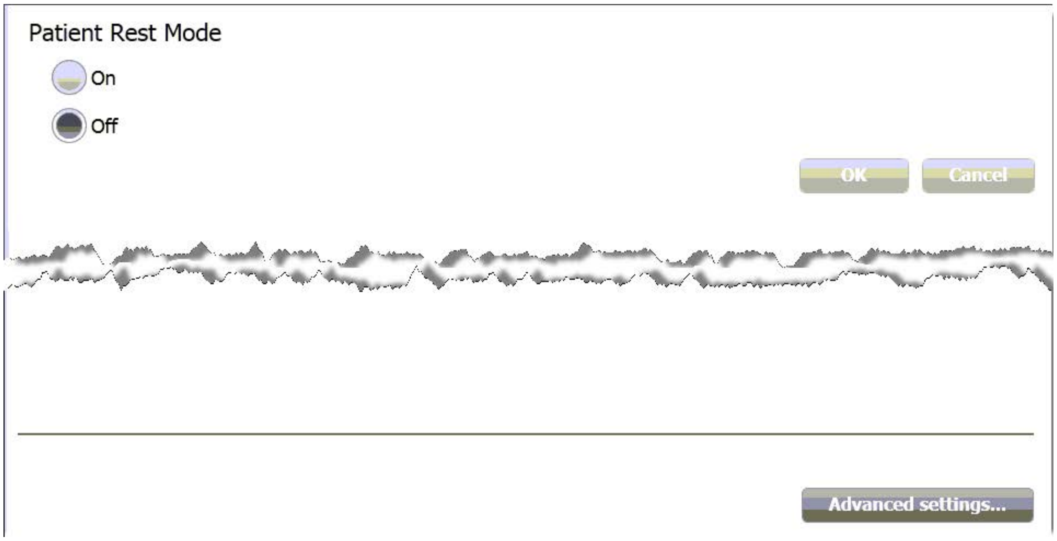
☑ Use cardiac alarm tone

Configure patient rest mode

When enabled, Patient rest mode introduces a layer after the Settings window but before the requirement to enter a User ID and Password. This allows clinical users to quickly manage Patient rest mode (either on or off) without having to login with their user credentials. See "Figure12-6: Settings > Patient rest mode control screen composite example"for a sample of controls available.

The **Advanced settings** button takes users to the login control window to manage Connex CS settings on the central station.

Figure12-6: Settings > Patient rest mode control screen composite example



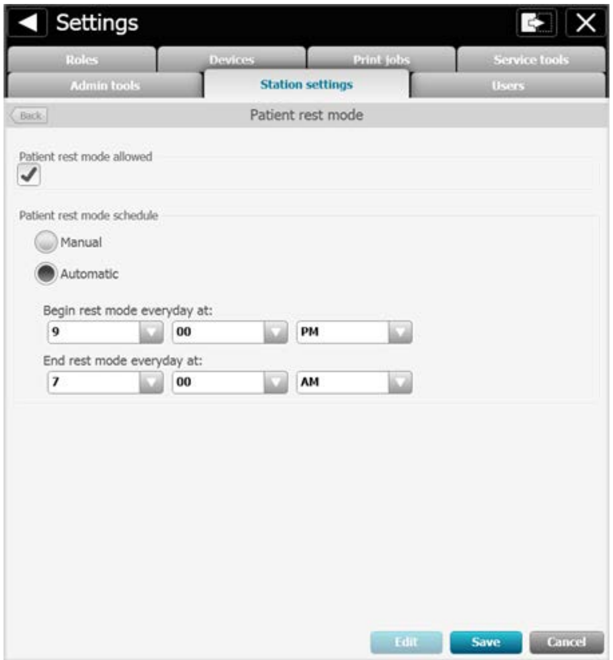
Patient Rest Mode

○ On

● Off

From the **Settings > Station Settings tab**, click **Patient rest mode**. The Patient rest mode configuraton window appears.

Figure 12-7: Patient rest mode configuration window



Patient rest mode

Patient rest mode allowed
☑

Patient rest mode schedule
○ Manual
● Automatic

Begin rest mode everyday at:
9 00 PM

End rest mode everyday at:
7 00 AM

1. Click **Edit** to make changes.
2. Click **Patient rest mode allowed** to enable this feature.
3. The **Patient rest mode schedule** radio buttons determine whether this feature is controlled by the On/Off button alone (Manual) or if the scheduling capability is enabled (Automatic).

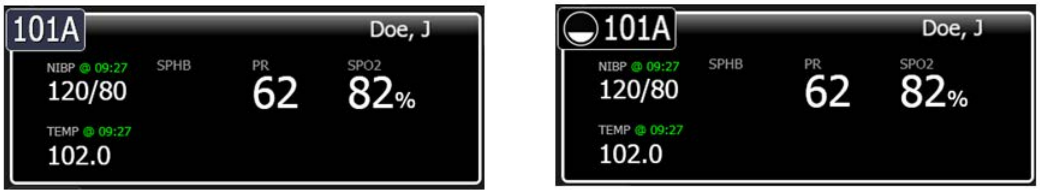
NOTE The manual On/Off control capability is enabled even when the schedule is set to Automatic. This allows you to override the scheduled on/off function.

4. When using the Automatic schedule feature, select the desired start and end times as shown in "Figure 12-7: Patient rest mode configuration window".
5. Click **Save** when finished, and click **Back** to return to the main Station Settings tab.

When the station is placed into Patient Rest mode by selecting **On** > **OK**, all enabled CVSM monitors connected to the station and running in Continuous profile will enter the rest mode.

"Figure 12-8: Central station patient tiles in normal state (left) and rest state (right)" illustrates the change in appearance of a patient tile at the Central station.

Figure 12-8: Central station patient tiles in normal state (left) and rest state (right)



Additionally, all new CVSM's that connect to the central station inherit the current rest state if enabled to support that feature.

Refer to the ***Welch Allyn Connex CS Directions for Use*** section title "Patient rest mode" for additional information about this feature.

NOTE Rest mode will terminate when the device connection to the central station is lost and an alarm condition occurs.

Configure continuous vital signs outbound

Continuous vital signs outbound controls:

1. From the **Settings** > **Advanced settings** (if required) > **Stations Settings** tab, click on **Continuous vital signs outbound**. The Continuous vital signs outbound window appears.

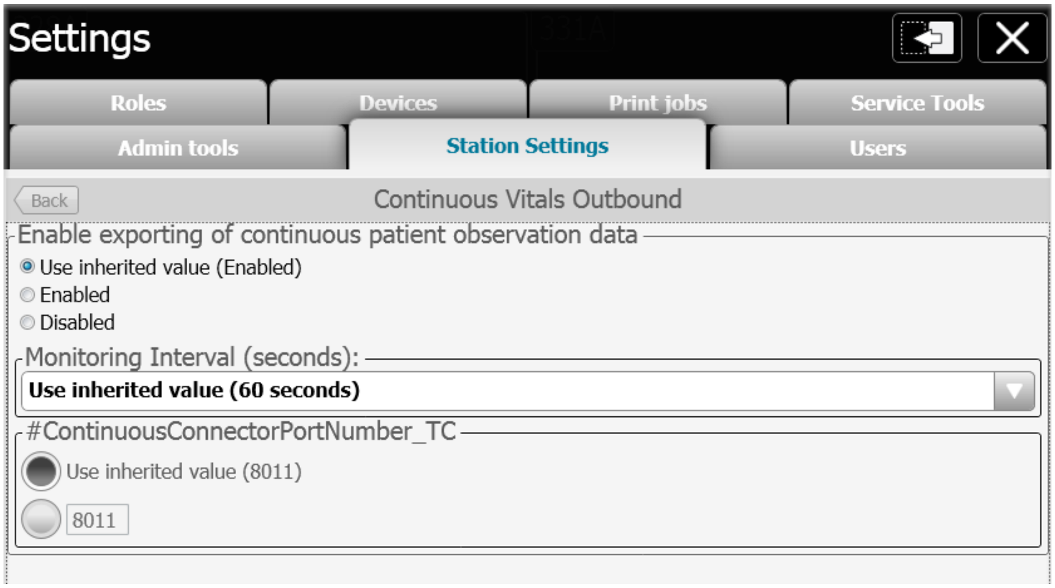
2. Select **Edit** to make changes.

3. By default, the station is configured to use the global inherited value. Click disabled to make a change, and use the drop-down menu to select an interval for sending continuous vitals data to the HIS application. An example is shown in "Figure 12-9: Continuous vital signs outbound configuration window example".

NOTE Only change the port number if directed by Welch Allyn Applications Engineering. This port is used for internal communication only between the central station and the Connex server Corepoint integration engine. This is not the port used for external communication with the facility's HIS application.

4. Click **Save** when finished, and click **Back** to return to the main Station Settings tab.

Figure 12-9: Continuous vital signs outbound configuration window example



Continuous Vitals Outbound

Enable exporting of continuous patient observation data

● Use inherited value (Enabled)
○ Enabled
○ Disabled

Monitoring Interval (seconds):

Use inherited value (60 seconds)

#ContinuousConnectorPortNumber_TC

● Use inherited value (8011)
○ 8011

Configure units of measure

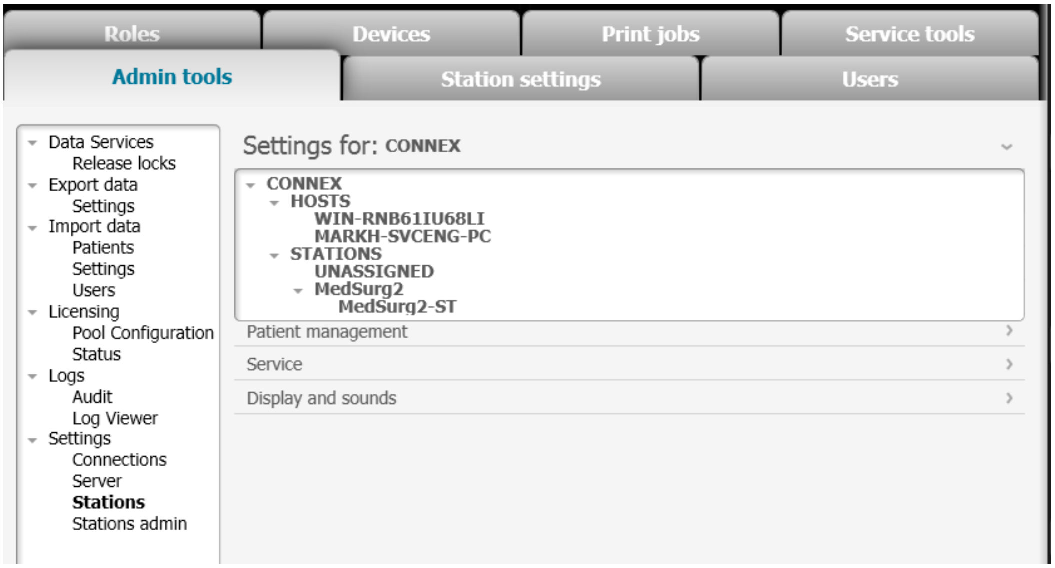
Changes to the Connex CS units of measure may be required as driven by customer preferences.

⚠ **CAUTION** Making changes to Units of measure on a live system or network will require a reboot of the Central Station / ALL Central Stations and all attached devices to ensure that all affected systems and devices are operating with the new settings. Plan your work and inform the clinical staff accordingly.

To change units of measure:

1. From the **Settings** > **Advanced settings** (if required) > **Admin tools** > **Settings** menu, click on **Stations**. The Station Settings window appears.
2. Above the Station Settings window header, click on Settings for: CONNEX. A menu tree appears. An example is shown below in "Figure 12-10: Station settings menu tree and hierarchy".

Figure 12-10: Station settings menu tree and hierarchy

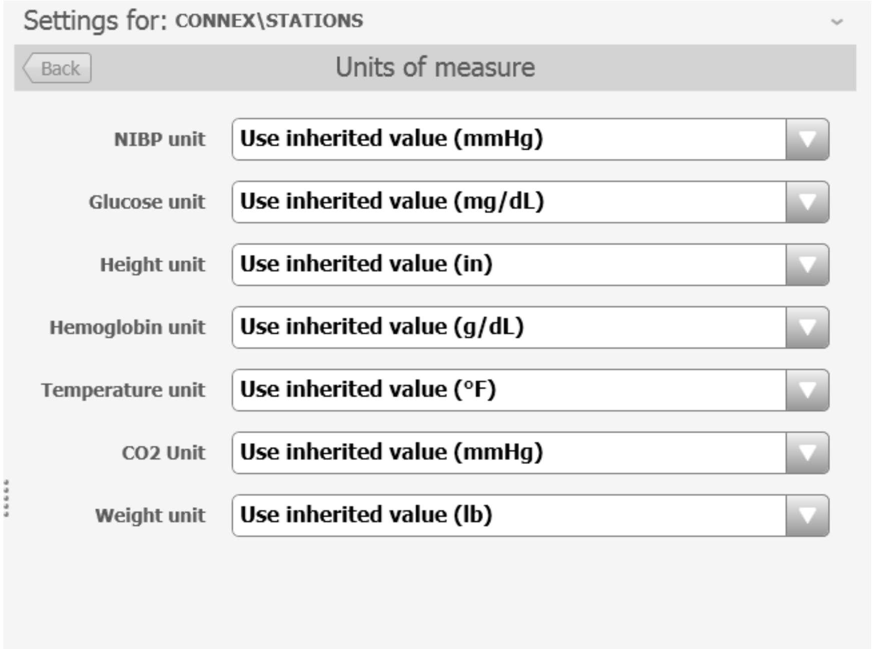


3. Click on **STATIONS** to make changes that affect all Central Stations on the network. The station settings menu changes and the units of measure choice appears.

⚠ **CAUTION** Although the menu tree allows for making changes to a specific Central Station, it is generally not recommended to have Central Stations and devices configured with different units of measure. In typical practice, units of measure are usually set at the facility level and applied to all systems and devices.

4. Click on **Units of Measure**. The Stations Settings menu tree window closes, and the hierarchy label appears as **Settings for: CONNEX/STATIONS**.
5. Click on **Units of measure** again. The Units of measure window appears. Click **Edit** to view options and make changes. See an example in "Figure 12-11: Units of measure window." on page 72.

Figure 12-11: Units of measure window.



Settings for: CONNEX\STATIONS

Units of measure

NIBP unit	Use inherited value (mmHg)
Glucose unit	Use inherited value (mg/dL)
Height unit	Use inherited value (in)
Hemoglobin unit	Use inherited value (g/dL)
Temperature unit	Use inherited value (°F)
CO2 Unit	Use inherited value (mmHg)
Weight unit	Use inherited value (lb)

6. Use the drop down to select available units of measure for specific parameters.
7. Make changes as needed, and click on **Save** when complete.

NOTE The Central Station controls the units of measure for connected devices, including CVSM, upon startup and connection to the Central Station. Thus devices inherit the same units of measure as the Central Station.

NOTE If changes are made to the Units of Measure at the Central Station while devices are connected, those devices receive the updated setting upon reconnecting to the station. To affect an immediate change at the device, power cycle the device and reconnect to the Central Station.

8. Reboot all Central Stations and all connected devices to ensure that all components are operating with the same values for units of measure.

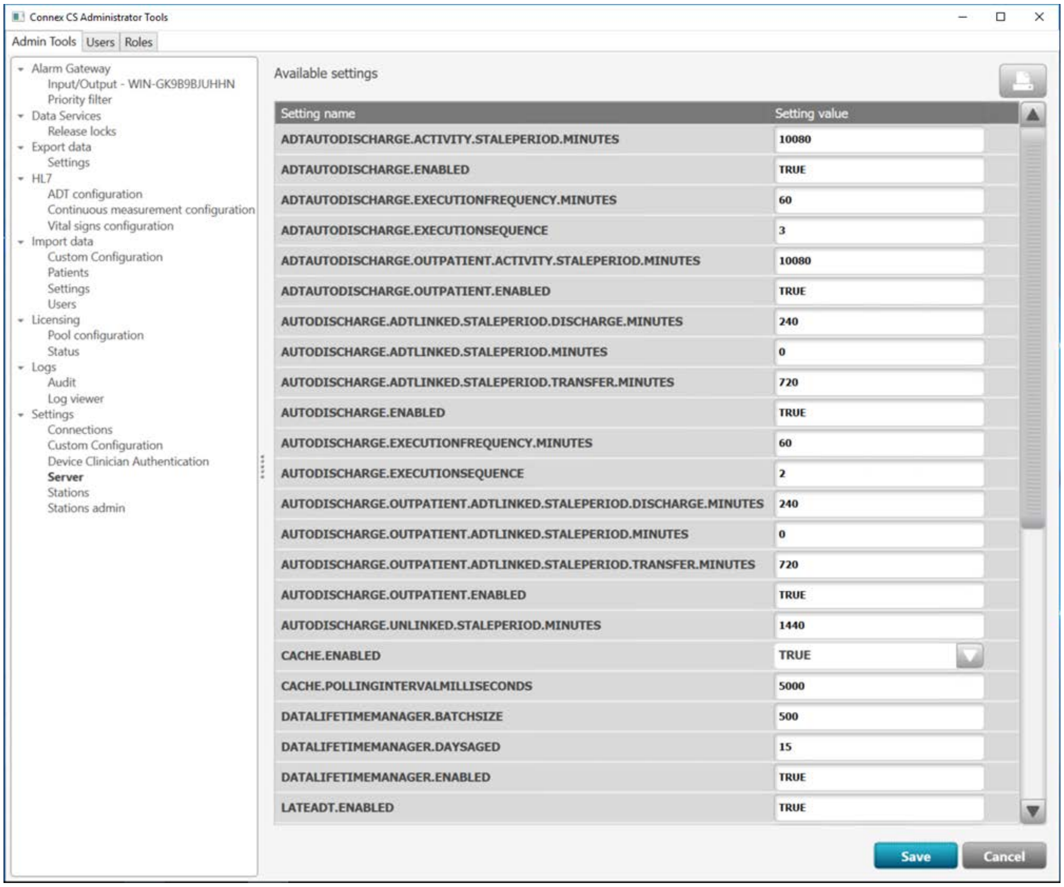
Configure auto discharge settings

The Welch Allyn ADT Task Scheduler Service provides a configurable service that runs automatically in the background to assist in managing the Patient List contents and remove old entries.

NOTE The automatic discharge feature is only applied to patients that are not currently being monitored on Connex CS

1. From a Central Station, navigate to **Settings** > **Advanced settings** (if required) > **Admin tools** > **Settings** menu, click on **Server**.
2. From Connex Server, launch the **Admin Tools launcher** > **Admin tools** tab > **Settings** menu, click on **Server**.
3. The server available settings window appears. An example is shown in "Figure 12-12: Automatic discharge settings controls available in Server settings window".
4. Select **Edit** to make changes.

Figure 12-12: Automatic discharge settings controls available in Server settings window



Setting name	Setting value
ADTAUTODISCHARGE.ACTIVITY.STALEPERIOD.MINUTES	10080
ADTAUTODISCHARGE.ENABLED	TRUE
ADTAUTODISCHARGE.EXECUTIONFREQUENCY.MINUTES	60
ADTAUTODISCHARGE.EXECUTIONSEQUENCE	3
ADTAUTODISCHARGE.OUTPATIENT.ACTIVITY.STALEPERIOD.MINUTES	10080
ADTAUTODISCHARGE.OUTPATIENT.ENABLED	TRUE
AUTODISCHARGE.ADTLINKED.STALEPERIOD.DISCHARGE.MINUTES	240
AUTODISCHARGE.ADTLINKED.STALEPERIOD.MINUTES	0
AUTODISCHARGE.ADTLINKED.STALEPERIOD.TRANSFER.MINUTES	720
AUTODISCHARGE.ENABLED	TRUE
AUTODISCHARGE.EXECUTIONFREQUENCY.MINUTES	60
AUTODISCHARGE.EXECUTIONSEQUENCE	2
AUTODISCHARGE.OUTPATIENT.ADTLINKED.STALEPERIOD.DISCHARGE.MINUTES	240
AUTODISCHARGE.OUTPATIENT.ADTLINKED.STALEPERIOD.MINUTES	0
AUTODISCHARGE.OUTPATIENT.ADTLINKED.STALEPERIOD.TRANSFER.MINUTES	720
AUTODISCHARGE.OUTPATIENT.ENABLED	TRUE
AUTODISCHARGE.UNLINKED.STALEPERIOD.MINUTES	1440
CACHE.ENABLED	TRUE
CACHE.POLLINGINTERVALMILLISECONDS	5000
DATALIFETIMEMANAGER.BATCHSIZE	500
DATALIFETIMEMANAGER.DAYSAGED	15
DATALIFETIMEMANAGER.ENABLED	TRUE
LATEADT.ENABLED	TRUE

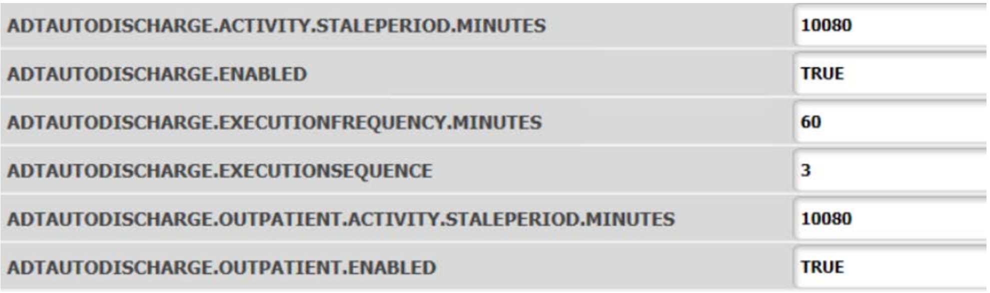
5. There are 3 different areas within auto discharge functions that can be managed, and are described in sections below.
6. Refer to the ***Welch Allyn Connex CS Directions for Use***, section titled "Automatic discharge" for general clinical information about this feature.

7. Make changes as needed.
8. Click **Save** when changes are complete.

ADT auto discharge settings

1. Settings starting with "**ADTAUTODISCHARGE**" controls automatic discharge behavior for patients or outpatients which have received an ADT message.

Figure 12-13: ADT patients auto discharge related settings



ADTAUTODISCHARGE.ACTIVITY.STALEPERIOD.MINUTES	10080
ADTAUTODISCHARGE.ENABLED	TRUE
ADTAUTODISCHARGE.EXECUTIONFREQUENCY.MINUTES	60
ADTAUTODISCHARGE.EXECUTIONSEQUENCE	3
ADTAUTODISCHARGE.OUTPATIENT.ACTIVITY.STALEPERIOD.MINUTES	10080
ADTAUTODISCHARGE.OUTPATIENT.ENABLED	TRUE

2. The following table describes the function of each setting.

Table 12-1: ADTAUTODISCHARGE setting functions and default values

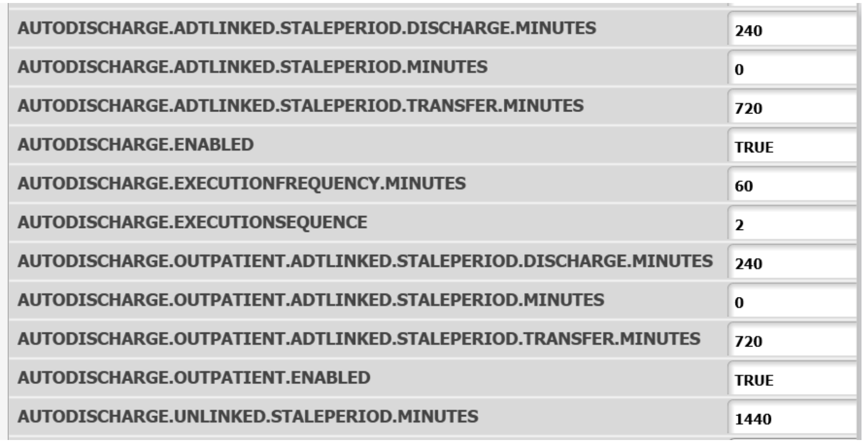
Setting Label	Function	Default value
ENABLED	Turns Auto Discharge functions on/off for patients which have received an ADT message.	TRUE (on)
ACTIVITY.STALEPERIOD.MINUTES	Determines a period of time in MINUTES for which no activity has taken place for the patient including ADT messages, monitoring, test taken, edits to demographics or visit data.	10080 (7 days)
OUTPATIENT.ENABLED	Same as ENABLED, but for outpatients.	TRUE (on)
OUTPATIENT.ACTIVITY.STALEPERIOD.MINUTES	Same as ACTIVITY.STALEPERIOD.MINUTES, but for outpatients.	10080 (7days)

CAUTION Do not change settings for **EXECUTION SEQUENCE** unless directed by Welch Allyn Engineering.

Auto discharge settings for confirmed patients

1. Settings starting with “**AUTODISCHARGE**” control automatic discharge behavior for confirmed patients or outpatients.

Figure 12-14: Confirmed patients auto discharge related settings



AUTODISCHARGE.ADTLINKED.STALEPERIOD.DISCHARGE.MINUTES	240
AUTODISCHARGE.ADTLINKED.STALEPERIOD.MINUTES	0
AUTODISCHARGE.ADTLINKED.STALEPERIOD.TRANSFER.MINUTES	720
AUTODISCHARGE.ENABLED	TRUE
AUTODISCHARGE.EXECUTIONFREQUENCY.MINUTES	60
AUTODISCHARGE.EXECUTIONSEQUENCE	2
AUTODISCHARGE.OUTPATIENT.ADTLINKED.STALEPERIOD.DISCHARGE.MINUTES	240
AUTODISCHARGE.OUTPATIENT.ADTLINKED.STALEPERIOD.MINUTES	0
AUTODISCHARGE.OUTPATIENT.ADTLINKED.STALEPERIOD.TRANSFER.MINUTES	720
AUTODISCHARGE.OUTPATIENT.ENABLED	TRUE
AUTODISCHARGE.UNLINKED.STALEPERIOD.MINUTES	1440

2. The following table describes the function of each setting.

Table 12-2: AUTODISCHARGE setting functions and default values

Setting Label	Function	Default value
ENABLED	Turns Auto Discharge functions on/off for confirmed patients	TRUE (on)
EXECUTIONFREQUENCY.MINUTES	Controls how often the process runs, in MINUTES	60
EXECUTIONSEQUENCE	Controls the run order between Late ADT Matching, Confirmed Auto Discharger, and ADT Auto Discharger processes.	2 (second)
UNLINKED.STALEPERIOD.MINUTES	Determines a period of time in MINUTES until automatic discharge of a patient for which no activity has taken place for the patient including ADT messages, Continuous Monitoring, Spot Vitals taken, edits to demographics or visit data.	1440 (24 hours)
ADTLINKED.STALEPERIOD.DISCHARGE. MINUTES	Determines a period of time in MINUTES until automatic discharge of a patient after: • receipt of an ADT discharge message, and • time of the last Spot Vitals taken or Continuous Monitoring sessions ends.	240 (4 hours)
ADTLINKED.STALEPERIOD.TRANSFER. MINUTES	Determines a period of time in MINUTES until automatic discharge of a patient after: • receipt of an ADT transfer message, and • time of the last Spot Vitals taken or Continuous Monitoring sessions ends.	240 (4 hours)

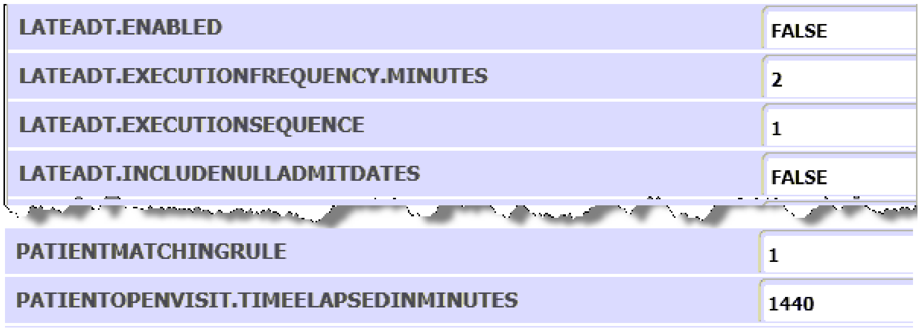
Setting Label	Function	Default value
ADTLINKED.STALEPERIOD.MINUTES	Determines a period of time in MINUTES until automatic discharge of a patient after: • time of the last Spot Vitals taken or • Continuous Monitoring sessions ends. A value of '0' disables this setting. Connex CS will use the discharge stale period after discharges even if the patient was previously transferred. The value should be more than those of ADTLINKED.STALEPERIOD. DISCHARGE.MINUTES and ADTLINKED. STALEPERIOD.TRANSFER.MINUTES or it will be overridden. In other words, the lower value will prevail.	0
OUTPATIENT.ENABLED	Same as ENABLED, but for outpatients.	TRUE (on)
OUTPATIENT.ADTLINKED.STALEPERIOD. DISCHARGE.MINUTES	Same as ADTLINKED.STALEPERIOD. DISCHARGE.MINUTES, but for outpatients.	240 (4 hours)
OUTPATIENT.ADTLINKED.STALEPERIOD. TRANSFER.MINUTES	Same as ADTLINKED.STALEPERIOD. TRANSFER.MINUTES, but for outpatients.	720 (12 hours)
OUTPATIENT.ADTLINKED.STALEPERIOD. MINUTES	Same as ADTLINKED.STALEPERIOD.MINUTES, but for outpatients.	0

⚠ **CAUTION** Do not change settings for **EXECUTION SEQUENCE** unless directed by Welch Allyn Engineering.

Late ADT settings

1. Settings starting with "**LATEADT**" control automatic discharge behavior for patients which have been under Continuous Monitoring or Spot Vitals taken, but the ADT message arrived late or after the fact. Some addition settings also control behavior related to late ADT settings.

Figure 12-15: Late ADT auto discharge related settings



LATEADT.ENABLED	FALSE
LATEADT.EXECUTIONFREQUENCY.MINUTES	2
LATEADT.EXECUTIONSEQUENCE	1
LATEADT.INCLUDENULLADMITDATES	FALSE
PATIENTMATCHINGRULE	1
PATIENTOPENVISIT.TIMEELAPSEDINMINUTES	1440

2. The table below describes the function of each setting.

Table 12-3: LATEADT setting related functions and default values.

Setting Label	Function	Default value
ENABLED	Turns Auto Discharge functions on/off for patients which have been under Continuous Monitoring or Spot Vitals taken, but the ADT message arrived late or after the fact.	TRUE (on)
EXECUTIONFREQUENCY.MINUTES	Controls how often the process runs, in MINUTES	2
EXECUTIONSEQUENCE	Controls the run order between Late ADT Matching, Confirmed Auto Discharger, and ADT Auto Discharger processes.	1 (first)
INCLUDENULLADMITDATES	Determines a period of time in MINUTES until automatic discharge of a patient for which no activity has taken place for the patient including ADT messages, Continuous Monitoring, Spot Vitals taken, edits to demographics or visit data.	FALSE (no)
PATIENTMATCHINGRULE	Determines which matching rule to apply. • 1 - if a single match is found, it is used. • 2 - if multiple matches are found, try to find a covering visit: use the ADT visit whose admit date is closest to the confirmed visit admit date and whose admit and discharge encompass the confirmed visit admit and discharge. • 3 - If multiple matches are found but a covering visit cannot be identified, use the best fit visit: use the ADT visit whose admit date is closest to the confirmed visits admit date	1
PATIENTOPENVISIT.TIMEELAPSED INMINUTES	Determines a period of time in MINUTES for how far back in history search for a patient match.	1440 (24 hours)

⚠ **CAUTION** Do not change settings for **EXECUTION SEQUENCE** unless directed by Welch Allyn Engineering.

13 Managing Device assignments

Connex central stations keep track of which devices are assigned to which station.

In the stand-alone environment, this fairly simple as there is only one central station for devices to connect to.

In a multi-system environment, devices are typically configured to connect with an assigned central station.

Assignment of devices to a central station can be managed at any central station.

Add a new device

As you will be interacting with both the Central Station and the CVSM, it is recommended that you locate the CVSM near the Central Station. By default, all new devices will attach to the central station designated as the default covered area. Refer to "Add a Covered area" on page 46 for additional information on configuring the default covered area.

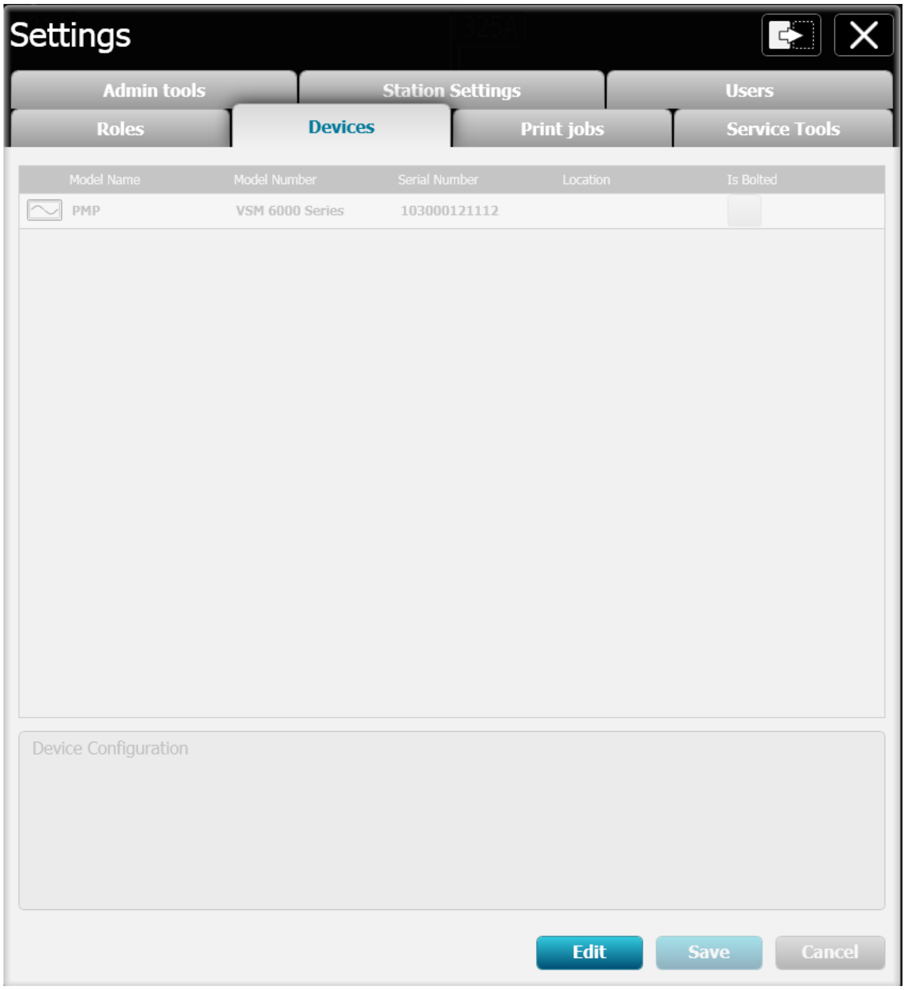
To assign a new device:

1. Power on a CVSM with continuous mode support.
2. Connect the CVSM to the network.
3. Enter some manual data on the CVSM, such as height or weight.
4. After a few moments, the CVSM appears in the Waiting area of the main screen on the Central Station.
5. On the CVSM select **Settings > Discontinue > Power Down** to cleanly break the connection between the CVSM and the Central Station.

NOTE Other methods of disconnecting the monitor, such as powering the CVSM off, or disconnecting a network cable may present alarms on both the CVSM and the central station. Some alerts and alarm conditions may not be simple to clear or present other issues.

6. On any central station, go to **Settings** > **Advanced settings** (if required) > **Devices** tab.
7. Confirm there is now an **entry corresponding to CVSM Serial Number.** An example is shown below in "Figure 13-1: Devices tab example with one device" on page 80.

Figure 13-1: Devices tab example with one device



Model Name	Model Number	Serial Number	Location	Is Bolted
∿ PMP	VSM 6000 Series	103000121112		□

8. Click **Edit** near the bottom of the window.

9. Click on the **Serial Number** of the recently connected CVSM. The Device Configuration window populates with information from the selected CVSM.

   a. Devices which are currently in use appear with a wave symbol ∿ on the left side.

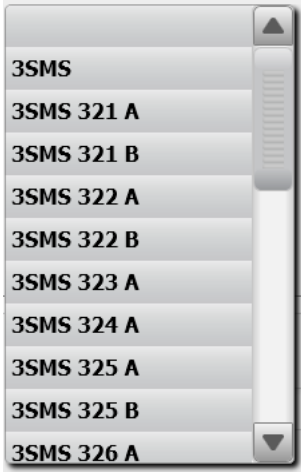
   b. Devices which are idle do not appear with a wave symbol on the left side.

NOTE Assignment of devices can only be taken when a device is not currently in use.

10. Use the Location drop down menu to select a Unit name to assign the device. An example is shown in "Figure 13-2: Device Location assignment drop down menu example" on page 81.

NOTE Typically assignments for devices are made on a Unit basis. This allows clinical user flexibility to move the device from any room/bed location throughout the covered area.

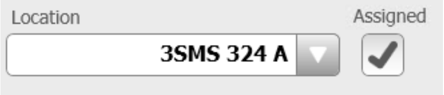
Figure 13-2: Device Location assignment drop down menu example



3SMS
3SMS 321 A
3SMS 321 B
3SMS 322 A
3SMS 322 B
3SMS 323 A
3SMS 324 A
3SMS 325 A
3SMS 325 B
3SMS 326 A

11. If the CVSM will always be located to a specific room, use the location drop down menu to select a **Unit, Room** and **Bed** location. Check the **Assigned** box to designate the monitor as permanently assigned to the select bed. An example is shown below in "Figure 13-3: Device Location assigned to a fixed room and bed example".

Figure 13-3: Device Location assigned to a fixed room and bed example



Location: 3SMS 324 A
Assigned: ☑

12. Repeat steps 1 through 11 for each additional continuous mode device.
13. Select **Save** when finished to store all device assignments.

Changing device assignments

During the course of using the system, it may become necessary to move a device from one location to another, such as another unit.

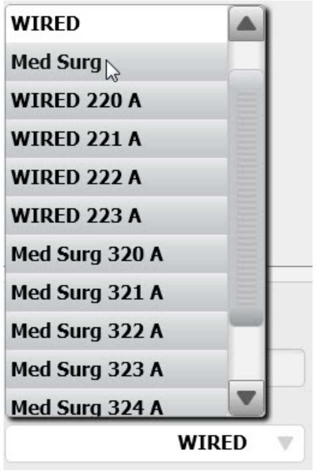
To change a device assignment:

1. On any central station, go to **Settings** > **Advanced settings** (if required) > **Devices** tab.
2. Click **Edit** near the bottom of the window.
3. Click on the **Serial Number** of the CVSM to be assigned to a different location. The Device Configuration window populates with information from the selected CVSM.

NOTE Assignment of devices can only be taken when a device is not currently in use.

4. Use the Location drop down menu to select the new desired location, typically a Unit name. An example is shown in "Figure 13-4: Location drop down menu with multiple units example" on page 82.

Figure 13-4: Location drop down menu with multiple units example

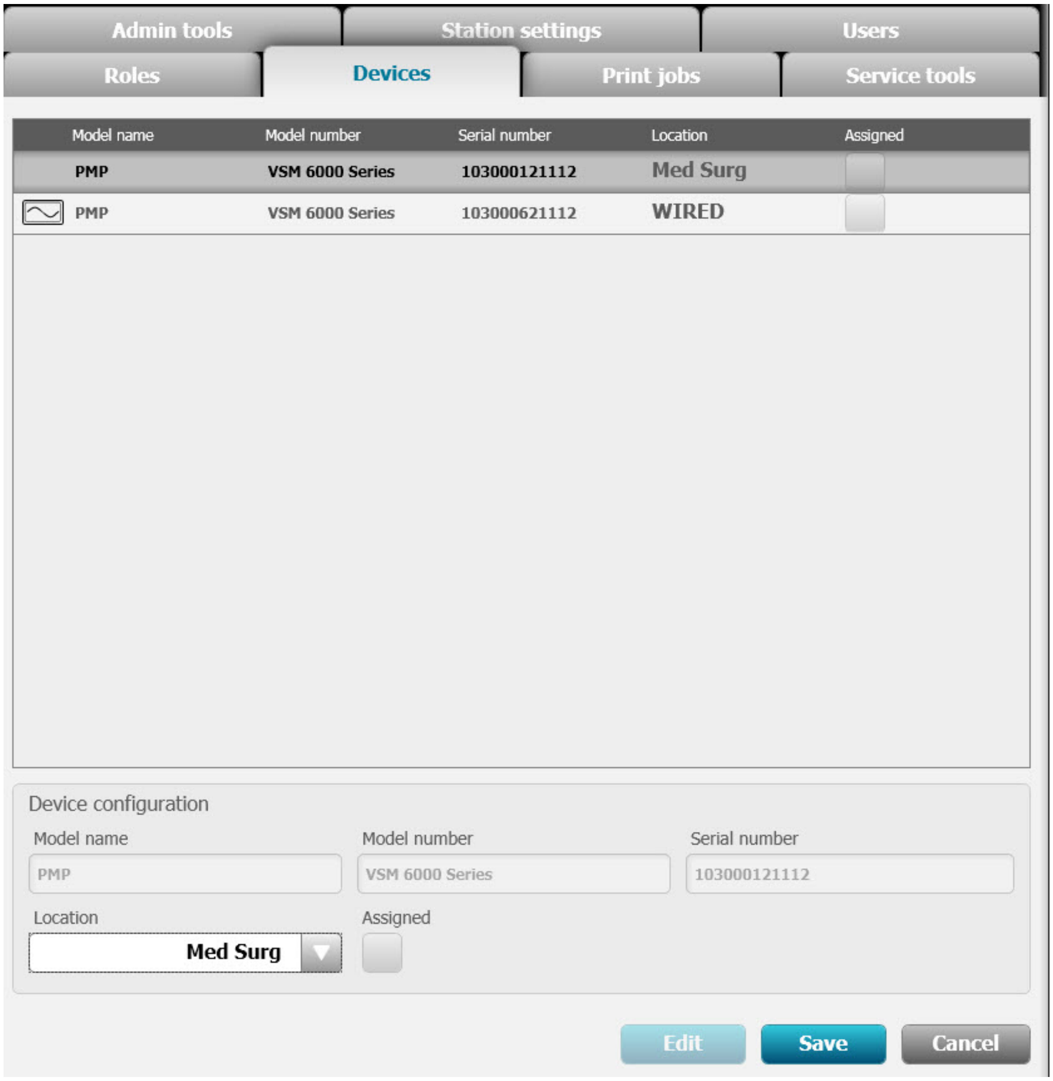


5. In the example above, the CVSM is currently assigned to the WIRED unit.

NOTE Typically assignments for devices are made on a Unit basis. This allows clinical user flexibility to move the device from any room/bed location throughout the covered area.

6. Upon selecting a new location, the new assigned location appears for the device in the table. An example is shown in "Figure 13-5: Device Location for a Bolted room and bed example" on page 83.

Figure 13-5: Device Location for a Bolted room and bed example



Model name	Model number	Serial number	Location	Assigned
PMP	VSM 6000 Series	103000121112	Med Surg	□
PMP	VSM 6000 Series	103000621112	WIRED	□

Device configuration

Model name	Model number	Serial number
PMP	VSM 6000 Series	103000121112

Location	Assigned
Med Surg	□

7. Repeat steps 1 through 6 to change locations for additional continuous mode devices.

8. Select **Save** when finished to store all updated device assignments.

9. Click **Back** to return to the Station Setting tab main menu.

14 Managing Views

The central station supports the ability for users to create and change views. Access to this area of the configuration is controlled by login and password. Ability to make views and change views is based on the user's assigned role.

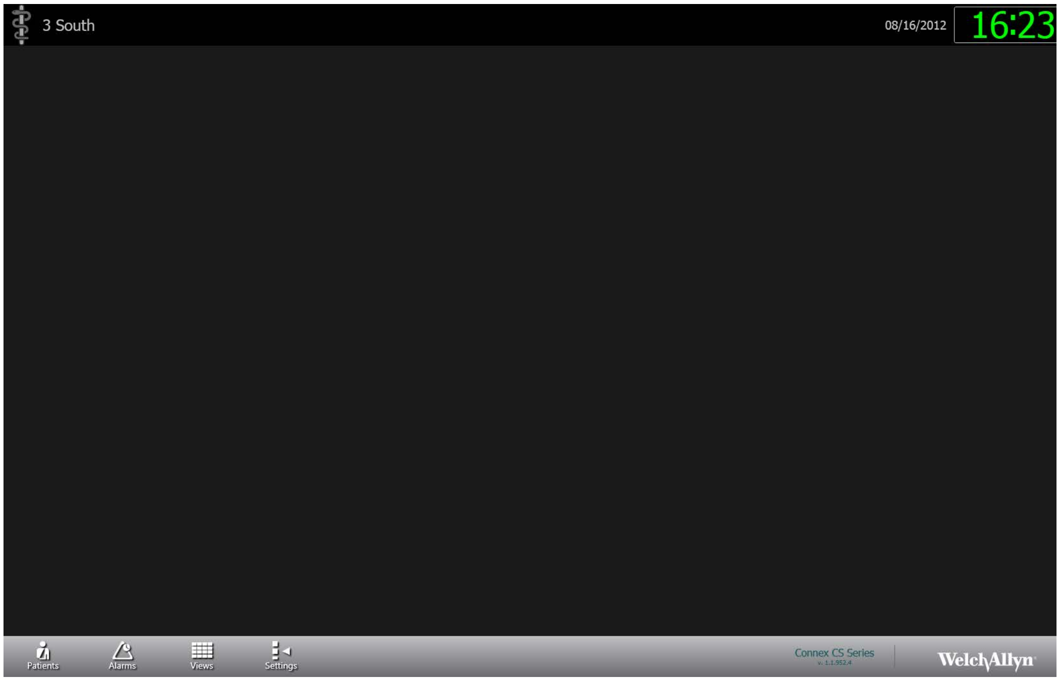
Create a View

The Connex Central Station allows users with certain privileges to create and manage customized tile layout or views. More information about view configuration can be found in the ***Directions for Use***.

1. Upon completion, the Connex CS application should start automatically and come up with default view.

2. If the station was newly assigned to the CPU (from a warm spare) there will be no view present. An example is shown below in Figure 14-1.

Figure 14-1: Main screen with no views yet created example



3. Observe that the **Covered Area name** for the station is displayed in the **upper left corner** of the screen. No rooms and beds are yet viewable at this point.

4. On the navigation area, click on **Views**. The login screen appears.

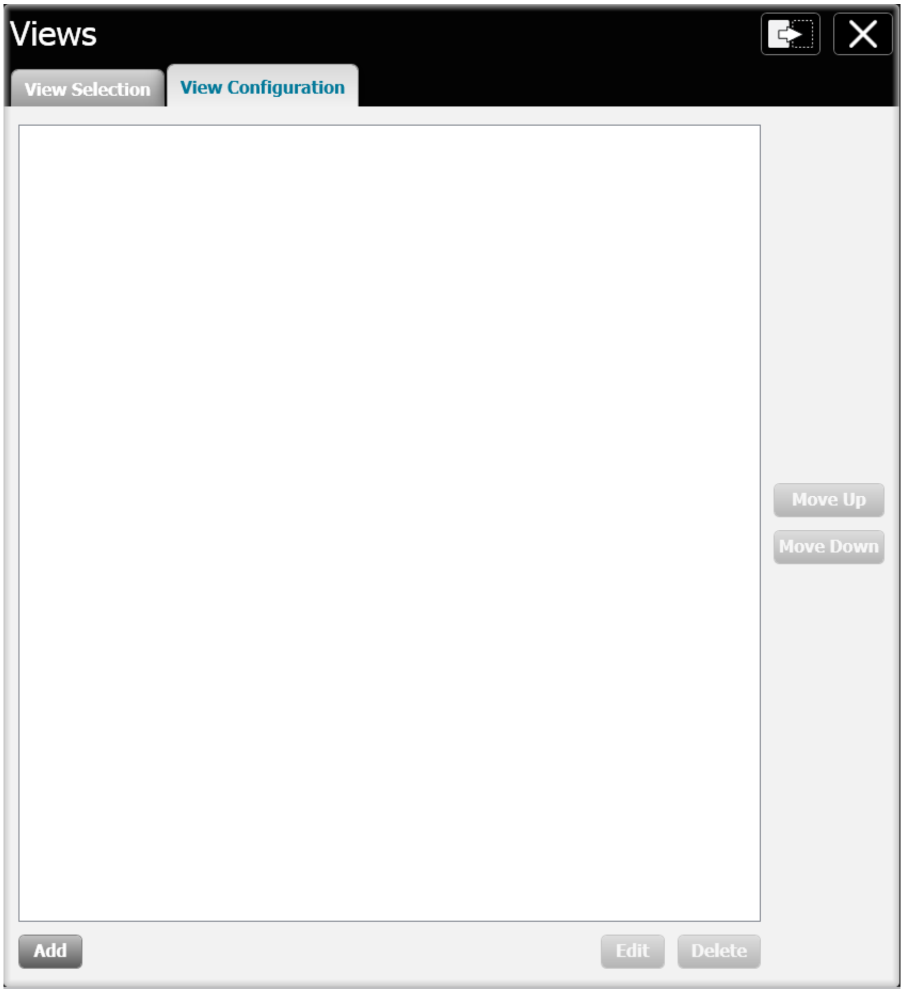
5. Login using the **service** account User ID and Password information. Upon success the Views window appears. An example is shown below in Figure 14-2.

6. Observe that there are two tabs available in the Views window.

    a. If views have been previously created for the station, the **View Selection** tab will be displayed by default.

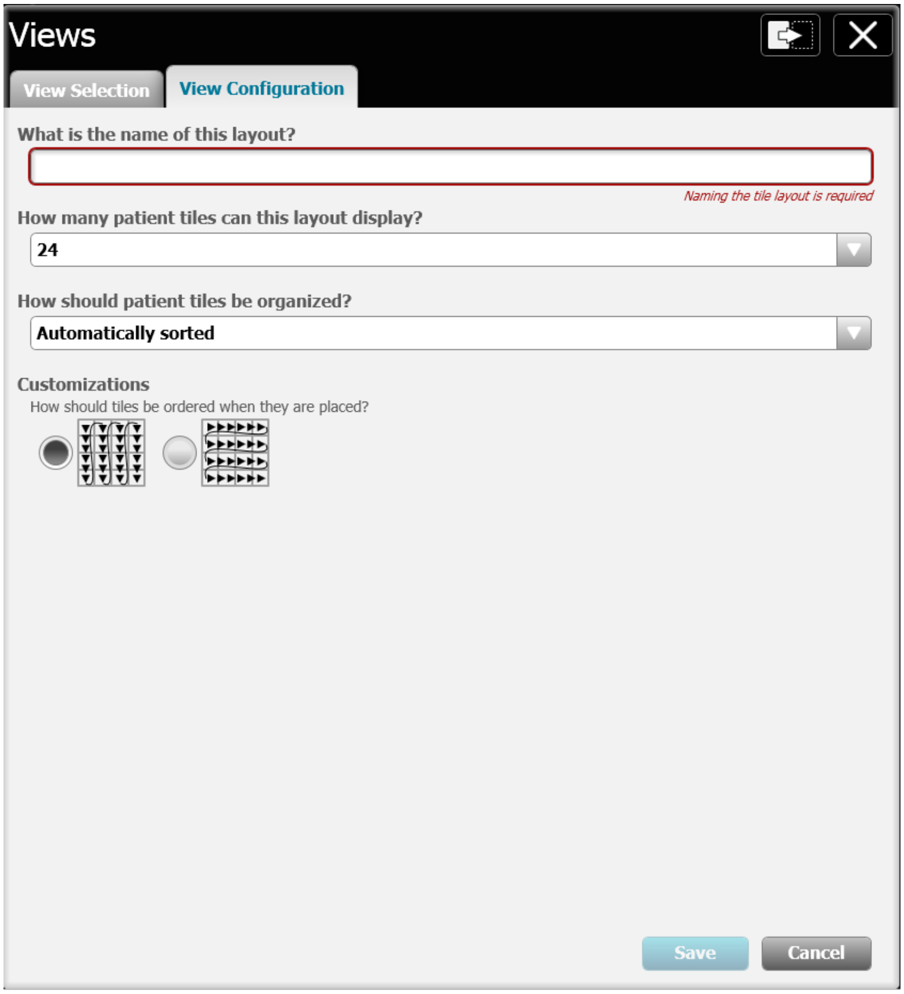
    b. If no views have been previously created, the **View Configuration** tab will be displayed by default, as in the example below.

Figure 14-2: Views window with no views yet created example



7. Click **Add** to create a new view. The window changes to display the View Configuration fields. An example is shown below in Figure 14-3.

Figure 14-3: View creation starting window example



What is the name of this layout?

Naming the tile layout is required

How many patient tiles can this layout display?
24

How should patient tiles be organized?
Automatically sorted

Customizations
How should tiles be ordered when they are placed?
● ○

8. **Enter a descriptive name** for the view or tile layout in the top field.

9. Use the drop down menu to **select the number of patient tiles** the layout will display. Patient tiles can be displayed in 8-, 12-, 24-, 36-, or 48-tile grids.

10. Use the drop down menu to select the **way in which the patient tiles will be organized**. Patient tiles can be automatically sorted, mapped by patient location, or manually placed in a tile location. An example view configuration is shown below in Figure 14-4.

    a. For an **Automatically sorted** view, choose the customization order from the samples provided.

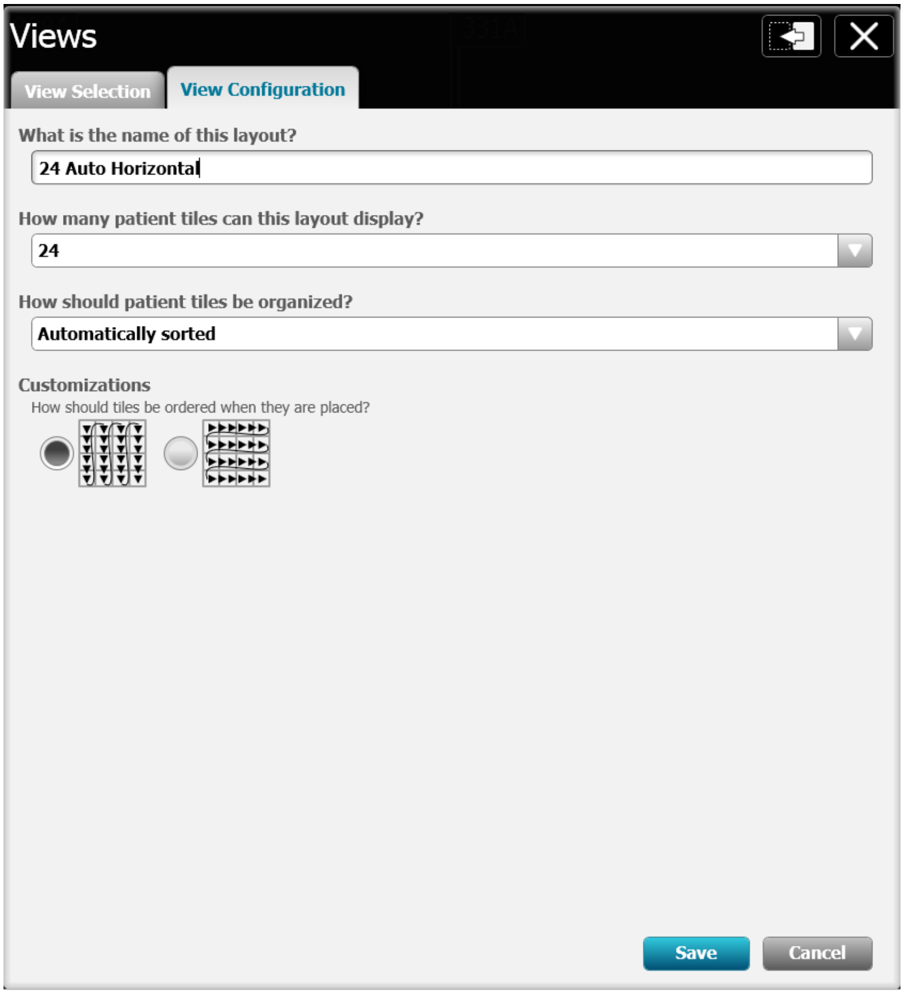
    b. For a **Manually placed in a tile location** view, no additional customizations are required. Users will be required to drag and drop a selected device from the Waiting Area to assign a view location.

    c. For a **Mapped by patient location** view, some additional steps are required. See "View Customizations for Mapped by patient location" on page 90.

11. Click **Save** when finished.

12. Repeat steps 7 through 11 to create additional views as desired.

Figure 14-4: View configuration example



What is the name of this layout?

24 Auto Horizontal

How many patient tiles can this layout display?

24

How should patient tiles be organized?

Automatically sorted

Customizations

How should tiles be ordered when they are placed?

● ○

13. Once a view has been saved, it will appear in the View Configuration window. An example with multiple views is shown below in Figure 14-5.

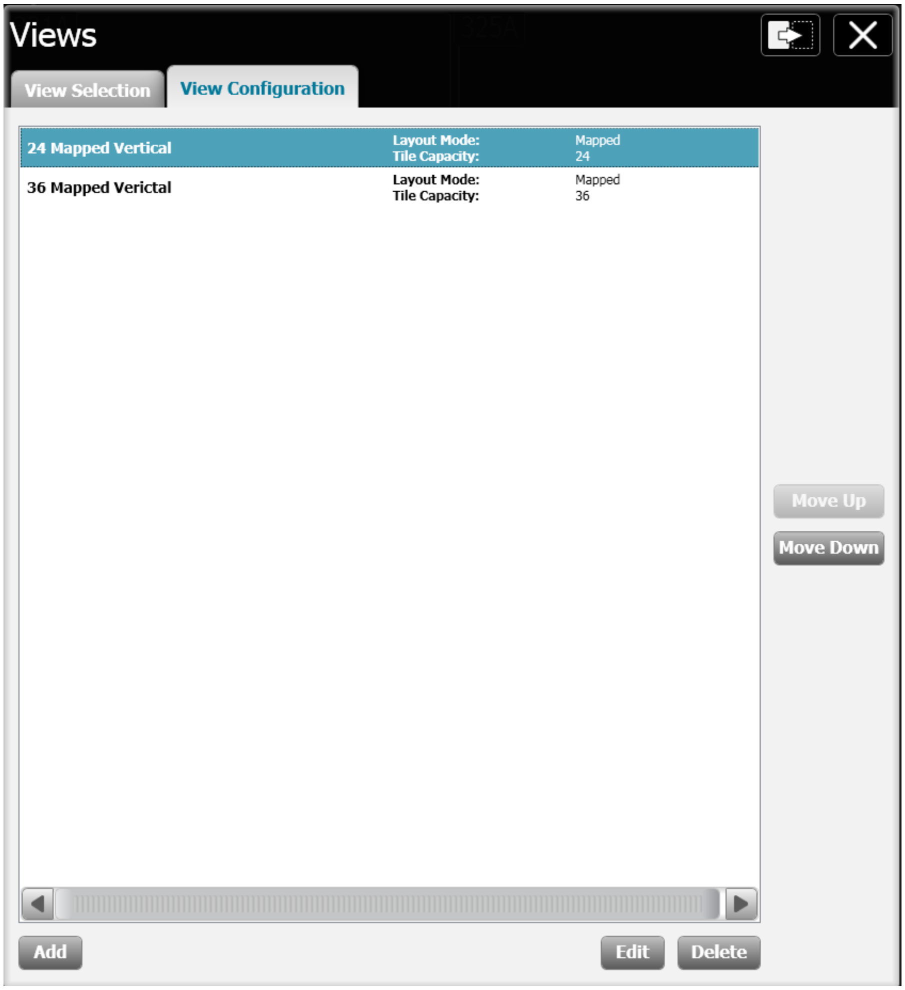
    a. Change the view display order with the **Move Up** and **Move Down** buttons on the right side.

    b. Modify a view with the **Edit** button.

    c. Remove a view with the **Delete** button.

⚠ **CAUTION** No confirmation step is required to delete a view. There is no means to cancel or recover once a view is deleted.

Figure 14-5: View configuration with multiple views created example



Views

View Selection | View Configuration

24 Mapped Vertical
Layout Mode: Mapped
Tile Capacity: 24

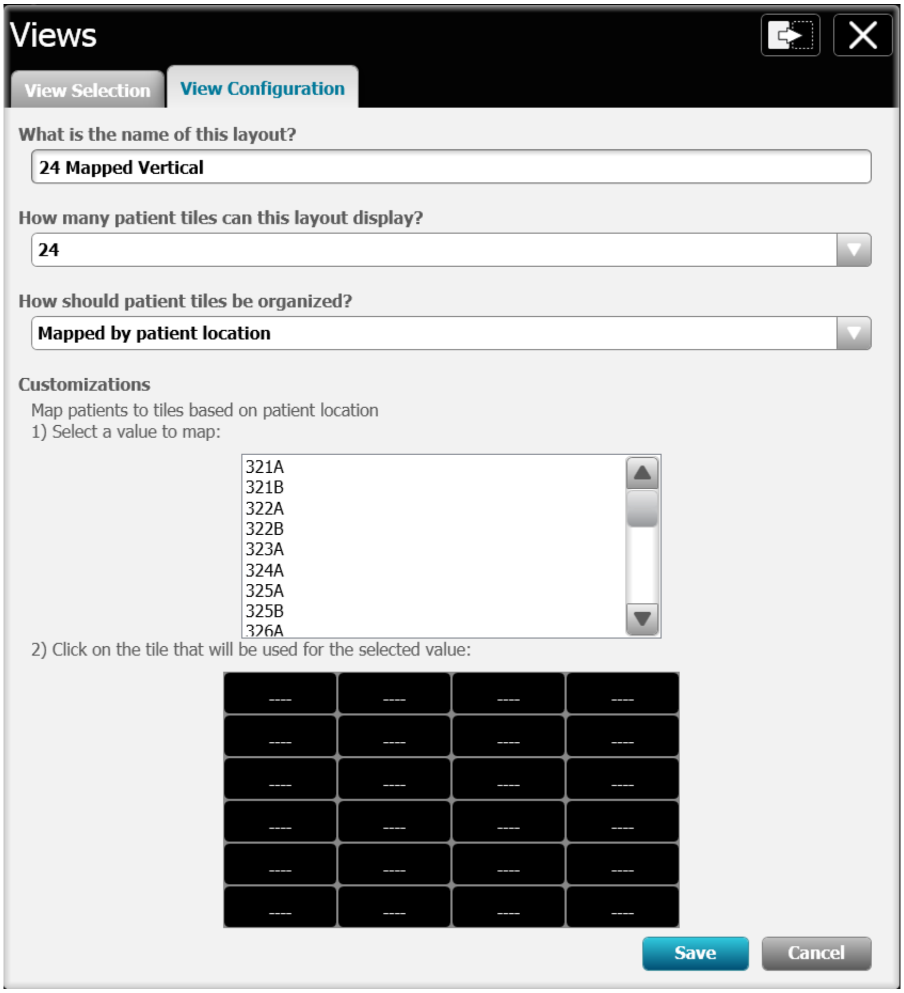
36 Mapped Verictal
Layout Mode: Mapped
Tile Capacity: 36

View Customizations for Mapped by patient location

As previously described, some additional steps are required when creating a view which is to be organized for Mapped by patient location.

1. Customization windows appear when this view organization is chosen. An example is shown below in Figure 14-6.

Figure 14-6: Mapped by patient location view configuration example



Views

View Selection | View Configuration

What is the name of this layout?
24 Mapped Vertical

How many patient tiles can this layout display?
24

How should patient tiles be organized?
Mapped by patient location

Customizations
Map patients to tiles based on patient location
1) Select a value to map:

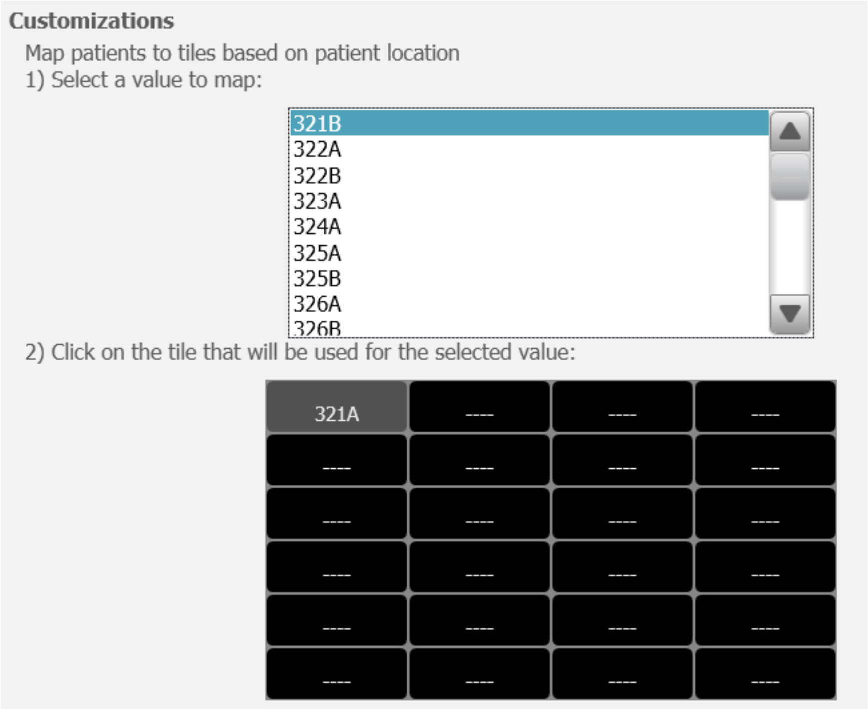
321A
321B
322A
322B
323A
324A
325A
325B
326A

2) Click on the tile that will be used for the selected value:

2. Observe that there are two sub-areas.
   - One area contains a bed list with rooms and beds in ascending order as previously configured for the covered area.
   - The second area contains a layout map for the view chosen.
3. To map a room and bed to a tile location:
   a. In the bed list, **click on the first room and bed** at the top.
   b. **Click on the desired tile location** in layout map. The room and bed now appear in the layout map.
   c. Once placed on the layout map, the room and bed are removed from the bed list.
   d. The **next room and bed are automatically selected** in the bed list and ready to be placed. An example is shown in Figure 14-7 below.

e. **Click on another tile** to place the next bed from the list.

Figure 14-7: Mapping a bed to a tile layout example



Customizations

Map patients to tiles based on patient location

1) Select a value to map:

321B
322A
322B
323A
324A
325A
325B
326A
326B

2) Click on the tile that will be used for the selected value:

321A	----	----	----
----	----	----	----
----	----	----	----
----	----	----	----
----	----	----	----
----	----	----	----

f. Repeat until all desired beds are placed into a tile location.

CAUTION While it is not required that all beds assigned to the covered area be displayed in all views, remember that unmapped beds will not be available. Use care to ensure that all desired beds are mapped to the view. An example use case may be creating a view where a number of beds will not be in use for some period of time due to construction or low census conditions.

4. To **undo a mapped bed**, simply **click on the tile location** to send the room and bed back to the bed list.

5. Click **Save** when customizations are finished.

15 Customizing Reports

Configure a custom facility logo

It may be desired to place the facility logo on some printouts from Connex CS. Custom logos are available for use on printouts from the Patient Review and Station Review functions.

The facility logo can be changed by replacing a file in 2 locations within the file system.

NOTE Connex CS supports logos up to the design layout size of 3.76”w x 0.72”h (271 x 52 pixels @ 72 dpi).

To insert a custom facility logo:

1. Obtain the logo file from the customer and copy the facility logo file onto the central station desktop.
2. Each central station must be updated separately to support using a custom facility logo.
3. In Windows shell, open a Windows Explorer window.
4. Navigate to the following location:

   C:\Program Files (x86)\Welch Allyn \ Connex\ CS\<CS Version>\Components\PatientReview\Images
5. **Rename** the file **FacilityLogo.png** to **WA-logo.png** to make a backup copy.
6. Copy the custom facility logo into the Images directory, and rename the file as **FacilityLogo**.
7. Navigate to the following location:

   C:\Program Files (x86)\Welch Allyn \ Connex\ CS\<CS Version>\Components\StationReview\Images
8. **Rename** the file **FacilityLogo.png** to **WA-logo.png** to make a backup copy.
9. Copy the custom facility logo into the Images directory, and rename the file as **FacilityLogo.**
10. Reboot the central station for changes to take affect.
11. After the Connex CS application restarts, open the Review function for a patient and perform a print function from one of the tabs.
12. Confirm that the logo appears in the upper right corner of the printout as desired.

NOTE It may be necessary to resize the logo if the logo does not fit or appears skewed in the print out.

NOTE The facility logo is not captured when exporting (backup) the system configuration files. Customer facility logos must be manually re-applied when restoring a configuration file.

16 Time Synchronization

If a facility does not have a time server available, it may be necessary to set up a time server on the Connex server. Central Stations should be configured to synchronize time with an authoritative time server.

Setting up an authoritative time server, on Connex server

It is to be noted that changing the time on the authoritative time server will not result in an immediate update of the time on all clients. There is an "Update Now" button in Internet Time options (on each client) to force an immediate re-synchronization. Otherwise the time will be re-synchronized at the next regularly scheduled update time (as set by the Windows operating system).

⚠ **WARNING** Prior to making any Windows Registry changes, it is highly recommended that a back up be made first.

NOTE Make sure UDP Port 123 is open in Windows Firewall.

To set up an authoritative time server:

1. Determine if NtpServer is already enabled (already a time server)
2. Login as the system administrator. From **Start > Search programs and files** type `cmd` <Enter>. A command line window opens.
3. Enter the following command:

   ```
   w32tm /query /configuration <Enter>
   ```

4. Scroll down the list and look for the following entries:

   ```
   NtpServer (Local)
   DllName: C:\Windows\system32\w32time.dll (Local)
   Enabled: 0 (Local)
   InputProvider: 0 (Local)
   ```

   NOTE The third line here indicates the status of the NtpServer. If '0' this machine is not configured to be a time server.

5. Update the registry to turn on the NtpServer functionality. Enter the command:

   ```
   reg add HKLM\system\CurrentControlSet\Services\W32Time\TimeProviders\
   NtpServer /v Enabled /t REG_DWORD /d 0x1 /f
   ```

6. Make sure W32Time is using NTP. Enter the command:

   ```
   reg add HKLM\system\CurrentControlSet\Services\W32Time\
   Parameters /v Type /t REG_SZ /d NTP /f
   ```

7. Mark the local computer as a reliable time server. Enter the command:

```
reg add HKLM\system\CurrentControlSet\Services\W32Time\Config /v
AnnounceFlags /t REG_DWORD /d 0x5 /f
```

8. Update the w32tm service. Enter the command:

```
w32tm /config /update
```

9. Verify that NtpServer is enabled. Enter the command:

```
w32tm /query /configuration
```

10. Scroll down the list and look for (Enabled: 1)

```
NtpServer (Local)
DllName: C:\Windows\system32\w32time.dll (Local)
Enabled: 1 (Local)
InputProvider: 0 (Local)
```

11. Reboot the server.

Configuring client sync with an authoritative time server

1. Right click on the clock in the system tray, or enter the command "**timedate.cpl**" from the command prompt.
2. Select the "**Internet Time**" tab.
3. Click “**Change Settings”**.
4. Enable “**Synchronize with an Internet time server**”.
5. In the server section, enter the IP address of the Authoritative Time Server, or one of the standard external time servers, such as **time.nist.gov**.
6. Click “**Update Now**” to force synchronize.
7. To change the interval at which the time should sync with the NTP Server, change a key in the registry located at:

```
HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\W32Time\TimeProv
iders\NtpClient
```

8. In the right pane, right-click **SpecialPollInterval**, and then click **Modify**.
9. Change from 604800 to 3600 decimal (3600 represents 60 minutes). You can change this number as per the polling intervals required by the system.).
10. Restart Windows Time service through command line using:

```
net stop w32time && net start w32time
```

11. Run the following command on computers other than the domain controller to reset each computer's time against the time server:

```
w32tm /resync /rediscover
```

17 Connex Database Restore

Before you begin...

Before starting any of the steps in this section you need to login to Central Station from the Windows shell. By default the central station is using CS Application as shell. Once you perform these steps you need to change the shell back to CS Application and restart the central station.

⚠ **WARNING** Database restore is a major database operation. This will impact following things:

1. Downtime: Entire system will be down for the entire period of the restore operation.

2. Potential loss of data: The data that is collected by the system after the backup will be lost. For example if the backup was taken at 12:00 AM on a specific date then the data collected after 12:00 AM will be lost.

Overview

There are five steps required to restore a database from backup. The five sections that follow detail each step. Execution of each step varies depending on the deployed environment and the type of database to be restored. Read each section carefully to determine the correct sequence of actions for your environment and for the database being restored.

Summary of database restore steps:

1. Preparation - Stop services, tasks, and CS Application.
2. Restore the database from backup.
3. Deprovision the restored database.
4. Restart the data sync service and wait for completion of the initial sync operation.
5. Restart services, scheduled tasks, and open the CS Application.

Preparation - Stop services, tasks and CS Application

The services and scheduled tasks described below must be stopped or disabled prior to restoring a database from backup. The list differs depending on the deployed environment and the platform to be restored.

For a connected environment with a Connex server:

1. If restoring any database in a connected environment with a Connex server, stop the data sync service on ALL central stations.
2. The sync service only runs on central station platforms and in a connected environment. This step is not necessary in a stand-alone environment.

Stop service: Welch Allyn Connex Data Synchronization Service

If restoring the database on the central server, in a connected environment

1. Stop the services and disable the tasks listed below.
    a. Stop service: Welch Allyn Process Monitor Service
    b. Stop service: Welch Allyn Network Rendezvous Service
    c. Stop service: Welch Allyn Episodic Connectivity Service
    d. Stop service: Welch AllynRSDSGateway
    e. Stop service: Welch Allyn Connex Client Services
    f. Disable Scheduled task: Welch Allyn Connex DataBackup
    g. Disable Scheduled task: Welch Allyn Connex Data Life Time Manager
    h. Disable Scheduled task: Welch Allyn Connex Late ADT Manager

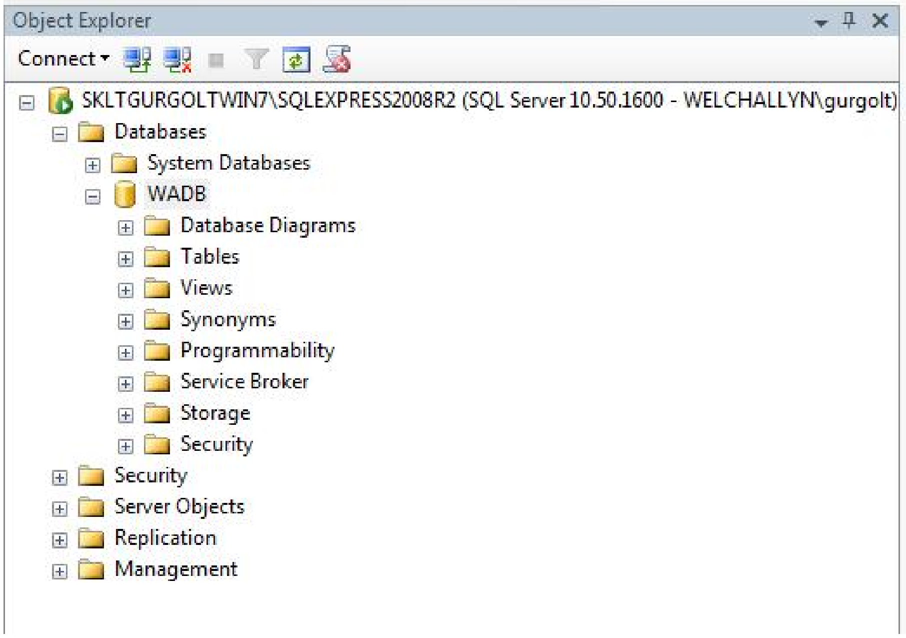
If restoring the database on a central station, in a connected environment or in a stand-alone environment

1. Close the CS application, stop the services, and disable the tasks listed below.
    a. Stop service: Welch Allyn Network Rendezvous Service
    b. Stop service: Welch Allyn Connex Continuous Connectivity Services
    c. Stop service: Welch AllynRSDSGateway
    d. Stop service: Welch Allyn Connex Trend Data Exporter Service
    e. Stop service: Welch Allyn Connex Client Services
    f. Disable Scheduled task: Welch Allyn Connex DataBackup
    g. Disable Scheduled task: Welch Allyn Connex Data Life Time Manager

Restore the database from backup

1. Open Object Explorer and expand the Databases node. An example is shown below in "Figure 17-1: Database object explorer example screen" on page 99.

Figure 17-1: Database object explorer example screen



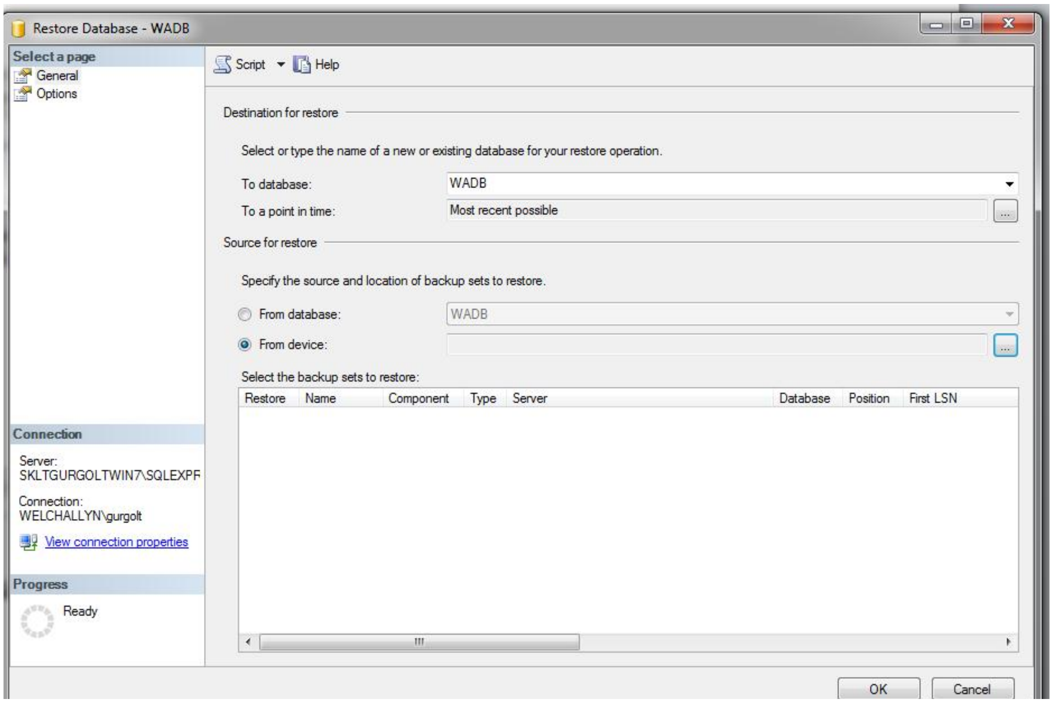
- SKLTGURGOLTWIN7\SQLEXPRESS2008R2 (SQL Server 10.50.1600 - WELCHALLYN\gurgolt)
  - Databases
    - System Databases
    - WADB
      - Database Diagrams
      - Tables
      - Views
      - Synonyms
      - Programmability
      - Service Broker
      - Storage
      - Security
  - Security
  - Server Objects
  - Replication
  - Management

2. If there is a WADB database, right-click on the WADB database node and select Tasks > Restore > Database.

3. If there is no WADB database, right-click on the Databases node and select “Restore Database…”

4. In the “Source for restore” section, select “From device”. An example is shown below in “Figure 17-2: Restore database source selection example screen”.

Figure 17-2: Restore database source selection example screen



Destination for restore

Select or type the name of a new or existing database for your restore operation.

To database: WADB

To a point in time: Most recent possible

Source for restore

Specify the source and location of backup sets to restore.

○ From database: WADB

● From device:

Select the backup sets to restore:

Restore	Name	Component	Type	Server	Database	Position	First LSN

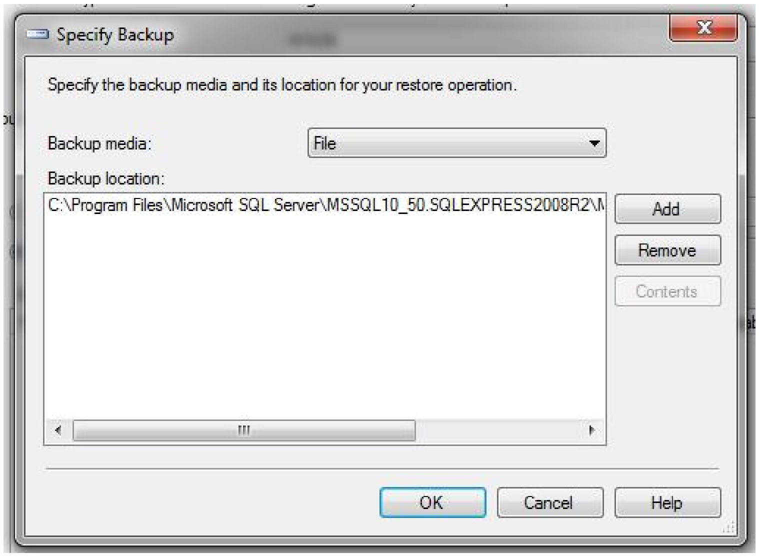
Server:
SKLTGURGOLTWIN7\SQLEXPR

Connection:
WELCHALLYN\gurgolt

Ready

5. Click on the "…" button to browse to the backup folder and select the backup file. Remove any locations listed in the Backup location box. Click the Add button and browse to the folder that contains the backup file. The Backup location box will display the selected folder containing the backup file as illustrated in the "Figure 17-3: Specify the backup location example screen" below.

Figure 17-3: Specify the backup location example screen



Specify Backup

Specify the backup media and its location for your restore operation.

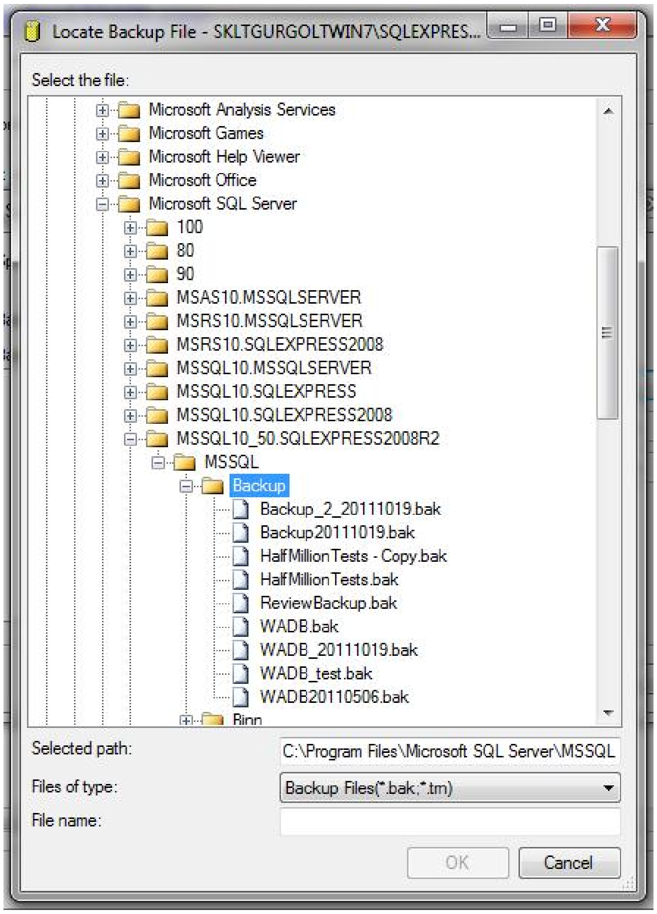
Backup media: File

Backup location:

C:\Program Files\Microsoft SQL Server\MSSQL10_50.SQLEXPRESS2008R2\M

6. Select the backup file and click **OK**. An example is shown below in "Figure 17-4: Locate the backup file example screen" on page 101.

Figure 17-4: Locate the backup file example screen



Select the file:

```
Microsoft Analysis Services
Microsoft Games
Microsoft Help Viewer
Microsoft Office
Microsoft SQL Server
    100
    80
    90
    MSAS10.MSSQLSERVER
    MSRS10.MSSQLSERVER
    MSRS10.SQLEXPRESS2008
    MSSQL10.MSSQLSERVER
    MSSQL10.SQLEXPRESS
    MSSQL10.SQLEXPRESS2008
    MSSQL10_50.SQLEXPRESS2008R2
        MSSQL
            Backup
                Backup_2_20111019.bak
                Backup20111019.bak
                HalfMillionTests - Copy.bak
                HalfMillionTests.bak
                ReviewBackup.bak
                WADB.bak
                WADB_20111019.bak
                WADB_test.bak
                WADB20110506.bak
            Binn
```

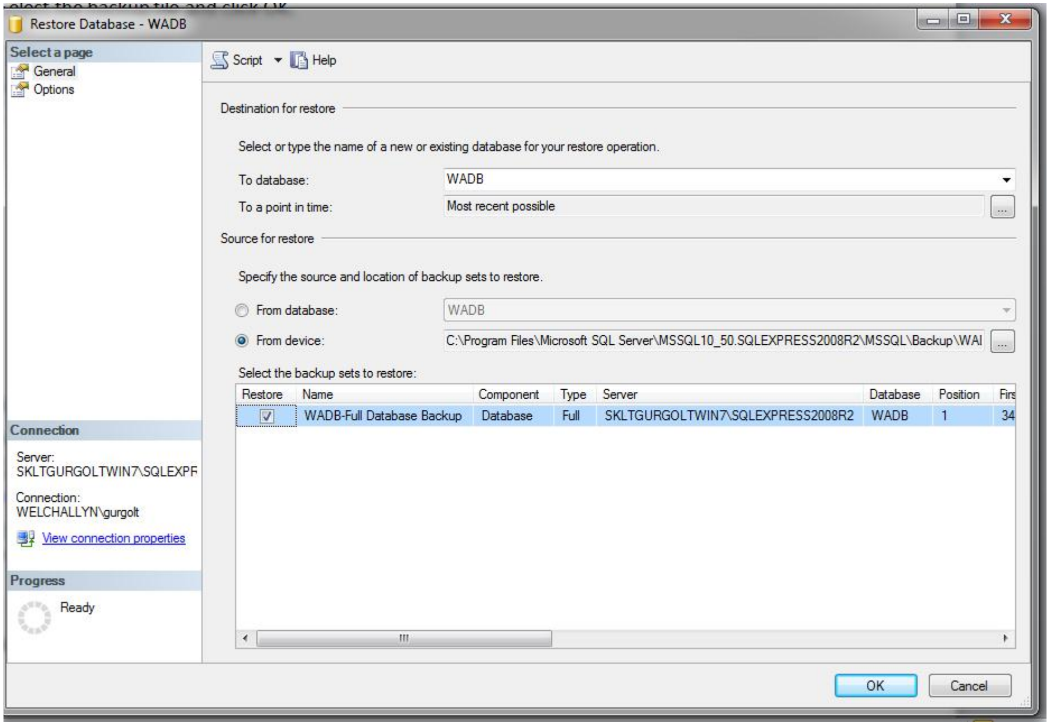
Selected path: C:\Program Files\Microsoft SQL Server\MSSQL

Files of type: Backup Files(*.bak;*.tm)

File name:

7. Click the **Restore checkbox** to select the backup. An example is shown below in "Figure 17-5: Select the restore option for the full database backup example screen".

Figure 17-5: Select the restore option for the full database backup example screen



Destination for restore

Select or type the name of a new or existing database for your restore operation.

To database: WADB

To a point in time: Most recent possible

Source for restore

Specify the source and location of backup sets to restore.

○ From database: WADB

● From device: C:\Program Files\Microsoft SQL Server\MSSQL10_50.SQLEXPRESS2008R2\MSSQL\Backup\WAI

Select the backup sets to restore:

Restore	Name	Component	Type	Server	Database	Position	Firs
☑	WADB-Full Database Backup	Database	Full	SKLTGURGOLTWIN7\SQLEXPRESS2008R2	WADB	1	34

Server:
SKLTGURGOLTWIN7\SQLEXPF

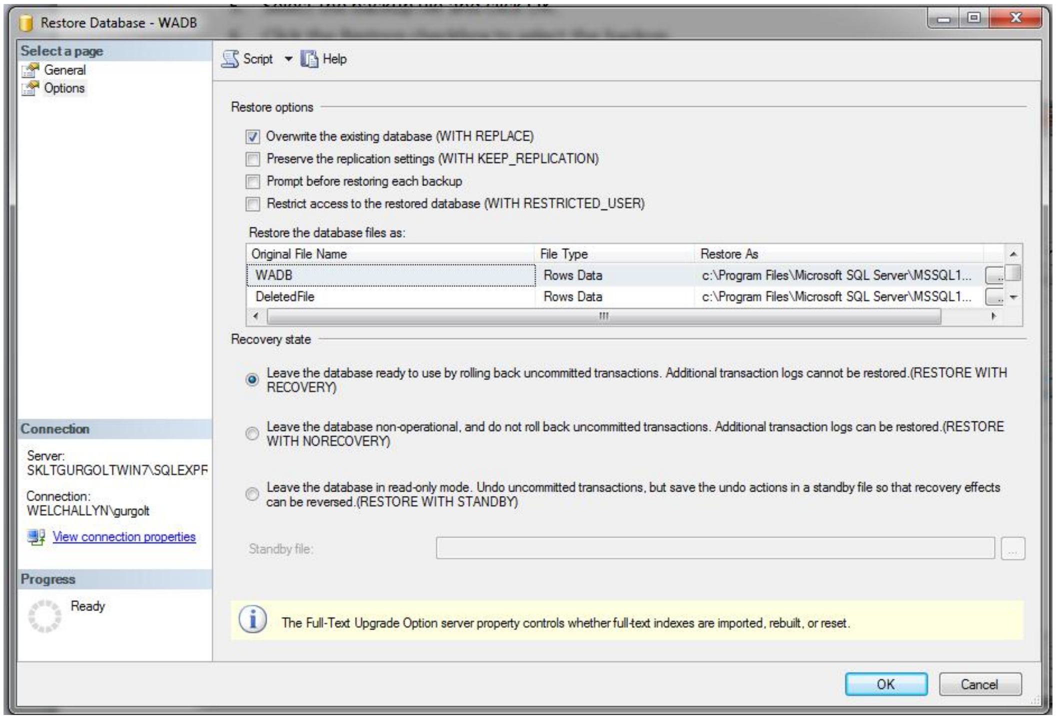
Connection:
WELCHALLYN\gurgolt

View connection properties

Ready

8. Click the Options tab and check the “Overwrite the existing database (WITH REPLACE)” as illustrated below in “Figure 17-6: Overwrite the existing database section example screen.”.

Figure 17-6: Overwrite the existing database section example screen.



Restore options

☑ Overwrite the existing database (WITH REPLACE)

□ Preserve the replication settings (WITH KEEP_REPLICATION)

□ Prompt before restoring each backup

□ Restrict access to the restored database (WITH RESTRICTED_USER)

Restore the database files as:

Original File Name	File Type	Restore As
WADB	Rows Data	c:\Program Files\Microsoft SQL Server\MSSQL1...
DeletedFile	Rows Data	c:\Program Files\Microsoft SQL Server\MSSQL1...

Recovery state

● Leave the database ready to use by rolling back uncommitted transactions. Additional transaction logs cannot be restored.(RESTORE WITH RECOVERY)

○ Leave the database non-operational, and do not roll back uncommitted transactions. Additional transaction logs can be restored.(RESTORE WITH NORECOVERY)

○ Leave the database in read-only mode. Undo uncommitted transactions, but save the undo actions in a standby file so that recovery effects can be reversed.(RESTORE WITH STANDBY)

Standby file:

The Full-Text Upgrade Option server property controls whether full-text indexes are imported, rebuilt, or reset.

Server:
SKLTGURGOLTWIN7\SQLEXPF

Connection:
WELCHALLYN\gurgolt

View connection properties

Ready

9. Click **OK** to complete the restore.

Deprovision the Restored Database

Follow these steps if the restored database is part of a connected environment. A connected environment is one in which:

- Many central stations are deployed at the same site
- AND a central server is deployed at the site
- AND the data from all central stations is kept in sync by the Connex Data Sync Service.

If the database is not part of a connected environment, it is not necessary to Deprovision the database.

To Deprovision a database with the command line utility:

1. Logon to the computer that hosts the restored database OR logon to a computer that is connected to the host via the windows network.
2. Open a command window and navigate to the directory where the Connex CS Provisioning utility has been deployed. (To locate the deployment folder, search for the program "WelchAllyn.Connex.ProvisioningUtility.exe" or consult the CS install documentation.)
3. Enter the following at the command prompt which specifies the database host address, the database instance, the database name, and the parameter which instructs the utility to Deprovision the database.
    - WelchAllyn.Connex.ProvisioningUtility.exe SERVERNAME=<server name>\<instance name> DATABASENAME=WADB APPLYDEPROVSCRIPT
4. Examine the messages produced by the Provisioning Utility to verify that the operation succeeded.

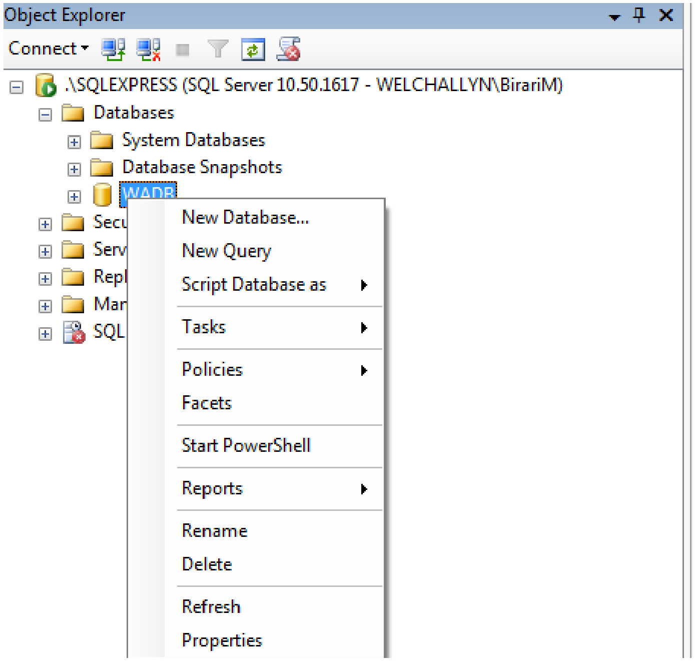
Reinstall the database on the central stations

Follow these steps only if the database is restored on the server as part of a client-server deployment, otherwise skip to "Restart Services, Scheduled Tasks, and Open the CS Application" on page 105.

To re-install the database on each central station:

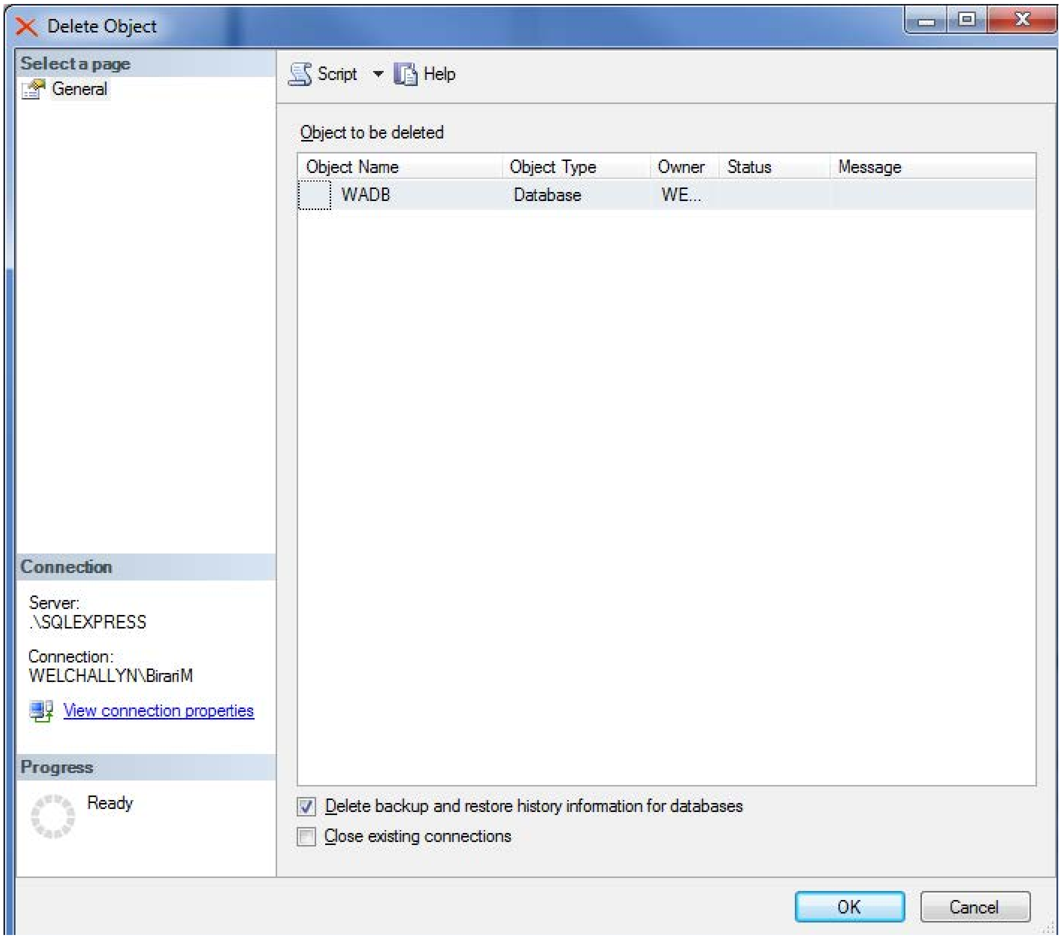
1. Open SQL Server management studio (SSMS). On CS central station this can be done by searching SSMS from the windows start menu.
2. Enter the correct login details in the pop-up dialog to enter SQL Server instance name.
3. Once SSMS is open, from the object explorer, select WADB database. Right click and the select **Delete**.

Figure 17-7: Right-click on WADB example



4. Once delete is clicked, following dialog will be shown.

Figure 17-8: Select WADB object to delete example



Object to be deleted

Object Name	Object Type	Owner	Status	Message
WADB	Database	WE...		

Server:
.\SQLEXPRESS

Connection:
WELCHALLYN\BirariM

☑ Delete backup and restore history information for databases

□ Close existing connections

5. Check the “**Close existing connections**”, and then click **OK**. The dialog will be closed once the WADB is deleted.

6. Open Windows Explorer and navigate to following path:

   C:\Program Files (x86)\Welch Allyn\Connex\Server\1.2\DataBaseInstaller.

NOTE The path may be different depending upon the location of the Program Files folder

7. Change the SQL Server name to match the local SQL Server instance name and the click **Create database**”

8. Once the WADB is installed, the installer will be closed automatically. Normally, the installer would display a successful installation message box. But this message box is not displayed if the feature **Message Box Default Reply** is enabled. In Windows 7 embedded, this feature is enabled by default. So on central stations the message box will not be displayed. But a message in the windows event log will be added confirming the success of the installation.

9. Also, after the installation is finished, a Windows message box stating that “**This program might not have installed correctly**” may be shown. Ignore this message and click **Program installed successfully** to finish the installation.

Restart the Data Sync Service and Wait for Completion of the Initial Sync Operation

Follow these steps only if the database is restored on the server as part of a client-server deployment, otherwise skip to “Restart Services, Scheduled Tasks, and Open the CS Application”.

In this step, the data sync service is restarted on ALL central stations. However, it is important to note that the best course of action is to start the data sync service on a single central station and to wait for the initial sync cycle to complete before moving on to the next central station. While the database on the central stations is empty, restarting data sync on all central stations simultaneously will result in unnecessary thrashing as all try to download data all at once from the server.

Restart Services, Scheduled Tasks, and Open the CS Application

1. Restart the services and scheduled tasks that were shutdown previously

2. Start the Connex CS Application.

Special circumstances...

In some cases over the course of use, it may be necessary to disconnect a client Central Station from the network for an extended period of time, such as construction projects.

In cases where the Central Station will be shut down or disconnected from the network for more than 30 days, it becomes necessary to purge to local database and start fresh. The local database must be dropped and recreated to maintain overall health of the system. A future update to this Administration Guide document will detail specific steps required.

18 Configure NRS

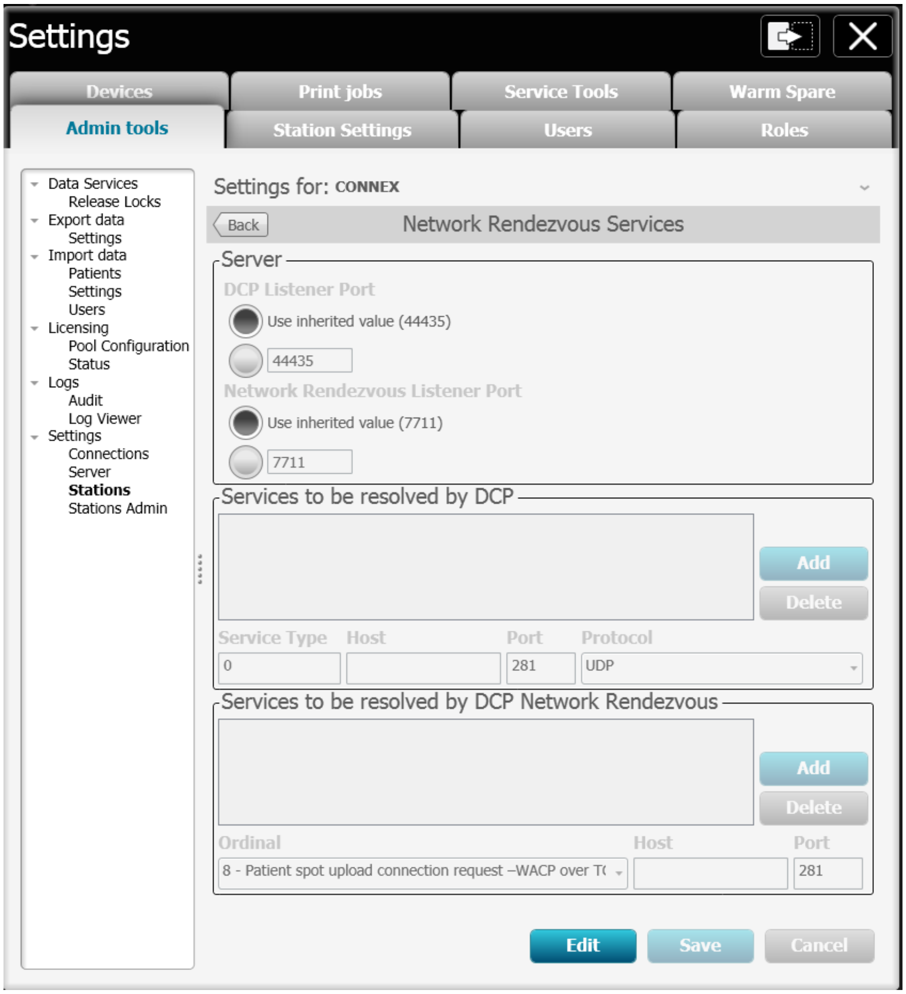
It may be necessary to configure Network Rendezvous Services. NRS runs on each central station and Connex server.

On the central station, NRS responds to devices which should be routed to the station it is running on. NRS uses the devices table to determine which station a device should be routed to. See "Managing Device assignments" on page 79 for additional information about configuring devices assignments.

To configure Network Rendezvous Services:

1. From the **Settings** > **Advanced settings** (if required) > **Admin tools** > **Stations** menu, click on **Networked Rendezvous Services**. The Network Rendezvous Services (NRS) window appears. An example is show below in "Figure 18-1: Network Rendezvous Services window example" on page 108.

Figure 18-1: Network Rendezvous Services window example



Settings for: CONNEX

Server

DCP Listener Port

● Use inherited value (44435)

○ 44435

Network Rendezvous Listener Port

● Use inherited value (7711)

○ 7711

Services to be resolved by DCP

Service Type	Host	Port	Protocol
0		281	UDP

Services to be resolved by DCP Network Rendezvous

Ordinal	Host	Port
8 - Patient spot upload connection request –WACP over T(		281

2. Observe that there are three sub-windows within the Network Rendezvous Services window.

3. Click on **Edit** near the bottom of the window.

Change Server Ports

1. In the Server window, click on the radio button next to the specific port numbers or DCP Listener Port, and NRS Listener Port.

2. Make port number changes as needed.

NOTE Refer to the *Connex CS Customer Project Req. Form* for port number information as needed. In general, these port numbers will never need to change. These port numbers should only be changed if there is more than one Connex CS server and/or stand alone central station on the same network.

Assign Host for DCP

1. In the **Services to be resolved by DCP** window, click in the **Host** field.

2. Enter the **IP address** of the **Connex CS Server** and click **Add**.

a. For a stand-alone central station, enter the IP address assigned to the COnnex Central Station computer.

b. For a networked central station, enter the IP address assigned to the Connex server.

c. Leave the **Service type** set to **0** to support legacy Spot LXi devices.

Assign Hosts for DCP Network Rendezvous

1. In the Services to be resolved by DCP Network Rendezvous window, click in the Host field to assign the proper IP address, Port, and Ordinal.

   IP address choices:

   a. Enter the IP address of the Connex CS Server (typical)

   b. For a stand-alone central station, enter the IP address assigned to the Connex Central Station CPU.

   c. For a networked central station (client-server), enter the IP address assigned to the Connex server.

2. Link the IP address for each Ordinal to be used by your devices.

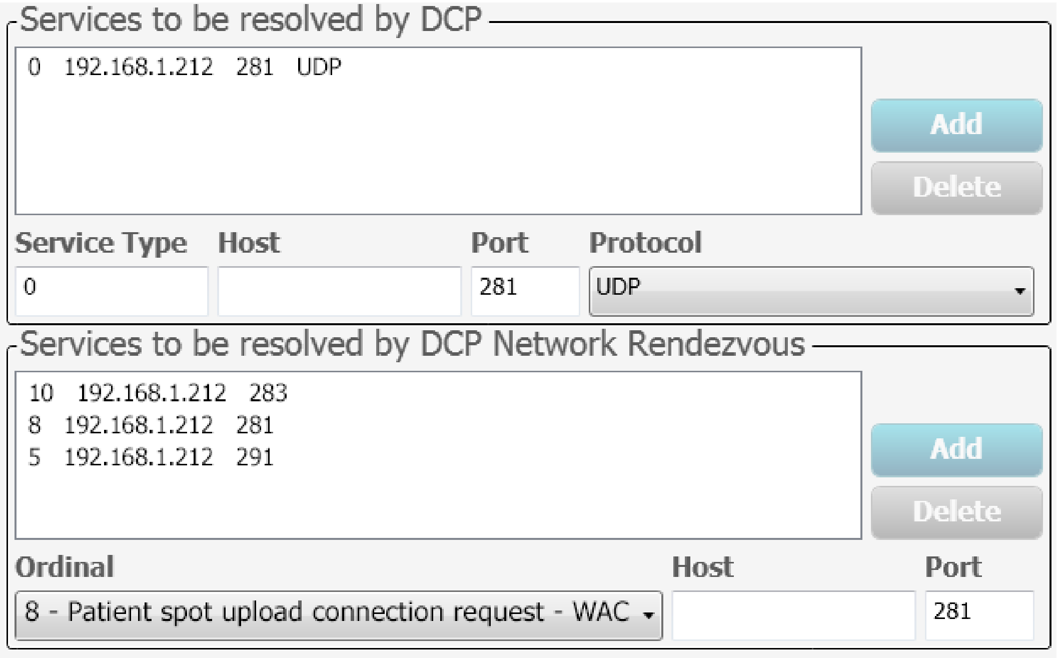
NOTE These types of connections (Ordinals) are available based on device compatibility and desired workflows. Connections typically used:

Ordinal	Device connection	Default port	Encryption
8	Spot connections (episodic) without encryption	281	
14	Spot connections (episodic) with encryption	7750	X
5	Continuous connections without encryption	291	
11	Continuous connections with encryption	7751	X
Remote services connection (Service Monitor)			
10	Remote Services connections without encryption	283	
15	Remote Services connections with encryption	16283	X

Refer to device documentation for available connectivity options.

The images below are just examples of NRS configurations. Customers may choose other Ordinal combinations as needed.

The image below depicts an example of an NRS configured without encryption.



Services to be resolved by DCP

```
0  192.168.1.212  281  UDP
```

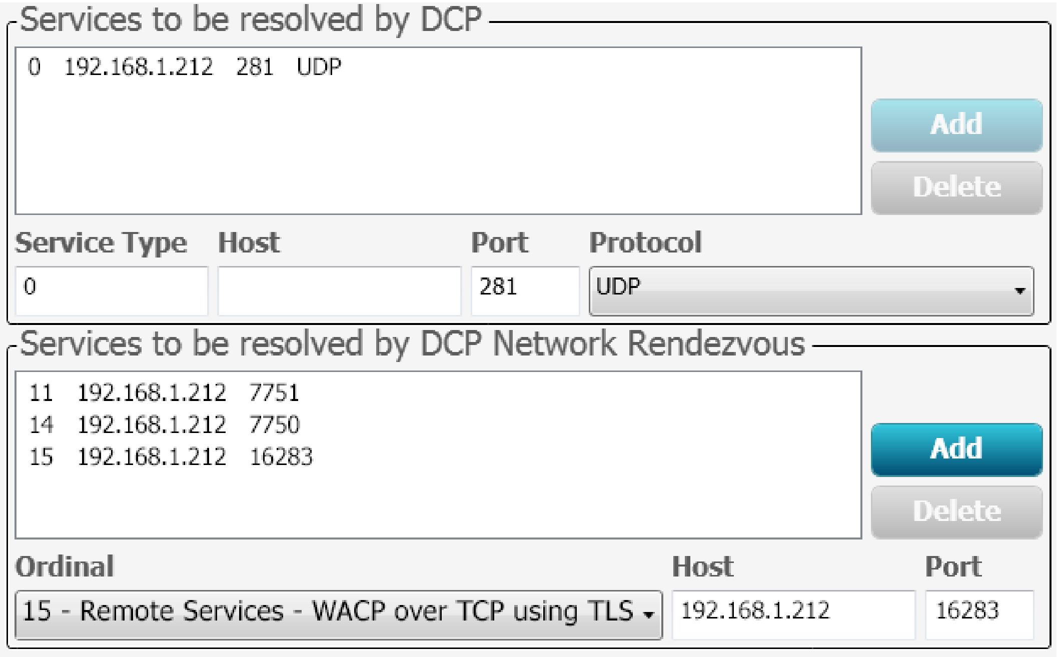
Service Type: 0
Host:
Port: 281
Protocol: UDP

Services to be resolved by DCP Network Rendezvous

```
10  192.168.1.212  283
8   192.168.1.212  281
5   192.168.1.212  291
```

Ordinal: 8 - Patient spot upload connection request - WAC
Host:
Port: 281

The image below depicts an example of an NRS configured with encryption.



Services to be resolved by DCP

```
0  192.168.1.212  281  UDP
```

Service Type: 0
Host:
Port: 281
Protocol: UDP

Services to be resolved by DCP Network Rendezvous

```
11  192.168.1.212  7751
14  192.168.1.212  7750
15  192.168.1.212  16283
```

Ordinal: 15 - Remote Services - WACP over TCP using TLS
Host: 192.168.1.212
Port: 16283

Adding an ordinal for Service Monitor

The Welch Allyn Service Monitor provides functionality to monitor the health of systems and devices on the network and provide data available to the customer via web page. To support devices sharing data with the Service Monitor service, an entry is require in the NRS settings.

In the Services to be resolved by DCP Network Rendezvous window:

1. Use the drop down menu to change the **Ordinal** to **10** or **15** (encrypted connection).
2. Click in the **Host** field, and enter the **IP address** of the **Connex CS Server** or **Service Monitor** host**.**
3. Click in the **Port** field, and enter the port number.
4. Click **Add**.
5. Click **Save** when all changes are complete.

When all NRS settings are complete...

1. Click **Save** to keep all changes.
2. Click on the **Back** button in the window header. The Stations menu appears.
3. Reboot the Central Station for changes to take effect.
4. If changes are made to a system that is in use, it may also be required to reboot all attached devices to obtain updates NRS settings information.

NRS conflicts with existing VM deployments

In some situations, changes may be required to support Connex CS applications coexisting with previously installed Connex VM deployments.

These can be managed by a number of different solutions.

- **Solution 1:** Setup each system and devices on separate networks or VLANs.
- **Solution 2:** Configure different broadcast listener ports for each central station and closet service instance.

NRS conflicts with multiple stand-alone Connex CS deployments

The same solutions may also be applied for customer environments where there are multiple stand-alone central stations within the same facility.

- **Solution 1:** Setup each system and devices on separate networks or VLANs.
- **Solution 2:** Configure different broadcast listener ports for each central station and closet service instance.

19 Configure Device connectivity

As Connex CS uses the facility's network to communicate with patient monitor devices, a number of different methods for Welch Allyn device clients to locate a server are supported, including DNS.

Device connectivity is configured and managed on each device, not at the Central Station or Connex server.

DNS Name support at device

- Use your local DNS solution.
- Compatible with Microsoft Server 2008 R2 and BIND 10.1
- Use a FQDN on the device, configurable up to 128 characters.
- Each hostname can be configured with up to 3 IP addresses, one for each Network Rendezvous Server to provide a robust solution. Refer to the ***Connex CS Customer Project Req. Form, Appendix B1*** for network information specific to your facility.
- Available with Connex CS 1.2 and higher, CVSM 2.00.05 and higher.

DHCP Option 43 / 60 support at device

- Available with Connex CS 1.5 and higher, CVSM 2.10.00 and higher.
- Customer must configure this option on the customer DHCP Server. Refer to supporting DHCP Option 43/60 documentation for selected DHCP Server types such as Microsoft, Linux, Aruba, Solaris and Cisco for assistance on setting up this type of communication system.

Network Rendezvous Service (NRS) IP at device

- Supports a standalone method for devices to locate a single system running NRS directly configured with a static IP address.
- NRS provides the IP address of the desired service, including episodic, continuous and service monitors.
- Available with Connex CS 1.2 and higher, CVSM 2.00.05 and higher.
- Manual IP setting on each device is required if changes are needed after installation.

Vitals Management (VM) IP at device

- Provides a method for existing legacy networks to maintain network communication methods with a Connex VM server using a static IP address.
- Usage of this method precludes the ability to use Welch Allyn Service Monitor and Dashboard tools.
- Manual IP setting on each device is required if changes are needed after installation.

UDP Broadcast

- Provides a method for CVSM and Spot LXi devices to communicate with Connex systems.
- Manual setting of port on each device is required if changes are needed after installation.

Roles and users

Connex CS supports the concept of Roles and Users. **Roles** define a set of system privileges. A **User** is a login identity, and each user is assigned a role.

Roles

- Click on **Settings > Advanced Settings > Roles**. The Roles window appears.
- The left hand column displays the list of existing roles.
- The box on the right displays the list of privileges, with the privileges assigned to this role checked.
- Selecting **Edit** allows the selected privileges for this role to be modified.
- The **Show System Roles** checkbox includes predefined non-clinical roles in the list if selected.

To create a new role

1. Click on **Create new role**.

   The Create New Role window appears.

2. Enter the name of the new role in the field at the top of the privileges box.
3. Select the desired privileges for this role.
4. Select **Save** to create the new role.

Users

- Click on Settings > Advanced Settings > Users. The Users window appears.
- The window displays the list of existing users.
- Clicking on a user will open the **Account Details** window displaying that user's information.
- Click **Edit** to modify a user's account.
- Click **Delete** to delete a user. Click **Yes** at the prompt.
- To find or narrow the users list, enter a search term and click **Search** to show User IDs that begin with your search term.

NOTE To reset or unlock a user's account or to edit their account, set the password to a new value, and select **Change your password the next time you log in** to force the user to change it (if desired).

To add a new user

1. Click **Add**.

   The Account Details window appears.

2. Enter the **User ID** and select the **User role.** The User ID is the logon ID for this user.
3. If needed, a Clinician ID may be assigned to this user.
4. A **Password** can be created for the user, and the user can be prompted to create a new password upon log in. If no password is specified, the configured default value is applied to this account.
5. Name information can also be entered.
6. Click **Save** to create the new user.

20 High Availability

Connex CS server (episodic only) can be deployed in a High Availability (Active-Active) configuration. The solution provides both *application redundancy* (CS Servers) and *data redundancy* (SQL Database).

About application redundancy

An active-active cluster is made up of at least two nodes, both actively running the same application service simultaneously. Application redundancy is achieved using one or more customer-provided load balancers (depending on the environment) responsible for routing traffic/load among the server instance(s). This arrangement can provide load balancing, as well as availability. If a Connex server instance is not accessible, the remaining instance(s) will continue to handle the clinical workflow.

About data redundancy

The Connex CS database, which is shared by each CS server instance, can utilize SQL Always On to achieve data redundancy. SQL Always On is a SQL Server configuration which provides a single *logical* SQL Server instance that load balances SQL traffic among a group ("Availability Group") of *actual* SQL Server instances whose databases are being kept synchronized. Since Connex CS stores most of its configuration in the database, those settings are shared between the multiple server instances.

Configuring High Availability

A minimum of four machines (not including the load balancer(s)) are required to deploy Connex CS:

- Two (2) running the Connex CS server software
- Two (2) (or more) forming the SQL Always On Availability Group

Due to the wide variety of customer network scenarios, customers are responsible for configuring and maintaining their unique High Availability networks. Refer to the ***Technical Systems Requirements (80024135), Appendix C*** to view a sample network diagram.

Changes for Network Rendezvous Service (NRS)

NRS runs on the Connex server and provides a lookup service to direct vital signs devices to the proper system upon connection to the network. The service pointers can be configured within the Connex CS Server's Admin Tool interface. Normally, NRS would point to a single Connex server. However, in High Availability configuration NRS should direct devices to the load balancer.

Changes for Corepoint Integration Engine (CIE)

Both Connex CS and Corepoint will be installed in duplicate. While each Connex CS instance can use a shared SQL Server (SQL Always On), the Corepoint instances each require their own SQL instance to avoid data conflict between each other. As such, here are the Corepoint DB configuration options:

- CIE1 uses the SQL Always On instance (along with Connex CS) while CIE2 uses a separate DB (local SQL Express or remote, non-Express SQL Server)
- Both CIE1 and CIE2 use separate DBs (local SQL Express or remote, non-Express SQL Server)

Load balancer considerations

Your infrastructure may have two load balancers:

- One handling inbound traffic between Connex vitals devices and the CS servers
- One handling outbound traffic from the CS servers to the electronic medical record (EMR)

Alternatively, a single load balancer may be used for both inbound and outbound traffic.

The load balancer(s) must be capable of maintaining 800 TCP/IP connections from Vitals devices as well as handling the EMR (ADT, ORU) traffic.

Troubleshooting

For troubleshooting, see “High Availability issues” on page 122.

A Troubleshooting

General

The following information is intended to provide frontline troubleshooting and diagnostic information. If problems cannot be corrected, contact Hillrom Technical Support for additional information.

Central Station Computer Startup

Problem	Steps
Power On LED is not on. CPU is not running.	Make sure that the AC power cord is firmly attached to the CPU and to the outlet. Ensure that the AC power outlet is “live”. Clear any paper or debris that may be blocking any of the fans on the rear of the CPU or vented covers. Press the POWER ON control to restart the CPU.
Connex CS Central Station screen is blank or frozen.	Ensure that the power is turned on for the display. Press the Input or Source control button on the display. Ensure that the correct input is being viewed. Make sure the display’s AC power cord is firmly attached to the display and to the outlet. Check all of the video cables between the CPU and the display to ensure there are no loose connections. Reboot the CPU and test again.
Keyboard does not respond Mouse does not respond.	Check the USB connectors, and extender cables if in use, to ensure that all connections are firm. Move the item to another USB connector and try. Reboot the CPU and test again.

Device & System Connectivity problems

NOTE The CSM device does not support continuous monitoring.

Problem	Diagnostic Steps / Causes / Corrections
The device not connecting to Central Station in continuous mode.	Ensure that device has a network connection (wired or wireless) with a valid assigned IP address. Make sure there is a valid network path between the device and the Central Station. Open a CMD line session on the Central Station (Settings > Advanced settings (if required) > Service tools > Command line) and ping the device by IP address (i.e. ping 172.29.0.253). On the device, confirm connection method is set properly (Settings > Advanced > Network > Server). Ensure that the proper method is in use, or confirm settings with a known working unit. Ensure IP address and port are set to correct values. On the device, confirm basic system connection with the Server Test button. (Settings > Advanced > Network > Server > Test button). Repeat after a few moments if test fails. If test passes, basic system connection is working. On the device, confirm Time zone, Date, and Time are matching those on the Central Station. Make adjustments if needed. Remember that the Central Station and Connex server may be set to automatically adjust for Daylight Savings Time (DST) or Summer Time. On the device, ensure that the Emulate Spot function is disabled. (Settings > Advanced > Data Management > Clinical Data). On the device, ensure that a patient is selected on the device (Patient List, Barcode scan, etc.). In continuous mode, data is required on the device to establish the on-screen presence at the Central Station (Room/Bed assigned or Waiting Area). On Central Station, confirm that all required services are up and running (Settings > Advanced settings (if required) > Admin tools > Settings > Connections). Note that Data Synchronization and Trend Data Exported are only used for a Client - Server environment, and may be in a red state on a stand-alone Central Station. Restart Services if required, in sequence from top to bottom.

Problem	Diagnostic Steps / Causes / Corrections
Device message “Unable to retrieve Patient List” appears on device when clicking Patients in any mode.	Ensure device connectivity is operational. See diagnostic steps above under “The device not connecting to Central Station in continuous mode.” On the Central Station, ensure there is at least one Unconfirmed patient in the Patient List. This is required to perform a Patient list retrieval at the device. Manually add a test patient if desired to test functionality, or wait for an ADT message to populate the Patient List with a new Unconfirmed patient.
On the device, the Central Station icon next to Network, toggles between connected state 🖥 and disconnected state 🖥 .	This is typically caused by Time zone, Date and Time mismatches between the device and Central Station / Connex server. On the device, confirm Time zone, Date, and Time are matching those on the Central Station. Make adjustments if needed. Remember that the Central Station and Connex server may be set to automatically adjust for Daylight Savings Time (DST) or Summer Time.

Sign on Problems: Imprivata® Single Sign On

Problem	Diagnostic Steps / Causes / Corrections
After scanning an authorized user’s badge, the user is not automatically signed into the system.	Make sure that the device on which the user is attempting a log in is connected to the network. Make sure the clinic uses Imprivata Single Sign On. To determine this, check the CS Server *Clinician Authentication* settings. If a security provider for Imprivata is present, then the clinic uses Imprivata Single Sign On. Check the CS Server *Clinician Authentication* settings and ensure that the Imprivata security provider is set up correctly. Check the ECS log files to see if the login grace period has been exceeded (c:\ProgramData\WelchAllyn\WelchAllyn.Connex.EpisodicConnectivityService\ECS\Logs). If the log files contain a message that indicates an unknown user name or password, then the login grace period may have been exceeded. Log in to Imprivata from a device or any station connected to the Imprivata system with proper credentials, including a password. This will restart the login grace period. For additional troubleshooting information, contact your Imprivata Administrator or contact Imprivata directly.

High Availability issues

The following table list some common failure points and suggestions on where to begin troubleshooting.

Assuming High Availability customer			
Issue	Symptom	Possible Cause	Additional Action
Sending vitals fail	Sending Vitals from Device to the LB always fails	• Device is improperly configured with an incorrect LB DNS Name or IP address. • The LB is improperly configured to forward traffic to the CS Servers • SQL Always On has failed or is improperly configured. Connex Client Services can't talk to the database. • The Connex DB has not synced to all servers within the Availability Group. • Check other typical connection issues for each CS Server	• Use device Serial numbers from the ECS logs to correlate with date & time stamps for where vitals are or are not being received. • Check Connex Client Services Logs for failures. • Have the customer confirm proper environmental configuration including the proper ports assignments and SQL Always On assets.
Sending vitals fail intermittently	Sending Vitals from Device to the LB intermittently fails	• (Strikethrough text for comparison only) ~~• Device is improperly configured with an incorrect LB DNS Name or IP address.~~ • The LB is improperly configured to forward traffic to the one of the two CS Servers • SQL Always On has failed or is improperly configured. Connex Client Services can't talk to the database. • The Connex DB has not synced to all servers within the Availability Group. • Check other typical connection issues for each CS Server	• Use device Serial numbers from the ECS logs to correlate with date & time stamps for where vitals are or are not being received. • Check Connex Client Services Logs for failures. • Have the customer confirm proper environmental configuration including the proper ports assignments and SQL Always On assets.

Clinician auth fails	Device fails to retrieve authenticated clinician details.	• Device is improperly configured with an incorrect LB DNS Name or IP address. • The LB is improperly configured to forward traffic to the CS Servers • SQL Always On has failed or is improperly configured. Connex Client Services can't talk to the database. • Check other typical connection issues for each CS Server • For Connex DB users only: SQL Always On has failed over and the Connex DB has not been syncing. • CS Servers' Clinician Authentication settings do not match • AD or Imprivata data entry is not correct •	• Use device Serial numbers from the ECS logs on each CS server to correlate with date & time stamps for where queries are or are not being received. • Check Connex Client Services Logs for failures. • Have the customer confirm proper environmental configuration including the proper ports assignments and SQL Always On assets.
Clinician auth fail intermittently	Device intermittently fails to retrieve authenticated clinician details.	• (Strikethrough text for comparison only) • ~~Device is improperly configured with an incorrect LB DNS Name or IP address.~~ • The LB is improperly configured to forward traffic to the CS Servers • SQL Always On has failed or is improperly configured. Connex Client Services can't talk to the database. • Check other typical connection issues for each CS Server • For Connex DB users only: SQL Always On has failed over and the Connex DB has not been syncing. • CS Servers' Clinician Authentication settings do not match • AD or Imprivata data entry is not correct	• Use device Serial numbers from the ECS logs on each CS server to correlate with date & time stamps for where queries are or are not being received. • Check Connex Client Services Logs for failures. • Have the customer confirm proper environmental configuration including the proper ports assignments and SQL Always On assets.
Call home fails	• Sync with Server fails. • Device details are not being delivered to Partners in Care solutions • Device configurations / updates not available	• Device is improperly configured when using settings other than NRS. • LB may be improperly configured for port 283 traffic to the dedicated CS server. • Partners in Care solutions software has been installed on BOTH servers. • NRS has been improperly configured.	Check Log files for: • Partners in Care solutions • ECS • NRS
ADT Fail	• New patients from the EMR are not being created. • Patient updates, transfers, and/or discharges intermittently not processing	• The LB is improperly configured to forward traffic to the CS Servers • Environment has sessions persistence configured preventing switching which CS server receives ADT traffic. • Check other typical connection issues for each CS Server	Check Log files for: • EGS • Corepoint

ADT intermittent fail	• New patients from the EMR are not being created. • Patient updates, transfers, and/or discharges • intermittently not processing	• The LB is improperly configured to forward traffic to the CS Servers • Environment has sessions persistence configured preventing switching which CS server receives ADT traffic. • Check other typical connection issues for each CS Server • One of the CS servers is not properly licensed.	Check Log files for: • EGS • Corepoint
ORU fail	• Outbounds not being received by the EMR	• Optional load balancer is improperly configured to send each CS servs connection to the EMR • EGS Vitals outbound not configured for 127.0.0.1 • CS and EMR connections contain port conflicts (Some EMRs can handle port sharing per connection but some cannot) • Environment has sessions persistence configured preventing switching which CS server sends ORU traffic. • Check other typical connection issues for each CS Server • One of the CS servers is not properly licensed.	Check Log files for: • EGS • Corepoint
ORU intermittent fail	• Outbounds occasionally not being received by the EMR	• Optional load balancer is improperly configured to send each CS servs connection to the EMR • CS and EMR connections contain port conflicts (Some EMRs can handle port sharing per connection but some cannot) • Environment has sessions persistence configured preventing switching which CS server sends ORU traffic. • Check other typical connection issues for each CS Server • One of the CS servers is not properly licensed.	Check Log files for: • EGS • Corepoint
Upgrades	• New features / DB schema not functioning properly	• CS servers traffic not restricted during upgrade	All but 1 server should have traffic restricted to begin the upgrade process. When CS servers are upgraded to the newest version, they can be left online with unrestricted traffic as long as the lower level servers have the do not contain database scheme changes.
Intentional Failover for CS (Verification) / Upgrades	• Vitals / ADT / ORU traffic to and from unintended server	• Unintended server is still running • Environment / Load balancer not configured to only send to the intended server • Firewall rule(s) blocking all CS related traffic not enabled	Depending on the environment, simply stopping CS services may not result in proper traffic control for verification. Customer cooperation may be required.

B Moving from Test to Production

This process is intended to be used to re-purpose an existing hardware or software installation of Connex CS from a test environment to a production environment. The process is often referred to as a customer's "go-live". The end-goal of this process is:

- Allow a customer to use the Connex CS system along with its other production systems (e.g. EMR/HIS).
- Remove test data from the Connex CS system so that test data is not mixed with data collection from patients in a production environment.
- Keep existing configuration and user accounts created.
- Keep existing Corepoint Action Lists modification for the HL7 interface in place, and only need to change endpoints.
- The outlined process can be used in either stand-alone or client server deployments.
- An additional step to complete the move to production involves applying a new customer provided MSSQL Standard License Key on the Connex Server. This must be implemented prior to go-live as the ship with license is for initial deployment testing purposes only.

Assumptions

- A Welch Allyn engineer (Integration or Field) is the person expected to perform this operation.
- There is a basic knowledge of how to navigate and use the Windows OS, how to gain access to the OS from the Connex CS application at the central station.
- None of the IP addresses for the connections between the Connex server or Connex CS central station PC's are changing.
- This process is not being run at night when a majority of automated system maintenance routines are being run.
- No new Connex CS central stations are being added to the deployment during this migration.

Preparation

1. On one Connex Central Station, go into **Settings** > **Advanced settings** (if required) > **Admin Tools** and make notes of the Master Bed List, Covered Area assignments, and licensing states prior to beginning.

2. If the customer is in a client-server deployment and has outbound ORU functionality, refer to the ***Connex CS Customer Project Req. Form, Section D***, to get the proper IP information for the customer's ORU HL7 interface.

3. In a client-server deployment, use the Corepoint Administration Console to **stop the Corepoint Integration Engine**. This will prevent any unwanted test results from being published to the EMR/HIS through the HL7 interface and any new test patient data coming from the test HIS/EMR system being introduced into the production system.

4. On the **server**, use the Windows Services tool to shut down Welch Allyn Connex CS services on the Connex server. **Shut down services in the following order**:

   - Process Monitor Service (if present)
   - Network Rendezvous Service
   - ADT Task Scheduler Service
   - Alarm Gateway Service
   - Episodic Connectivity Service
   - Enterprise Gateway service
   - License Service
   - Connex Client Services

5. For each **central station, including a stand-alone central station or Warm Spare station,** use the Windows Services tool to shut down Welch Allyn Connex CS services on the central station PC. **Shut down services in the following order**:

   - Process Monitor Service (if present)
   - Data Synchronization Service
   - Trend Data Exporter Service
   - Network Rendezvous Service
   - ADT Task Scheduler Service
   - Alarm Gateway Service
   - Continuous Connectivity Services
   - License Service
   - Connex Client Services

6. Copy the scripts required for this operation from DIR# 70025909.

Create a database restore point

Since this overall process or moving from test to production is intended to clear out test data, by definition, the data should not need to be recovered at a later point. However, the existing data can be backed up if necessary based on the customer's expectations and customization of the environment:

1. If the desire is to be able to restore test system data back exactly the way it was before the data is removed including patient, visits, ADT, tests, user accounts and configuration data:

   a. By default, the Connex Database Backup utility takes a database backup every night by default at approximately 12:00 a.m. (midnight). This backup can be used to restore the data in the system.

   b. Manually run the Connex Database Backup utility through the Windows Task Scheduler to get a backup as of right now.

2. If the desire is to only restore configuration and user account information: Use the Administration tools to export configuration and user account information to an XML file

that can be used to restore this data later. Refer to "Backup users and configuration" on page 25 as needed for steps to complete this function.

Clearing test data from the WADB database

Test data needs to be removed from the system acting as the server for deployment model.

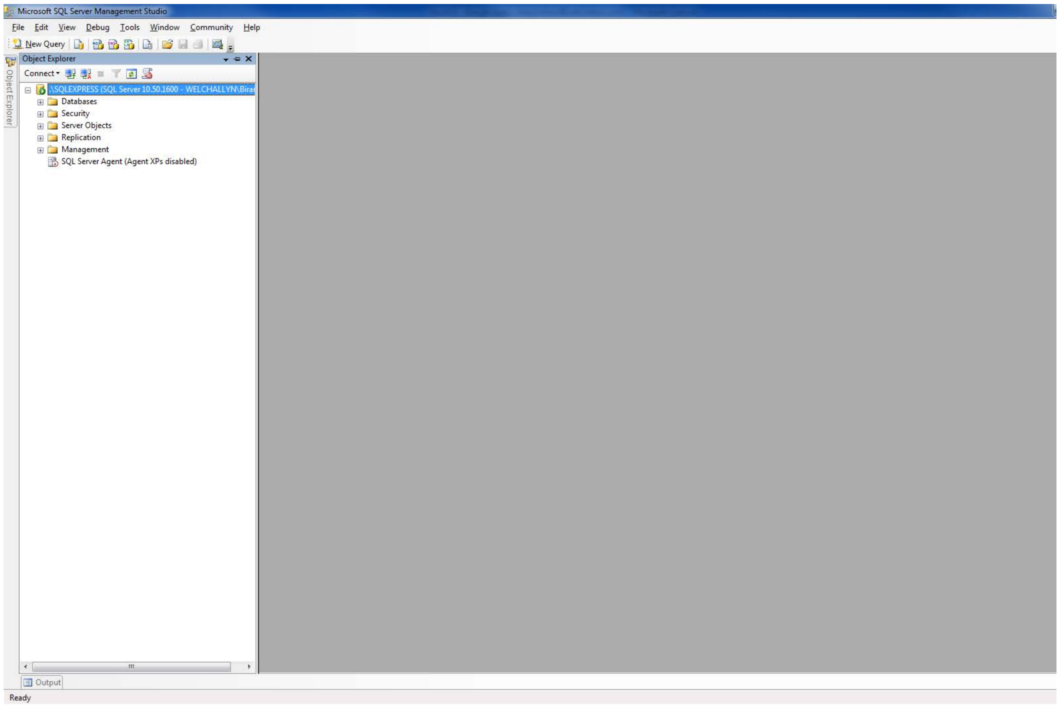
- For the client-server deployment, perform these steps on the Connex server.
- For the stand-alone deployment, perform these steps on the central station PC.

To remove test data:

1. Open the SQL Server Management Studio (SSMS).
2. From the Windows Desktop, click on **Start** > **Programs** or All Programs.
3. Navigate to **Microsoft SQL Server 2008 R2 > SQL Server Management Studio**.
4. After opening, the login screen appears on top of the SQL Server Management Studio (SSMS) application.
5. Click on **Connect**. The SSMS navigator tool appears.

NOTE It may be required to select the correct **Server name** first, using the drop-down menu tool, to choose the proper SQL Server name.

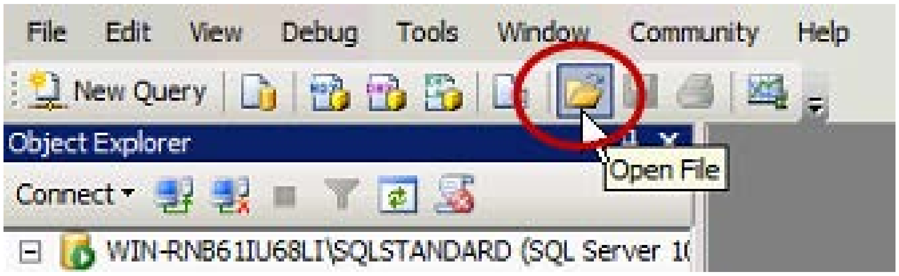
Figure B-2: Studio management navigation startup window



6. The **Object Explorer** should be visible on the left side menu.
   a. If you cannot see the object explorer, shown on the left side of the screen, click on **View > Object Explorer**.

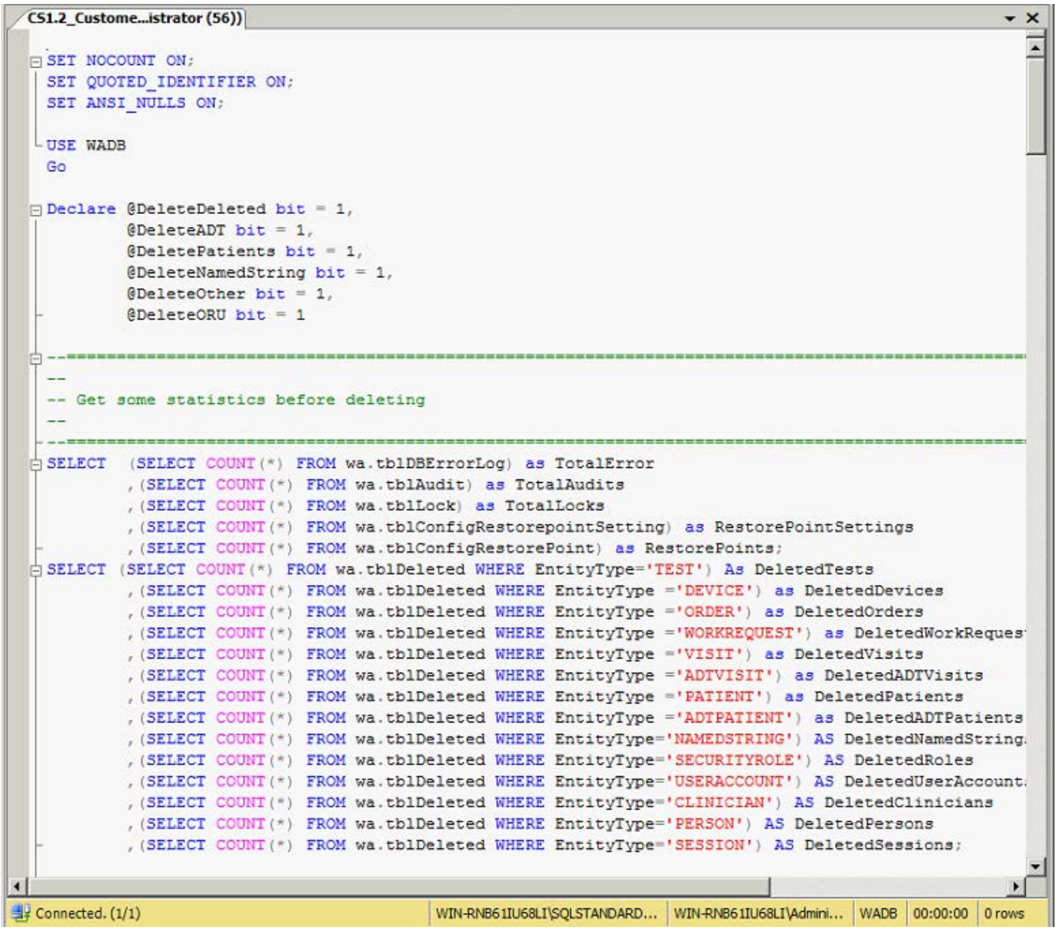
7. Click on the Open File icon.

Figure B-3: Open file icon on SSMS toolbar



8. Navigate to and select the file **CS1.2_CustomerPurge.sql**. After a few moments the script contents appear in the work window.

Figure B-4: CustomerPurge script contents in working window example

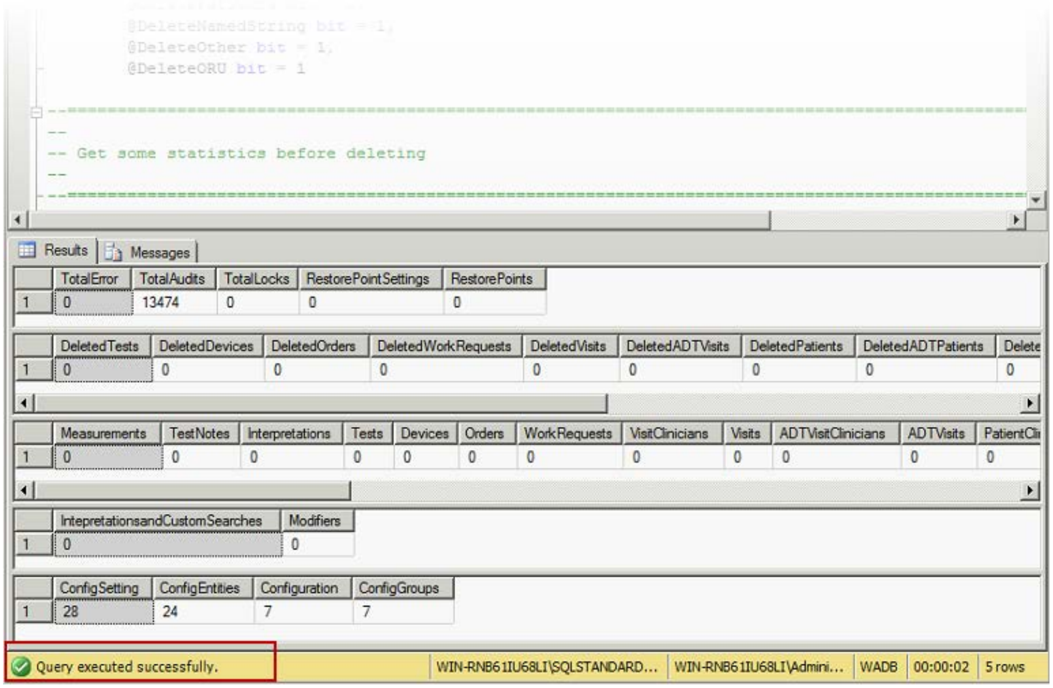

CS1.2_Custome...istrator (56))
Connected. (1/1)
WIN-RNB61IU68LI\SQLSTANDARD...
WIN-RNB61IU68LI\Admini...
WADB
00:00:00
0 rows

```
SET NOCOUNT ON;
SET QUOTED_IDENTIFIER ON;
SET ANSI_NULLS ON;

USE WADB
Go

Declare @DeleteDeleted bit = 1,
        @DeleteADT bit = 1,
        @DeletePatients bit = 1,
        @DeleteNamedString bit = 1,
        @DeleteOther bit = 1,
        @DeleteORU bit = 1

--===============================================================================================
--
-- Get some statistics before deleting
--
--===============================================================================================
SELECT  (SELECT COUNT(*) FROM wa.tblDBErrorLog) as TotalError
        ,(SELECT COUNT(*) FROM wa.tblAudit) as TotalAudits
        ,(SELECT COUNT(*) FROM wa.tblLock) as TotalLocks
        ,(SELECT COUNT(*) FROM wa.tblConfigRestorepointSetting) as RestorePointSettings
        ,(SELECT COUNT(*) FROM wa.tblConfigRestorePoint) as RestorePoints;
SELECT (SELECT COUNT(*) FROM wa.tblDeleted WHERE EntityType='TEST') As DeletedTests
        ,(SELECT COUNT(*) FROM wa.tblDeleted WHERE EntityType ='DEVICE') as DeletedDevices
        ,(SELECT COUNT(*) FROM wa.tblDeleted WHERE EntityType ='ORDER') as DeletedOrders
        ,(SELECT COUNT(*) FROM wa.tblDeleted WHERE EntityType ='WORKREQUEST') as DeletedWorkReques
        ,(SELECT COUNT(*) FROM wa.tblDeleted WHERE EntityType ='VISIT') as DeletedVisits
        ,(SELECT COUNT(*) FROM wa.tblDeleted WHERE EntityType ='ADTVISIT') as DeletedADTVisits
        ,(SELECT COUNT(*) FROM wa.tblDeleted WHERE EntityType ='PATIENT') as DeletedPatients
        ,(SELECT COUNT(*) FROM wa.tblDeleted WHERE EntityType ='ADTPATIENT') as DeletedADTPatients
        ,(SELECT COUNT(*) FROM wa.tblDeleted WHERE EntityType='NAMEDSTRING') AS DeletedNamedString
        ,(SELECT COUNT(*) FROM wa.tblDeleted WHERE EntityType='SECURITYROLE') AS DeletedRoles
        ,(SELECT COUNT(*) FROM wa.tblDeleted WHERE EntityType='USERACCOUNT') AS DeletedUserAccount
        ,(SELECT COUNT(*) FROM wa.tblDeleted WHERE EntityType='CLINICIAN') AS DeletedClinicians
        ,(SELECT COUNT(*) FROM wa.tblDeleted WHERE EntityType='PERSON') AS DeletedPersons
        ,(SELECT COUNT(*) FROM wa.tblDeleted WHERE EntityType='SESSION') AS DeletedSessions;
```

9. Click on Execute or press the ***F5*** key to run the script. After a few moments, the script output appears in a grid view table near the bottom of the working window.

NOTE The amount of time it takes for the script to complete will vary slightly depending on how much test data is present in the database.

Figure B-5: Purge script executed successfully example



```
        @DeleteNamedString bit = 1,
        @DeleteOther bit = 1,
        @DeleteORU bit = 1

--==========================================================================================
--
-- Get some statistics before deleting
--
--==========================================================================================
```

	TotalError	TotalAudits	TotalLocks	RestorePointSettings	RestorePoints
1	0	13474	0	0	0

	DeletedTests	DeletedDevices	DeletedOrders	DeletedWorkRequests	DeletedVisits	DeletedADTVisits	DeletedPatients	DeletedADTPatients	Delete
1	0	0	0	0	0	0	0	0	0

	Measurements	TestNotes	Interpretations	Tests	Devices	Orders	WorkRequests	VisitClinicians	Visits	ADTVisitClinicians	ADTVisits	PatientCli
1	0	0	0	0	0	0	0	0	0	0	0	0

	IntepretationsandCustomSearches	Modifiers
1	0	0

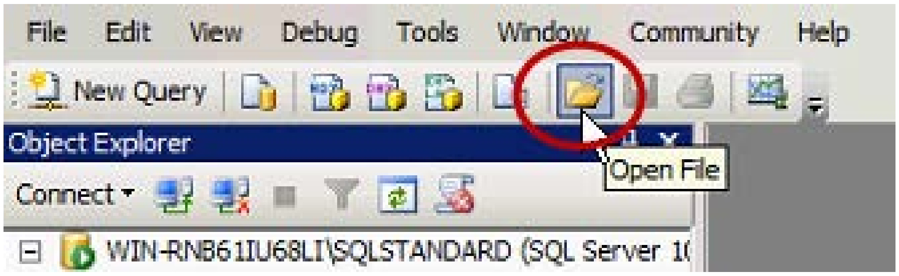
	ConfigSetting	ConfigEntities	Configuration	ConfigGroups
1	28	24	7	7

Query executed successfully. | WIN-RNB61IU68LI\SQLSTANDARD... | WIN-RNB61IU68LI\Admini... | WADB | 00:00:02 | 5 rows

10. Confirm that the yellow status bar at the bottom of the working window displays "*Query executed successfully*".

11. Click on the **Open File** icon.

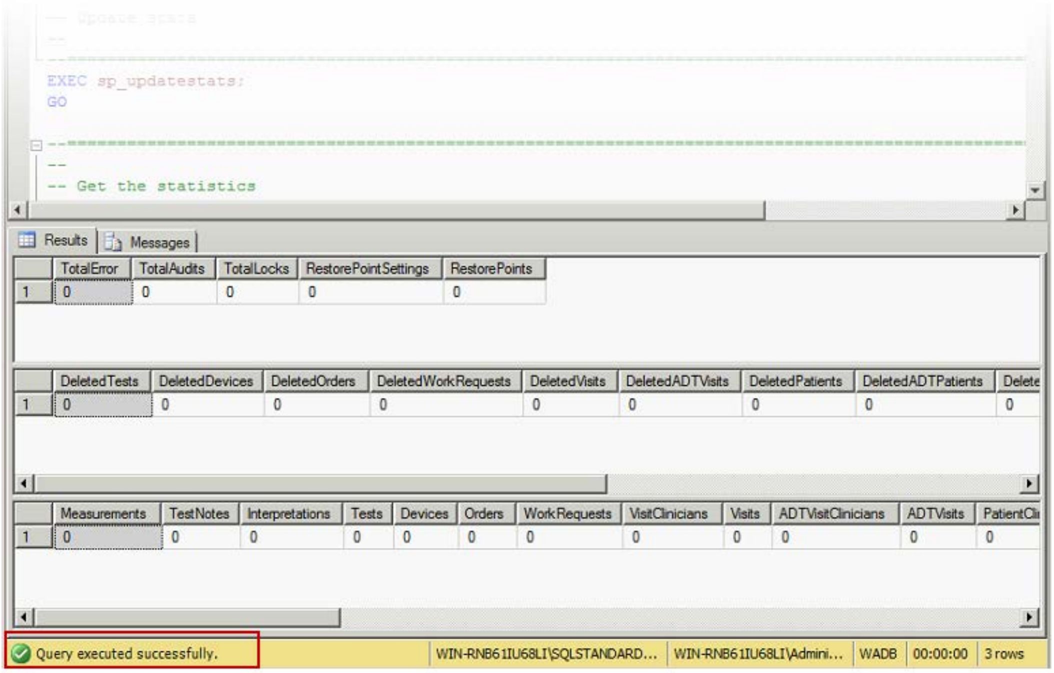
Figure B-6: Open file icon on SSMS toolbar



12. Navigate to and select the file **CS1.2_CustomerPurge_Verification.sql**. After a few moments the script contents appear in the work window.

13. Click on Execute or press the ***F5*** key to run the script. After a few moments, the script output appears in a grid view table near the bottom of the working window.

Figure B-7: Purge verification script executed successfully example



```
-- Update stats
--
--=====================================================================

EXEC sp_updatestats;
GO

--=====================================================================
--
-- Get the statistics
```

	TotalError	TotalAudits	TotalLocks	RestorePointSettings	RestorePoints
1	0	0	0	0	0

	DeletedTests	DeletedDevices	DeletedOrders	DeletedWorkRequests	DeletedVisits	DeletedADTVisits	DeletedPatients	DeletedADTPatients	Delete
1	0	0	0	0	0	0	0	0	0

	Measurements	TestNotes	Interpretations	Tests	Devices	Orders	WorkRequests	VisitClinicians	Visits	ADTVisitClinicians	ADTVisits	PatientCli
1	0	0	0	0	0	0	0	0	0	0	0	0

Query executed successfully. | WIN-RNB61IU68LI\SQLSTANDARD... | WIN-RNB61IU68LI\Admini... | WADB | 00:00:00 | 3 rows

14. Confirm that the yellow status bar at the bottom of the working window displays "*Query executed successfully*".

15. Confirm that all counts appear as zeros.

16. Close the SSMS application.

17. If necessary, make changes to the IP address on Ethernet port LAN2 on the Connex server, using Windows standard network configuration tools.

18. Reboot the Connex server or central station PC to restart all services in the proper sequence.

19. For a stand-alone deployment, go to "Restart after synchronization is complete" on page 133 to continue.

Configure HL7 connections, if required

1. If the network has an HL7 ADT interface workflow, perform the following. Otherwise, skip this step.

    a. Work with the HL7 Interface developer at the customer to change (or setup) the endpoint in the customer's ADT system to point to the endpoint that Corepoint is listening for ADT messages on.

    b. Using the Corepoint Administration screen, confirm that the connection is up and active.

2. If the network has a HL7 ORU outbound workflow, perform the following. Otherwise, skip this step.

    a. Using Corepoint, modify the ORU outbound connection(s) to publish observation data to the endpoints identified in step 1 in the Preparation section.

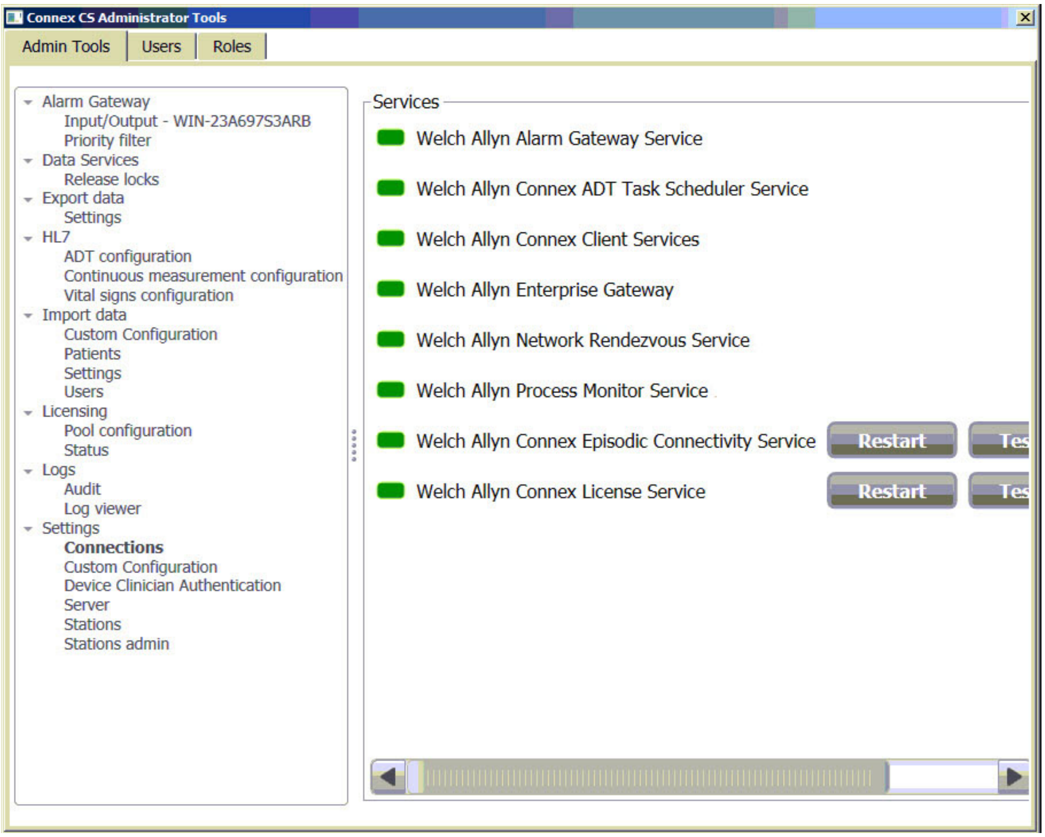
b. Using the Corepoint Administration screen, confirm that the connection(s) is up and active.

Confirm Connex server operation, client-server only

These steps are only applicable for the client-server deployment. For a stand-alone deployment, go to “Restart after synchronization is complete” on page 133 to continue.

1. After the Connex server reboot is complete, login as with the Windows administrator account.
2. Click on Cx to Open the Connex CS Admin Tools launcher from the desktop.
3. In the Admin Tools, navigate to **Settings > Connections**. The Services window appears.

Figure B-8: Connex server connections and services window example



Services

🟩 Welch Allyn Alarm Gateway Service

🟩 Welch Allyn Connex ADT Task Scheduler Service

🟩 Welch Allyn Connex Client Services

🟩 Welch Allyn Enterprise Gateway

🟩 Welch Allyn Network Rendezvous Service

🟩 Welch Allyn Process Monitor Service

🟩 Welch Allyn Connex Episodic Connectivity Service

🟩 Welch Allyn Connex License Service

4. Confirm that all services are in a green state. Click on **Restart** button to restart a service if required.

Synchronize central stations, client-server only

1. At each **central station, including a Warm Spare station,** use the Windows Services tool to start Welch Allyn Connex CS services on the central station PC. **Start services in the following order**:

- Connex Client Services
- License Service
- Continuous Connectivity Services
- Alarm Gateway Service
- ADT Task Scheduler Service
- Network Rendezvous Service
- Trend Data Exporter Service
- Data Synchronization Service
- Process Monitor Service (if present)

2. Wait 30 minutes (minimum). This will give time for the database changes (deletes) to synchronize with all the central stations.

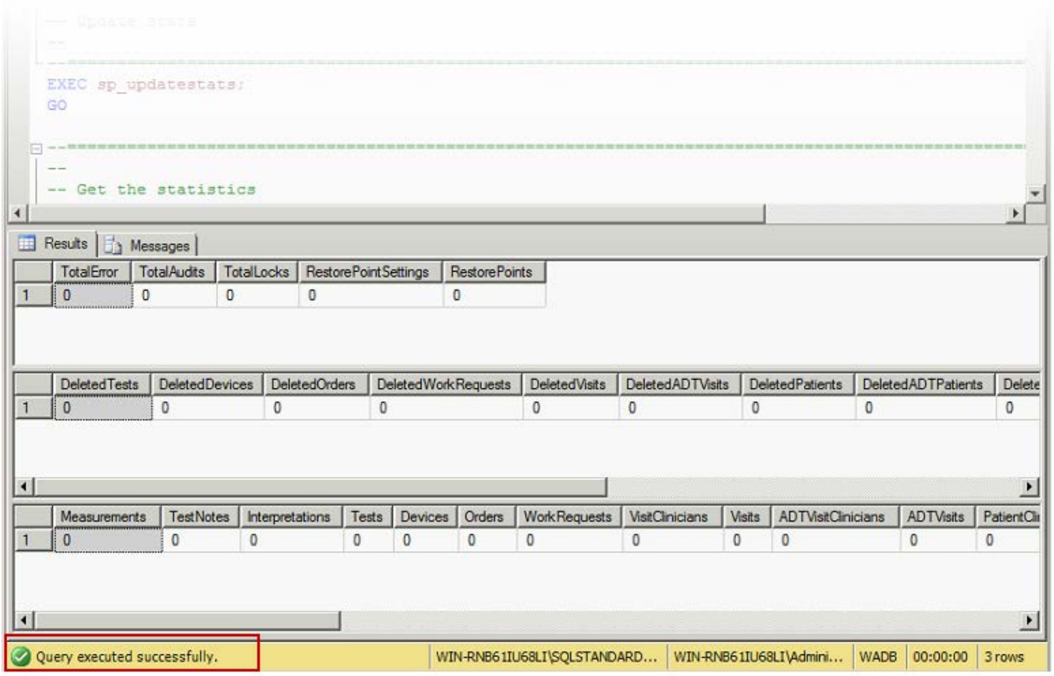
NOTE The amount of time necessary for the synchronization to occur may vary depending on the amount of data to be synchronized and the number of central stations in the environment.

3. Verify that each central station has synchronized with the Connex server database. This can be verified by performing any of the following on each central station:

   a. Within the Connex CS Application, navigate to the **Patient list** > **Search tab** and perform a patient search. The resulting list should return zero (0) records.

   b. From the SSMS tool, open the file **CS1.2_CustomerPurge_Verification.sql**, and click on Execute or press the *F5* key to run the script. After a few moments, the script output appears in a grid view table near the bottom of the working window.

Figure B-9: Purge verification script executed successfully example



```
-- Update stats
--
--=========================================================
EXEC sp_updatestats;
GO

--=========================================================
--
-- Get the statistics
```

	TotalError	TotalAudits	TotalLocks	RestorePointSettings	RestorePoints
1	0	0	0	0	0

	DeletedTests	DeletedDevices	DeletedOrders	DeletedWorkRequests	DeletedVisits	DeletedADTVisits	DeletedPatients	DeletedADTPatients	Delete
1	0	0	0	0	0	0	0	0	0

	Measurements	TestNotes	Interpretations	Tests	Devices	Orders	WorkRequests	VisitClinicians	Visits	ADTVisitClinicians	ADTVisits	PatientCli
1	0	0	0	0	0	0	0	0	0	0	0	0

```
Query executed successfully.    WIN-RNB61IU68LI\SQLSTANDARD...  WIN-RNB61IU68LI\Admini...  WADB  00:00:00  3 rows
```

   c. Using Windows explorer, navigate to **C:\ProgramData\Welch Allyn\Welch Allyn Connex Data Synchronization Service 1.0** and check the sync logs on the central station for any errors.

Restart after synchronization is complete

1. In a client-server deployment, restart the Connex Server. After the server restart is complete, restart each central station or Warm Spare station.
2. In a stand-alone deployment, just restart the central station.

NOTE Restarting provides the easiest way to restart all services in the proper order after all synchronization activity is complete.

Finalizing the Environment

Once the test data has been cleared and the Connex Server and or Connex CS central stations have been rebooted, there may be a few additional steps:

1. On one of the Connex CS central stations, go into the administration tools within the CS Application and confirm that the Master Bed List, Covered Areas and licensing are all setup appropriately. Compare the current state with notes collected during the preparation phase as appropriate.
2. In a client-server deployment where there is an HL7 ADT interface configured with the customer's HIS/EMR system, perform the following. Otherwise, skip this step.
   a. Have the customer start sending HL7 ADT messages from the HIS/EMR.
   b. Wait for 2 to 5 minutes and then go to one of the Connex CS central stations and go to the Search screen to see that patients are showing up when a search is executed. If no patients are showing up, then work with the HL7 Interface programmer to resolve HL7 interface problems as necessary.
3. Turn on and start using the Welch Allyn devices. The devices should be able to do patient list and patient look up activities and the Connex CS central station(s) should start displaying tiles with data as patients are either monitored or episodic readings are taken on the patients.
4. In a client-server deployment where the customer has an HL7 ORU outbound workflow, perform the following. Otherwise, skip this step.
   a. Work the with the customer's HL7 Interface Developer to confirm that any episodic data captured since step 3 of this section have been published to the customer's HIS/EMR.
   b. If no episodic readings have been taken on a patient since step 3, work with the customer to get an episodic reading taken to verify that the readings are making it from the device to the Connex Server to the customer's HIS/EMR.
   c. Work the with the customer's HL7 Interface Developer to confirm that any continuous data captured since step 3 of this section have been published to the customer's HIS/EMR.
   d. If no patients have been continuously monitored since step 3, work with the customer to start continuously monitoring a patient to verify that the continuous data is making it from the device to the Connex Central Station to the customer's HIS/EMR.

Troubleshooting test to production issues

If problems arise in the process of moving from a test to production environment, at least two things can be done:

1. Perform the database restore operation as outlined in the "Connex Database Restore" on page 97, on the backup that was taken in the "Create a database restore point" on page 126.
2. Uninstall and re-install the database per the instruction in "Connex Database Restore" on page 97. Once this is done, the Admin Tool import function can be used to import the user accounts and configuration data that were exported in the Preparation section.

C ProView

Intended use

Welch Allyn Connex® ProView allows the user to review data actively being processed by the Welch Allyn Connex® CS system for the purpose of troubleshooting issues with data processing. As part of system installation and verification, ProView also allows the user to create a vitals test record in order to test EMR connectivity.

Users of ProView are expected to have strong computer skills and will use the software as a means to help diagnose workflow, networking, or configuration issues that might prevent patient data from reaching the EMR. Typical users include Welch Allyn service team members and HL7 system administrators.

Installation and setup

To install ProView

1. Copy the Connex ProView Installer to the local disk and run **ConnexProViewSetup.exe**.

   A setup window appears.

2. Click **Next** to begin the installation.

   A license agreement appears.

3. Read and accept the license agreement and click **Next**.
4. Enter the Connex Server IP address in the Connex Server Address dialog box and click **Next**.

NOTE If you are installing ProView on a server, ensure that **localhost** is entered in the IP address input box. Otherwise, enter the IP address of the target server.

5. Setup installs the program files to the local system. Click **Finish** to complete the installation.

   ProView is now installed. A shortcut for ProView is created on the desktop.

Create roles and users

Before using ProView, roles and users must be created.

Create the ProView role

1. From the Connex CS Server desktop, launch Connex CS Administrator Tools (Cx).
2. Select the **Role** tab and click **Create new role**.
3. Enter **ProView** as the new role, and select the **AdminSystem** privilege.
4. Click **Save**.

   A confirmation dialog appears indicating the role is saved.
5. Click **OK**.

Create the VitalTestApp role

⚠ **WARNING** Patient data risk. Create the VitalTestApp role only in your network's test environment. Do not create this role in an environment that interacts with actual patients. Sending vitals tests to a live hospital network may interfere with current patient data.

1. If necessary, launch Connex CS Administrator Tools.
2. Select the **Role** tab and click **Create new role**.
3. Enter **VitalTestApp** as the new role, select the **AdminSystem**, **CreatePatient**, **CreateTest**, and **EditAnyPatient** privileges.
4. Click **Save**.

   A confirmation dialog appears indicating the role is saved.
5. Click **OK**.

Create the ProView user

1. If necessary, launch Connex CS Administrator Tools.
2. Select the **User** tab and click **Add**.
3. Enter the user information and select **ProView** in the **User Roles** section.
4. Click **Save**.

   A confirmation dialog appears indicating the role is saved.
5. Click **OK**.

Create the VitalTestApp user

1. If necessary, launch Connex CS Administrator Tools.
2. Select the **User** tab and click **Add**.
3. Enter the user information and select **VitalTestApp** in the **User Roles** section.
4. Click **Save**.

   A confirmation dialog appears indicating the role is saved.
5. Click **OK**.

Create the BioMed user

1. If necessary, launch Connex CS Administrator Tools.
2. Select the **User** tab and click **Add**.
3. Enter the user information and select **BioMed** in the **User Roles** section.
4. Click **Save**.

   A confirmation dialog appears indicating the role is saved.
5. Click **OK**.

Using ProView for data review

ProView allows you to review patient data and vital signs test data to verify the data currently being processed by the Connex CS system for the troubleshooting of issues.

NOTE It is important to keep in mind that Proview is designed to display raw patient and vital signs data out of the central station database. The data is not formatted for display as it would be for clinical use. This design facilitates investigation into data processing issues, although it can require additional effort on the part of the user to perform functions like the conversion of Units of Measure.

Logging in

1. On the desktop, double-click the Connex ProView icon.

   A login screen appears.
2. Enter your User ID and Password, and click **Login**.

   The ProView home screen appears.

Display the patient list

1. Log in to the program as described.

   The home screen appears.
2. Click **Patients** to open the patient list.

   The patient list appears.

Search the patient list

1. Log in to the program as described.

   The home screen appears.

2. Click **Patients** to open the patient list.

   The patient list appears.

3. Enter the search criteria in the **Search Patient** window located at the top of the screen.

4. (Optional) To perform an advanced search, click **Advanced search**.

   The Advanced search window appears.

5. (Optional) To filter by care unit, select the desired care unit from the **Care unit** pull-down menu.

6. To sort the patient list, select the desired sorting method from the **Arrange by** pull-down menu.

   - Click the sort icon (▲▼) to change the sorting order.
   - Click the refresh icon (⟳) to refresh the list.

7. Click the print icon (🖨) to print the list. In the **Printing options window**, verify the correct printer, page size, and orientation are selected, and click **Print**.

Display the vitals test list

1. Log in to the program as described.

   The home screen appears.

2. Click **Tests** in the tab on the left.

   The vitals test list window appears.

3. (Optional) Adjust the timeline bar to surround the desired time of interest. The vitals test list is displayed.

4. (Optional) Click the Refresh icon to refresh the list, or click 🖨 to print the list.

5. If you are printing the list, verify that the correct printer, page size, and orientation are selected, and click **Print**.

Using a vitals test record to test EMR connectivity

In addition to the review functionality, the program allows you to create a vitals test without having the central station involved. Use this method to test the EMR connectivity.

Create a vitals test record

⚠ **WARNING** Patient data risk. Sending vitals tests to a live hospital network may interfere with current patient data. Perform this function only in your network's test environment.

1. Log in to ProView using the **VitalTestApp** role.

   The Home screen appears.

2. Select a patient from the list and go to the Patient Details screen.

   The **Take Measurements** button appears on the top right of the screen.

NOTE ProView does not provide a means to create a new patient. New patients must be added to Connex CS via inbound ADT data.

3. Click **Take Measurements**.

   The measurement entry screen appears.

4. Use the pre-populated default values or enter values for the current vitals measurements. Episodic measurements represent confirmed data, and simulated continuous measurements represent unconfirmed data.

NOTE Any text entered in the Note area on this screen will not be passed through to the EMR.

5. If you are sending episodic measurements, make sure you click the checkbox next to **Confirmed by fake clinician**. If you are sending simulated continuous measurements, make sure the checkbox next to **Confirmed by fake clinician** is not checked.

6. Click **Save**.

   The test record is displayed in the Patient Details test list. Use the EMR Status to verify that the test record was successfully sent to the EMR.

NOTE This screen does not automatically update. Once the vitals test record is sent, the vitals measurements return to the pre-populated default values.

7. To start a new vitals test, return to step 2. You must click **Save** each time you want to send a new test record.

Reference

Uninstall ProView

1. Open the Control Panel (Start > Control Panel) and select Programs>Uninstall a program.
2. Navigate to Welch Allyn Connex ProView and right-click on the item.
3. Select **Uninstall**. If a confirmation dialog pops up, click **Yes**.

Update the server IP address

If ProView's target server has changed, update the program's configuration file to change all service endpoints to ensure that they are pointing to the new server IP address.

1. Navigate to **C:\Program Files (x86)\Welch Allyn\Connex\ProView\1.0**
2. Open the file **ConnexProView.exe.config** in the text editor. Search for the endpoint with a name LicenseLocal. Update the address as indicated below with the new server IP address and save the changes.

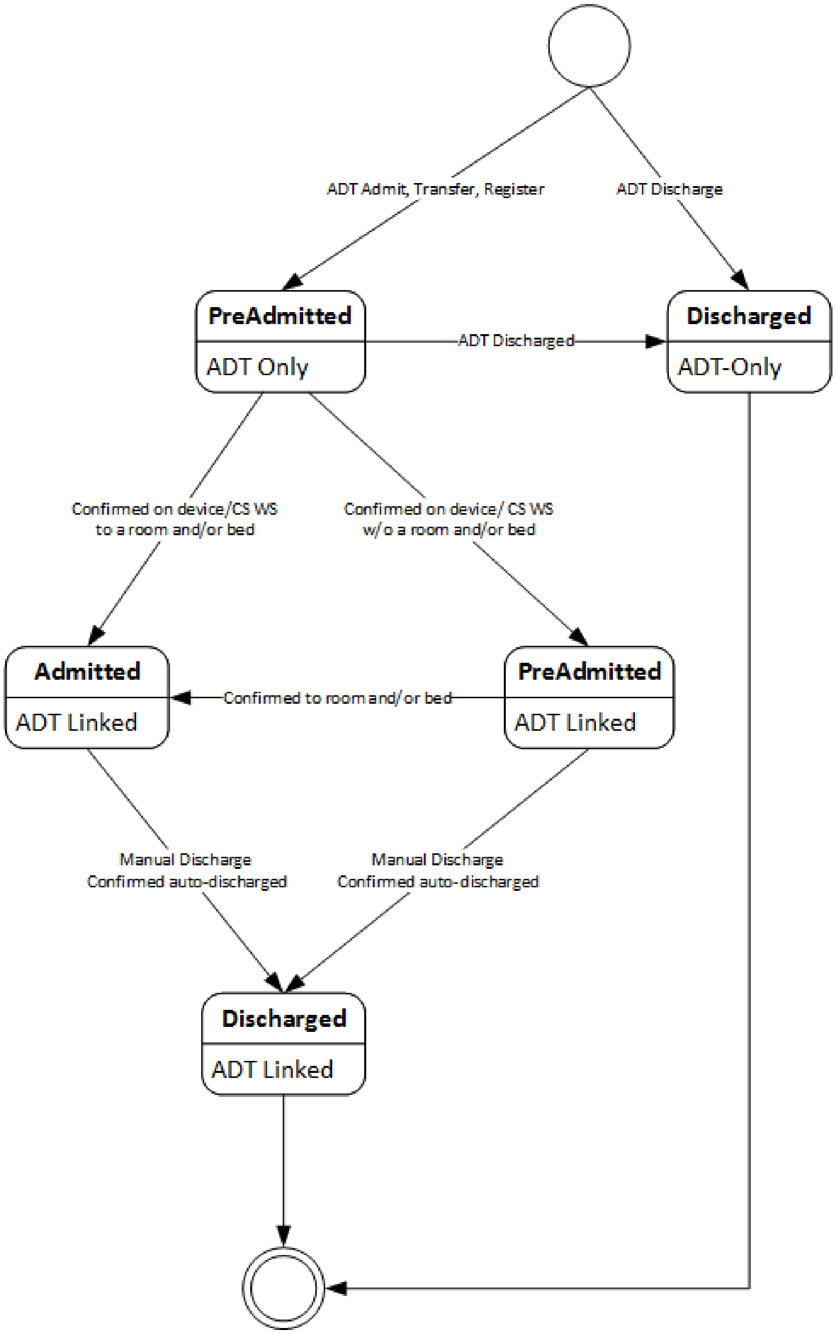
   ```
   <endpoint name="LicenseLocal" address="net.tcp://172.29.2.22:7733/LicenseServices/Secure" ... />
   ```

3. Update the address of other endpoints with name **SessionLocal**, **DataLocal**, **AdminLocal**, and **AboutLocal**.

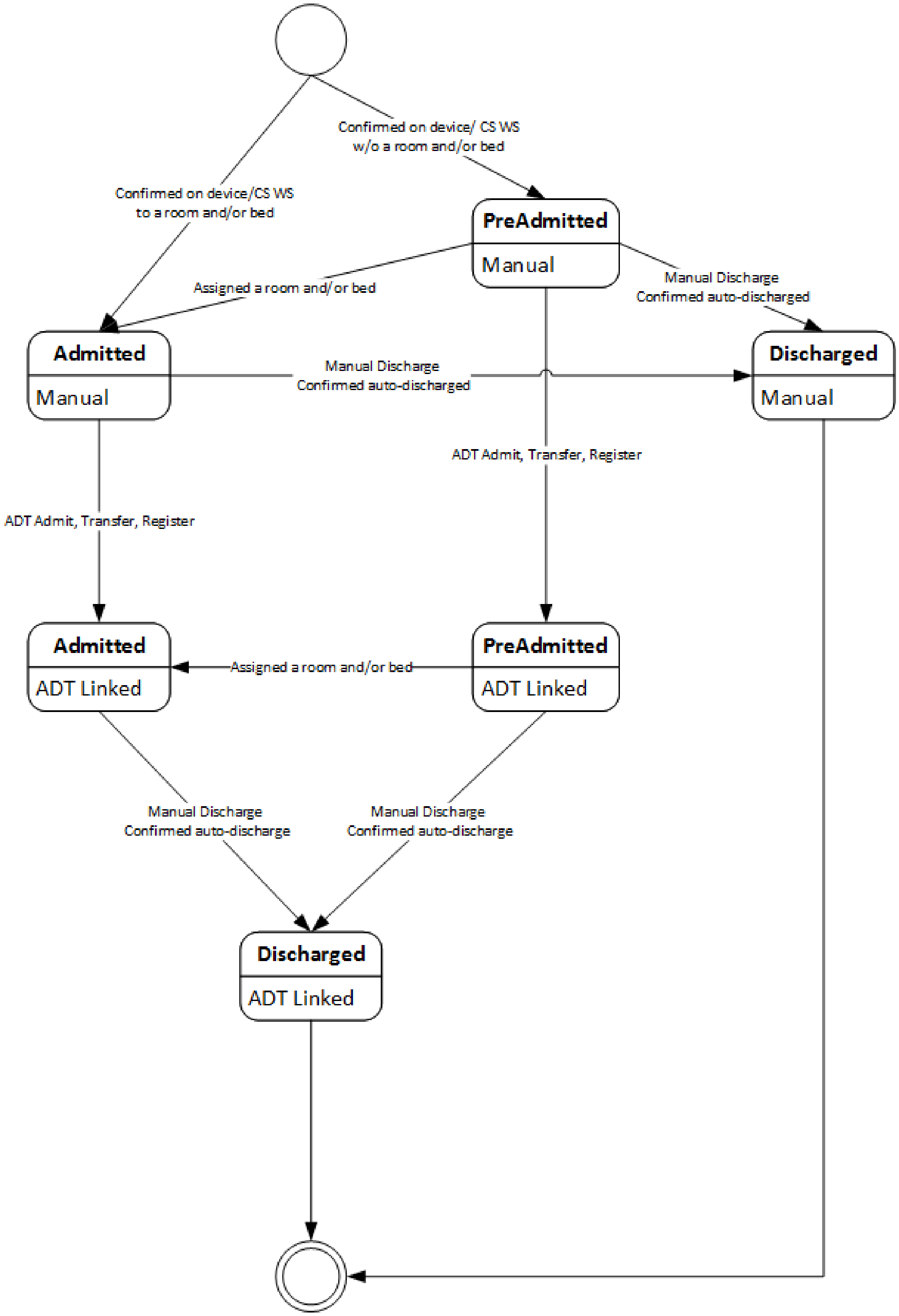
Patient states

Viewing patient data in ProView provides access to the various states a patient can have within the central station database. Effective use of this information requires an understanding of the state machines associated with patients being PreAdmitted, Admitted, and Discharged. The following figures illustrate the state machines for patients created via an ADT message into Connex CS (Figure on page 141), and patients created manually within Connex CS (Figure on page 142).

Patients created via an ADT message into Connex CS


ADT Admit, Transfer, Register
ADT Discharge
PreAdmitted
ADT Only
ADT Discharged
Discharged
ADT-Only
Confirmed on device/CS WS to a room and/or bed
Confirmed on device/ CS WS w/o a room and/or bed
Admitted
ADT Linked
Confirmed to room and/or bed
PreAdmitted
ADT Linked
Manual Discharge Confirmed auto-discharged
Manual Discharge Confirmed auto-discharged
Discharged
ADT Linked

Patients created manually within the central station


Confirmed on device/ CS WS w/o a room and/or bed
Confirmed on device/CS WS to a room and/or bed
PreAdmitted
Manual
Assigned a room and/or bed
Manual Discharge Confirmed auto-discharged
Admitted
Manual
Manual Discharge Confirmed auto-discharged
Discharged
Manual
ADT Admit, Transfer, Register
ADT Admit, Transfer, Register
Admitted
ADT Linked
Assigned a room and/or bed
PreAdmitted
ADT Linked
Manual Discharge Confirmed auto-discharge
Manual Discharge Confirmed auto-discharge
Discharged
ADT Linked

D HL7 parameter labels and units of measurement

This appendix is intended to collect the site specific HL7 configuration settings required to modify Labels and Units of Measure on the Connex CS Server. This information can be used to modify the HL7 configuration on the HL7 ORU Interface. Typically these options will be configured when the Server is installed.

- On the server, open the Administration Tools.
- On the Admin tools tab, navigate to **Continuous measurement configuration** to view the Continuous measurement configuration window.
- Navigate to **Vital signs configuration** to view the Vitals outbound configuration window.
- On both windows, click **Save** to save your changes or click **Reset** to reset to the original values.

Units of Measure – Continuous Measurement Configuration (Unconfirmed)

Continuous measurement configuration between Connex CS and HIS

This data is used to determine the "Units of Measure" when sending observations to the HIS. These settings are applied to the Connex CS Server.

□ **Use defaults**

CO2 (Default is Kilopascal)

Unit Name Kilopascal □ mmHg □
Precision (0-3)
ETCO2 (0 is Default)
FICO2 (0 is Default)
Export □

IPI

Export □

Patient Motion

Export □

Patient Turn

Export □

Pulse Rate

Unit Name Beats Per Minute
Export □

Hemoglobin (Default is gdL)

Unit Name gdL □ mmolL □
Precision (0-3, 1 is Default)
Export □

Pulse Oximetry

Export □

Respiration

Export □

Notes

Units of Measure – Vitals Outbound Configuration

Vitals measurement configuration between Connex CS and HIS

This data is used to determine the "Units of Measure" when sending observations to the HIS. These settings are applied to the Connex CS Server.

□ **Use defaults**

Glucose (Default is Molarity)

Unit Name Molarity □ Mass Concentration □
Precision (0-3, 1 is Default)
Export □

Pulse Rate

Unit Name Beats Per Minute
Export □

Height (Default is Millimeter)

Unit Name Millimeter □ Centimeter □ Inch □ Foot □
Precision (0-3, 1 is Default)
Export □

Hemoglobin (Default is gdL)

Unit Name gdL □ mmolL □
Precision (0-3, 1 is Default)
Export □

NIBP (Default is Pascal)

Unit Name Pascal □ Kilopascal □ Torr □ mmHg □
mbar □ Bar □ Atmosphere □ PSI □
Precision (0-3)
SYS (0-3, 0 is Default)
DIA (0-3, 0 is Default)
MAP (0-3, 0 is Default)
Export □

Pain

Export □

Pulse Oximetry

Export □

Respiration

Export □

Temperature (Default is Kelvin)

Unit Name Kelvin □ Celsius □ Fahrenheit □
Precision (0-3, 1 is Default)
Export □

Weight (Default is Gram)

Unit Name Gram □ Milligram □ Kilogram □ Ounce □ Pound □
Precision (0-3, 1 is Default)
Export □

Notes

Sample continuous ORU message

The following HL7 message is a sample Continuous HL7 message. In the example, defaults are used for available observation labels. Use this sample as a reference to assist in completing the table below.

```
MSH|^~\&|Connex|WelchAllyn|HIS|WelchAllyn|20120719154306||ORU^R01|20121101061743034|P|2.5

PID|||20120719151725447340

PV1||I|||||||||||||||||20120719151725457340

OBR||||C|||20120719154100||||||||||||||||||R

OBX|1|NM|SPO2||97|||N|||R|||20120719154100|120613001

OBX|2|NM|HR||109|BeatsPerMinute||N|||R|||20120719154100|120613001

OBX|3|NM|ETCO2||6|Kilopascal||N|||R|||20120719154100|120613001

OBX|4|NM|FICO2||1|Kilopascal||N|||R|||20120719154100|120613001

OBX|5|NM|IPI||8|||N|||R|||20120719154100|120613001

OBX|6|NM|RESP||35|||N|||R|||20120719154100|120613001

OBX|7|NM|HL||13|gdL||N|||R|||20120719154100|120613001
```

Continuous Measurement Configuration Labels

Observation Identifier Labels – Continuous (Unconfirmed) data. This data is used to determine the Label names when sending continuous observations to the HIS.
These settings are applied to the Connex CS Server.

NOTE The vaules listed in the following table are color coded as follows:

NOTE OBX-3-1 Observation identifier code for vital

NOTE OBX-3-1 Observation identifier code for vital modifier

USE	SOURCE NAME	TARGET NAME	NEW TARGET NAME	TARGET found in Example Line number
□	CO2	CO2	See ETCO2 and FICO2 below	–
□	CO2-ETCO2	ETCO2		OBX|3|NM|ETC02||6|
□	CO2-FICO2	FICO2		OBX|4|NM|FIC02||1|
□	IPI	IPI		OBX|5|NM|IPI||8|
□	Patient Motion	MOTION		–
□	Patient Turn	TURN		–
□	Pulse Rate	HR		OBX|2|NM|HR||109|
□	Hemoglobin	HL		OBX|7|NM|HL||13|
□	Pulse Oximetry	SPO2		OBX|1|NM|SPO2||97|
□	Respiration	RESP		OBX|6|NM|RESP||35|

Notes:

Sample Episodic ORU message

The following HL7 message is a sample Episodic HL7 message. In the example, defaults are used for available observation labels. Use this sample as a reference to assist in completing the table below.

```
MSH|^~\&|Connex|Welch Allyn|HIS|Welch Allyn|20120719123509||ORU^R01|201211010617430348|P|2.5

PID|||20120719070503148

PV1||I||||||||||||||||20120719070503548

OBR||||S|||20120719123503|||20120719070503893^Tailor^John|||||||||||||R

NTE|1||This is Sample Note

OBX|1|NM|StringModifier||3|||N|||R|||20120719123503|20120719070503895|20120719070503893^Tailor^John

OBX|2|NM|GLUC||1800.0|MassConcentration||N|||R|||20120719123503|2012071907|20120719070503893^Tailor^John

OBX|3|ST|RESPMETH||Spontaneous|||N|||R|||20120719123503|2012071907050389|20120719070503893^Tailor^John

OBX|4|ST|RESPPP||Standing|||N|||R|||20120719123503|20120719070503895|20120719070503893^Tailor^John

OBX|5|NM|RESP||60|||N|||R|||20120719123503|20120719070503895|20120719070503893^Tailor^John

OBX|6|ST|MODE||Venous|||N|||R|||20120719123503|20120719070503895|20120719070503893^Tailor^John

OBX|7|NM|HL||12|gdL||N|||R|||20120719123503|20120719070503895|20120719070503893^Tailor^John

OBX|8|NM|SYS||10532|Pascal||N|||R|||20120719123503|20120719070503895|20120719070503893^Tailor^John

OBX|9|NM|DIA||11332|Pascal||N|||R|||20120719123503|20120719070503895|20120719070503893^Tailor^John

OBX|10|NM|MAP||11065.8|Pascal||N|||R|||20120719123503|20120719070503895|20120719070503893^Tailor^John

OBX|11|ST|BPSITE||LArm|||N|||R|||20120719123503|20120719070503895|20120719070503893^Tailor^John

OBX|12|ST|BPPP||Lying|||N|||R|||20120719123503|20120719070503895|20120719070503893^Tailor^John

OBX|13|ST|BPCUFF||Adult|||N|||R|||20120719123503|20120719070503895|20120719070503893^Tailor^John

OBX|14|ST|TEMPSITE||Oral|||N|||R|||20120719123503|20120719070503895|20120719070503893^Tailor^John

OBX|15|NM|TEMP||371.2|Kelvin||N|||R|||20120719123503|20120719070503895|20120719070503893^Tailor^John

OBX|16|ST|SPO2METH||RoomAir|||N|||R|||20120719123503|20120719070503895|20120719070503893^Tailor^John

OBX|17|ST|SPO2SITE||Forehead|||N|||R|||20120719123503|20120719070503895|20120719070503893^Tailor^John

OBX|18|NM|SPO2FLOW||1|||N|||R|||20120719123503|20120719070503895|20120719070503893^Tailor^John

OBX|19|NM|SPO2CONC||21|||N|||R|||20120719123503|20120719070503895|20120719070503893^Tailor^John

OBX|20|NM|SPO2||10|%||N|||R|||20120719123503|20120719070503895|20120719070503893^Tailor^John

OBX|21|ST|WTQUAL||Dry|||N|||R|||20120719123503|20120719070503895|20120719070503893^Tailor^John

OBX|22|ST|WTMETH||Chair|||N|||R|||20120719123503|20120719070503895|20120719070503893^Tailor^John

OBX|23|NM|WT||72000000.0|Gram||N|||R|||20120719123503|20120719070503895|20120719070503893^Tailor^John

OBX|24|ST|HRSITE||Right|||N|||R|||20120719123503|20120719070503895|20120719070503893^Tailor^John

OBX|25|ST|HRMETH||Doppler|||N|||R|||20120719123503|20120719070503895|20120719070503893^Tailor^John

OBX|26|ST|HRPP||Lying|||N|||R|||20120719123503|20120719070503895|20120719070503893^Tailor^John

OBX|27|NM|HR||75|BeatsPerMinute||N|||R|||20120719123503|20120719070503895|20120719070503893^Tailor^John

OBX|28|ST|HTQUAL||Actual|||N|||R|||20120719123503|20120719070503895|20120719070503893^Tailor^John

OBX|29|NM|HT||5486400.0|Millimeter||N|||R|||20120719123503|20120719070503895|2012071907050389^Tailor^John

OBX|30|ST|PAINMATH||Verbal|||N|||R|||20120719123503|20120719070503895|20120719070503893^Tailor^John

OBX|31|NM|PAIN||5|||N|||R|||20120719123503|20120719070503895|20120719070503893^Tailor^John
```

Episodic Measurement Configuration Labels

Observation Identifier Labels – Episodic (Confirmed) data. This data is used to determine the Label names when sending episodic observations to the HIS.
These settings are applied to the Connex CS Server.

NOTE The values listed in the following table are color coded as follows:

NOTE OBX-3-1 Observation identifier code for vital

NOTE OBX-3-1 Observation identifier code for vital modifier

NOTE OBX-5 Observation Value for Vital Modifier

USE	SOURCE NAME	TARGET NAME	NEW TARGET NAME	TARGET found in Example Line number
□ Use defaults				
□	GLUCOSE	GLUC		OBX|2|NM|GLUC||1800.0|
□	Serial Number	Serial number		–
□	Custom	Custom		–
□	Pulse rate [1, 2, 3]	HR		OBX|27|NM|HR|||75|
□	Site	HRSITE		–
□	None	None		–
□	Unknown	Unknown		–
□	Left	Left		–
□	Right	Right		–
□	Method	HRMETH		–
□	None	None		–
□	Unknown	Unknown		–
□	Auscultate	Auscultate		–
□	Doppler	Doppler		–
□	Palpation	Palpation		–
□	Position	HRPP		–
□	None	None		–
□	Unknown	Unknown		–
□	Lying	Lying		–
□	Sitting	Sitting		–
□	Standing	Standing		–
□	Custom	Custom		–
□	Height [a, b, c]	HT		OBX|29|NM|HT||5486400.0|
□	Quality	HTQUAL		OBX|28|ST|HTQUAL||Actual|
□	None	None		–
□	Unknown	Unknown		–

USE	SOURCE NAME	TARGET NAME	NEW TARGET NAME	TARGET found in Example Line number
□	Actual	Actual		OBX|28|ST|HTQUAL||Actual|
□	Estimated	Estimated		–
□	Custom	Custom		–
□	Hemoglobin[a, b]	HL		OBX|7|NM|HL||12|
□	Mode[a, b] (Automatic via CVSM)	MODE		OBX|6|ST|MODE||Venous|
□	None	None		–
□	Unknown	Unknown		–
□	Arterial	Arterial		–
□	Venous	Venous		OBX|6|ST|MODE||Venous|
□	Custom	Custom		–
□	NIBP[a, b, c]	NIBP	See SYS and DIA below	–
□	Systolic[a, b, c]	SYS		OBX|8|NM|SYS||10532|Pascal|
□	Diastolic[a, b, c]	DIA		OBX|9|NM|DIA||11332|Pascal|
□	Map	MAP		OBX|10|NM|MAP||11065.8|Pascal|
□	Cuff Location[a, b]	BPSITE		OBX|11|ST|BPSITE||LArm|
□	None	None		–
□	Unknown	Unknown		–
□	LArm	LArm		OBX|11|ST|BPSITE||LArm|
□	RArm	RArm		–
□	LLeg	LLeg		–
□	RLeg	RLeg		–
□	Potision[a, b]	BPPP		OBX|12|ST|BPPP||Lying|
□	None	None		–
□	Unknown	Unknown		–
□	Lying	Lying		OBX|12|ST|BPPP||Lying|
□	Sitting	Sitting		–
□	Standing	Standing		–
□	Cuff Size[a, b]	BPCUFF		OBX|13|ST|BPCUFF||Adult|
□	None	None		–
□	Unknown	Unknown		–
□	Neo1	Neo1		–
□	Neo2	Neo2		–
□	Neo3	Neo3		–
□	None	None		–
□	Unknown	Unknown		–

USE	SOURCE NAME	TARGET NAME	NEW TARGET NAME	TARGET found in Example Line number
□	Neo1	Neo1		–
□	Neo2	Neo2		–
□	Neo3	Neo3		–
□	Neo4	Neo4		–
□	Neo5	Neo5		–
□	SmallInfant	SmallInfant		–
□	Infant	Infant		–
□	SmallChild	SmallChild		–
□	Child	Child		–
□	SmallAdult	SmallAdult		–
□	Adult	Adult		OBX|13|ST|BPCUFF||Adult|
□	AdultLong	AdultLong		–
□	LargeAdult	LargeAdult		–
□	LargeAdultLong	LargeAdultLong		–
□	Thigh	Thigh		–
□	Custom	Custom		–
□	Pain [a, b, c]	PAIN		OBX|31|NM|PAIN||5|
□	Method	PAINMETH		–
□	None	None		–
□	Unknown	Unknown		–
□	Verbal	Verbal		–
□	NonVerbal	NonVerbal		–
□	Custom	Custom		–
□	Pulse Oximetery [a, b, c]	SPO2		OBX|20|NM|SPO2||10|
□	Method	SPO2METH		–
□	None	None		–
□	Unknown	Unknown		–
□	AerosolHumidifierMask	AerosolHumidifierMask		–
□	FaceTent	FaceTent		–
□	NasalCannula	NasalCannula		–
□	Nonrebreather	Nonrebreather		–
□	PartialRebreater	PartialRebreater		–
□	Tpiece	Tpiece		–
□	TracheostomyCollar	TracheostomyCollar		–
□	Ventilator	Ventilator		–
□	VenturiMask	VenturiMask		–

USE	SOURCE NAME	TARGET NAME	NEW TARGET NAME	TARGET found in Example Line number
□	RoomAir	RoomAir		OBX|16|ST|SPO2METH||Room Air|
□	Oxymizer	Oxymizer		–
□	Location [a, b]	SPO2SITE		OBX|17|ST|SPO2SITE||Forehead|
□	None	None		–
□	Unknown	Unknown		–
□	Ear	Ear		–
□	Finger	Finger		–
□	Toe	Toe		–
□	Forehead	Forehead		OBX|17|ST|SPO2SITE||Forehead|
□	Flow Rate [a, b]	SPO2FLOW		OBX|18|NM|SPO2FLOW||1|
□	Concentration [a, b]	SPO2CONC		OBX|19|NM|SPO2CONC||21|
□	Custom	Custom		–
□	Respiration [b, c]	RESP		OBX|5|NM|RESP||60|
□	Method	RESPMETH		–
□	None	None		–
□	Unknown	Unknown		–
□	AssistedbyVentilator	AssistedbyVentilator		–
□	ControlledbyVentilator	ControlledbyVentilator		–
□	Spontaneous	Spontaneous		–
□	Position	RESPP		–
□	None	None		–
□	Unknown	Unknown		–
□	Lying	Lying		–
□	Sitting	Sitting		–
□	Standing	Standing		–
□	Custom	Custom		–
□	Temperature [a, b, c]	TEMP		OBX|15|NM|TEMP||
□	Mode [a, b, c]	TEMPSITE		OBX|14|ST|TEMPSITE||Oral|
□	None	None		–
□	Unknown	Unknown		–
□	Oral	Oral		OBX|14|ST|TEMPSITE||Oral|
□	Rectal	Rectal		–
□	PediatricAxillary	PediatricAxillary		–
□	CalibrationKey	CalibrationKey		–
□	Tympanic	Tympanic		–

USE	SOURCE NAME	TARGET NAME	NEW TARGET NAME	TARGET found in Example Line number
□	Custom	Custom		–
□	Weight [a, b, c]	WT		OBX|23|NM|WT||72000000.0|
□	BMI	BMI		–
□	Quality	WTQUAL		–
□	None	None		–
□	Unknown	Unknown		–
□	Actual	Actual		–
□	Dry	Dry		–
□	Estimated	Estimated		–
□	Method	WTMETH		–
□	None	None		–
□	Unknown	Unknown		–
□	Bed	Bed		–
□	Chair	Chair		–
□	Standing	Standing		–
□	Custom	Custom		–
Notes:				

1. CVSM 2.x in a non-continuous mode (depending on hardware options installed)
2. VSM 1.7 in “Monitor” mode (depending on hardware options installed)
3. Spot LXi

Connex CS Code Sets

The values in the following tables are in Connex Central Station. If your facility is using nonstandard code set values, please provide the values your facility will be using.

The header of each table below calls out the HL7 Specification Table number, the Table Description and the corresponding HL7 Segment and Field where the value is used. The body of the table also lists supported values for each field.

In the columns on the right, please modify or update the table with the corresponding values and descriptions used at your facility so that these can be integrated into the HL7 Interface Configuration and the appropriate mapping between the two systems can be completed.

□ Use defaults for all code sets

PID-8 – Administrative Sex Code Set

Connex CS		**Site Specifics**	
Value	Description	Value	Description
F	Female		
M	Male		
O	Other		

Connex CS		Site Specifics	
U	Unknown		
A	Ambiguous		
N	Not Applicable		
Notes:			

PV1-2 – Patient Class Code Set

Connex CS		Site Specifics	
Value	Description	Value	Description
F	Female		
O	Outpatient		
P	Preadmit		
I	Inpatient		
R	Recurring patient		
E	Emergency		
B	Obstetric		
N	Not Applicable		
C	Commercial Account		
Notes:			

OBX-8 – Alarm Code Code Set

Connex CS		Site Specifics	
Value	Description	Value	Description
N	Normal (applies to non-numeric results)		
B	Better – Use when direction is not relevant		
HH	Above upper panic limits		
LL	Below lower panic limits		
A	Abnormal (applies to non-numeric results)		
>	Above absolute high – off instrument scale		
<	Below absolute low – off instrument scale		
null	No range defined, or normal ranges do not apply		
MS	Moderately susceptible. Indicates for microbiology susceptibilities only.		
Notes:			

E HL7 interface test plan

The following table lists operations that should be considered in the HIS patient registration system testing, along with the associated result in Connex and the ADT event type. This list is just an example of one possible test plan for eight different Message Event Types and Triggers. This test does not represent an all-inclusive test. The test should be modified to include all of the Event Type and Triggers identified as “in use” by your facility within Section D of the Project Requirements Form.

All steps must be performed in sequence on the same test patient. The expected result must be verified in Connex CS after each operation before moving on to the next step.

The process can be repeated for multiple patients.

Sample test plan

	Task	**Expected result**
1	Admit the patient (ADT^A01)	The patient is displayed in the Connex CS “current Patient List” as an Unconfirmed patient with specific patient ID, DOB and Gender. Confirm patient location.
2	Cancel the admit (ADT^A11)	The patient is no longer displayed in the Current Patient List (patient can still be seen on Patient List Search tab with no Patient ID)
3	Admit the patient (ADT^A01)	The patient is displayed in the Connex CS “Current Patient List” as an Unconfirmed patient with specific patient ID, DOB and Gender. Confirm patient location.
4	Update the patient's name, DOB, and gender (ADT^A08)	The information is updated on the Current Patient List.
5	Transfer the patient (ADT^A02)	The patient is displayed in the Patient List. Confirm the new patient location.
6	Cancel the transfer (ADT^A12)	The patient is displayed in the Patient List. Confirm the original patient location.
7	Discharge the patient (ADT^A03)	The patient is no longer displayed in the Current Patient List.
8	Cancel the discharge (ADT^A13)	The patient is displayed in the Current Patient List as an Unconfirmed patient.
9	Enter a vitals reading with all the Connex workflows, values, and qualifiers to be used.	The patient moves from the Unconfirmed patient list to the Confirmed patient list and shows on a tile on the Connex Central Station main screen.
10	Test the ORU interface to ensure the correct data goes into the correct placement in the chart and is displayed appropriately.	

F Server Authentication and Encryption

Introduction

Connex CS introduces encryption and server authentication to the Connex CS System for episodic and continuous connections with devices.

Devices must have root certificates installed, and Central Station encryption and authentication configuration must be enabled for continuous host connection to work.

Enable Encrypted Device Connections

Connex CS supports TLS encryption for Episodic connection and DTLS encryption for Continuous Connection. In order to use TLS encryption for Episodic connections with devices, the port number configured for WACPTLSTCPPort should be used on the devices with encryption enabled for episodic host connection. In order to use DTLS encryption for Continuous connections with devices, the port number configured WACPDTLSUDPPort should be used on the devices with encryption enabled for continuous host connection.

Enable Server Authentication From Devices

Server Authentication configuration allows the devices connecting to Connex CS System to authenticate the Connex CS systems using server certificate. Server Authentication may be applied to Episodic TLS connections (Episodic Connectivity Service) and Continuous DTLS connections (Continuous Connectivity Service).

In order to apply server authentication to Episodic TLS connection, Connex CS allows user to select a server authentication certificate for Episodic Connectivity Service on the system. The certificate's thumbprint (a publicly available field, no security concern) will be saved to the ECS application configuration file. (WelchAllyn.Connex.EpisodicConnectivityServer.exe.config). The port number configured for WACPTLSTCPPort should be used on the devices for episodic host connection. The devices must have the root certificates installed for and encryption and authentication configuration should be enabled for episodic host connection.

In order to apply server authentication to Continous DTLS connection Connex CS allows user to select a server authentication certificate for Continuous Connectivity Service on the system. The certificate's thumbprint (a publicly available field, no security concern) will be saved to the CCS application configuration file. (WelchAllyn.Continuous.CCS.exe.config). The port number configured for WACPDTLSUDPPort should be used on the devices for continuous host connection.

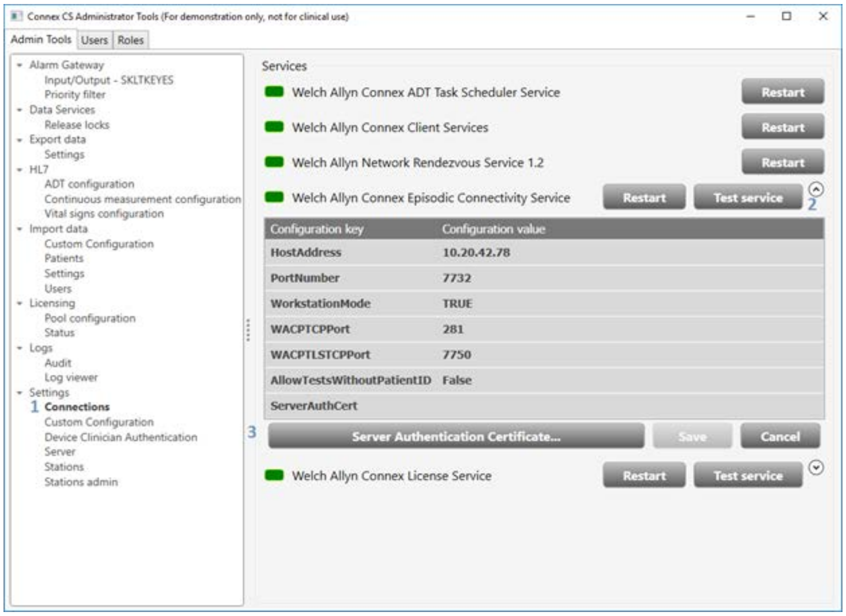
An additional security measure for devices using encrypted connections is to authenticate the Connex CS host using certificates.

Episodic Device Connections (TLS)

1. In the Admin Tools on the Server, enter Admin Tools (or for a stand-alone configuration, in CS Advanced Settings), and select **Connections**.

2. Expand the Welch Allyn Episodic Connectivity Service

3. Select **Server Authentication Certificate…**


Connex CS Administrator Tools (For demonstration only, not for clinical use)
Admin Tools
Users
Roles
Alarm Gateway
Input/Output - SKLTKEYES
Priority filter
Data Services
Release locks
Export data
Settings
HL7
ADT configuration
Continuous measurement configuration
Vital signs configuration
Import data
Custom Configuration
Patients
Settings
Users
Licensing
Pool configuration
Status
Logs
Audit
Log viewer
Settings
1
Connections
Custom Configuration
Device Clinician Authentication
Server
Stations
Stations admin
Services
Welch Allyn Connex ADT Task Scheduler Service
Restart
Welch Allyn Connex Client Services
Restart
Welch Allyn Network Rendezvous Service 1.2
Restart
Welch Allyn Connex Episodic Connectivity Service
Restart
Test service
2
3
Server Authentication Certificate...
Save
Cancel
Welch Allyn Connex License Service
Restart
Test service

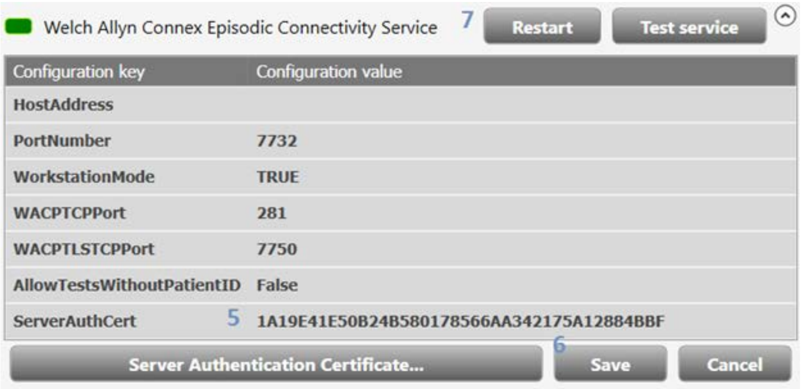
Configuration key	Configuration value
HostAddress	10.20.42.78
PortNumber	7732
WorkstationMode	TRUE
WACPTCPPort	281
WACPTLSTCPPort	7750
AllowTestsWithoutPatientID	False
ServerAuthCert	

4. Select a certificate from the Windows pop up. Only applicable certificates are displayed.

5. The ServerAuthCert field within ECS is populated with the selected certificate's thumbprint. To verify it is the correct thumbprint, you can access the certificates properties from the previous dialog or the Windows OS.

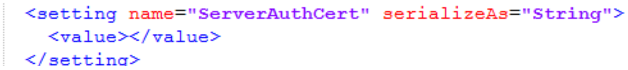
6. Click **Save**.

7. Click **Restart** to apply the change.


Welch Allyn Connex Episodic Connectivity Service
7
Restart
Test service
5
6
Server Authentication Certificate...
Save
Cancel

Configuration key	Configuration value
HostAddress	
PortNumber	7732
WorkstationMode	TRUE
WACPTCPPort	281
WACPTLSTCPPort	7750
AllowTestsWithoutPatientID	False
ServerAuthCert	1A19E41E50B24B580178566AA342175A12884BBF

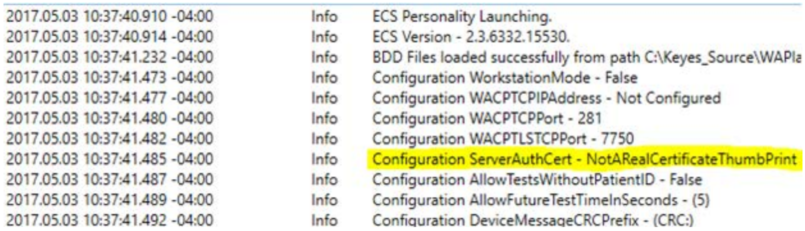
ECS checks the configuration value on start up. If the configuration is empty (as shown below), then ECS will not use server authentication. If there as a valid setting, ECS will use server authentication.



```
<setting name="ServerAuthCert" serializeAs="String">
  <value></value>
</setting>
```

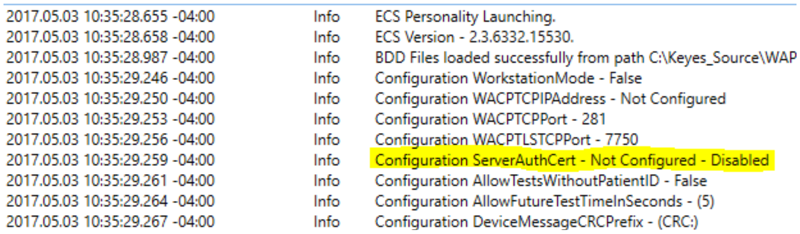
Aside from testing with a device, ECS also logs which state the configuration is in during start up. Two examples are shown below.

Server authentication configured



```
2017.05.03 10:37:40.910 -04:00     Info   ECS Personality Launching.
2017.05.03 10:37:40.914 -04:00     Info   ECS Version - 2.3.6332.15530.
2017.05.03 10:37:41.232 -04:00     Info   BDD Files loaded successfully from path C:\Keyes_Source\WAPla
2017.05.03 10:37:41.473 -04:00     Info   Configuration WorkstationMode - False
2017.05.03 10:37:41.477 -04:00     Info   Configuration WACPTCPIPAddress - Not Configured
2017.05.03 10:37:41.480 -04:00     Info   Configuration WACPTCPPort - 281
2017.05.03 10:37:41.482 -04:00     Info   Configuration WACPTLSTCPPort - 7750
2017.05.03 10:37:41.485 -04:00     Info   Configuration ServerAuthCert - NotARealCertificateThumbPrint
2017.05.03 10:37:41.487 -04:00     Info   Configuration AllowTestsWithoutPatientID - False
2017.05.03 10:37:41.489 -04:00     Info   Configuration AllowFutureTestTimeInSeconds - (5)
2017.05.03 10:37:41.492 -04:00     Info   Configuration DeviceMessageCRCPrefix - (CRC:)
```

Server authentication not configured



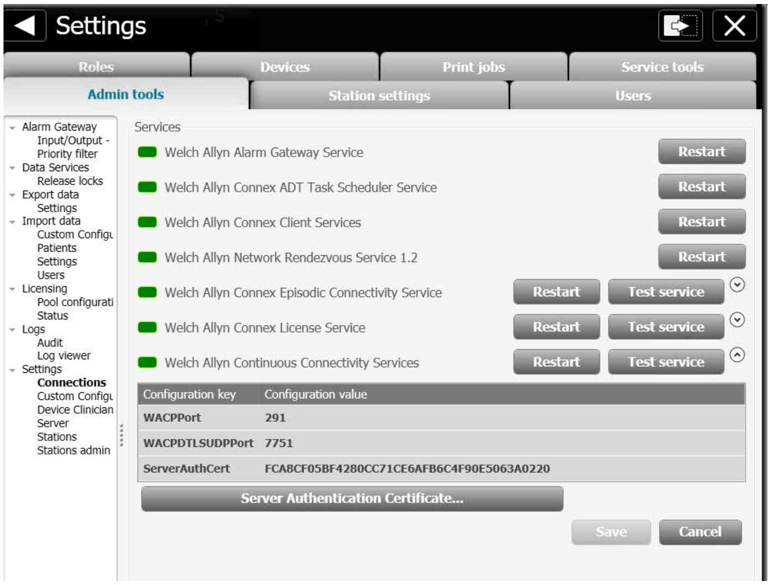
```
2017.05.03 10:35:28.655 -04:00     Info   ECS Personality Launching.
2017.05.03 10:35:28.658 -04:00     Info   ECS Version - 2.3.6332.15530.
2017.05.03 10:35:28.987 -04:00     Info   BDD Files loaded successfully from path C:\Keyes_Source\WAP
2017.05.03 10:35:29.246 -04:00     Info   Configuration WorkstationMode - False
2017.05.03 10:35:29.250 -04:00     Info   Configuration WACPTCPIPAddress - Not Configured
2017.05.03 10:35:29.253 -04:00     Info   Configuration WACPTCPPort - 281
2017.05.03 10:35:29.256 -04:00     Info   Configuration WACPTLSTCPPort - 7750
2017.05.03 10:35:29.259 -04:00     Info   Configuration ServerAuthCert - Not Configured - Disabled
2017.05.03 10:35:29.261 -04:00     Info   Configuration AllowTestsWithoutPatientID - False
2017.05.03 10:35:29.264 -04:00     Info   Configuration AllowFutureTestTimeInSeconds - (5)
2017.05.03 10:35:29.267 -04:00     Info   Configuration DeviceMessageCRCPrefix - (CRC:)
```

Continuous Device Connections (DTLS)

Apply Certificate Authentication

For systems that use Central Stations for Continuous monitoring, you may also provide a server certificate for each Central Station.

Navigate to the Connections Setting on the Central Station(s), but this time expand "Welch Allyn Continuous Connectivity Services".



🟩 Welch Allyn Alarm Gateway Service
🟩 Welch Allyn Connex ADT Task Scheduler Service
🟩 Welch Allyn Connex Client Services
🟩 Welch Allyn Network Rendezvous Service 1.2
🟩 Welch Allyn Connex Episodic Connectivity Service
🟩 Welch Allyn Connex License Service
🟩 Welch Allyn Continuous Connectivity Services

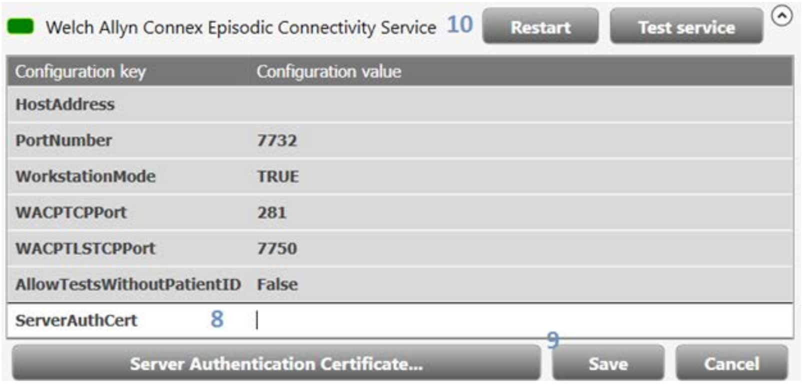
Configuration key	Configuration value
WACPPort	291
WACPDTLSUDPPort	7751
ServerAuthCert	FCA8CF05BF4280CC71CE6AFB6C4F90E5063A0220

Apply the same steps as above, but this time restart the CCS service to apply the change.

Disable Server Authentication From Devices

Remove a server authentication certificate

1. To clear the setting, delete the value in ServerAuthCert.
2. Click **Save**.
3. Click **Restart ECS** to apply the change.



Welch Allyn Connex Episodic Connectivity Service

Configuration key	Configuration value
HostAddress	
PortNumber	7732
WorkstationMode	TRUE
WACPTCPPort	281
WACPTLSTCPPort	7750
AllowTestsWithoutPatientID	False
ServerAuthCert	

Corepoint Certificates

Reinstall and Rebind Corepoint Security Certificates

CorePoint Integration Engine also uses certificates. Corepoint Integration Engine, beginning with release 6.0.0, uses HTTPS for web communications to ensure a secure protocol for all remote connections. The Corepoint integration Engine installer installs a security certificate, signed by Corepoint Health, for use as the default security certificate. To replace the default security certificate, obtain a certificate from a trusted certificate authority and deploy it via Microsoft IIS.

To manually reinstall and rebind the default Corepoint security certificate, launch the application **CreateSite.exe** as an Administrator. This application is located at C:\Program Files\Corepoint Health\Corepoint Integration Engine\Bin. For information about IP changes, see "If the Corepoint IP address changes" in the chapter "Network Change and Configuration."

G Configure Clinician Authentication

Authentication type can be selected and configured using the Connex Admin tools. Launch **Admin tools** and select **Settings > Device Clinician Authentication**.

The following example contains a basic workflow to configure and use this feature. Further details are provided in the content below.

NOTE Once authentication provider configuration is completed, Episodic Connectivity Service (ECS) must be restarted for changes to take effect.

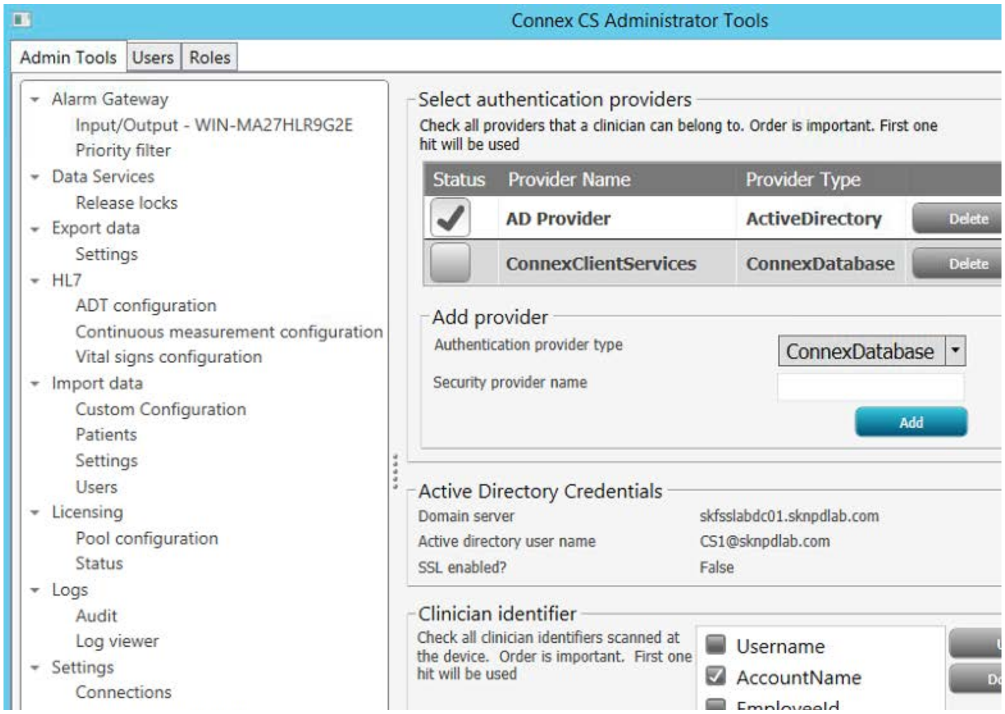
⚠ **CAUTION** In a client-server deployment, all configuration for Device Clinician Authentication must take place at the Connex server, not the Connex Central Station. These steps are included for configuration of the Connex server.

Multiple Security Providers

The admin tool supports creation of multiple security providers: ConnexDatabase, Imprivata OneSign and Microsoft Active Directory service.

View Clinician Authentication settings

1. From the Server’s Admin Tools application, navigate to the **Admin Tools tab > Device Clinician Authentication**.



Select authentication providers

Check all providers that a clinician can belong to. Order is important. First one hit will be used

Status	Provider Name	Provider Type
☑	AD Provider	ActiveDirectory
□	ConnexClientServices	ConnexDatabase

Add provider

Authentication provider type: ConnexDatabase

Security provider name:

Active Directory Credentials

Domain server: skfsslabdc01.sknpdlab.com

Active directory user name: CS1@sknpdlab.com

SSL enabled?: False

Clinician identifier

Check all clinician identifiers scanned at the device. Order is important. First one hit will be used

□ Username

☑ AccountName

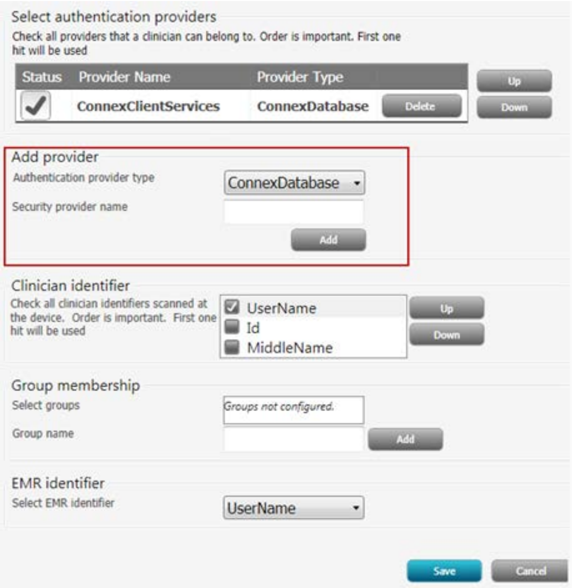
□ EmployeeId

2. The authentication providers area includes a list of providers.

3. A Provider Name listed with a “check” in the Status column indicates that it is currently in use.

Configure for use with Connex Database

1. Select **ConnexDatabase** to authenticate against the Connex CS Database. This is the default setting.



Select authentication providers

Check all providers that a clinician can belong to. Order is important. First one hit will be used

Status	Provider Name	Provider Type
☑	ConnexClientServices	ConnexDatabase

Add provider

Authentication provider type: ConnexDatabase

Security provider name:

Clinician identifier

Check all clinician identifiers scanned at the device. Order is important. First one hit will be used

☑ UserName
□ Id
□ MiddleName

Group membership

Select groups: Groups not configured.

Group name:

EMR identifier

Select EMR identifier: UserName

2. Settings may be modified as indicated above.

Configure Clinician Identifier for Connex CS Database

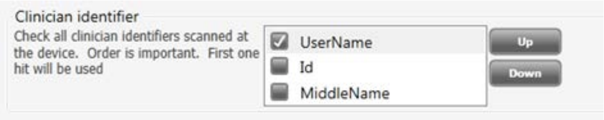
The list of clinician identifiers are available when authenticating against the Connex CS Database are described in the table below.

Identifier	**Meaning**
UserName	User account name in the Connex Database
ID	Clinician identifier
MiddleName	User's middle name

To configure clinician identifier settings:

1. Check the box for each identifier that a clinician could use at the device.

2. Click on the identifier name to select, and use the **Up** and **Down** buttons to indicate the relative importance of each clinician identifier.



Clinician identifier

Check all clinician identifiers scanned at the device. Order is important. First one hit will be used

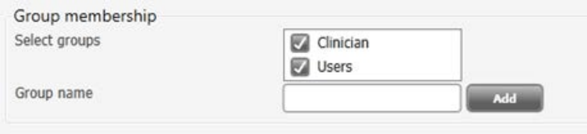
☑ UserName
□ Id
□ MiddleName

3. The security provider will verify in the sequence provided.

4. The first successful authentication or lookup will be used.

Configure Group Membership for Connex CS Database

A clinician might be required to be a member of a group for successful authentication. When groups are configured, a clinician must be a member of at least one group.



Group membership

Select groups ☑ Clinician ☑ Users

Group name

To configure group membership settings:

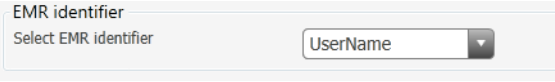
1. Check each group that applies.
2. Key in additional group names as needed and press the Add button.
3. Each new group must already exist in the Connex CS database

Configure EMR Identifier for Connex CS Database

Upon successful authentication or lookup, the security provider returns the configured EMR identifier to the device (along with clinician first name and last name). The device sends the EMR Identifier with test vitals and outbound ORU messages to the EMR.

To configure EMR identifier settings:

1. Select the clinician identifier for use as the EMR Identifier.
2. The selected ID should be recognizable and valid in the hospital's EMR.
3. If an EMR identifier is not specified, the primary clinician identifier is returned as the EMR ID: Username.



EMR identifier

Select EMR identifier UserName

⚠ **CAUTION** Select an EMR ID mapping even though it may not be required by the admin tool and verify that the mapped attribute cannot contain a null value or blank value. If the specified mapping contains an empty value for an authenticated clinician, the Connex CS security provider returns the empty value to the device as the EMR ID. An empty EMR ID on the device prevents transmission of episodic test records from the device to ECS.

> Example: A clinician authenticates at the device with a valid clinician number and password. EMR ID is mapped to clinician middle name. But, not all clinicians have a middle name. the Connex CS security provider returns an empty EMR ID to the device when that clinician authenticates at the device. The uploads will not be successfully transmitted to the EMR because the clinician ID is not valid.

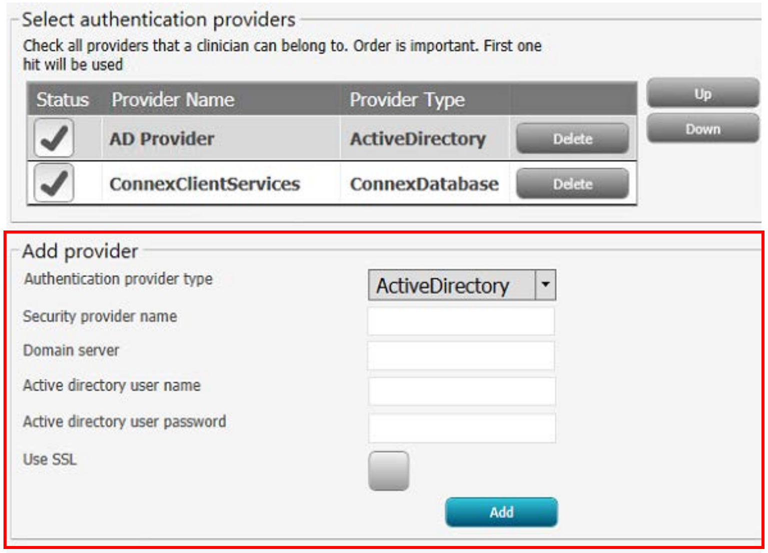
When changes are complete

1. Click on the Save button at the bottom of the working window.
2. Restart ECS for all changes to take effect.

Configure for use with Active Directory

Add a provider for Active Directory

1. On the main window, in the "Add provider" area, select **ActiveDirectory** from the drop-down list. An example is shown highlighted below.



Select authentication providers

Check all providers that a clinician can belong to. Order is important. First one hit will be used

Status	Provider Name	Provider Type
✓	AD Provider	ActiveDirectory
✓	ConnexClientServices	ConnexDatabase

Add provider

Authentication provider type: ActiveDirectory

Security provider name

Domain server

Active directory user name

Active directory user password

Use SSL □

2. Configure **Security provider** name.

   a. Enter a friendly name which identifies the hospital's active directory instance.

   b. A name is required since multiple active directory providers may be configured.

3. Configure the **Domain server** address.

   a. Enter the IP address or domain name of the active directory domain controller.

   b. Refer to the *Connex CS Customer Project Req. Form, Appendix B1* as needed for this information.

4. Configure **Active directory user name**.

   a. Enter a user name that has privileges for accessing the active directory.

   b. This is the account name which will be used by the Connex CS system to make the connection to the facility's active directory service. Refer to the *Connex CS Customer Project Req. Form, Appendix B1* as needed for this information.

5. Configure **Active directory user password**.

   a. Enter the valid password of the active directory user.

   b. This is the account password which will be used by the Connex CS system to make the connection to the facility's Active Directory service. Refer to the *Connex CS Customer Project Req. Form, Appendix B1* as needed for this information.

6. If enabling SSL via certificates with LDAP (Active Directory) connections, check the box "Use SSL."

NOTE The AD server CA root certificate must first be installed in the Trusted Root CA store of the Connex CS server.

7. Click **Add**. This verifies that the domain address is valid as well as that the user credentials exist in the active directory.

   To change the SSL setting, manually edit the security provider configuration file by setting the “Use SSL” value to True or False. To do so, browse to the path below, from the folder in which CSAS was installed. Note that “[Version]” below is a placeholder, since the version number may vary.

   \Welch Allyn\Connex\ECS\[VERSION]\DeviceSecurityProviderConfiguration/xml

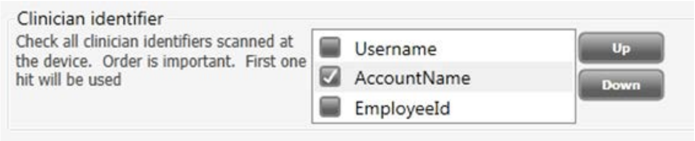
8. Upon success, the added security provider will be available under **Select Authentication Providers**.

9. All other settings can now be configured.

NOTE If messages appear during configuration that **Add** function is not being accepted, confirm settings listed in the *Connex CS Customer Project Req. Form* are input properly. Consult with the facility IT staff to confirm settings if problems still persist.

Configure Clinician identifier with Active Directory

The default identifiers are available when authenticating against active directory are shown below. These represent active directory attributes which are common to all instances of active directory.



Clinician identifier

Check all clinician identifiers scanned at the device. Order is important. First one hit will be used

□ Username
☑ AccountName
□ EmployeeId

1. Check each clinician identifier that applies. Refer to the *Connex CS Customer Project Req. Form, Appendix B1* as needed for input data in these fields.

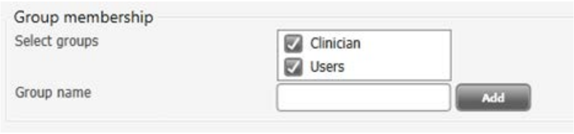
2. Click on the Identifier name to select, and use the **Up** and **Down** buttons to indicate the relative importance of each clinician identifier.

NOTE The order matters as the first item which matches in the active directory query will be used.

3. Additional active directory attributes can be specified as described in “Add a Custom active directory identifier” on page 167.

Configure Group membership with Active Directory

A clinician may be required to be a member of a group for successful authentication. When groups are configured, a clinician must be a member of at least one group.



Group membership

Select groups

☑ Clinician
☑ Users

Group name

1. Check each group that applies. Refer to the *Connex CS Customer Project Req. Form, Appendix B1* as needed for input data in these fields.

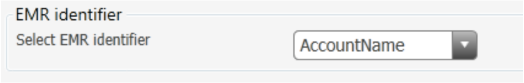
2. Key in additional group names as needed and click **Add**.

NOTE Each new group must already exist in the hospital's Active Directory instance.

Configure EMR identifier with Active Directory

Upon successful authentication or lookup, the security provider returns the configured EMR identifier to the device (along with clinician first name and last name). The device sends the EMR Identifier with test vitals and outbound ORU messages to the EMR.

1. Select the clinician identifier for use as the EMR identifier. Refer to the *Connex CS Customer Project Req. Form, Appendix B1* as needed for input data in these fields.
2. The selected ID must be recognizable and valid in the hospital's EMR.
3. If an EMR identifier is not specified, the primary clinician identifier is returned as the EMR ID: AccountName as shown in the example below.



EMR identifier

Select EMR identifier: AccountName

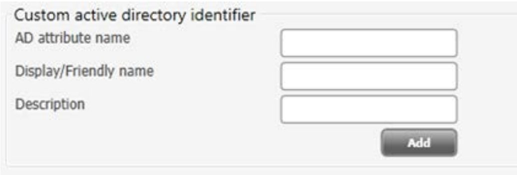
CAUTION Select an EMR ID mapping even though it may not be required by the admin tool and verify that the mapped attribute cannot contain a null value or blank value. If the specified mapping contains an empty value for an authenticated clinician, the active directory security provider returns the user account name as the EMR ID. The user account name may not be recognized by the EMR as a valid clinician identifier. This will likely cause problems in the EMR when episodic tests are uploaded.

Example: A clinician authenticates at the device with a valid user account name and password. EMR ID is mapped to display name. Display name is not required in active directory and a clinician may not have a display name. In this case, the active directory security provider returns the user account name as the EMR ID when that clinician authenticates at the device. The clinician takes many episodic tests from many patients and uploads. The uploads will not be successfully transmitted to the EMR because the clinician ID is not valid.

Add a Custom active directory identifier

There are many user attributes available in active directory (in addition to the defaults above). Further, active directory supports creation of custom user attributes. Any of these attributes could be used by the hospital for clinician authentication.

The admin tool supports capture of other attribute and custom attribute usage. Refer to the *Connex CS Customer Project Req. Form, Appendix B1* as needed for input data in these fields.



Custom active directory identifier

AD attribute name

Display/Friendly name

Description

1. Navigate to the Custom active directory identifier area.
2. Enter the attribute's LDAP display name as defined in active directory.
3. Enter a friendly name for the attribute (i.e. Badge Number).

4. Enter a description for the attribute.

5. Press **Add**. Upon a successful add, the attribute will be available for selection as a clinician identifier as described above. The list above will show the friendly name.

⚠ **CAUTION** Entries are not verified or validated against the hospital's active directory instance. You must ensure correct spelling of the AD attribute name. Key-in the attribute's LDAP display name as defined in active directory. The spelling must match the entry in active directory or authentication and lookup will not be successful.

When changes are complete

1. Click **Save** at the bottom of the working window.

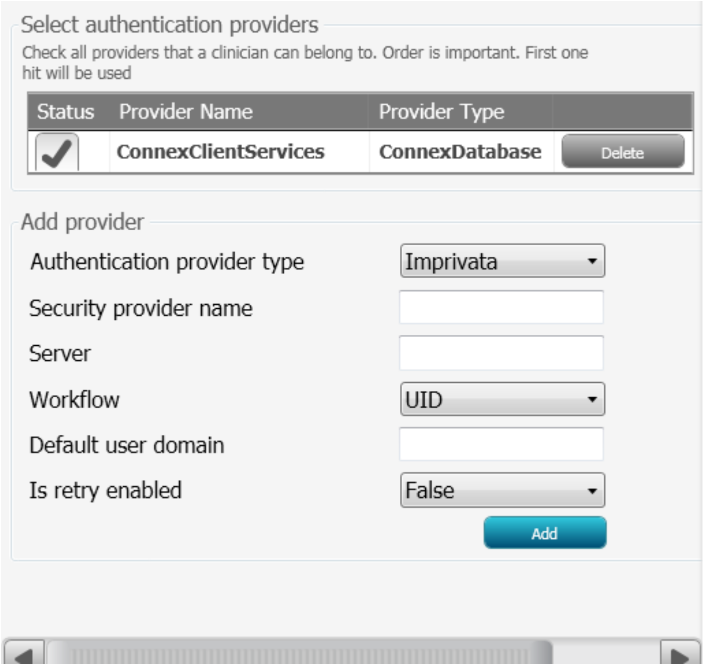
2. Restart ECS for all changes to take effect.

Configure for use with Imprivata OneSign

NOTE Make sure that the Admin Tool is launched with elevated privileges (**Run As Administrator**) before changing any security provider settings.

Add a provider for Imprivata

1. From the main window select **Imprivata** from the drop-down list of the **Add provider** area.



Select authentication providers

Check all providers that a clinician can belong to. Order is important. First one hit will be used

Status	Provider Name	Provider Type	
☑	ConnexClientServices	ConnexDatabase	Delete

Add provider

Authentication provider type	Imprivata
Security provider name	
Server	
Workflow	UID
Default user domain	
Is retry enabled	False

2. Enter the **Security provider name.**

   a. Enter a friendly name which identifies the hospital's Imprivata instance.

   b. A name is required since multiple Imprivata providers may be configured.

3. Enter the Imprivata **Server**.

   a. Enter the IP address (or DNS name) of the Imprivata server.

   b. Refer to the Connex CS Customer Project Req. Form, Appendix B1 as needed for this information.

4. Configure the Workflow. This setting should agree with the Imprivata server's **Medical device workflows** > **Log in** configured authentication method(s).

   a. There are two choices:

      - **UID (Unique Identifier)**

        This mode correlates to the Imprivata Proximity card authentication method. Depending on the Imprivata server's second factor configuration, clinicians may also need to enter a password or PIN.

      - **USR (Username and password)**

        This mode correlates to the Imprivata Password first factor authentication method.

   b. Refer to the Connex CS Customer Project Req. Form, Appendix B1 as needed for this information.

5. Enter the **Default user domain**. This setting is only used in the USR workflow.

   a. Enter the default Imprivata domain to use when one isn't specified in the username (i.e. "[domain]/[username]").

   b. Refer to the Connex CS Customer Project Req. Form, Appendix B1 as needed for this information.

6. Configure **Is retry enabled**. This setting is only used in the UID workflow.

   a. Select whether Connex CS should retry failed authentications using the USR workflow.

   b. Refer to the Connex CS Customer Project Req. Form, Appendix B1 as needed for this information.

7. Click **Add**.

8. If successful, the added security provider is available under **Select Authentication Providers**.

9. Click **Save**.

10. Restart ECS to enable all changes.

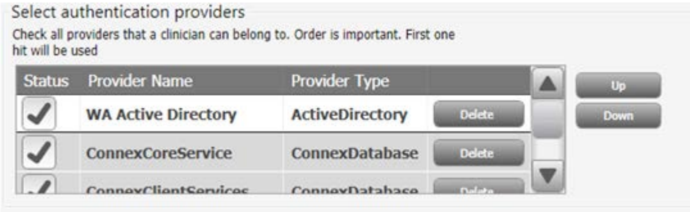
Order the security providers

NOTE Make sure that the Admin Tool is launched with elevated privileges (**Run As Administrator**) before changing any security provider settings.

The admin tool provides the capability to reorder the security providers.

1. Check the Status box for each identifier to be used.

2. Click on the Provider Name to select, and use the Up and Down buttons to change its order in the list.



Select authentication providers

Check all providers that a clinician can belong to. Order is important. First one hit will be used

Status	Provider Name	Provider Type	
☑	WA Active Directory	ActiveDirectory	Delete
☑	ConnexCoreService	ConnexDatabase	Delete
☑	ConnexClientServices	ConnexDatabase	Delete

NOTE The order is important when multiple security providers are configured and selected. The first successful authentication or lookup is used. The remaining providers in the list are not queried.

Delete a security provider

If required, the Admin tool provides the capability to delete a security providers.

1. Identify the provider to be deleted.
2. Click **Delete** in the "Select authentication providers" section.

CAUTION Do not delete the item associated with **ConnexDatabase**. This is the default setting in software and should be left in place. If the facility will not be using the ConnexDatabase, uncheck the Status in the "Select authentication providers" area instead.

H Connex database restore and reinstallation

Connex database restore

⚠ **WARNING** Database restore is a major database operation. This will impact the following things:

1. **Downtime**. The entire system will be down for the entire period of the restore operation.
2. **Potential loss of data**. The data that is collected by the system after the backup will be lost. For example if the backup was taken at 12:00 am on a specific date then the data collected after 12:00 am will be lost.

NOTE Before starting any of the steps in this section you need to login to Central Station from the Windows shell. By default the central station is using the Connex CS Application as a shell. Once you perform these steps you need to change the shell back to CS Application and restart the central station.

Based on the deployed environment, the steps for restore are different. The sections below outline these steps. The sections that follow detail each step.

For Standalone deployment:

1. Stop services, scheduled tasks, and close the Connex CS Application on the central station.
2. Restore the database from backup on the central station.
3. Restart services, scheduled tasks, and open the Connex CS Application on the central station.

For Client-Server deployment:

1. Stop services, scheduled tasks, and close the Connex CS Application on server and all central stations.
2. Restore the database from backup on the server.
3. De-provision the restored database.
4. Reinstall the fresh database on all the central stations.
5. Restart the data sync service and wait for completion of the initial sync operation.
6. Restart services, scheduled tasks, and open the CS Application.

Stop Services, Scheduled Tasks, and close the CS Application

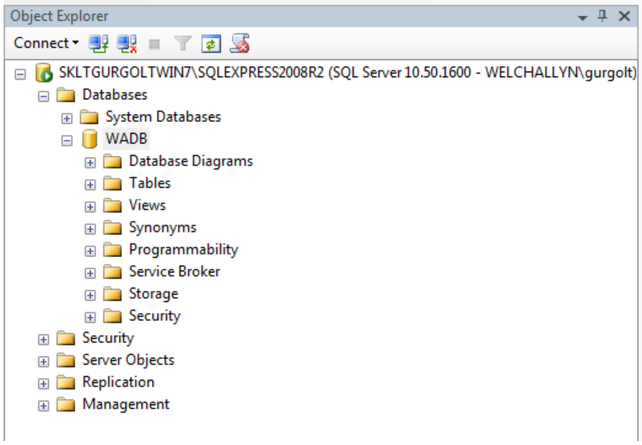
The services and scheduled tasks described below must be stopped or disabled prior to restoring a database from backup. The list differs depending on the deployed environment and the platform to be restored.

If restoring the database on the server, in a connected environment, stop the services and disable the scheduled tasks on the server. For a complete list of services and components on server, please refer to "Confirm Connex Server operational state".

Close the CS application, stop the services, and disable the tasks on ALL the central stations involved in the deployment. This step is applicable to central stations in connected as well as standalone deployment.

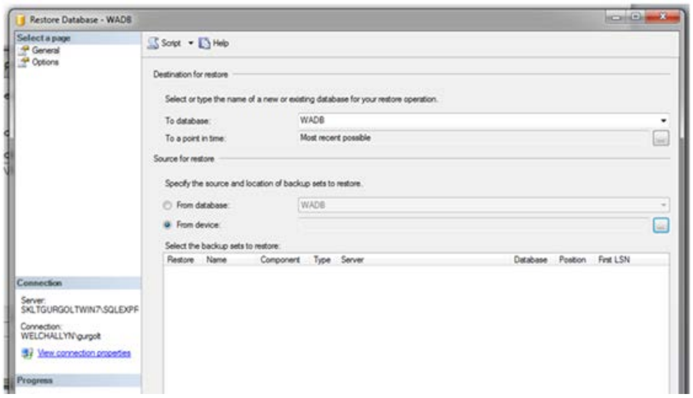
Restore the database from backup

1. Open the Microsoft SQL Server Management Suite (SSMS) tool, and under Object Explorer and expand the **Databases** node.



2. If there is a WADB database, right-click on the **WADB** database node and select **Tasks>Restore>Database**. If there is no WADB database, right-click on the Databases node and select **Restore Database…**

3. In the **Source for restore** section, select **From device**.



Destination for restore

Select or type the name of a new or existing database for your restore operation.

To database: WADB

To a point in time: Most recent possible

Source for restore

Specify the source and location of backup sets to restore.

○ From database: WADB

● From device:

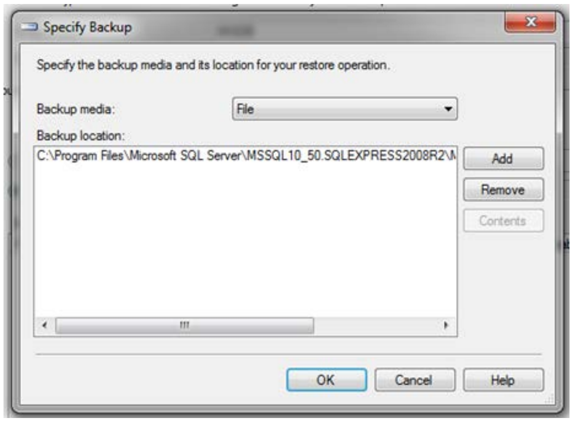
Select the backup sets to restore:

Restore	Name	Component	Type	Server	Database	Position	First LSN

Server:
SKLTGURGOLTWIN7\SQLEXPF

Connection:
WELCHALLYN\gurgolt

4. Click on the **...** button to browse to the backup folder and select the backup file. Remove any locations listed in the Backup location box. Click **Add** and browse to the folder that contains the backup file. The Backup location box will display the selected folder containing the backup file as illustrated in the screenshot below.



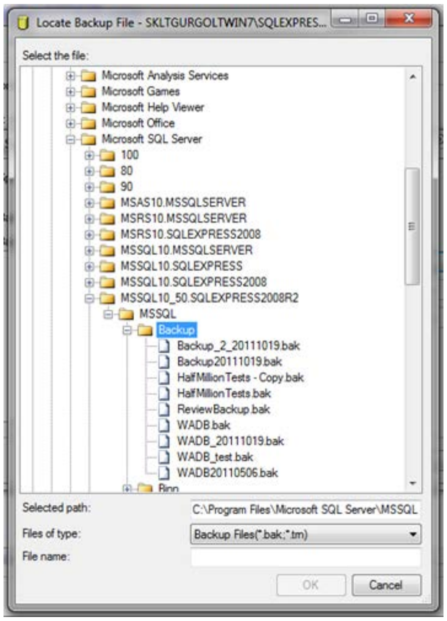
Specify the backup media and its location for your restore operation.

Backup media: File

Backup location:

C:\Program Files\Microsoft SQL Server\MSSQL10_50.SQLEXPRESS2008R2\M

5. Select the backup file and click **OK**.



Select the file:

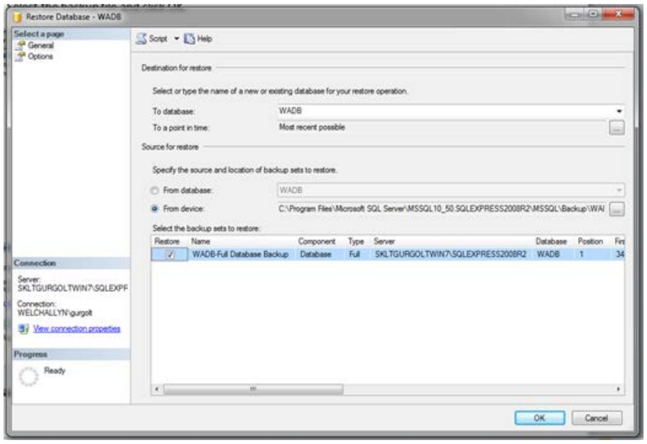
```
Microsoft Analysis Services
Microsoft Games
Microsoft Help Viewer
Microsoft Office
Microsoft SQL Server
    100
    80
    90
    MSAS10.MSSQLSERVER
    MSRS10.MSSQLSERVER
    MSRS10.SQLEXPRESS2008
    MSSQL10.MSSQLSERVER
    MSSQL10.SQLEXPRESS
    MSSQL10.SQLEXPRESS2008
    MSSQL10_50.SQLEXPRESS2008R2
        MSSQL
            Backup
                Backup_2_20111019.bak
                Backup20111019.bak
                HalfMillionTests - Copy.bak
                HalfMillionTests.bak
                ReviewBackup.bak
                WADB.bak
                WADB_20111019.bak
                WADB_test.bak
                WADB20110506.bak
            Binn
```

Selected path: C:\Program Files\Microsoft SQL Server\MSSQL

Files of type: Backup Files(*.bak;*.tm)

File name:

6. Click the **Restore** check box to select the backup.



Restore Database - WADB

Destination for restore

Select or type the name of a new or existing database for your restore operation.

To database: WADB

To a point in time: Most recent possible

Source for restore

Specify the source and location of backup sets to restore.

○ From database: WADB

● From device: C:\Program Files\Microsoft SQL Server\MSSQL10_50.SQLEXPRESS2008R2\MSSQL\Backup\WAI

Select the backup sets to restore:

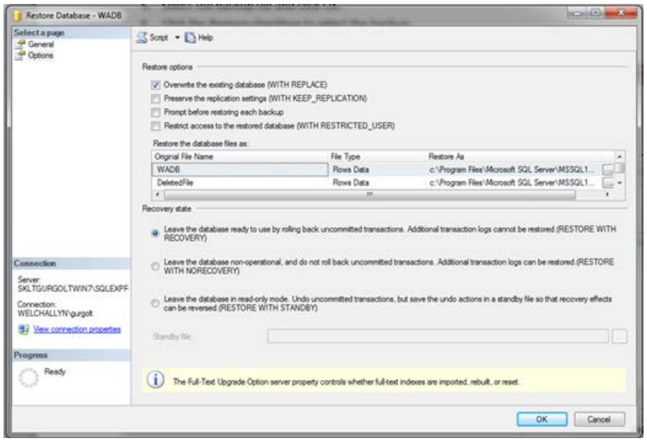
Restore	Name	Component	Type	Server	Database	Position	Fir
☑	WADB-Full Database Backup	Database	Full	SKLTGURGOLTWIN7\SQLEXPRESS2008R2	WADB	1	34

Connection

Server: SKLTGURGOLTWIN7\SQLEXPF

Connection: WELCHALLYN\gurgolt

7. Click the Options tab and check **Overwrite the existing database (WITH REPLACE)**.



Restore Database - WADB

Restore options

☑ Overwrite the existing database (WITH REPLACE)

□ Preserve the replication settings (WITH KEEP_REPLICATION)

□ Prompt before restoring each backup

□ Restrict access to the restored database (WITH RESTRICTED_USER)

Restore the database files as:

Original File Name	File Type	Restore As
WADB	Rows Data	c:\Program Files\Microsoft SQL Server\MSSQL1...
DeletedFile	Rows Data	c:\Program Files\Microsoft SQL Server\MSSQL1...

Recovery state

● Leave the database ready to use by rolling back uncommitted transactions. Additional transaction logs cannot be restored (RESTORE WITH RECOVERY)

○ Leave the database non-operational, and do not roll back uncommitted transactions. Additional transaction logs can be restored (RESTORE WITH NORECOVERY)

○ Leave the database in read-only mode. Undo uncommitted transactions, but save the undo actions in a standby file so that recovery effects can be reversed (RESTORE WITH STANDBY)

Standby file:

The Full-Text Upgrade Option server property controls whether full-text indexes are imported, rebuilt, or reset.

Connection

Server: SKLTGURGOLTWIN7\SQLEXPF

Connection: WELCHALLYN\gurgolt

8. Click **OK** to complete the restore.

9. For Standalone deployment skip to "Restart Services, Scheduled Tasks, and Open the CS Application." on page 177

De-provision the Restored Database

Follow these steps only if the database is restored on the server as part of a client-server deployment, otherwise skip to "Restart Services, Scheduled Tasks, and Open the CS Application." on page 177

To De-provision a database with the command line utility:

1. Logon to the computer that hosts the restored database OR logon to a computer that is connected to the host via the windows network.

2. Open a command window and navigate to the directory where the Connex CS Provisioning utility has been deployed. (To locate the deployment folder, search for the program "WelchAllyn.Connex.ProvisioningUtility.exe" or consult the CS install documentation.)

3. Enter the following at the command prompt which specifies the database host address, the database instance, the database name, and the parameter which instructs the utility to De-provision the database.

   WelchAllyn.Connex.ProvisioningUtility.exe SERVERNAME=<server name>\<instance name> DATABASENAME=WADB APPLYDEPROVSCRIPT

4. Examine the messages produced by the Provisioning Utility to verify that the operation succeeded.

Reinstall the database on the central stations

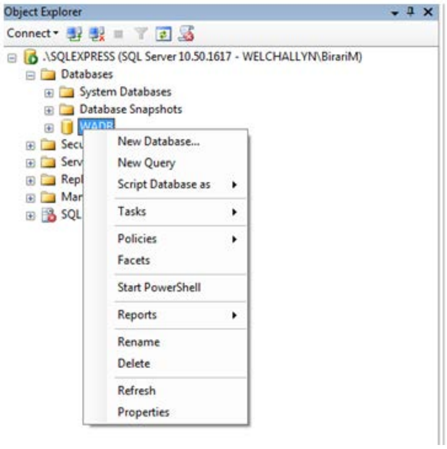
Follow these steps only if the database is restored on the server as part of a client-server deployment, otherwise skip to "Restart Services, Scheduled Tasks, and Open the CS Application." on page 177

To re-install the database on each central station:

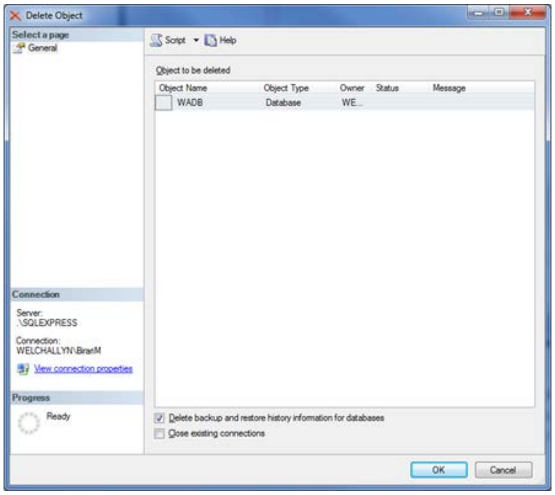
1. Open SQL Server management studio (SSMS). On CS central station this can be done by searching SSMS from the windows start menu.

2. Enter the correct login details in the pop-up dialog to enter SQL Server instance name.

3. Once SSMS is open, from the object explorer, select **WADB database**. Right click and select **Delete**.



4. Once **Delete** is clicked, following dialog displays.



Object to be deleted

Object Name	Object Type	Owner	Status	Message
□ WADB	Database	WE...		

Connection

Server:
.\SQLEXPRESS

Connection:
WELCHALLYN\BrianM

View connection properties

Progress

Ready

☑ Delete backup and restore history information for databases

□ Close existing connections

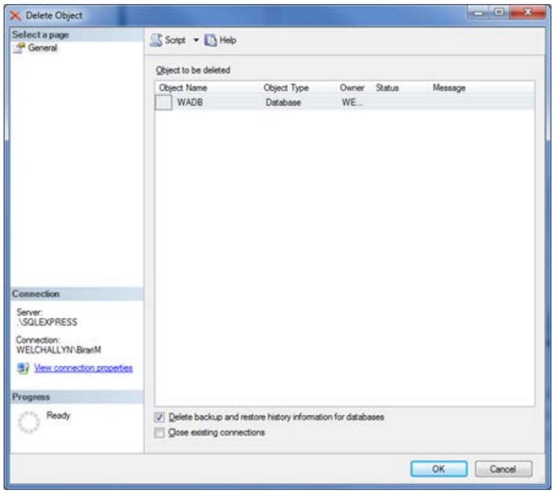
5. Check the **Close existing connections** box, and click **OK**. The dialog will be closed once the WADB is deleted.

6. Open the windows explorer and navigate to following path:

   C:\Program Files (x86)\Welch Allyn\Connex\Server\<version>\DataBaseInstaller.

NOTE The path may be different depending upon the location of the Program Files folder.

7. Double-click on **DatabaseInstaller.exe**. The following dialog displays.



Object to be deleted

Object Name	Object Type	Owner	Status	Message
□ WADB	Database	WE...		

Connection

Server:
.\SQLEXPRESS

Connection:
WELCHALLYN\BrianM

View connection properties

Progress

Ready

☑ Delete backup and restore history information for databases

□ Close existing connections

8. Change the SQL Server name to match the local SQL Server instance name and the click **Create database**.

9. Once the WADB is installed, the installer closes automatically. Normally, the installer would display a successful installation message box. But this message box is not displayed if the feature **Message Box Default Reply** is enabled. In Windows 7 embedded, this feature is enabled by default. So on Connex CS central stations the message box will not be displayed. But a message in the windows event log will be added confirming the success of the installation.

10. Also, after the installation is finished, a windows message box stating that “This program might not have installed correctly” may be showed. Ignore this message and click **Program installed successfully** to finish the installation.

Restart the Data Sync Service and Wait for Completion of the Initial Sync Operation

Follow these steps only if the database is restored on the server as part of a client-server deployment, otherwise skip to “Restart Services, Scheduled Tasks, and Open the CS Application.” on page 177.

In this step, the data sync service is restarted on ALL central stations. However, it is important to note that the best course of action is to start the data sync service on a single central station and to wait for the initial sync cycle to complete before moving on to the next central station. While the database on the central stations is empty, restarting data sync on all central stations simultaneously will result in unnecessary thrashing as all try to download data all at once from the server.

Restart Services, Scheduled Tasks, and Open the CS Application.

1. Restart the services and scheduled tasks that were shutdown previously
2. Start the Connex CS Application.

Special circumstances

In some cases over the course of use, it may be necessary to disconnect a client Central Station from the network for an extended period of time, such as construction projects.

In cases where the Central Station will be shut down or disconnected from the network for more than 30 days, it becomes necessary to purge to local database and start fresh. The local database must be dropped and recreated to maintain overall health of the system. A future update to this Administration Guide document will detail specific steps required.

Connex database reinstallation

There are some situations when a database reinstallation might become necessary, such as moving a client station from one network to a different network. Information from the old network must be removed prior to connection to the new network or the database will become corrupted with incorrect settings and location information.

In some instances, it may be more feasible to replace the database with a clean and empty database, and re-load the configuration from a previous backup.

⚠ **WARNING** When the WADB database is deleted and re-installed, all patient data, history, users, settings and location information will be lost. Do not undertake these steps without having a known-state backup configuration file to import at the end of the process.

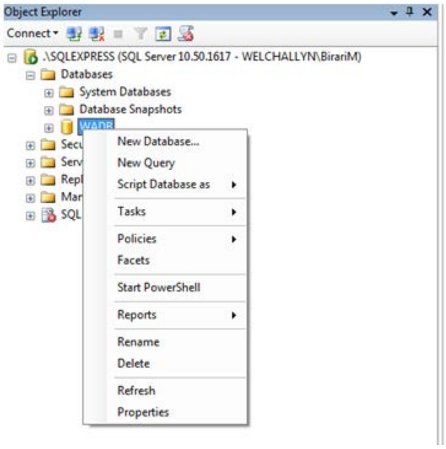
1. Run the Admin tools on the server and export the configuration settings that include master bed list and covered area. This includes the following
   - **Configuration settings**. This will ensure that the Master bed list and covered areas can be migrated to production environment.
   - **Users**. This will make sure that the User accounts will be migrated to production environment. Export users only if the users need to be migrated.
2. Shutdown all the Connex services that may be running on the server. The Connex Client Services should be shut down last (the following is not a complete list, but a representation of the major components that may be running based on deployment. For a complete list of services per configuration, reference Connex Install - Configuration guide):
   - ECS
   - EGS
   - Connex Data Backup
   - Connex Data Lifetime Manager
   - Connex Client Services.
3. Shutdown all the Connex services including process monitor component that may be running on ALL the central stations.
4. Do following steps first on server and then on all central stations:
   a. Open SQL Server management studio (SSMS). On server this can be done by entering SSMS into Start > Search. While on CS central station, this can be done by following steps:
   - Open up Task manager and click **New Task**.
   - Open the following:

     C:\Program Files (x86)\Microsoft SQL Server\100\Tools\Binn\VSShell\Common7\IDE\SSMS.exe.

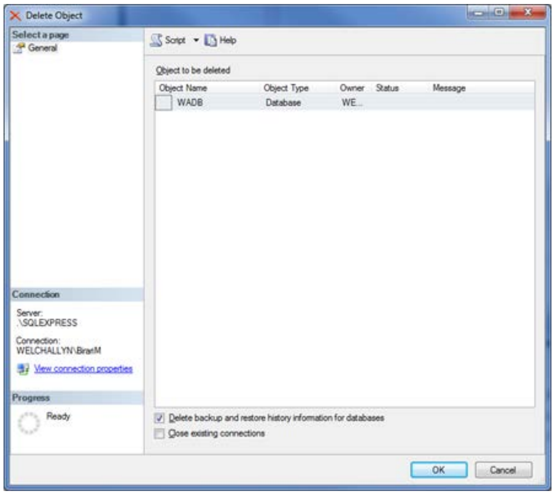
NOTE The path may be different depending upon the Program files folder.

   b. Enter the correct login details in the pop-up dialog to enter SQL Server instance name.

c. Once SSMS is open, from the object explorer, select the **WADB** database. Right click and select **Delete**.



5. Once delete is clicked, following dialog will be shown.



Server:
.\SQLEXPRESS

Connection:
WELCHALLYN\BirariM

Ready

Object to be deleted

Object Name	Object Type	Owner	Status	Message
WADB	Database	WE...		

☑ Delete backup and restore history information for databases

☐ Close existing connections

6. Check **Close existing connections** and click **OK**.

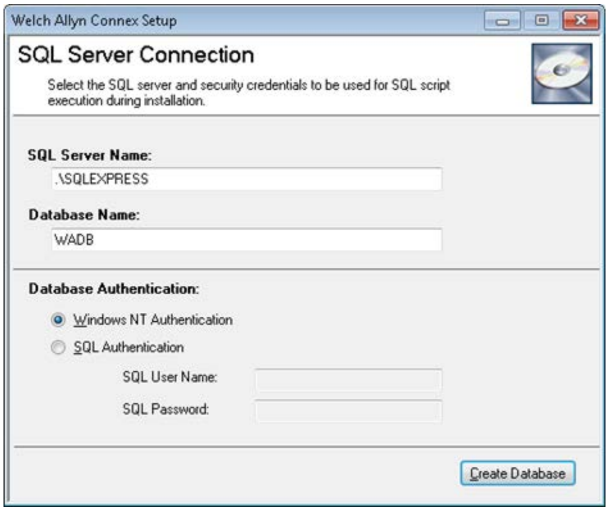
7. The dialog will be closed once the WADB is deleted.

8. Open the windows explorer and navigate to following path:

C:\Program Files (x86)\Welch Allyn\Connex\Server\<version>\DataBaseInstaller

NOTE The path may be different depending upon the Program files folder.

9. Double-click on the **DatabaseInstaller** application. The following dialog displays.



Welch Allyn Connex Setup

SQL Server Connection

Select the SQL server and security credentials to be used for SQL script execution during installation.

SQL Server Name: .\SQLEXPRESS

Database Name: WADB

Database Authentication:

● Windows NT Authentication

○ SQL Authentication

SQL User Name:

SQL Password:

a. Change the SQL Server name to match the local SQL Server instance name and click **Create database**.

b. Once the WADB is installed, a message box confirms the successful installation.

10. On the server, start all the Connex services.

11. On the server, start the admit tools. Import the configuration settings to restore the master bed list and covered area that were imported at the start of the process.

12. If there any new machines are added, activate the license for those machines.

13. Start all the services on all of the central stations. Do NOT start the Connex CS application yet.

14. Wait 10 minutes. This will give time for the configuration changes to sync with all the central stations. Then start the Connex CS application on all central stations.

I Network change and configuration

Network IP change overview

The change in the IP Address of one or more systems involved in the Connex CS network might cause many components to break. This requires updating the specific configurations in the system used by such components.

This section describes the step-by-step instructions to accomplish the IP address change of Connex Server and/or Connex Central Station in all possible deployments (viz. Standalone, and Client/Server) and external systems like EMR and 3rd Party Alarm Management System. The instructions are categorized based on the System Node (machine in CS network).

Refer to the *Connex CS Customer Project Req. Form, Appendix B1* for a known list of IP address assignments. Contact the customer IT staff or project manager if this information is unknown.

⚠ **CAUTION** Changes to the network interfaces on a live network will cause outages, and should be planned with the facility. Additional changes may also be required on each Central Station if the IP address of the Server that supports them is changed. Refer to the *Connex CS Software Install Guide* for additional information.

⚠ **CAUTION** All changes need to be completed during a planned downtime as most of the systems need to be restarted after making the required changes.

⚠ **CAUTION** Scenarios involving IP Address changes to multiple system nodes should follow the instructions from all relevant sections below. For example, in a client-server deployment, if the IP address of both the Connex Server and EMR Server changes, follow the instructions from both sections one after the other.

⚠ **CAUTION** Scenarios not mentioned here have no impact to any functionality. The person making the changes must have administrative rights on all systems in order to change the application configuration files.

Client Server deployment

If the IP address of the Connex server changes

This scenario should be handled as summarized below.

1. Follow the instructions in "EMR-side changes" on page 182 before changing the server's network interface. This needs to be communicated to the administrator managing EMR at the customer site.

2. Go to the Connex server; change the network interface with new IP address; follow the instructions in "Connex server-side changes" on page 182 and reboot the server. This will make all Connex Central Stations continue to operate in disconnected mode.

3. Go to each Connex Central Station and follow the instructions in "Each central station client-side changes" on page 185. Reboot the Connex Central Station. After reboot, the Connex Central Station will be running in a connected mode to the server.

EMR-side changes

1. Update the EMR's configuration, which is used to connect to Corepoint connections, with the following:

    a. **WA_ADT_IB** on the Connex server to use the new IP address. This may be required to make in-bound data flow properly.

    b. **WA_ORU_OB_CONFIRMED** and **WA_ORU_OB_UNCONFIRMED** on the Connex server to use new IP addresses if required. These may be required to make out-bound data flow properly.

Connex server-side changes

1. Use standard Microsoft Windows functions to change the network interface with the new IP address settings as needed.

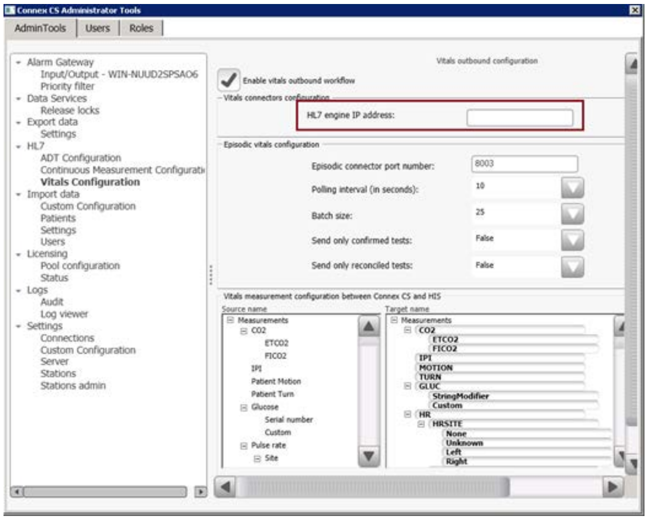
2. Update the new Server IP Address (HL7 Engine IP Address) in Episodic Vitals Configuration through Admin Tools. Typically, this will be the second interface on the server. This is used by both EGS and TDE for Episodic and Continuous vitals outbound.

    a. Launch the **Admin Tools Launcher**.

    b. Navigate to **HL7 > Vitals Configuration** screen.

    c. Change the **HL7 engine IP address** and save the changes.

    d. See below for an example.



Vitals outbound configuration

☑ Enable vitals outbound workflow

Vitals connectors configuration

HL7 engine IP address:

Episodic vitals configuration

Episodic connector port number: 8003

Polling interval (in seconds): 10

Batch size: 25

Send only confirmed tests: False

Send only reconciled tests: False

Vitals measurement configuration between Connex CS and HIS

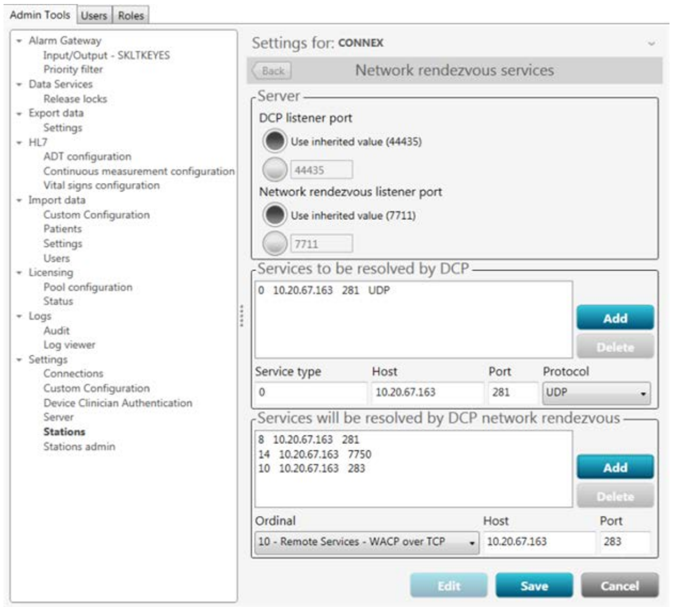
Source name	Target name
Measurements	Measurements
CO2	CO2
ETCO2	ETCO2
FICO2	FICO2
IPI	IPI
Patient Motion	MOTION
Patient Turn	TURN
Glucose	GLUC
Serial number	StringModifier
Custom	Custom
Pulse rate	HR
Site	HRSITE
	None
	Unknown
	Left
	Right

Update the SERVER NRS configuration

1. Launch the **Admin Tools Launcher** and navigate to **Stations > Network rendezvous services**.

2. Click **Delete** to delete the existing host entry under group **Services to be resolved by DCP**.

3. Add a new host entry by entering new the IP Address of Server under Host textbox and click **Add**. This will add the ECS entry as shown below.



Settings for: CONNEX

Network rendezvous services

Server

DCP listener port

● Use inherited value (44435)

○ 44435

Network rendezvous listener port

● Use inherited value (7711)

○ 7711

Services to be resolved by DCP

0 10.20.67.163 281 UDP

Service type	Host	Port	Protocol
0	10.20.67.163	281	UDP

Services will be resolved by DCP network rendezvous

8 10.20.67.163 281
14 10.20.67.163 7750
10 10.20.67.163 283

Ordinal	Host	Port
10 - Remote Services - WACP over TCP	10.20.67.163	283

4. Similarly, update ALL host entries for **Services will be resolved by DCP network rendezvous** as shown in the example above. Include entries for the following:

   a. Ordinal 8 using port 281, for Episodic data.

   b. Ordinal 10 using port 283, for Service Monitor data.

   c. Ordinal 14 using port 7750, for Secure Episodic data.

5. Click **Save** to save the changes.

Update additional Server settings for ECS and EGS

1. Update WACP IP Address in ECS service configuration file.

   a. Use standard Windows explorer tool to navigate to the location:

      C:\Program Files (x86)\Welch Allyn\Connex\ECS\<version>

   b. Open the file **WelchAllyn.Connex.EpisodicConnectivityService.exe.config** in any text editor.

   c. Search for the setting with a key **WACPTCPIPAddress**

   d. Update the setting value as indicated in the example below with new server IP address and save the changes.

```
<setting name=”WACPTCPIPAddress” serializeAs=”String”>
            <value>192.168.78.20</value>
      </setting>
```

2. Update WACP IP Address in EGS service configuration file.

   a. Use standard Windows explorer tool to navigate to the location:

      C:\Program Files (x86)\Welch Allyn\Connex\EGS\<version>

   b. Open the file **WelchAllyn.Connex.EnterpriseGateway.exe.config** in any text editor.

   c. Search for the IP address you want to change. If no search results are found, the file is using 'localhost' and no changes are necessary.

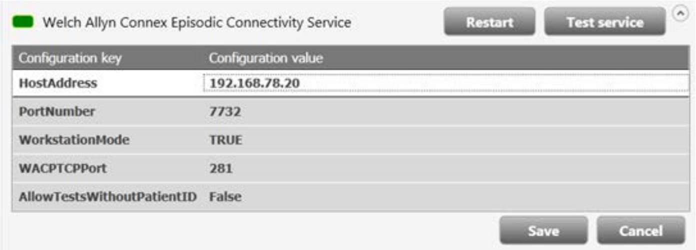
   d. Execute a find and replace for the old and new IP address values.

3. Ensure the Host address through Admin Tools

   a. Launch **Admin Tools** and navigate to the **Connections** screen.

   b. Expand the configuration details for **Welch Allyn Connex Episodic Connectivity Service** by clicking the expander button.

   c. Ensure that the configuration value for the Host Address is either set to **localhost** or new the IP address of the server as shown below.



Configuration key	Configuration value
HostAddress	192.168.78.20
PortNumber	7732
WorkstationMode	TRUE
WACPTCPPort	281
AllowTestsWithoutPatientID	False

4. Reboot the server. This will make all Connex Central Stations continue to operate in disconnected mode.

Each central station client-side changes

Update the application configuration file WelchAllyn.Connex.DataSync.exe.config to use the new Server IP address to point to Remote Database.

1. Use standard Windows explorer tool to navigate to the location:

   C:\Program Files (x86)\Welch Allyn\Connex\Data Synchronization Service\1.0

2. Open the file "WelchAllyn.Connex.DataSync.exe.config", in any text editor.

3. Search for the setting with a key "Sync:HubInstanceName".

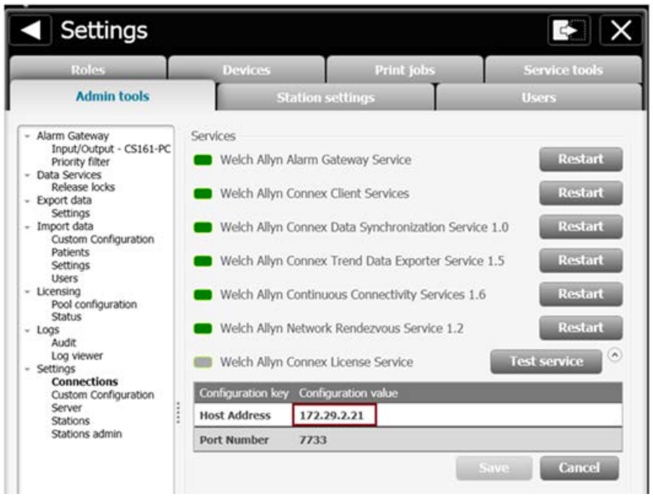
4. Update the setting value as indicated in the example below with new server IP address and save the changes.

   <add key="Sync:HubInstanceName" value="**172.29.2.22**\SQLSTANDARD"/>

Update Central Station license service

1. On the central station, navigate to **Settings > Advance Settings** (if needed) **> Admin Tools > Connections** screen.

2. Expand the configuration details for "Welch Allyn Connex License Service" by clicking the expander button as shown.



Configuration key	Configuration value
Host Address	172.29.2.21
Port Number	7733

3. Change the configuration value for the **Host Address** with the new IP address of the server as shown in the screenshot above.

4. Click **Save** to save the changes.

5. Reboot the Connex Central Station. After reboot, the Connex Central Station is connected to the sever.

6. Repeat steps 1 through 5 at each Central Station on the network, and the Warm Spare station if included.

If the IP address of the Connex Central Station changes

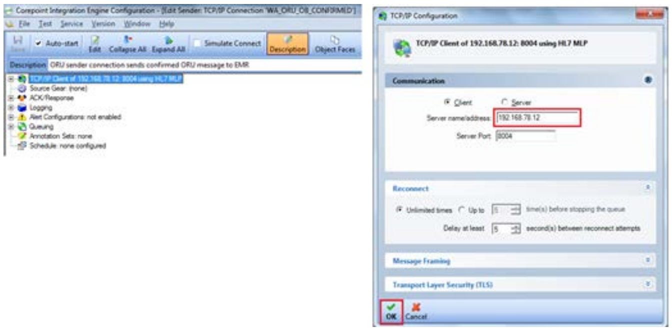
1. Change the Connex Central Station's network interface with new IP address.

2. Reboot the Connex Central Station system. After reboot it will re-register its new listening endpoint for AGS. Connex Server will automatically re-discover them.

If the IP Address of the EMR Server Changes

Corepoint-side change on Connex Server: Update Corepoint connections WA_ORU_OB_CONFIRMED and WA_ORU_OB_ UNCONFIRMED to point to new EMR server address. This is required for Episodic and Continuous vitals outbound messages to be successfully sent to EMR.

1. On the Connex server, launch **Start > Corepoint Health > Configuration**. Enter the login credentials.
2. Find the connection **WA_ORU_OB_CONFIRMED** under Objects.
3. Double-click on the connection and then its **TCP/IP Configuration** to open the connection details as shown below.



Corepoint Integration Engine Configuration - [Edit Sender: TCP/IP Connection 'WA_ORU_OB_CONFIRMED']

Description: ORU sender connection sends confirmed ORU message to EMR

- TCP/IP Client of 192.168.78.12: 8004 using HL7 MLP
- Source Gear: (none)
- ACK/Response
- Logging
- Alert Configurations: not enabled
- Queuing
- Annotation Sets: none
- Schedule: none configured

TCP/IP Configuration

TCP/IP Client of 192.168.78.12: 8004 using HL7 MLP

Communication

● Client ○ Server

Server name/address: 192.168.78.12

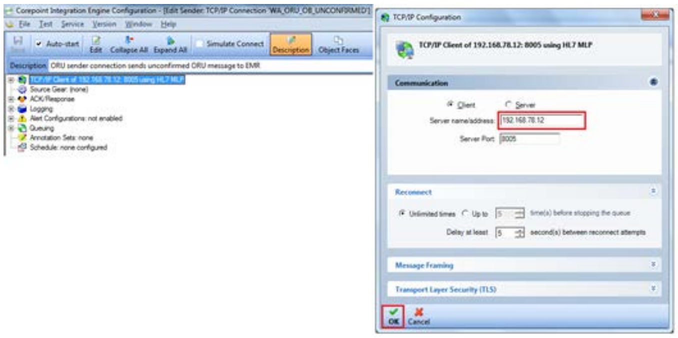
Server Port: 8004

Reconnect

● Unlimited times ○ Up to 5 time(s) before stopping the queue

Delay at least 5 second(s) between reconnect attempts

4. Change the **Server name/address** field with the new EMR server IP address as highlighted above.
5. Click **OK**. Close the connection details.
6. Similarly, find the connection **WA_ORU_OB_UNCONFIRMED** under Objects. Double-click on the connection and then its **TCP/IP Configuration** to open the connection details as shown below.



Corepoint Integration Engine Configuration - [Edit Sender: TCP/IP Connection 'WA_ORU_OB_UNCONFIRMED']

Description: ORU sender connection sends unconfirmed ORU message to EMR

- TCP/IP Client of 192.168.78.12: 8005 using HL7 MLP
- Source Gear: (none)
- ACK/Response
- Logging
- Alert Configurations: not enabled
- Queuing
- Annotation Sets: none
- Schedule: none configured

TCP/IP Configuration

TCP/IP Client of 192.168.78.12: 8005 using HL7 MLP

Communication

● Client ○ Server

Server name/address: 192.168.78.12

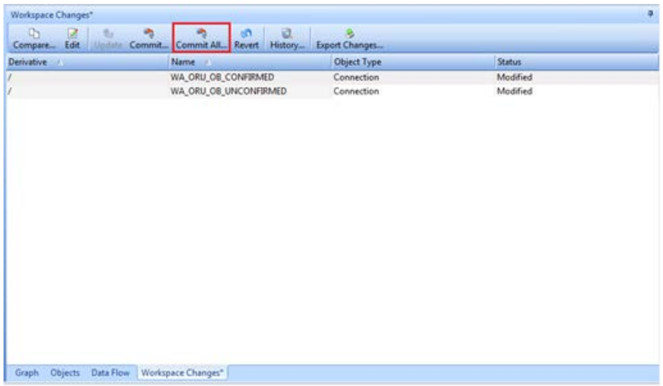
Server Port: 8005

Reconnect

● Unlimited times ○ Up to 5 time(s) before stopping the queue

Delay at least 5 second(s) between reconnect attempts

7. Change the “Server name/address” field with the new EMR server IP Address as highlighted above.
8. Click **OK**. Close the connection details.
9. Navigate to and select the **Workspace Changes** tab.



Derivative	Name	Object Type	Status
/	WA_ORU_OB_CONFIRMED	Connection	Modified
/	WA_ORU_OB_UNCONFIRMED	Connection	Modified

10. Click **Commit All** to apply the changes of both connections. A confirmation message appears.

11. Click **Commit and Activate** to save the changes and restart the services to take effect immediately.

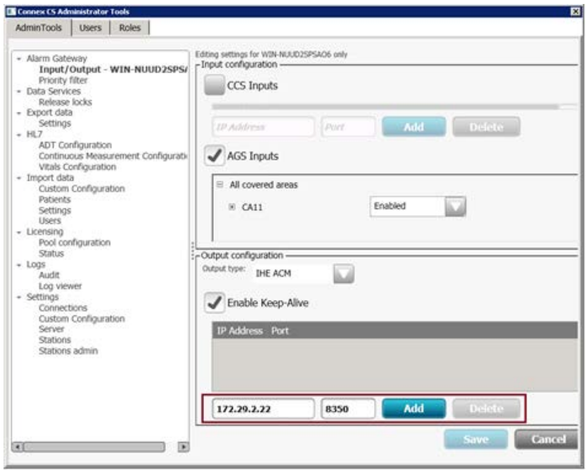
If the IP Address of the Third Party Alarm Server changes

Update the IHE ACM Configuration through Admin Tools to use the new IP address of the Third Party Alarm Server.

1. On the Connex server, launch the **Admin Tools Launcher**.

2. Navigate to **Alarm Gateway > Input/Output** screen.

3. Click **Delete** to delete the existing IP Address/Port entry.



Editing settings for WIN-NUUD2SPSAO6 only

□ CCS Inputs

☑ AGS Inputs

CA11: Enabled

Output type: IHE ACM

☑ Enable Keep-Alive

172.29.2.22 8350

4. Add the new **IP Address/Port entry** by entering new the IP Address of the Third Party Alarm Server in the textbox highlighted above and click **Add**.

5. Click **Save** to save the changes. It will ask to restart the Alarm Gateway Service.

6. Navigate to the **Connections** screen and restart the Alarm Gateway Service.

If the Corepoint IP address Changes

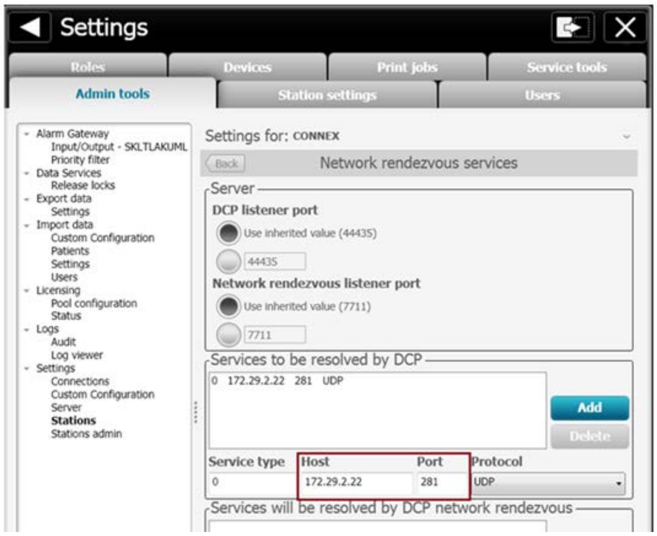
If you change your system's IP address or hostname, you will need to rerun the application CreateSite.exe as an Administrator to reconfigure the website bindings, ensuring that Corepoint Integration Engine Monitor will function correctly. This application is located at C:\Program Files\Corepoint Health\Corepoint Integration Engine\Bin. See the "Server Authentication" chapter for information about Corepoint security certificates.

Standalone deployment

If the IP address of the standalone central station system changes

Update the NRS configuration

1. On the central station, navigate to **Settings** > **Advanced Settings** (if required) > **Stations** > **Network rendezvous services** screen.
2. Click **Delete** to delete the existing host entry under group **Services to be resolved by DCP**.
3. Add a new host entry by entering new the IP Address of Server under Host textbox and click **Add**. This will add the ECS entry as seen below.



Settings for: CONNEX

Network rendezvous services

Server

DCP listener port

● Use inherited value (44435)

○ 44435

Network rendezvous listener port

● Use inherited value (7711)

○ 7711

Services to be resolved by DCP

0 172.29.2.22 281 UDP

Service type	Host	Port	Protocol
0	172.29.2.22	281	UDP

Services will be resolved by DCP network rendezvous

4. Similarly, update all host entries for **Services will be resolved by DCP network rendezvous** if defined.
5. Click **Save** to save the changes.
6. Navigate to the **Connections** screen and restart **Welch Allyn Network Rendezvous Service**.

Update additional settings for ECS

1. Update WACP IP Address in ECS service configuration file.

   a. Use standard Windows explorer tool to navigate to the location:

      C:\Program Files (x86)\Welch Allyn\Connex\ECS\1.6

   b. Open file “WelchAllyn.Connex.EpisodicConnectivityService.exe.config” in any text editor; search for the setting with a key “WACPTCPIPAddress.”

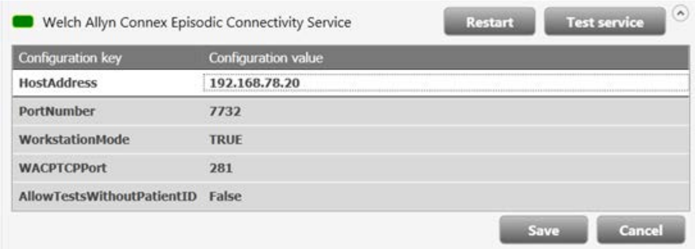
   c. Update the setting value as indicated in the example below with new server IP address and save the changes.

```
<setting name=”WACPTCPIPAddress” serializeAs=”String”>
        <value>192.168.78.20</value>
    </setting>
```

2. Ensure Host address through Admin Tools

   a. Launch **Admin Tools** and navigate to **Connections** screen.

   b. Expand the configuration details for “Welch Allyn Connex Episodic Connectivity Service” by clicking the expander button. An example is shown below.



Configuration key	Configuration value
HostAddress	192.168.78.20
PortNumber	7732
WorkstationMode	TRUE
WACPTCPPort	281
AllowTestsWithoutPatientID	False

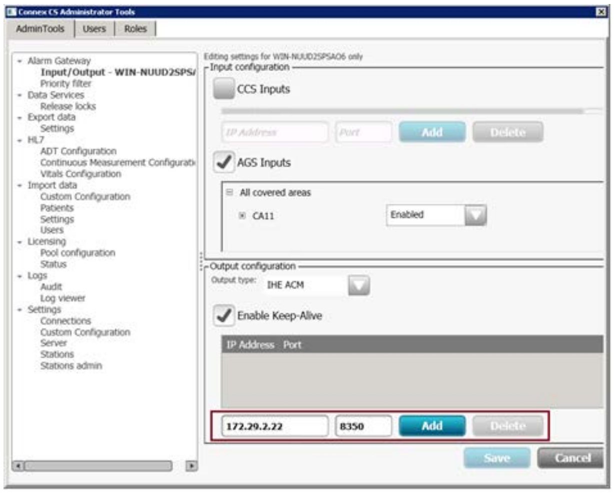
   c. Ensure that the configuration value for the Host Address is either set to “localhost” or new IP address of the server as shown above.

3. Restart the system.

If the IP address of the Third Party Alarm Server Changes

Update the IHE ACM Configuration through Admin Tools to use the new IP address of the Third Party Alarm Server.

1. On the Central Station, navigate to **Settings** > **Advanced settings** (if required) **> Admin Tools tab** > **Alarm Gateway** > **Input/Output** screen.
2. In the **Output configuration** area, click **Delete** to delete the existing IP Address/Port entry.
3. Add the new IP Address/Port entry by entering new the IP Address of the Third Party Alarm Server in the textbox highlighted below and click **Add**.
4. Click **Save** to save the changes. A message appears asking the user to also restart the Alarm Gateway Service.
5. Navigate to the **Connections** screen and **Restart** the Alarm Gateway Service.



Editing settings for WIN-NUUD2SPSAO6 only

Input configuration

□ CCS Inputs

☑ AGS Inputs

All covered areas

CA11 Enabled

Output configuration

Output type: IHE ACM

☑ Enable Keep-Alive

172.29.2.22 8350

J Anti-virus Software Exclusion Folders

Hillrom recommends using virus protection software in accordance with industry best practices.

Exclusion Overview

⚠ **CAUTION** The anti-virus system on your computer may attempt to block certain files that are necessary to successfully install and run the software. To address this issue, refer to the exclusion lists below for the appropriate exclusion information.

Connex CS Exclusions

- %ProgramData%\Welch Allyn
- [INSTALL LOCATION]\Welch Allyn

Corepoint Exclusions

- %ProgramData%\Corepoint Health