

Welch Allyn Connex® VM data management system

Administrator guide

© 2010 Welch Allyn. All rights are reserved. To support the intended use of the product described in this publication, the purchaser of the product is permitted to copy this publication, for internal distribution only, from the media provided by Welch Allyn. No other use, reproduction, or distribution of this publication, or any part of it, is permitted without written permission from Welch Allyn. 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.

Welch Allyn, Connex, and Spot Vital Signs are registered trademarks of Welch Allyn. Microsoft, Windows, and SQL Server are registered trademarks of Microsoft Corporation. Citrix and ICA are registered trademarks of Citrix Systems, Inc. XenApp is a trademark of Citrix Systems, Inc.

Software in this product is Copyright 2010 Welch Allyn or its vendors. All rights are reserved. The software is protected by United States of America copyright laws and international treaty provisions applicable worldwide. Under such laws, the licensee is entitled to use the licensed software as intended in its directions for use. The software may not be copied, decompiled, reverse-engineered, disassembled, or otherwise reduced to human-perceivable form. This is not a sale of the software or any copy of the software; all right, title, and ownership of the software remain with Welch Allyn or its vendors.

Federal law restricts this device to sale by or on the order of a physician.

For information about any Welch Allyn product, call Welch Allyn Technical Support:

USA	+1 800 289 2501	Australia	+61 2 9638 3000
Canada	+1 800 561 8797	China	+86 21 6327 9631
European Call Center	+353 46 90 67790	France	+33 1 55 69 58 49
Germany	+49 695 098 5132	Japan	+81 3 6383 0852
Latin America	+1 305 669 9003	Netherlands	+31 202 061 360
Singapore	+65 6419 8100	South Africa	+27 11 777 7555
Sweden	+46 85 853 6551	United Kingdom	+44 207 365 6780

DIR 80015957 Ver. C

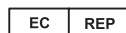
Connex VM Administrator Guide



Manufacturer

Welch Allyn, Inc.
4341 State Street Road
Skaneateles Falls, New York 13153-0220
USA

www.welchallyn.com



European Community representative

European regulatory manager
Welch Allyn, Ltd.
Navan Business Park
Dublin Road, Navan
County Meath, Republic of Ireland



Meets essential
requirements of European
Medical Device Directive
93/42/EE

Contents

About this guide	1
Safety symbols	1
Reference documents	3
Introduction	5
Connex VM system	5
Workflows	8
First-time setup	11
Connex VM client application	13
Authentication	13
Allowed values for manually entered vital signs data	14
Concurrency locks	14
Program configuration	15
User management	23
Connex VM roles and privileges	23
User accounts	27
Location management	31
Patient management	33
Create a new patient	33
Import patients	33
View or edit a patient record	36
Delete a patient	36
Configuration	37
Adjust server configuration settings	37
Configure settings for Welch Allyn services	40
Configure Enterprise Gateway Service	43
Maintenance	47
Disaster recovery	47
HL7 connectivity	48

Reconciliation in the Connex VM system 53

Virtual desktop environment 55

 Thin client setup 55

Troubleshooting 57

 Logs 57

 Troubleshooting services 58

 Troubleshooting network problems 60

 Troubleshooting specific problems 61

Reference 67

 Welch Allyn services 67

 TCP/UDP ports used 68

 Medical device connectivity requirements 69

About this guide

This guide is for network administrators and others with a background in information technology. Topics include configuring, managing, and troubleshooting the Connex VM data management system.

For information on clinical use and basic administration of the system, refer to the **Help** menu in the Connex VM client application.

For information on using the devices that connect to the system, consult the directions for use that came with the devices or visit our product catalog at welchallyn.com.

Safety symbols



WARNING statements in this manual identify conditions or practices that could lead to illness, injury, or death.



Caution statements in this manual identify conditions or practices that could result in damage to the equipment or other property.



Consult operating instructions.

Reference documents

Description	Part number
Connex VM directions for use	100600-2 For each language, a PDF file of the directions for use (Connex.pdf) is located in the Help Files folder on the Connex VM installation DVD. The directions for use can also be found in the Help menu of the client application.
VSM 6000 Series directions for use	103501
Spot Vital Signs LXi directions for use	705310
Spot Vital Signs LXi wireless radio accessory directions for use (b radio)	4500-921
Spot Vital Signs LXi wireless radio accessory directions for use (a/b/g radio)	4500-923
Spot Vital Signs directions for use	4200-87E
VSM 300 directions for use, Masimo	810-2250-01
VSM 300 directions for use, Nellcor	810-2252-01

Introduction

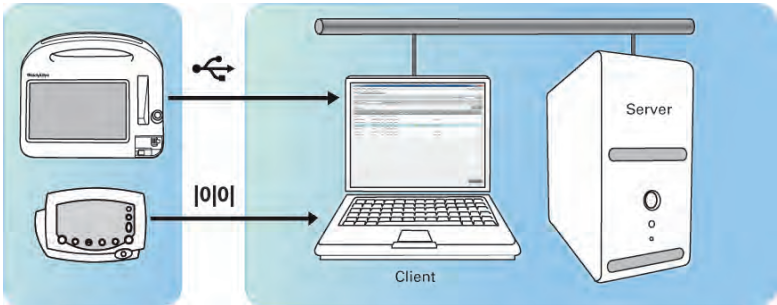
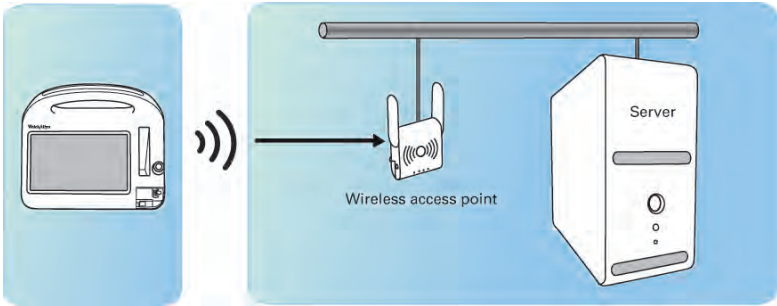
Connex VM system

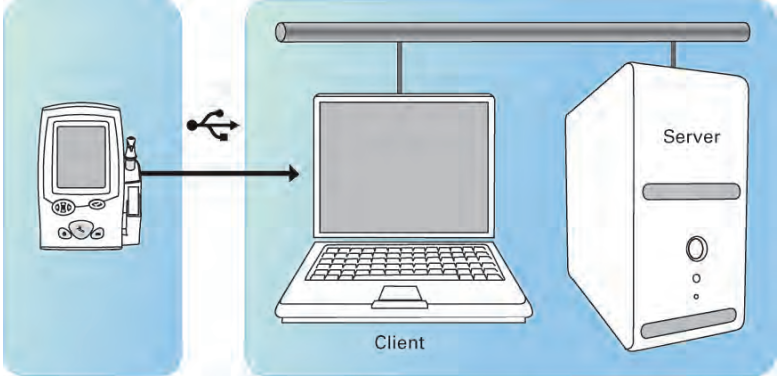

The Welch Allyn Connex VM data management system is a software system that enables users to collect patient data from a variety of vital signs devices, enter data manually, review data, and send data to a hospital information system (HIS).

Hardware configurations

The following table shows examples of hardware configurations. Your site might have one or more configurations deployed.

Symbols:  Data flow  USB  Serial  Radio signal  Network

Configuration	Description
Workstation-to-server A vital signs device is connected to the client workstation via USB or serial cable. The workstation pulls data from the device, and then sends the data to the server.	
Wireless The vital signs device sends data wirelessly to the server.	

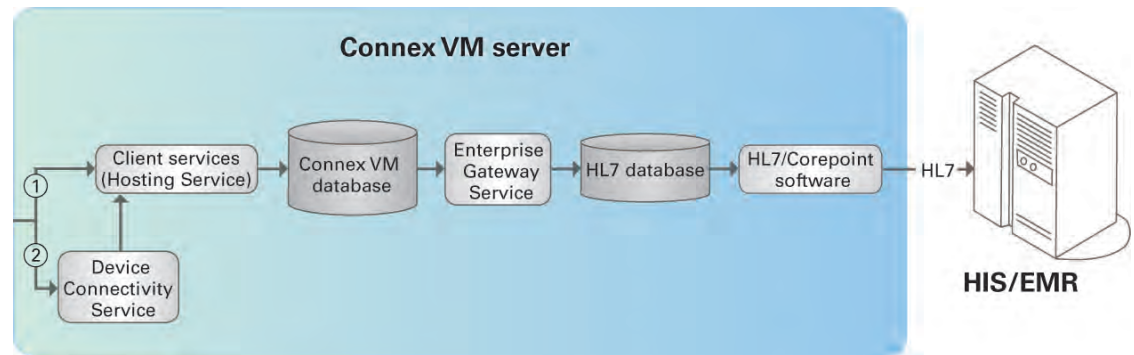
Configuration	Description
Connex VM vitals kiosk A vital signs device is connected to the client kiosk via USB. The device pushes data to the kiosk. The kiosk then sends the data to the server.	 <p>The diagram illustrates the 'Connex VM vitals kiosk' configuration. On the left, a vital signs device is shown. A USB cable connects it to a client kiosk (a laptop) in the center. The kiosk is labeled 'Client'. To the right of the kiosk is a server tower labeled 'Server'. A horizontal line above the kiosk and server indicates a network connection.</p>
Device-to-server The vital signs device connects to the server via Ethernet connection.	 <p>The diagram illustrates the 'Device-to-server' configuration. On the left, a vital signs device is shown. On the right is a server tower labeled 'Server'. A horizontal line above both devices indicates a direct Ethernet connection between them.</p>

Connex VM server

The Connex VM server stores and serves Connex VM system data and patient medical information.

Component	Description
Device Connectivity Service (DCS)	Facilitates device access to the server.
Client services (Welch Allyn Hosting Service)	Facilitate Connex VM client application access to the server.
Connex VM database	Holds Connex VM system data (user accounts, audit logs, and settings) and patient medical information.
Enterprise Gateway Service	Facilitates communication between the server and external systems (HIS, EMR, and files).
HL7 database	Holds inbound ADT data and outbound vital signs data until they are processed.
HL7/Corepoint software (integration engine)	Exchanges inbound and outbound messages with the HIS.

The diagram shows the flow of outbound data. Inbound flow is the reverse of outbound flow.



Item	Shows how data flows through the server in a...
①	Workstation-to-server configuration Connex VM vitals kiosk configuration
②	Wireless configuration Device-to-server configuration

Software components

The system includes the following software components. For more information on Welch Allyn services, refer to the "Reference" section.

Device Connection Protocol (DCP)

The DCP Service provides the Device Connection Protocol for determining where Welch Allyn Device Connectivity Service (DCS) resides.

Because DCP relies on UDP network broadcasts, it is assumed that one DCP Server will be installed per network. If DCP broadcasts (UDP port 44435) are forwarded by the infrastructure network routers to the Connex VM server, then only one DCP Server is required.

Device Connectivity Service (DCS)

Device Connectivity Service (DCS) is the device connectivity solution for Welch Allyn devices. DCS receives messages and requests from the devices and processes them for use by the Connex VM server.

Enterprise Gateway Service (EGS)

Enterprise Gateway Service (EGS) connects the Connex VM server to the customer's enterprise, specifically HL7-based ADT and hospital information systems.

Workflows

The system can capture vital signs from a number of devices used in a variety of workflows. After the data is saved, the server sends the data immediately to the hospital information system.

The following summarizes the characteristics of each workflow.

Workflow	Description
Wireless workflow	This workflow supports a vital signs device with a wireless radio. The device also enables clinicians to enter patient identification either manually or from a barcode scanner. The clinician sends readings directly from the device to the server. No workstation user interface is needed. The server sends the data immediately to the hospital information system. Typically the device is mobile and running on battery power.
Ethernet workflow	This workflow supports a vital signs device with an Ethernet connection. The device also enables clinicians to enter patient identification either manually or from a barcode scanner. The clinician sends readings directly from the device to the server. No workstation user interface is needed. The server sends the data immediately to the hospital information system. Typically the device is stationary and plugged in to an electrical outlet.
Batch spot-check vitals	This workflow supports a vital signs device that enables clinicians to enter patient identification either manually or from a barcode scanner. The clinician uses the device to capture multiple patients' vital signs. The clinician then connects the device to a workstation via USB and uses the client application to import all readings at once. The server sends the data immediately to the hospital information system. Typically the device is mobile and running on battery power.
Push from device/auto reconcile batch	This workflow supports a vital signs device that enables clinicians to enter patient identification either manually or from a barcode scanner. The clinician uses the device to capture multiple patients' vital signs. The clinician then connects the device to a kiosk via USB and uses the device to upload all readings at once. The server sends the data immediately to the hospital information system. Typically the device is mobile and running on battery power.
Computer-based vital signs	In this workflow, a vital signs device and a workstation are mounted together. Both the device and a barcode scanner are connected to the workstation. The clinician uses the client application to start vital signs readings and enter additional patient data. After the clinician saves the data, the server sends the data immediately to the hospital information system.
Vital signs monitoring without patient identification at the device	This workflow supports a device capable of continuous vital signs monitoring. The device monitors a single patient. The clinician then connects the device to a workstation, uses the client application to identify the patient, and uploads the readings. The server sends the data immediately to the hospital information system.
Vital signs monitoring with patient identification at the device	This workflow supports a device capable of continuous vital signs monitoring. The device also enables clinicians to enter patient identification either manually or from a barcode scanner. The device monitors a single patient and saves the data. The clinician then sends the data via the push, wireless, or Ethernet workflow.
Triage	In this workflow, the device is permanently attached to a workstation. A barcode scanner might also be attached to the workstation. The clinician uses the client application to start vital signs readings and enter additional

Workflow	Description
	patient data. After the clinician saves the data, the server sends the data immediately to the hospital information system.

First-time setup

After the system is installed, follow these steps to configure it for use.

Task	For instructions or more information
1. Set up client application settings.	"Program configuration"
2. Set up user roles and privileges.	"Connex VM roles and privileges"
3. Set up user accounts. Ensure that you set up a minimum of one administrator account and one clinician account.	"User accounts"
4. Set up locations (premium service).	"Location management"
5. Create patients.	"Patient management"
6. Configure firewalls, virus software, and router access lists to allow Connex VM applications and ports. This might need to be done on workstations, servers, and network routers, based on your computer and network environment.	"Reference"

Connex VM client application

The client application (also referred to as "program" in this guide) enables you to perform many administrative tasks. In this guide, instructions for these tasks assume that you are logged on to the application and have the appropriate level of authorization.

This section covers program configuration and some aspects of the user experience.

Authentication

Depending on the configuration, the server authenticates users by one of these methods:

- Connex VM user name and password ("standard sign-on")
- Active Directory user name and password ("single sign-on")

Each method affects the user experience in the following ways.

Standard sign-on

If the server is configured for standard sign-on, the logon window appears whenever a user opens the client application.

To log on, enter Connex VM user name and password.

To log off, do any of the following:

- Click **Log off** in the upper right corner of the main window.
- In the menu bar, click **File > Log off**.

Both options end the current session and return the logon window.

Alternatively, click **File > Exit** to close the program.

Single sign-on

If the server is configured for single sign-on, the user is logged on automatically using Active Directory credentials. When the user opens the application, the logon window is bypassed, and the **Home** page appears.

To log off, click **File > Switch user** to end the current session and open the logon window.

Because only those with Connex VM user accounts can log on through this window, this feature is primarily intended for use by administrators.

Alternatively, click **File > Exit** to close the program.

In single sign-on mode, neither the **Log off** button nor **File > Log off** is available.

Allowed values for manually entered vital signs data

The client application validates manually entered vital signs data. Users can type only values that meet these requirements.

Measurement	Allowed range	Allowed characters
NIBP systolic	25 mmHg–260 mmHg	0..9
NIBP diastolic	10 mmHg–235 mmHg	0..9
Pulse rate	20–250	0..9
Pulse oximetry (SpO2)	1–100	0..9
Temperature	68.0°F–110.0°F (20.0°C–43.3°C)	0..9, decimal separator
Respiration	1–99	0..9
Pain	0–99	0..9
Height	0.0 in–100.0 in (0 cm–254 cm)	0..9, decimal separator (0..9)
Weight	0.0 lb–499.0 lb (0.0 kg–226.3 kg)	0..9, decimal separator
Glucose	0 mg/dl–600 mg/dl (0.0 mmol/l–33.3 mmol/l)	0..9 (0..9, decimal separator)
Comments	Not applicable	Any character

Concurrency locks

When you start to edit a record in the database, the database locks the record so that other users cannot edit the same record.

The lock releases automatically if you do not save the record after a designated period. The default lock time is 20 minutes and can be configured on the **Server configuration** page in **Administrator tools**.

In **Administrator tools**, you can also search for locked records and release them manually.

Release concurrency locks manually

1. In the menu bar, click **Administration > Administrator tools**.
2. In the navigation bar on the left side of the page, click **Locks > Release Locks**.
3. Search for locked records by entity type.
 - a. Select an item from the **Entity type** drop-down list.
 - b. Click **Search**.

Search results appear under **Lock item lists**.

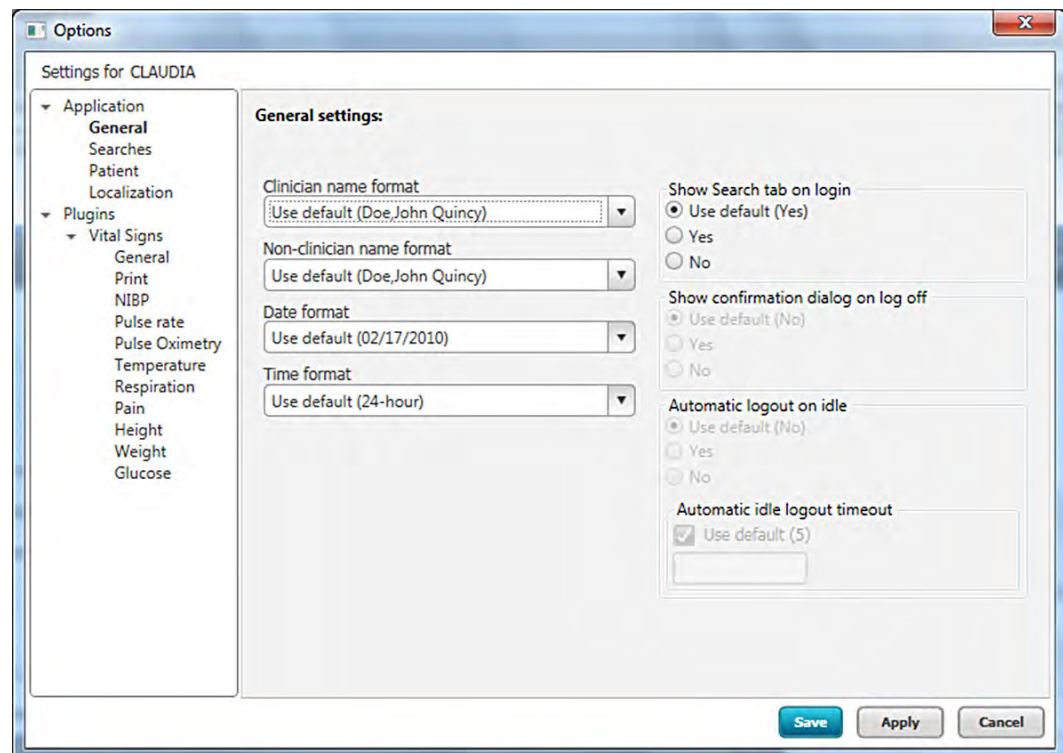
4. Release locks.

- If you want to release the lock on a specific record, click the record to select it. At the bottom of the page, click **Release locks**.
- If you want to release the locks on all records, click **Release all locks**.

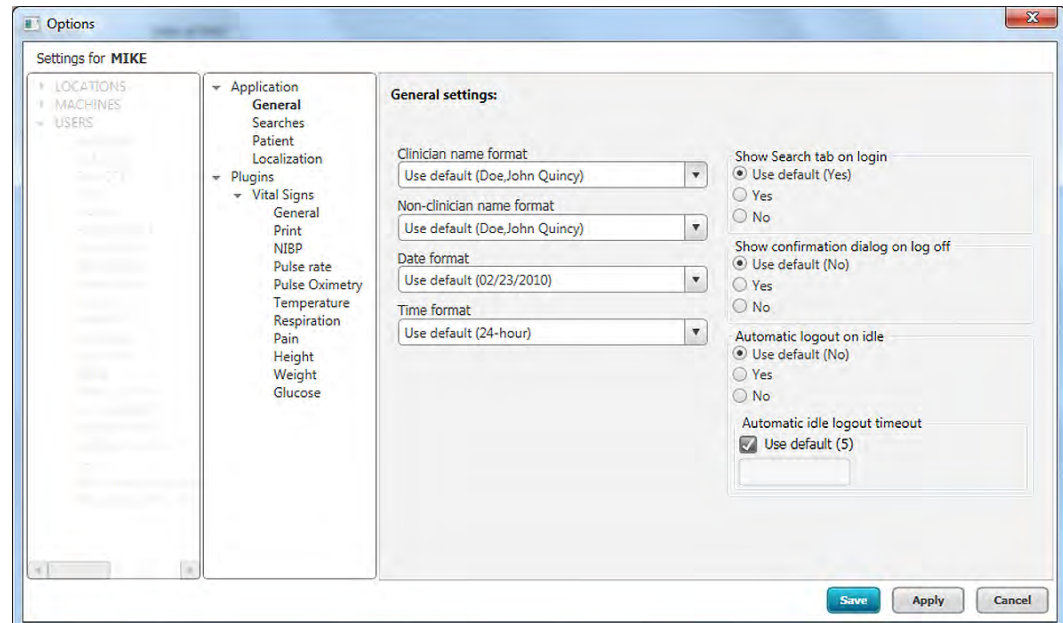
Program configuration

In **Tools > Options**, many aspects of the client application can be customized. Depending on the privileges assigned to them, users can customize settings for themselves or for others.

For users who are authorized to adjust their own settings only, the Options window has only one panel at the left side.



Users with additional privileges see an additional panel at the left side. This panel lists all locations, workstations ("machines"), and users in the Connex VM system. Click each item—**LOCATIONS**, **MACHINES**, **USERS**, and the items in those lists—to access the corresponding settings.



LOCATIONS

LOCATIONS specifies vital signs alert limits. You can set the same limits for all locations or customize limits for each location.

Item	Affects...	Hierarchy
LOCATIONS	All locations	
A location in the LOCATIONS list	That location only	These settings override those in LOCATIONS . If Use default value is selected, the value from LOCATIONS takes effect.

Set the same alert limits for all locations



WARNING If you adjust vital signs alert limits, verify the limits before you save them. Vital signs values appear as alerts in the Connex VM system only if they fall outside of the set limits.

- In the menu bar, click **Tools > Options**.
The Options window appears.
- Change the alert limits at the **LOCATIONS** level:
 - In the left pane, click the word **LOCATIONS**. The word changes to bold.
 - In the middle pane, expand the **Plugins > Vital Signs** list.
 - Click the parameter for which you want to change the limits. The limits for that parameter appear in the right pane.
 - In the right pane, click **Edit**.

- e. Clear the **Use default value** check box.
 - f. Make the desired changes.
 - g. Repeat steps c through f as much as desired.
 - h. Click **Apply**.
3. For each location, ensure that the **Use default value** check box is selected for each parameter:
 - a. In the left pane, expand the **LOCATIONS** list.
 - b. Click the first location.
 - c. In the middle pane, click each parameter and ensure in the right pane that the **Use default value** check box is selected. If not, click **Edit** and select the box.
 - d. Repeat steps b and c for each location.
4. Click **Save** or **Close**.

Customize alert limits for a location



WARNING If you adjust vital signs alert limits, verify the limits before you save them. Vital signs values appear as alerts in the Connex VM system only if they fall outside of the set limits.

1. In the menu bar, click **Tools > Options**.
The Options window appears.
2. In the left pane, expand the **LOCATIONS** list.
3. Click the location name.
The name changes to bold.
4. In the middle pane, expand the **Plugins > Vital Signs** list.
5. Click the parameter for which you want to change the limits.
The limits for that parameter appear in the right pane.
6. In the right pane, click **Edit**.
7. Clear the **Use default value** check box.
8. Make the desired changes.
9. Repeat steps 5 through 8 as much as desired.
10. Click **Save**.

MACHINES and USERS

MACHINES and **USERS** contain settings that affect what appears on the screen and in printouts. Clicking **MACHINES**, **USERS**, or any item in those lists reveals the same settings.

When a user logs on to the client application, the application determines which settings take effect based on this hierarchy:

- If a value is set for the user, that value is used. If **Use default** is selected, then...
- The value is inherited from the workstation that the user is logged on to. If **Use default** is selected at this level, then...
- The value is inherited from the **USERS** node. If **Use default** is selected at this level, then...
- The value is inherited from the **MACHINES** node.

By default, administrators can change values at all levels in the hierarchy. Users (non-administrators) can change their own values. Users can also add new modifier values that everyone can select from the Capture Vitals Signs window. These modifiers cannot be mapped to the HIS and, as a result, will not appear in outbound HL7 messages.

Note It is strongly recommended that you disable users' ability to make changes. In the Roles and Privileges window, clear the **Change own setting** and **Change group setting** check boxes for the User, Doctor, and Manager roles.

Program settings

The following provides descriptions of settings available in **MACHINES** and **USERS**.

This list is not comprehensive. Only those settings that require description are listed; others are self-explanatory.

Note Changes to modifier labels (for example, "Cuff size") and values (for example, "Large") must be made to the **MACHINES** level in the settings hierarchy to allow for system-wide mapping of those values to the HIS. If modifiers are not mapped, they will not appear in outbound HL7 messages.

Before changing a vital signs modifier, you must first clear its **Use default** check box. If you want to create modifiers in multiple languages without having to change the language for the whole program, use the **Settings locale** list, located in the upper-right corner of each vital signs settings window. Modifier labels and values can have a maximum of 30 characters.

Any time you change modifier labels or values at the **MACHINES** level, log on to each workstation as ADMIN and verify that the changes appear in the Capture Vital Signs window.

The Enterprise gateway configuration wizard lists the labels and values supplied to the HIS and enables you to define additional settings.

Tools > Options > Application > General

Setting	Description
Show Search tab on login	<ul style="list-style-type: none"> Yes: The Search tab is present by default. No: The Search tab is absent by default. The user can open it from the menu bar: View > Search.
Show confirmation dialog on log off	<ul style="list-style-type: none"> Yes: A confirmation prompt appears when the user logs off. No: No confirmation prompt appears when the user logs off.
Automatic logout on idle	<ul style="list-style-type: none"> Yes: Whenever the program has been unused for the designated idle period, it logs the user off. In single sign-on configurations, which require that users log on only to the operating system, the program closes instead. No: The program does not log users off or close automatically.
Automatic idle logout timeout	The number of minutes in the idle period.

Tools > Options > Application > Searches

Setting	Description
Standard searches (for example, My locations)	<ul style="list-style-type: none"> • Available searches: The standard (built-in) searches that appear in the Show list on the Home page. • Search options: The settings for the standard searches. To view or change these settings, you must select the search name. Before you can make changes to My locations, you must clear the Use default locations check box.
Saved searches	The saved searches that appear in the Show list on the Home page.

Tools > Options > Application > Patient

Setting	Description
Default patient action	<p>The action that occurs after the user double-clicks a patient name.</p> <ul style="list-style-type: none"> • View selected patient record • Acquire vitals • Do nothing
Show patient location	<ul style="list-style-type: none"> • Yes: Patient locations are displayed at the top of the Capture Vital Signs window and at the top of the patient record. • No: Patient locations are not displayed.

Tools > Options > Application > Localization

Setting	Description
Languages available	<p>This option sets the language used by the Connex VM program. The first item in the list attempts to match the Connex VM language to the language selected in Windows. If not available, English is chosen. The remaining items in the list specify a language directly.</p> <p>Note After changing the language, log off and back on to make the setting take full effect.</p>

Tools > Options > Plugins > Vital Signs > General

Setting	Description
Available measurements	The measurements (NIBP, pulse rate, etc.) that appear when the user is capturing vital signs or viewing patient records.
Display modifiers	<ul style="list-style-type: none"> • Yes: If any modifiers (site, method, position, etc.) were entered during a vital signs capture, they appear in the patient record. • No: Modifiers remain in the database but do not appear in the patient record.

Setting	Description
Patient history ordering	The order in which patient information is listed. <ul style="list-style-type: none"> • Newest to oldest • Oldest to newest
Missing clinician action	The action that occurs if the clinician ID is unspecified when vital signs readings are saved. <ul style="list-style-type: none"> • Leave empty • Use current user

Tools > Options > Plugins > Vital Signs > Print

Setting	Description
Print after test taken	<ul style="list-style-type: none"> • Yes: Results are automatically printed whenever a test is taken. • No: No automatic printouts occur when a test is taken.
Print after test saved/updated	<ul style="list-style-type: none"> • Yes: Results are automatically printed whenever a test is saved or updated (edited and resaved). • No: No automatic printouts occur when a test is saved or updated.
Reports to print after test taken	The types of reports that print after tests are taken. <ul style="list-style-type: none"> • PatientSummary: Numerical data in a table. • PatientSummaryGraphical: Data plotted on a graph.
Reports to print after test saved/updated	The types of reports that print after tests are saved or updated (edited and resaved).

Tools > Options > Plugins > Vital Signs > NIBP

Setting	Description
NIBP unit	The unit of measure.
NIBP Modifiers	<ul style="list-style-type: none"> • Location modifier: The anatomical site where the measurement was taken. • Position modifier: The patient's position when the measurement was taken. • Cuff size modifier: The size of the cuff.
Show MAP	<ul style="list-style-type: none"> • Yes: Mean arterial pressure (MAP) is displayed. • No: MAP is not displayed.

Tools > Options > Plugins > Vital Signs > Pulse rate

Setting	Description
Pulse rate	<ul style="list-style-type: none">• Site modifier: The anatomical site where the measurement was taken.• Method modifier: The method by which the measurement was taken.• Position modifier: The patient's position when the measurement was taken.

Tools > Options > Plugins > Vital Signs > Pulse Oximetry

Setting	Description
Pulse Oximetry	<ul style="list-style-type: none">• Method modifier: The method by which the measurement was taken.• Location modifier: The anatomical site where the measurement was taken.

Tools > Options > Plugins > Vital Signs > Temperature

Setting	Description
Temperature unit	The unit of measure. If you choose Celsius with conversion or Fahrenheit with conversion , the temperature appears in both units during the capture of vital signs.
Location modifier	The anatomical site where the measurement was taken.

Tools > Options > Plugins > Vital Signs > Respiration

Setting	Description
Respiration	<ul style="list-style-type: none">• Method modifier: The method by which the measurement was taken.• Position modifier: The patient's position when the measurement was taken.

Tools > Options > Plugins > Vital Signs > Pain

Setting	Description
Pain	Method modifier: The method by which the rating was taken.

Tools > Options > Plugins > Vital Signs > Height

Setting	Description
Height unit	The unit of measure.
Quality modifier	The quality of the measurement.

Tools > Options > Plugins > Vital Signs > Weight

Setting	Description
Weight unit	The unit of measure.
Show BMI	<ul style="list-style-type: none">• Yes: The body mass index is displayed.• No: The body mass index is not displayed.
Quality modifier	The quality of the measurement.
Method modifier	The method by which the measurement was taken.

Tools > Options > Plugins > Vital Signs > Glucose

Setting	Description
Glucose unit	The unit of measure.

User management

Connex VM roles and privileges

Roles and associated privileges grant users permission to perform designated tasks in the system. During installation, default roles are created. In **Administration > Roles and privileges**, you can view and modify these roles, create new roles, and delete roles to suit your facility's needs. You can then assign roles to users when you create user accounts.

Default roles and associated privileges

The table compares the default roles created during installation.

Note It is strongly recommended that you deselect **Change own setting** and **Change group setting** for the User, Manager, and Doctor roles. Otherwise, users could, for example, add modifier values that everyone could use, and those modifiers would not appear in vital signs readings sent to the HIS.

Privilege	Manager	User	Admin	Doctor
Change any setting			X	
Change group setting	X		X	
Manage configurations			X	
Manage roles			X	
Manage users			X	
Cancel any edit			X	
Change own setting	X	X	X	X
Change password	X	X	X	X
Manage custom searches	X		X	
Create patient	X	X	X	X

Privilege	Manager	User	Admin	Doctor
Delete patient			X	
Edit any patient	X		X	X
Edit assigned patient	X	X	X	X
Edit personal info	X	X	X	X
View any patient	X	X	X	X
View assigned patient	X		X	X
Assign patients	X	X	X	X
Create test	X	X	X	X
Edit any test	X		X	X

Create a new role

1. In the menu bar, click **Administration > Roles and privileges**.
The Roles and Privileges window appears.
2. In the lower part of the left pane, click **Create new role**.
3. In the **Privileges** pane, type the new role name in the **New Role** box.
4. Select check boxes next to privileges that you want to associate with the role.
5. Click **Save**.

Modify a role

1. In the menu bar, click **Administration > Roles and privileges**.
The Roles and Privileges window appears.
2. In the left pane, click a role.
3. Click **Edit**.
4. In the **Privileges** pane, select or clear privilege check boxes.
5. Click **Save**.

Copy a role

You can create a new role with similar privileges or the same privileges as an existing role.

1. In the menu bar, click **Administration > Roles and privileges**.
The Roles and Privileges window appears.
2. Next to the role you are copying, click ▼ and select **Copy**.
3. In the **Privileges** pane, type the new role name in the **Copy Of (role name)** box.
4. (Optional) Select and clear check boxes next to privilege names.

5. Click **Save**.

Delete a role

1. In the menu bar, click **Administration > Roles and privileges**.
The Roles and Privileges window appears.
2. Next to the role, click ▼ and select **Delete**.

Privileges

The following tables describe the privileges in the Roles and Privileges window. To open this window, click **Administration > Roles and privileges**.

Some privileges are part of a hierarchical family that represents levels of authorization for a particular task. When one of these privileges is selected for a role, it supersedes any lower-level privileges that are also selected.

Administration

Privilege	Superseded privileges	Description
Change any setting*	Change group setting Change own setting	If selected, the user can view and edit the settings of any configurable element in Tools > Options .
Change group setting*	Change own setting	If selected, the user can view and edit the settings of his user account and immediate parent group in Tools > Options .
Manage configurations*		If selected, the user can view and edit the settings of any configurable element in the app-machine tree.
Manage roles*		If selected, the user can view and make changes to roles in Administration > Roles and privileges .
Manage users*		If selected, the user has access to the flyout menu items in search results in Search > Users .
Cancel any edit*		If selected, the user can release locks on the Release Locks page.

Users

Privilege	Superseded privileges	Description
Change own setting*		If selected, the user can view and edit the settings of his user account in Tools > Options .

Privilege	Superseded privileges	Description
		If not selected, the user can view the settings of his user account in Tools > Options but cannot edit them.
Change password		If selected, the user can change his password.
Manage custom searches		If selected, the user can create and edit saved searches.

Patient records

Privilege	Superseded privileges	Description
Create patient		If selected, the user can create a new patient.
Delete patient		If selected, the user can delete patients.
Edit any patient	Edit assigned patient	If selected, the user can edit information in the Patient Summary window for any patient.
Edit assigned patient		If selected, the user can edit information in the Patient Summary window for only assigned patients.
Edit personal info		If selected, the user can edit his user account information. To enable this privilege, the Manage users privilege must also be selected.
View any patient		If selected, the user can view the patient details for any patient.
View assigned patient		If selected, the user can view the patient details for only assigned patients.
Assign patients		If selected, the Assign/Unassign button is enabled for patient search results.

Testing

Privilege	Superseded privileges	Description
Create test		If selected, the user can create tests, including vital signs readings.
Edit any test		If selected, the user can edit tests, including vital signs readings.

* It is strongly recommended that these privileges be made available for administrators only. Otherwise, users could, for example, add modifier values that everyone could use, and those modifiers would not appear in vital signs readings sent to the HIS.

User accounts

Create a user account and assign roles

1. In the menu bar, click **Administration > New user**.
The New User window appears.
2. Specify account details.
 - a. Enter ID information.
 - b. (Optional) Select the **Account is active** check box.
If you do not select this box, you can activate the account later.
 - c. (Optional) Select the **Change the password at next logon** check box.
The password is set, and the user can change it at the next logon.
 - d. Select the **Set password** check box, and then enter and confirm the password.
3. Type the user title and name in the **Clinician name** boxes.
4. Select a settings group.
5. Select check boxes next to one or more user roles.
6. Click **Save**.

Import users

You can create a batch of user accounts by importing user information from a comma delimited (.csv) file.

Note This task is for adding new users only. If you import a record for a user who already has an account, the existing record is not updated.

Prepare file for user import

To import new user accounts into the system, prepare a .csv file according to these guidelines.

1. Export user information from another source to a comma delimited (.csv) file.
2. Ensure that the first line in the file contains the header shown below.
 UserName,ClinicianNumber,FirstName,MiddleName,LastName,IsActive,
 PasswordChangeRequired,ManagerRole,UserRole,AdminRole,DoctorRole
3. Ensure that each subsequent line contains the information for one user. UserName is required, and one role must be set to true. Optional fields must be delimited even if they do not contain data. For example:
 SAM,XXXYYYYZZZ,John,Adam,Sam,true,true,true,,,
4. If any field contains leading zeros, enclose the data in double quotes. For example, if a user ID is 000345, it must appear as "000345" in the CSV file.
5. Save the file with a .csv extension.

Field name	Description	Possible value
UserName	Connex VM user name.	Alphanumeric characters up to 50 characters.
ClinicianNumber	User's clinician ID.	Alphanumeric characters up to 20 characters.
FirstName		Alphanumeric characters up to 20 characters.
MiddleName		Alphanumeric characters up to 20 characters.
LastName		Alphanumeric characters up to 30 characters.
IsActive	Indicates whether this user account is active.	True or false. No value, or any value other than true, is treated as false. If this field is set to false, the user cannot log on to the system.
PasswordChangeRequired	Indicates whether password change is required on next logon.	True or false. No value, or any value other than true, is treated as false.
ManagerRole UserRole AdminRole DoctorRole	Indicates the role assigned to the user. These four roles are created at installation. If you deleted one of these roles or created additional roles, see the note below.	True or false. No value, or any value other than true, is treated as false. You must assign the user at least one role.

Note If you created additional roles in the Roles and Privileges window, you can add fields to the file after DoctorRole. The field name should contain the role name plus the word "Role." For example, if you added a new role called "SuperAdmin," the field name should be "SuperAdminRole."

If you deleted a default role in the Roles and Privileges window, remove the field for the deleted role.

Import user account file

After you prepare a .csv file of user information, follow these steps to import the data into the system.

1. In the menu bar, click **Administration > Administrator tools**.
2. In the navigation bar on the left side of the screen, click **Import > Import users**.
3. Next to the **Select file** box, click **Browse**.
The Select File to Import window appears.
4. Browse to the comma delimited file that you created.
5. Double-click the file.

The file name appears in the **Select file** box.

6. Click **Import**.

The default password for a new user is WelchAllyn.

Modify a user account

1. Click the **Search** tab or go to **View > Search**.
2. Click **Users**.
3. Enter your search criteria.
4. Click **Search**.

A list appears.

5. Next to the user ID, click ▼ and select **Edit user details**.

The Modify User window appears.

6. Click **Edit**.
7. Modify information.
8. Click **Save**.

Inactivate or activate a user account

1. Click the **Search** tab or go to **View > Search**.
2. Click **Users**.
3. Enter your search criteria.
4. Click **Search**.

A list appears.

5. Next to the user ID, click ▼ and select **Edit user details**.

The Modify User window appears.

6. Click **Edit**.
7. Clear or select the **Account is active** check box.
8. Click **Save**.

Delete a user account

1. Click the **Search** tab or go to **View > Search**.
2. Click **Users**.
3. Enter your search criteria.
4. Click **Search**.

A list appears.

5. Next to the user ID, click ▼ and select **Delete**.

Location management

The **Location Management** page (available from the menu bar under **Administration > Administrator tools**) provides the ability to add locations, edit location names, and delete locations.

The location associated with a patient must be defined via **Location Management** for vital signs capture to work as expected. A location mismatch will affect patient result display. Excessive patient location mismatches might impact system operation. Because **Location Management** has a profound effect on proper functioning of the system, only Welch Allyn Technical Support personnel can make adjustments to locations.

Contact your Technical Support representative for more information.

Patient management

Create a new patient

In many configurations, patient records are automatically kept in-sync with the hospital information system. In those configurations, it is generally not necessary or even desirable to enter patient information manually. If the configuration at your facility allows it, you can create a patient by following these steps.

1. Select **File > New Patient**.
2. Enter patient information.
3. Click **Save**.

Import patients

You can create a batch of patient records by importing patient information from a comma delimited (.csv) file.

Note This task is for adding new patients only. If you import a record for a patient that already exists in the system, the existing record is not updated.

Prepare file for patient import

To import new patient records into the system, prepare a .csv file according to these guidelines.

1. Export patient information from another source to a comma delimited (.csv) file.
2. Ensure that the first line in the file contains the header shown below.

FirstName,LastName,MiddleName,MRN,Prefix,Suffix,DOB,AdmissionStatus,AdmitDateTime, Building,Floor,Room,Bed,Facility,Unit,Gender,AdmitStatus,StreetAddress,StateProvince, PostalCode,OtherDesignation,County,Country,City,Value,AreaCode,CountryCode, Extension,LocalNumber,Race

3. Ensure that each subsequent line contains information for one patient record. FirstName, LastName, MRN, and DOB are required. Optional fields must be delimited even if they do not contain data.

Example of a patient record with all fields filled in:

Mike,Smith,Alan,XXXXYZZZZ,Mr,Jr,1/13/1980,yes,10/10/2009,Building 1,Floor 1,1,77,Facility 1,Unit 1,2,2,4341 State Street Road,NY,13153,PO Box,Onondaga,USA,Skaneateles Falls,mike.email@welchallyn.com,800,1,11,8002892501,2

Example of a patient record with some optional fields left blank:

Mike,Smith,Alan,XXXXYZZZZ,,1/13/1980,yes,10/10/2009,Building 1,Floor 1,1,77,Facility 1,Unit 1,2,2,4341 State Street Road,NY,13153,PO Box,Onondaga,USA,Skaneateles Falls,,,,,8002892501,2

4. Save the file with a .csv extension.

Field name	Description	Possible value
FirstName*		Alphanumeric characters up to 20 characters.
LastName*		Alphanumeric characters up to 30 characters.
MiddleName		Alphanumeric characters up to 20 characters.
MRN*	Medical record number.	Alphanumeric characters up to 20 characters.
Prefix	Title, such as Mr., Mrs., and Miss.	Alphanumeric characters up to 5 characters.
Suffix	Generational suffix, such as Jr. and Sr.	Alphanumeric characters up to 5 characters.
DOB*	Date of birth.	A date in Windows short date format.
AdmissionStatus	Indicates whether a visit needs to be created.	Yes or no. If the value is yes, the file must also include AdmitDateTime, Floor, Room, Bed, Facility, Unit, and AdmitStatus.
AdmitDateTime	Date on which the patient was admitted to the location for this visit.	A date in Windows short date format.
Building		Alphanumeric characters up to 20 characters.
Floor		Alphanumeric characters up to 20 characters.
Room		Alphanumeric characters up to 20 characters.
Bed		Alphanumeric characters up to 20 characters.
Facility		Alphanumeric characters up to 20 characters.
Unit		Alphanumeric characters up to 20 characters.
Gender		The following numbers can be used: <ul style="list-style-type: none"> • 0 = Unknown • 1 = Female • 2 = Male

Field name	Description	Possible value
		<ul style="list-style-type: none"> • 3 = Other • 4 = Ambiguous • 5 = Irrelevant
AdmitStatus	Defines the stage of the patient's admittance to a location.	<p>The following numbers can be used:</p> <ul style="list-style-type: none"> • 0 = Unknown • 1 = Preadmitted • 2 = Admitted • 3 = Discharged
StreetAddress		Alphanumeric characters up to 200 characters.
StateProvince		Alphanumeric characters up to 30 characters.
PostalCode		Alphanumeric characters up to 15 characters.
OtherDesignation	Additional information about an address such as a post office box or an apartment number.	Alphanumeric characters up to 50 characters.
County		Alphanumeric characters up to 50 characters.
Country		Alphanumeric characters up to 50 characters.
City		Alphanumeric characters up to 30 characters.
Value	Email address.	Alphanumeric characters up to 100 characters.
AreaCode	Telephone area code.	Alphanumeric characters up to 5 characters.
CountryCode	Telephone country code	Alphanumeric characters up to 5 characters.
Extension	Telephone extension number.	Alphanumeric characters up to 5 characters.
LocalNumber	Local telephone number.	Alphanumeric characters up to 20 characters.
Race		<p>The following numbers can be used:</p> <ul style="list-style-type: none"> • 0 = Unknown • 1 = Other • 2 = White • 3 = Black or African American • 4 = American Indian or Alaska Native

Field name	Description	Possible value
		<ul style="list-style-type: none"> 5 = Asian 6 = Native Hawaiian and/or Pacific Islander

* Required field.

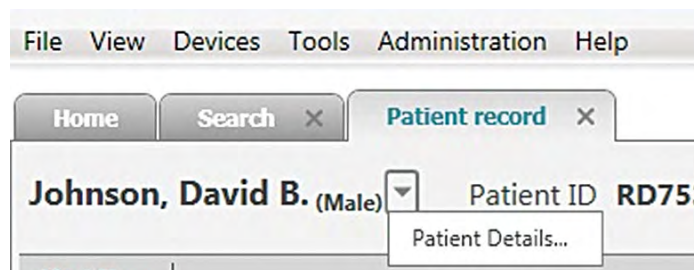
Import patient record file

After you prepare a .csv file of patient information, follow these steps to import the data into the system.

1. In the menu bar, click **Administration > Administrator tools**.
2. In the navigation bar on the left side of the screen, click **Import > Import patients**.
3. Next to the **Select file** box, click **Browse**.
The Select File to Import window appears.
4. Browse to the comma delimited file that you created.
5. Double-click the file.
The file name appears in the **Select file** box.
6. Click **Import**.

View or edit a patient record

1. Locate the correct patient name in the list on your **Home** page.
2. Next to the patient name, click ▼ and click **View patient record**.
The **Patient record** page appears.



3. Next to the patient's name, click ▼ and then click **Patient details**.
The Patient Summary window appears.
4. (Optional) Click **Edit**. Add, change, or remove patient information.

Delete a patient

When you delete a patient, the patient record moves to the recycle bin. The deleted record cannot be viewed, updated, or restored.

1. On the **Home** page or **Search** page, click ▼ next to the patient name.
2. Select **Delete Patient**.

Configuration

Adjust server configuration settings

In **Administrator tools**, the **Server configuration** page enables you to configure settings, such as password policy, patient matching, patient IDs, authentication, auditing, search results, location format, and concurrency lock timeout.

1. In the menu bar, click **Administration > Administrator tools**.
2. In the navigation bar on the left side of the page, click **Configuration Setting > Server configuration**.
3. In the list, find the setting that you want to change.
4. Next to the setting name, click ▼ and select **Edit**.
5. At the bottom of the page, make the desired changes.
6. Click **Save**.

Server configuration settings

This topic describes the settings on the **Server configuration** page. To find this page, click **Administration > Administrator tools > Configuration Setting > Server configuration**.

Setting name	Description	Default value
CONNEXWORKSTATION.APP.SEARCHMAXRESULTS	Maximum number of search results returned on the Home page (and any Search page when paging is disabled).	1000
CONNEXWORKSTATION.APP.SEARCHRESULT PAGESIZE	Number of results displayed per page in paging search results (only applies when paging is enabled).	20
CONNEXWORKSTATION.APP.SEARCHRESULT PAGINGENABLED	TRUE: Paging is enabled for Search pages. (Home page is always non-paging.) FALSE: Paging is disabled for Search pages.	TRUE



Setting name	Description	Default value
CONNEXWORKSTATION. PATIENTMANAGEMENT. LOCATIONFORMAT	<p>Format used for patient locations.</p> <p>The following identifiers can be used:</p> <ul style="list-style-type: none"> {u} = Unit {r} = Room {b} = Bed <p>Examples:</p> <p>Given the following data:</p> <ul style="list-style-type: none"> Unit: Ward A Room: 302 Bed: B <p>{r}{b} = 302B</p> <p>{u}, {r}{b} = Ward A, 302B</p> <p>{u} - {r} - {b} = Ward A - 302 - B</p> <p>{u}, Room {r}{b} = Ward A, Room 302B</p>	{r}{b}
PASSWORDPOLICY. DEFAULTPASSWORD	Default password that users get when their accounts are created.	WelchAllyn
PASSWORDPOLICY. ENABLED	<p>TRUE: Password policy settings (PASSWORDPOLICY.*) are enabled.</p> <p>FALSE: Password policy settings (PASSWORDPOLICY.*) are disabled.</p>	FALSE
PASSWORDPOLICY. EXPIRATIONINDAYS	Number of days before users are required to change their password.	90
PASSWORDPOLICY. VALIDATIONRULE	<p>Requires a regular expression to enforce password requirements:</p> <ul style="list-style-type: none"> Minimum number of total characters Minimum number of lowercase characters Minimum number of uppercase characters Minimum number of numeric characters Minimum number of special characters (not alphanumeric) 	<p>The default expression defines these requirements:</p> <ul style="list-style-type: none"> Minimum number of total characters: 8 Minimum number of lowercase characters: 1 Minimum number of uppercase characters: 1 Minimum number of numeric characters: 1 Minimum number of special characters: 1 <pre><?xml version="1.0" encoding="utf-8" ? ><PasswordPolicy><PolicyItem Key="EightCharReq" Regex="(?.{8,})" / ><PolicyItem Key="OneLowerReq" Regex="(?.*[a-z])" / ><PolicyItem</pre>

Setting name	Description	Default value
		Key="OneUpperReq" Regex="{?=[A-Z]}" / ><PolicyItem Key="OneNumericReq" Regex="{?=[0-9]}" / ><PolicyItem Key="OneSpecialReq" Regex="{?=[!@#\$%^&*~`~\W]}" /></ PasswordPolicy> If you would like this setting changed, call Welch Allyn Technical Support.
PASSWORDPOLICY.WARNINGINDAYS	Specifies when users will be notified that their passwords will expire soon. This value is the number of days before the password expires.	15
PATIENTMATCHINGRULE	Attributes used to help prevent duplicate entry of patient information when patient information is obtained from an external or untrusted data source (e.g., ADT, device, or imported file). Possible values: <ul style="list-style-type: none"> 1 = MRN only 2 = MRN, DOB, Gender 3 = MRN, DOB, Gender, LastName 	1
PATIENTOPENVISIT.TIMELAPSEINMINUTES	Length of time (in minutes) that the server will look in the past to find a closed visit to associate a test to, if no open visit exists.	1440
PVIDFIELD	Reflects the patient ID used for barcode wristbands or manually entered into a vital signs device. The Connex VM system displays the patient ID in the client application and uses it to match imported vital signs readings to patient records in the database. Options: <ul style="list-style-type: none"> Patient.MRN: The patient's medical record number. Patient.GovernmentNumber: The patient's government-assigned number (for example, Social Security number in the US). Visit.AccountNumber: The patient's account number. Visit.VisitNumber: The number assigned to the patient for a particular visit. 	Patient.MRN

Setting name	Description	Default value
SERIALNUMBER	Serial number of Connex VM. For Welch Allyn use only. Do not modify.	Seven-digit alphanumeric.
SINGLESIGNON.DEFAULTSECURITYROLE	If single sign-on is enabled, this setting specifies which user role and privileges a user gets when he logs on to the system for the first time using Active Directory credentials. This setting requires a RoleId value from the Connex VM database.	The default value indicates the doctor role: 7DD3994E-7F0E-4A64-B79D-FF66C51495BD. If you would like this setting changed, call Welch Allyn Technical Support.
SINGLESIGNON.ENABLED	TRUE: Single sign-on is enabled. FALSE: Standard sign-on is enabled.	FALSE
SYSTEMAUDIT.ENABLED	TRUE: Auditing is enabled. FALSE: Auditing is disabled.	TRUE
TIMEOUTS.LOCKSINMINUTES	Length of time (in minutes) that a concurrency lock lasts.	20
CONNEXWORKSTATION.MYLIST.STANDARD SEARCHES	For Welch Allyn use only. Do not modify.	<?xml version="1.0" encoding="utf-8"?><Searches><Search Guid="4a286f91-31f9-4a6c-ab30-70a00ba930a0" /></Searches>

Configure settings for Welch Allyn services

From the **Server setting** page, you can change the connection information and settings for Welch Allyn services running on the local machine. For changes to take effect, you must restart the service from the Microsoft Management Console snap-in for Services.

- From the machine that you want to configure, open **Admin Tools** using one of these methods:
 - From the Windows taskbar, click **Start > All Programs > Welch Allyn > Connex > Welch Allyn Connex Admin Tools**.
 - From the client application, click **Administration > Administrator tools**.
- In the navigation bar on the left side of the page, click **Configuration Setting > Server setting**.
- On the right side of the page, click  next to the desired service.
The settings page for that service appears.
- In the **Configuration Settings** list, find the property that you want to change.
- Next to the property name, click  and select **Edit**.
- At the bottom of the page, make the desired changes.
- Click **Save**.

Server settings

The **Server setting** page displays the Welch Allyn services running on the local machine. You can access this page from the Windows taskbar (**Start > All Programs > Welch Allyn > Connex > Welch Allyn Connex Admin Tools > Configuration Setting > Server setting**) or through the client application when available (**Administration > Administrator tools > Configuration Setting > Server setting**).

DCS

Use this section to specify the connection information for Welch Allyn Device Connectivity Service.

Property name	Description and default value
HostAddress	IP address of the server.
PortNumber	Port used with the above host address to establish the connection. For standard installations, the default value is 8732.
WorkstationMode	Only available on a kiosk. Defines whether the client application can be used to import and capture data from vital signs devices. Possible values are <code>true</code> or <code>false</code> . True: The client application can be used to import and capture data from vital signs devices. Devices cannot push data to the machine. False: The client application cannot be used to import and capture data from vital signs devices. Rather, devices can push data to the machine. False is the default for a kiosk.

Enterprise Gateway

Use this section to specify the connection information for Enterprise Gateway Service.

Property name	Description and default value
HostAddress	IP address of the server.
PortNumber	Port used with the above host address to establish the connection. For standard installations, the default value is 8732.

Services

Use this section to specify the connection information for Welch Allyn Hosting Service.

Property name	Description and default value
HostAddress	IP address of the server.

Property name	Description and default value
PortNumber	Port used with the above host address to establish the connection. For standard installations, the default value is 8732.
DataBase Name	Name of the SQL database that houses the Connex VM data. The default name is WADB.
DataBase Location	Name of the SQL instance used during installation. If you are using the default database that was provided during Connex VM installation, and you selected the defaults during installation, the default name is .\sqlexpress. Otherwise, contact your database administrator for this information.

License Admin

Use this section to specify the connection information for the Connex License service.

Property name	Description and default value
HostAddress	IP address of the server.
PortNumber	Port used with the above host address to establish the connection. For standard installations, the default value is 8732.

Admin Tools

Use this section to specify the connection information for Welch Allyn Connex Admin Tools.

Property name	Description and default values
HostAddress	IP address of the server.
Enable Cache	Defines whether the client application can be used while it is disconnected from the server. Possible values are <code>true</code> or <code>false</code> . True: When the workstation is not connected to the server, users can import and enter data into the application, which saves the data to its local file system. When the server is available again, the data will be uploaded to the server. False: The application cannot operate until access to the server is restored.
PortNumber	Port used with the above host address to establish the connection. For standard installations, the default value is 8732.

Workstation

Use this section to specify the connection information for the local Welch Allyn Connex Workstation. The parameters affect only the machine that you are viewing this information from.

Property name	Description and default values
HostAddress	IP address of the server.
Enable Cache	<p>Defines whether the client application can be used while it is disconnected from the server. Possible values are <code>true</code> or <code>false</code>.</p> <p>True: When the workstation is not connected to the server, users can import and enter data into the application, which saves the data to its local file system. When the server is available again, the data will be uploaded to the server.</p> <p>False: The application cannot operate until access to the server is restored.</p>
PortNumber	<p>Port used with the above host address to establish the connection.</p> <p>For standard installations, the default value is 8732.</p>
AllowMultipleInstances	<p>Defines whether multiple instances of the client application can be launched. Possible values are <code>true</code> or <code>false</code>.</p> <p>This setting should only be set to <code>true</code> on a system hosting a virtual desktop environment such as Citrix XenApp or Microsoft Remote Desktop Services.</p> <p>True: Multiple instances of the client application can be launched. This enables multiple thin clients to simultaneously access the application over the network.</p> <p>False: Multiple instances of the client application cannot be launched.</p>

Configure Enterprise Gateway Service

The **EGS Configuration** page enables you to change the settings that control the handling of HL7 messages into and out of the system.

1. In the menu bar, click **Administration > Administrator tools**.
2. In the navigation bar on the left side of the page, click **EGS > EGS Configuration**.

The **Enterprise gateway configuration wizard** appears.

3. Make the desired changes on each screen. Click **Next** to move from screen to screen.
4. After you have made all changes, click **Finish** on the final screen.

A message window appears, which indicates that the EGConfiguration file and Measurement Conversion XSLT were generated successfully in the EGS installation folder. The default installation folder is C:\Program Files\Welch Allyn\ConnexVM\EGS.

EGS configuration settings

This topic describes the options on the **EGS Configuration** page. To find this page, click **Administration > Administrator tools > EGS > EGS Configuration**.

EGS screen 1: Select supported transactions

Use this screen to select the message types that can flow between the server and the hospital information system (HIS).

Item	Description
Patient inbound transactions	If this is selected, EGS will process inbound HL7 ADT messages sent from the HIS to the Connex VM server.
Vitals outbound transactions	If this is selected, EGS will generate HL7 ORU messages from vital signs readings in the Connex VM server.

EGS screen 2: Configuration for vitals - HL7 generation

Use this screen to control what information is included in the HL7 ORU messages sent from the server.

Available exclusions

The **Available exclusions** list contains test and patient fields that can be excluded from outbound ORU messages. To exclude an item from outbound messages, click the item and then click the arrow button to move the item to the **Selected exclusions** list. Items in the **Selected exclusions** list will not be included in the Test XML that is generated using the test data from the database.

Item	Description
Test.CreatedBy	Name of the person who created the test for the patient.
Test.LastModifiedBy	Name of the person who last modified the test.
Test.TakenBy	Name of the person who took the test.
Test.ConfirmedBy	Name of the person who confirmed the test.
Patient.Medications	Medications taken by a patient.
Patient.Notes	Notes taken by the clinician for a particular patient.
Measurement.DeviceRef	The device that was used to record the measurements.
Patient.Pharmacies	Patient pharmacies.
BasicPerson.Identifiers	Identifiers for the person.
Test.TakenByDateTime	Date and time when the test was taken.

Rules

A number of rules control what information is sent from the server.

Item	Description
Send only confirmed vitals tests to HIS	For future use. Do not select this setting
Visit information required in the output HL7	If this is selected, every HL7 message generated through EGS will contain visit information. If the server does not have visit information for the patient, the HL7 message will contain dummy visit information.
Order information required in the output HL7	If this is selected, every HL7 message generated through EGS will contain the Common Order (ORC) and Observation Request (OBR) segments. If the server does not have this information, the HL7 message will contain dummy information.
Send unreconciled tests to HIS	If this is selected, HL7 messages will be sent for readings with unreconciled information (i.e., unknown clinician ID).
Send unreconciled patient tests to HIS	If this is selected, HL7 messages will be sent for readings with unreconciled patient information (i.e., unknown patient ID).

EGS screen 3: Configuring vitals measurement names between ConnexVM and HIS

Use this screen to configure and map measurement names, modifiers, and units used by the Connex VM server and the HIS.

Item	Description
Source name	Denotes the measurement names and modifiers used by the Connex VM server. Modifiers can be configured in the client application under Tools > Options > MACHINES > Plugins > Vital Signs .
Target name	Sets the measurement names and modifiers supplied in the ORU message sent to the HIS. Click a name to edit it.
Unit name	<p>Sets the unit of measure supplied in the ORU message.</p> <p>To select a unit, click the corresponding measurement name under Source name to enable the Unit name menu. Select the unit from the menu.</p>

EGS screen 4: Enterprise Integration Engine (EIE) Database Configuration

Use this screen to configure the parameters for the Enterprise Integration Engine (EIE) database.

Item	Description and default values
Database name	<p>Name of the SQL database that houses the EIE data.</p> <p>The default name is <code>WA_EIE_DB</code>.</p>
Database location	<p>Name of the SQL instance where the EIE database (<code>WA_EIE_DB</code>) resides.</p> <p>If you are using the default database that was provided during Connex VM installation, and you selected the defaults during installation, the default name is <code>.\SQLEXPRESS</code>. You can also use <code>machine_name\SQLEXPRESS</code> where <code>machine_name</code> is the name of the machine where the <code>WA_EIE_DB</code> resides.</p> <p>Otherwise, contact your database administrator for this information.</p>
User name	<p>Name of the user that has access to the SQL instance and will be used to create and access the EIE database.</p> <p>If you are using the default database that was provided during Connex VM installation, and you selected the defaults during installation, the default name is <code>eieapp</code>.</p> <p>Otherwise, contact your database administrator for this information.</p>
Password	<p>If you are using the default database that was provided during Connex VM installation, and you selected the defaults during installation, the default password is <code>eieapp</code>.</p> <p>Otherwise, contact your database administrator for this information.</p>

Maintenance

Disaster recovery

Back up server databases

Back up the Welch Allyn Connex VM database (WADB) and the Welch Allyn Enterprise Integration Engine database (WA_EIE_DB) on a regular basis by following your facility IT guidelines and policies for backing up patient data. Welch Allyn recommends a full backup to simplify data recovery.

You can automate this process by using a commercial database backup utility that can back up a live MS SQL database.

If your facility does not have a backup procedure, use Microsoft SQL Server Management Studio to back up the databases.

For more information, see "How to: Back Up a Database (SQL Server Management Studio)":

- For SQL Server 2008: <http://msdn2.microsoft.com/en-us/library/ms187510.aspx>
- For SQL Server 2005: [http://msdn.microsoft.com/en-us/library/ms187510\(SQL.90\).aspx](http://msdn.microsoft.com/en-us/library/ms187510(SQL.90).aspx)

Restore server databases

Follow your facility IT guidelines and policies to restore the Welch Allyn Connex VM database (WADB) and the Welch Allyn Enterprise Integration Engine database (WA_EIE_DB).

If your facility does not have a restore procedure and you use Microsoft SQL Server Management Studio (SSMS) to back up the databases, use SSMS to restore them. If you have a service agreement with Welch Allyn, call Technical Support before proceeding.

For more information, see "How to: Restore a Database Backup (SQL Server Management Studio)":

- For SQL Server 2008: <http://msdn2.microsoft.com/en-us/library/ms177429.aspx>
- For SQL Server 2005: [http://msdn.microsoft.com/en-us/library/ms177429\(SQL.90\).aspx](http://msdn.microsoft.com/en-us/library/ms177429(SQL.90).aspx)

Note Changes made to the database since the last backup are not restored.

HL7 connectivity

Corepoint Integration Engine

The Corepoint Integration Engine transfers inbound and outbound data between the Connex VM HL7 database and the HIS. Through the Corepoint Administration Console (Corepoint Integration Engine - Administration), you can monitor and manage connectivity and HL7 messages.

Note When the SQL Server that hosts the Connex VM and HL7 databases is offline or cannot be reached, stop the Corepoint Integration Engine service via the Corepoint Administration Console or the Microsoft Management Console snap-in for Services. For more information on stopping the Corepoint Integration Engine service, refer to the Corepoint Help file.

Corepoint user profiles

Corepoint provides two user profiles: View Only and Manager. For more information, refer to the Corepoint Help file.

Privileges

Privilege category	Privilege	View Only	Manager
General			
	Start & Stop Service		X
	View Engine Log	X	X
	Manage Licenses		X
	View & Export Configuration Objects		X
Connections			
	View Connection Status	X	X
	Start & Stop Connections		X
	View Alerts	X	X
	Resolve Alerts		X
	View Connection Logs	X	X
	View Messages	X	X
	Save Messages		X
	Resend Messages		X

Privilege category	Privilege	View Only	Manager
	Apply to All Connections	X	X
Operational Perspectives			
	Apply to All Operational Perspectives	X	X

User names and passwords

User names and passwords are case-sensitive.

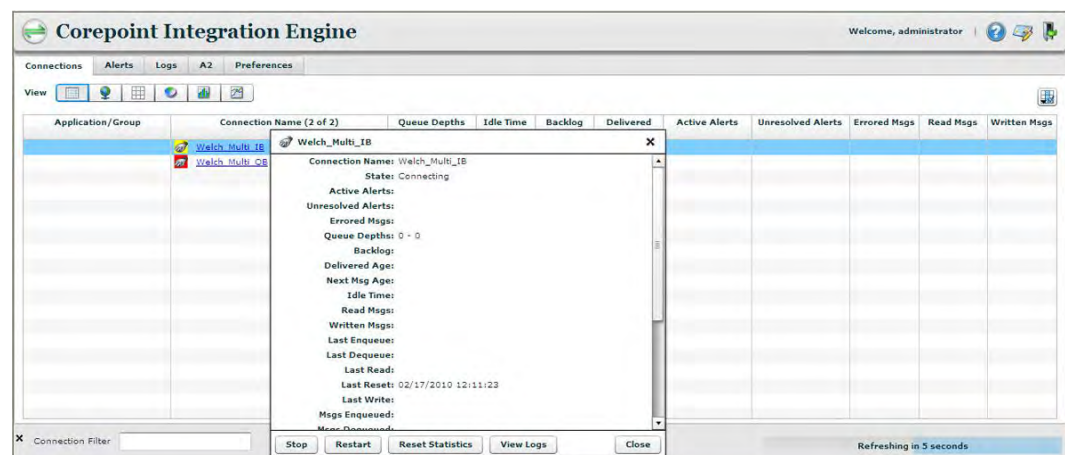
Profile	User name	Password
View Only	View	ViewOnly
Manager	Manager	ManageHL7

View HL7 messages

The Corepoint application provides information about each message sent between the server and an HL7 system. You can view all messages or apply filters to view only the desired messages. For more information, refer to the Corepoint Help file.

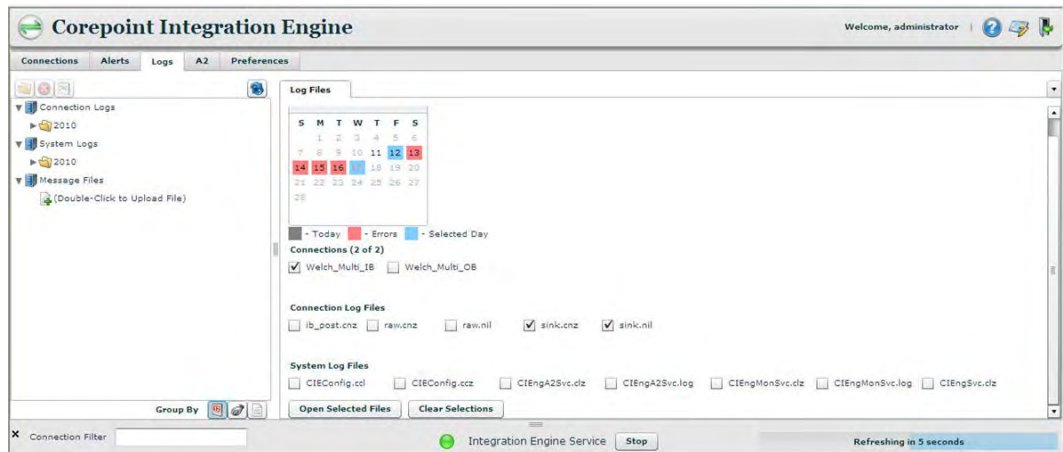
1. On the Windows taskbar, click **Start > All Programs > Corepoint Health > Corepoint Integration Engine > Corepoint Integration Engine - Administration**.
2. If prompted, log on.
3. Click the appropriate connection.

A window similar to the following appears.



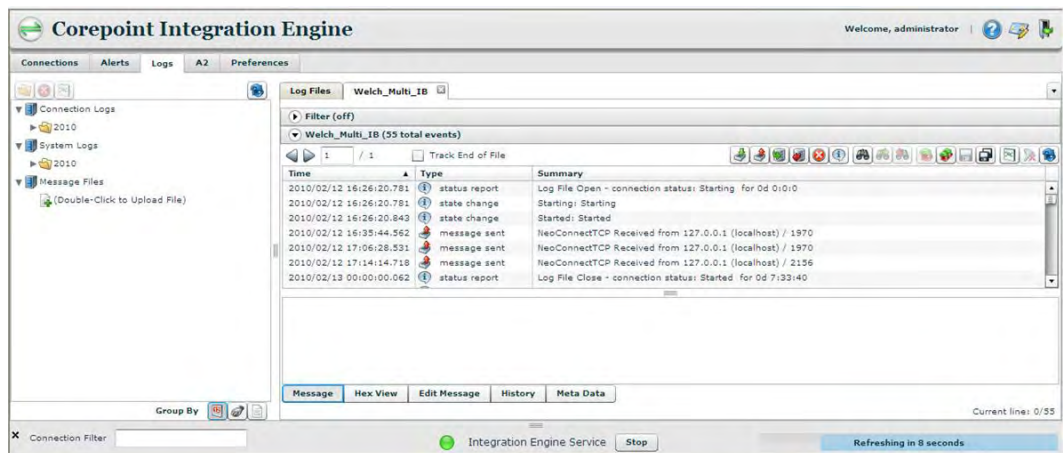
4. Click **View Logs**.

The **Log Files** page appears. For example:



5. On the **Log Files** page, define the parameters of the files you want to view. Select a date by clicking it on the calendar. If multiple dates are desired, click the dates while holding down the Ctrl key.
6. Click **Open Selected Files**.

A page similar to the following appears.

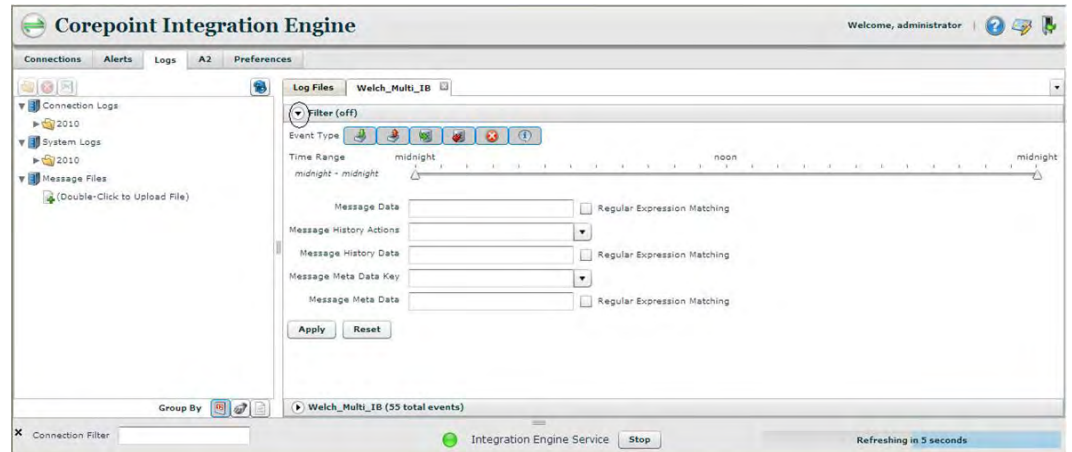


7. (Optional) Filter the messages as desired by using these features:

- Click the icons on the right side of the page.



- If you need more filter options, click the arrow next to **Filter** at the top of the page.

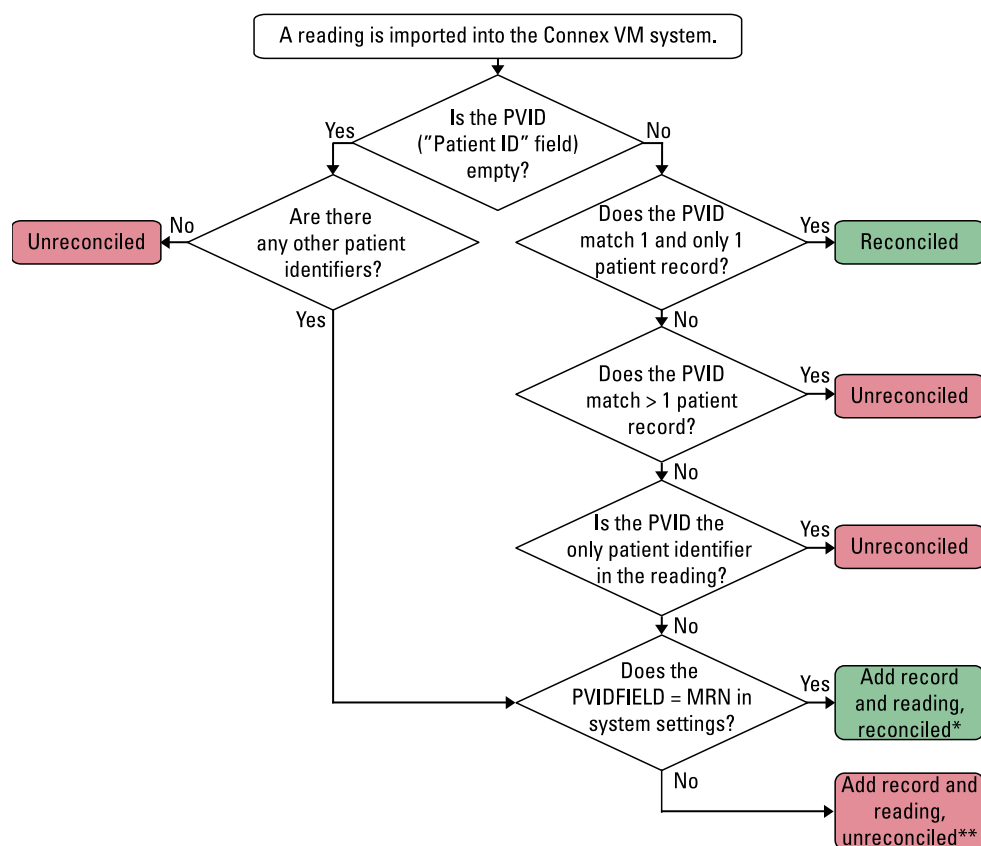


Reconciliation in the Connex VM system

When a reading is imported from a vital signs device, the Connex VM system attempts to match the reading to a patient record in the Connex VM database.

"Reconciled" means the system successfully matches the reading to a patient record in the database. The system adds the reading to the record and sends the reading to the HIS.

"Unreconciled" means the system cannot match the reading to a patient record. The system saves the reading as unreconciled data and does not send it to the HIS. The reading can be viewed or deleted from the Search page.

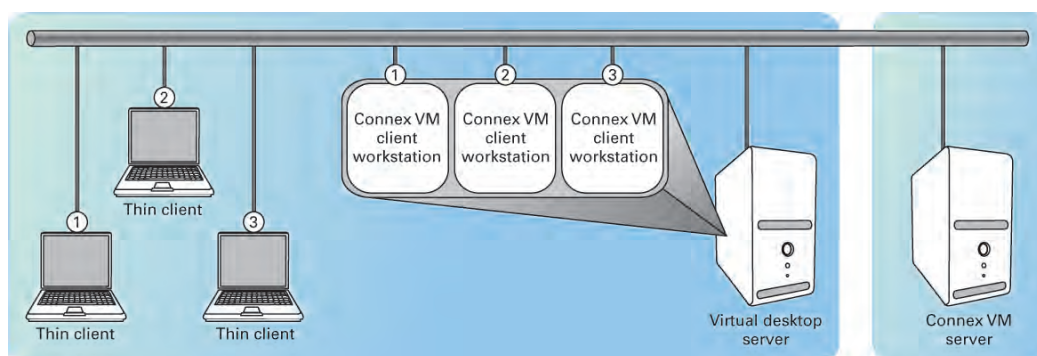


* The system creates a new patient record, saves the reading to the record, and sends the record to the HIS.

** The system creates a new patient record, but saves the record and the reading as unreconciled data. The record is unusable; it cannot be updated or sent to the HIS.

Virtual desktop environment

In a virtual desktop environment, the Connex VM client application is installed on a virtual desktop server and configured to support multiple, simultaneous client sessions. Companies that provide virtual desktop capabilities include Microsoft and Citrix.



Thin client setup

On each thin client, you must do one or both of the following to enable the client to capture and transfer data from vital signs devices.

- If you want to connect vital signs devices via serial cable, enable COM port forwarding through the virtual desktop application on the client (for example, Citrix or Microsoft Remote Desktop Connection).
- If you want to connect vital signs devices to the client via USB cable, install Welch Allyn Virtual Channel Client (VCC) on the client. VCC enables the virtual desktop server to see USB-connected devices.

For more information on enabling COM port forwarding through Citrix or Remote Desktop Connection, refer to documentation from Citrix or Microsoft.

For more information on VCC, visit welchallyn.com or contact your Welch Allyn sales representative.

Troubleshooting

Logs

View, print, and delete audit logs

An audit log is a record of activity in the system, including all events and user transactions.

1. In the menu bar, click **Administration > Administrator tools**.
2. In the navigation bar on the left side of the page, click **Logs > Audit log**.
3. Search the audit log by selecting search criteria from the drop-down lists. Multiple search criteria can be used to narrow down the search results.
4. Click **Search**.

Search results appear in the **Audit items list**.

5. (Optional) Print the list or delete audit items.
 - Print the list: Click the **Print** button.
 - Delete audit items: In the **Audit items** list, click items to select them. Click **Delete selected**.

Audit log search criteria

The following tables describe the search criteria drop-down lists on the **Audit log** page (available from the menu bar under **Administration > Administrator tools > Logs**).

Audit type

Option	Description
Add Update Delete Select	Shows records for the selected transaction for record data types of User, Patient, Location, Test, and Configuration parameters.
Print	Shows all Print transactions.
Login	Shows all Login transactions.

Option	Description
Logout	Shows all Logout transactions.
SetPassword	Shows all password changes to user accounts.
DeviceConnection	Shows all instances when a device was connected to a Connex VM workstation or kiosk.

Entity type

Option	Description
Clinician	Shows changes (add, update, etc.) related to clinicians.
Configuration	Shows changes to global system settings or workstation-specific changes.
Group	Shows changes to general settings for users, locations, and workstations.
Patient	Shows changes made to patient information.
SecurityRole	Shows changes made to roles.
Test	Shows changes related to measurement data.
Visit	Shows changes to visit information.
UserAccount	Shows changes related to user accounts.

View application logs

Application logs are primarily for Welch Allyn Technical Support.

1. In the menu bar, click **Administration > Administrator tools**.
2. In the navigation bar on the left side of the screen, click **Logs > Application logs**.
3. Under **Select folder**, select a folder from the drop-down list.
4. Click **Search**. Log files appear in the **Log file list**.
5. In the list, find the file that you want to view.
6. Next to the file name, click ▼ and select **View**.
The Log Viewer window appears.
7. (Optional) Apply filters.
 - Next to the word **Filters**, click **Priority** and select or clear filters from the drop-down list.
 - Click **Category** and select or clear filters from the drop-down list.

Troubleshooting services

The system contains several Windows services that control data transfer. If one part of the system is not communicating with another, the service that controls the connection might be the source of the problem.

In your troubleshooting procedure, include these tasks:

- Verify that the appropriate service is running. If the service is not running, start it.
- When troubleshooting the connection between a workstation and the server, test the service on the workstation to verify that it can connect to the server.

If you are accustomed to starting and testing Windows services, use the methods you prefer. If you do not have experience with these tasks, you can use the client application for troubleshooting. The following sections provide instructions.

To learn more about each service and its purpose, refer to the "Reference" section.



Verify that a service is running

1. In the menu bar, click **Administration > Administrator tools**.

If you cannot start the program, open Admin Tools from the Windows taskbar: **Start > All Programs > Welch Allyn > Connex > Welch Allyn Connex Admin Tools**.

2. In the navigation bar on the left side of the page, click **Configuration Setting > Server setting**.
3. Next to the service name, check the status message.

Examples of possible messages:

 Welch Allyn Device Connectivity Service is Running Welch Allyn Device Connectivity Service is Stopped


Start a service

1. In the menu bar, click **Administration > Administrator tools**.

If you cannot start the program, open Admin Tools from the Windows taskbar: **Start > All Programs > Welch Allyn > Connex > Welch Allyn Connex Admin Tools**.

2. In the navigation bar on the left side of the page, click **Configuration Setting > Server setting**.
3. Next to the service that you want to start, click **Restart Service**.

When the service starts, a message similar to this one appears next to the service name.

 Welch Allyn Device Connectivity Service is Running

Restart a service

For service settings changes to take effect, the service needs to be restarted. To restart a service that is running, do not use the **Administrator tools** restart function in the Connex VM client application, but instead go to the Microsoft Management Console snap-in for Services.

1. From the Windows taskbar, click **Start > Control Panel > Administrative Tools > Services**.

The Services window appears.

2. Right-click the appropriate service and select **Stop**.
3. Wait 30 seconds.
4. Right-click the service and select **Start**.

Test a service

You can use this feature to verify that a service on a workstation can connect to the server.

1. In the menu bar, click **Administration > Administrator tools**.

If you cannot start the program, open Admin Tools from the Windows taskbar: **Start > All Programs > Welch Allyn > Connex > Welch Allyn Connex Admin Tools**.

2. In the navigation bar on the left side of the page, click **Configuration Setting > Server setting**.
3. Next to the service name, click **Test Service**.

The application directs the default web browser to open an HTML page on the server to see whether the service can connect to the server via the specified IP address and port number.

If the service connects to the server, a page with the title "SessionService Service" appears.

If the connection fails, a page with the title "The page cannot be displayed" appears. This problem has two possible causes:

- The service is pointing to the wrong IP address or port.
- A firewall on the workstation or network is preventing the service from connecting to the server.

Troubleshooting network problems

Use a protocol analyzer to capture network traffic

A network protocol analyzer can be used to assist in determining if information is flowing between the Connex VM server and the devices, workstations, and kiosks used within the Connex VM system. This section is intended for individuals familiar with IP networks and the use of a protocol analyzer. It is suggested that the selected protocol analyzer is capable of capturing network traffic and operating at full network interface speed.

The network traffic of particular interest is the DCP traffic (UDP/44435). The goal is to observe that DCP discovery packets are received from the device. The easiest approach is to suppress all unwanted traffic using the packet filtering capability of your protocol analyzer. The initial filter setting should limit traffic to and from the device in question by IP address. Other traffic of interest is traffic from the device to the DHCP server.

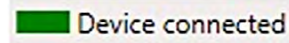
As an example, a device sends a UDP broadcast to port 44435 on the network. The DCP application replies to the device with the IP address and TCP port of the Connex VM server, and subsequent communications are done via TCP.

Note This operation might require the configuration of an IP helper address in a routed network.

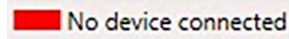
Troubleshooting specific problems

Problem: Client application does not acknowledge a connected device.

The client application displays one of two messages in the bottom right corner of the main window.



A device is connected and communicating with the application.



A device is disconnected or not communicating with the application.

If you connect a device to the workstation and **No device connected** persists, follow these troubleshooting steps.

Possible cause	Corrective action
The application does not recognize the device.	Right-click No device connected and select Refresh devices . The message changes to Device connected .
The device is turned off or does not have power.	Turn on the device. Connect the device to a power source. If the device is running on batteries, ensure that the batteries have sufficient charge to operate the device.
The connectivity cable is not attached to the device or the workstation.	Attach the cable to the device and the workstation.
The connectivity cable is damaged.	Use another cable.
The device has been replaced with another device.	Exit the application, unplug and reattach the cable, and then restart the application.
The device is not configured properly.	Verify that the device is configured properly to send data, per the directions for use that came with the device.
The device driver is corrupt.	Reinstall the driver.
The USB port is damaged.	Plug the device into a different USB port.
The Welch Allyn Device Connectivity Service (DCS) is not running.	Start the service.

Problem: Workstation is not communicating with the server.

Possible cause	Corrective action
When I open the client application, I get an error message.	View application logs.

Possible cause	Corrective action
The wireless network connection has been lost.	<p>Move the computer where there is a known network connection.</p> <p>Use <i>PING</i> or <i>TRACERT</i> from the Windows Command Prompt to confirm that the workstation can connect to the server.</p>
The network is down; a path to the Connex VM Server cannot be found.	<p>Check other software for the same difficulty. If other applications (for example, a web browser) work, verify that the Welch Allyn Hosting Service is reachable through Administrator tools > Configuration Setting > Server setting > Test Service. If this is unsuccessful, verify that the Hosting Service is running on the Connex VM Server and, if needed, restart the service.</p> <p>Use a protocol analyzer to analyze network traffic.</p>
The Connex VM Server is down.	<p>Verify that the Connex VM Server is running with all of the necessary services.</p> <p>Check the application logs for error conditions.</p> <p>Verify network connectivity to the Connex VM Workstation or Kiosk in question using <i>PING</i> or <i>TRACERT</i>.</p>
The workstation is not connected to the network.	<p>Plug the workstation into the network and verify that the workstation shows a LINK light for the Connex VM Workstation or Connex VM Kiosk.</p> <p>Verify that the workstation has the proper IP settings (cmd > ipconfig /all).</p>
The wrong IP address for the Connex VM Server was entered into the Connex VM Workstation.	<p>Use All Programs > Welch Allyn > Connex > Welch Allyn Connex Admin Tools to verify the server IP address. Correct as necessary.</p>

Problem: Server did not receive data from a wireless device.

Possible cause	Corrective action
The device is turned off or does not have power.	<p>Turn on the device.</p> <p>Connect the device to a power source. If the device is running on batteries, ensure that the batteries have sufficient charge to operate the device.</p>
The barcode that was scanned was for the wrong clinician or patient.	<p>Verify that the correct barcodes were used.</p> <p>Verify that the barcodes are assigned properly.</p>
Temperature was taken in Monitoring Mode.	<p>Verify that temperature was not taken in Monitoring Mode. Temperatures read in Monitoring Mode cannot be transferred to the server.</p>

Possible cause	Corrective action
The device, wireless radio, null modem connectors, and barcode scanner are not configured or cabled properly.	<p>Verify that the device, wireless radio, null modem connectors, and barcode scanner are configured and cabled properly.</p> <p>From any Connex VM workstation, ping the radio from the Windows Command Prompt to confirm that the radio can connect to the server.</p>
The device is in a location with a weak signal or no signal.	Move the device where there is a known network connection.
The Welch Allyn Device Connectivity Service (DCS) is not running.	Start the service.
Device Connection Protocol (DCP) is not running.	Start DCP.
DCP is listening on the wrong port.	<p>Verify that DCP is listening on UDP port 44435 as follows:</p> <p>From the Connex VM server, issue the command <code>netstat -na</code> from the Windows Command Prompt.</p> <p>If the results include port 44435, DCP is correctly configured. If port 44435 is not listed, configure the service to listen on this port.</p>
DCS is listening on the wrong port.	Verify that DCS is listening on TCP port 281. If not, configure the service to listen on this port.
DCP is not getting the discovery packets from the device.	Use a protocol analyzer to analyze network traffic.

Problem: Service or database is unavailable.

Possible cause	Corrective action
The network is not available.	<p>Verify that the network to the Welch Allyn Hosting Service is available and that the workstation is connected to it.</p> <p>Verify that the network connection between the Welch Allyn Hosting Service and the database is available and working.</p>
The server that the services or database is on is shut down.	Verify and, if necessary, reboot the server.
The Welch Allyn Hosting Service is not running.	<p>Reboot the server that the service is running on.</p> <p>Restart the service using the Microsoft Management Console snap-in for Services.</p> <p>Verify that the service is running under the appropriate credentials.</p>

Possible cause	Corrective action
The database is not running.	Reboot the server that the database is running on. Restart the SQL Server service using the Microsoft Management Console snap-in for Services.
The client application is not configured properly.	Verify that the endpoint definitions are set up to the proper TCP endpoint. Verify that the "localhost" certificate is installed.
The Welch Allyn Hosting Service is not configured properly.	Verify that the service is publishing on the right endpoint addresses. Verify that the "localhost" certificate is installed. Verify that the connection string to the database is set up to talk to the right database. Verify that the connection string to the database is using the correct authentication type and security token.
The database is not configured for remote access.	Make sure that the SQL Server Browser service is running on the server with the database. Verify that the database is configured to communicate using the TCP/IP communication protocol. Check the properties of the SQL Server instance and make sure that instance is configured to allow remote connections.

Problem: Data is locked.

Possible cause	Corrective action
Someone else is editing or attempting to delete the same data.	Retry later, or use the Release Locks page to determine who is editing the data and contact that person.
When someone else was editing or attempting to delete the same data, the application "crashed."	Retry later, or manually release the lock from the Release Locks page.
When someone else was editing or attempting to delete the same data, the database or services became unavailable.	Manually release the lock from the Release Locks page.

Problem: I cannot log on to a Citrix server from a Citrix ICA client.

When you try to log on, an error message appears.

Possible cause	Corrective action
A vital signs device is connected to the Citrix ICA client via USB cable.	Unplug the device from the client, then log on to the Citrix server. Reconnect the device.

Problem: Customizations to modifiers do not appear in the Capture Vital Signs window.

Possible cause	Corrective action
Customizations were made at the MACHINES level, but the workstation is not listed in the MACHINES list.	Log on to the workstation with the ADMIN account. This action adds the workstation to the MACHINES list. Verify that the customizations appear in the Capture Vital Signs window.

Problem: Corepoint Administration Console displays errored messages.

Possible cause	Corrective action
The SQL Server that hosts the Connex VM and HL7 databases is offline or cannot be reached.	<div>Verify that SQL Server is running.</div> <div>Verify network connectivity to SQL Server.</div> <div>Note While SQL Server is unavailable, stop the Corepoint Integration Engine service via the Corepoint Administration Console or the Microsoft Management Console snap-in for Services.</div>

Reference

Welch Allyn services

The following tables describe the services that are installed as part of the system.

Welch Allyn Connex

Service name	Description	Runs on
DCP Daemon	Provides the Device Connection Protocol for Welch Allyn wireless vital signs devices. If this service is not running, the devices cannot connect to the server and send vital signs data.	Server
Welch Allyn Hosting Service	Provides the connectivity for workstations. If this service is not running, the workstations cannot connect to the server.	Server
Welch Allyn Device Connectivity Service	Enables vital signs devices to send data to the server. If this service is not running, both wired and wireless devices cannot connect to the server. This service depends on the Welch Allyn Hosting Service.	Server and workstation
Welch Allyn Enterprise Gateway Service	Processes patient data and passes data between the Corepoint Integration Engine and the Connex VM database. If this service is not running, HL7 messages to and from the hospital information system are not processed.	Server

Welch Allyn Remote Service Delivery System (RSDS)

Service name	Description	Runs on
Axeda Desktop Server	Provides secure remote service and support delivery used by RSDS.	Server and workstation

Service name	Description	Runs on
WelchAllynRSDSGateway	Provides real-time communication and data collection for remote software and hardware resource monitoring.	Server and workstation

Corepoint HL7

Service name	Description	Runs on
Corepoint Integration Engine	Processes inbound and outbound HL7 messages between the server and the hospital information system. If this service is not running, HL7 messages to and from the hospital information system are not processed.	Server
Corepoint Integration Engine Assured Availability	High availability service for the Corepoint Integration Engine.	Server
Corepoint Integration Engine Monitor Service	Provides web-based monitoring and control of the Corepoint Integration Engine.	Server

TCP/UDP ports used

The installation program assigns ports to system applications.

The following tables list the port assignments. After installation, you can use this information to configure the firewalls, virus software, and router access lists for your facility.

The installation program configures the default Microsoft Windows firewall automatically if the firewall is running at the time of installation.

Note The ports are configurable (if needed), but must be matched in both the service's and workstation's configuration files.

Welch Allyn Connex

Application	Port number	Protocol
DCP Daemon	44435	UDP
DCP Daemon	7711	UDP
Welch Allyn Device Connectivity Service	281	TCP
Welch Allyn Hosting Service	8732	TCP
Welch Allyn Hosting Web Service (for testing from the workstation)	8731	HTTP (TCP)

Welch Allyn Remote Service Delivery System (RSDS)

Application	Port number	Protocol
AxedaDesktopServer	5920	TCP
AxedaDesktopServer	5920	UDP
WelchAllynRSDSGateway	3011	TCP
WelchAllynRSDSGateway	3030	TCP
Welch Allyn Remote Service Delivery System (RSDS) - External Connection	443	HTTPS (TCP)

Corepoint HL7

Application	Port number	Protocol
Inbound ADT HL7 Interface Port	Port is defined at system installation	TCP
Outbound HLT Interface Port	Port is defined at system installation	TCP

Medical device connectivity requirements

To communicate with the server, supported devices require the hardware and software listed in this table. The table also provides guidance on device configuration.

Device	Workflow	Recommended minimum software revision	Connectivity kits	Additional accessory kits	Configuration
VSM 300 (5300)	Vital signs monitoring without patient identification at the device Computer-based vital signs	1.2	5300-170	See Note 1	No configuration on the device is required to work with the serial connection.
Spot Vital Signs	Computer-based vital signs	2.18	4200-170	See Note 1	No configuration on the device is required to work with the serial (infrared) connection.

Device	Workflow	Recommended minimum software revision	Connectivity kits	Additional accessory kits	Configuration
Spot Vital Signs LXi (wired)	Computer-based vital signs Batch spot-check vitals Push from device/auto reconcile batch	6.0	4500-925	4500-915	No configuration on the device is required to work with the USB cable. For batch spot-check vitals and push from device/auto reconcile batch, the device should be configured for patient and clinician identification. For push from device/auto reconcile batch, the Information System setting in the Configuration Menu should be turned on.
Spot Vital Signs LXi (wireless)	Wireless workflow	6.0	4500-922 (802.11a/b/g) 4500-920 (802.11b), US and Canada only	4500-926 or 4500-927 (See Note 2) 4500-906, Spot LXi Radio Config CD 4500-907, Spot LXi Firmware Upgrade CD 4500-915	See 4500-921, DFU, Spot LXi b Radio or 4500-923, DFU, Spot LXi a/b/g Radio. See DIR 80012309 Version D for radio configuration option. See DIR 80012310 Version D for Spot LXi firmware upgrade procedure.
VSM 6300	Computer-based vital signs Batch spot-check vitals Push from device/auto reconcile batch Ethernet workflow	All	60000-925 660-0321-00, 660-0320-00, or 660-0138-00 (see Note 3)	6000-915 or 6000-915HS (see Note 4)	Only wired communications are available for this model. The device should be configured for patient and clinician identification. Initial configuration for Ethernet is done on the device. The Welch Allyn Service Tool (103521) is used to complete the configuration.

Device	Workflow	Recommended minimum software revision	Connectivity kits	Additional accessory kits	Configuration
					See the VSM 6000 directions for use (103501) for Connex VM specific configuration requirements for desired workflow(s).
VSM 6400	Same as the VSM 6300 Wireless workflow with radio upgrade (see VSM 6500)	All	60000-925 660-0321-00, 660-0320-00, or 660-0138-00 (see Note 3) 6000-920 (see Note 5)	6000-915 or 6000-915HS (see Note 4)	The device should be configured for patient and clinician identification. Initial configuration for Ethernet is done on the device. The Welch Allyn Service Tool (103521) is used to complete the configuration. See the VSM 6000 directions for use (103501) for Connex VM specific configuration requirements for desired workflow(s).
VSM 6500	Same as the VSM 6300 with the addition of the wireless workflow	All	60000-925 660-0321-00, 660-0320-00, or 660-0138-00 (see Note 3)	6000-915 or 6000-915HS (see Note 4)	The device should be configured for patient and clinician identification. Initial configuration for Ethernet and wireless is done on the device. The Welch Allyn Service Tool (103521) is used to complete the configuration. See the VSM 6000 directions for use (103501) for Connex VM specific configuration requirements for desired workflow(s).

For instructions on how to check the firmware version on a device, refer to the directions for use that came with the device or visit our product catalog at welchallyn.com.

Note 1: For PCs with a USB port and no DB-9 serial ports, a Keyspan DB-9 to USB adapter may be required (Welch Allyn PN: PC-USB-SER).

Note 2: To configure the 4500-920 (IT, WIRELESS RADIO, SPOT ULTRA) and 4500-922 (KIT, 802.11 A/B/G RADIO, SPOT LXI) radio options, either 4500-926 (CABLE FOR WIRED CONN, KEYSpan; for PC with USB and no DB-9 serial port) or 4500-927 (USB/SERIAL CABLE KIT FOR SPOT LXI; for PC with DB-9 serial port) is required.

Note 3: The different connectivity kits provide different capabilities. 6000-925 is a USB cable for wired connectivity via USB interface. Part numbers 660-0321-00 (Patch cable, 50'), 660-0320-00 (Patch cable, 100'), and 660-0138-00 (Patch cable, 5') are for Ethernet connectivity.

Note 4: Additional accessories are barcode scanners. 6000-915 includes an HS-1M 2D barcode scanner, mounting bracket, license, and hardware. 6000-915HS includes an HS-1M 2D barcode scanner, coiled USB cable, and license.

Note 5: To upgrade this device for wireless communication, a 6000-920 Internal 802.11 a/b/g wireless radio kit is required.

