Medtronic

Installation Manual

Vital Sync™

Virtual Patient Monitoring Platform and Informatics Manager

Table of Contents

Table of Contents

List of Figures

List of Figures

List of Figures

Page Left Intentionally Blank

List of Tables

Page Left Intentionally Blank

1 Introduction

1.1 Overview

This manual provides information on installation and setup of Vital Sync™ virtual patient monitoring platform and informatics manager software components, as well as other software required for their installation and use, including prerequisites, installation procedures, and configuration details.

Note:
Before installation, carefully read this manual, any necessary system documentation, and precautionary information and specifications.

1.2 Conventions

Text and terminology conventions used in this manual include the following:

- Button names, menu options, and field names generally appear in **boldface** text.
- The term "click" refers to the action activating buttons and menus in an application's user interface. If using a touchscreen monitor or mobile device, substitute "touch" for "click" where it appears in the text.
- The terms "platform", "components", "software", and "software components" generally refer to part or all of the Vital Sync™ virtual patient monitoring platform, the Vital Sync™ informatics manager, or both.

1.3 Labeling Symbols

This section contains definitions for the symbols used on the product labeling.

Table 1-1. Labeling Symbol Definitions

Symbol	Definition
Rx ONLY	Federal (U.S.A.) law restricts the use of the application to sale by or on the order of a physician.
	Consult instructions for use.
	Manufacturer.

1.4 Applicable Version

This manual applies to installing version 2.7 of the Vital Sync™ virtual patient monitoring platform and informatics manager. Version information for supporting software is indicated in other sections of this manual.

1.5 Safety Information

This section contains generally applicable safety information for this product.

1.5.1 Safety Symbols

Table 1-2. Safety Symbol Definitions

Symbol	Definition
	WARNING **Warnings alert users to potential serious outcomes (death, injury, or adverse events) to the patient, user, or environment.**
	Caution **Cautions alert users to exercise appropriate care for safe and effective use of the product.**
	Note Notes provide additional guidelines or information.

1.5.2 Warnings

WARNING:
The Vital Sync™ Virtual Patient Monitoring Platform and Informatics Manager is intended to supplement and not to replace any part of the facility's monitoring. Do not rely on the Vital Sync™ Virtual Patient Monitoring Platform and Informatics Manager as the sole source of alarms.

In order to assure a timely response to device alarms, a clinician (not necessarily the clinician viewing data in the platform) must be within visual and/or audible range of the alarming device. In order to provide medical intervention, a clinician must interact with the device at the bedside.

WARNING:
The platform is intended only as an adjunct in patient assessment. It must be used in conjunction with clinical signs and symptoms and periodic patient observations.

WARNING:
The dedicated bedside display unit is designed for use in conjunction with the Vital Sync™ Virtual Patient Monitoring Platform and Informatics Manager. Do not rely on the dedicated bedside display unit as a primary source of alarms.

WARNING:
Always follow the facility's established patient safety protocols when using the Vital Sync™ Virtual Patient Monitoring Platform and Informatics Manager.

WARNING:
The alarm rule functionality within the software is intended to supplement and not replace any part of the facility's monitoring. Do not rely on the platform as the sole source of alarms.

WARNING:
Alarm rules should adhere to facility policy, procedures, and alarm management protocols. This alarm management protocol should address alarm safety and the potential impact of alarm fatigue in all patient care areas within the facility.

WARNING:
Alarm priority normalization and ranking functionality within the software is intended to supplement and not replace any part of the facility's monitoring. Do not rely on the platform as the sole source of alarms.

WARNING:
The default alarm priority is determined by the connected device, and cannot be changed on the device. The *same* alarm condition may be reported with a *different* priority on *different* device models. Carefully review the Alarm Normalization Report for default alarm priorities for each connected device model.

WARNING:
Alarm priorities in the software should not be set to be lower than those on the actual device. Use caution if changing the priority of a device alarm in the software to a different level than is indicated on the actual device, especially for devices that are life-sustaining.

WARNING:
Alarms from connected devices should not be set as notifications in the platform, especially for devices that are life-sustaining. Because notifications do not audibly annunciate, setting an alarm as a notification may cause users to not respond or delay in responding to a clinically significant event.

WARNING:
Notifications from connected devices should not be set as alarms in the platform, especially for events not requiring clinical intervention. Setting a notification as an alarm may create nuisance audible alerts that are not clinically significant.

WARNING:
If using audible alerts, ensure the sound volume of the PC or mobile device on which the software is used is sufficient for alerts to be heard and recognized.

WARNING:
It is possible for the platform's audible alert tone to be confused with audible alarm tones from connected devices when in close physical proximity. Users should carefully attend to all audible indicators when within audible range of connected devices.

WARNING:
When setting alarm rules and priorities in the software for any device, consult the operator's manual for the device in question for default priority levels of device alarms, and for a description of each device alarm. Obtain a detailed understanding of the patient or device conditions that trigger any alarm before creating an alarm rule or adjusting the alarm's priority in the software.

WARNING:
Medtronic does not assume any responsibility for accuracy, reliability, or clinical relevance of user-designed derived parameter algorithms.

1.5.3 Cautions

Caution:
Do not set alarm limits to extreme values that render the monitoring system useless. Ensure alarm limits are appropriate for each patient.

Caution:
Connected devices report data to the platform periodically, not continuously. Because of this, as well as delays caused by network bandwidth or hardware limitations or network loading, the true duration of any device alarm will be longer than the delay set in this screen for that alarm.

Carefully consider these factors when choosing delay settings, and use the shortest delay settings that are practical to reduce nuisance alarms, to avoid undue delay in response to events actually requiring direct clinical intervention.

Caution:
Loss of patient privacy may occur if using the Vital Sync™ Virtual Patient Monitoring Platform and Informatics Manager on unsecured or unencrypted networks. Always adhere to facility patient privacy practices and procedures to ensure security of patient data on the facility's network.

1.5.4 Notes

Note:
Some mobile devices do not support the sounding of audible alerts from the platform due to device limitations. Make sure to test audible alert capability on any mobile device to be used.

Note:
Audible alerts only sound to indicate alarms on devices linked to patients. Audible alerts do **not** sound for notifications.

Note:
The platform has been verified on systems using Microsoft™* Windows™* and Windows™*-based software. User experience may vary with other operating systems and hardware and software configurations.

1.6 Obtaining Technical Assistance

1.6.1 Technical Services

For technical information and assistance, if unable to correct a problem while using the software, contact Medtronic or a local Medtronic representative.

Medtronic Technical Services

15 Hampshire Street

Mansfield, MA 02048 USA

1 800 497 4968, or 1 925 463 4635,

or contact a local Medtronic representative

HIMSupport@Covidien.com

When calling Medtronic or a local Medtronic representative, provide the software version number, build number and date of build, shown on the About screen.

1.6.2 Related Documents

Before installing, carefully read this manual as well as installation documentation for the supporting software. This information is essential for understanding the installation process and information shown during installation.

1.7 Warranty Information

The information contained in this document is subject to change without notice. Medtronic makes no warranty of any kind with regard to this material, including, but not limited to, the implied warranties or merchantability and fitness for a particular purpose. Medtronic shall not be liable for errors contained herein or for incidental or consequential damages in connection with the furnishing, performance, or use of this material.

1.8 Licensing Information

For more details regarding software licenses, refer to the following sections.

1.8.1 Vital Sync™ and Third Party Software

Licenses obtained from Medtronic for use of the virtual patient monitoring platform (including the informatics manager) do not include licenses for any third party software, including software identified in Chapters 2, 3, and 5 of this manual. (Refer to *Prerequisites*, page 2-1; *Recommended Configuration*, page 2-3; *Supporting Software*, page 3-1; and *Additional Configuration*, page 5-1.)

Users must obtain their own licenses for the downloading and use of such third party software.

1.8.2 Open Source Software Disclosure

This section identifies the open source software that may be separately called, executed, linked, affiliated, or otherwise utilized by this Vital Sync™ software product.

Such open source software is licensed to users subject to the terms and conditions of the separate software license agreement for such open source software.

Use of the open source software by users of the Vital Sync™ virtual patient monitoring platform and informatics manager shall be governed entirely by the terms and conditions of such license.

Obtain the source or object code and applicable license for any open source software at the following sites:

- **NCalc**—https://www.nuget.org/packages/ncalc/
- **RestSharp**—http://restsharp.org/
- **Ninject**—https://www.nuget.org/packages/Ninject/4.00-beta-0134
- **NHibernate**—http://nhibernate.info/
- **Newtonsoft.Json**—https://www.nuget.org/packages/Newtonsoft.Json/
- **D3**—https://d3js.org/
- **Spin.js**—https://spin.js.org/

- **Foundation**—http://foundation.zurb.com
- **JQuery**—http://jquery.com
- **JQuery blockUI**—http://malsup.com/jquery/block/
- **JQuery DateTimePicker**—https://github.com/xdan/datetimepicker
- **JQuery Tools**—http://flowplayer.org/tools/
- **JQuery UI**—http://jqueryui.com
- **JQuery Validation**—http://jqueryvalidation.org/
- **CSS Browser Selector**—http://rafael.adm.br/css_browser_selector
- **MvcPaging**—https://www.nuget.org/packages/MvcPaging/

1.9 HIPAA Disclaimer

The Vital Sync™ Virtual Patient Monitoring Platform and Informatics Manager is a software application used in conjunction with electronic medical devices within the customer's secure health information system. Healthcare providers using the software are expected to take appropriate security measures to protect the confidentiality of all data created, stored or transmitted on their systems.

Although the software contains certain features to assist users in the users' steps to protect their data, Medtronic cannot provide any assurance that the user's use of the software will comply with HIPAA regulations or be otherwise in compliance with the customer's obligations as a covered entity.

Page Left Intentionally Blank

2 Product and Installation Overview

2.1 Overview

This chapter describes the requirements and general process for installation and configuration of Vital Sync™ virtual patient monitoring platform and informatics manager software components, as well as for supporting software.

2.2 Prerequisites

In order to install and use software components, the systems in question must meet certain hardware and operating system requirements, and must also have other supporting software installed and configured. Instructions for installation and setup of some of the supporting software are included in this manual.

Note:
To install software, administrative rights are required on the destination systems.

2.2.1 Minimum Requirements

See Table 2-1 and Table 2-2 for minimum hardware and software requirements.

Table 2-1. Minimum Hardware Requirements (physical server)

Requirement	Server with components installed	Central monitoring station desktop
CPU	3.1 GHz, 8M cache, 5 GT/s QPI, 4 core	1–1.65 GHz, dual core
RAM	16 GB	4 GB
Hard drive capacity	500 GB	50 GB
External storage	External tape or other customer-sourced backup for data archive	None
Network	100/1000 Mbps Ethernet	
Wireless network	Bandwidth (Kbps) equal to 5.7X+270Y (X=number of active devices; Y=number of active display devices)	

Table 2-1. Minimum Hardware Requirements (physical server) (Continued)

Requirement	Server with components installed	Central monitoring station desktop
Other hardware	Uninterruptible power supply	Touch-enabled display with 1920×1080 resolution Video card compatible with touch-enabled display Speakers (monitor-mounted or external)

Table 2-2. Minimum Hardware Requirements (virtual machine)

Requirement	Database server	Web / Data collector server
CPU	2.0 GHz 6 VCPU	2.0 GHz 4 VCPU
RAM	16 GB	8 GB
Hard drive capacity	580 GB (minimum 4 drives)	80 GB
External storage	External tape or other customer-sourced backup for data archive	None
Network	100/1000 Mbps Ethernet	
Wireless network	Bandwidth (Kbps) equal to 5.7X+270Y (X=number of active devices; Y=number of active display devices)	

Table 2-3. Minimum Software Requirements

Requirement	Server with components installed	Central monitoring station desktop
Operating system	Microsoft™* Windows™* Server 2012 R2 Standard	Microsoft™* Windows™* 7 (64-bit)
Database software	Microsoft™* SQL Server™* 2012 Standard Edition R2 with Service Pack 4 (required only on the server hosting the database component)	None
Supporting software	Microsoft™* Web Deploy 3.0 Internet Information Services (IIS) 8.0 Microsoft™* .NET Framework 4.6.2	Microsoft™* Internet Explorer 11 Adobe™* Reader™*

Note:
Specific deployments may have higher minimum requirements than those listed here. Consult with Medtronic Professional Services for more information.

2.2.2 Recommended Configuration

Note:
While all components can be installed on a single system, Medtronic recommends that the Informatics Web and Database components should be installed on separate systems, especially if a large number of users will be accessing and using the software, or if a large number of patients and devices will be connected and monitored.

The Data Collection Service, Applet Manager Service (if used), and Informatics Web components should be installed on a server separate from the Database component, so that resource-intensive functions requiring database access (such as reporting) will not interfere with ongoing clinical operations. Refer to *Distributed Deployment*, page 5-8, for more information.

See Table 2-4 for recommended software.

Table 2-4. Recommended Software

Requirement	Servers with components installed	Central monitoring station desktop
Operating system	Microsoft™* Windows™* Server 2016 Standard with all current updates	Microsoft™* Windows™* 10 (64-bit)
Database software	Microsoft™* SQL Server™* 2016 Standard Edition with Service Pack 1 (required only on the system hosting the database component)	None
Supporting software	Microsoft™* Web Deploy 3.0 Internet Information Services (IIS) 10.0 Microsoft™* .NET Framework 4.6.2)	Microsoft™* Edge (version 42) or Google™* Chrome™* (version 67) Adobe™* Reader™*

For best results when using Web browsers to access the software and perform program functions, ensure that the display resolution is set to at least 1024 x 768 (1920 x 1080 for a central monitoring station).

Note:
To maximize performance, and for best connectivity with remote devices, Medtronic recommends that the Vital Sync™ virtual patient monitoring platform and informatics manager, its necessary supporting software, and related applications (such as the Vital Sync™ early warning score application) should be the **only** applications running on the systems on which they are installed.

Note:
Some mobile devices do not support sounding of audible alerts due to device limitations. Make sure to test audible alert capability on all mobile devices to be used.

2.3 Installation Process

Note:
Licenses obtained from Medtronic for installation and use of the Vital Sync™ virtual patient monitoring platform (including the informatics manager) do not include licenses for any third party software identified in this chapter. Users must obtain their own licenses for the downloading and use of such third party software.

2.3.1 Initial Installation

For a first-time installation of the software, the process includes the following steps:

- Ensure applicable supported updates for Microsoft™* Windows™* Server have been downloaded and installed, as described in the release notes.
- Add IIS role services and (if necessary) message queuing. Refer to *Add IIS Role Services* and *Install Message Queuing* (Chapter 3).
- Configure the default IIS application pool. Refer to *Configure the IIS Application Pool* (Chapter 3).
- Install and configure Microsoft™* SQL Server™*. Refer to *Install the Database Server* and *Distributor Configuration* (Chapter 3). The 2016 version of the software does not include Microsoft™* SQL Server™* Management Tools; if needed, install these separately.
- Set up database connectivity for remote users. Refer to *Enable Remote Connection* (Chapter 3).
- Install Vital Sync™ software components. Refer to *Installing Software Components* (Chapter 4).
- If needed to enable HL7 message and/or alarm message availability for external systems, configure the Vital Sync HL7 Reporter Service, Vital Sync ADT In Adapter Service, and Vital Sync Alarm Reporter Service. Refer to *Connectivity to External Systems* (Chapter 6).
- If needed, perform LDAP and active directory server integration. Refer to *Connectivity to External Systems* (Chapter 6).
- If using a Lantronix™* gateway with the Vital Sync™ software, enable and configure unique device identification. Refer to *Connectivity to External Systems* (Chapter 6).
- Start database agents running to fully enable replication. Refer to *Database Agent Startup* (Chapter 5).
- Confirm that firewall ports are properly configured to allow the software to communicate with the network and with devices to be monitored. Refer to *Firewall Configuration* (Chapter 5).
- Perform date and time synchronization on all systems. Refer to *Time Synchronization* (Chapter 5).
- If needed, configure reporting to connect to the Data Warehouse server. Refer to *Distributed Deployment* (Chapter 5).
- For a multi-system deployment, perform additional configuration procedures as needed. For an example of such a deployment, refer to *Distributed Deployment* (Chapter 5).

2.3.2 Upgrade Installation

To upgrade from a previous version of the software, the process includes the following steps:

- Before installing any software, make backups of all application database files created with the previous installation of the software, and save the backups in a safe location. The backup process prevents data loss in the event that problems occur during installation of the current version of the software.
- Ensure supporting software is already installed on all systems to be used with the upgraded version, as described in Chapter 3. Additional installation of supporting software should not be necessary unless the deployment configuration has changed from that used for the previous version of the software.
- Install Vital Sync™ software components. Refer to *Installing Software Components* (Chapter 4).
- If needed, perform additional configuration procedures as described in Chapter 5 and Chapter 6. Additional steps necessary will vary depending on deployment.

Note:

If upgrading from a version of the software previous to v2.5.x, uninstall the older version before installing the current version.

if upgrading from version 2.5.x of the software, to avoid potential problems with database functions, first upgrade to version 2.6.x, then upgrade to version 2.7.0.

Page Left Intentionally Blank

3 Supporting Software

3.1 Overview

This chapter provides details on installing and configuring supporting software required before installing Vital Sync™ virtual patient monitoring platform and informatics manager software components.

The primary task is the installation of Microsoft™* SQL Server™* on the system where certain specific Vital Sync™ software components will reside.

At certain points, the following steps are also required to allow systems and software components to communicate and properly exchange information:

- Adding Microsoft™* Windows™* Server Internet Information Services (IIS) roles and configuring the default application
- Configuring the database servers to allow replication
- Enabling remote connection to the database servers

Note:
Licenses obtained from Medtronic for installation and use of the Vital Sync™ virtual patient monitoring platform (including the informatics manager) do not include licenses for any third party software identified in this chapter. Users must obtain their own licenses for the downloading and use of such third party software.

Note:
To install and configure software, administrative rights are required on destination systems.

Note:
Setup and configuration procedures in this chapter are to support the Vital Sync™ virtual patient monitoring platform and informatics manager software,

3.2 Operating System Updates

Before performing any procedures detailed in this manual, ensure supported Microsoft™* Windows™* service packs and updates have been downloaded to and installed on the affected system or systems. Reference the release notes for this version of the software for more information.

3.3 Add IIS Role Services

After ensuring that supported operating system updates and service packs are installed, add IIS role services.

The Add Roles wizard shows a series of screens for selection of options. If changes are required to selections already made, click **Back** to go back to the previous screen, then make the change.

In any screen, if needed, click **Cancel** to stop configuration and exit the wizard.

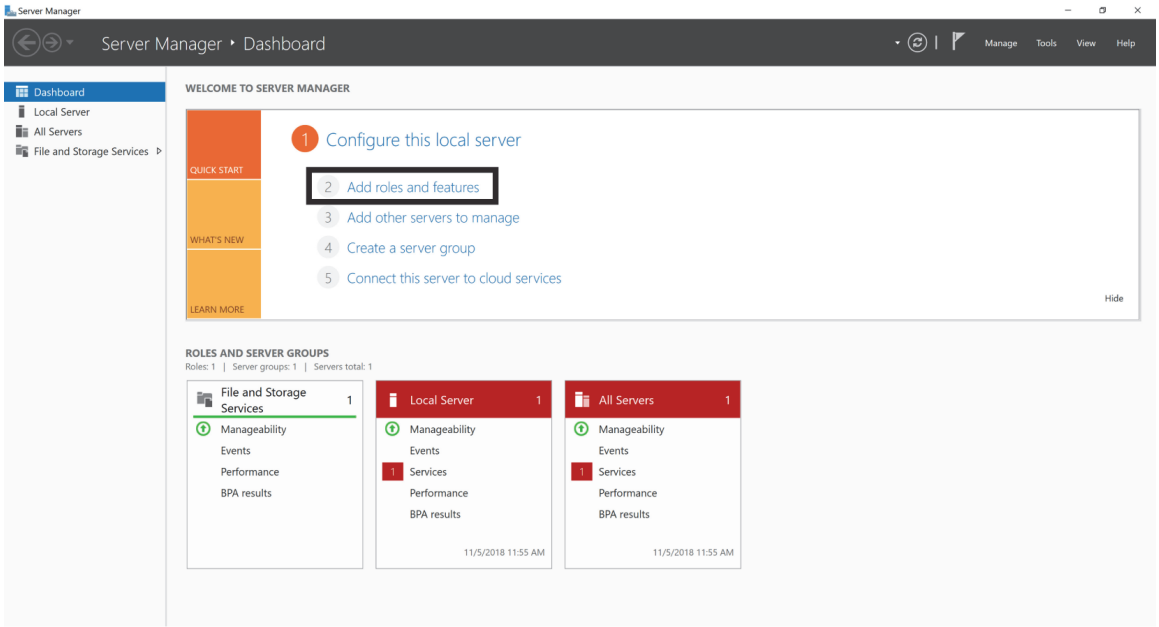
Note:
Add IIS role services to the same system where the Data Collection Service and Informatics Web components are to be installed. (Refer to *Distributed Deployment*, page 5-8, for details on installation in a distributed environment.)

Note:
This manual shows screen captures for adding IIS role services using version 8.0 of IIS. Version 7.0 of IIS is also supported. The procedure does not differ significantly between the two versions. If encountering problems during or after adding IIS role services, contact Medtronic Professional Services.

To add IIS role services:

1. From the Start menu, select **Administrative Tools**.
2. Open the Server Manager.

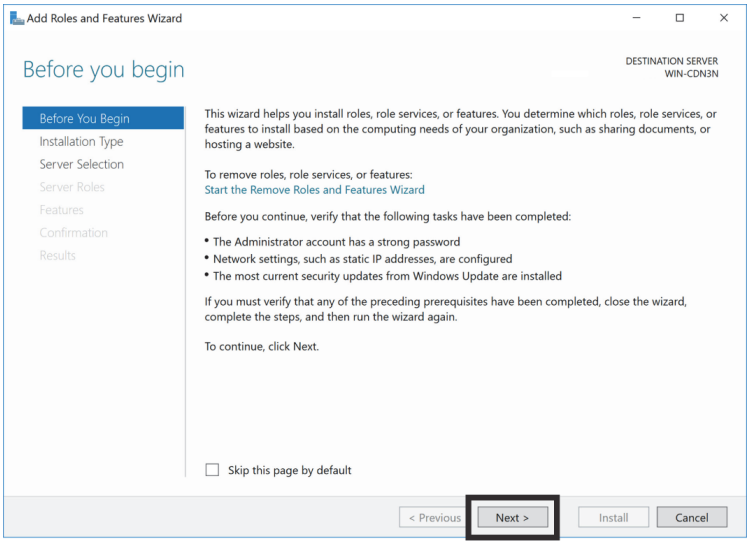
Figure 3-1. Server Manager



INF_10004_D

3. In the Dashboard pane, click on **Add Roles and Features** to start the Add Roles and Features wizard.

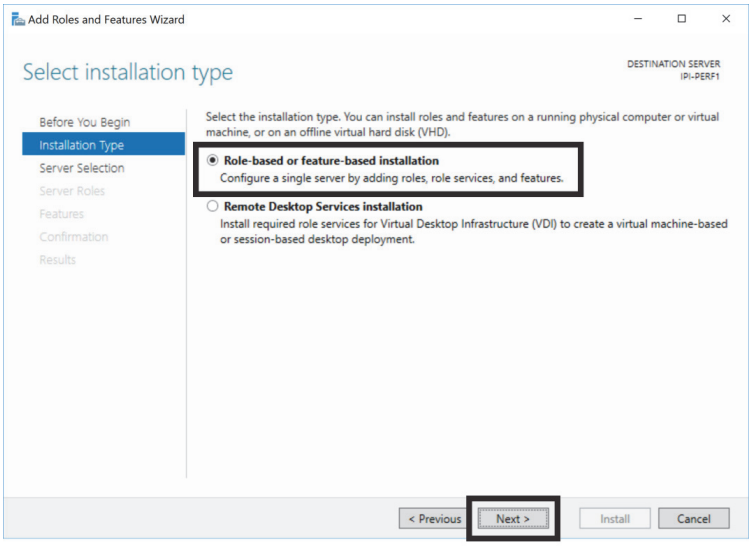
Figure 3-2. IIS Add Roles and Features Wizard—Start Page



INF_10005_D

4. Verify that tasks listed on the page have been completed, then click **Next** to access the Installation Type page.

Figure 3-3. IIS Add Roles and Features Wizard—Installation Type Page

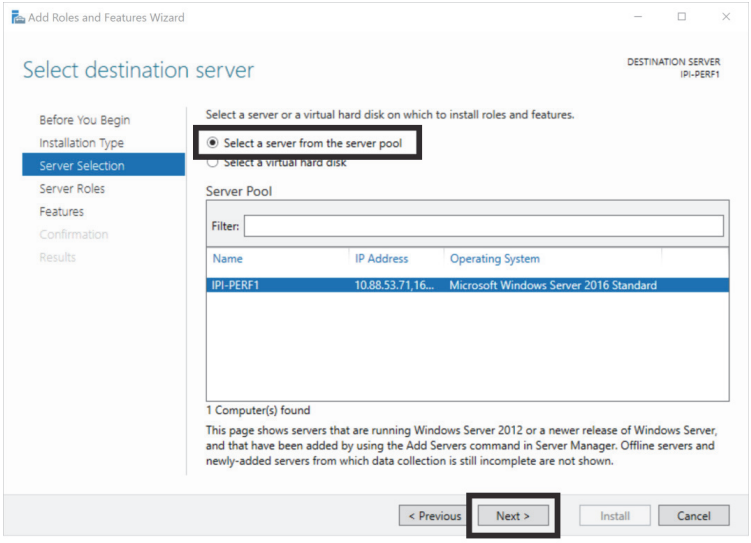


INF_10492_B

5. Click the **Role-based or feature-based installation** radio button if it is not already selected.

6. Click **Next** to access the Destination Server Selection page.

Figure 3-4. IIS Add Roles and Features Wizard—Destination Server Selection Page



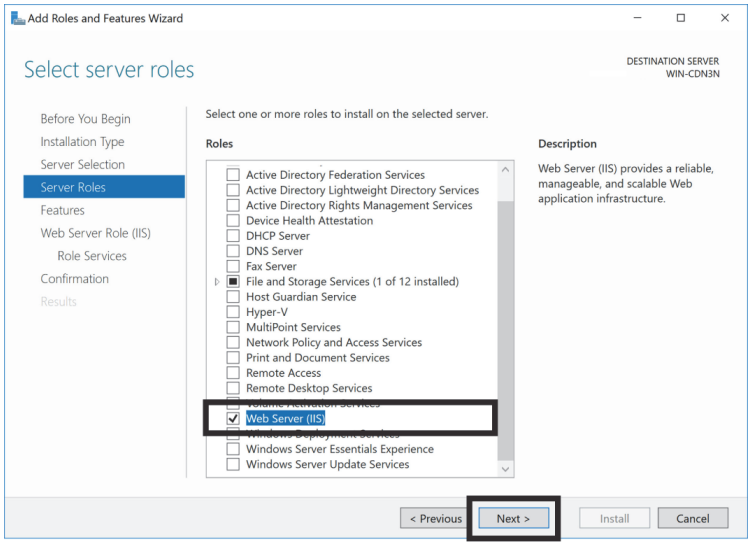
INF_10493_B

7. Click the **Select a server from the server pool** radio button if it is not already selected.

8. In the Server Pool pane, find the desired server and click on it to select it.

9. Click **Next** to access the Select Server Roles page.

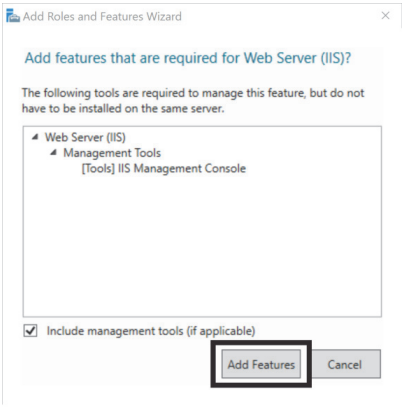
Figure 3-5. IIS Add Roles and Features Wizard—Select Server Roles Page



INF_10006_D

10. Check the **Web Server (IIS)** check box, then click **Next** to access the Add Required Features page.

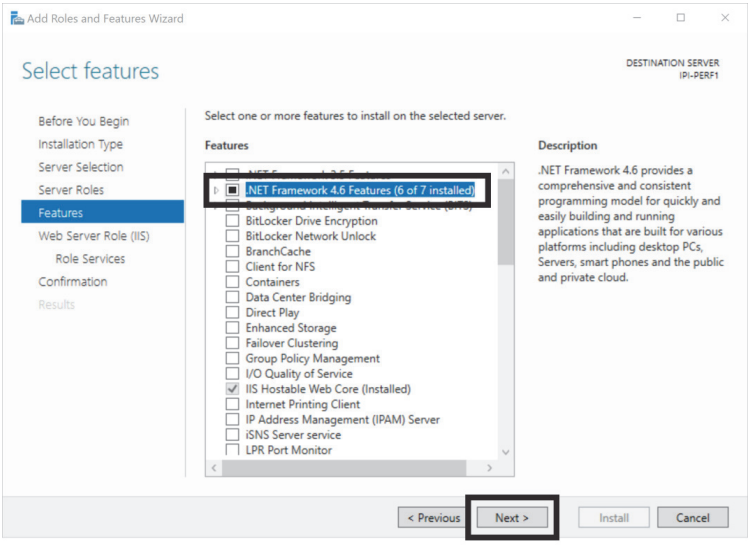
Figure 3-6. IIS Add Roles and Features Wizard—Add Required Features Page



INF_10494_B

11. Ensure that the **Include management tools** check box is checked, then click **Add Features** to access the Select Features page.

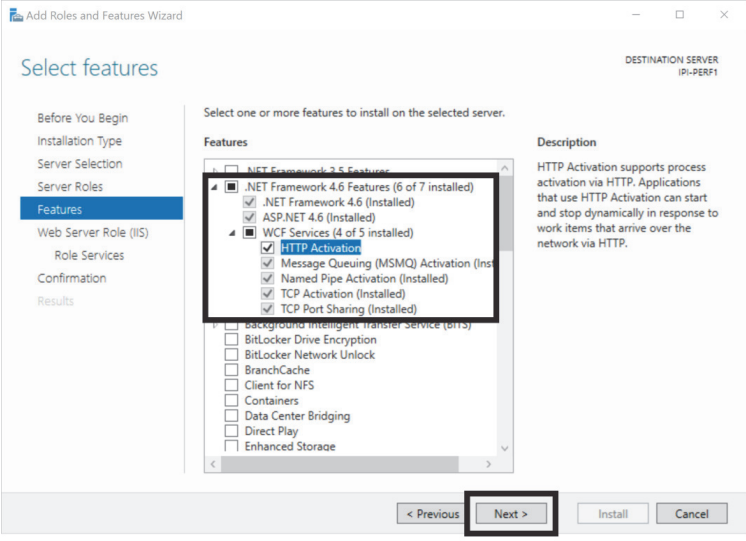
Figure 3-7. IIS Add Roles and Features Wizard—Select Features Page



INF_10499_B

12. Click the triangle next to the **.NET Framework 4.6 Features** check box to show available options.

Figure 3-8. IIS Add Roles and Features Wizard—Select Features Page (.NET Framework 4.6 fields shown)

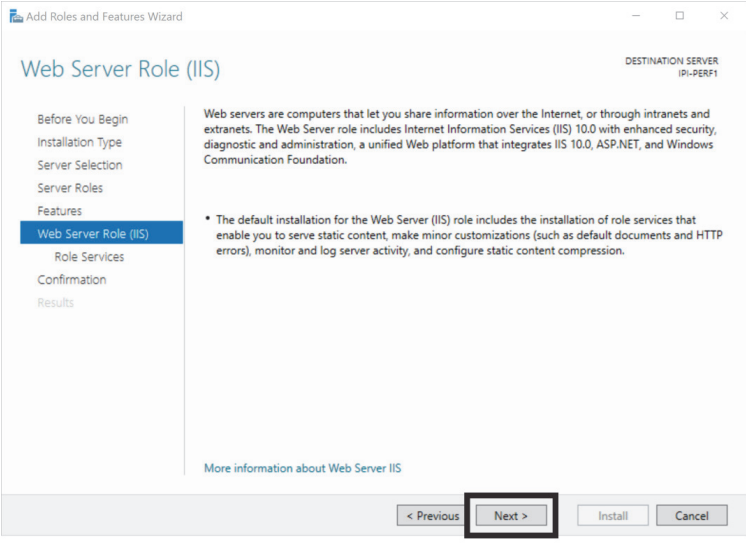


INF_10500_B

13. Click the triangle next to the **WCF Services** check box to show available options.

14. Make selections as shown in Figure *3-8*, then click **Next** to access the Web Server Role (IIS) page.

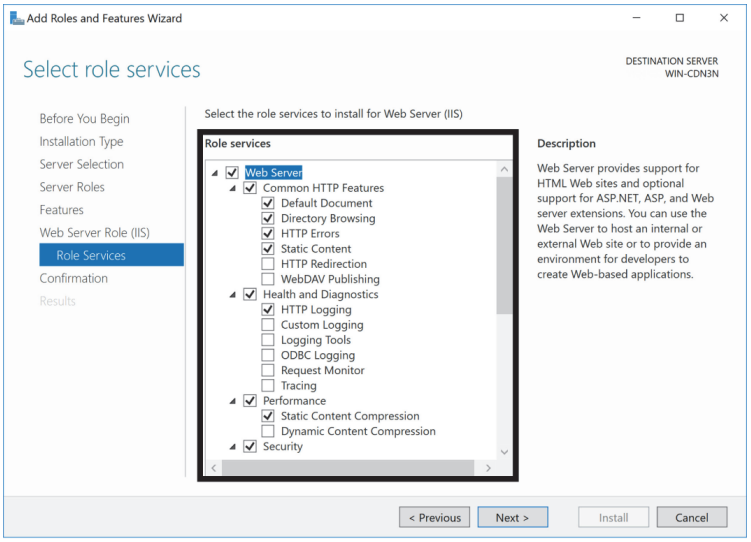
Figure 3-9. IIS Add Roles and Features Wizard—Web Server Role (IIS) Page



INF_10501_B

15. If needed, review the text on the page, then click **Next** to access the Select Role Services page.

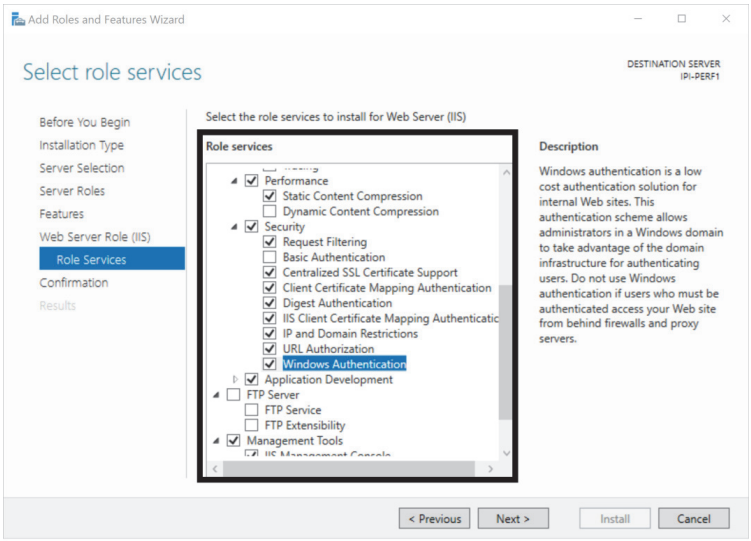
Figure 3-10. IIS Add Roles and Features Wizard—Select Role Services Page (common HTTP and health/diagnostics options)



INF_10007_D

16. Make selections in the role services fields as shown in Figure *3-10*, then scroll down in the pane.

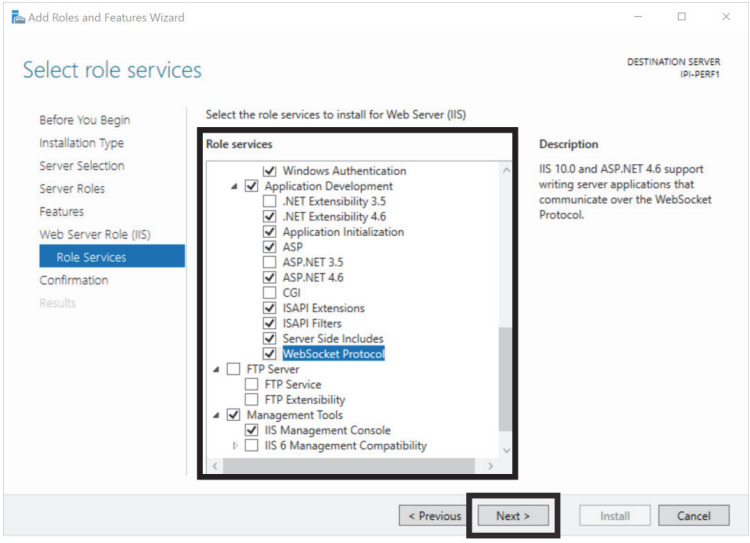
Figure 3-11. IIS Add Roles and Features Wizard—Select Role Services Page (performance and security options)



INF_10502_B

17. Make additional selections in the role services fields as shown in Figure *3-11*, then scroll down in the pane.

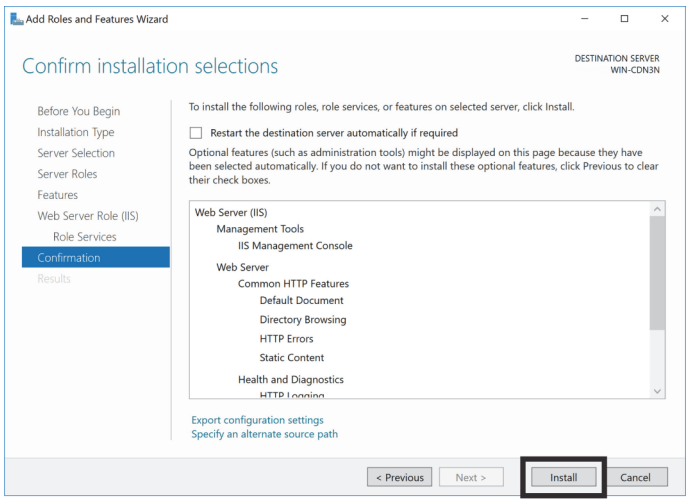
Figure 3-12. IIS Add Roles and Features Wizard—Select Role Services Page (application development options)



INF_10503_B

18. Make additional selections in the role services fields as shown in Figure *3-12*, then click **Next** to access the confirmation page.

Figure 3-13. IIS Add Roles and Features Wizard—Confirmation Page



INF_10008_D

19. If desired, scroll down to view installation selections, then click **Install**. (Click **Cancel** to stop installation.)

20. The results screen indicates whether the installation was successful, and lists role services installed. If desired, click the **Print, e-mail, or save** link to print, e-mail or save the installation report, then click **Close** to exit the wizard.

Note:
If installation is unsuccessful, problems that occurred will be shown in the results screen. Resolve the problems and repeat the procedure for adding IIS role services before continuing with the other procedures in this chapter.

3.4 Install Message Queuing

After adding IIS role services, add the Microsoft™* Message Queuing feature. For details on installation, reference the technical document *Installing and Managing Message Queuing*, available online at the following URL:

https://docs.microsoft.com/en-us/previous-versions/windows/it-pro/windows-server-2008-R2-and-2008/cc771474(v=ws.11)

Note:
Installing message queuing is only necessary if configuring the Vital Sync Alarms Reporter Service. See *MSMQ Queue Configuration* on page *6-6* for details.

Note:
Install message queuing on the same systems where IIS role services were just added. (Refer to *Distributed Deployment*, page 5-8, for details on installation in a distributed environment.)

3.5 Configure the IIS Application Pool

After adding IIS role services, update the default Microsoft™* Windows™* Server Internet Information Services (IIS) application pool to ensure that the Informatics Web component (when installed) will have appropriate authority to run reports.

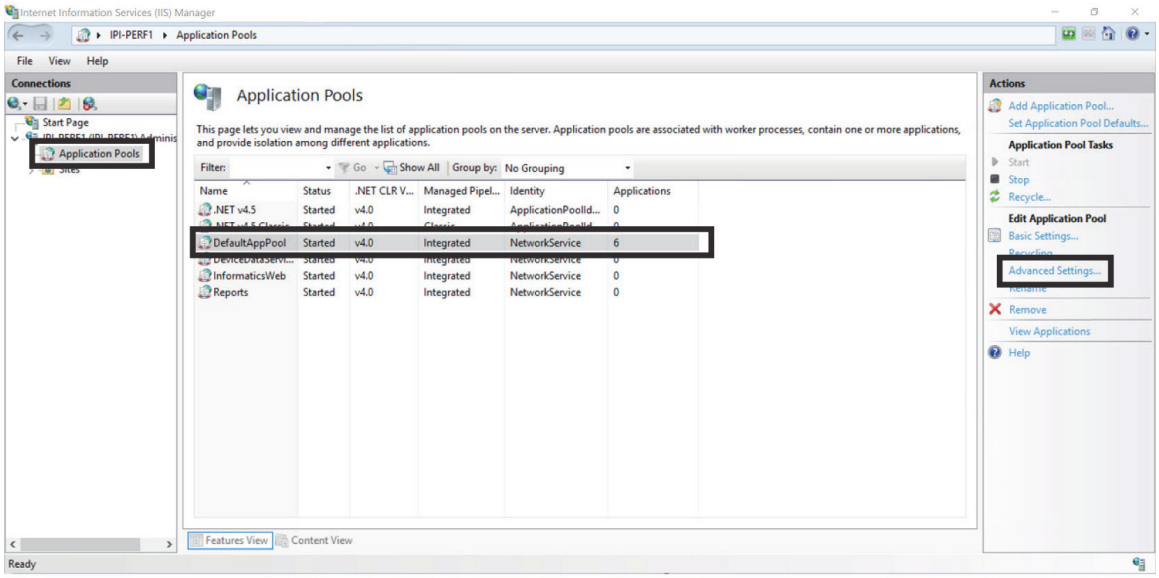
Note:
Configure the IIS application pool on the same systems where IIS role services are installed.

Note:
This manual shows screen captures for application pool configuration using version 10.0 of IIS. Version 8.0 of IIS is also supported. The procedure does not differ significantly between the two versions. If encountering problems during or after configuration, contact Medtronic Professional Services.

To configure the IIS application pool:

1. Open the IIS Manager.

Figure 3-14. Internet Information Services (IIS) Manager (application pools shown)

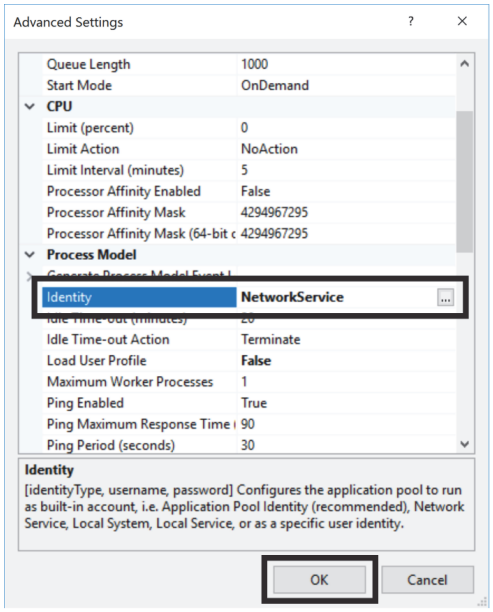


INF_10011_D

2. Click **Application Pools** in the far left pane.

3. Click on **DefaultAppPool** to select it, then click **Advanced Settings** under **Edit Application Pool** in the far right pane to open the Advanced Settings dialog.

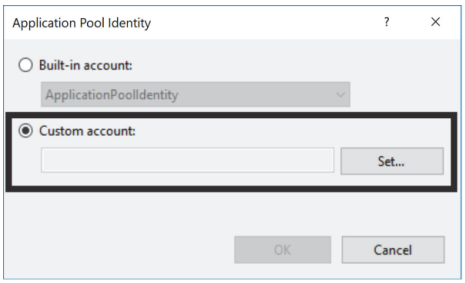
Figure 3-15. Edit Application Pools (Advanced Settings dialog)



INF_10495_B

4. In the **Identity** field, click the **...** button to open the Application Pool Identity dialog.

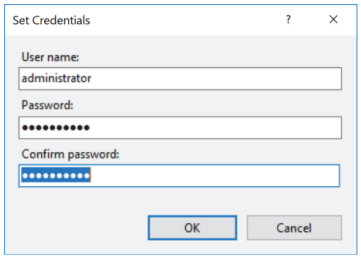
Figure 3-16. Application Pool Identity Dialog



INF_10013_D

5. Click the **Custom account** radio button, then click **Set** to open the Set Credentials dialog.

Figure 3-17. Set Credentials Dialog



INF_10014_D

6. **User name**—Enter the user name for an appropriate administrative user with authority to run reports. Often, the same user will also be set up as the administrator when Microsoft™* SQL Server™* is installed. Refer to *Install the Database Server*, page 3-12.

7. **Password**—Enter the password for the specified administrative user.

8. **Confirm password**—Enter the password just entered in the **Password** field.

9. Click **OK** to save and return to the Application Pool Identity dialog.

10. Click **OK** to save application pool identity settings and return to the Advanced Settings dialog.

11. Click **OK** to save advanced settings for the default application pool and return to the IIS Manager.

12. Exit the IIS Manager.

3.6 Install the Database Server

After configuring the IIS application pool, install and configure the database server software.

The installation wizard shows a series of screens for selection of application options. needing to change a selection already made, click **Back** to go back to the previous screen, then make the change.

In any screen, if needed, click **Cancel** to stop the installation and exit the wizard.

Note:
Install the database server software on the system where the Database component is to be installed. If using a distributed deployment with separate Online Transaction Processing (OLTP) and Data Warehouse systems, install the database server software on both systems.

To access the installation program:

1. Find and right-click on the icon for the computer on the desktop, then click **Explore**, or navigate to the computer in Windows Explorer™*.
2. Double-click on the directory containing the installation files to open the directory.
3. Find **Setup.exe**.

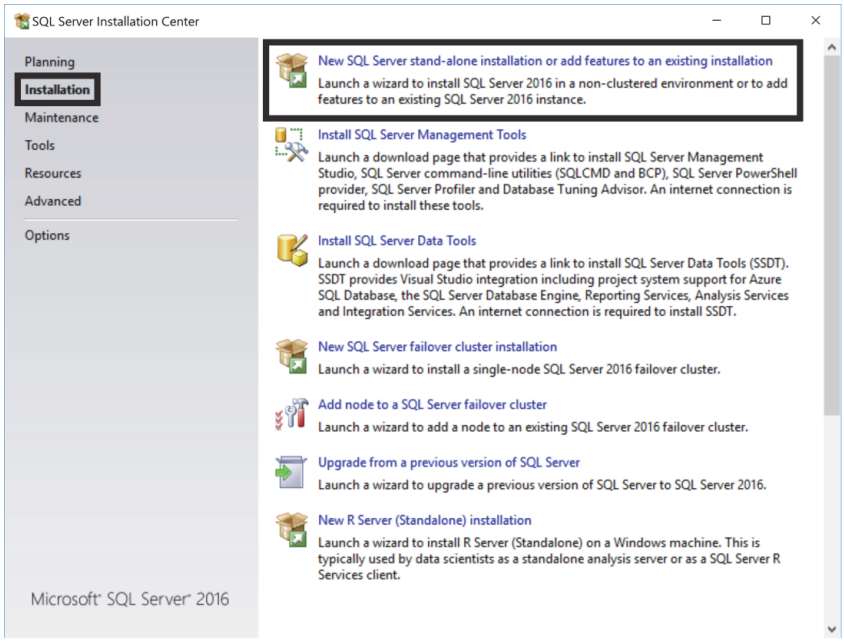
Note:
Refer to *Distributed Deployment*, page 5-8, for details on additional installation and setup steps for distributing database operations across multiple systems.

Note:
This manual shows the installer for Microsoft™* SQL Server™* 2016. Microsoft™* SQL Server™* 2012 is also supported. The installation procedure for Microsoft™* SQL Server™* 2012 does not differ significantly; refer to its installation documentation for more detailed information. If encountering problems during or after installing Microsoft™* SQL Server™*, contact Medtronic Professional Services.

To install Microsoft SQL Server:

1. Double-click **Setup.exe** to run the installer.
2. If a user account control dialog appears asking for confirmation that changes should be made to this computer, click **Yes** to continue. The Installation Center screen will appear, allowing selection of the type of installation to perform.

Figure 3-18. Microsoft™* SQL Server™* Installation Center

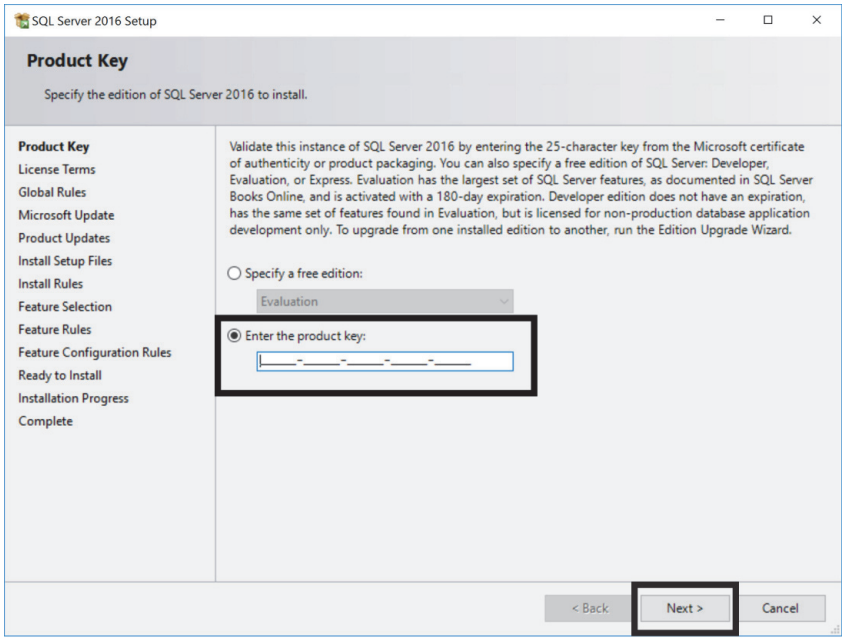


INF_10018_D

3. Click **Installation** in the left panel.

4. Click **New SQL Server stand-alone installation or add features to an existing installation** to open the setup wizard and access the Product Key page.

Figure 3-19. Microsoft™* SQL Server™* Setup Wizard—Product Key Page

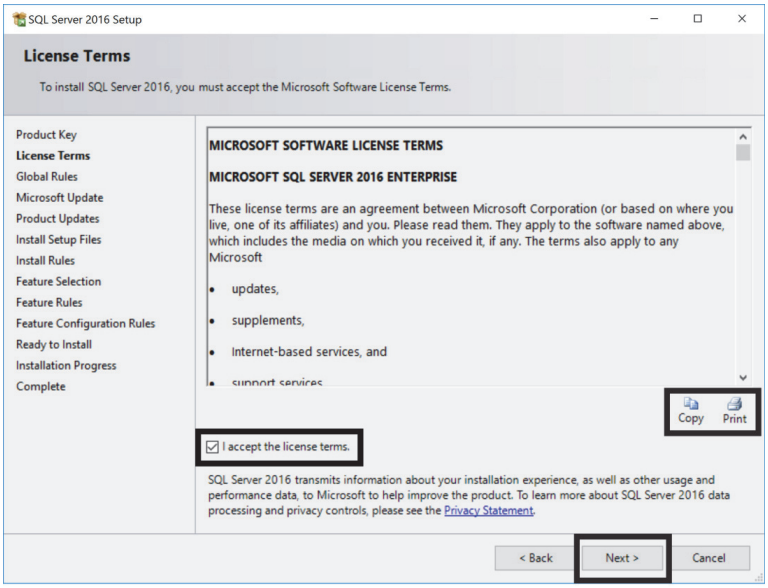


INF_10023_D

5. Click the **Enter the product key** radio button to access the product key field, then (if needed) enter the 25-character product key provided with Microsoft™* SQL Server™*. Click **Next** to proceed to the License Terms page.

Note:
If the software was downloaded directly from the manufacturer, the product key may automatically appear on this page.

Figure 3-20. Microsoft™* SQL Server™* Setup Wizard—License Terms Page



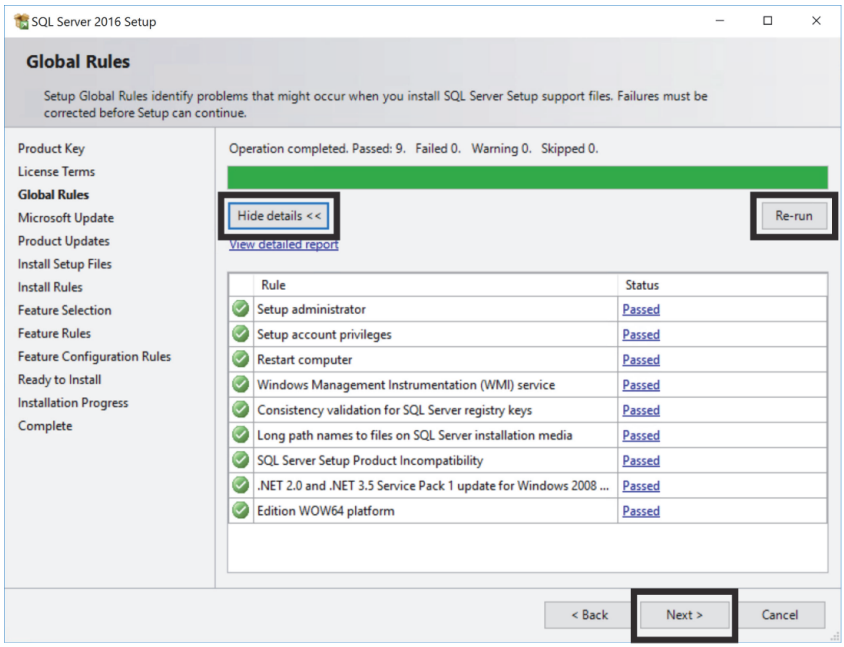
INF_10024_D

6. End-user license agreement (EULA) terms are shown in the License Terms page. If desired, click **Copy** to copy the EULA text to the clipboard; click **Print** to print the EULA.

7. To continue with the installation, click the **I accept the license terms** check box (and the **Send feature usage data** check box if desired), then click **Next** to proceed.

8. The installer will check for problems that could arise from installing support files. A progress bar shows the level of completion of the check.

Figure 3-21. Microsoft™* SQL Server™* Setup Wizard—Global Rules Page (details shown)



INF_10019_D

Click **Show Details** to view a list of items checked; click **Hide Details** to hide the list. If the check indicates problems, resolve them, then click **Re-run**.

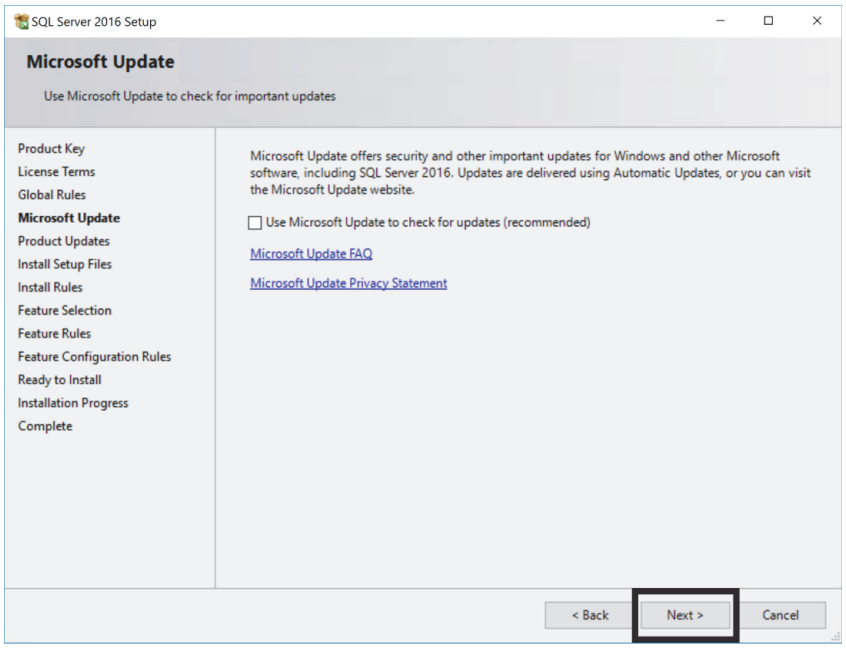
Note:

Users must resolve the underlying cause of any operation indicated as having failed before the installation can proceed.

Users should check the underlying cause of any operation indicated as having a warning, but operations with warnings do not prevent the installation from continuing.

9. The installer will automatically check for any updates, and will automatically download and extract the updates if any are available.

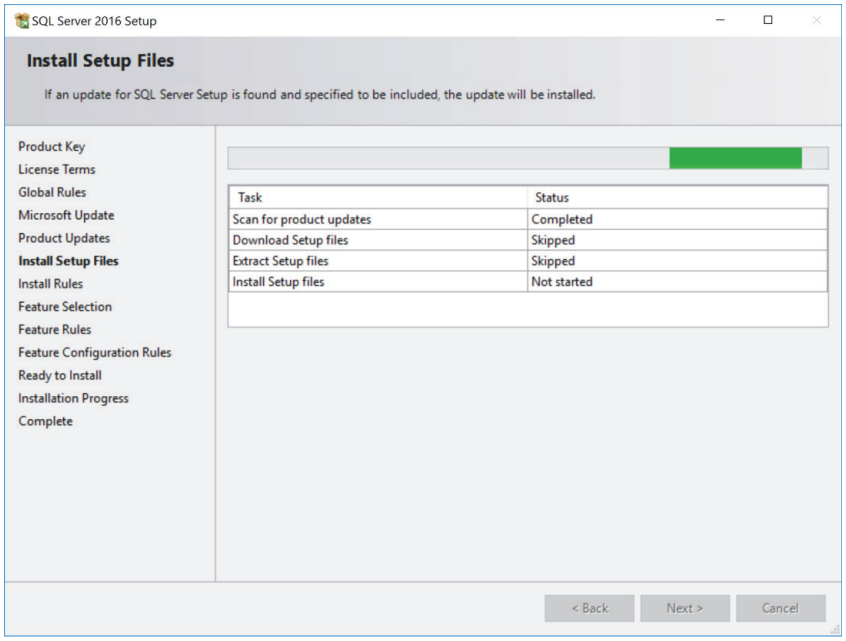
Figure 3-22. Microsoft™* SQL Server™* Setup Wizard—Microsoft™* Update Page (updates shown)



INF_10517_A

10. When the update check is complete, the wizard will proceed to the Product Updates page. If updates are available, a list of the updates downloaded appears on the screen, including links to a document showing more information about each update. If no updates are currently available, a message indicating this will appear. In either case, click **Next** to proceed to the Install Setup Files page.

Figure 3-23. Microsoft™* SQL Server™* Setup Wizard—Install Setup Files Page (details shown)

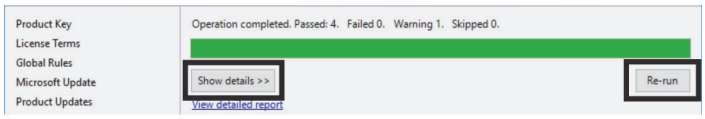


INF_10497_B

11. The installer will automatically install setup files. The status of this operation and the product update operations are shown in the middle of the page.

12. When finished installing setup files, the wizard will proceed to the Install Rules screen and will automatically check for problems that could arise from installing support files. A progress bar shows the level of completion of the check.

Figure 3-24. Microsoft™* SQL Server™* Setup Wizard—Install Rules Page (Details and Re-run buttons)



INF_10178_C

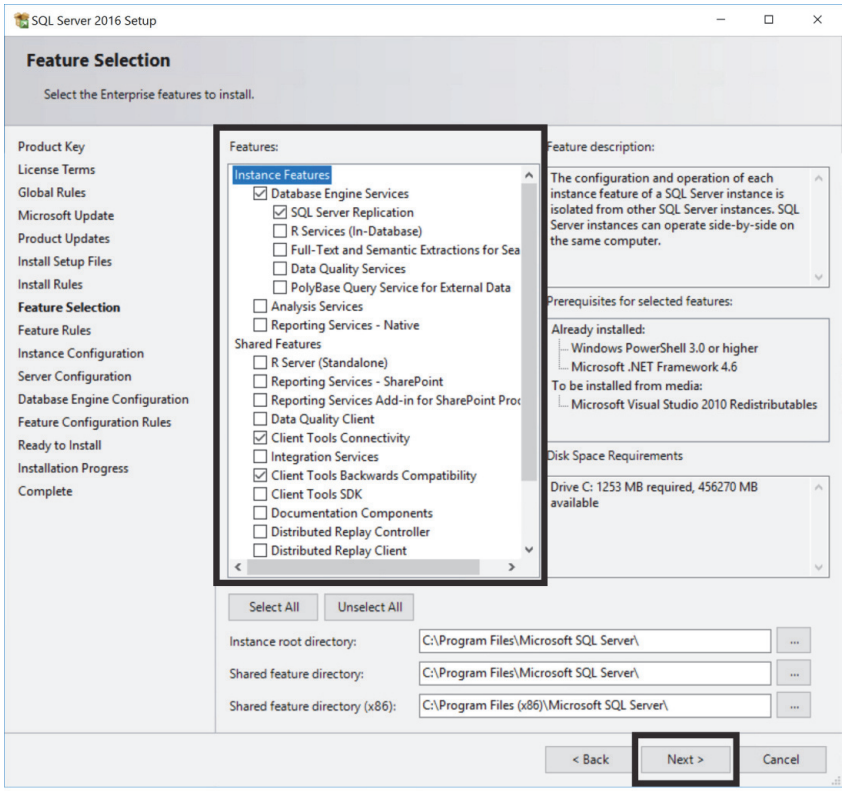
Click **Show Details** to view a list of items checked; click **Hide Details** to hide the list. If the check indicates problems, resolve them, then click **Re-run**.

Note:
Users must resolve the underlying cause of any operation indicated as having failed before the installation can proceed.

Users should check the underlying cause of any operation indicated as having a warning, but operations with warnings do not prevent the installation from continuing.

13. After resolving any problems, or if no problems occur, click **Next** to proceed to the Feature Selection page.

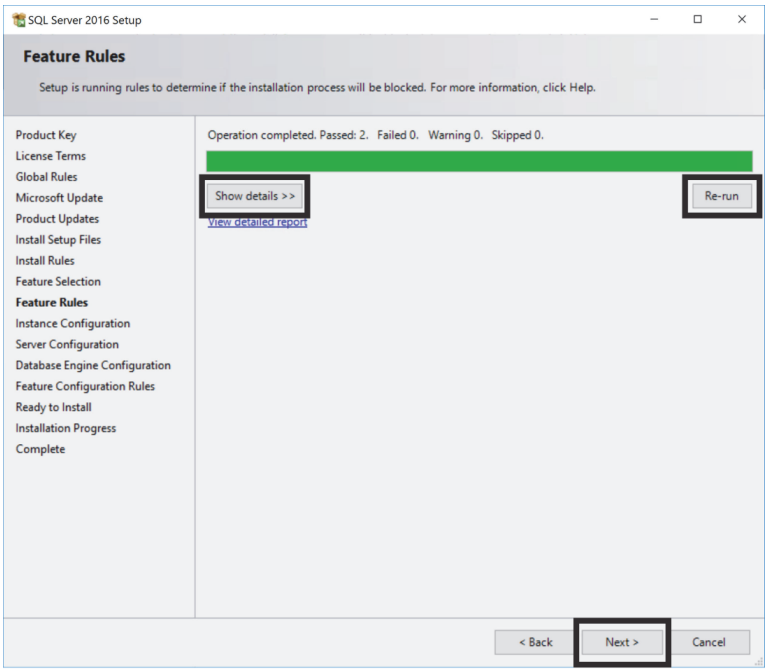
Figure 3-25. Microsoft™* SQL Server™* Setup Wizard—Feature Selection Page



INF_10026_D

14. Make selections in the **Instance Features** and **Shared Features** check boxes as shown in Figure *3-25*, then click **Next** to proceed to the Feature Rules page.

Figure 3-26. Microsoft™* SQL Server™* Setup Wizard—Feature Rules Page



INF_10027_D

15. The installer will again check for problems that could interfere with installation. A progress bar shows the level of completion of the check. Click **Show Details** to view a list of items checked; click **Hide Details** to hide the list.

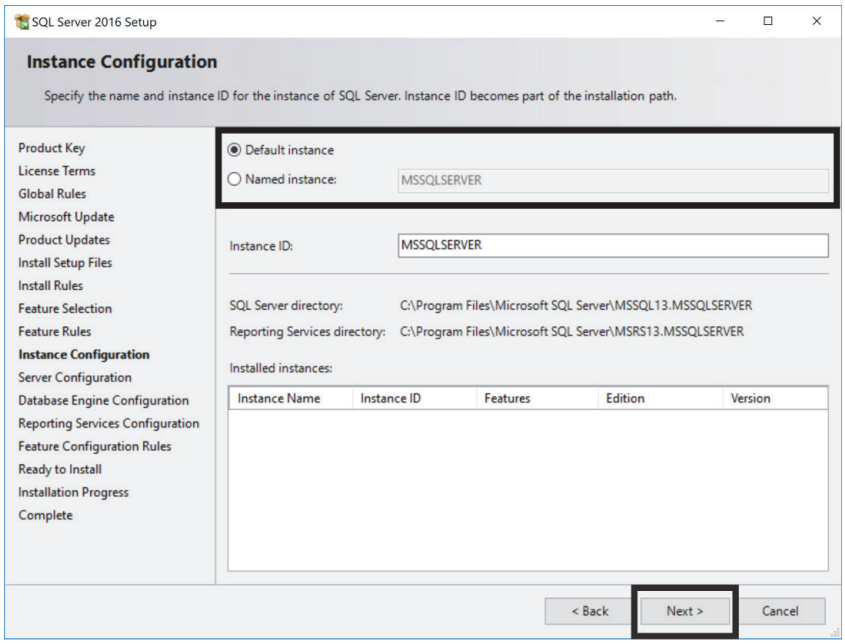
    If the check indicates problems, resolve them, then click **Re-run**.

Note:
Users must resolve the underlying cause of any operation indicated as having failed before the installation can proceed.

Users should check the underlying cause of any operation indicated as having a warning, but operations with warnings do not prevent the installation from continuing.

16. After resolving any problems, click **Next** to proceed to the Instance Configuration page.

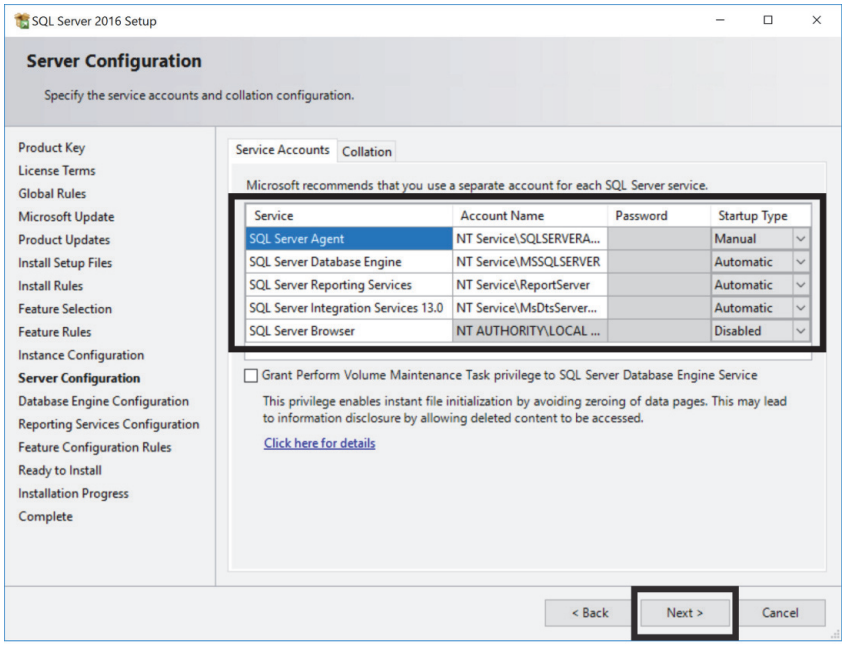
Figure 3-27. Microsoft™* SQL Server™* Setup Wizard—Instance Configuration Page



INF_10028_D

17. If no SQL server instances exist on the system, click the **Default Instance** radio button. Otherwise, click the **Named Instance** radio button and enter a name for the new instance. When ready to continue, click **Next** to proceed to the Server Configuration page.

Figure 3-28. Microsoft™* SQL Server™* Setup Wizard—Server Configuration Page



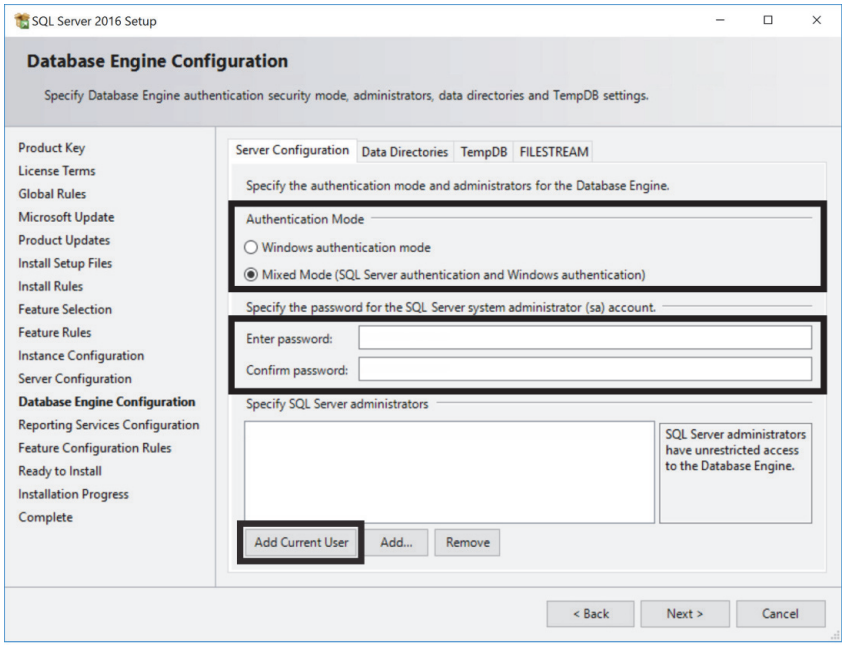
INF_10030_E

18. On the Service Accounts tab, ensure **NT Service\SQLSERVERAGENT** appears in the **Account Name** column for SQL Server Agent, and **NT Service\MSSQLSERVER** appears in the **Account Name** column for SQL Server Database Engine.

19. In the **Startup Type** column, make selections from the appropriate drop-down boxes as shown in Figure *3-28*.

20. Click **Next** to proceed to the Database Engine Configuration page.

Figure 3-29. Microsoft™* SQL Server™* Setup Wizard—Database Engine Configuration Page



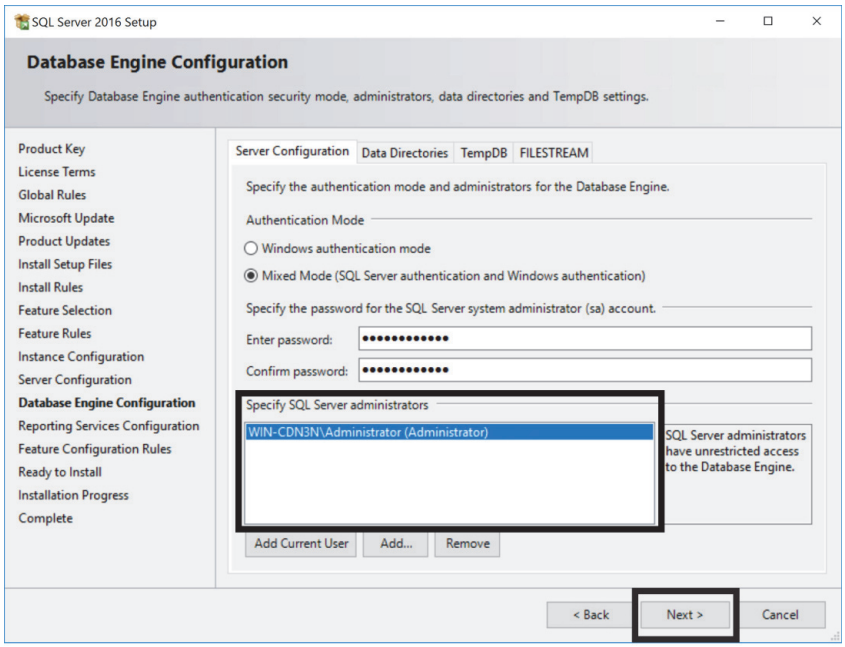
INF_10031_D

21. On the Account Provisioning tab, in the **Authentication Mode** area, click the **Mixed mode** radio button.

22. Enter the desired authentication password in the **Enter password** and **Confirm password** fields.

23. Below the Specify SQL Server Administrators pane, click **Add Current User** to add the current user as an administrator for this SQL server instance. The username of the current user will appear in the pane.

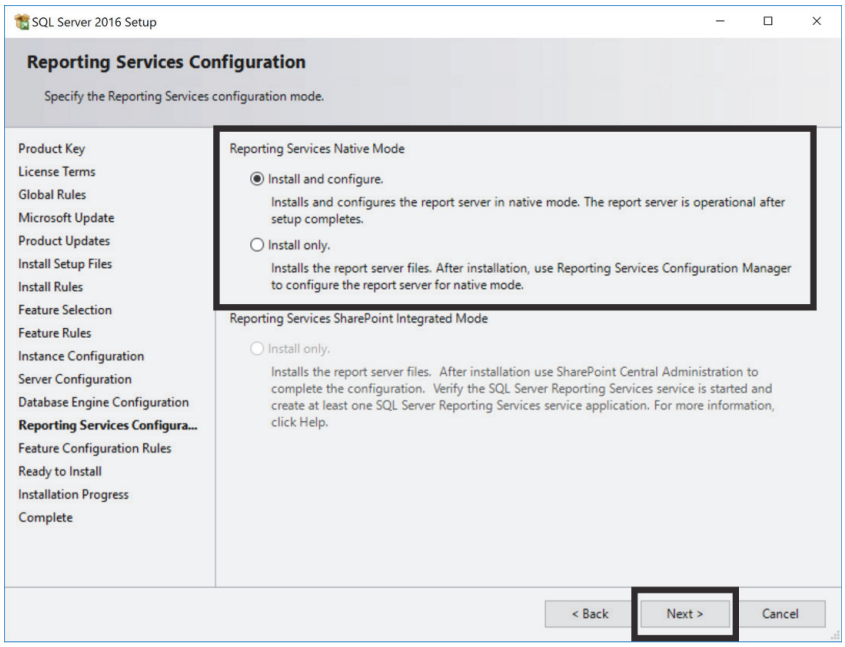
Figure 3-30. Microsoft™* SQL Server™* Setup Wizard—Database Engine Configuration Page (administrator added)



INF_10498_B

24. Click **Next** to proceed to the Reporting Services Configuration page.

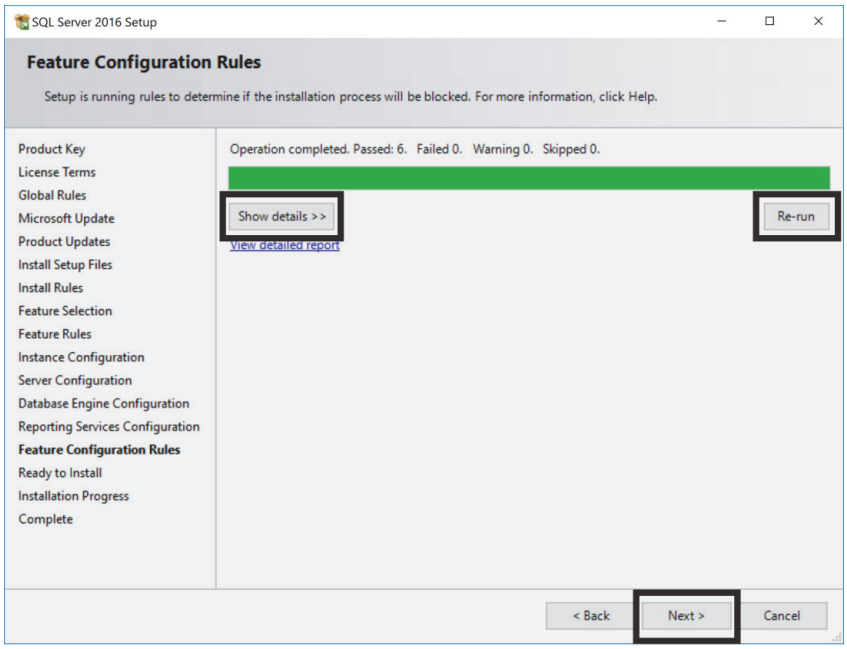
Figure 3-31. Microsoft™* SQL Server™* Setup Wizard—Reporting Services Configuration Page



INF_10512_A

25. If desired, click the check box to send error reports to Microsoft or a corporate server, then click **Next** to proceed to the Feature Configuration Rules page.

Figure 3-32. Microsoft™* SQL Server™* Setup Wizard—Feature Configuration Rules Page



INF_10034_D

26. The installer will once again check for any problems that could interfere with installation. A progress bar shows the level of completion of the check. Click **Show Details** to view a list of items checked; click **Hide Details** to hide the list.

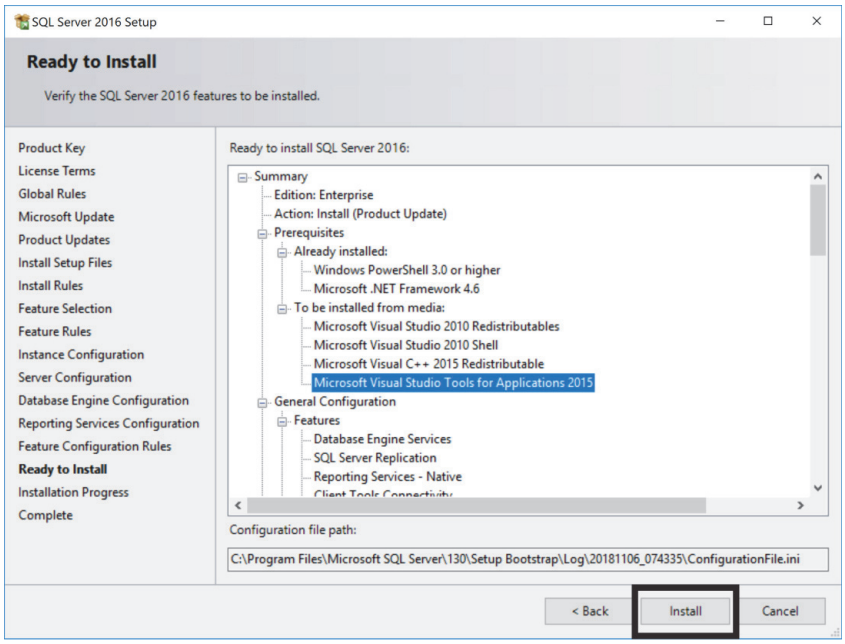
    If the check indicates problems, resolve them, then click **Re-run**.

Note:
Users must resolve the underlying cause of any operation indicated as having failed before the installation can proceed.

Users should check the underlying cause of any operation indicated as having a warning, but operations with warnings do not prevent the installation from continuing.

27. After resolving any problems, click **Next** to proceed to the Ready to Install page.

Figure 3-33. Microsoft™* SQL Server™* Setup Wizard—Ready to Install Page

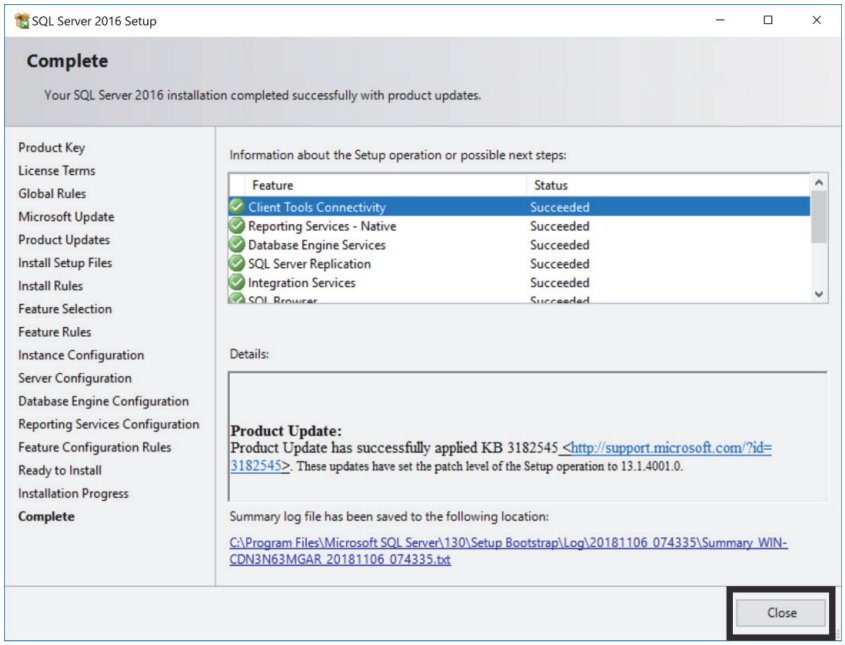


INF_10035_D

28. The Ready to Install page shows all software components to be installed on the destination machine. Review the list if desired, then click **Install**.

29. Once the installer has finished, the finish page will appear.

Figure 3-34. Microsoft™* SQL Server™* Setup Wizard—Finish Page



INF_10036_D

Note:
If no problems occurred during installation, a message indicating successful installation (denoted by a green check mark) will appear. If any problem occurred, a descriptive message (denoted by a red octagon) will appear.

30. After reviewing installation information, click **Close** to exit the installation wizard. (If problems occurred during installation, resolve them, then repeat this procedure until installation is successful.)

31. If desired or otherwise indicated, restart the system before continuing with the additional application installation and configuration procedures detailed in this manual.

3.7 Distributor Configuration

After installing the database server software, configure the database server as a distributor to enable and support replication.

The configuration wizard shows a series of screens for selection of application options. If changes are required to selections already made, click **Back** to go back to the previous screen, then make the change.

In any screen, if needed, click **Cancel** to stop configuration and exit the wizard.

Note:
The default configuration selections indicated here are recommended. If different selections are required, consult with Medtronic Professional Services.

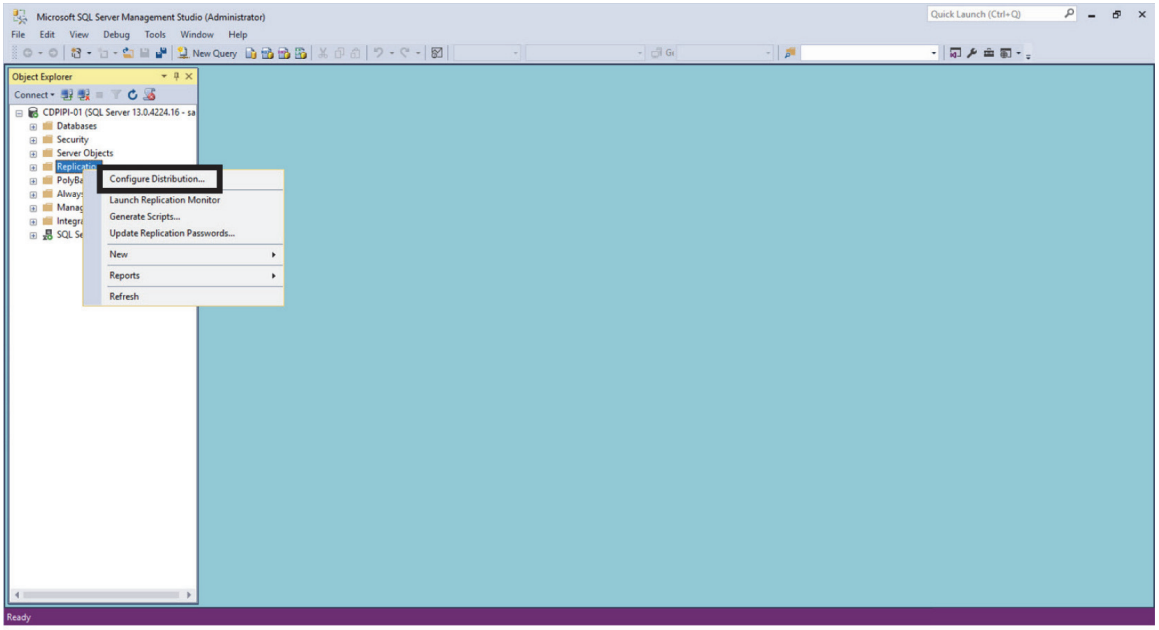
Note:
The procedure shown in this section assumes that Microsoft™* SQL Server™* 2016 is installed. If Microsoft™* SQL Server™* 2012 is installed, the procedure does not differ significantly. If encountering problems, consult with Medtronic Professional Services.

Note:
Server names shown in this section are for illustrative purposes only; actual server names will vary.

To configure the database server as a distributor:

1. In the Object Explorer in Microsoft™* SQL Server™* Management Studio, find the SQL database server installed for use with the Vital Sync™ software.

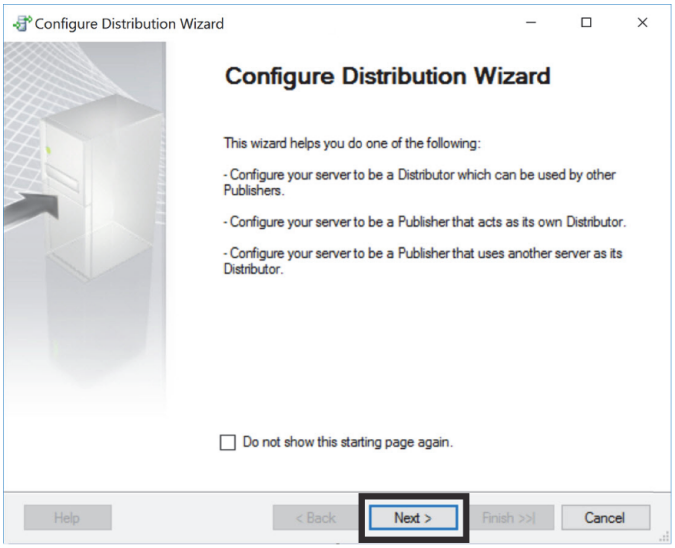
Figure 3-35. Microsoft™* SQL Server™* Management Studio Object Explorer—Replication Folder Context Menu



INF_10039_D

2. Right-click on the **Replication** folder icon to open a context menu, then select **Configure Distribution** to launch the Configure Distribution wizard.

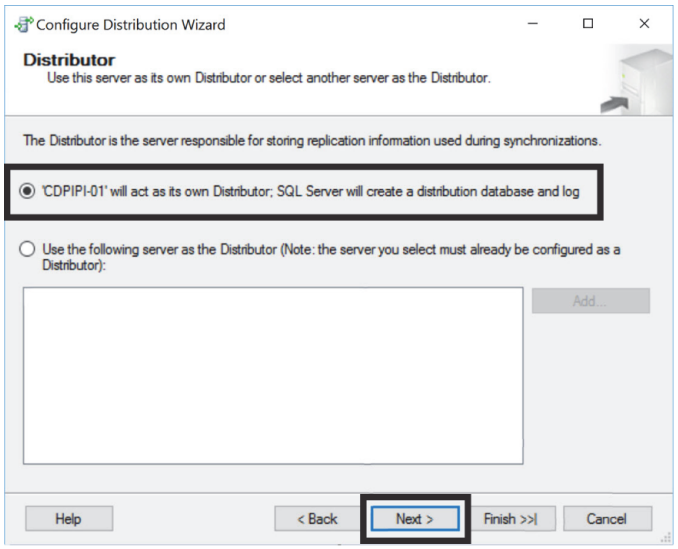
Figure 3-36. Configure Distribution Wizard—Start Page



INF_10363_C

3. Click **Next** to proceed to the Distributor page.

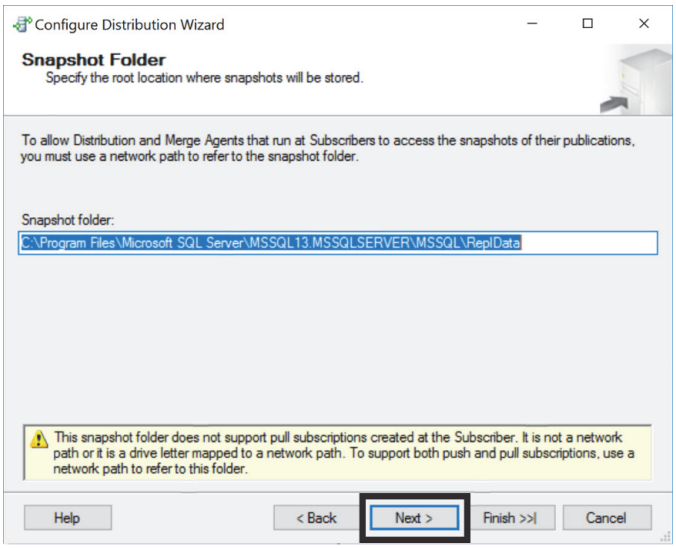
Figure 3-37. Configure Distribution Wizard—Distributor Page



INF_10364_C

4. Make sure the top radio button (indicating that this server will act as its own distributor) is selected, then click **Next** to proceed to the SQL Snapshot Folder page.

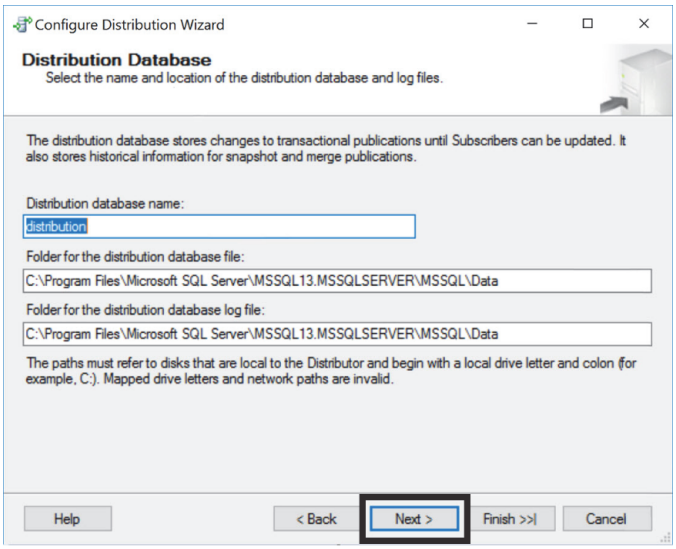
Figure 3-38. Configure Distribution Wizard—Snapshot Folder Page



INF_10366_C

5. Click **Next** to accept the default path for the snapshot folder and proceed to the Distribution Database page.

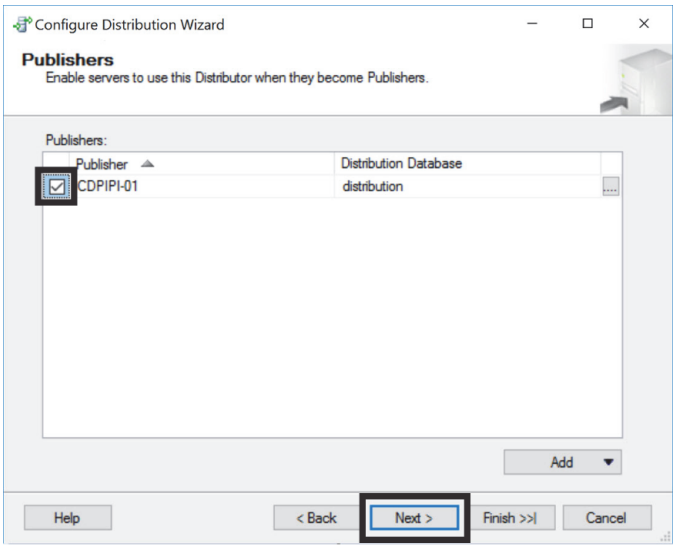
Figure 3-39. Configure Distribution Wizard—Distribution Database Page



INF_10367_C

6. Click **Next** to accept the default distribution database name and default paths for the database and database log files, and proceed to the Publishers page.

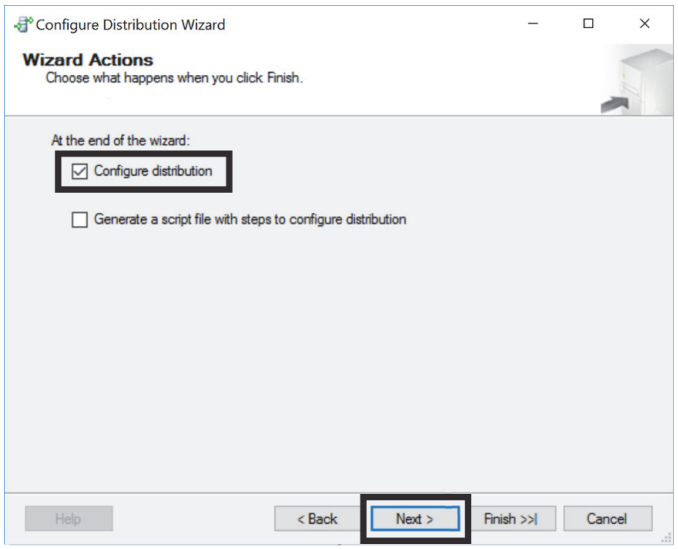
Figure 3-40. Configure Distribution Wizard—Publishers Page



INF_10368_C

7. Make sure the check box next to the database just installed is checked, then click **Next** to proceed to the Wizard Actions page.

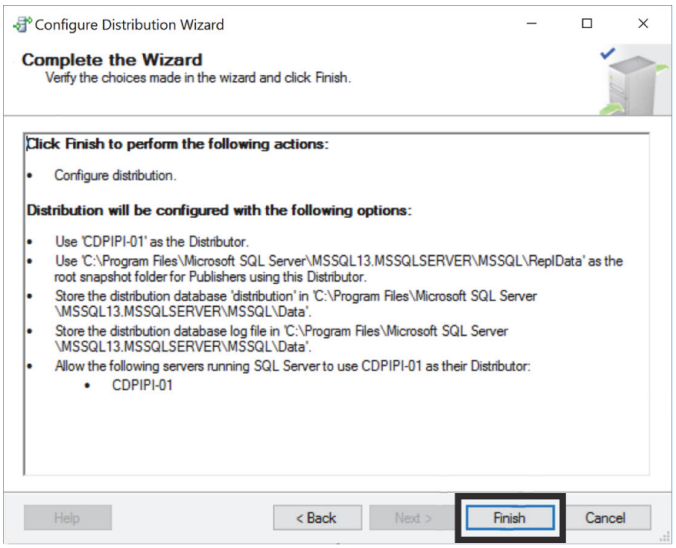
Figure 3-41. Configure Distribution Wizard—Wizard Actions Page



INF_10369_C

8. Make sure the **Configure distribution** check box is checked, then click **Next** to proceed to the finish page.

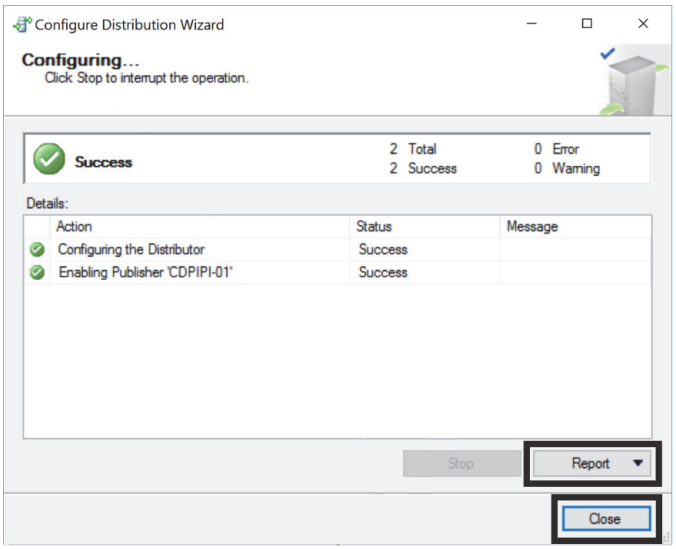
Figure 3-42. Configure Distribution Wizard—Finish Page



INF_10370_C

9. Review selections, then click **Finish** to configure distribution.

Figure 3-43. Configure Distribution Wizard—End Page



INF_10371_C

10. A screen indicating progress will appear; green check marks indicate success of each operation. If any problems occur during configuration, click **Report** to view details, then resolve any issues and rerun the wizard.

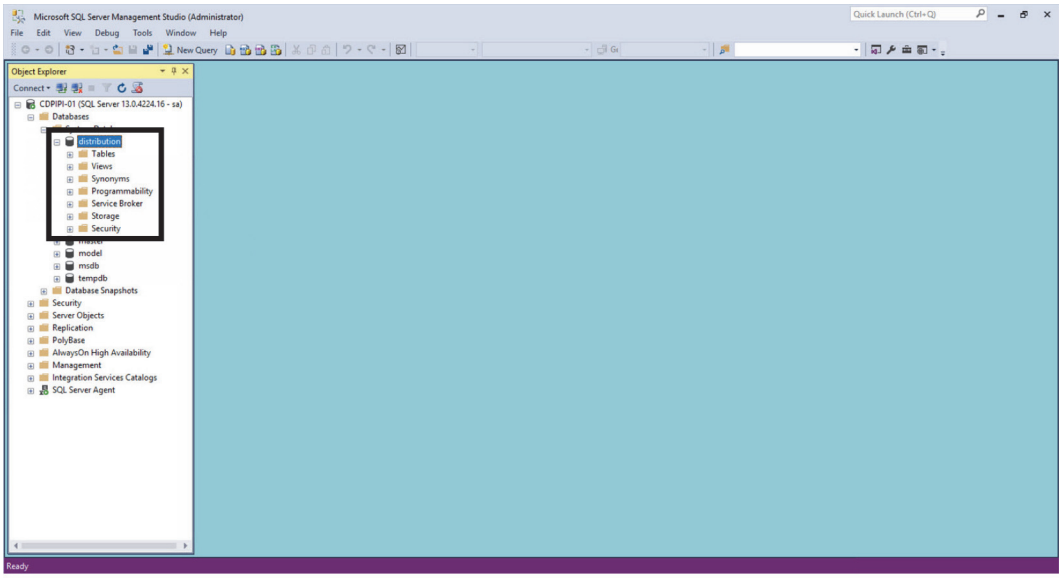
11. If no problems occur, or once problems are resolved and rerunning the wizard indicates success for all configuration operations, click **Close** to exit the wizard.

Note:

If configuration is unsuccessful, it is possible the SQL Server Agent is not set to automatically launch. Check the status of the SQL Server Agent in the SQL Server Configuration Manager; ensure that the agent is running and set to Automatic. Refer to *Enable Remote Connection*, page 3-30, for access details.

On completion of distributor configuration, a new database icon will be visible in the System Databases list in the Microsoft™* SQL Server™* Management Studio Object Explorer. This icon will have the name selected in the distribution database setup screen (refer to step 6 of this procedure).

Figure 3-44. Microsoft™* SQL Server™* Management Studio Object Explorer (new database shown)



INF_10372_C

3.8 Enable Remote Connection

After installing all supporting software and application components, adjust the database configuration to enable remote users to connect to the database.

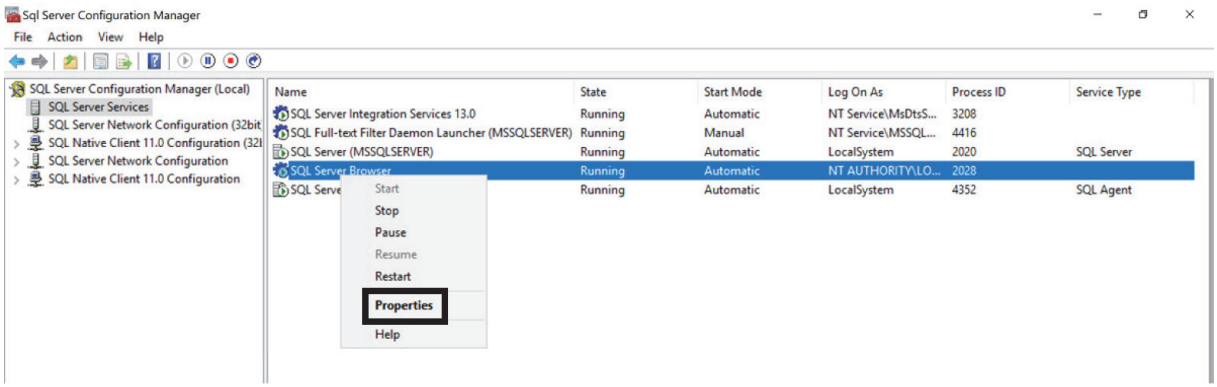
Note:
Only perform the steps listed in this section if application components are installed on multiple systems. If using a distributed deployment with separate Online Transaction Processing (OLTP) and Data Warehouse systems, perform the steps in this section on both systems.

Note:
The procedure shown in this section assumes that Microsoft™* SQL Server™* 2016 is installed. If Microsoft™* SQL Server™* 2012 is installed, the procedure does not differ significantly. If encountering problems, consult with Medtronic Professional Services.

To enable remote connection:

1. Launch the SQL Server Configuration Manager.
2. In the left pane, click on **SQL Server Services**.
3. Right-click on **SQL Server Browser** (in the right pane) to open a context menu.

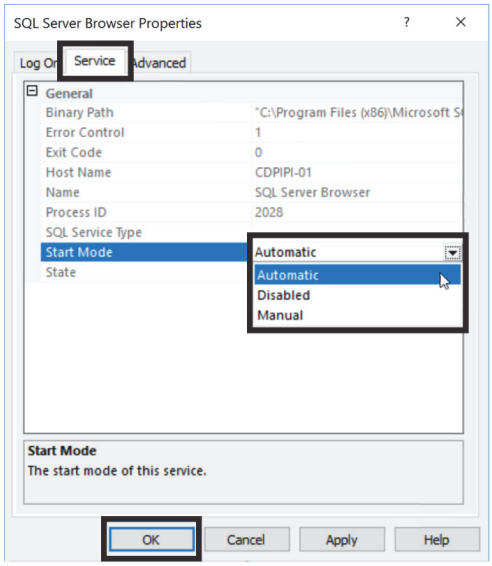
Figure 3-45. Microsoft™* SQL Server™* Configuration Manager—SQL Server Browser Context Menu



INF_10065_D

4. Select **Properties** to open the Properties window.

Figure 3-46. Microsoft™* SQL Server™* Configuration Manager—SQL Server Browser Properties Dialog



INF_10066_D

5. Click on the **Service** tab to access it.

6. Click on the drop-down box next to **Start Mode** and select **Automatic**.

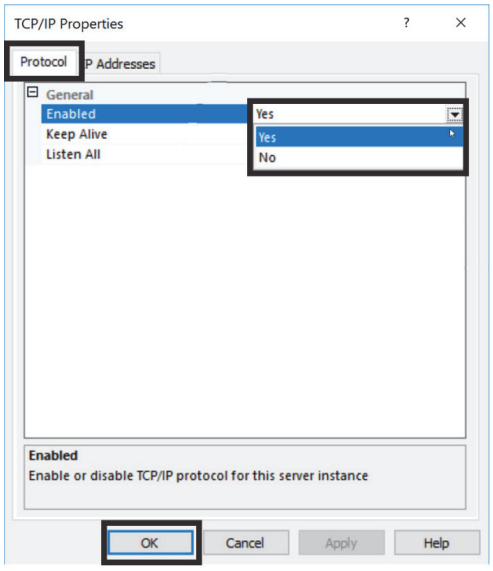
7. Click **OK** to exit the Properties window and return to the SQL Server Configuration Manager window. In the right pane, the value in the **State** column for the SQL Server Browser should be **Running**.

8. In the left pane, click on the triangle next to the **SQL Server Network Configuration** icon to expand the directory, then click on **Protocols for MSSQLSERVER** (or the server and instance name selected for the database during installation, if different) to show protocols in the right pane.

9. Check the value in the **Status** column in the right pane for the TCP/IP protocol. If not set to **Enabled**, right-click on **TCP/IP** to open a context menu.

10. Select **Properties** to open the Properties window.

Figure 3-47. Microsoft™* SQL Server™* Configuration Manager—TCP/IP Properties Dialog



INF_10067_D

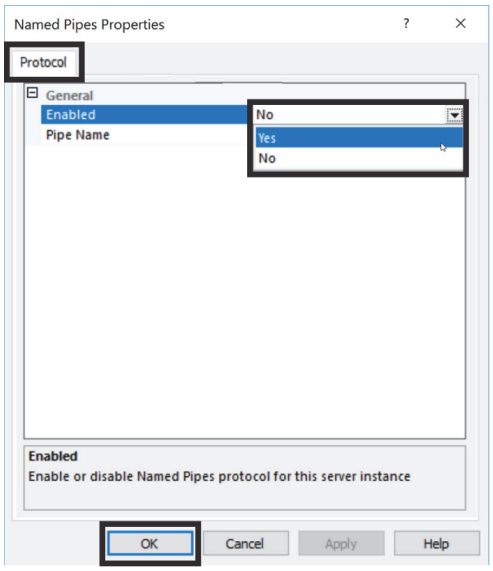
11. Click on the drop-down box next to **Enabled** and select **Yes**.

12. Click **OK** to return to the SQL Server Configuration Manager window.

13. Check the value in the **Status** column in the right pane for the Named Pipes protocol. If not set to **Enabled**, right-click on **Named Pipes** to open a context menu.

14. Select **Properties** to open the Properties window.

Figure 3-48. Microsoft™* SQL Server™* Configuration Manager—Named Pipes Properties Dialog



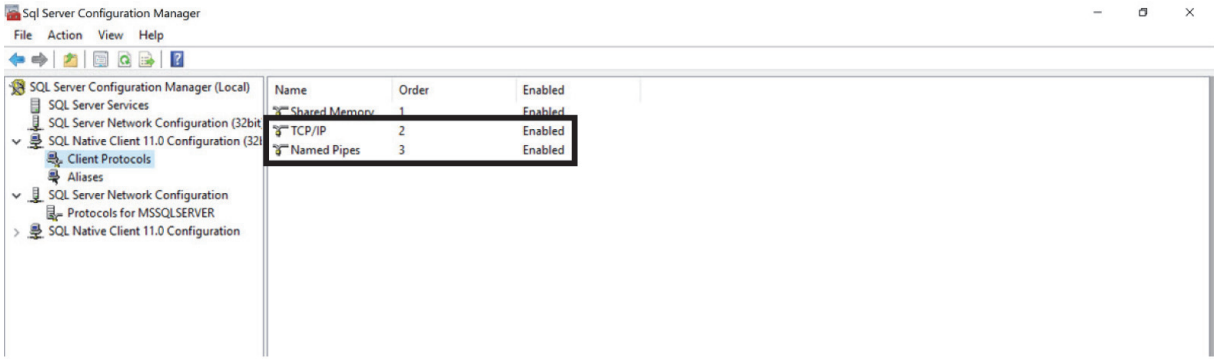
INF_10068_D

15. Click on the drop-down box next to **Enabled** and select **Yes**.

16. Click **OK** to return to the SQL Server Configuration Manager window.

17. In the left pane, click on the plus sign next to the **SQL Native Client 11.0 Configuration (32bit)** icon to expand the directory if needed, then click on **Client Protocols** to show protocols in the right pane.

Figure 3-49. Microsoft™* SQL Server™* Configuration Manager—Native Client 11.0 (32-Bit) Client Protocols



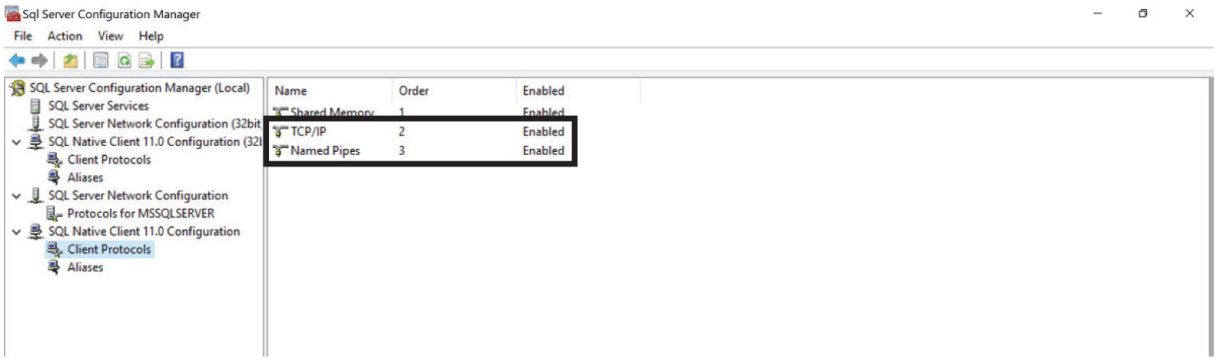
INF_10069_D

18. Ensure the value in the **Enabled** column both for TCP/IP and for Named Pipes is **Enabled**. If not, apply steps 9 through 15 of this procedure as needed to change affected items.

19. A warning dialog will appear indicating that the client protocol changes will be saved, but will not take effect until affected services are restarted. Click **OK** to save changes and return to the SQL Services Configuration Manager window.

20. In the left pane, click on the triangle next to the **SQL Native Client 11.0 Configuration** icon to expand the directory if needed, then click on **Client Protocols** to show protocols in the right pane.

Figure 3-50. Microsoft™* SQL Server™* Configuration Manager—Native Client 11.0 Client Protocols



INF_10070_D

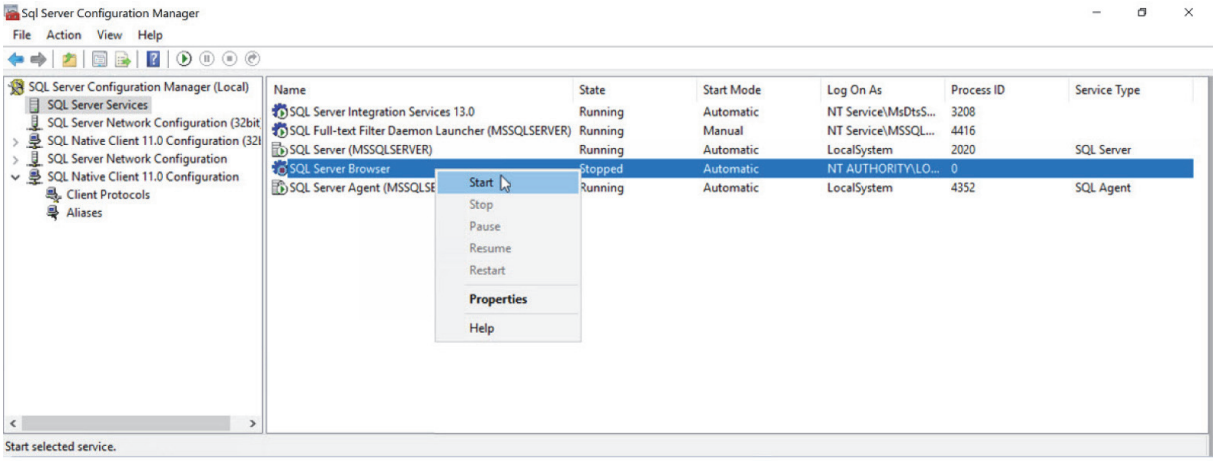
21. Ensure the value in the **Enabled** column both for TCP/IP and for Named Pipes is **Enabled**. If not, apply steps 9 through 15 of this procedure as needed to change affected items.

22. A warning dialog will appear indicating that the client protocol changes will be saved, but will not take effect until affected services are restarted. Click **OK** to save changes and return to the SQL Services Configuration Manager window.

23. In the left pane, click on **SQL Server Services**.

24. In the right pane, the value in the **State** column for the SQL Server Browser should be **Stopped**. Right-click on **SQL Server Browser** to open a context menu.

Figure 3-51. Microsoft™* SQL Server™* Configuration Manager—SQL Server Browser Start

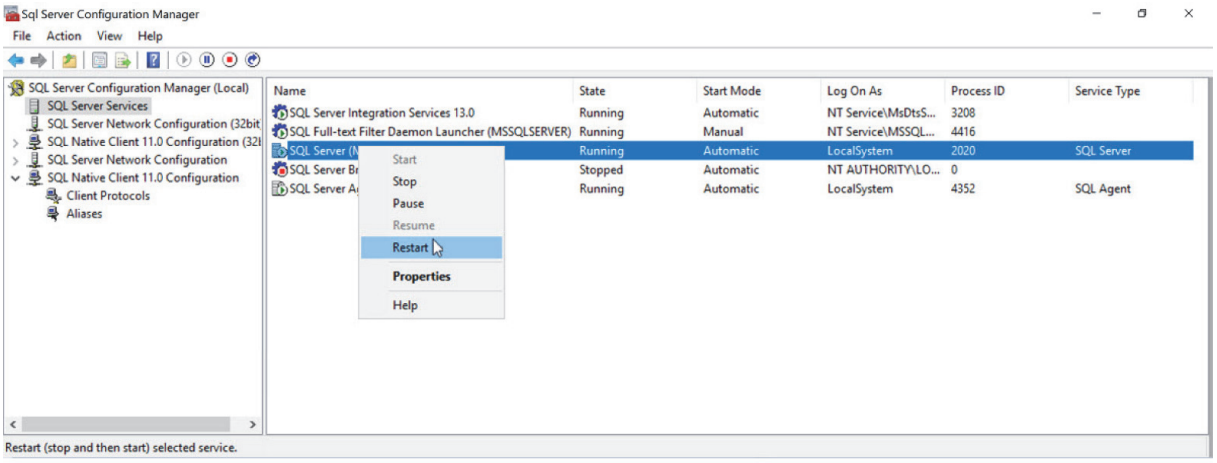


INF_10071_D

25. Select **Start** to start the SQL Server Browser running.

26. Right-click on **SQL Server (MSSQLSERVER)** (or if different, the server and instance name selected during installation) to open a context menu.

Figure 3-52. Microsoft™* SQL Server™* Configuration Manager—SQL Server Restart

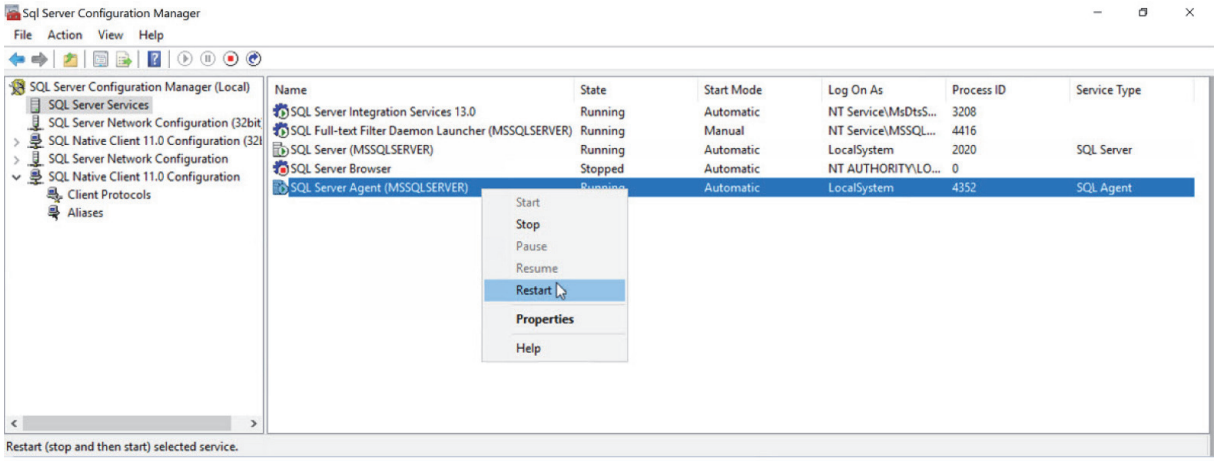


INF_10072_D

27. Select **Restart** to restart the SQL server service, with the configuration changes made.

28. Right-click on **SQL Server Agent (MSSQLSERVER)** (or if different, the server and instance name selected for the database during installation) to open a context menu.

Figure 3-53. Microsoft™* SQL Server™* Configuration Manager—SQL Server Agent Restart



INF_10073_D

29. Select **Restart** to restart the SQL server agent, with the configuration changes made.

Page Left Intentionally Blank

4 Installing Software Components

4.1 Overview

This chapter provides information on installation of components of the Vital Sync™ virtual patient monitoring platform and informatics manager software.

Note:
While all components can be installed on a single system, Medtronic recommends that the Informatics Web and Database components should be installed on separate systems, especially if a large number of users will access and use the software, or if a large number of patients and devices will be connected and monitored. Reference hardware and software configurations in Chapter 2, or consult with Medtronic Professional Services or with facility IT personnel for more information.

Note:
If upgrading from a previous version, make backups of all database files before installing the current version of the software.

Note:
If upgrading from a version of the software previous to v2.5.x, uninstall the older version before installing the current version.

If upgrading from version 2.5.x, to avoid potential problems with database functions, first upgrade to version 2.6.x before upgrading to version 2.7.0.

4.2 Installation

All components are included in the Vital Sync™ software installation package, received from Medtronic Professional Services.

Note:
To install software, administrative rights are required on destination systems.

4.2.1 Component Constraints

Certain components must be installed on specific systems, based on the supporting software installed on those systems.

- Install the Database component on a system where Microsoft™* SQL Server™* is already installed.
- Install the Data Collection Service, Applet Manager Service (if used), Reports, and Informatics Web components on the same system where Microsoft™* Windows™* Server IIS role service and application pool setup is already complete.

Reference Chapter 3 for more information on supporting software. Reference Chapter 5 for more information on multi-system installation.

4.2.2 Access

To access the installer:

1. Find and right-click on the icon for the computer on the desktop, then click **Explore**, or navigate to the computer in Windows™* Explorer™*.
2. Navigate to the following location in the directory where the installation files reside: **Installers\Virtual Patient Monitoring Platform**
3. Find **informatics_setup.exe**.

4.2.3 Component Installation

The installation wizard shows a series of screens for selection of software options. If needing to change a selection already made, click **Back** to go back to the previous screen and make the change.

In any screen, if needed, click **Cancel** to stop the installation and exit the wizard.

To install components:

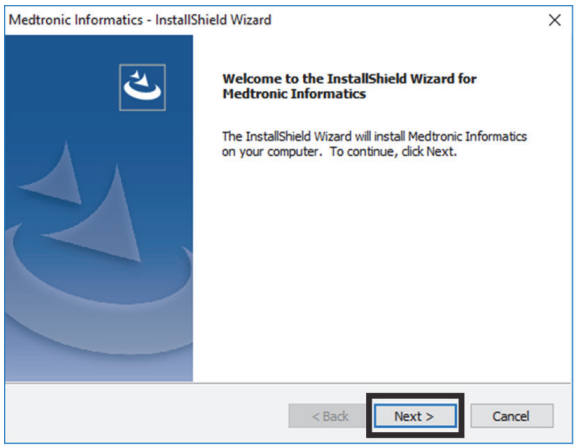
1. Double-click **Informatics_setup.exe** to run the installer.
2. If a dialog appears asking for confirmation that changes should be made to this computer, click **Yes** to continue.
3. If Microsoft™* .NET Framework 4.6.2 is not present on the system, the Requirements page will appear. Click **Install** to install the missing software, entering administrative user credentials if necessary to confirm the installation. (Click **Cancel** to exit the installation wizard.)

Note:
The Microsoft™* Web Deploy utility is installed along with the Vital Sync™ software components.

4. The system may need to be rebooted before continuing. If so, log onto the system after rebooting, using the same credentials. The installation wizard should automatically start again; if not, restart the wizard (see *Access* on page *4-2*).

5. Once all necessary supporting software is installed on the system, the Welcome page will appear.

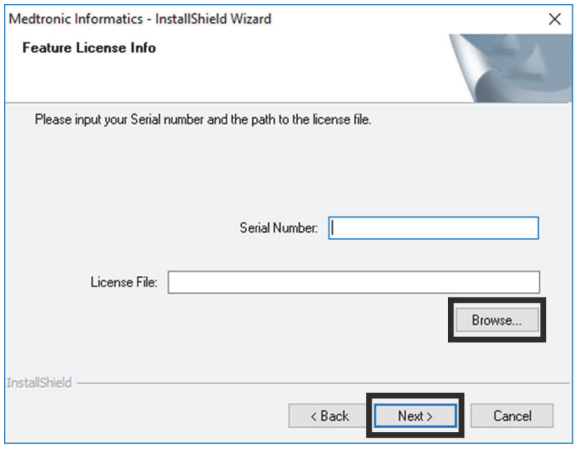
Figure 4-1. Informatics Installation Wizard—Welcome Page



INF_10373_C

6. Click **Next** to proceed to the Feature License Information page.

Figure 4-2. Informatics Installation Wizard—Feature License Information Page



INF_10305_D

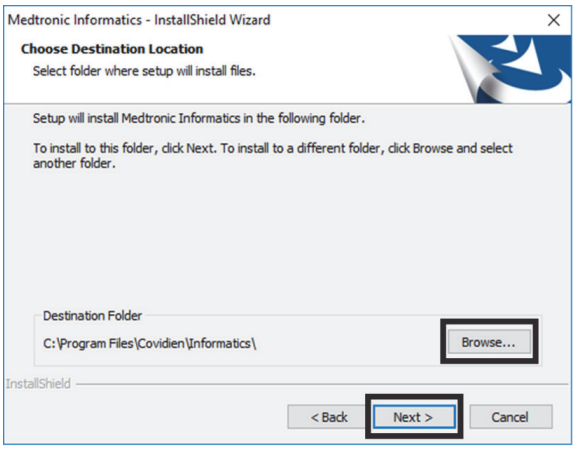
7. **Serial Number**—Enter the license key received from Medtronic Professional Services.

8. **License File**—Enter the filename of the license file received from Medtronic, or click **Browse...** and navigate to the directory where the license file resides. The license file has a **.lic** file extension, and will typically have the license key as its filename.

Note:
The license file is provided directly by Medtronic Professional Services, separately from the other installation files.

9. Click **Next** to proceed to the Destination Location page.

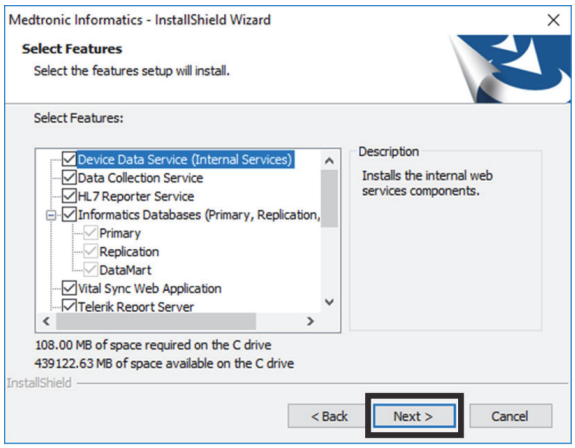
Figure 4-3. Informatics Installation Wizard—Destination Location Page



INF_10374_C

10. The Destination Location page shows the default destination location for installation of software components. If the components should be installed in a different location, click **Browse** and navigate to the desired location. When finished, or if accepting the default location, click **Next** to proceed to the Select Features page.

Figure 4-4. Informatics Installation Wizard—Select Features Page



INF_10375_C

11. The Select Features page shows available components, as well as the amount of disk space required to install selected components (currently selected components are denoted by checked boxes). Click on any component listed to show a brief description of that component in the **Description** pane.

Note:
If installing on multiple systems, some components must be installed on specific systems. Refer to *Component Constraints*, page 4-2, and *Distributed Deployment*, page 5-8.

Note:
Depending on the licensing status of components in the installation package, not all screens shown in this procedure description may appear. For details on licensing of individual components, consult with Medtronic.

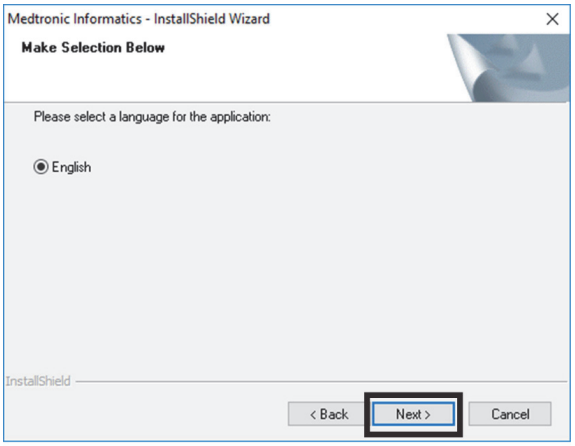
12. Click in check boxes to check or uncheck them until all components to be installed are selected (indicated by a checked box).

Note:
If a component is not currently licensed, its check box will be unchecked when this page first appears. The description will still appear when clicking an unlicensed component, but will indicate that the component is unlicensed; the component's check box for selection will be unavailable.

Note:
The Nurse Station Client component and the Bedside Station Client component cannot be installed simultaneously. If installing either of these components, make sure the check box for the other component is unchecked before proceeding.

13. Click **Next** to proceed to the Language Options page.

Figure 4-5. Informatics Installation Wizard—Language Options Page

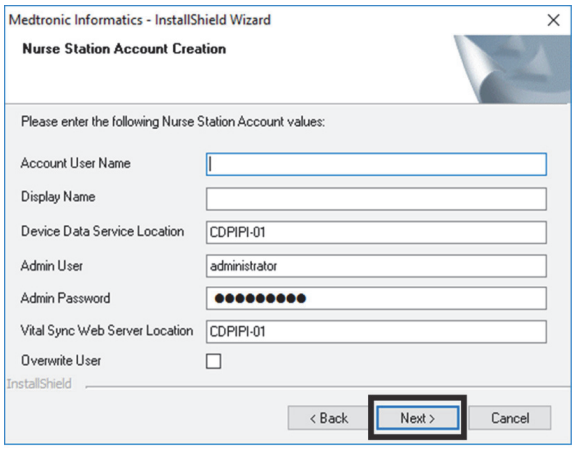


INF_10513_A

14. English is the only language available to be shown in the software user interface, and is already selected. Click **Next** to proceed.

15. If creating an account for a central nurse station (as chosen in step *12*), the Nurse Station Account Creation page will appear. (If not creating this account, skip to step *24*. If not creating a central nurse station account or a bedside display user account, the Failover Log File page will appear; skip to step *33*.)

Figure 4-6. Informatics Installation Wizard—Nurse Station Account Creation Page



INF_10279_E

16. **Account User Name**—Enter the username of the nurse station account (this can be the name of the nurse station at which the platform is to be used).

17. **Display Name**—Enter the display name for the nurse station. (This name will appear on the user function button in the platform user interface.)

Note:
The display name should be as short as is practical; space on the user function button is limited.

18. **Device Data Service Location**—Enter the host name or IP address for the system on which the Device Data Service component is to be installed.

19. **Admin User**—Accept the default value (**administrator**).

20. **Admin Password**—Accept the default value, or enter a password conforming to facility guidelines.

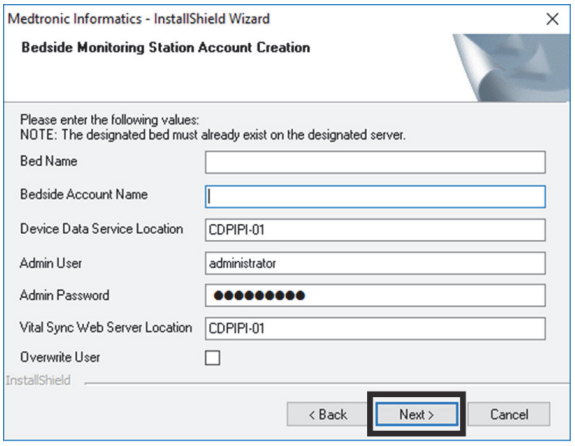
21. **Vital Sync Web Server Location**—Enter the host name or IP address for the system on which the Vital Sync Web Server component is to be installed.

22. **Overwrite User**—Accept the default value (unchecked) to create a new account, or check the box to overwrite an existing central nurse station account (also called a remote monitoring station account in earlier releases of the software).

23. Click **Next** to proceed.

24. If creating an account for a bedside display user, the Bedside Monitoring Station Account Creation page will appear. (If not creating this account, skip to step *33*.)

Figure 4-7. Informatics Installation Wizard—Bedside Monitoring Station Account Creation Page



INF_10377_C

25. **Bed Name**—Enter the name of the bed at which the bedside display is to be used.

26. **Bedside Account Name**—Enter the name for the bedside account. (This name will appear in the platform user interface.)

27. **Device Data Service Location**—Enter the hostname or IP address for the system on which the Informatics Web component is to be installed.

28. **Admin User**—Accept the default value (**administrator**).

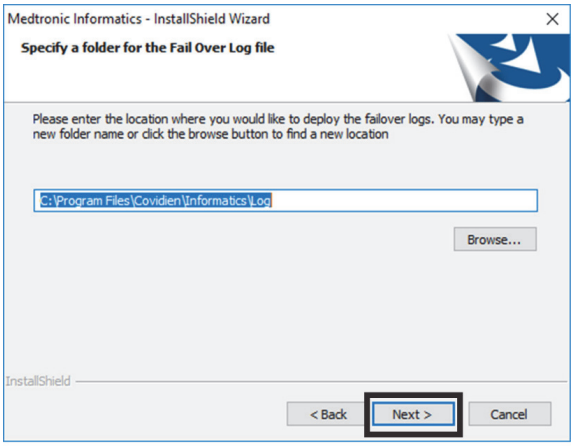
29. **Admin Password**—Accept the default value, or enter a password conforming to facility guidelines.

30. **Vital Sync Web Server Location**—Enter the hostname or IP address for the system on which the Informatics Web component is to be installed.

31. **Overwrite User**—Accept the default value (unchecked) to create a new account, or check the box to overwrite an existing bedside monitoring station account.

32. Click **Next** to proceed to the Failover Log File page.

Figure 4-8. Informatics Installation Wizard—Failover Log File Page

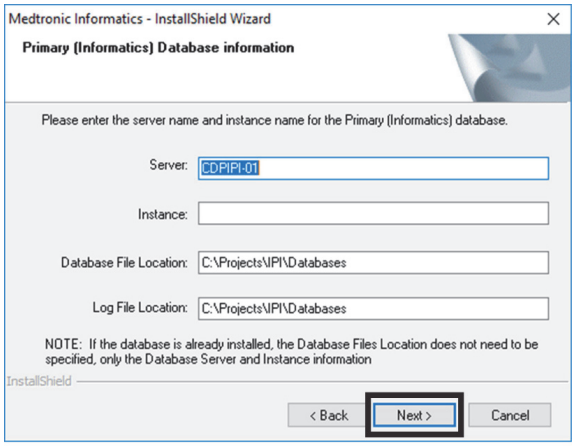


INF_10376_C

33. The default location for the failover log file (the file in which the software will record events if the regular event log is inaccessible) is shown. If desired, enter an alternate directory path, or click **Browse** and navigate to the desired directory. When finished, or if accepting the default location, click **Next** to proceed.

34. If the selected destination folder for the failover log file does not exist, a dialog will appear asking if the folder should be created. Click **Yes** to create the folder and proceed to the Primary (Informatics) Database Information page, or click **No** to return to the failover log location screen to select an existing folder, then click **Next** to proceed.

Figure 4-9. Informatics Installation Wizard—Primary (Informatics) Database Information Page



INF_10054_F

35. **Server**—Enter the server name for the SQL server instance that will support primary clinical and supervisory operations. (Use the server name selected during SQL server software installation on the system where the SQL server instance that supports operations is installed. Reference *Install the Database Server*, step *17*.)

Note:
If using distributed deployment, with a dedicated Online Transaction Processing (OLTP) system supporting primary clinical and supervisory operations, enter information for the SQL server instance on the OLTP system into the fields on the Operations Database Information page. Refer to *Distributed Deployment*, page 5-8.

Note:
Network configuration settings may require an IP address to be used instead of a server name alone. If so, append the IP address after the server name, separating them with an @ sign (e.g., ServerName@100.12.15.88). If needed, consult with facility IT personnel to obtain the IP address of the system where the SQL server instance is installed.

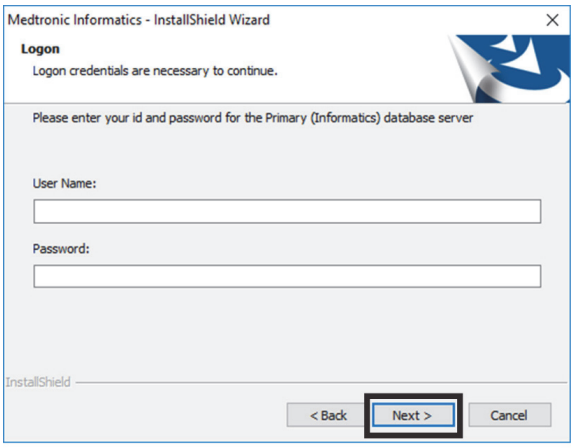
36. **Instance**—If using the default instance, leave this field blank. If not using the default instance, enter the instance name for the instance to be used.

37. **Database File Location**—If not using the default directory path, enter the desired directory path for the database file.

38. **Log File Location**—If not using the default directory path, enter the desired directory path for the log file.

39. When finished, click **Next** to proceed to the Primary (Informatics) logon information page.

Figure 4-10. Informatics Installation Wizard—Primary (Informatics) Logon Information Page



INF_10306_D

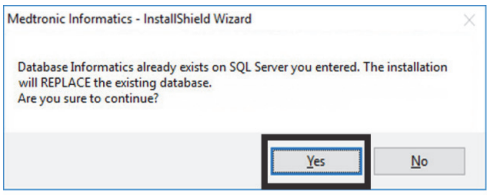
40. **User Name**—Enter **sa**.

41. **Password**—Enter the password set up for the SQL server instance that will support primary clinical and supervisory operations. (Refer to *Install the Database Server*, step *22*.)

42. Click **Next** to proceed.

43. If a primary operations database already exists on the system (for example, if an older version of the software was previously installed), a dialog will appear, with a warning that the existing database will be overwritten during installation.

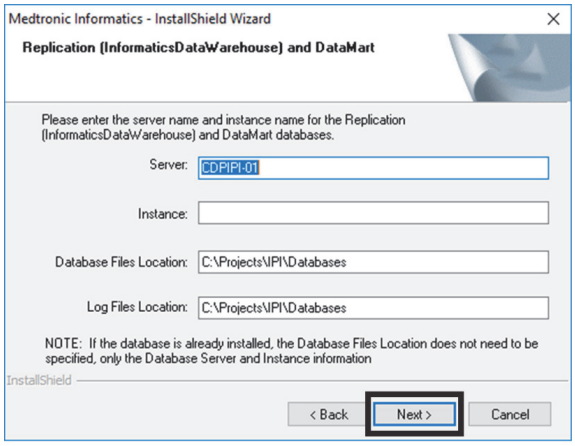
Figure 4-11. Informatics Installation Wizard—Database Overwrite Warning Dialog



INF_10332_D

44. If backups already exist for the primary operations database file used with the earlier version of the software, click **Yes** to proceed to the Replication (Informatics Data Warehouse) and DataMart page. If not, click **No** to return to the previous screen, then click **Cancel** to exit the installation wizard. (After creating a backup of the database file, reopen the installation wizard and repeat all previous steps in this procedure, then click **Yes** in the dialog when it appears again to proceed with installation.)

Figure 4-12. Informatics Installation Wizard—Replication (InformaticsDataWarehouse) and DataMart Page



INF_10181_E

45. **Server**—Enter the server name for the SQL server instance that will support the Informatics Data Warehouse and DataMart database.

Note:
If using distributed deployment, with a dedicated Data Warehouse system supporting reporting functions, enter information for the SQL server instance on the Data Warehouse system into the fields on the Reporting Database Information page. Refer to *Distributed Deployment*, page 5-8.

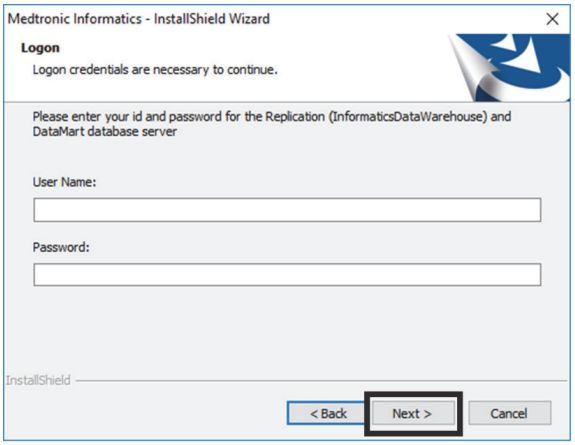
46. **Instance**—Enter the instance name for the desired SQL server instance, if needed.

47. **Database File Location**—If not using the default directory path, enter the desired directory path for the database file.

48. **Log File Location**—If not using the default directory path, enter the desired directory path for the log file.

49. When finished, click **Next** to proceed. If using separate instances for primary clinical and supervisory operations and for reporting functions, the Replication (Informatics Data Warehouse) and DataMart logon information page will appear.

Figure 4-13. Informatics Installation Wizard—Replication (InformaticsDataWarehouse) and DataMart Logon Information Page



INF_10182_E

Note:
If using the same instance for both primary operations and reporting functions, the Reporting Logon Information page will not appear.

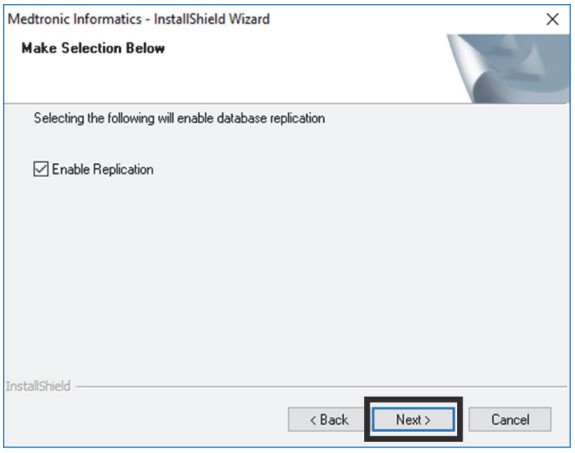
50. **User Name**—Enter **sa**.

51. **Password**—Enter the password set up for the SQL server instance that will support reporting functions. (Refer to *Installing the Database Server*, step *22*.)

52. Click **Next** to proceed.

53. If a database for primary functions and/or reporting is already installed, but the installation currently in progress is not an upgrade, a confirmation dialog will appear indicating that the existing databases will be deleted when the new databases are created. Click **OK** to proceed to the Enable Replication page, or click **Cancel** to exit the installation wizard if the existing databases should be backed up before proceeding.

Figure 4-14. Informatics Installation Wizard—Enable Replication Page

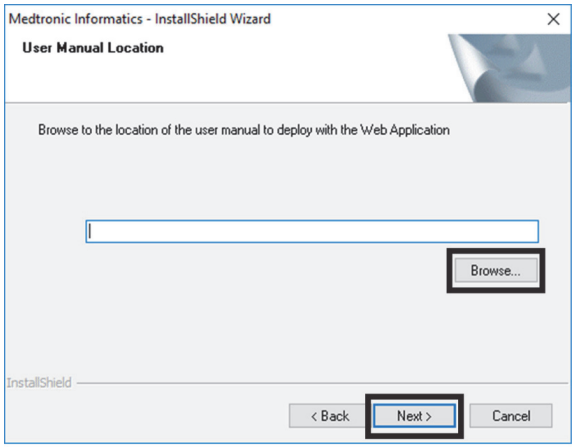


INF_10514_A

54. **Enable Replication**—To enable database replication, leave the box checked. To disable replication, click in the box to uncheck it.

55. Click **Next** to proceed to the User Manual Location page.

Figure 4-15. Informatics Installation Wizard—User Manual Location Page



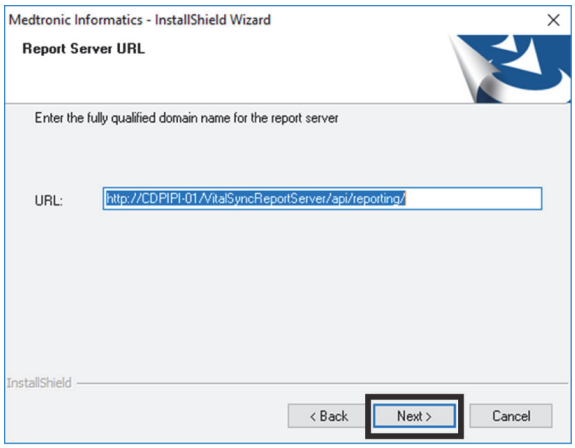
INF_10515_A

56. Enter the directory path to the electronic version of this reference manual, or click **Browse...** and navigate to the directory where the file resides. The reference manual file has a **.pdf** file extension.

Note:
The directory path for the manual is provided by Medtronic Professional Services at the time of installation.

57. Click **Next** to proceed to the Report Server URL page.

Figure 4-16. Informatics Installation Wizard—Report Server URL Page



INF_10516_A

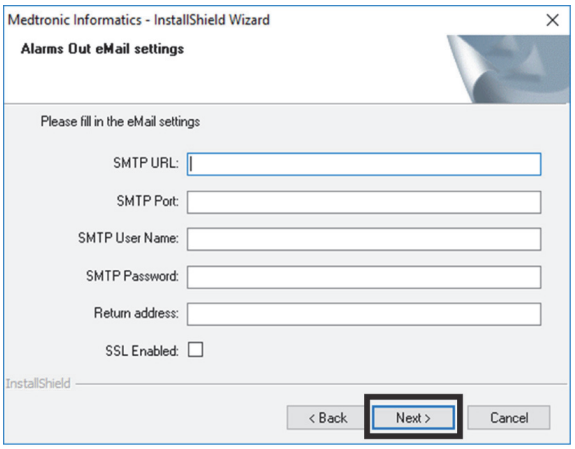
58. **URL**—The default URL for the report server is shown. If desired, enter an alternate URL. When finished, or if accepting the default location, Enter the URL for the report server.

Note:
The report server URL is provided by Medtronic Professional Services at the time of installation.

59. Click **Next** to proceed.

60. If installing the Alarms Out to SMTP component (selected in step *12*), the Alarms Out Email Settings page will appear. (If not installing this component, skip to step *68*.)

Figure 4-17. Informatics Installation Wizard—Alarms Out Email Settings Page



INF_10307_D

Note:
The facility must have existing email services from an appropriate provider in order to use the Alarms Out to SMTP functionality. Obtain settings information for entry in the Alarms Out Email Settings page from facility IT personnel.

61. **SMTP URL**—Enter the address for the email server from which system-generated email messages sent to users of the platform should be sent.

62. **SMTP Port**—Enter the SMTP server port number to be used.

63. **SMTP Username**—Enter the appropriate username for the SMTP server.

64. **SMTP Password**—Enter the appropriate password for the SMTP server.

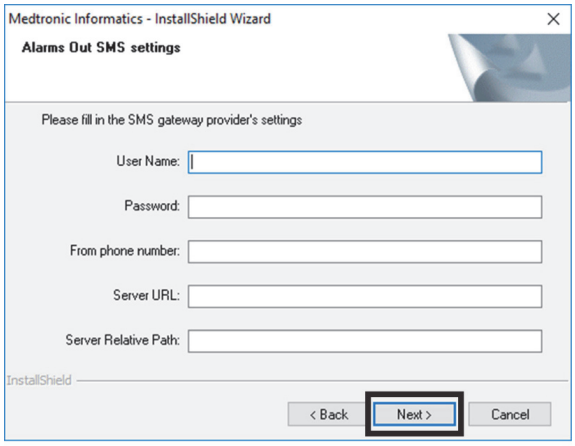
65. **Return Address**—Enter the address that will appear as the "From" address on email messages sent to users of the platform.

66. **SSL Enabled**—Check the box to use Secure Socket Layer (SSL) communication with the email server. (If not checked, messages sent to the email server will be treated as all other clear network traffic.

67. Click **Next** to proceed.

68. If installing the Alarms Out to SMS component (selected in step *12*), the Alarms Out SMS Settings page will appear. (If not installing this component, skip to step *75*.)

Figure 4-18. Informatics Installation Wizard—Alarms Out SMS Settings Page



INF_10308_D

Note:
The facility must have existing SMS messaging services from an appropriate provider in order to use the Alarms Out to SMS functionality. Obtain settings information for entry in the Alarms Out SMS Settings page from facility IT personnel.

69. **User Name**—Enter the user name for the SMS gateway via which system-generated SMS messages sent to users of the platform should be sent.

70. **Password**—Enter the appropriate password for the SMS gateway.

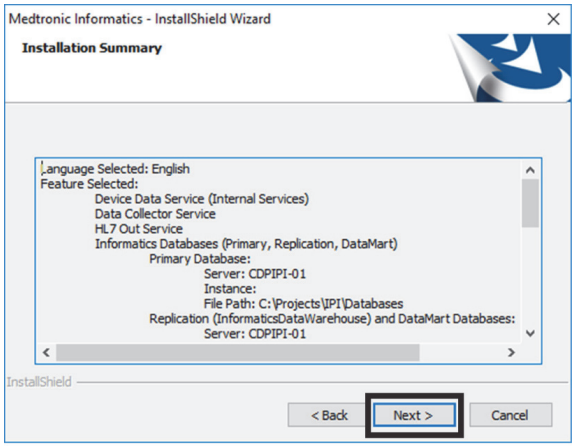
71. **From phone number**—Enter the phone number that will appear as the "from" number on the mobile device of the user receiving the SMS message.

72. **Server URL**—Enter the appropriate SMS gateway address.

73. **Server Relative Path**—Enter the appropriate path to the SMS gateway.

74. Click **Next** to proceed to the Installation Summary page.

Figure 4-19. Informatics Installation Wizard—Installation Summary Page

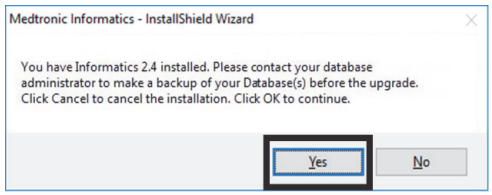


INF_10183_F

75. If desired, review the list of components to be installed, as well as database configuration details. When ready to continue, click **Next**.

76. If upgrading from a previously installed version of the software, a dialog showing version information for the older installation will appear.

Figure 4-20. Informatics Installation Wizard—Previous Installation Dialog

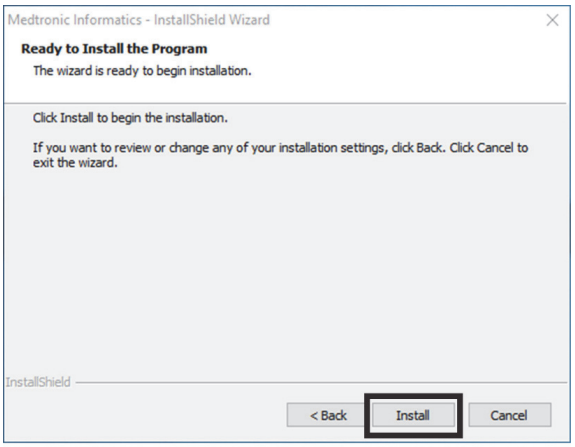


INF_10184_F

Note:
If upgrading from a version of the software previous to v2.5.x, exit the installation wizard and uninstall the older version before installing the current version.

77. If backups already exist for all database files used with the previous version of the software, click **OK** to proceed to the Confirmation page. If not, click **Cancel** to exit the installation wizard. After creating backup database files, reopen the installation wizard and repeat all previous steps in this procedure, then click **OK** in the dialog when it appears again to proceed with installation.

Figure 4-21. Informatics Installation Wizard—Confirmation Page

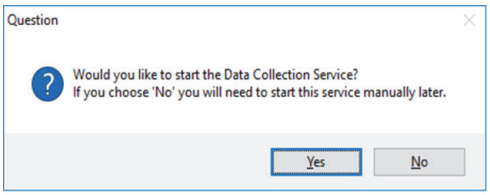


INF_10056_F

78. If ready to install components, click **Install**. If not, click **Back** as needed to return to earlier screens in the wizard, make any desired changes, then return to the Confirmation page and click **Install**.

79. A progress window (along with a series of command windows) will appear showing installation progress. Once the installation is complete, a dialog will appear asking whether or not to start the Data Collection Service.

Figure 4-22. Informatics Installation Wizard—Data Collection Service Start Dialog

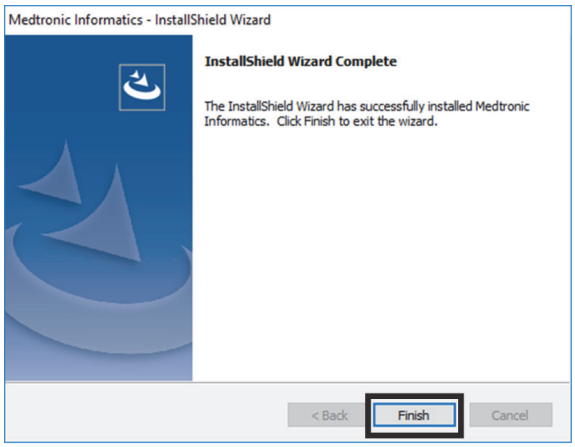


INF_10396_B

80. If ready to start the Data Collection Service, click **Yes**. If not ready to start the Data Collection Service, click **No**. (It is recommended to click **No** and manually start the service later once all software installation is complete).

81. A progress window (along with a series of command windows) will appear showing installation progress. Once the installation is complete, a dialog will appear asking whether or not to start the Data Collection Service.

Figure 4-23. Informatics Installation Wizard—Finish Page



INF_10057_F

82. Click **Finish** to exit the wizard.

83. Restart the system before continuing with the remaining configuration procedures detailed in this manual.

Note:
If installing components on multiple systems, repeat appropriate steps of the installation procedure in this chapter for each component or set of components, until all required components have been successfully installed on the appropriate systems.

5 Additional Configuration

5.1 Overview

This chapter provides information on final configuration steps before using the Vital Sync™ virtual patient monitoring platform and informatics manager software.

Note:
To install and configure software, administrative rights are required on destination systems.

Note:
The procedures shown in this chapter assume that Microsoft™* SQL Server™* 2016 is installed. If Microsoft™* SQL Server™* 2012 is installed, the procedures do not significantly differ. If encountering problems during or after configuration, consult with Medtronic Professional Services.

Note:
Setup and configuration procedures in this chapter are to support the Vital Sync™ virtual patient monitoring platform and informatics manager software,

5.2 Database Agent Startup

Once the database server software and the software components are installed and configured, the database server is ready for replication.

To fully enable replication, start the SQL Server and Snapshot agents.

Note:
While performing the procedures in this chapter, have the name of the SQL database server installed for use with the Vital Sync™ software readily available, to ensure the correct server is chosen.

5.2.1 SQL Server Agent

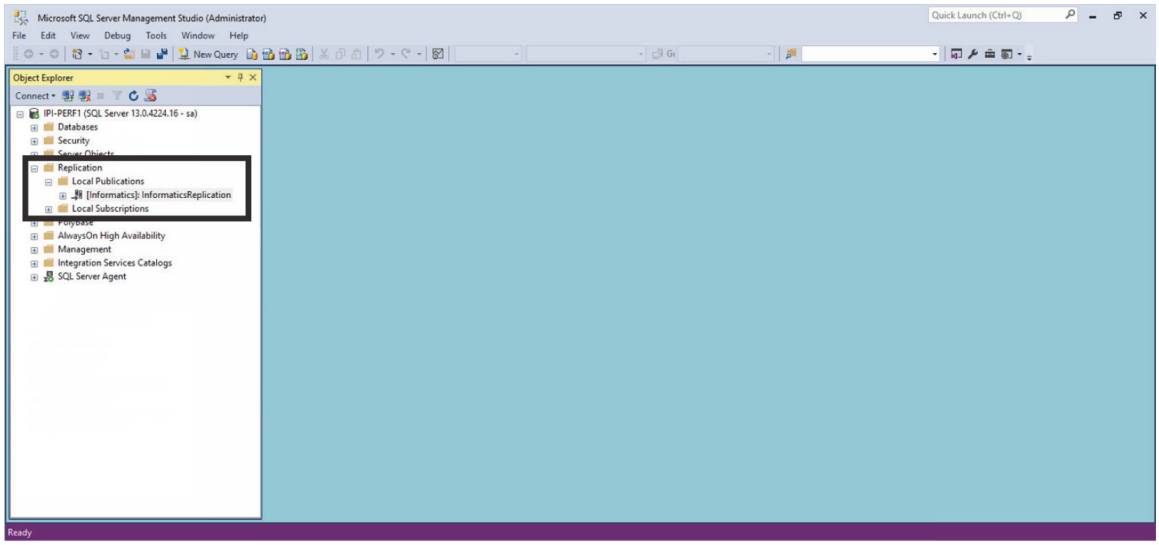
To start the SQL Server database agent:

1. In the Microsoft™* SQL Server™* Management Studio Object Explorer, find the SQL database server installed for use with the Vital Sync™ software.

2. Click the plus sign next to the **Replication** folder to expand the directory.

3. Click the plus sign next to the Local Publications folder to expand the directory. A publication named **[Informatics]: InformaticsReplication** should be present.

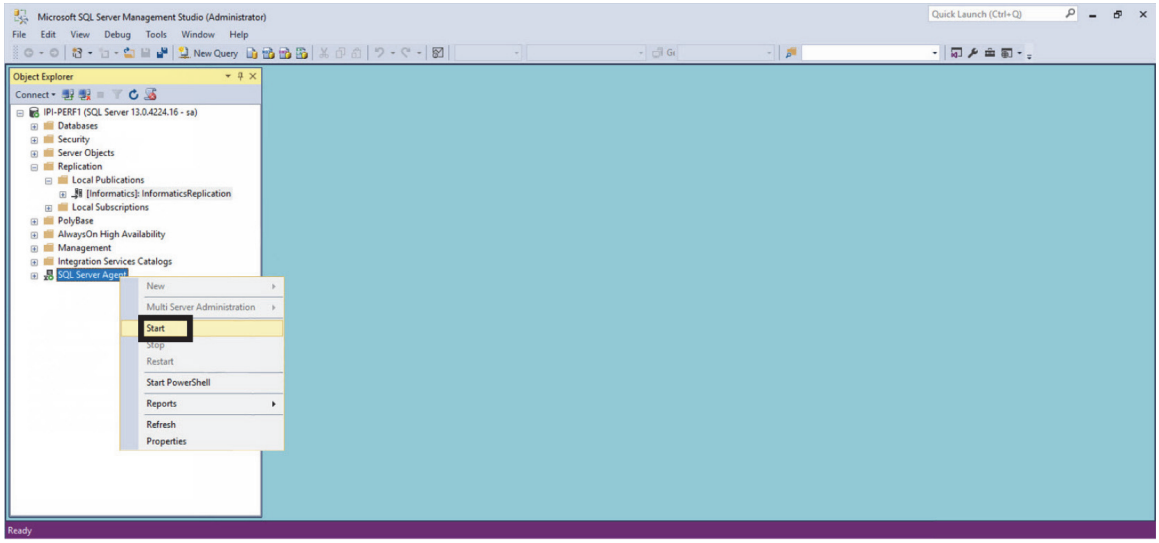
Figure 5-1. Microsoft™* SQL Server™* Management Studio (Informatics Replication publication shown)



INF_10058_D

4. Right-click on the **SQL Server Agent** icon to open a context menu.

Figure 5-2. Microsoft™* SQL Server™* Management Studio—SQL Server Agent Start



INF_10059_D

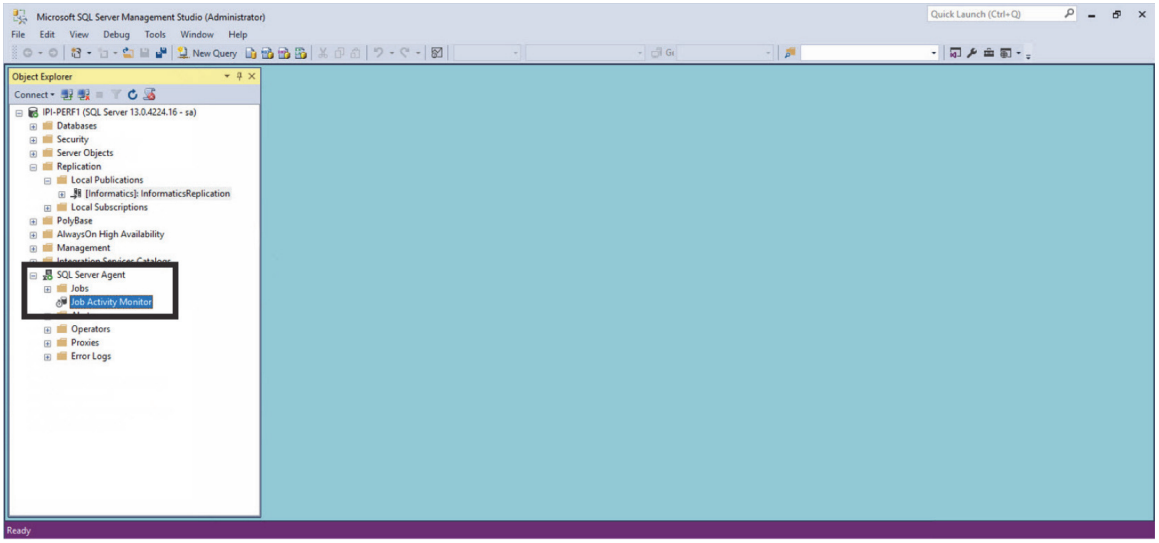
5. Select **Start**.

6. Click **Yes** to confirm startup of the SQL Server Agent. (Click **No** to abort startup.)

7. A progress bar shows the level of completion of the startup process. If startup is successful, click **Close**.

8. Click the plus sign next to the **SQL Server Agent** icon.

Figure 5-3. Microsoft™* SQL Server™* Management Studio (Job Activity Monitor icon present)



INF_10060_D

9. Confirm that an icon for the Job Activity Monitor is present.

Note:
Once the SQL Server Agent is running, do **not** stop it at any time. Stopping the SQL Server Agent prevents database replication in the Vital Sync™ software.

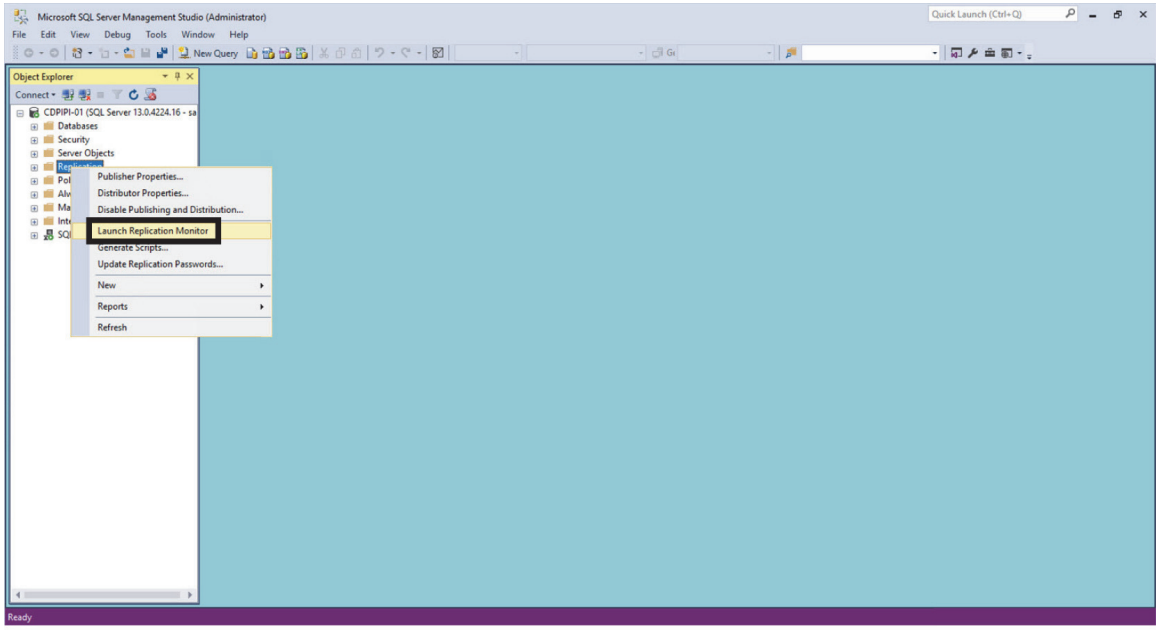
5.2.2 Snapshot Agent

To start the Snapshot Agent:

1. In the Microsoft™* SQL Server™* Management Studio Object Explorer, find the SQL database server installed for use with the Vital Sync™ software.

2. Right-click on the **Replication** icon to open a context menu.

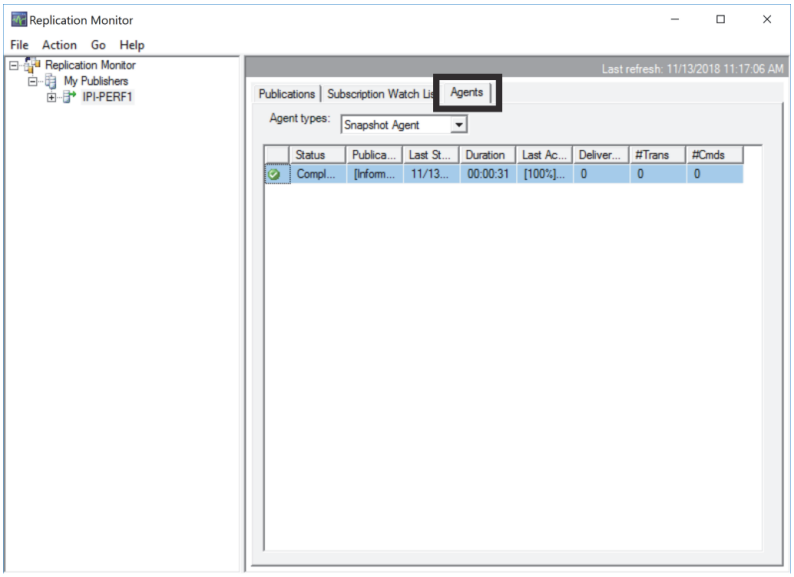
Figure 5-4. Microsoft™* SQL Server™* Management Studio—Replication Monitor Launch



INF_10061_D

3. Select **Launch Replication Monitor** to access the Replication Monitor screen.

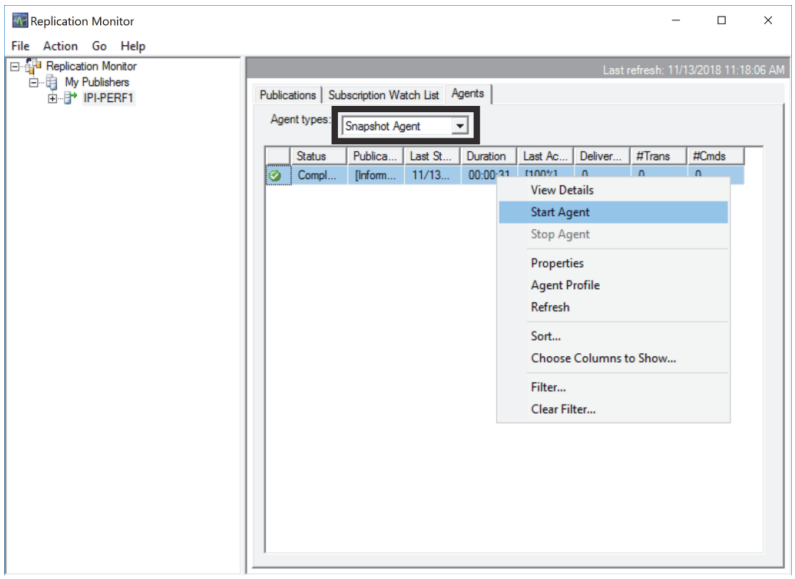
Figure 5-5. Replication Monitor Screen



INF_10062_D

4. In the Replication Monitor screen, click on the **Agents** tab.

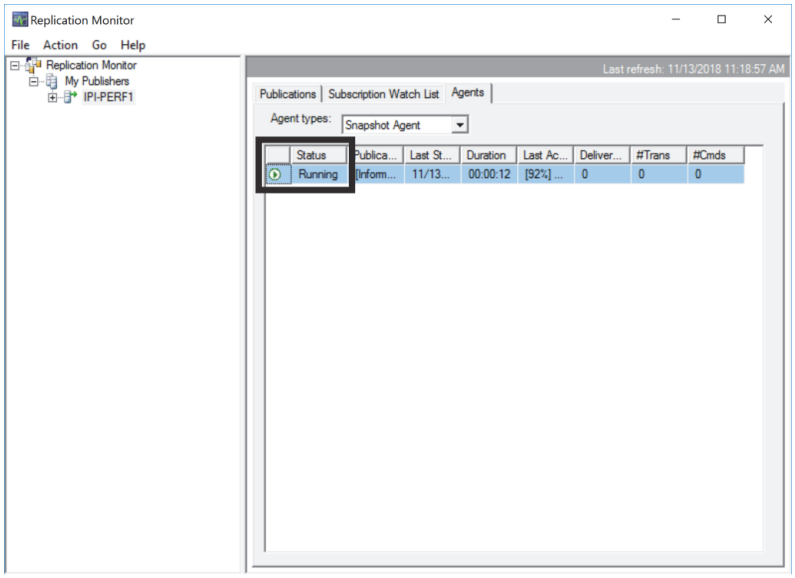
Figure 5-6. Replication Monitor Screen (Agents Tab)—Snapshot Agent Start



INF_10063_D

5. In the **Agent Type** drop-down box, select **Snapshot Agent** to show that agent on the Agents tab.
6. Right-click on the Snapshot Agent in the Agents tab to open a context menu.
7. Select **Start Agent** to start the agent.

Figure 5-7. Replication Monitor Screen (Agents Tab) (Snapshot Agent running)



INF_10064_D

8. Confirm that **Running** appears in the **Status** field for the Snapshot Agent.

Note:
Check the status of the Snapshot Agent at any time by opening the Replication Monitor and selecting **Snapshot Agent** from the **Agent Type** drop-down box on the Agents tab.

Note:
Once the Snapshot Agent is running, do **not** stop it at any time. Stopping the Snapshot agent prevents database replication in the Vital Sync™ software.

5.3 Firewall Configuration

After installing components and supporting software and configuring database agent operations and remote connection, ensure that the correct firewall ports are open to enable communications with the wireless network and with devices to be monitored, as indicated. Also ensure correct serial-to-Wi-Fi converter and device settings, to allow the software to connect and automatically reconnect as needed during normal operations.

WARNING:
Ensure that devices connected to the serial-to-Wi-Fi converter use the correct ports, so that the devices will be available in the device inventory when connected. Please contact Medtronic Professional Services for assistance if necessary.

See Table *5-1* for a list of ports to be opened, and on which system or systems.

Table 5-1. Firewall Ports To Be Opened

Port	System
3001	System with Informatics Web and Data Collection Service installed
3002	System with Informatics Web and Data Collection Service installed
3010	System with Informatics Web and Data Collection Service installed
3020	System with Informatics Web and Data Collection Service installed
3021	System with Informatics Web and Data Collection Service installed
3050	System with Informatics Web and Data Collection Service installed
4001	System with Informatics Web and Data Collection Service installed
5100	System with Informatics Web and Data Collection Service installed
5101	System with Informatics Web and Data Collection Service installed
10001	System with Informatics Web and Data Collection Service installed
80	Internet Information Services (IIS) server
443	IIS server (only required if SSL is enabled)
1433	OLTP and Data Warehouse servers (only if using distributed deployment)
2382	OLTP and Data Warehouse servers (only if using distributed deployment)

Specific Medtronic devices and protocols use certain ports to communicate with the software. See Table 5-2.

Table 5-2. Medtronic Device/Protocol Destination Ports

Device / Device Type	Communication Protocol	Port
Puritan Bennett™ 840 ventilator	Puritan Bennett Vent Listener SNDF	3001
Puritan Bennett™ 840 ventilator	Puritan Bennett Last Breath	3002
Nellcor™ N600X, Nellcor™ N600X-A, Nellcor™ Bedside Respiratory Patient Monitoring System, (pulse oximeters)	Nellcor ASCII	3010
Nellcor™ OxiMax N-85 handheld pulse oximeter	Nellcor Oridion	3020
Capnostream™ 20, Capnostream™ 20p, Capnostream 35 (capnography monitors)	Nellcor Oridion	3021
Newport™ HT70 ventilator	Newport HT70	3050
Puritan Bennett™ 840 ventilator	Puritan Bennett Vent Listener SNDA	4001
INVOS™ 5100C (regional saturation monitor)	Somanetics	5100
BIS™ Vista (bispectral index monitor)	Aspect BIS Vista	5101
Nellcor™ N600X, Nellcor™ N600X-A, Nellcor™ Bedside Respiratory Patient Monitoring System, (pulse oximeters)	Nellcor SHIP/SPDOut (Clinical)	10001

The local port settings listed in Table 5-2, in conjunction with the IP address, enable the software to automatically reconnect to each serial-to-Wi-Fi converter.

All devices using Ethernet or Wi-Fi require source and destination ports to establish identity and location. Recommended source ports are listed in Table 5-3.

Table 5-3. Recommended Source Ports for Device Communication

Device	Tunnel 1 (Odd Ports)	Tunnel 2(Even Ports)
Nellcor™ N600X, Nellcor™ N600X-A, Nellcor™ OxiMax N-85, Nellcor™ Bedside Respiratory Patient Monitoring System,	50001–50997	50002–50998
Puritan Bennett™ 840 ventilator, Puritan Bennett™ 980 ventilator	51001–51997	51002–51998
Capnostream™ 20, Capnostream™ 20p, Capnostream 35	52001–52997	52002–52998
BIS™ Vista	53001–53997	53002–53998
INVOS™ 5100C	54001–54997	54002–54998

The source port settings listed in Table 5-3, in conjunction with the source IP address, enable the software to automatically reconnect.

Note:

Medtronic recommends that each serial-to-Wi-Fi converter should be assigned a unique local port to connect to the system on which the Data Collection Service is installed.

Medtronic also recommends that each logical connection should be assigned a unique local port to connect to the system on which the Data Collection Service is installed, to maintain consistent status in the database.

Note:
Since all Medtronic devices support multiple baud rates, ensure that the baud rate is the same on each device as on the serial-to-Wi-Fi converter, so that the device will communicate properly.

Note:
The software is configurable to support connection with devices at different baud rates, or to allow use of different firewall ports than those listed in this manual. Please contact Medtronic Professional Services for assistance with POC network interface configuration.

5.4 Time Synchronization

If components are installed on multiple systems, ensure dates and times on all systems are synchronized, either via the network or by using a time server.

5.5 Distributed Deployment

For environments where there will be many users, monitored patients and/or monitored devices, a distributed deployment of Vital Sync™ software components and supporting software can be performed to improve efficiency and performance. One such deployment configuration is detailed in this section.

5.5.1 System Configuration

The distributed deployment described here uses four systems:

- The Online Transaction Processing (OLTP) system, also referred to as the OLTP database server, hosts the application database and the Database component.
- The Data Warehouse system, also referred to as the Data Warehouse database server, hosts the Data Warehouse database.
- The application system hosts the Data Collection Service, Reports, and Informatics Web components.
- The services system hosts the IPI Web Services connector component.

The OLTP database server supports primary clinician and supervisor platform functions, including patient/device summary and detail displays, device/patient associations, and patient and area assignment.

The Data Warehouse database server, meanwhile, supports the software's reporting functions, and also serves as a backup to the OLTP database server.

Reporting functions can be resource-intensive, particularly when a very large data set needs to be generated for a particular report. Distributed deployment allows simultaneous reporting tasks and clinical and supervisory tasks without an adverse effect on performance, as the different tasks will not directly compete for resources on the same system.

5.5.2 Setup Process

Once components are installed on the appropriate servers as described in Chapter 4, perform subsequent distributed development setup as follows:

- Ensure that services installed on the services system are pointed to the application database on the OLTP server. Refer to *Enable Remote Connection*, page 3-30.
- Ensure that replication is configured to point to the Data Warehouse server database from the OLTP server database. Refer to *Enable Remote Connection*, page 3-30.
- To enable reporting functionality for multi-server installations that use a Data Warehouse server, configure the Worldwide Web Publishing Service to point to the Data Warehouse server database.
- If interfacing with an external system using HL7 messages, configure the IPI HL7 Adapter to point to the correct system.

5.5.3 Reporting Configuration

Certain multi-server installations of the Vital Sync™ software will require changes to the Worldwide Web Publishing Service configuration to support reporting functionality.

Installation

The Worldwide Web Publishing Service is installed with Microsoft™* Windows™* Internet Information Services (IIS).

Configuration

The Vital Sync™ software installer automatically configures the connection string for the Worldwide Web Publishing Service during installation. This string denotes the database to which the service should initially connect to correctly enable reporting functionality.

If installing the Vital Sync™ remote monitoring system software, no further configuration is necessary.

If installing the Vital Sync™ virtual patient monitoring platform and informatics manager software on multiple servers including a Data Warehouse system, follow the procedure in this section.

Note:
Making changes to configuration files may adversely affect service or adapter performance. Do not make changes other than those described in this section. Always use caution when changing configuration files.

Note:
Always make a backup copy of the configuration file before making any changes to the file.

To change the connection string parameter setting:

1. Navigate to the directory with the configuration file (typically, **C:\inetpub\wwwroot\VitalSyncReport-Server\Config**).
2. Open **ConnectionStrings.config**.
3. Find the **<ReportData>** section of the file.
4. On the **connectionString** line, change the **Initial Catalog** setting to **InformaticsDataWarehouse**.
5. Save and close the configuration file.
6. Stop the Worldwide Web Publishing Service.
7. Restart the service to implement the new setting.

5.5.4 Subscription Configuration

After configuring report services to point to the Data Warehouse report server, set up a subscription to replace the local subscription, so that replication will also point to the Data Warehouse server.

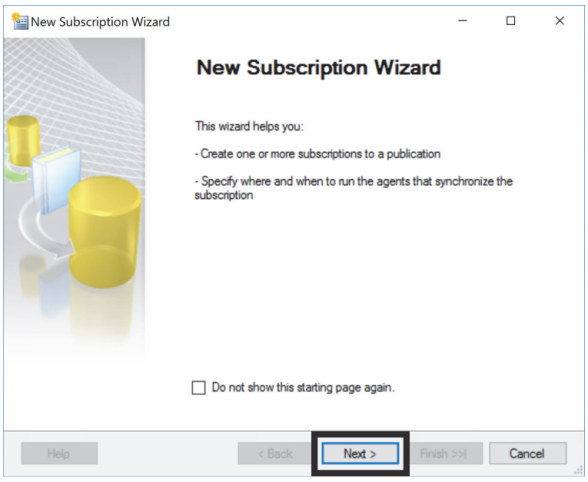
The wizard accessed during the subscription setup process shows a series of screens for selection of options. If needing to change a selection already made, click **Back** to go back to the previous screen and make the change.

In any screen, if needed, click **Cancel** to stop configuration and exit the wizard.

To configure replication to point to the Data Warehouse report server:

1. In the Microsoft™* SQL Server™* Management Studio Object Explorer on the application system, find the SQL database server instance installed to support the Vital Sync™ software.
2. Click the plus sign next to the **Replication** folder to expand the directory.
3. Click the plus sign next to the Local Publications folder to expand the directory. A publication named **[Informatics]: InformaticsReplication** should be present.
4. Right-click on **[Informatics]: InformaticsReplication** to open a context menu, then select **New Subscriptions...** to open the New Subscription wizard.

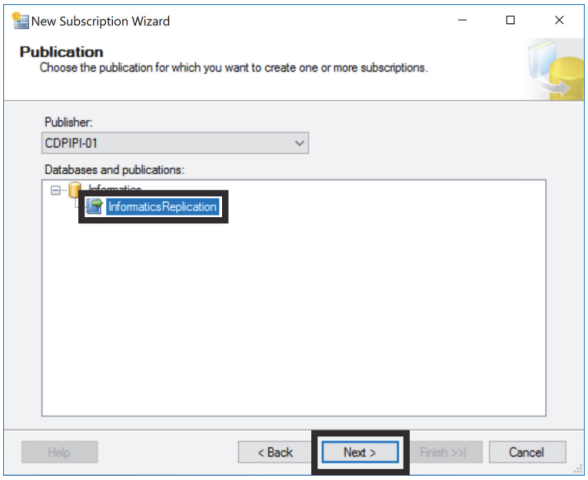
Figure 5-8. New Subscription Wizard—Start Page



INF_10104_D

5. Click **Next** to proceed to the Publication page.

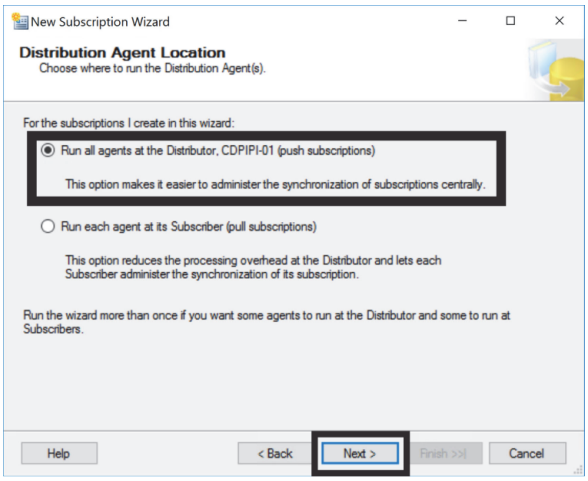
Figure 5-9. New Subscription Wizard—Publication Page



INF_10105_D

6. Ensure that **InformaticsReplication** is highlighted, then click **Next** to proceed to the Distribution Agent Location page.

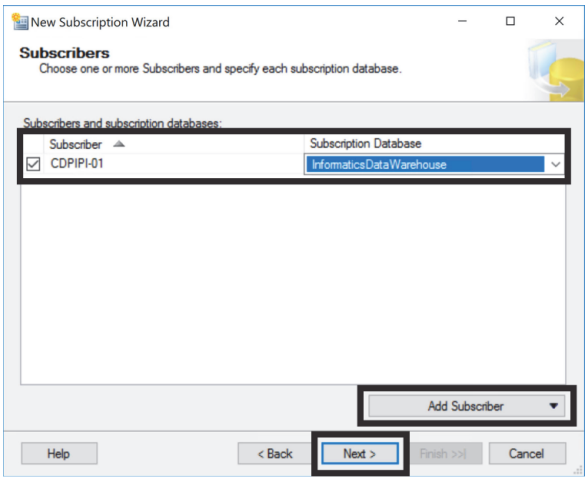
Figure 5-10. New Subscription Wizard—Distribution Agent Location Page



INF_10106_D

7. Ensure the **Run all agents at the Distributor** radio button is selected, then click **Next** to proceed to the Subscribers page.

Figure 5-11. New Subscription Wizard—Subscribers Page



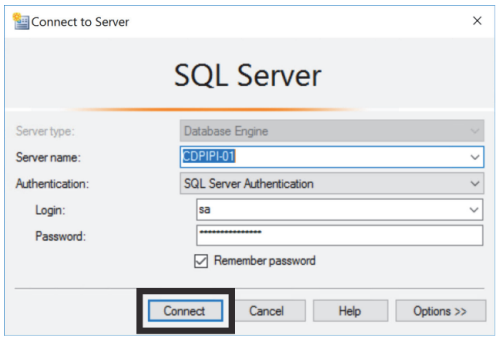
INF_10107_D

8. Click the check box next to the desired subscriber. A drop-down menu will appear in the **Subscription Database** column for the subscriber selected.

9. Click on the subscription database drop-down menu to open it, then select **InformaticsDataWarehouse**.

10. Click on the **Add Subscriber** drop-down menu to open it, then select **Add SQL Server Subscriber...** to open a connection dialog for adding the Data Warehouse report server database.

Figure 5-12. Connection Dialog (for Data Warehouse server)



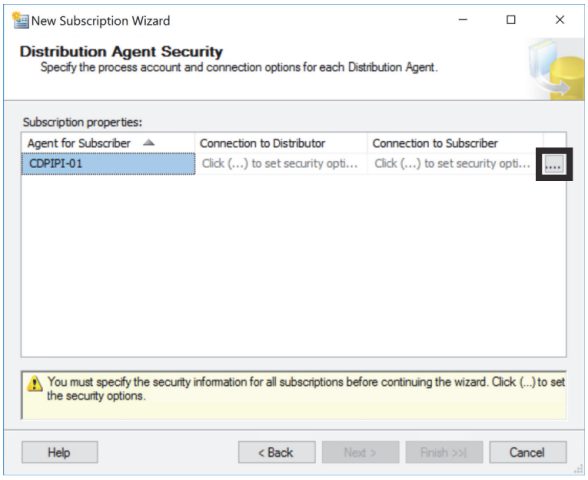
INF_10108_D

11. Enter server information (server name, authentication type, username, and password) for the Data Warehouse report server.

12. Click **Connect** to connect to the Data Warehouse report server.

13. Click **Next** to proceed to the Distribution Agent Security screen.

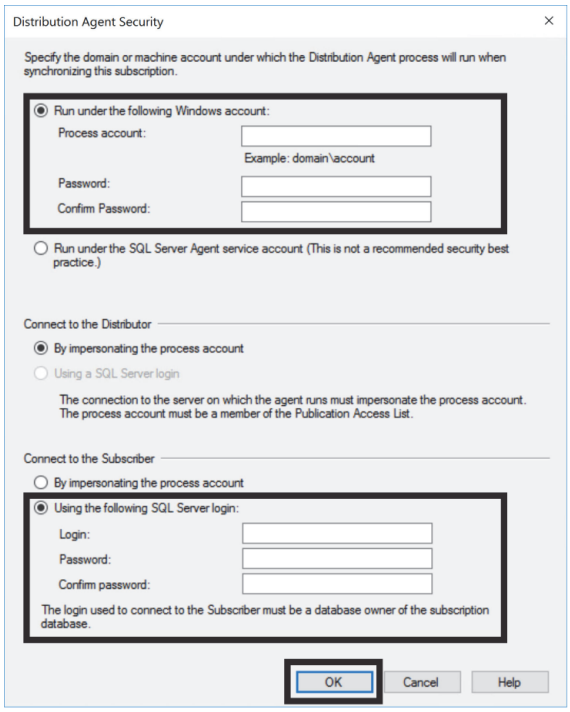
Figure 5-13. New Subscription Wizard—Distribution Agent Security Page



INF_10109_D

14. Click the **...** button on the Data Warehouse report server line to open a dialog box for selection of security options.

Figure 5-14. Distribution Agent Security Dialog (account fields)



INF_10185_C

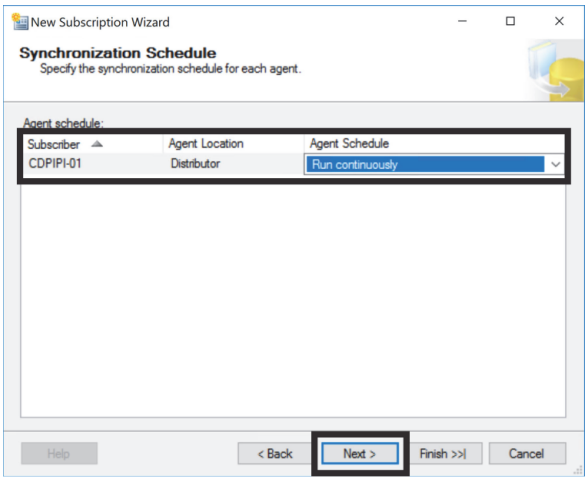
15. Click the **Run under the following Windows account** radio button.

16. Enter the login name and password of an appropriate administrative user on the system on which the Informatics Web component is installed.

17. In the **Connect to the Subscriber** fields, click the **Using the following SQL Server login** radio button, then enter the SQL server user login name and password on the Data Warehouse report server. (Typically, the account used is the system administrator account set up during database server installation on the Data Warehouse server. Refer to *Install the Database Server*, step *22*.)

18. Click **OK** to return to the Distribution Agent Security page, then click **Next** to proceed to the Synchronization Schedule page.

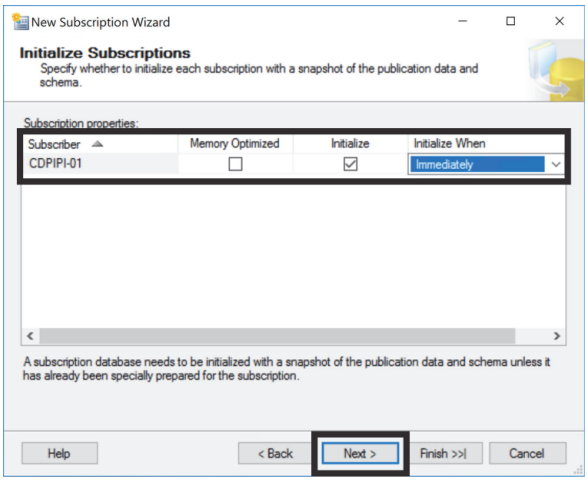
Figure 5-15. New Subscription Wizard—Synchronization Schedule Page



INF_10111_D

19. Ensure the **Agent Schedule** field for the Data Warehouse report server shows **Run continuously**, then click **Next** to proceed to the Initialize Subscriptions page.

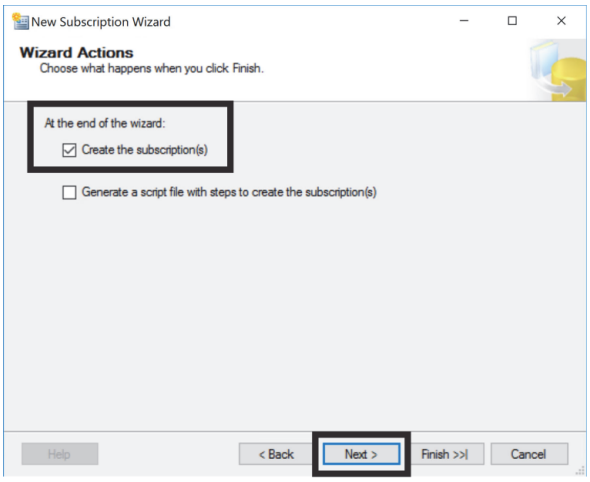
Figure 5-16. New Subscription Wizard—Initialize Subscriptions Page



INF_10112_D

20. Ensure the **Initialize When** field for the Data Warehouse report server shows **Immediately**, then click **Next** to proceed to the Wizard Actions page.

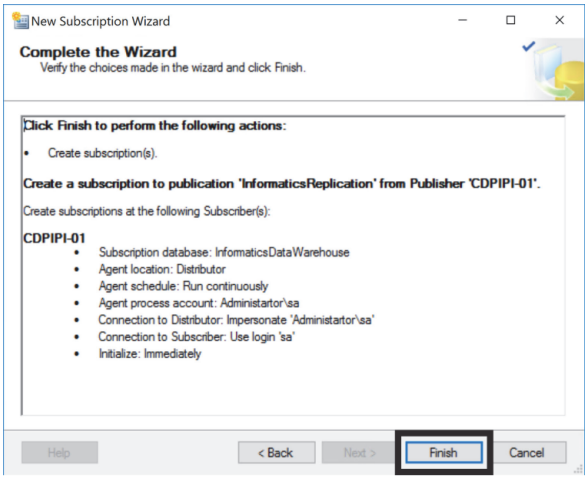
Figure 5-17. New Subscription Wizard—Wizard Actions Page



INF_10113_D

21. Ensure the **Create the subscription(s)** check box is checked, then click **Next** to proceed to the confirmation page.

Figure 5-18. New Subscription Wizard—Confirmation Page

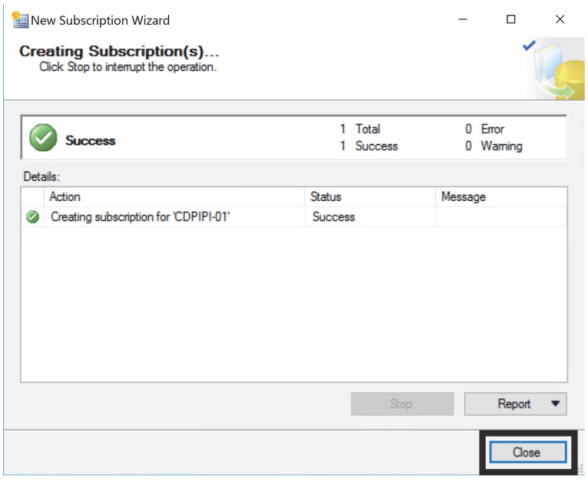


INF_10114_D

22. The confirmation page shows details of the new subscription. Review the list if desired, then click **Finish** to create the subscription.

23. The wizard will indicate the level of completion of the operation on the finish page, indicating success or failure of each step.

Figure 5-19. New Subscription Wizard—Finish Page

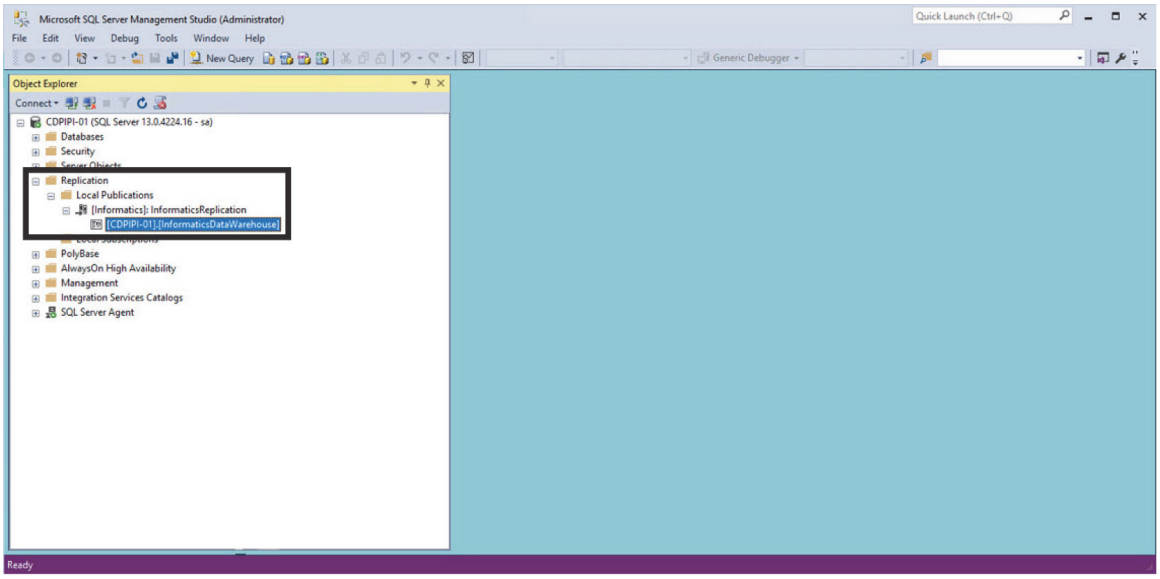


INF_10115_D

24. After reviewing information, click **Close** to exit the wizard. (If problems occurred, resolve them, then repeat all previous steps in this procedure until creation is successful.)

25. In the SQL Server Management Studio Object Explorer, the new subscription will appear under **[Informatics]: InformaticsReplication**, with the name of the Data Warehouse report server listed in brackets.

Figure 5-20. Microsoft™* SQL Server™* Management Studio Object Explorer (Data Warehouse report server shown)



INF_10116_D

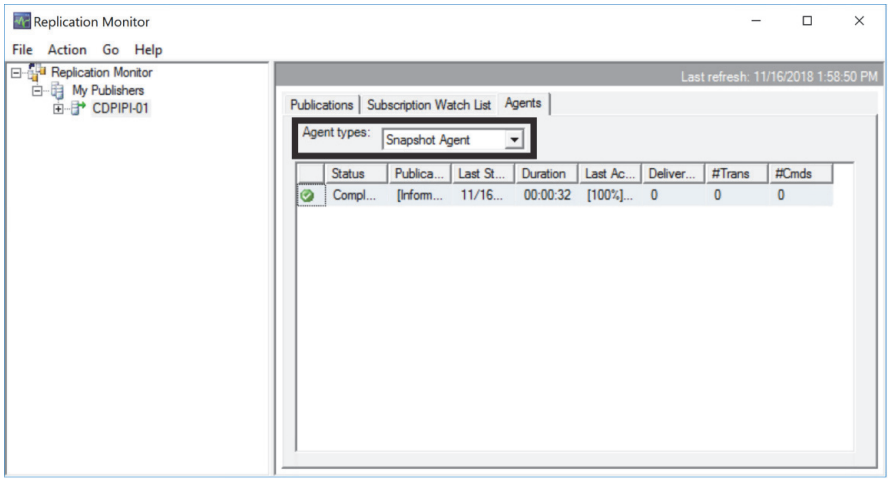
26. Right-click on the local server subscription (i.e., the subscription that does **not** have the name of the Data Warehouse report server) shown under **[Informatics]: Informatics Replication** to open a context menu, then select **Delete**.

27. A dialog box will appear for confirmation of deletion. Click **Yes** to delete the local subscription, or click **No** to cancel and return to the Object Explorer.

28. Right-click on the Data Warehouse server subscription to open a context menu, then select **Launch Replication Monitor**.

29. In the right pane, click on the **Agent** tab.

Figure 5-21. Replication Monitor Screen (Agents Tab) (Snapshot Agent shown)



INF_10117_D

30. Ensure **Snapshot Agent** is shown in the **Agent types** drop-down box.

31. Confirm that "Completed" shows in the Status field, then right-click on it to open a context menu, and select **Start Agent** to start the Snapshot Agent running.

Note:
If the Snapshot Agent does not start properly, or an error message appears, check the credentials of the user entered in step *16* of this procedure to ensure privileges are sufficient to run reports on the Data Warehouse report server.

5.5.5 IPI Adapter Services Configuration

If the Vital Sync™ software is to be set up to send data to an external system (such as an Electronic Medical Record system), changes may be necessary to the default configuration for IPI adapter services to allow proper communication between the software and the external system. Reference Chapter 6 for details.

6 Connectivity to External Systems

6.1 Overview

This chapter provides information on additional installation and configuration steps to allow the Vital Sync™ virtual patient monitoring platform and informatics manager software to interface with certain external systems.

Note:
To install and configure software, administrative rights are required on destination systems.

Note:
Software performance and system health should be consistently monitored to allow timely detection and resolution of problems, especially with communication of alarm messages.

A real-time listing of application events, as well as system performance reports, are available in the Vital Sync™ software. Refer to the reference manual for details.

6.2 Vital Sync HL7 Reporter Service

Users of external systems that accept HL7 messages, such as Electronic Medical Record (EMR) systems, can access device and patient data gathered by the Vital Sync™ Virtual Patient Monitoring Platform and Informatics Manager via the Vital Sync HL7 Reporter Service. Once the service is installed and configured, the external system can receive platform data via TCP/IP.

Note:
Users of the Vital Sync™ virtual patient monitoring platform and informatics manager software do not confirm HL7 data sent to external systems. Clinicians will acknowledge and confirm HL7 data received into the EMR or other external system using the appropriate software on that system.

To obtain additional information regarding support for HL7 standards, consult with Medtronic Professional Services or with a local Medtronic representative.

Note:
The Vital Sync™ virtual patient monitoring platform and informatics manager software also supports use of a solicited interface. For more information about how to configure the Vital Sync HL7 Reporter Service to work with a solicited interface, consult with Medtronic Professional Services.

6.2.1 Installation

The Vital Sync HL7 Reporter Service is installed with the Vital Sync HL7 Reporter Adapter component of the Vital Sync™ software.

The service is located in the same directory with all other IPI services, and is registered on the system as a Microsoft™* Windows™* service. In the Services Management Console, the service appears as **Vital Sync HL7 Reporter Service**.

Files specific to the service are located in the **AdapterPlugins** subdirectory of the system's **Config** directory.

6.2.2 Additional Configuration

The Vital Sync™ software installer automatically configures the service during installation. In most cases, the default settings require no modification.

However, depending on facility needs, changes may be necessary to configuration settings for data output, or for connectivity to the external system or to Vital Sync™ software components.

Note:
Making changes to configuration files may adversely affect service or adapter performance. Do not make changes other than those described in this section. Always use caution when changing configuration files.

Note:
Always make a backup copy of the configuration file before making any changes to the file.

Data-Related Settings

The **scheduleInterval** setting in the **TimerTrigger** section specifies how frequently the service sends HL7 messages. This may require adjustment to accurately account for network or system latency.

To change the schedule interval setting:

1. Navigate to the directory with the configuration file (for example, **C:\Program Files\Covidien\Informatics**).
2. Open **VitalSync.HL7ReporterService.exe.config**.
3. Find the **<TimerTrigger>** section in the file.
4. Change the **scheduleInterval** setting as appropriate to facility needs. The value is specified in milliseconds. The default setting is 60000.
5. Save and close the configuration file.
6. Stop the Vital Sync HL7 Reporter Service.
7. Restart the service to implement the new setting.

Note:
Typically, the service will send HL7 data at approximately the frequency indicated by the **scheduleInterval** setting. However, latency due to system processing or in communication between systems may cause delay. If such a delay routinely occurs, adjust the schedule interval parameter appropriately to optimize performance.

External Connectivity-Related Settings

Multiple **HL7OutputPluginWithLogging** settings specify how the Vital Sync HL7 Reporter Service connects to the external system that will receive HL7 messages. These settings may require adjustment to account for the facility's network configuration.

- The **server** setting identifies the external system to which the service will attempt to connect.
- The **portNumber** setting specifies the TCP port to which the service will attempt to connect.
- The **numberOfRetries** setting specifies the number of times the service will try again to connect with the external system after failing in its initial attempt.
- The **waitBetweenRetries** setting specifies how long the service will wait after a failed connection attempt before its next attempt to connect with the external system.

To change external connectivity settings:

1. Navigate to the directory with the configuration file (for example, **C:\Program Files\Covidien\Informatics**).
2. Open **VitalSync.HL7ReporterService.exe.config**.
3. Find the **<HL7OutputPluginWithLogging>** section of the file.
4. If needed, change the **server value** setting to either the name or the IP address of the external system which will be receiving HL7 messages.
5. If needed, change the **portNumber value** setting to the TCP port number to which the adapter service will attempt to connect.
6. If needed, change the **numberOfConnectRetries** setting to a different value. The default setting is 5, indicating that the adapter will make five additional connection attempts after an initial failure before abandoning the sending of that specific HL7 message.
7. If needed, change the **waitBetweenConnectRetries** setting to a different value. The default setting is 1000, indicating that the adapter will wait 1000 milliseconds before making its next connection attempt after an initial connection failure.
8. Save and close the configuration file.
9. Stop the Vital Sync HL7 Reporter Service.
10. Restart the service to implement the new settings.

6.3 Vital Sync ADT In Adapter Service

Users of ADT systems that send HL7 messages can send patient data to the Vital Sync™ virtual patient monitoring platform and informatics manager software via the Vital Sync ADT In Adapter Service. Once the service is installed and configured, the external system can send platform data via TCP/IP.

To obtain additional information regarding support for HL7 standards, consult with Medtronic Professional Services or with a local Medtronic representative.

6.3.1 Installation

The Vital Sync ADT In Adapter Service is installed with the Vital Sync ADT In Adapter component of the Vital Sync™ software.

The service is located in the same directory with all other IPI services, and is registered on the system as a Microsoft™* Windows™* service. In the Services Management Console, the service appears as **Vital Sync ADT In Adapter**.

Files specific to the adapter service are located in the **AdapterPlugins** subdirectory of the system's **Config** directory.

6.3.2 Additional Configuration

The Vital Sync™ software installer automatically configures the service during installation. In most cases, the default settings require no modification.

However, depending on facility needs, changes may be necessary to configuration settings for data input, or for connectivity to the external system or to Vital Sync™ software components.

Note:
Making changes to configuration files may adversely affect service or adapter performance. Do not make changes other than those described in this section. Always use caution when changing configuration files.

Note:
Always make a backup copy of the configuration file before making any changes to the file.

Connectivity-Related Settings

The **Port** setting in the **TcpIpInputTrigger** section specifies the TCP/IP port on which the adapter service will listen for connections from the external system.

To specify a port on which to listen:

1. Navigate to the directory with the configuration file (for example, **C:\Program Files\Covidien\Informatics**).
2. Open **VitalSync.ADTin.AdapterService.exe.config**.

3. Find the **<TcpIpInputTrigger>** section of the file.
4. Change the **Port value** setting to the port on which the ADT In Adapter should listen for connections.
5. Save and close the configuration file.
6. Stop the Vital Sync ADT In Adapter Service.
7. Restart the service to implement the new settings.

The **RemoteIpValidation** setting in the **TcpIpInputTrigger** section specifies whether the ADT system should accept connections only from a particular remote IP address.

To enable remote IP validation:

1. Navigate to the directory with the configuration file (for example, **C:\Program Files\Covidien\Informatics**).
2. Open **VitalSync.ADTin.AdapterService.exe.config**.
3. Find the **<TcpIpInputTrigger>** section of the file.
4. Change the **RemoteIpValidation** setting to **true**.
5. Change the **RemoteIp** setting to the remote IP sending ADT messages.
6. Save and close the configuration file.
7. Stop the Vital Sync ADT In Adapter Service.
8. Restart the service to implement the new settings.

6.4 Vital Sync Alarm Reporter Service

Users of external systems that accept alarm messages in IHE PCD-04 format, such as alarm management systems, can receive alarm data gathered by the Vital Sync™ virtual patient monitoring platform and informatics manager software via the Vital Sync Alarm Reporter Service.

To obtain additional information regarding support for IHE and HL7 standards, consult with Medtronic Professional Services or with a local Medtronic representative.

Note:
Facility IS personnel should consistently monitor the system's "dead letter queue" for the presence of any unsent alarm messages. If any messages are present in the queue, investigate and resolve any issues preventing messages from being sent.

6.4.1 Installation

The Vital Sync Alarm Reporter Service is installed as a component of the Vital Sync™ software.

The service is located in the same directory with all other IPI services, and is registered on the system as a Microsoft™* Windows™* service. In the Services Management Console, the service appears as **Vital Sync Alarm Reporter Service**.

Files specific to the service are located in the **AdapterPlugins** subdirectory of the system's **Config** directory.

6.4.2 Dependencies

The service has dependencies on three other system components: Microsoft™* Message Queuing; the Data Collection Service component of the Vital Sync™ software; and the Applet Manager Service component of the Vital Sync™ software.

Message queuing and the Data Collection Service should already be installed, and the Applet Manager should also already be installed if platform-related applications or derived parameter algorithms are being used. Refer to *Install Message Queuing*, page 3-9, and *Component Installation*, page 4-2.

6.4.3 MSMQ Queue Configuration

The Data Collection Service component sends alarm events to a specific message queue. The Vital Sync Alarm Reporter Service retrieves events from the same queue, transforms the events as appropriate for the external system accessing them, and then forwards the event data to the external system.

To enable MSMQ functionality for alarm events:

1. Create a queue for alarm events. Reference the Microsoft™* technical document *Administering Queues*, available online at the following URL:

   http://technet.microsoft.com/en-us/library/cc772532.aspx

Note:
The preferred name for the queue is **ipiCoreEvents**, the default name used by the Vital Sync™ Virtual Patient Monitoring Platform and Informatics Manager.

2. Set security permissions so that the Vital Sync Alarm Reporter Service, Data Collection Service, and Applet Manager Service (if used) can access the queue. The permission settings required will depend on the accounts under which services are run, and whether the queue resides on a different machine than the machine on which the Vital Sync Alarm Reporter Service, the Data Collection Service, or the Applet Manager service (if used) run. Reference the Microsoft™* technical document *Set Permissions for Computer and Queue Objects*, available online at the following URL:

   http://technet.microsoft.com/en-us/library/cc753761(v=ws.10).aspx

6.4.4 Additional Configuration (Alarm Output and Retrieval)

The Vital Sync™ software installer automatically configures the Vital Sync Alarm Reporter Service during installation. In most cases, the default settings require no modification.

Depending on facility needs, changes may be necessary to configuration settings for data output, or for connectivity to the external system or to Vital Sync™ software components.

By default, output of alarm events for access by external systems is disabled. Additional configuration is required in the Data Collection Service to allow the Vital Sync Alarm Reporter Service to receive alarms for subsequent forwarding to an external system.

Note:
Making changes to configuration files may adversely affect service or adapter performance. Do not make changes other than those described in this section. Always use caution when changing configuration files.

Note:
Always make backup copies of configuration files before making any changes to them.

Alarm Output Settings

The **messageService** and **externalGateway** parameters are used to enable or disable output of alarm events for access by external systems.

To enable output of alarm events from the Data Collection Service:

1. Navigate to the directory with the configuration file (for example, **C:\Program Files\Covidien\Informatics**).
2. Open **VitalSync.DataCollectionService.exe.config**.
3. Find the **<messageService>** section of the file.
4. If the **<messageService>** section is currently commented out, remove commenting marks.
5. Change the **msmqReceiveQueue** setting to match the full name of the MSMQ queue created for alarm events (for example, **\Private\ipiCoreEvents**). Refer to *MSMQ Queue Configuration*, page 6-6.
6. Find the **<externalGateway>** section of the file.
7. If the **<externalGateway>** section is currently commented out, remove commenting marks.
8. Change the **subscribeToCoreEvents** setting to **true**.
9. Save and close the configuration file.
10. Stop the Data Collection Service.
11. Restart the service to implement the new setting.

To enable output of alarm events from the Applet Manager Service:

1. Navigate to the directory with the configuration file (for example, **C:\Program Files\Covidien\Informatics**).
2. Open **VitalSync.AppletManagerService.exe.config**.
3. Find the **<messageService>** section of the file.
4. If the **<messageService>** section is currently commented out, remove commenting marks.
5. Change the **msmqReceiveQueue** setting to match the full name of the MSMQ queue created for alarm events (for example, **\Private\ipiCoreEvents**). Refer to *MSMQ Queue Configuration*, page 6-6.
6. Find the **<externalGateway>** section of the file.
7. If the **<externalGateway>** section is currently commented out, remove commenting marks.
8. Change the **subscribeToCoreEvents** setting to **true**.
9. Save and close the configuration file.
10. Stop the Applet Manager Service.
11. Restart the service to implement the new setting.

Alarm Retrieval Settings

The **msmqReceiveQueue** setting in the **messageService** section specifies the name of the queue from which the Vital Sync Alarm Reporter Service will retrieve alarm events.

To change the parameter setting:

1. Navigate to the directory with the configuration file (for example, **C:\Program Files\Covidien\Informatics**).
2. Open **VitalSync.AlarmReporterService.exe.config**.
3. Find the **<messageService>** section of the file.
4. Change the **msmqSendQueue** setting to match the full name of the MSMQ queue created for alarm events (for example, **\Private\ipiCoreEvents**). Refer to *MSMQ Queue Configuration*, page 6-6.
5. Change the **msmqReceiveQueue** setting to match the full name of the MSMQ queue created for alarm events (for example, **\Private\ipiCoreEvents**). Refer to *MSMQ Queue Configuration*, page 6-6.
6. Save and close the configuration file.
7. Stop the Vital Sync Alarm Reporter Service.
8. Restart the service to implement the new setting.

6.4.5 Additional Configuration (HL7, Email, SMS, and Paging)

The Vital Sync Alarm Reporter Service can be configured to allow alerts from the platform to be communicated externally using HL7, email, SMS, or TAP.

HL7 Configuration Settings

This is the default configuration for the Vital Sync Alarm Reporter Service.

Multiple **HL7OutputPluginWithLogging** settings specify how the service connects to the external system that will receive PCD-04 messages. These settings may require adjustment to account for the facility's network configuration.

- The **server** setting identifies the external system to which the service will attempt to connect.
- The **portNumber** setting specifies the TCP port to which the service will attempt to connect.
- The **numberOfRetries** setting specifies the number of times the service will try again to connect with the external system after failing in its initial attempt.
- The **waitBetweenRetries** setting specifies how long the service will wait after a failed connection attempt before its next attempt to connect with the external system.

To change external connectivity settings:

1. Navigate to the directory with the configuration file (for example, **C:\Program Files\Covidien\Informatics**).
2. Open **VitalSync.AlarmReporterService.exe.config**.
3. Find the **<HL7OutputPluginWithLogging>** section of the file.
4. If needed, change the **server value** setting to either the name or the IP address of the external system which will be receiving the PCD-04 messages.
5. If needed, change the **portNumber value** setting to the TCP port number to which the service will attempt to connect.
6. If needed, change the **numberOfRetries** setting to a different value. The default setting is 5, indicating that the adapter will make five additional connection attempts after an initial failure before abandoning the sending of that specific HL7 message.
7. If needed, change the **waitBetweenRetries** setting to a different value. The default setting is 1000, indicating that the adapter will wait 1000 milliseconds before making its next connection attempt after an initial connection failure.
8. Save and close the configuration file.
9. Stop the Vital Sync Alarm Reporter Service.
10. Restart the service to implement the new settings.

SMS Configuration Settings

The Vital Sync Alarm Reporter Service is capable of sending alarm information from the platform via SMS message, using the Twilio™* messaging service.

To enable this functionality, each affected user needs the following:

- A valid phone number to which SMS messages can be sent, set up in the Vital Sync™ software using the Manage Users function in the Vital Sync™ informatics manager
- A valid user account with the Twilio™* service, for use in communicating with the REST API

To enable SMS connectivity:

1. Navigate to the directory with the configuration file (for example, **C:\Program Files\Covidien\Informatics**).
2. Open **VitalSync.AlarmReporterService.exe.config**.
3. Find the **<adapterservice.pipeline>** section of the file.
4. Change the **<pluginTypes>** element to contain **SMSPlugin**.
5. Find the **<SMSPlugin>** section of the file.
6. Update the **SMSUserName** setting to reflect the user name associated with the Twilio™* account.
7. Update the **SMSPassword** setting to reflect the password associated with the Twilio™* account.
8. Update the **SMSFromNumber** setting to reflect the phone number associated with the Twilio™* account.
9. Save and close the configuration file.
10. Stop the Vital Sync Alarm Reporter Service.
11. Restart the service to implement the new settings.

Email Configuration Settings

The Vital Sync Alarm Reporter Service is capable of sending alarm information from the platform via email, using an SMTP server.

To enable this functionality, each affected user needs the following:

- A valid email address, set up in the Vital Sync™ software using the Manage Users function in the Vital Sync™ informatics manager
- A valid user account on the SMTP server used for sending emails

To enable email connectivity:

1. Navigate to the directory with the configuration file (for example, **C:\Program Files\Covidien\Informatics**).
2. Open **VitalSync.AlarmReporterService.exe.config**.

3. Find the **<adapterservice.pipeline>** section of the file.
4. Change the **<pluginTypes>** element to contain **EmailPlugin**.
5. Find the **<EmailPlugin>** section of the file.
6. Update the **EmailSMTPUser** setting to reflect the user name associated with the SMTP server account.
7. Update the **EmailSMTPPassword** setting to reflect the password associated with the SMTP server account.
8. Update the **EmailFromAddress** setting to reflect the email from which messages are sent.
9. Update the **EmailSMTPServer** setting to reflect the SMTP server address.
10. Update the **EmailSMTPServerPort** setting to reflect the SMTP server port number.
11. Save and close the configuration file.
12. Stop the Vital Sync Alarm Reporter Service.
13. Restart the service to implement the new settings.

Paging (TAP) Configuration Settings

The Vital Sync Alarm Reporter Service is capable of sending alarm information from the platform to an external paging system (using the TAP protocol), via either a direct COM port connection or a TCP/IP connection.

To enable TAP connectivity via COM port:

1. Navigate to the directory with the configuration file (for example, **C:\Program Files\Covidien\Informatics**).
2. Open **VitalSync.AlarmReporterService.exe.config**.
3. Find the **<adapterservice.pipeline>** section of the file.
4. Change the **<pluginTypes>** element to contain **TAPTranslationPlugin**, **TAPPostProcessingPlugin**, and **TAPOutputPlugin**.
5. Find the **<TAPOutputPlugin>** section of the file.
6. Change settings as follows in this section (all values apply to the COM port to which the paging system is connected):
   a. **portNumber**: Change this to the identifier used for the COM port.
   b. **BaudRate**: Change this to the appropriate baud rate value.
   c. **DataBits**: Change this to the appropriate data bits setting.
   d. **DtrEnable**: Change this value to the appropriate DTR Enable setting.
   e. **RtsEnable**: Change this value to the appropriate RTS Enable setting.

7. Save and close the configuration file.
8. Stop the Vital Sync Alarm Reporter Service.
9. Restart the service to implement the new settings.

To enable TAP connectivity via TCP/IP:

1. Navigate to the directory with the configuration file (for example, **C:\Program Files\Covidien\Informatics**).
2. Open **VitalSync.AlarmReporterService.exe.config**.
3. Find the **<adapterservice.pipeline>** section of the file.
4. Change the **<pluginTypes>** element to contain **TAPTranslationPlugin**, **TAPPostProcessingPlugin**, and **TAPEthernetOutputPlugin**.
5. Find the **<TAPEthernetOutputPlugin>** section of the file.
6. Change the **portNumber** setting to the port number of the TAP paging system.
7. Change the **serverIP** setting to the IP address of the TAP paging system.
8. Save and close the configuration file.
9. Stop the Vital Sync Alarm Reporter Service.
10. Restart the service to implement the new settings.

6.5 LDAP Integration

The application supports integration with an LDAP server for external authentication and authorization of users. The following instructions are intended to assist with configuration of the application for LDAP integration. However, since LDAP server configuration needs can vary significantly, contact Medtronic for approaches and suggestions to consider for LDAP integration.

Configuring for LDAP server authentication requires changing membership and role manager parameter settings in the **web.config** file after installation.

To change the membership and role manager settings:

1. Navigate to the directory with the **web.config** file and open the file.
2. Find the **<system.web>** section of the file.
3. Change the **membership defaultProvider** value to **LdapMembershipProvider**.
4. Change the **roleManager defaultProvider** value to **LdapRoleProvider**.
5. Save and close the configuration file.

Some LDAP-server-related **LdapClient** parameter values relating to connectivity and the structure of the LDAP server schema may also need to be changed. Refer to Table *6-1*.

Table 6-1. Additional LdapClient Parameter Values

LDAP Client Configuration	Description	Default Value
LdapServer	IP address or machine name of the LDAP server on the network	localhost
LdapPortNumber	The port number to use	389
LdapUser	The administrative username	cn=manager,dc=maxcrc,dc=com
LdapPassword	The administrative password	secret
LdapProtocolVersion	The LDAP protocol version to use	3
DistinguishedNameRoot	Root distinguished name used for queries	dc=maxcrc,dc=com
UserIdKey	Key used to represent user ID	uid
UserPasswordKey	Key used to represent user password	userPassword
UserEmailKey	Key used to represent user email address	mail
UserFirstNameKey	Key used to represent user first name	fn
UserMiddleNameKey	Key used to represent user middle name	mn
UserLastNameKey	Key used to represent user last name	ln
GroupMemberKey	Key used to represent group members	member
CommonNameKey	Key used to represent common name of a group or user	cn
UserObjectClass	Class name of the user class	person
RoleObjectClass	Class name of the role / group class	groupofnames
OrganizationalUnitKey	Key used to represent user's organizational unit	ou
OrganizationalUnit	Type of organizational unit	people

6.6 AD Integration

The application supports integration with an Active Directory (AD) server for external authentication and authorization of users. The following instructions are intended to assist with configuration of the application for AD integration. However, since server configuration needs can vary significantly, contact Medtronic for approaches and suggestions to consider for integration.

Configuring for AD server authentication requires changing membership and role manager settings in the **web.config** file after installation.

Note:
To support AD integration, users authenticating against the Active Directory must have permission to query for their user attributes and group memberships in order to synchronize this data in the Vital Sync™ database.

To change the membership and role manager settings:

1. Navigate to the directory with the **web.config** file and open the file.
2. Find the **<system.web>** section of the file.
3. Change the **membership defaultProvider** value to **ActiveDirectoryMembershipProvider**.
4. Change the **roleManager defaultProvider** value to **ActiveDirectoryRoleProvider**.
5. Find the **<ActiveDirectoryClient>** section of the file.
6. Update settings in the existing **<ActiveDirectoryConnection>** section to reflect settings associated with the Active Directory Server. Refer to Table *6-2*.
7. If needed, add more **<ActiveDirectoryConnection>** sections to support other Active Directory servers or search paths.
8. Save and close the configuration file.

Some AD server-related parameter values relating to connectivity and the structure of the AD server schema may also need to be changed. Refer to Table *6-2*.

Table 6-2. Additional AD Server Parameter Values

LDAP Client Configuration	Description	Default Value
ActiveDirectoryServer	AD server path	No default value
AuthenticationType	The type of AD server authentication	Secure
GetAllUserAttributesQuery	Query to obtain user attributes	(&(objectClass=person)(sAMAccountName={0}))
GetRolesForUserQuery	Query to obtain user roles	(&(objectClass=group)(member={0}))
KeyToUseForRolesQuery	Key to use in roles query	distinguishedName
DistinguishedNameKey	Distinguished name key used for queries	distinguishedName
UserIdKey	Key used to represent user ID	cn
UserEmailKey	Key used to represent user email address	mail
UserFirstNameKey	Key used to represent user first name	givenName
UserMiddleNameKey	Key used to represent user middle name	initials
UserLastNameKey	Key used to represent user last name	sn
UserNameActiveDirectoryKey	Key used to represent username	sAMAccountName
RoleNameKey	Key used to represent role name	cn
RoleMappings	Mapping from external role IDs to internal IDs	No default value

6.7 Gateway Configuration

This section provides configuration instructions if using a Lantronix™* PremierWave™* XN or equivalent gateway.

Note:
Making changes to configuration files may adversely affect performance. Do not make changes other than those described in this section. Always use caution when changing configuration files.

Note:
Always make a backup copy of the configuration file before making any changes to it.

6.7.1 Ensuring Unique Device Identifiers

To ensure that all devices communicate a unique device identifier (UDI), thereby assisting clinicians in easy identification of the device within the user interface, the platform supports integration with the Lantronix™* PremierWave™* XN gateway. Users can configure the gateway to transmit identity information upon initial connection from a device, to ensure that every device is properly identified.

Medtronic recommends using this specific gateway, with identity turned on, when connecting to the following devices:

- Nellcor™ N595, N600, N600x, or N600x-A pulse oximeters
- Puritan Bennett™ PB840 or PB980 ventilators
- INVOS™ 5100C regional saturation monitor

For devices with a serial number (including the Puritan Bennett™ PB840 and PB980 ventilators, the Nellcor™ PM1000N bedside respiratory patient monitoring system, and the Oridion™ Capnostream 20 and Oridion™ Capnostream 20P capnography monitors), always use the device serial number as the UDI number, to ensure correct device auto-association in the application. If the device sends a serial number different than the UDI number, the serial number will be changed after the device is connected, causing auto-association to not work properly. This also leads to user confusion, since the serial number of the device will visibly change in the application.

Also, for the DCI and Breath connections for the Puritan Bennett PB840 or PB980 ventilators, always use the same serial number for both connections, ensuring that this number matches the serial number of the ventilator. These connections provide a serial number; once it is changed, it will be different than the one specified for the UDI. Therefore, not using the serial number as the device identifier will cause the linking logic to work improperly.

6.7.2 Configuring Unique Device Identifier Settings on the Gateway

The Unique Device Identifier (UDI) configuration settings on the Lantronix™* PremierWave XN gateway are in the Tunnel menu. Refer to the gateway instructions for details on accessing this menu.

To configure UDI settings:

1. Select the tunnel (**Tunnel 1** or **Tunnel 2**).
2. For the connection mode, select **Always**.
3. Click on the **Host 1** or **Host 2** box.
4. In the **Address** box, enter the IP address for the appropriate Vital Sync Virtual Patient Monitoring Platform and Informatics Manager server.
5. In the **Port** box, enter the port on which the software is listening.
6. Set the **Initial Send** box as follows:
   <PWXN_UDI><SERIAL>%s</SERIAL><MACID>%m</MACID>
   <CUSTOM>SomeOtherString</CUSTOM></PWXN_UDI>
7. Choose the **Text** option.
8. Save the configuration settings.
9. Reboot the gateway to implement the new settings.

6.8 High Availability Failover

For high availability requirements, it is possible to set up secondary failover servers for the application. Contact Medtronic Professional Services to review approaches and suggestions to consider.

6.9 Customizable XSLT Email Subjects

The software supports customization of XSLT email subjects. Consult Medtronic Professional Services for details.

Index

Index

Rx ONLY

Part No. PT00094643 Rev B 2018-12

U.S. patents:
www.medtronic.com/patents

Made in USA. Printed in USA.

Covidien llc
15 Hampshire Street, Mansfield, MA 02048 USA

www.medtronic.com [T] 1.800.635.5267

Medtronic