Baxter

SmartCare Remote Management — cloud version

Setup guide

This product may contain software known as “free” or “open source” software (FOSS). Baxter uses and supports the use of FOSS. We believe that FOSS makes our products more robust and secure and gives us and our customers greater flexibility. To learn more about FOSS that may be used in this product, please visit our FOSS website at baxter.com/opensource. Where required, a copy of FOSS source code is available on our FOSS website.

For information about any Baxter product, contact Baxter Technical Support:
baxter.com/contact-us

REF 80028398 Ver. F

Revision date: 2024-01

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

baxter.com

Contents

Introduction

Purpose

SmartCare Remote Management helps the user to service assets, such as devices or beds, remotely. It supports the following service-related tasks.

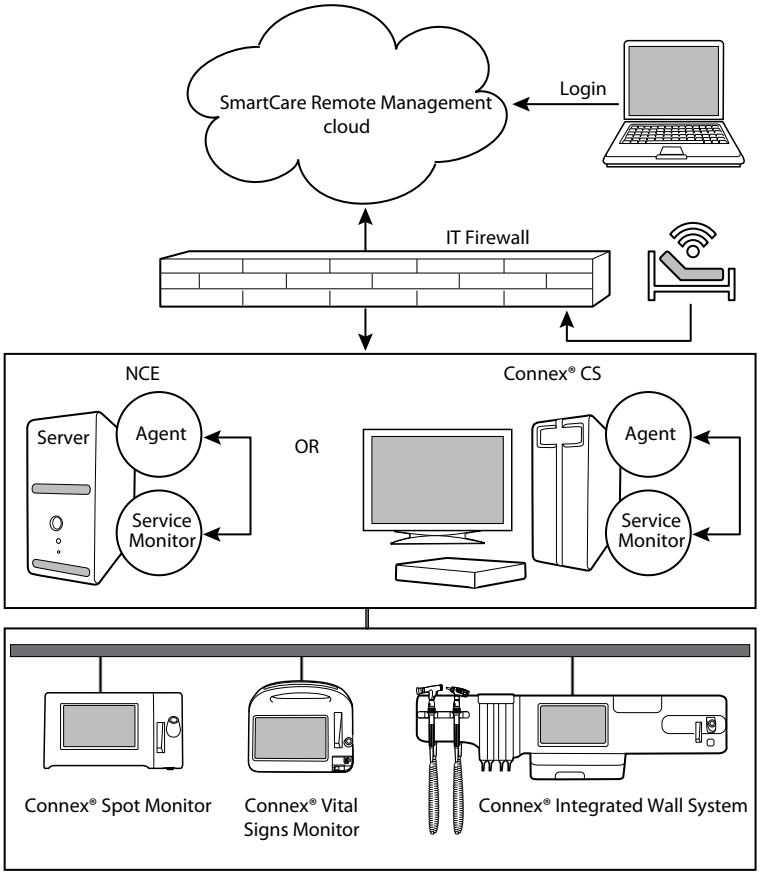
NOTE The specific items from the list below that apply to your asset may vary depending on asset type.

NOTE See *SmartCare Remote Management instructions for use* for a more detailed product overview and a more detailed purpose description.

- Remote update configuration
- Remote upgrade asset firmware
- Review asset preventive maintenance due date
- Remote asset log retrieval
- Remote asset location tracking
- Error code notification

Architect design

Assets that are compatible with **SmartCare** Remote Management appear in the diagrams below. Connections to your network, whether wired or wireless, vary by configuration and/or asset type. For any of these assets at your facility, **SmartCare** Remote Management provides quick access to cloud-based service data.



System requirements

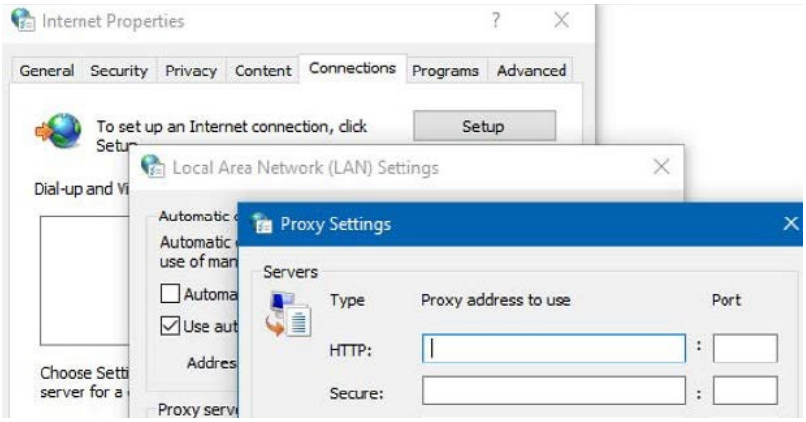
Vital signs assets that use **PartnerConnect** must have either the **Connex** Clinical Surveillance System (**Connex** CS) or **Connex** Device Integration Suite – Network Connectivity Engine (CDIS-NCE) system installed, and the asset's network must be configured to use Network Rendezvous Service (NRS) communication.

Proxy server requirements for the **PartnerConnect** Agent

You may choose to route internet traffic through a Proxy Server (optional).

The following requirements must be met for this option to work.

- The proxy needs to be configured to handled HTTP/HTTPS traffic to through port 443. If the proxy is subject to firewall rules, inbound traffic on the proxy port and outbound traffic need to have rules to allow this traffic. Any other rules (e.g. to disable ports not expected to be used by the proxy) are up to the customer.
- Configure the firewall (local or infrastructure) to connect to the appropriate proxy port number.
- Enable the proxy from the agent machine by following the steps below to configure the control panel settings:
  1. From Control Panel, navigate to Internet Options.
  2. Select the **Connections** tab.
  3. Choose **LAN settings**.
  4. Click the checkbox to enable the proxy server.
  5. Click **Advanced**.



  6. Configure the HTTP and SECURE fields to point to the proxy and to the configured port for proxies that typically use the CONNECT feature. This turns an HTTP proxy connection into a TCP proxy connection, effectively removing the ability for the proxy itself to read the transmitted data.

Host hardware/OS for the **PartnerConnect** Agent

Supported operating systems	
Server	**Micosoft Windows** Server 2016
	Micosoft Windows Server 2019

Computer requirements	
Processor	1.4 GHz 64-bit processor
RAM	8 GB
Disk space	32 GB

Network connection	
NIC	1 GB or higher recommended

Network configuration

To ensure the system functions properly, you may update your network according to the following table:

Application/service	Domain name, IP address, port	Protocol	Connection
PartnerConnect Agent	iot.hillrom.com 52.224.38.138 Port: 443	TCP (HTTPS)	External
Welch Allyn Service Monitor	283 7721	TCP TCP	Internal Internal
SmartCareRemote Management	https://smartcareremotemanagement.hillrom.com 52.224.38.138 Port: 443 For beds: MQTT Port: 8883	TCP (HTTPS)	Not applicable
RetinaVue 700 Fleet Management Server	Production Service: https://service.retinavue.net Port:22	TCP (SFTP)	External
DCP	NRS port: 7711	UDP	Internal
File outbound types	.log,.zip, .txt, .csv	Not applicable	Not applicable
File inbound types	.tar.gz, .tar, .zip, .pim, .xml, *.settings, *.txt, *.pdf, .wa update, *.bas, *.json, .csv	Not applicable	Not applicable

Application and asset compatibility

Asset name	Min. software
Centrella Smart+ Bed	1.36.000
Progressa Smart+ Bed	1.0
CVSM (**Connex** Vital Signs Monitor)	2.x or later except version 2.40.x  **NOTE** Emulate **Spot** Vital Sign Lxi must be disabled for the asset to show up on **SmartCare** Remote Management.
CIWS (**Connex** Integrated Wall System)	2.x or later except version 2.40.x  **NOTE** Emulate **Spot** Vital Sign Lxi must be disabled for the asset to show up on **SmartCare** Remote Management.
CSM (**Connex Spot** Monitor)	1.24 or later
Connex CS (Central Station Server)	1.8x, 1.7x
Connex CS (Central Station Client)	1.8x
Connex CS (Central Station Standalone)	1.8x
DCP	3.0.1.1
CDIS-NCE/Cerner VitalsLink	5.1.0.16
RV700 (**RetinaVue** 700 Imager)	1.30.00-A0002 or later
Welch Allyn Configuration Tool	1.8.9 20181220 or later

Determine account infrastructure layout

NOTE This section is not applicable to the **RetinaVue** 700 Imager, for which data is inherited from the **RetinaVue** Network. It is also not applicable to the **Centrella Smart+** Bed and the **Progressa Smart+** Bed.

A single installation supports up to 2,000 connected assets. If an organization has more than 2,000 connected assets between locations, then you must use multiple server installations.

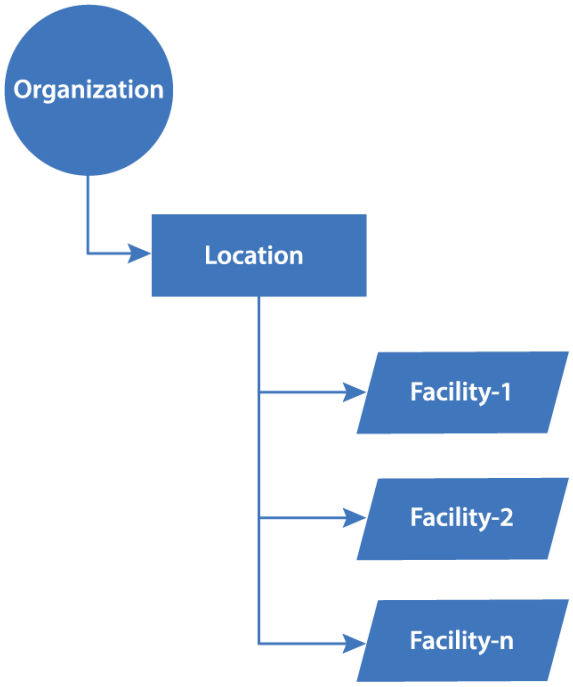
SmartCare Remote Management offers a 3-level organization hierarchy: organization, location, and facility. Depending on how you want to view and manage your assets, you have flexibility in how you utilize the hierarchy. Organization and location are defined at the time of installation. Facility is defined based on the asset location configuration field.

The layout options in the diagrams below offer guidance to help you to determine your **SmartCare** Remote Management layout and installation. The "Layout options graphic key" provides information to accompany the diagrams.

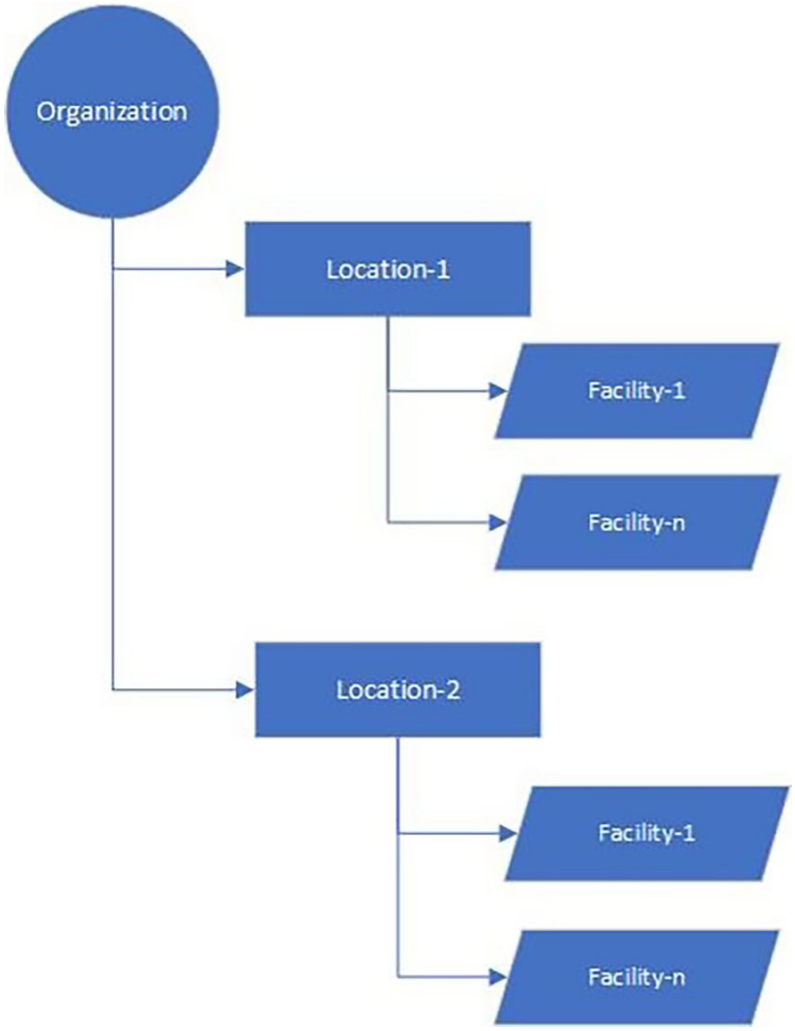
Layout options graphic key

Organization	Organization is the highest node level. You may choose to have more than one organization node.
Location	Location is the second node level. You may choose to have more than one location under an organization. The installation sets the organization-location level. For user access, you may request to set up users who can only view and manage a single location.
Facility	The facility node level is not set during the installation. It is driven by asset configuration, such as asset location and asset tag configurations.

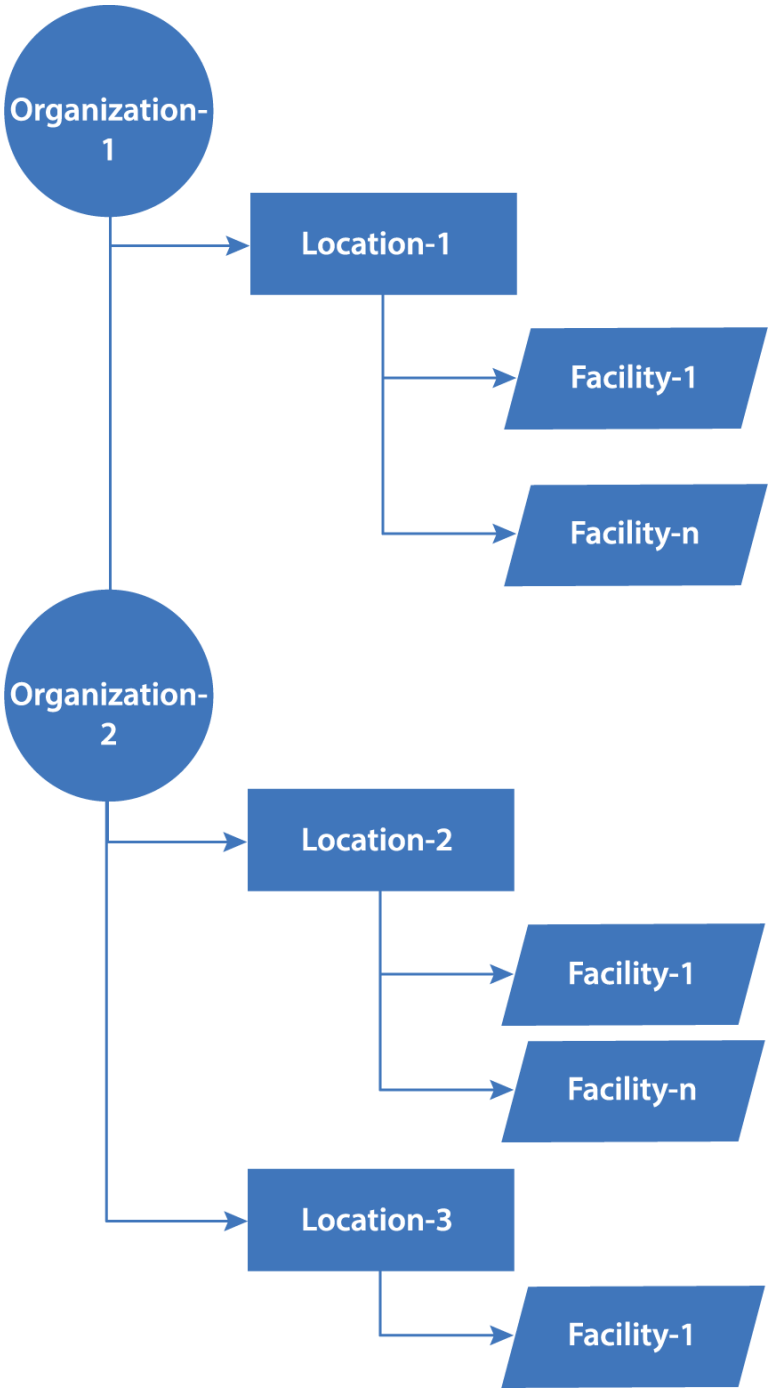
Option 1 – Single server installation with 1 location and up to 2,000 connected assets.



Option 2 – Single organization, two or more locations, with multiple facilities and at least two server installations, as well as more than 2,000 connected assets.



Option 3 – Multiple organizations, two or more locations, with multiple facilities and at least three server installations, as well as more than 2,000 connected assets.



Configuration request for SmartCare Remote Management

The Baxter Solution Architect should open a sales lead in Sales Force and assign it to a project manager.

Third party suppliers: Please submit an email request to servicehub@hillrom.com with subject line "Service Hub Request."

When the above is completed, Baxter will respond to the request with an email containing a ticket number and a checklist of items that need to be sent back by replying to the email.

Reply to this email with the following information to have **SmartCare** Remote Management set up correctly; any request without the items above will be rejected and delayed.

NOTE Use the Administrator's Guide and not this email alone, as the email only details the information that Baxter requires for setting up the account in the **PartnerConnect** cloud system.

The checklist will be similar to the one below.

- Project manager's name:

  ☐ Contact name

  ☐ Contact email address

- Customer/**SmartCare** Remote Management user contact information:

  ☐ Company name

  ☐ Contact name

  ☐ Contact phone number

  ☐ User email address(es) to be used for **SmartCare** Remote Management access

  ☐ Configuration tool login email address (if available)

- For CSM and CVSM/CIWS assets that use Gateway Agent, the customer's operating system is supported, and the customer's host hardware/OS meets requirements:

  ☐ **Microsoft Windows** 2016

☐ **Microsoft Windows** 2019

- For CSM and CVSM/CIWS assets, the customer's network is preconfigured for the appropriate application/configurations:

  ☐ **PartnerConnect**

  ☐ Service Monitor

  ☐ DCP

  ☐ NCE/Cerner Vitals Link

  ☐ **Connex** CS

- Type of **SmartCare** Remote Management account:

  ☐ Existing update – Include user email address

  ☐ New

- Software applications that Baxter must install for CSM and CVSM/CIWS assets:

  ☐ **PartnerConnect**

  ☐ Service Monitor

  ☐ DCP

  ☐ NCE/Cerner Vitals Link

  ☐ **Connex** CS

- Supported assets/applications meet minimum software versions:

  NOTE Confirm the latest supported versions with the *SmartCare Remote Management — cloud version Setup guide*.

  ☐ **Centrella Smart+** Bed – 1.36.000

  ☐ **Progressa Smart+** Smart+ Bed – 1.0

  ☐ CIWS (**Connex** Integrated Wall System) – 2.x or later except version 2.40.x

  ☐ CSM (**Connex** Spot Monitor) – 1.24 or later

  ☐ CVSM (**Connex** Vital Signs Monitor) – 2.x or later except version 2.40.x

  ☐ **Connex** CS (Central Station Server) – 1.8x or later

  ☐ **Connex** CS (Central Station Client) – 1.8x or later

  ☐ DCP – 3.1.0

  ☐ NCE/Cerner VitalsLink – NCE 5.1.0.16

☐ NCE/Cerner Vital Links – NCE 5.1.0.16

☐ RV700 (**RetinaVue** 700 Imager)

- Number of CSM and CVSM/CIWS assets that each **PartnerConnect** Agent instance will support:

  ☐ ≤ 2,000 (per single agent installation)

  ☐ > 2,000 (per single agent installation)

- Requested infrastructure layout for the account (for CSM and CVSM/CIWS assets only):

  NOTE Confirm the latest supported options with the *SmartCare Remote Management — cloud version Setup guide*.

  ☐ Single server, Option 1 – One bootstrap.json file

  ☐ Two or more servers, Option 2 – Two or more bootstrap.json files

  ☐ Two or more servers, Option 3 – Three or more bootstrap.json files

- Single sign-on (customer option) requirement:

  NOTE The single sign-on method allows customers to authenticate their credentials through the company's existing Active Directory (**Windows** login). This method eliminates the need to provide a username and password at every login.

  NOTE Single sign-on is available to customers with corporate accounts that are compatible with SmartCare Remote Management.

  ☐ Confirm that customers are using the cloud-based **Microsoft** Azure Active Directory (no on-prem legacy). The user authentication must be compatible with the **SmartCare** Remote Management single sign-on option.

- Attachments that are required:

  Signed Statement of Work (SOW). See the software subscription agreement (DIR 20017092).

  bootstrap.json files, quantity dependent on option selected above (only applicable to **PartnerConnect** Agent and CSM and CVSM/CIWS assets)

  NOTE Important! Any request without the items listed above will be rejected and will not result in setup.

Software requirements and installation

NOTE The "Software requirements and installation" section is not applicable to any of the following assets: the **RetinaVue** 700 Imager, the **Centrella Smart+** Bed, and the **Progressa Smart+** Bed.

Prepare for software installation

1. Run an installation to update to the latest version, regardless of the installed version.
2. Verify all system requirements are met.
3. See "Determine account infrastructure layout." If you have Option 1 with more than 2,000 assets, Option 2, or Option 3, then the following applies: Each server that does not have **Connex** CS or NCE will need to have DCP, Service Monitor, and **PartnerConnect** Agent installed. DCP will need to be configured on these servers to have vital signs routed to port 281 for one of the following ordinals: 5, 8, or 12, depending on the type the customer is using to point to the NCE or **Connex** CS server. Configure port 281 on ordinal 8 for the service monitor connection pointing to the server with DCP installed.
4. Obtain **PartnerConnect** agent software.
5. Obtain **Welch Allyn** Service Monitor software.
6. Ensure you have administrator's rights on the host machine.
7. Ensure you have chosen an Account Infrastructure Layout option. (See "Determine account infrastructure layout.")

NCE software installation

For details about installing NCE, follow the installation instructions provided as needed by the project manager. These instructions are not part of this document as the installation should be done prior to this step.

Install PartnerConnect software

NOTE If you have already installed **PartnerConnect**, please see the "Removing PartnerConnect software" section for instructions about uninstalling previous versions.

1. Access the **PartnerConnect** file provided to you. To request the **PartnerConnect** software, you can contact customer service at:

Phone: +1 800 535 6663
Fax: +1 315 685 4091

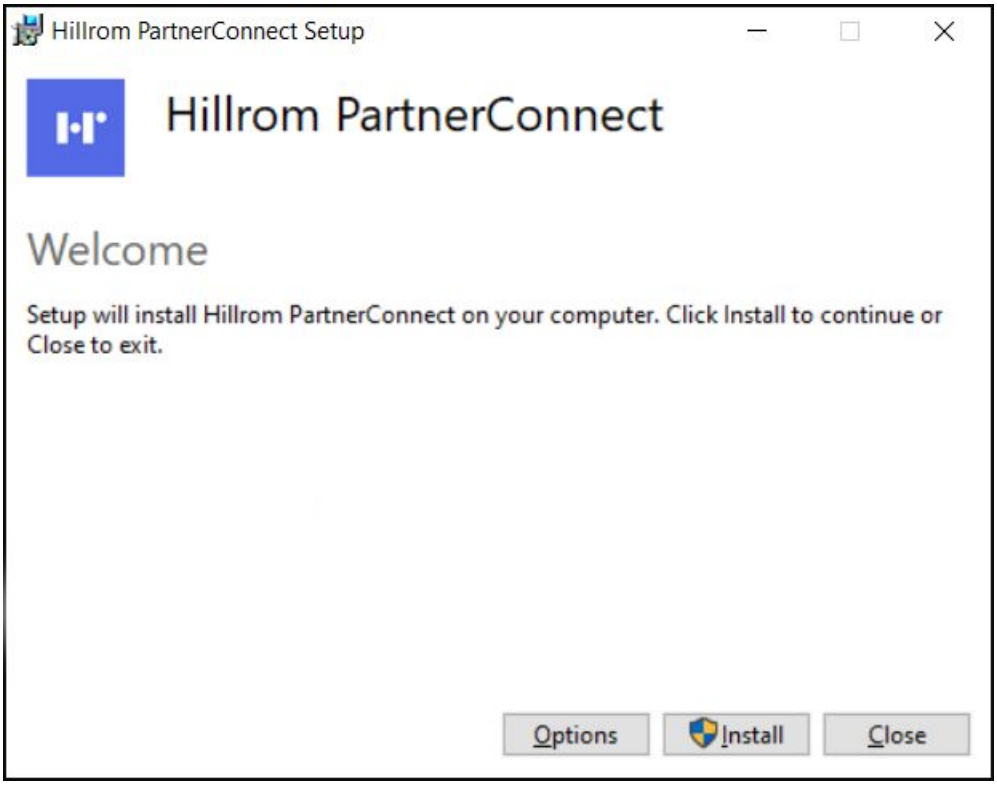
Welch Allyn Inc. Corporate Headquarters
4341 State Street Road
Skaneateles Falls, NY 13153

Or, you can find your nearest location at www.baxter.com/location-selector

During the interaction with Baxter support, you will provide a user ID (email address) and password. You will use this login information during the software download and again for the registration process below.

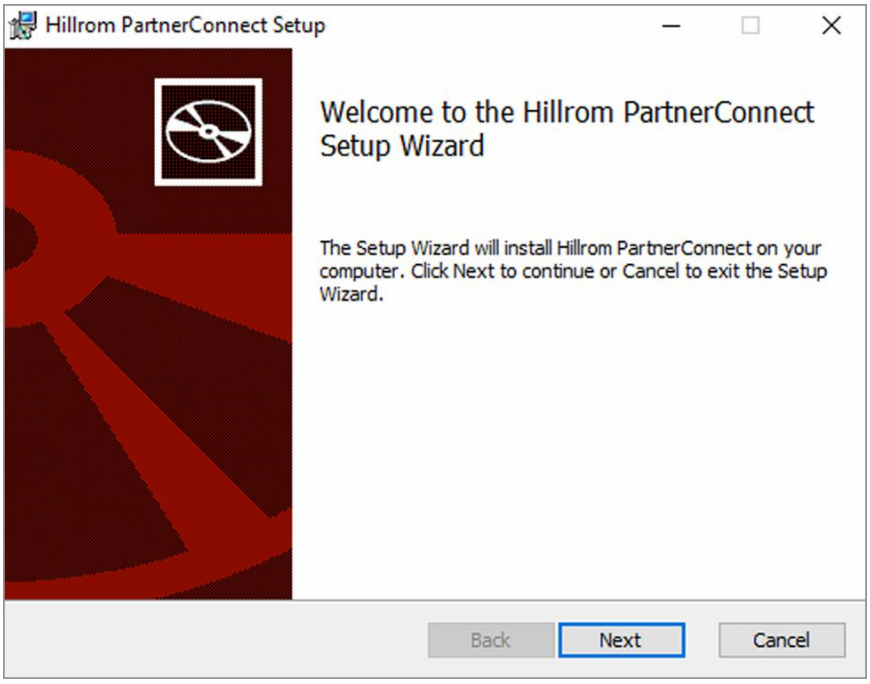
2. Extract the installation program, PartnerConnect.exe, from the zip file.
3. Double click the PartnerConnect.exe file.

   The Setup screen appears.



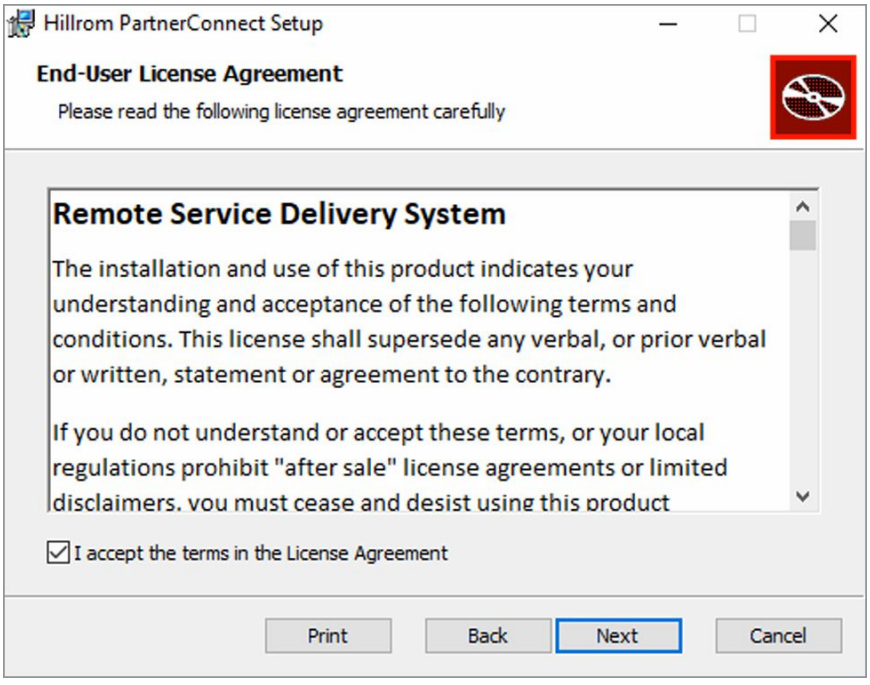
4. Click **Install**.

The Welcome screen appears.



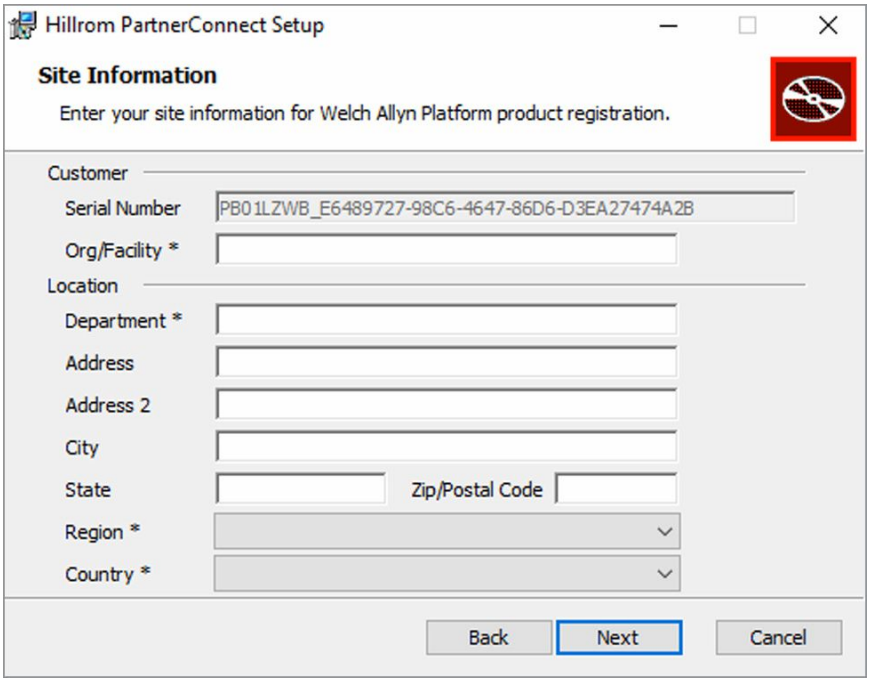
5. Click **Next**.

The License Agreement screen appears.



6. Check to accept the license and click **Next**.

The Site Information screen appears.



NOTE After accepting the license agreement, if a previous version of **PartnerConnect** was installed, you will be prompted to uninstall.

7. Enter the site information that you need to register **PartnerConnect** for your organization.

NOTE The following table provides additional details about the fields that you need to complete. This information allows Baxter to quickly and efficiently locate this system for remote connection.

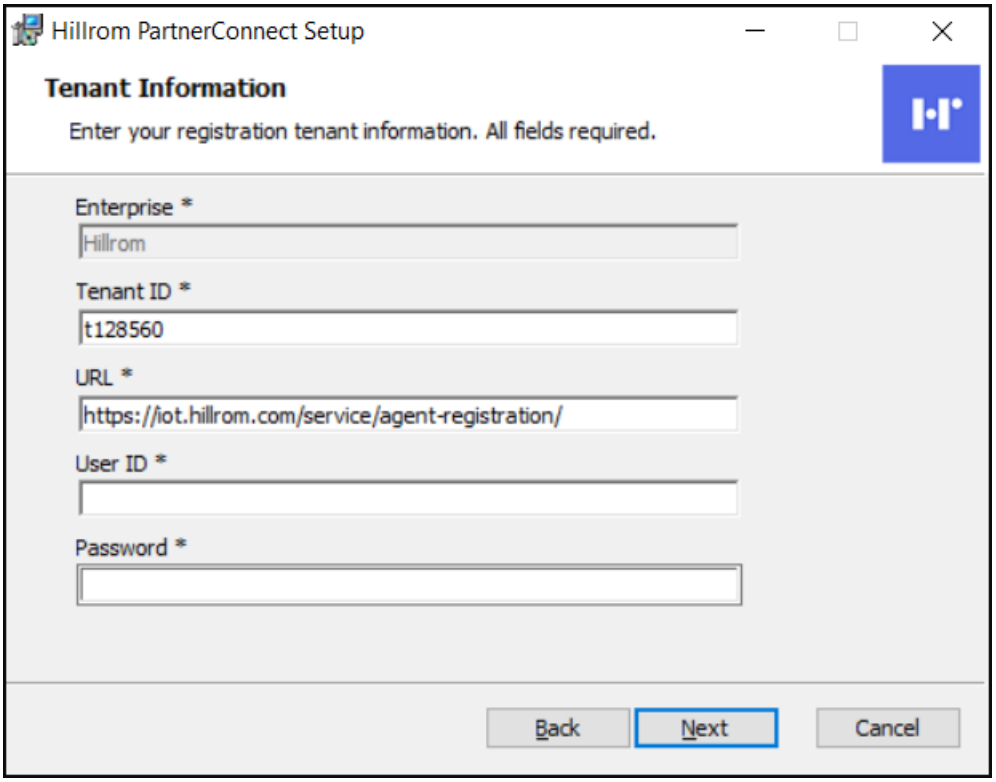
NOTE Ensure that the **Org/Facility** name or any other field does *not* contain special or non-English characters because **PartnerConnect** does not support them.

Field	Description
Customer	
Serial Number	This field auto-populates.
Org/Facility*	Enter the organization (customer) name followed by its city and state (for example, ABC Hospital System-New York NY). For more information, see your product documentation.
Location	
Department*	Enter your department information.
Address 1 and 2	Enter the street address or post office box.
City	Enter the city of the organization location.
State	Enter the state or province of the organization location.
Region*	Select a region that matches your location from the pull-down list.
Country*	Enter the country of the organization location.

* Required field

8. Confirm settings and click **Next**.

   The Tenant Information screen appears. See the example below.



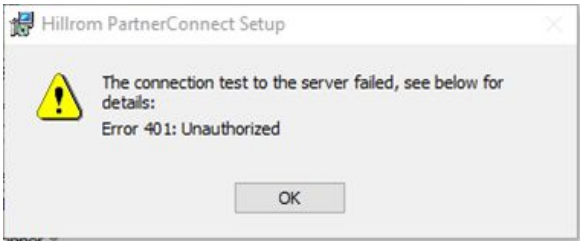
   The installer will auto-populate the Tenant ID and the end-point URL. Enter the user ID and password used during account setup with **s**upport.

9. If you are prompted to uninstall a previous version of PartnerConnect, follow the uninstall prompts and then continue.

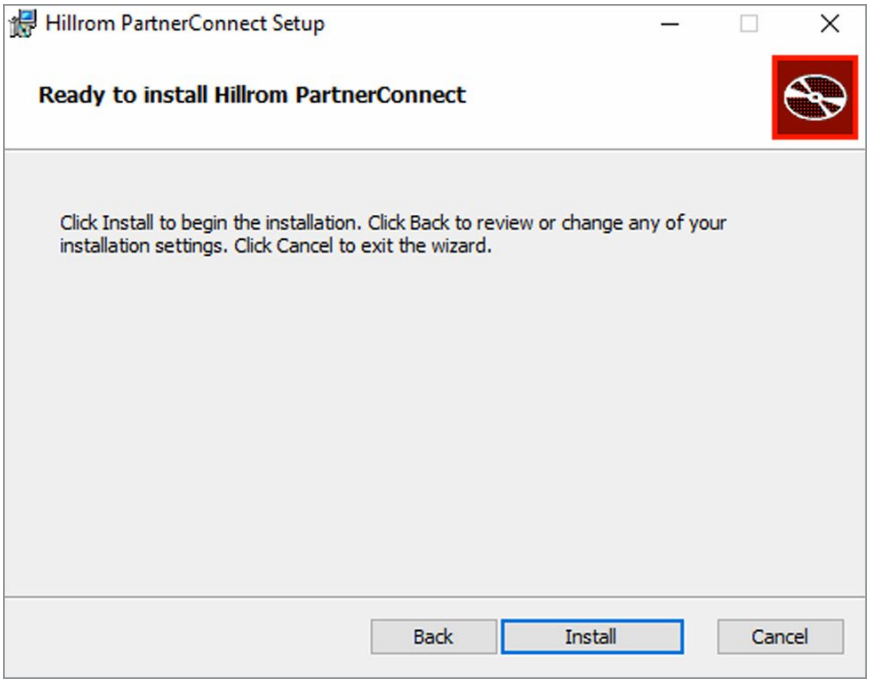
10. Click **Next**.

    The installer will then perform a connection test to the service platform.

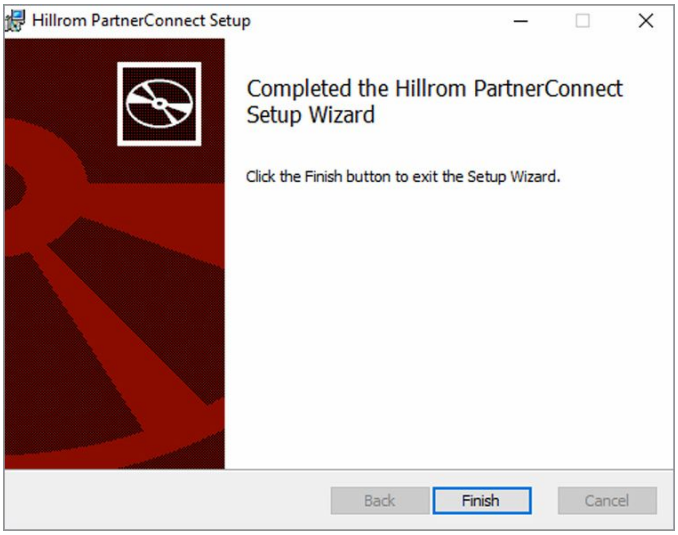
    NOTE An error message will appear if there is a problem completing this test. See the image below. If you receive this message, please verify your user ID and password are correct, confirm you have Internet access, and try again. Otherwise contact technical support.



    If no error message appears, the installer is ready to begin the installation.



11. Click **Install** to install **PartnerConnect**.



Setup verifies a successful installation.

12. Click **Finish** to exit the Setup wizard.

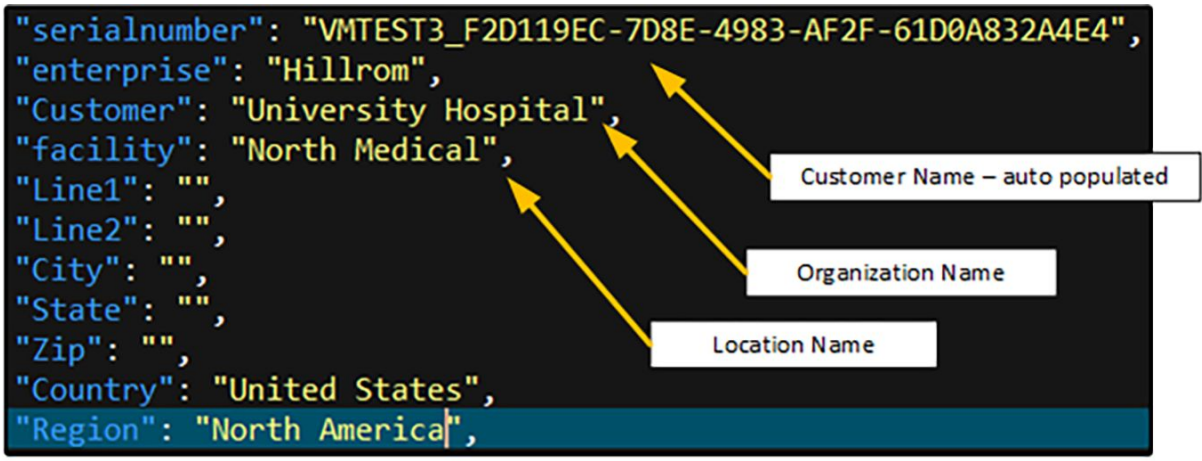
    The "Installation Successfully Completed message" displays.

13. Click **Close**.

    NOTE To complete your registration, please contact your Baxter support representative to activate your account.

14. To verify the successful installation and registration and to collect registration information for setting up your **PartnerConnect** Remote Management access, please obtain the following file: C:\Program Files (x86)\Welch Allyn\PartnerConnect\config\bootstrap.json

    The file contains the following information as the result of a successful installation:



Moving a device from one **PartnerConnect** agent to another

If you are moving a device from one **PartnerConnect** agent to a new or different one, the device will not connect to the new agent until you remove the device from the former agent.

Devices need **PartnerConnect** to register to **SmartCare** Remote Management. The **Welch Allyn** Service Tool (WAST) also uses the **PartnerConnect** agent with which it is associated and that is on the same computer on which it is installed. Because of this association, sometimes you may need to move a device from one **PartnerConnect** agent to another.

Moving a device connected to the Welch Allyn Service Tool

New devices that connect to the **Welch Allyn** Service Tool (WAST) first before connecting to **SmartCare** Remote Management will register to the **PartnerConnect** agent associated with WAST. In this case, contact Baxter Support to register the new device to **SmartCare** Remote Management.

NOTE You may prevent a new device from registering to the **PartnerConnect** agent on WAST by stopping the **PartnerConnect** service on the computer where WAST is installed. For example, you may want to do so if calibration, certificate downloads, or firmware updates are needed. After the work is done, restart the **PartnerConnect** service.

Moving a device currently in SmartCare Remote Management

If your device is currently registered in **SmartCare** Remote Management and it will be used in WAST, then you do not need to take any actions.

The **PartnerConnect** Agent that works with WAST pulls firmware from the cloud and stores the data locally. Services through WAST only need a local connection, so you do not need to register the device to the **PartnerConnect** agent.

NOTE If you have multiple **PartnerConnect** agents and, therefore, do need to move the device from one agent to another, you can delete the device in **SmartCare** Remote Management from the first agent so that it can register to the second agent.

Download and install the **Welch Allyn** Service Monitor application

NOTE As a reminder, this section is not applicable to **RetinaVue** 700.

1. Navigate to https://smartcareremotemanagement.hillrom.com and Scroll and click **Service Monitor** to download.
2. Log in to your host server as Administrator.
3. Start **Windows Explorer** and open the Service Monitor download.
4. Double click **setup.exe**.

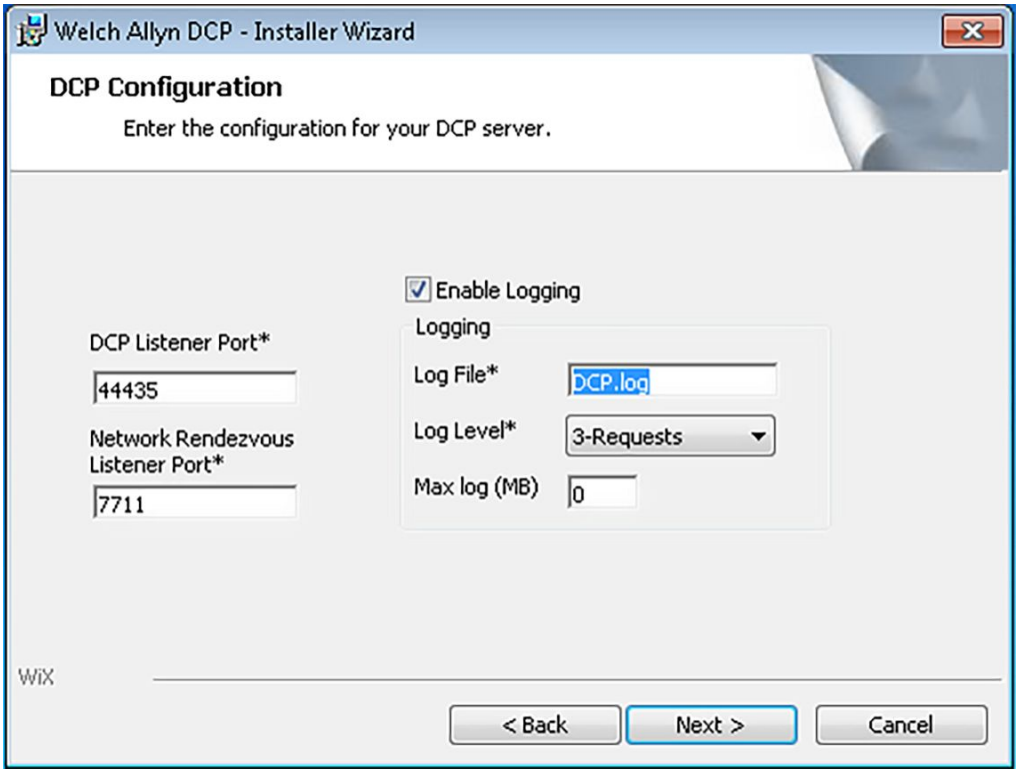
   The installation package setup wizard screens appear.
5. Click **Next**.
6. Click **Next** without changing the installation location.
7. Click **Install**.
8. Click **Close**.

   The Service Monitor application is installed.

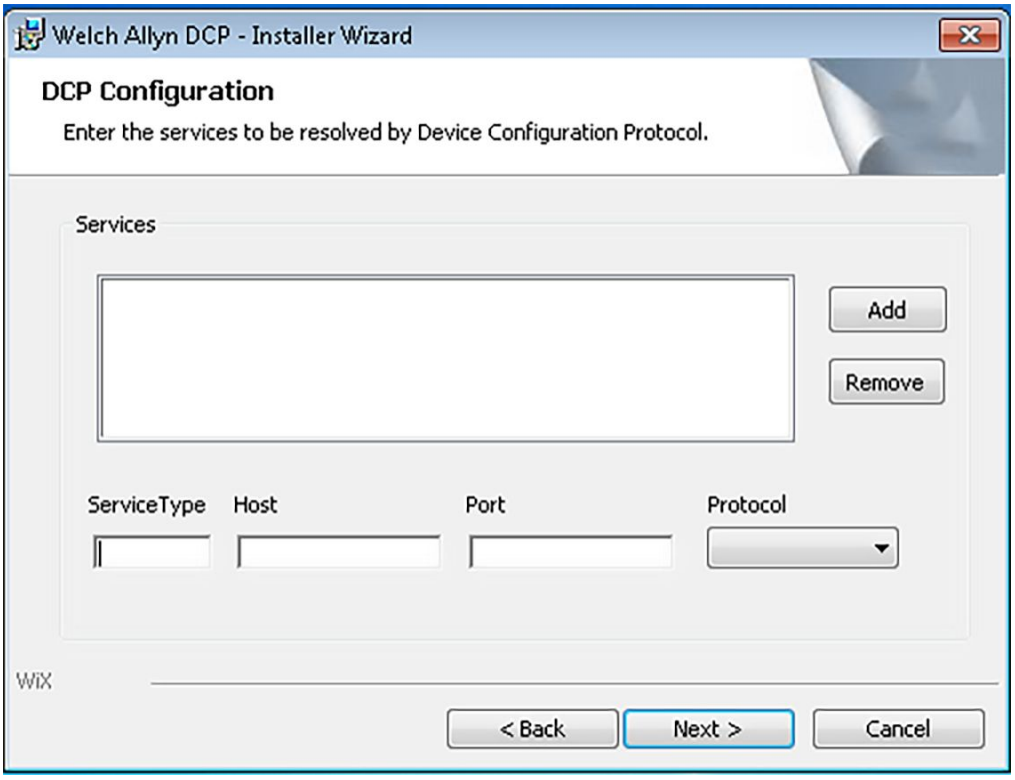
Download and install the **Welch Allyn** DCP application

This is for a **SmartCare** Remote Management dual server option that is not on a **Connex** CS or NCE installation. The DCP component is part of a CDIS-NCE system. The CDIS-NCE documentation provides comprehensive DCP installation and configuration instructions.. The following steps are for your reference only and are only applicable for the **SmartCare** Remote Management system setup.

1. Log in as Administrator.
2. Navigate to http://smartcareremotemanagement.hillrom.com and scroll and click **DCP** to download.
3. With the exception of the screens called out below, install the software by selecting **Next** or similar on each screen.

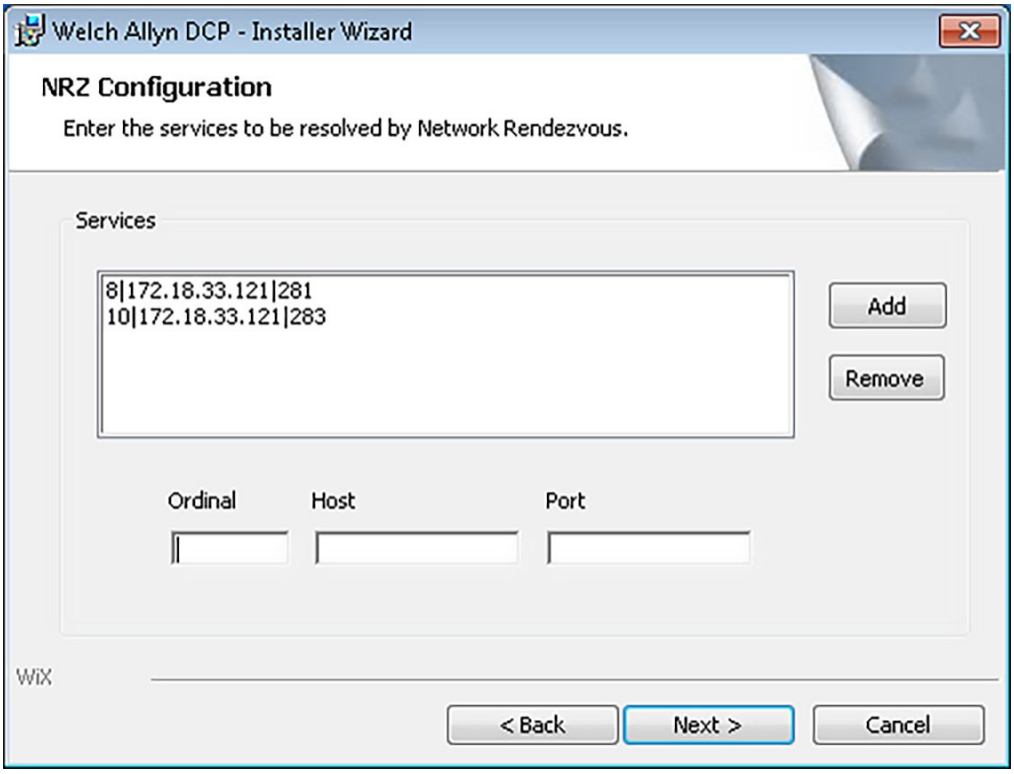


4. Skip the next screen for CVSM and CSM. (See below.)



5. Update ordinal settings to include ordinal 10 as shown below.

Ordinal	Description	Host	Port
10	Remote services	IPv4 address of the Service Monitor server	283



Welch Allyn Product Configuration Tool (CSM only)

Perform the steps below to create an account if an existing account is not present for the organization. If an account is already created, there is no need to create a new account.

1. Go to the following website: https://config.welchallyn.com/configurator/
2. Click **Register Here**.
3. Populate the request form with user details. The email address must be professional business email only: Gmail or Yahoo accounts cannot be used.
4. Click **Register**.

System verification

This chapter explains how to verify your system setup and proper access to your account.

Verify that the asset can connect to the data gateway software (for CSM and CVSM/CIWS assets)

This process verifies that the asset can connect to the wireless network, that there is a valid network path to the server, that DCP is configured correctly (for NCE installations only), and that NCE is installed correctly.

1. From the asset, navigate to the server display and go to **Settings > Advanced > Network > Server**.
2. Touch the **Test** button.
3. If the test fails, check the following (and try again).
    a. Make sure the asset has an IP address.

        CVSM: Navigate to **Settings > Advanced > Network > Status**.

        CSM: Navigate to **Settings > Advanced > Service > Ethernet stats**.

    b. Make sure the asset's connectivity is set to NRS IP. To check, navigate through the following path: **Network > Server > Connectivity**.
    c. Make sure the asset's IP address is set to the server address containing DCP software. To check, navigate through the following path: **Network > Server > IP Address**.
    d. Make sure the asset's Port is 7711. To check, navigate through the following path: **Network > Server > Port**.
    e. Make sure the server(s) have the following ports open: TCP 281, TCP 283, UDP 7711, UDP 293.

Acceptance Criteria: After touching the test button, the asset contains a message stating that the test passed.

Verify that the asset can connect to remote service

This verifies that the asset can connect to the wireless network, that there is a valid network path to the server, that DCP is configured correctly, and that the Service Monitor and **PartnerConnect** are configured correctly.

NOTE **PartnerConnect** does not support devices moving from one agent to another. Turn off the PartnerConnect service during device updates using the **Welch Allyn** Service Tool (WAST). Otherwise, your asset may not appear in **SmartCare** Remote Management, and you will need to contact Baxter support.

Verify **Connex** Vital Signs Monitor/**Connex** Integrated Wall System connection

1. From the device, navigate to the Server display and go to **Settings > Advanced > Service**.
2. Touch the PartnerConnect **Sync with server** button.
3. If the test fails, check the steps in the "System requirements" section (and try again).
4. If it passes, go to **SmartCare** Remote Management (https://smartcareremotemanagement.hillrom.com) and verify that the device is visible under the new account and is online.

Verify **Connex** Spot Monitor connection

1. From the device, navigate to the Server display.
2. Go to **Settings > Advanced > Settings > Service > General**.
3. Touch the Service Monitor **Sync Now** button.
4. If the test fails, check the steps in the "System requirements" section (and try again).
5. If it passes, go to **SmartCare** Remote Management (https://smartcareremotemanagement.hillrom.com) and verify that the device is visible under the new account and is online.

Acceptance Criteria: After touching the **Sync with server** button the device contains a message stating that the test passed.

Verify **RetinaVue** 700 connection

1. From the device, navigate to the main Patients screen.
2. Touch the menu button in the lower left corner of the screen.
3. Touch **Settings**.
4. Scroll to and touch **Advanced settings**.
5. Press **Service connection**.
6. Press **Sync now**.

   The screen will display the message “Syncing in progress...” Once the sync is complete, the screen will display the message “Sync with server is complete.”

Verify **Centrella Smart+** Bed or **Progressa Smart+** Bed connection

1. From the bedside display (GCI), touch the **Settings** menu control.
2. Touch **Bed Service**.
3. Enter **812** and then touch **Enter**.
4. Navigate to the Remote Service option.

5. Touch **Remote Service**.

   The screen shows the customer name.

6. If the screen does not show the customer name, touch **Update Facility**.

Verify account setup

NOTE This is completed after Baxter performs the configuration setup of the **SmartCare** Remote Management account for you.

1. Go to https://smartcareremotemanagement.hillrom.com.
2. Log in to the account with your username/password.
3. For a **PartnerConnect** Agent with CSM and/or CVSM/CIWS, verify that the organization, location, and facility setup match the user configuration of each option.
4. For the **Centrella Smart+** Bed or the **Progressa Smart+** Bed, verify that the organization and location are populated based on the Baxter sales record.
5. Verify that the assets show up on **SmartCare** Remote Management.
6. Verify that the customer's configuration files (CSM only) appear on the account and match what is present on the Configuration Tool.

Appendices

Appendix A – Statement of work (SOW) and warranty terms

The SOW, also referred to as the Scope of work document or Statement of work document, must be completed before the performance of any installation work. See the software subscription agreement (DIR 20017092).