Baxter

SmartCare

Remote Management — cloud version

Setup guide

Baxter, Centrella, Connex, PartnerConnect, Progressa, RetinaVue, SmartCare and Welch Allyn are trademarks of Baxter International Inc. or its subsidiaries.

Any other trademarks, product names or brand images appearing herein are the property of their respective owners.

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 at https://baxter.com/contact-us.

REF 80028398 Ver. K

Revision date: 2025:03

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

baxter.com

Contents

Introduction

Purpose

SmartCare Remote Management allows you to remotely service connected Baxter products. The list below contains all the service-related and monitoring tasks available.

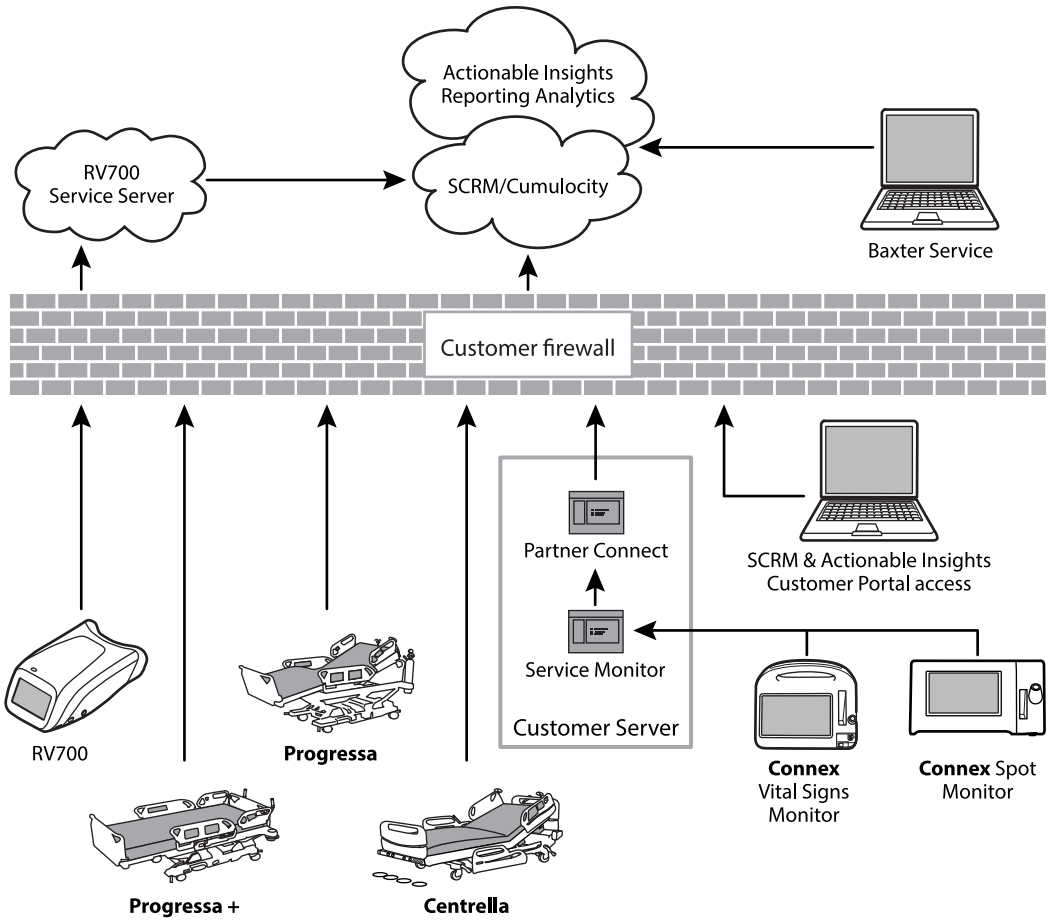
NOTE Some features in the comprehensive list below may not apply to your connected Baxter products. Contact your Baxter representative for information about the specific features that are available for your connected Baxter products.

- Remotely retrieve logs
- Track preventive maintenance
- View error code notifications
- View component health alerts
- Access and print report
- Access and deploy configuration and custom data files
- Upgrade firmware
- Locate connected Baxter products via access point (AP) mapping information

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.

NOTE See the *SmartCare Remote Management Feature compatibility matrix* for more information.



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.

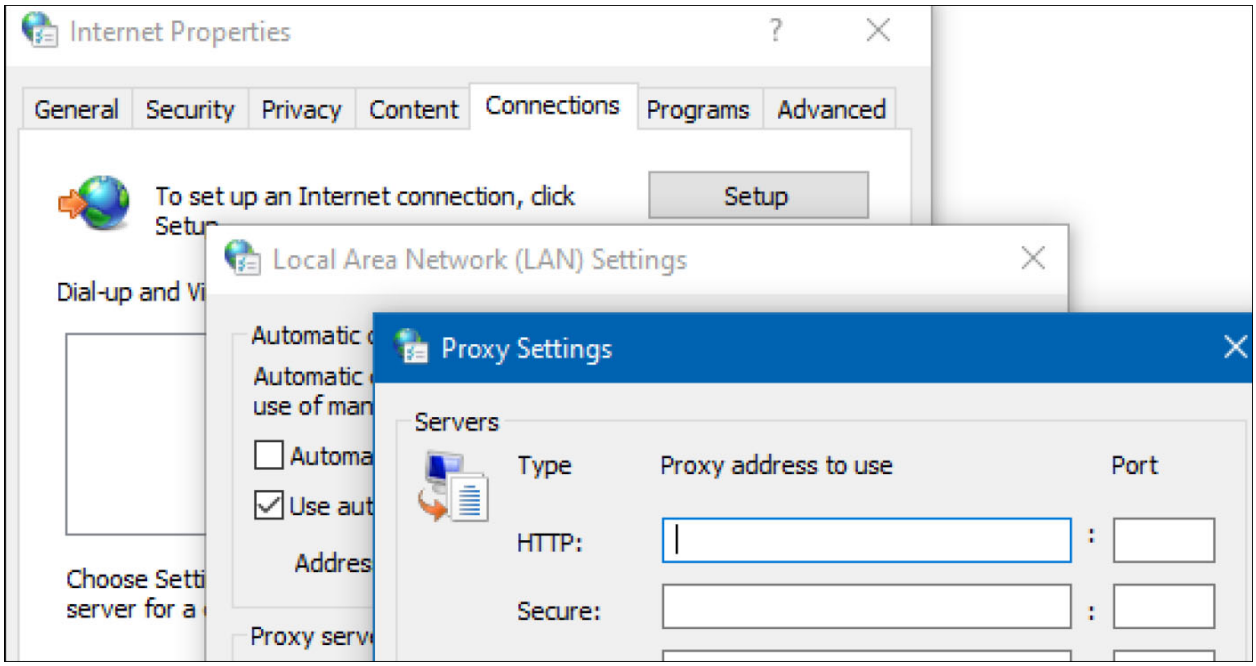
Proxy server requirements for the **PartnerConnect** Agent

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 needs 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 the Control Panel, navigate to the Internet Options..
2. Select the Connections tab.
3. Choose LAN settings.
4. Click the check-box 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	Microsoft **Windows** Server 2016
	Microsoft **Windows** Server 2019
	Microsoft **Windows** Server 2022
	Microsoft **Windows** 10
	Microsoft **Windows** 11

Minimum 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
PartnerConnect Agent	https://t128564.iot.hillrom.com https://t128560.iot.hillrom.com Port: 80 **NOTE** NOTE: The Tenant ID number (t#####) can change based on the tenant the server is pointing to. Please verify the Tenant ID with your Solutions Architect or Project Manager	TCP (HTTPS)	External
Welch Allyn Service Monitor	283 7721	TCP	Internal

Application/service	Domain name, IP address, port	Protocol	Connection
SmartCare Remote Management	https://smartcareremotemanagement.hillrom.com 52.224.38.138 Port: 443 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
Actionable Insights (PowerBi) Backend APIs	`*.analysis.windows.net` Port: 443	TCP	External
Actionable Insights (PowerBi) Backend APIs	`*.pbidedicated.windows.net` Ports: 443, 1443	TCP	External
Actionable Insights (PowerBi) Content Delivery Network (CDN)	`content.powerapps.com` Port: 443	TCP	External
Actionable Insights (PowerBi) Portal	`*.powerbi.com` Port: 443	TCP	External
Actionable Insights (PowerBi) Power Query Online	`*.powerquery.microsoft.com` Port: 443	TCP	External
Actionable Insights (PowerBi) Manage gateways, connections, and data policies (preview)	`gatewayadminportal.azure.com` Port: 443	TCP	External
Actionable Insights (PowerBi) Service telemetry	`dc.services.visualstudio.com` Port: 443	TCP	External
File outbound types	`.log, .zip, .txt, .csv`	Not applicable	Not applicable
File inbound types	`.tar.gz, .tar, .zip, .pim, .xml, *.txt, *.pdf, .waupdate, *.bas, *.json, .csv`	Not applicable	Not applicable

Application and asset compatibility

Asset name	Minimum software
Centrella Smart+ Bed	1.41.000
Progressa Smart+ Bed	GCI:1.27.0.0
	WAM: 1.3

Asset name	Minimum software
CVSM (**Connex** Vital Signs Monitor)	2.x or later except version 2.40.x  **NOTE** Emulate **Spot Vital Signs** 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 Signs** 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	3.1
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

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 facilities, then you must use multiple server installations.

SmartCare Remote Management offers a 3-level organization hierarchy: organization, facility, and location ID. Depending on how you want to view and manage your assets, you can use the hierarchy in different ways.

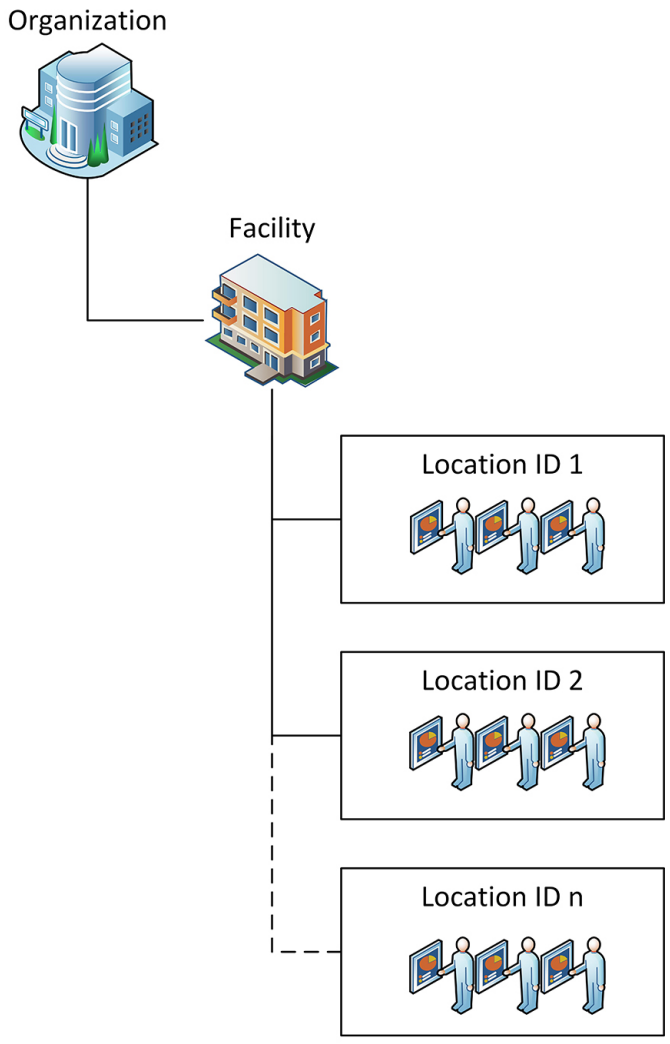
Organization and facility are defined at the time of installation. Location is defined based on the asset location ID configuration field.

The layout options in the diagrams and corresponding table below can help you to determine your **SmartCare** Remote Management layout and installation.

	Layout options explained
Organization	Organization is the highest node level. You may choose to have more than one organization node. You enter "Organization" on the registration form when you install the **PartnerConnect** Agent. The name you enter in that form field for "Organization" will be displayed as the top-level organization in SCRM.
Facility	Facility is the second node level and it is entered into the **PartnerConnect** Agent registration form in the "Facility" field. Depending on the layout, this field can be changed on different **PartnerConnect** Agent installations. For example, you may request a set-up in which users can only view and manage a single facility.

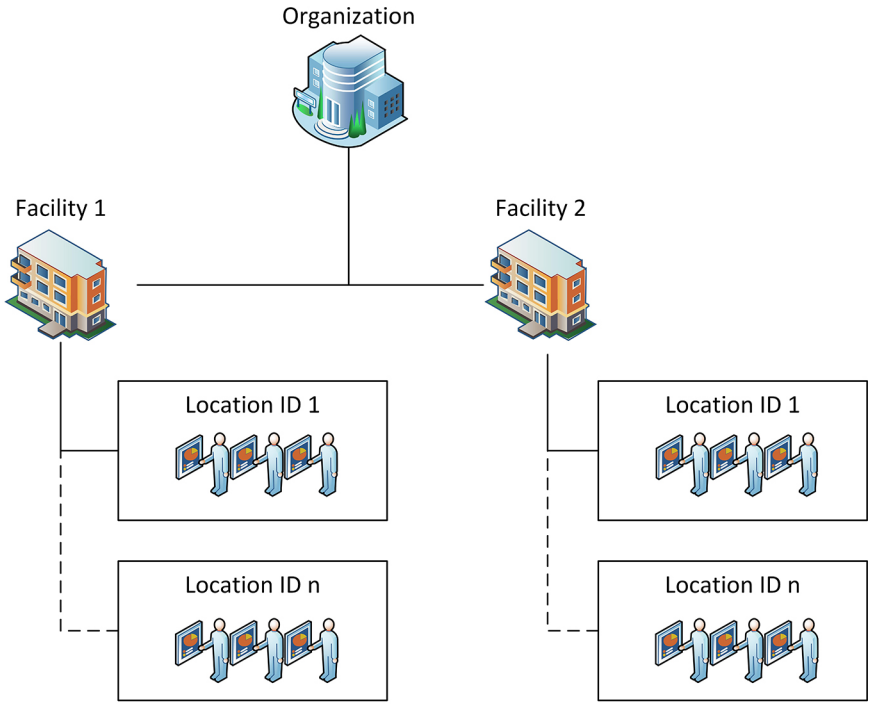
Server installation options

Option 1 for single server installation



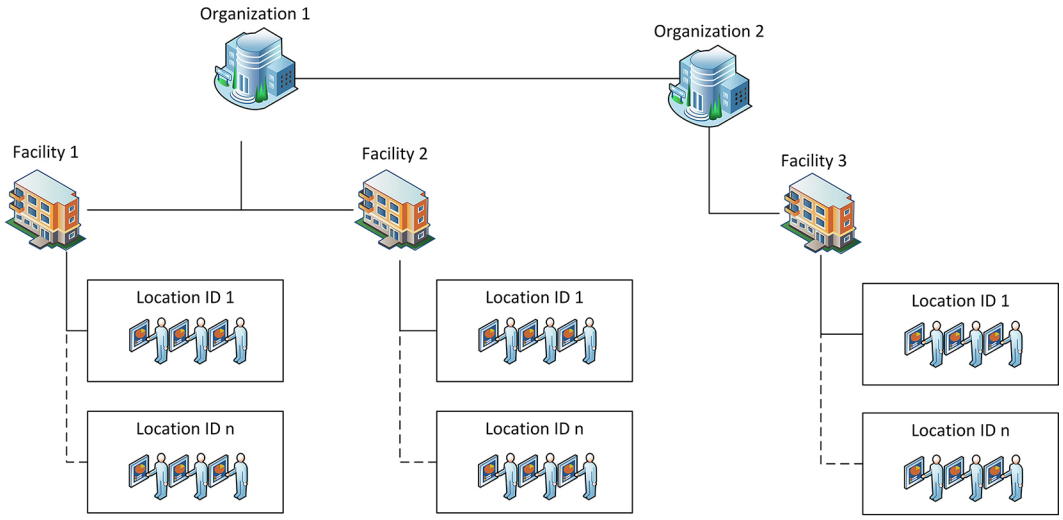
Option 1 – Single server installation with 1 facility and up to 2,000 connected assets.

Option 2 for two or more facilities



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

Option 3 for multiple organizations and facilities



Option 3 – Multiple organizations, two or more facilities, with multiple location IDs 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 below will be rejected and delayed.

NOTE Any request without the required items will be rejected and delayed.

NOTE Use this setup guide and not the 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)

  ☐ User email address(es) to be used for **PartnerConnect** download and installation

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

  ☐ Microsoft **Windows** 2016

  ☐ Microsoft **Windows** 2019

  ☐ Microsoft **Windows** 2022

  ☐ Microsoft **Windows** 10

  ☐ Microsoft **Windows** 11

- For CSM and CVSM/CIWS assets, confirm that 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 – 1.41.000

☐ **Progressa** Smart+ Bed – GCI: 1.27.0.0 / WAM: 1.3

☐ 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) – 1.7x, 1.8x or later

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

☐ DCP – 3.1

☐ 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 the **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 the **PartnerConnect** agent software using this link to the **PartnerConnect** *Software Installation Guide* https://www.hillrom.com/content/dam/hillrom-aem/us/en/sap-documents/LIT/80016/80016392LITPDF.pdf.
5. Obtain the Welch AllynService 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, which the project manager provides as needed.

Download and install the Welch Allyn Service Monitor application

NOTE As a reminder, this section is not applicable to **RetinaVue** 700 (RV700).

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

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

10. Set the settings.xml ForceConfig to "True."

    This action happens at the following location:

    C:\ProgramData\Baxter\Service Monitor\Settings\Settings.xml

    <ApplicationSettings>

    <CallHomePeriod>PT15M</CallHomePeriod>

    <DeviceSessionLimit>PT3M</DeviceSessionLimit>

    <DataRetrievalPeriod>PT0S</DataRetrievalPeriod>

    <PartnerConnectTimeout>PT3M</PartnerConnectTimeout>

    <MinimumRetentionDaysForLogs>30</MinimumRetentionDaysForLogs>

    <MaximumSimultaneousDeviceConnections>96</MaximumSimultaneousDeviceConnections>

    <DeploymentMode>false</DeploymentMode>

    <ForceConfig>true</ForceConfig>

    </ApplicationSettings>

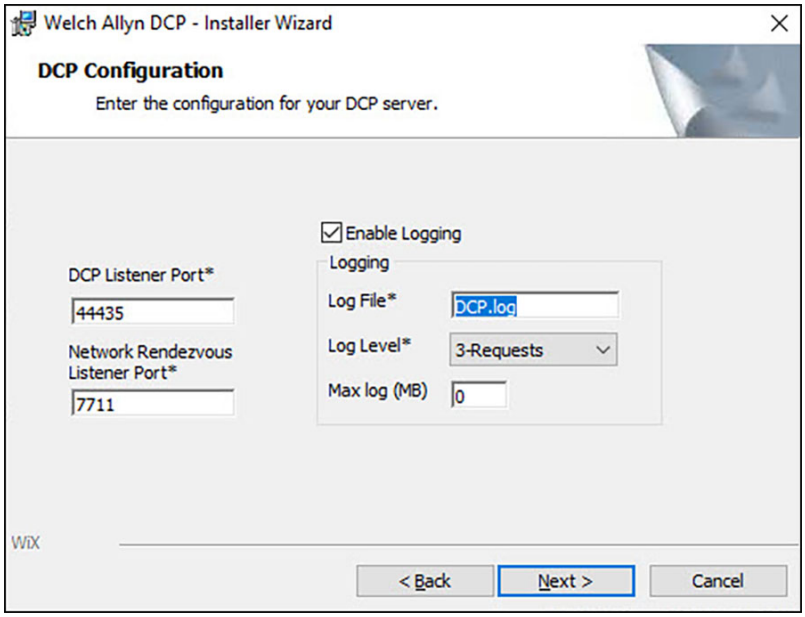
11. Restart the Service Monitor.

    The Service Monitor application is installed.

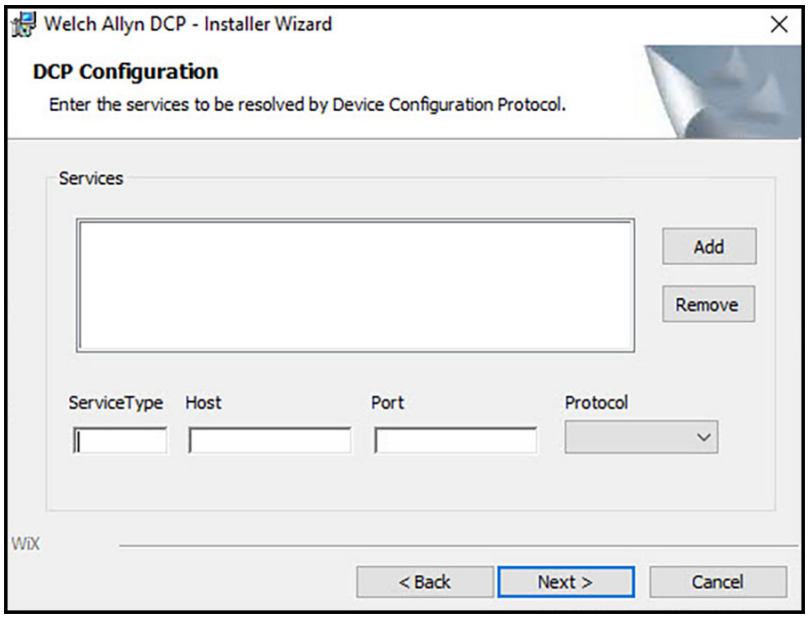
Download and install the Welch Allyn DCP application

This section 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 an 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 a similar option on each screen.

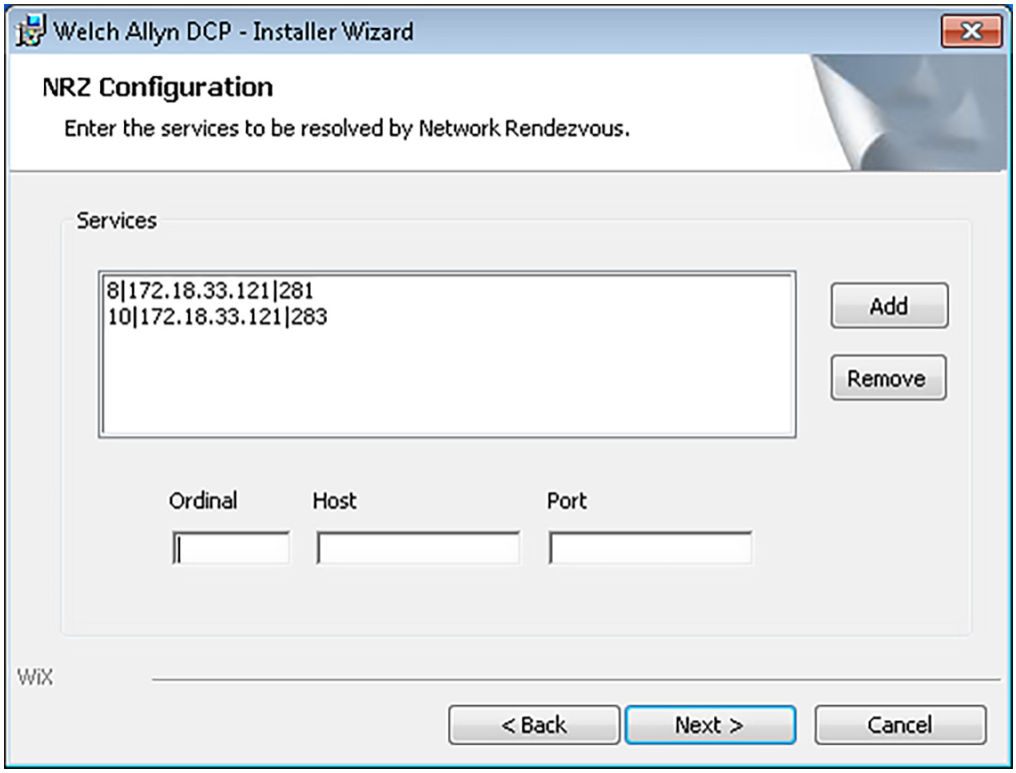


4. Skip the next screen for CVSM and CSM. (See below.)



5. Update the 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 already exists, 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's connectivity is set to NRS IP. To check, navigate through the following path: **Network > Server > Connectivity**.

      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 > IP Address**.
   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 on page 3 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.

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

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 on page 3 section (and try again).
5. If it passes, go to 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 Remote Management account for you.

1. Go to https://smartcareremotemanagement.hillrom.com.
2. Log in to the account with your username and password.
3. For a **PartnerConnect** agent with CSM and/or CVSM/CIWS, verify that the organization, facility, and location ID 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).