iBed Server

Installation/Configuration Manual

Version 3.x

REF 5212



EN

5212-409-001 Rev AC.0 2025-05

Table of Contents

Warning/Caution/Note Definition 2
Introduction 3
- Installing the iBed Server software 3
- System requirements and recommendations 3
- Product connection requirements 5
- Contact information 5

Installation 6
- Server configuration 6
  - Windows Server 2019/2022 6
- Stryker iBed Server Application 16
  - Stryker iBed Server Tools 25
- Stryker iBed Wireless Configuration Tool 27
- Verify Stryker iBed Server Tool installation 28

Setup 30
- Adding devices (clients) to the Master Device List 30
- Adding locator IDs and hospital locations 31
- Adding more Stryker interfaces 33
  - Integrating Engage 33
  - Integrating Smart Equipment Management (SEM) 33
  - Integrating Vision 33
- Adding a third-party interface 33
  - Integrating **Rauland Responder®** 5 33

Configuring the wireless router (Stryker device configuration) 34
Configuring the wireless network connection settings 36
Resetting the wireless module to factory default settings (Med-Surg bed) 37
Resetting the wireless module to factory default settings (Model FL27 InTouch) 38
Resetting the wireless module to factory default settings (Model 3009 ProCuity) 39
Troubleshooting 40
- Basic 40
- Advanced 43
  - Connectivity issues 43
  - Third-party communication issues 44
  - Device not connecting to server 44
  - Connectivity issues of one or more devices 45
  - Cannot communicate with device 47
  - Cannot communicate with device (DNS only) 48
- Smart Equipment Management option - troubleshooting 49
- Email alerts 51

Warning/Caution/Note Definition

The words **WARNING**, **CAUTION**, and **NOTE** carry special meanings and should be carefully reviewed.

WARNING

Alerts the reader about a situation which, if not avoided, could result in death or serious injury. It may also describe potential serious adverse reactions and safety hazards.

CAUTION

Alerts the reader of a potentially hazardous situation which, if not avoided, may result in minor or moderate injury to the user or patient or damage to the product or other property. This includes special care necessary for the safe and effective use of the device and the care necessary to avoid damage to a device that may occur as a result of use or misuse.

Note - Provides special information to make maintenance easier or important instructions clearer.

Introduction

This manual assists you with the operation or maintenance of your Stryker product. Read this manual before operating or maintaining this product. Set methods and procedures to educate and train your staff on the safe operation or maintenance of this product.

Note - Stryker continually seeks advancements in product design and quality. This manual contains the most current product information available at the time of printing. There may be minor discrepancies between your product and this manual. If you have any questions, contact Stryker Customer Service or Technical Support at 1-800-327-0770.

Installing the iBed Server software

1. Copy the files listed to the **Public Documents** folder.
   - BBIDList.xml
   - DeviceBBIDLocationAssociation.xml
   - DeviceURLs.xml
   - HospitalLocationList.xml
2. Uninstall the application.
3. Install the new application.

   Install directory\Stryker\iBedServerApplication\Data

   Note - The new application imports the files from the **Public Documentation** folder.
4. Using the iBed Server Tool, configure the Master Device List and the Locator Associations.

   Stryker disclaims all responsibility for information transmitted off of its devices.

System requirements and recommendations

Note

- If the minimum system requirements are not met, the system performance is impacted.
- Always apply relevant software updates and patches.
- The minimum system requirements for the server hardware depend on the number of products that are connected to the system.

Hardware requirements	
Capacity	**Requirement**
1-300 connected products	2.x GHz processor or better with a total of 4 cores Memory: 8 GB RAM Hard drive: 150 GB
301-600 connected products	2.x GHz processor or better with 8 cores Memory: 16 GB RAM Hard drive: 150 GB
601-800 connected products	2.x GHz processor or better with 16 cores Memory: 32 GB RAM Hard drive: 150 GB
801-1,000 connected products	2.x GHz processor or better with 24 cores Memory: 32 GB RAM Hard drive: 150 GB

Hardware requirements	
Capacity	**Requirement**
1,001-1,300 connected products	2.x GHz processor or better with 32 cores Memory: 64 GB RAM Hard drive: 150 GB
1,300+ connected products	For systems that have over 1,300 connected products, add a core for every 50 products.

Note

- Two server environments for the server are recommended: test and production.
- The server is supported in either physical or virtual environments.
- The server supports high availability in Active - Passive configuration. Contact the Stryker Wireless Implementation Team for more information.

Software and setup requirements		
Scope	**Requirement**	**Requirement**
Operating system	Microsoft Windows Server 2019	Microsoft Windows Server 2022
Server roles	Add roles • Web server (IIS) (installed) • Roles services ◦ Application development – ASP.NET 3.5 (installed) – ASP.NET 4.5 (or higher) (installed) – ASP (installed) • Management tools ◦ IIS management console (installed)	Add roles • Web server (IIS) (installed) • Common HTTP features • Performance • Security ◦ Application development – .Net Extensibility 4.8 – ASP.NET 4.8 – ISAPI Extensions – ISAPI Filters • Management tools ◦ IIS management console (installed)
Server features	• .NET Framework 3.5 features (installed) • .NET Framework 4.5 (or higher) features (installed) • Telnet client ◦ WCF services – HTTP Activation	• .NET Framework 4.8 features (installed) • .NET Framework 4.8 (or higher) features (installed) • Telnet client ◦ WCF services – HTTP Activation
Other	Update the server for all current Microsoft priority updates. **Note** - For Windows Server 2019, download and install .Net Framework 4.8 runtime from the official Microsoft site (https://dotnet.microsoft.com/en-us/download/dotnet-framework/net48).	Update the server for all current Microsoft priority updates and optional updates for .NET Framework 4.8.

To make sure that your network is secure, Stryker recommends the following:

- Use antivirus/malware protection
- Close unused network ports
- Disable unused services
- Manage access to system/network infrastructure (firewall, approved IP addresses, or other cybersecurity strategy)
- Monitor network activity for irregularities
- Disable TLS 1.0 and 1.1 on servers and enforce TLS 1.2 or TLS 1.3
- Disable weak SSL cipher suites

You may need more configuration or setup depending on equipment and other variables. Contact Stryker Technical Support at 1-800-327-0770 if you have difficulties with:

- Installation
- Setup
- Configuration
- Connections (between the server and Stryker wireless clients)

Product connection requirements

Note - If the product can travel to multiple subnets, you are required to use the DNS naming convention for each Stryker product.

- DHCP connections - use a reserved IP address for each product via its MAC address
- Static connections - use a static IP address for each product via its MAC address
- DNS naming convention - use a product hostname that is hardcoded to each product (hostname example = SYK-82453f21f0c2 [SYK product MAC address])

Contact information

Contact Stryker Customer Service or Technical Support at: 1-800-327-0770.

Stryker Medical
3800 E. Centre Avenue
Portage, MI 49002
USA

Email: medicaliBedWirelessSupport@stryker.com

Installation

Server configuration

Windows Server 2019/2022

1. In the **Server Manager**, navigate to the Dashboard.
2. Select the **Add Roles and Features** link (Figure 1).

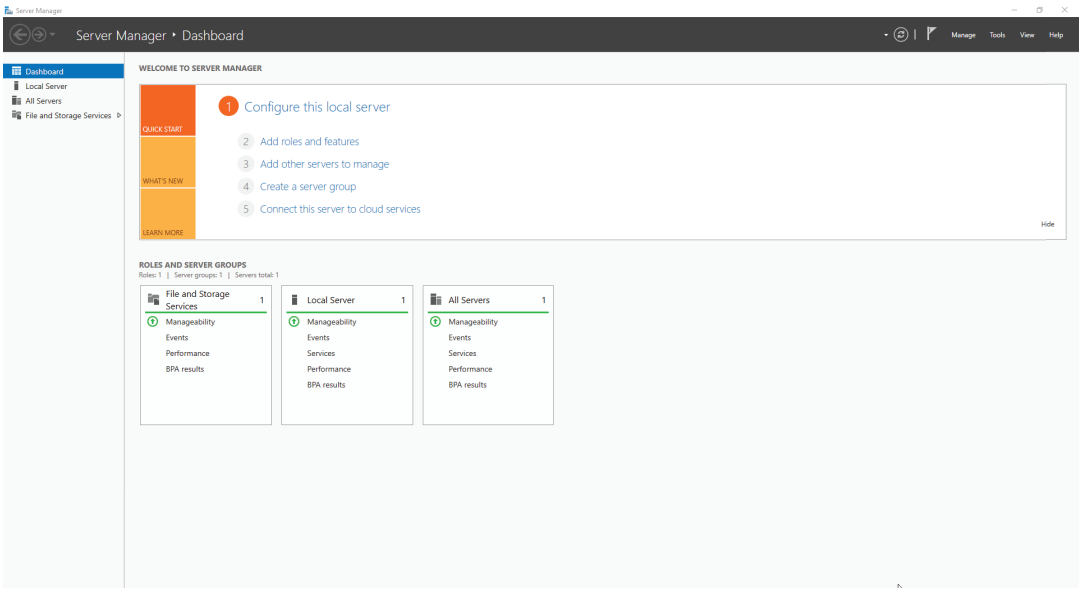


Figure 1 – Add Roles and Features

3. In the **Add Roles and Features Wizard**, select **Next** (Figure 2).

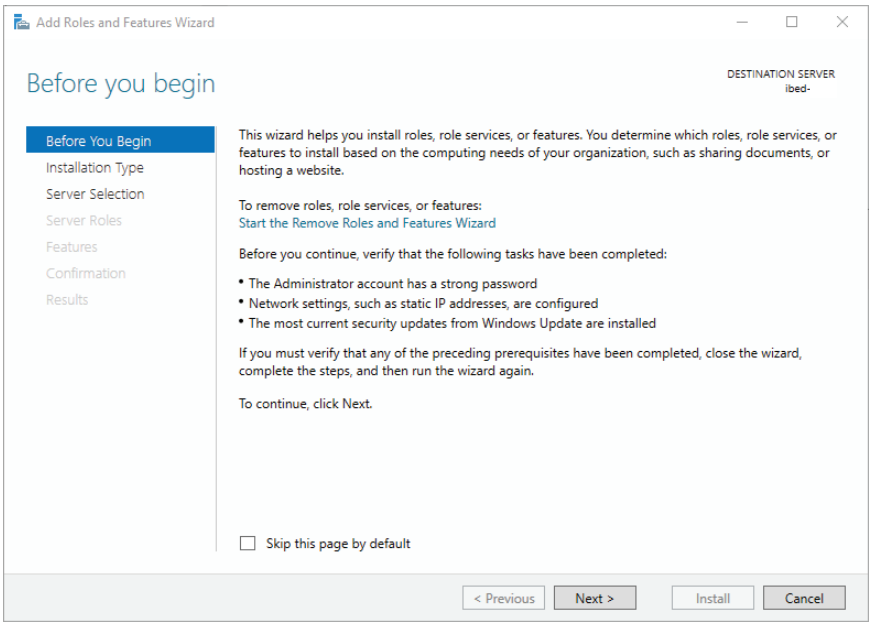


Figure 2 – Add Roles and Features Wizard

4. In the **Select installation type**, select **Role-based or feature-based installation**. Select **Next** (Figure 3).

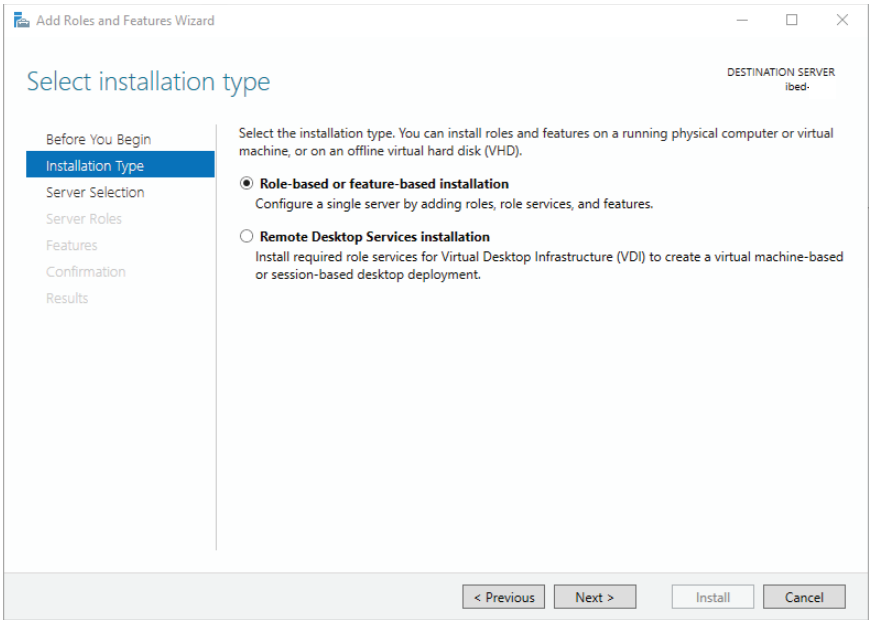


Figure 3 – Installation Type

5. In the **Select destination server**, select **Select a server from the server pool**. Verify that the server is correct in the **Server Pool** box. Select **Next** (Figure 4).

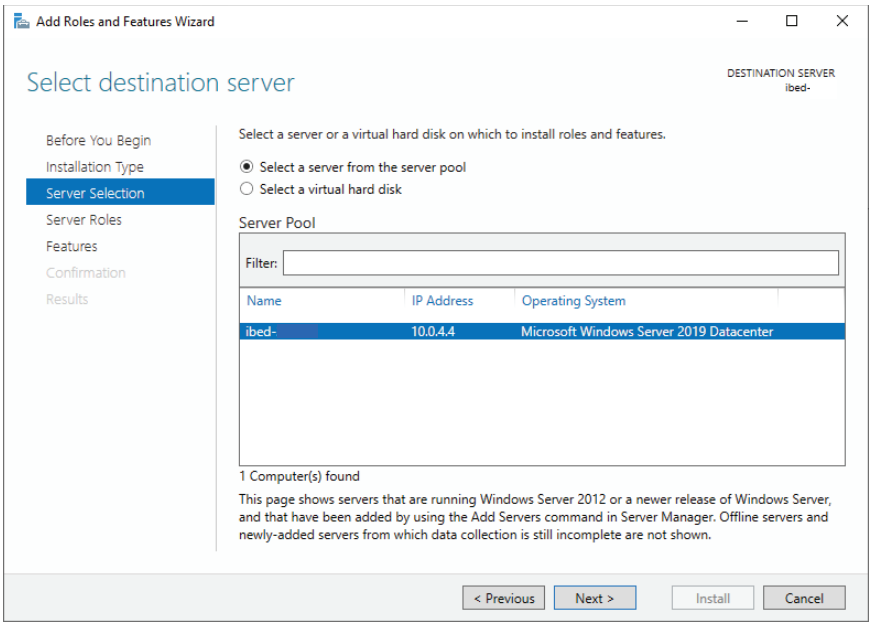


Figure 4 – Server Selection

6. In the **Select server roles**, scroll through the options under **Roles**. Select **Web Server (IIS)** (Figure 5).

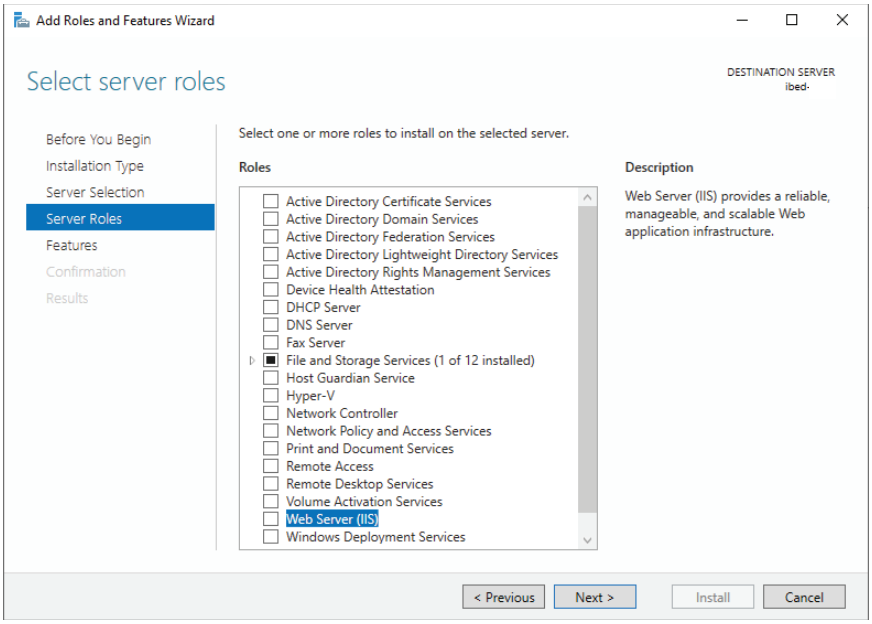


Figure 5 – Web Server (IIS)

7. In the **Add features that are required for Web Server (IIS)**, select **Add Features** (Figure 6).

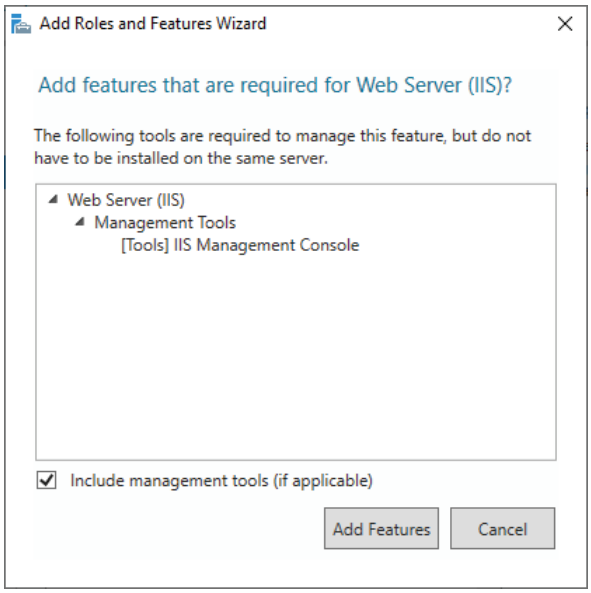


Figure 6 – Add Features

8. In the **Select server roles**, select **Next** (Figure 7).

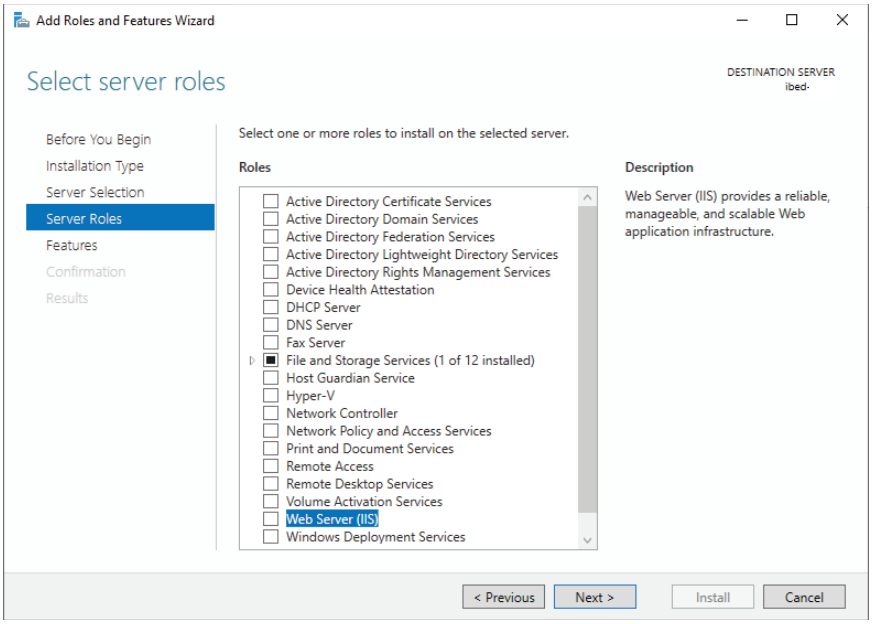


Figure 7 – Server confirmation

9. In the **Select features**, select **.NET Framework 3.5 Features**, **.NET Framework 4.7 Features**, and **Telnet Client** in the **Features** box (Figure 8).

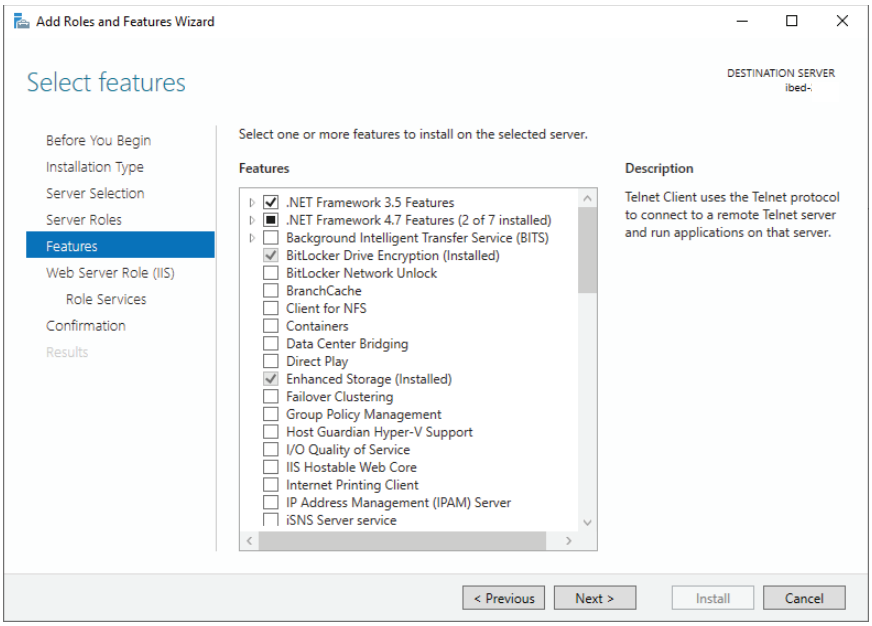


Figure 8 – Features selection

10. In the **Web Server Role (IIS)**, select **Next** (Figure 9).

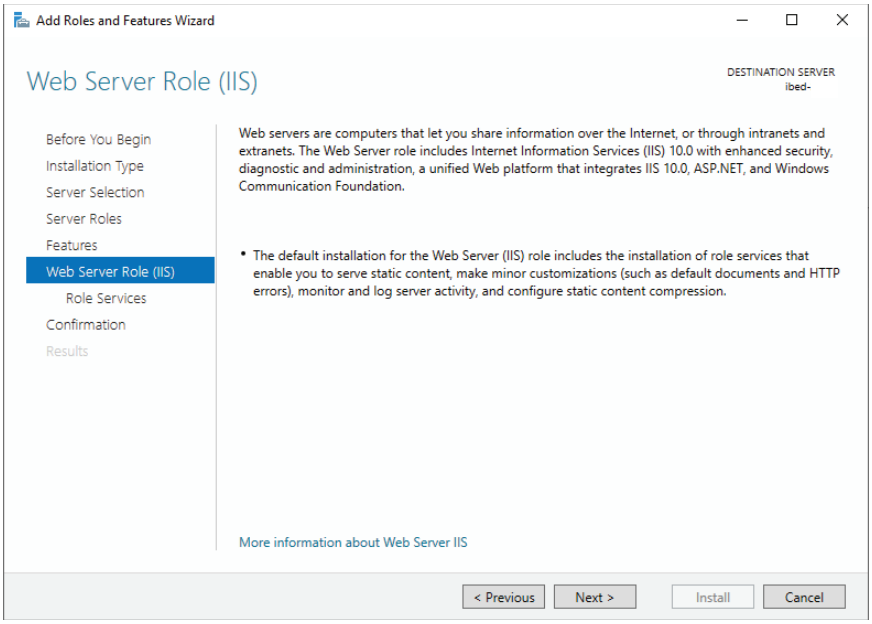


Figure 9 – Web Server Role (IIS)

11. In the **Edit Services**, select **Next** (Figure 10).

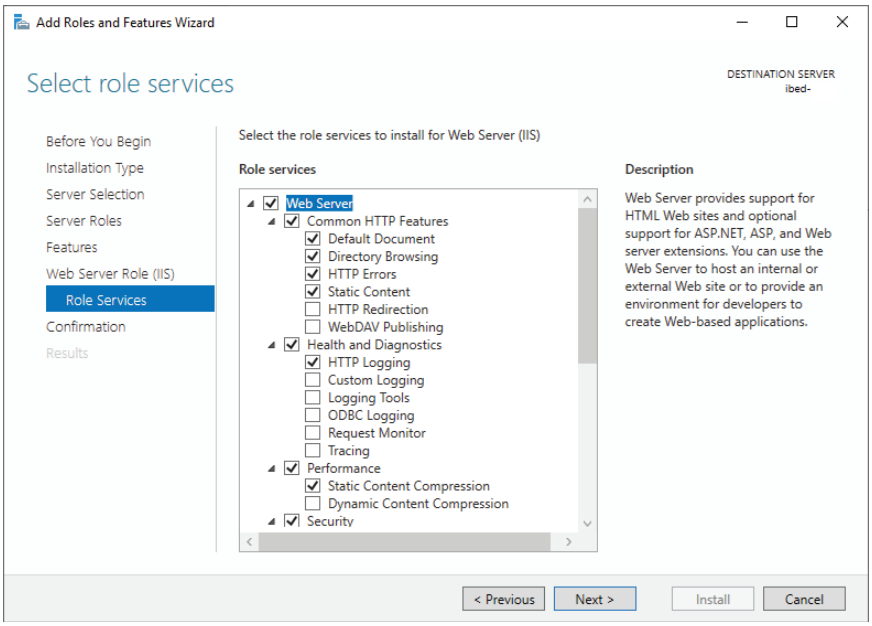


Figure 10 – Role Services

12. In the **Confirmation installation selections**, select **Install**. The installation of the role and feature starts (Figure 11).

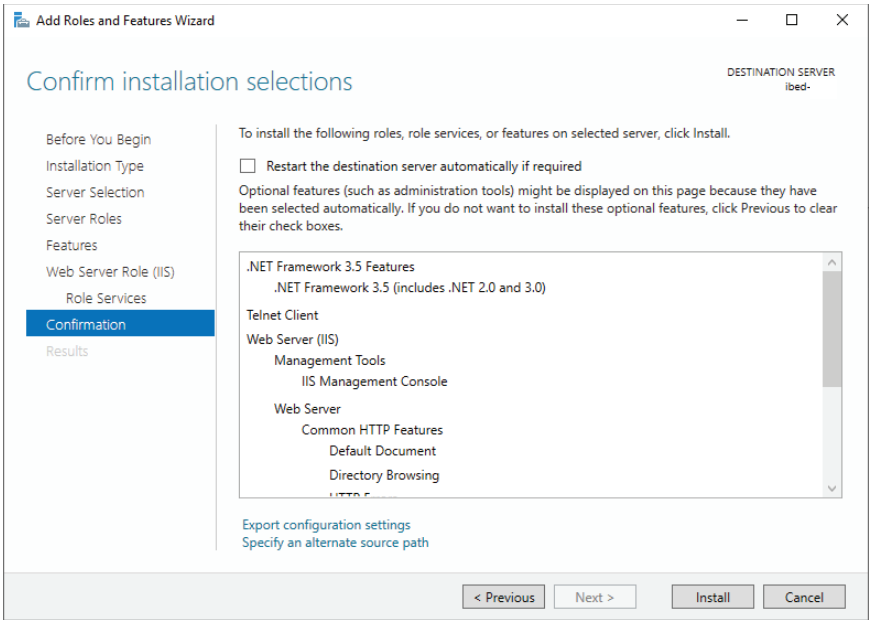


Figure 11 – Install confirmation

13. When the installation is finished, select **Close** (Figure 12).

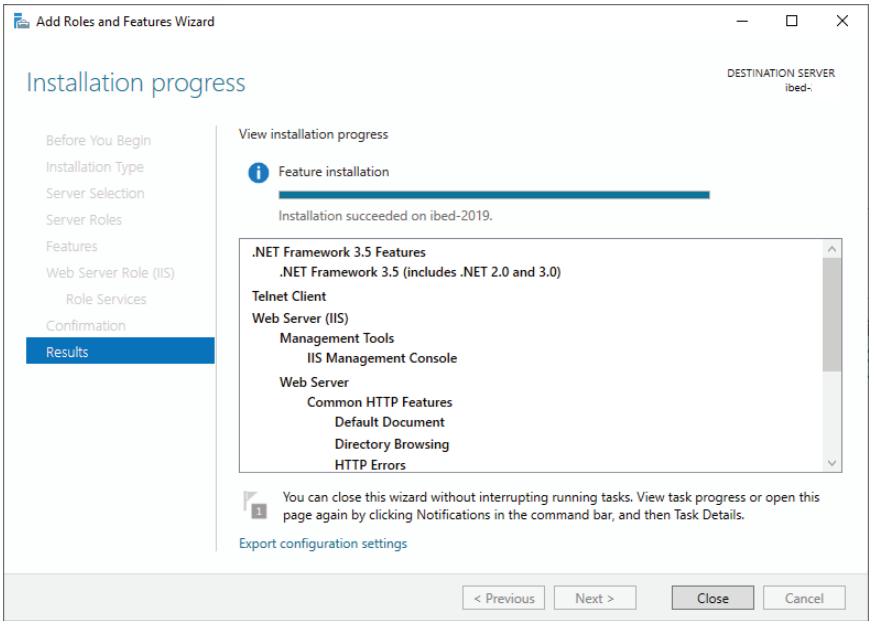


Figure 12 – Completed installation

14. Select the **Add Roles and Features** link (Figure 13).

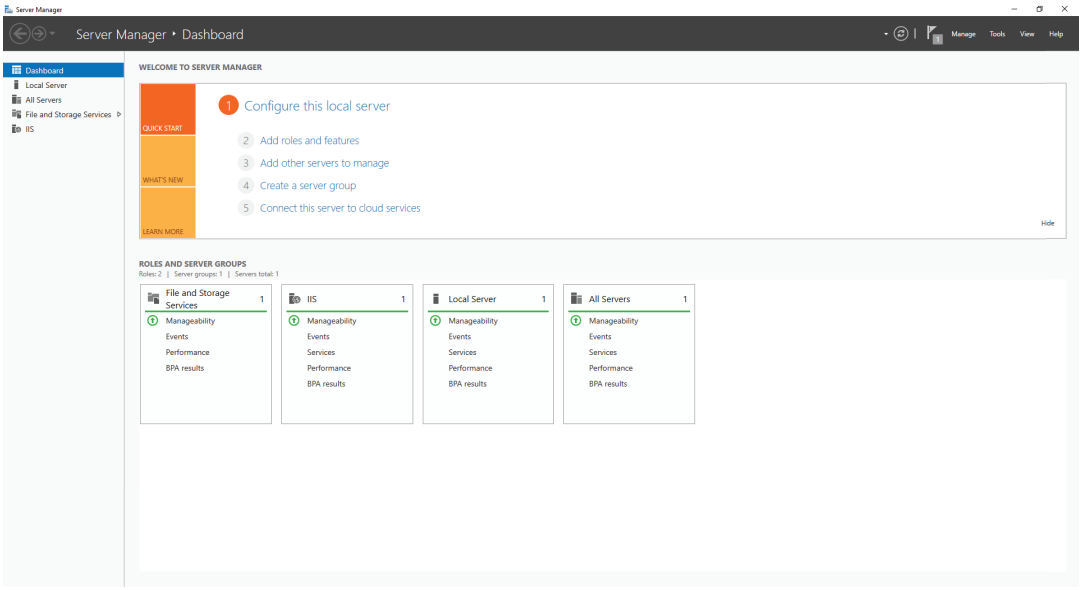


Figure 13 – Add Roles and Features

15. In the **Add Roles and Features Wizard**, select **Next** (Figure 14).

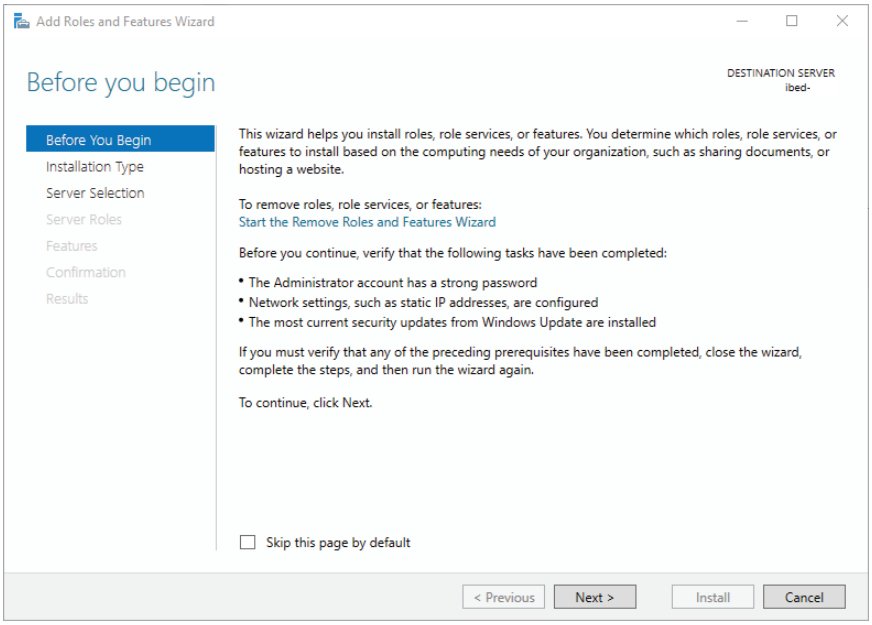


Figure 14 – Add Roles and Features Wizard

16. In the **Select installation type**, select **Role-based or feature-based installation**. Select **Next** (Figure 15).

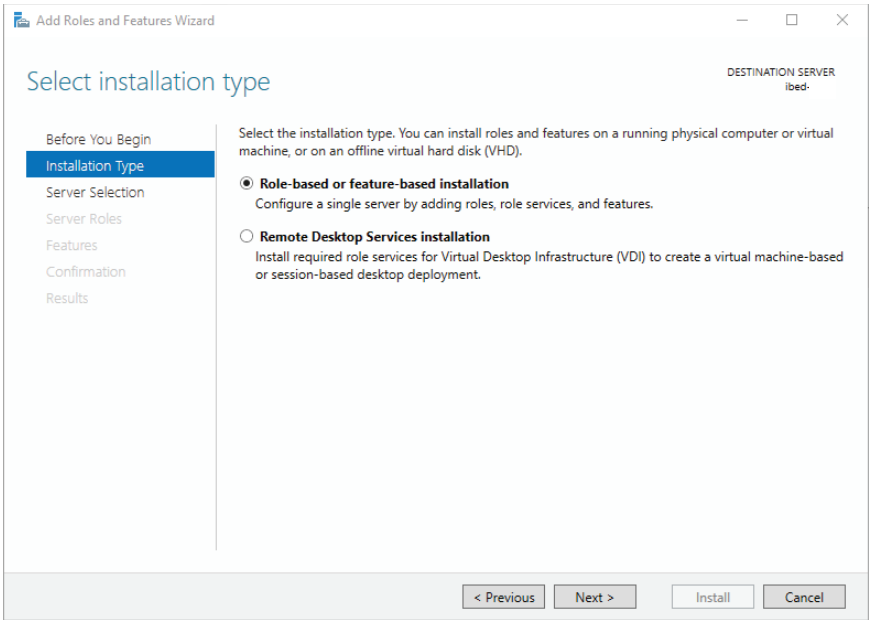


Figure 15 – Installation Type

17. In the **Select destination server**, select **Select a server from the server pool**. Verify that the server is correct in the **Server Pool** box. Select **Next** (Figure 16).

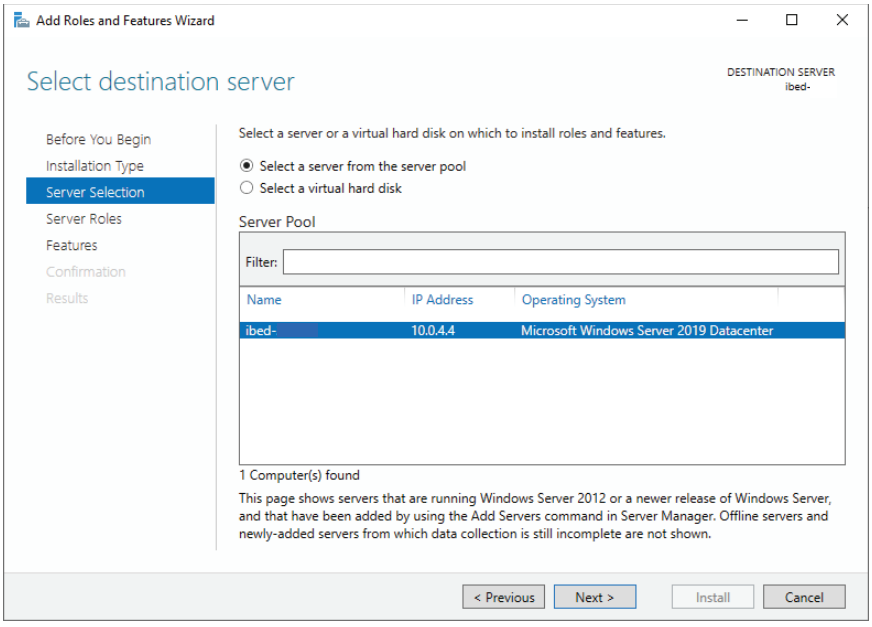


Figure 16 – Server Selection

18. In the **Select server roles** in the **Roles** box, expand the **Web Server (IIS)** heading, the **Web Server** heading, and the **Application Development** heading. Select **ASP.NET 3.5** and **ASP.NET 4.7**. Select **Next** (Figure 17).

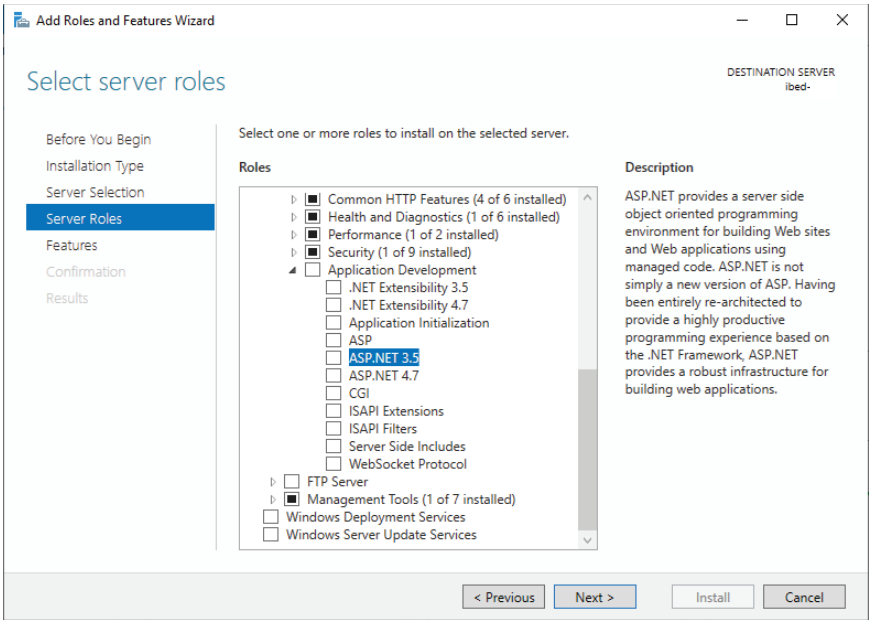


Figure 17 – Server Roles

19. In the **Add features that are required for ASP.NET 3.5**, select **Add Features** (Figure 18).

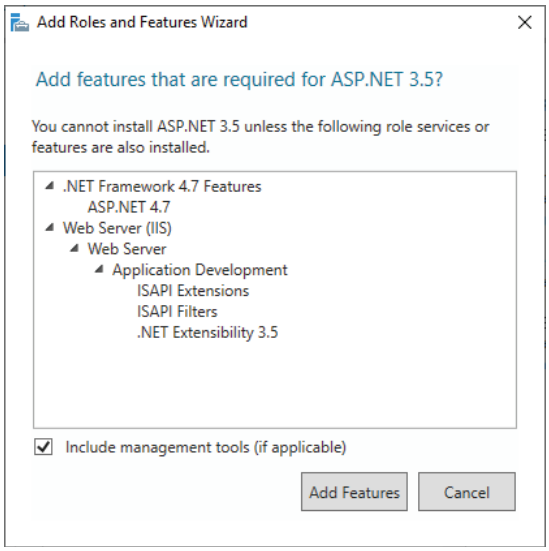


Figure 18 – Add Features

20. In the **Select server roles**, select **ASP**. Select **Next** (Figure 19).

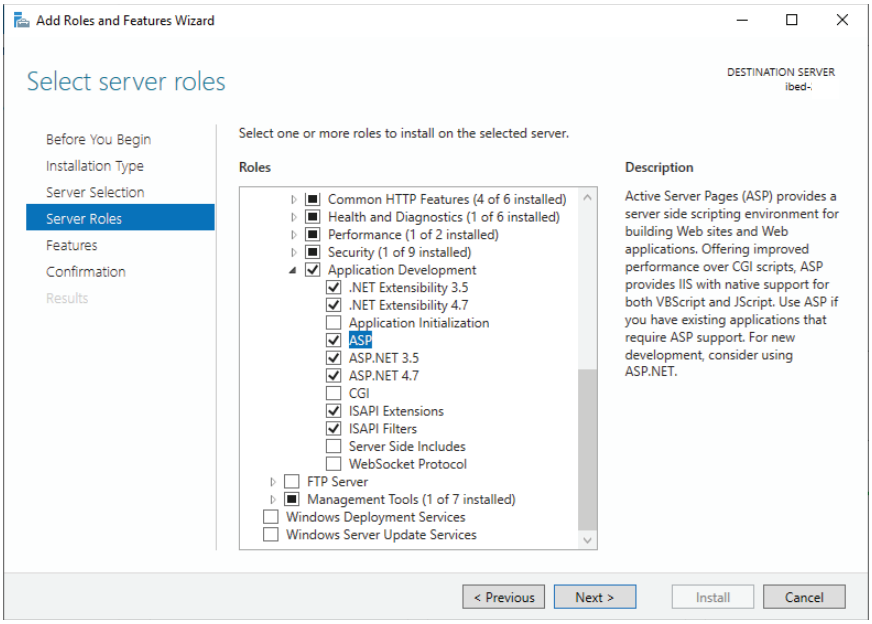


Figure 19 – ASP

21. In the **Select features**, select **Next** (Figure 20).

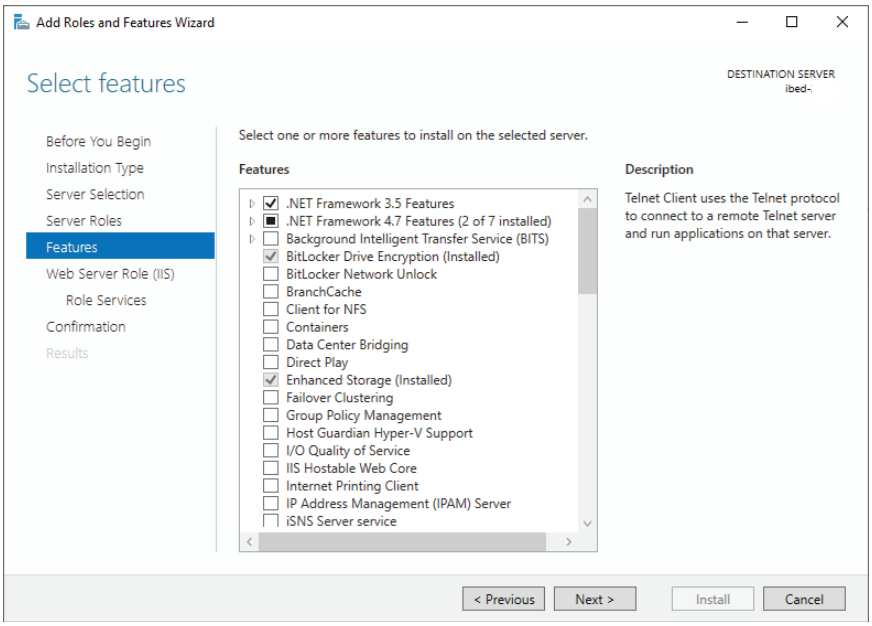


Figure 20 – Features selection

22. In the **Confirm installation selections**, select **Install** (Figure 21).

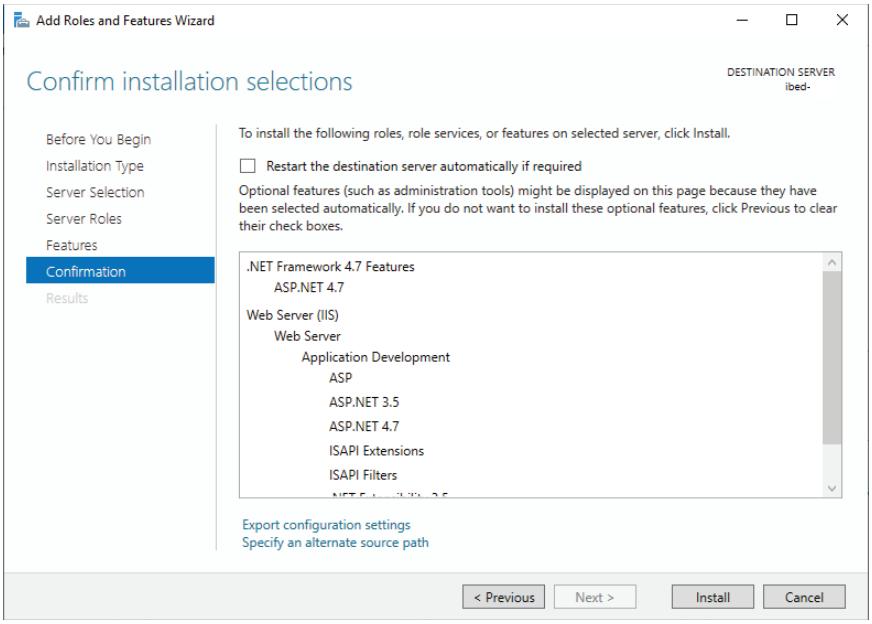


Figure 21 – Confirm installation

23. When installation is complete, select **Close** (Figure 22).

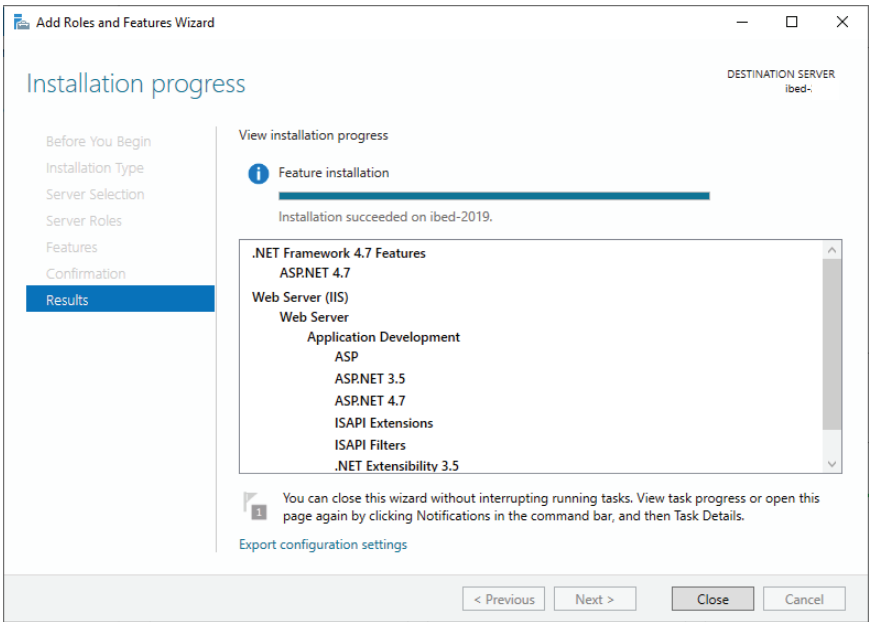


Figure 22 – Installation complete

24. Restart the server.
25. Run **Windows Update** to look for any important or optional updates. Install the updates. Restart the server if required.

Stryker iBed Server Application

1. Right-click the **5212-502-001 Server Application Setup.exe** file. Select **Run as Administrator** to start the **Stryker iBed Server Application** installation.
2. If Microsoft SQL Server 2022 Express is not already installed, the **Install Shield Wizard** requirements window opens. Select **Install** (Figure 23).

Note - If Microsoft SQL Server 2022 Express is installed, go to step 15.

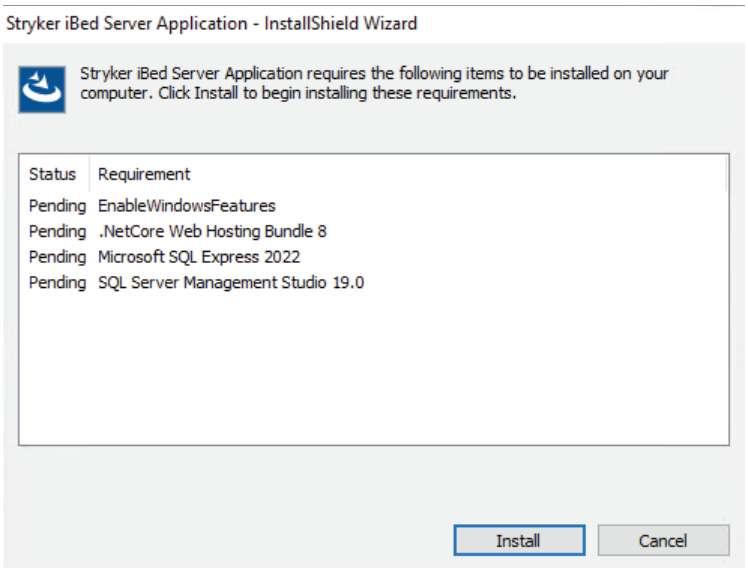


Figure 23 – Microsoft SQL service

3. Select **Install** to enable Windows feature.

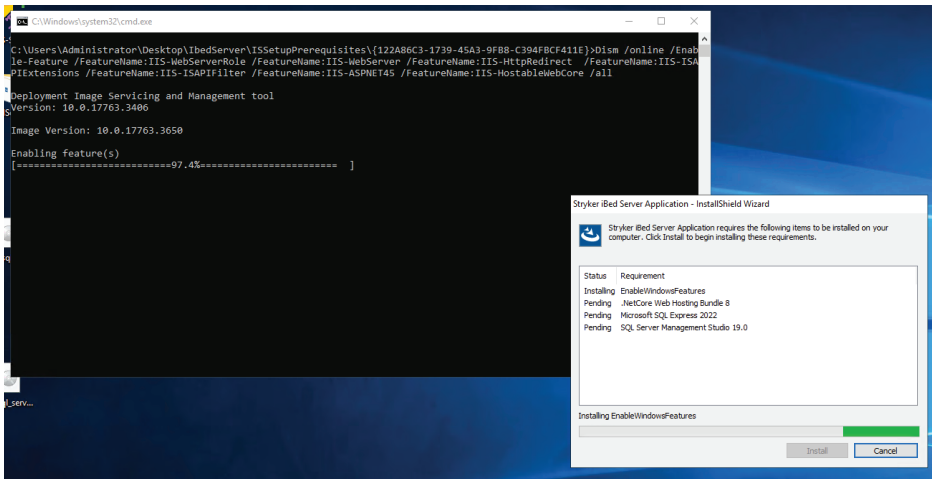


Figure 24 – Install

4. Select **Yes** in the confirmation window to start the .NetCore Web Hosting Bundle installation (Figure 25).

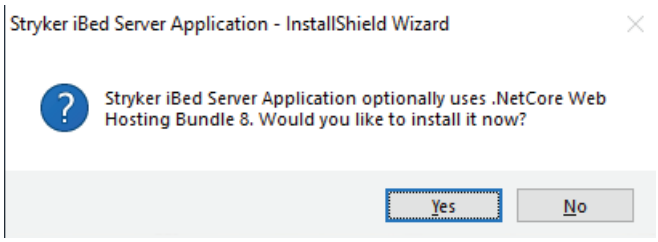


Figure 25 – .NetCore confirmation

5. Select **Yes** in the confirmation pop-up to start the Microsoft SQL Server installation (Figure 26).

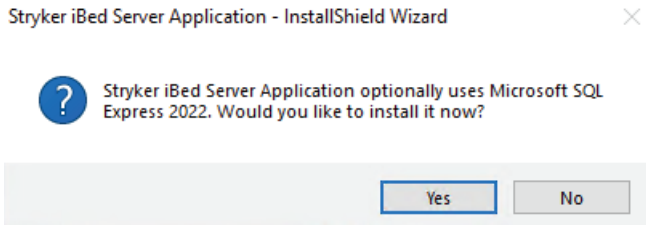


Figure 26 – SQL confirmation

6. The **Choose Directory For Extracted Files** window appears (Figure 27).
   a. If you are using the recommended location, input **C:\temp\sqlserver**.
   b. If you are using a different location, select **Browse**...

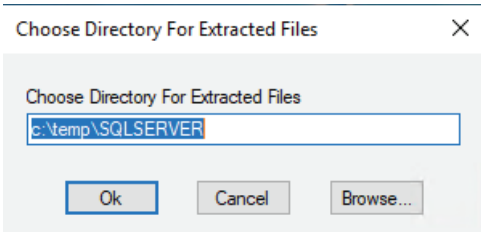


Figure 27 – Choose Directory for Extracted Files

7. Select **I accept the license terms** box. Select **Next** (Figure 28).

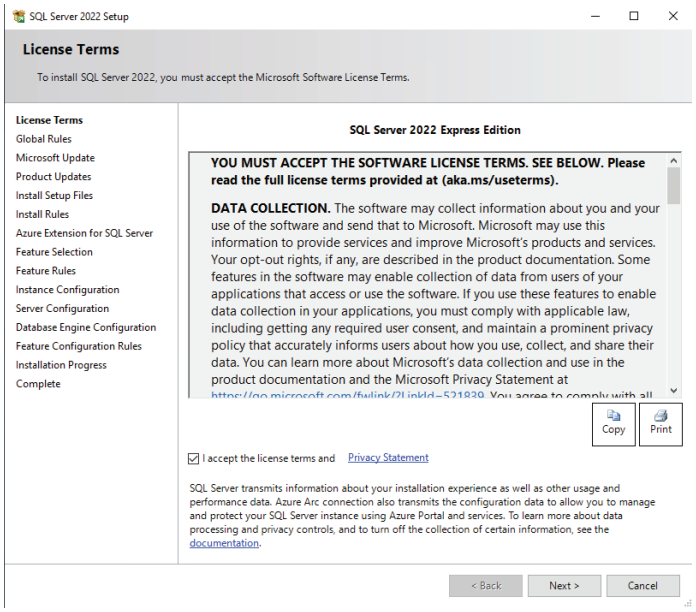


Figure 28 – SQL license

8. In the **Feature Selection**, leave the **Features** selection at the defaults. If the **Shared feature directory** does not default to **C:\Program Files**, browse or create the new destination location for the installation. Select **Next** (Figure 29).

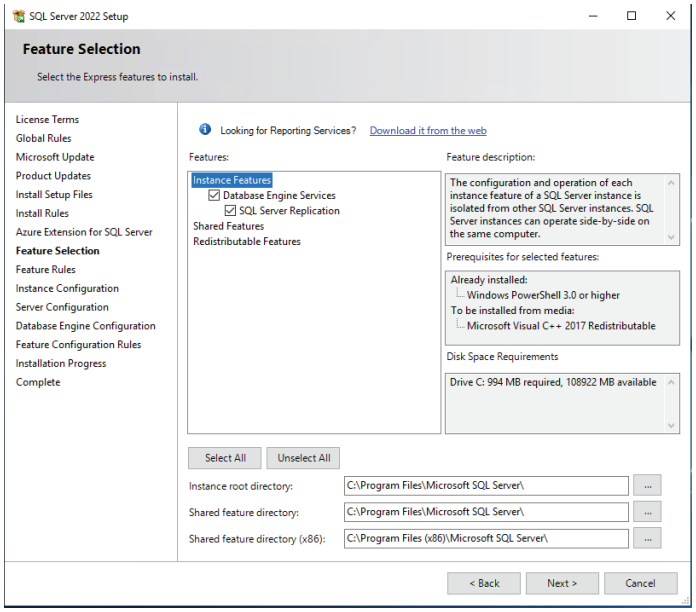


Figure 29 – SQL features

9. In the **Instance Configuration**, select **Next** (Figure 30).

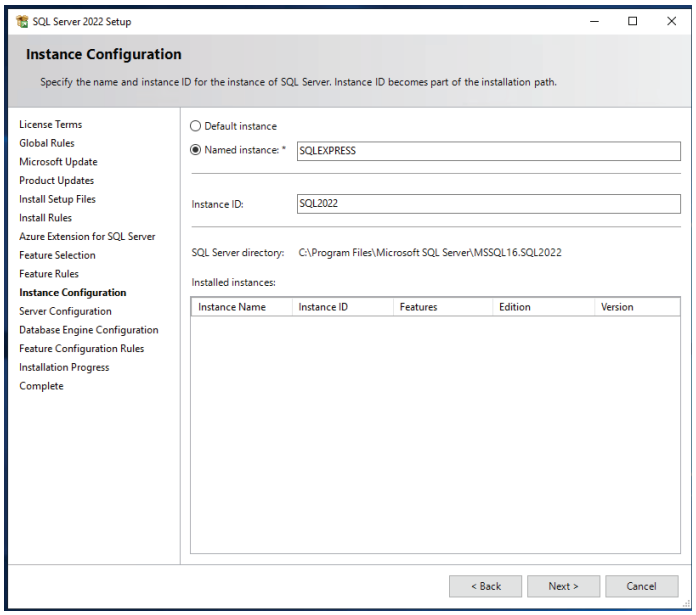


Figure 30 – Instance Configuration

10. In the **Server Configuration**, select **Next** (Figure 31).

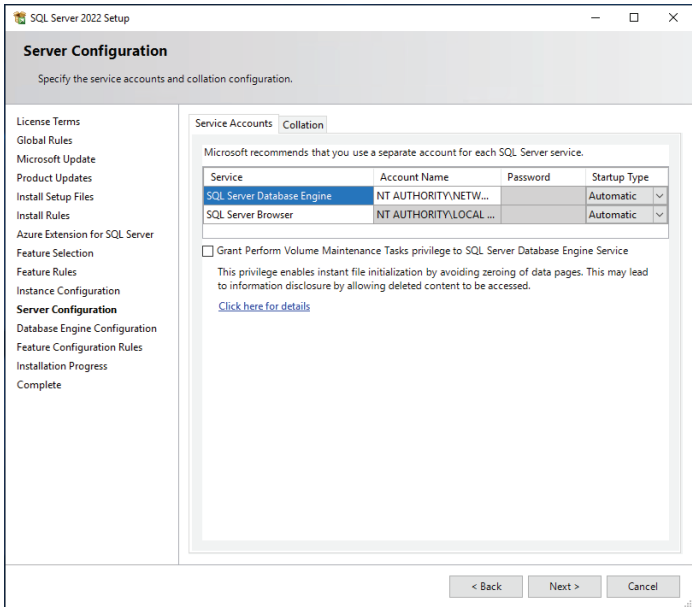


Figure 31 – Server Configuration

11. In the **Database Engine Configuration**, select **Next** (Figure 32).

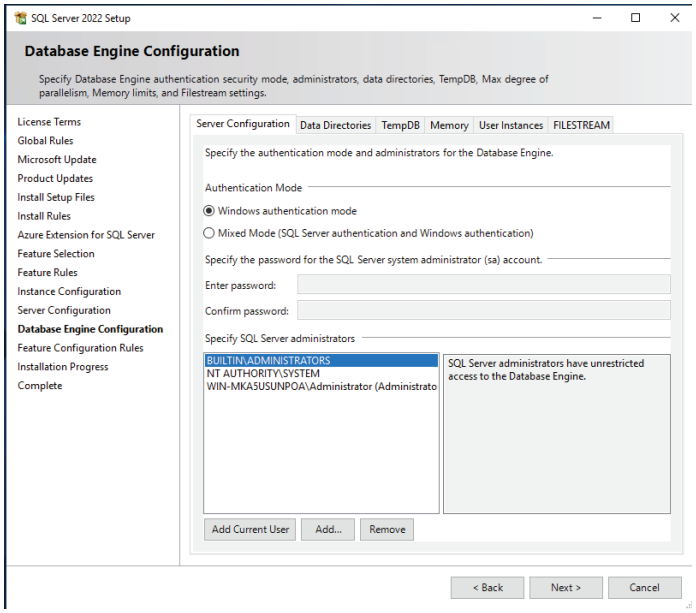


Figure 32 – Database Engine Configuration

12. When installation is complete, select **Close** in the **Complete** window. The **SQL Server Management Studio** installation (Figure 33) starts.

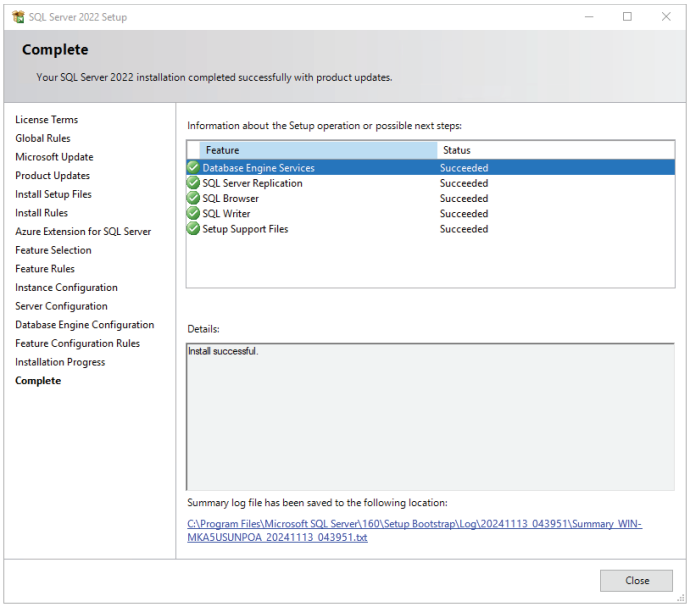


Figure 33 – SQL server installation complete

13. Select **Yes** in the confirmation window to start the **SQL Server Management Studio** installation (Figure 34).

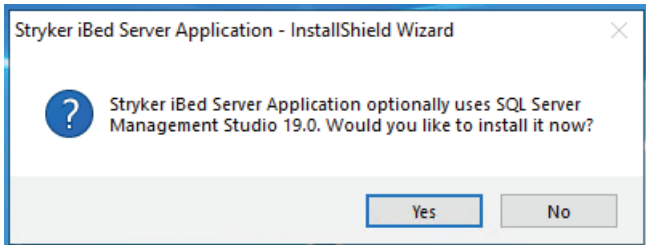


Figure 34 – SQL Server Management Studio confirmation

14. The **SQL Server Management Studio** installation window appears (Figure 35).
    a. If you are using the default location, select **Install**.
    b. If you are using a different location, select **Change** and then **Install** to confirm.

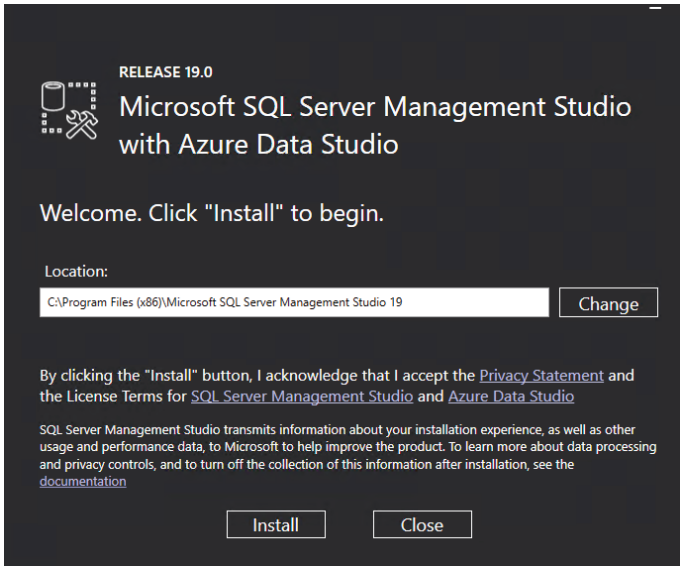


Figure 35 – SQL Server Management Studio installation

15. When installation is complete, **SQL Server Management Studio** requires a restart. Select **Restart** to continue (Figure 36).

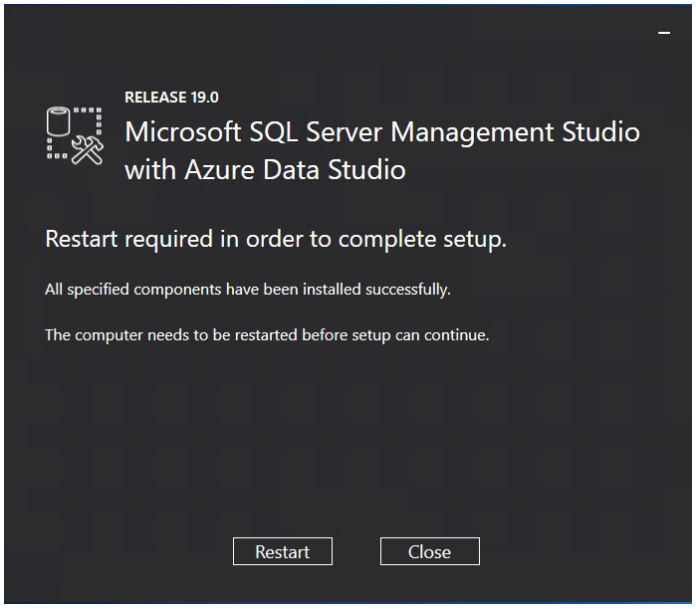


Figure 36 – SQL Server Management Studio restart

16. When the restart is complete, the **InstallShield Wizard** window appears. Select **Next** (Figure 37).

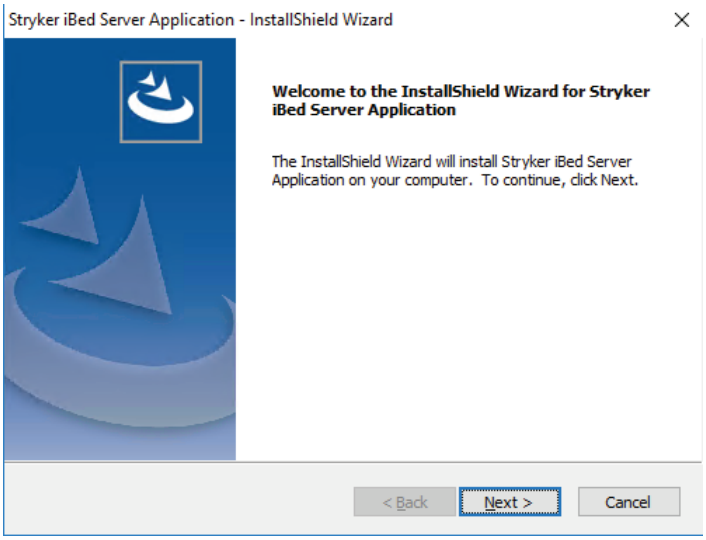


Figure 37 – InstallShield Wizard

17. In the **iBed Server Application** window, enter the site information. Select **Next** (Figure 38).

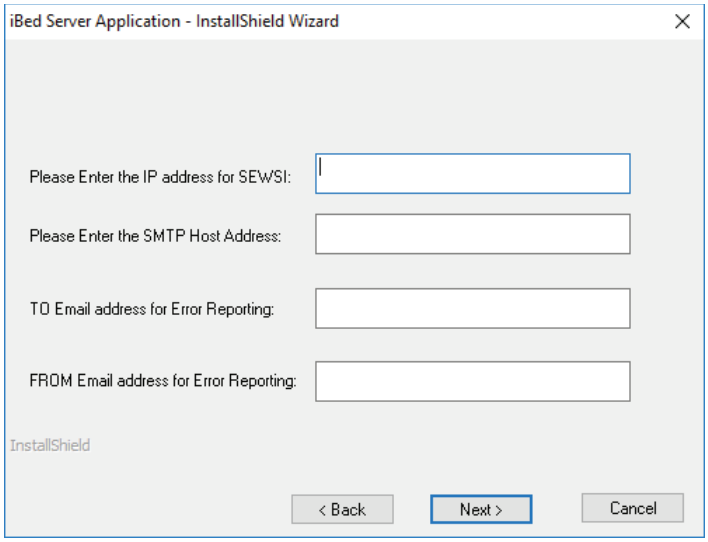


Figure 38 – Application configuration

18. The **Choose Destination Location** window appears (Figure 39).
    a. If you are using the default location, select **Next**.
    b. If you are using a different location, select **Change** and then **Next** to confirm.

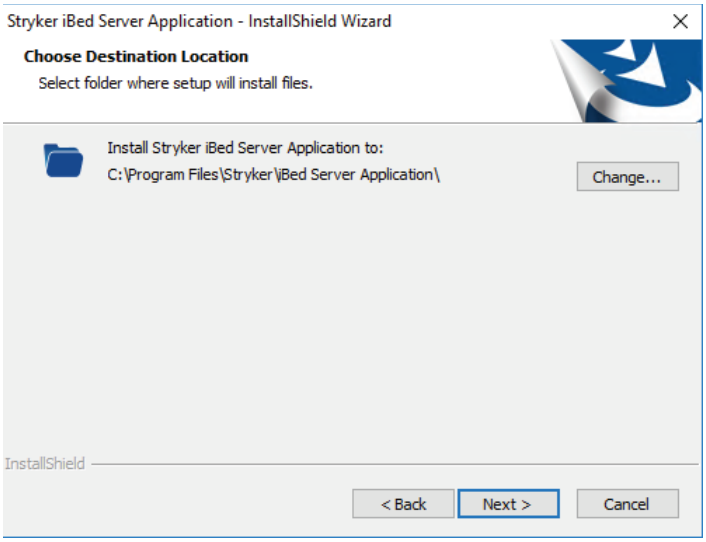


Figure 39 – Choose Destination Location

19. The **Select Program Folder** window appears (Figure 40).
    a. If you are using the default folder, select **Next**.
    b. If you are using a different folder, create a different folder name and select **Next**.

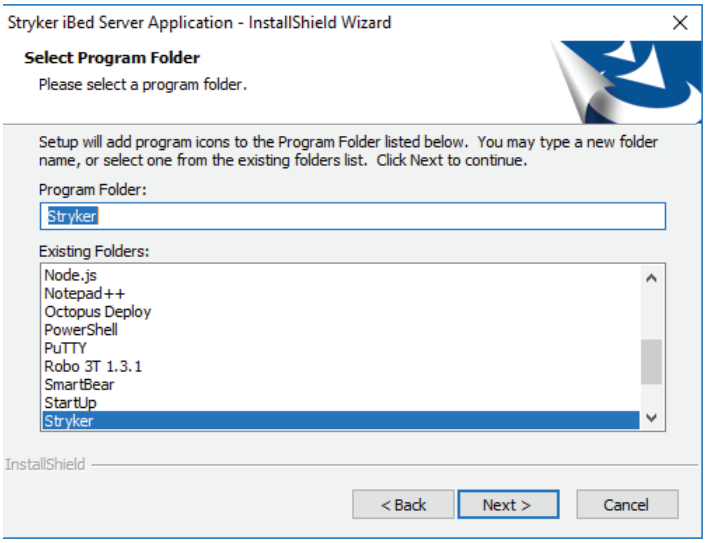


Figure 40 – Select Program Folder

20. Select **Install** to start the installation (Figure 41).

    Note - To return to the **Select Program Folder**, select **Back**.

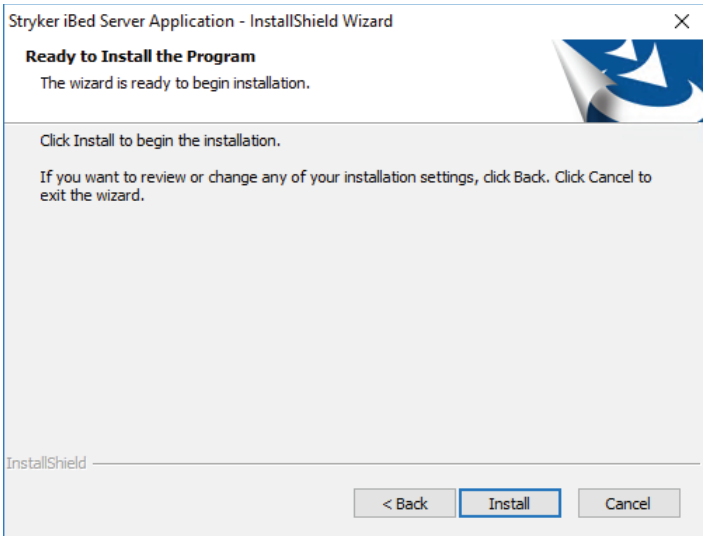


Figure 41 – Install

21. Select **Finish** to exit the **InstallShield Wizard** (Figure 42).

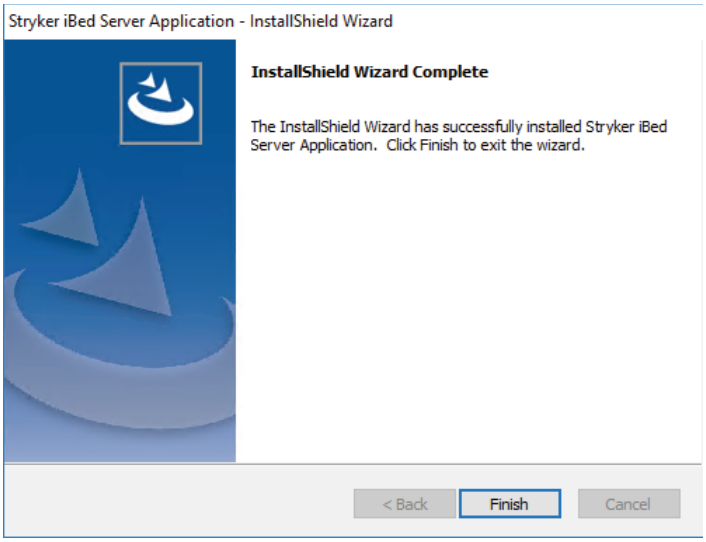


Figure 42 – Finish

Stryker iBed Server Tools

1. Right-click the **5212-502-001 Server Tools Setup.exe** file. Select **Run as Administrator** to start the **Stryker iBed Server Tools** installation.
2. In the **InstallShield Wizard** window, select **Next** (Figure 43).

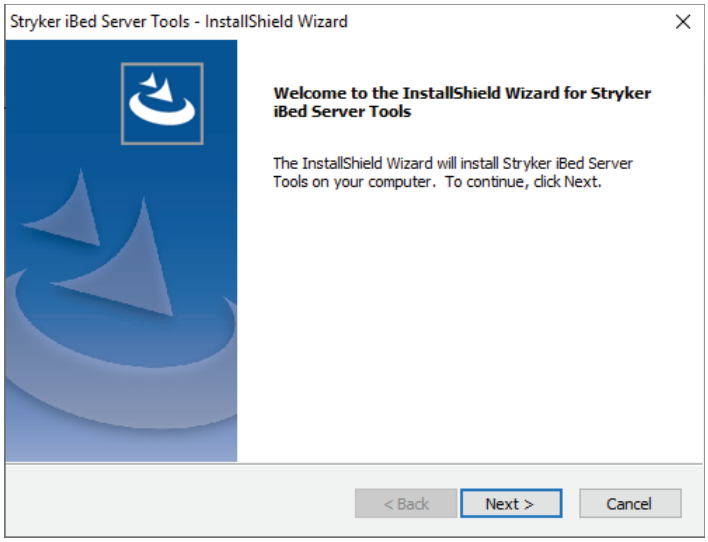


Figure 43 – InstallShield Wizard

3. The **Choose Destination Location** screen appears (Figure 44).
   a. If you use the default location, select **Next**.
   b. If you use a different location, select **Change** and then **Next** to confirm.

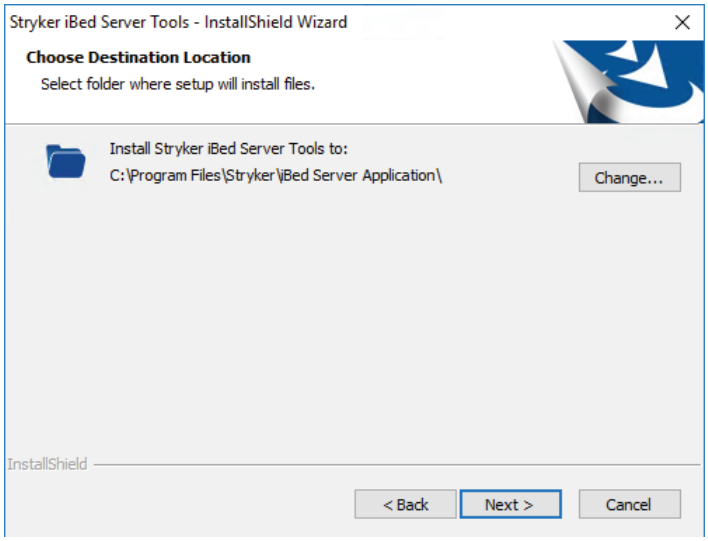


Figure 44 – Choose Destination Location

4. Select **Finish** to exit the **InstallShield Wizard** (Figure 45).

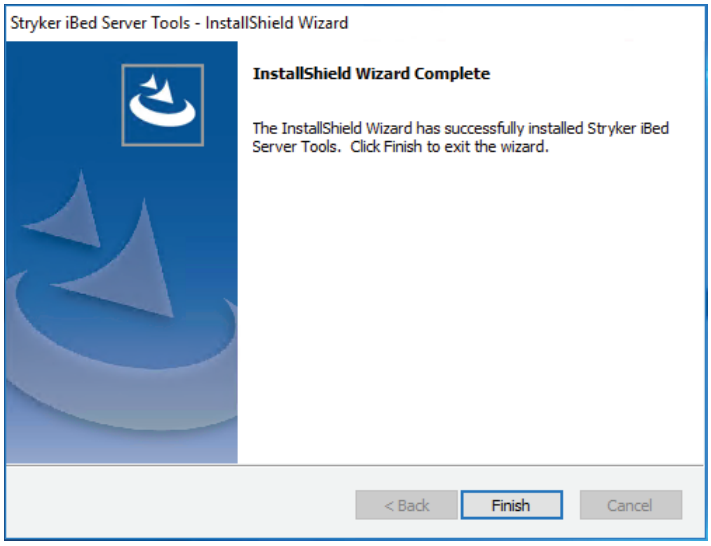


Figure 45 – Finish

Stryker iBed Wireless Configuration Tool

1. Double-click the **5212-503-001 Stryker iBed Wireless Configuration Tool Setup.exe** file to start the wireless configuration for the source location.
2. In the **InstallShield Wizard** window, select **Next** (Figure 46).

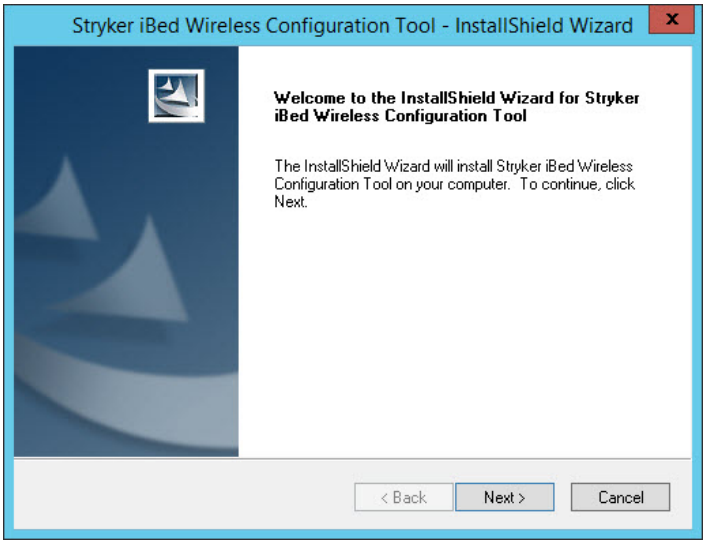


Figure 46 – InstallShield Wizard

3. The **Choose Destination Location** window appears (Figure 47).
   a. If you are using the default location, select **Next**.
   b. If you are using a different location, select **Change** and then **Next** to confirm.

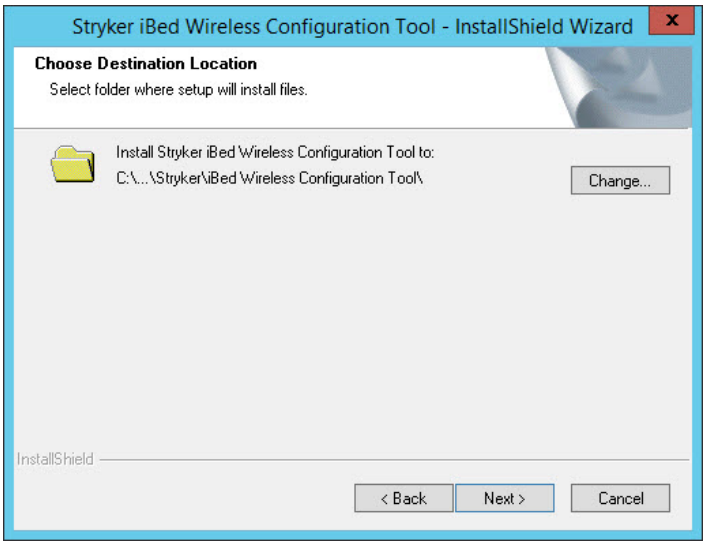


Figure 47 – Choose Destination Location

4. Select **Finish** to exit the **InstallShield Wizard** (Figure 48).

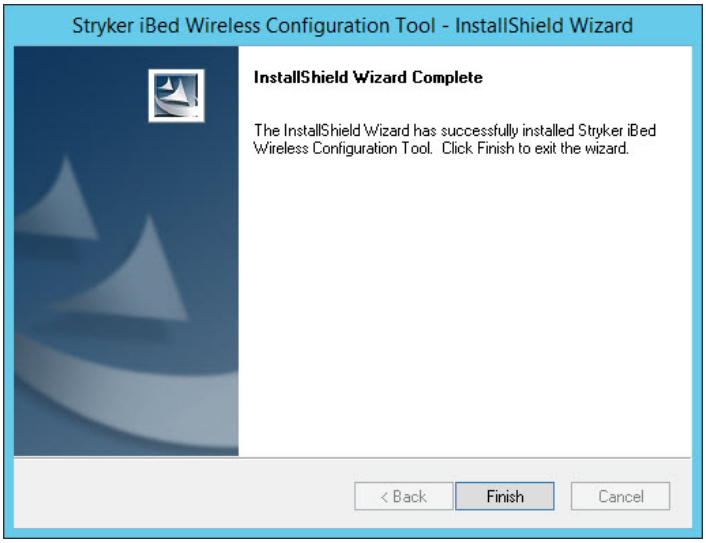


Figure 48 – Finish

Verify Stryker iBed Server Tool installation

To verify that the Stryker iBed Server Tool is installed:

1. Open the **Stryker iBed Server Tool**. Select **Start→All Programs→Stryker→Stryker iBed Server Tool** or click the  icon.

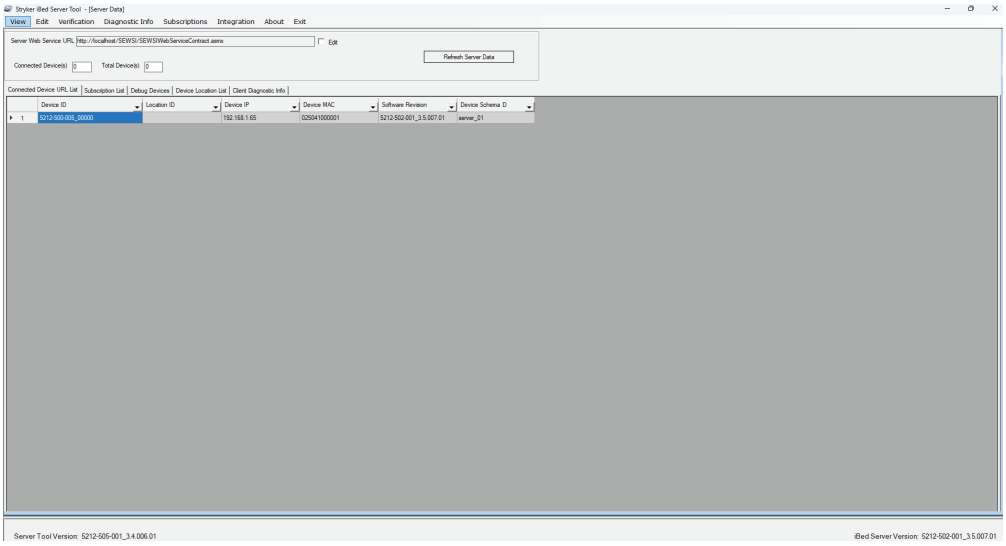


Figure 49 – Stryker iBed Server Tool

2. Select **Verification→Server** in the task bar.
3. In the **Stryker iBed Server Verification** window, select **Verify Server** (Figure 50).

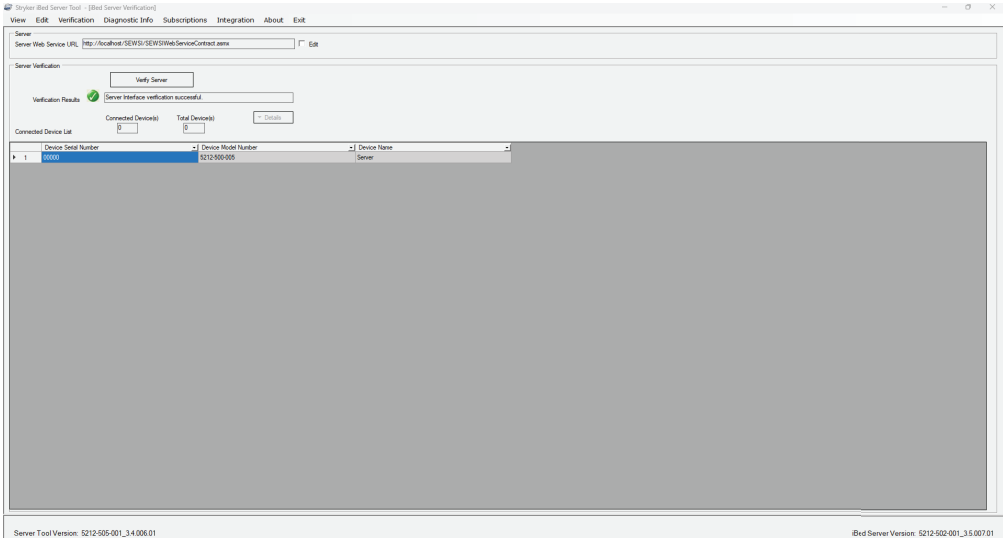


Figure 50 – Verify iBed Server

   a. If the server interface verification is successful, the system returns a green check.
   b. If the server interface verification is unsuccessful, the system returns a red X.

      Note - Before you continue to install the **Stryker iBed Server Tool**, you must resolve this error. To resolve the error, return to the installation process. Make sure that all steps are executed. For further troubleshooting details, see *Troubleshooting* (page 40).

4. If the installation is successful, continue to *Adding devices (clients) to the Master Device List* (page 30).

Setup

Adding devices (clients) to the Master Device List

To add devices to the Master Device List:

1. Open the **Stryker iBed Server Tool**. Select **Start→All Programs→Stryker→Stryker iBed Server Tool** or click the  icon.
2. In the **Stryker iBed Server Tool** window, select **Edit→Master Device List** (Figure 51).

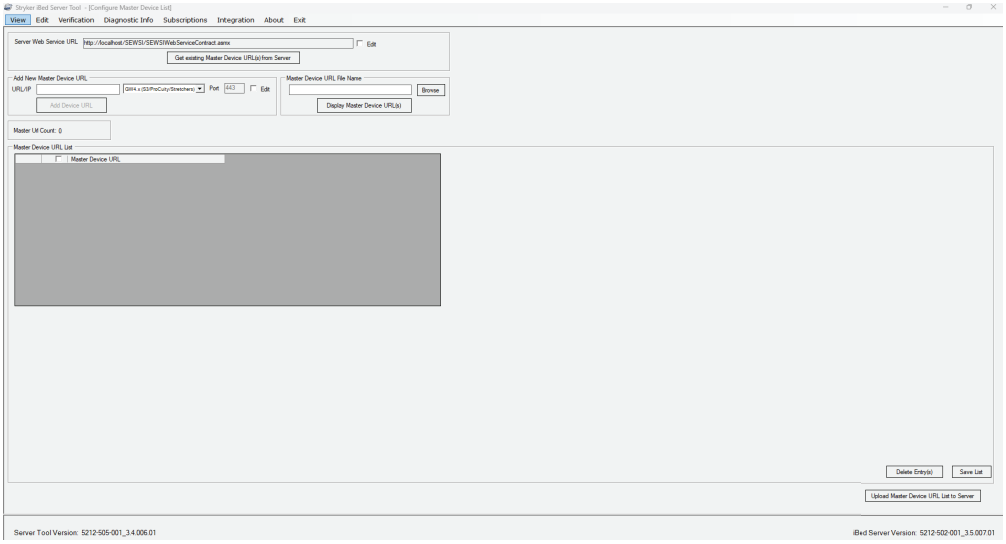


Figure 51 – Edit Master Device List

3. In the **Add New Device URL** box, enter in the URL of the device and then select **Add Device URL** (example: http://10.32.56.101:1639 or http://syk-84253f2356a.stryker.com:1639) (Figure 52).

   Note - Make sure that you enter the web extension http:// and the Stryker communication port:1639 to the IP or DNS name for each device (client).

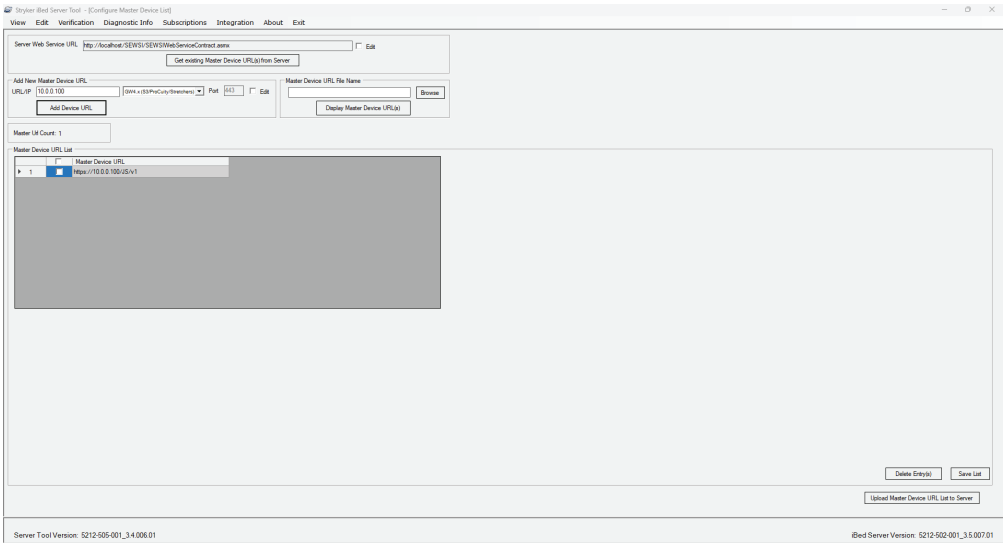


Figure 52 – Add Device URL

4. Repeat step 3 until all new devices have been added.

5. Once all new devices are in the list, check the **Select All** box of the **Master Device URL List**.
6. Select **Upload Master Device URL List to the Server** (Figure 53).

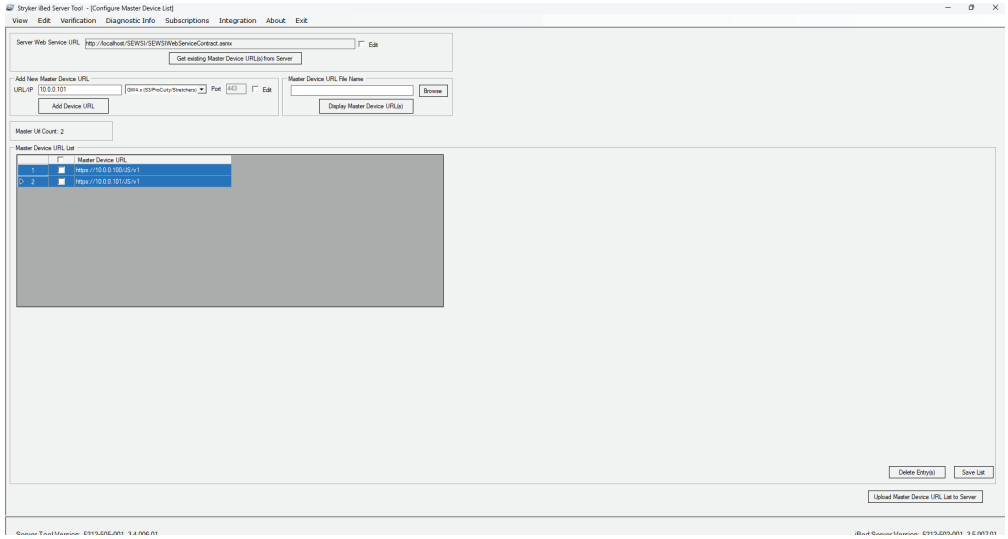


Figure 53 – Master Device URL List

7. Select **OK** in the **Alert** window to confirm that the **Master Device URL List** uploaded to the server.
8. Verify that the **Master Device URL List** uploaded. Open the **iBed Server Tool** window and select **View→iBed Server**.

   Note - Allow time for synchronization before you check the **Master Device URL List**.

Adding locator IDs and hospital locations

To add locator IDs and hospital locations:

1. Open the **Stryker iBed Server Tool**. Select **Start→All Programs→Stryker→Stryker iBed Server Tool** or click the  icon.
2. In the **iBed Server Tool** window, select **Edit→Location Association** (Figure 54).

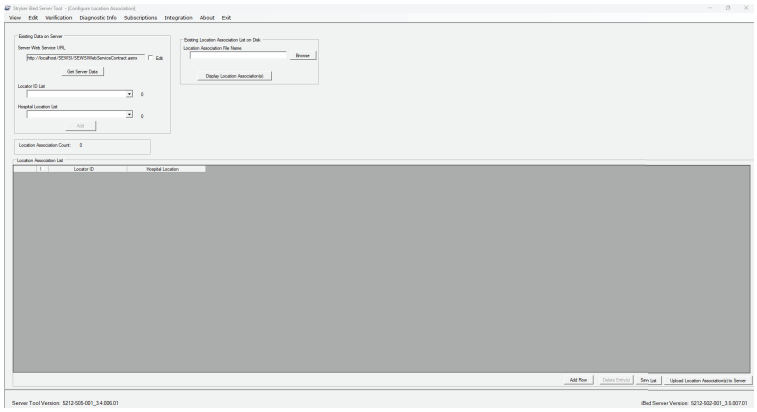


Figure 54 – Location Association

3. In the **Location Association List** box, check the **Locator ID** box and enter the ID from the locator (Figure 55).

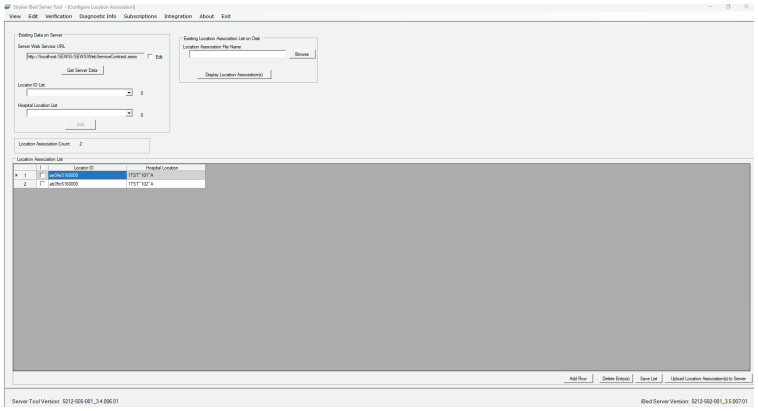


Figure 55 – Add Location Association

4. In the **Location Association List**, check the **Hospital Location** box and enter the Hospital Location.

   Note - The Hospital Location is formatted with the alias name. For example, location HL7.

5. To add another association, select **Add Row**.
6. Repeat steps 3 and 4 until all new Locator IDs and Hospital Locations have been entered.
7. Once all new location associations have been made, check the upper left **Select All** box of the Location Association List. Select **Upload Location Associations to Server** (Figure 56).

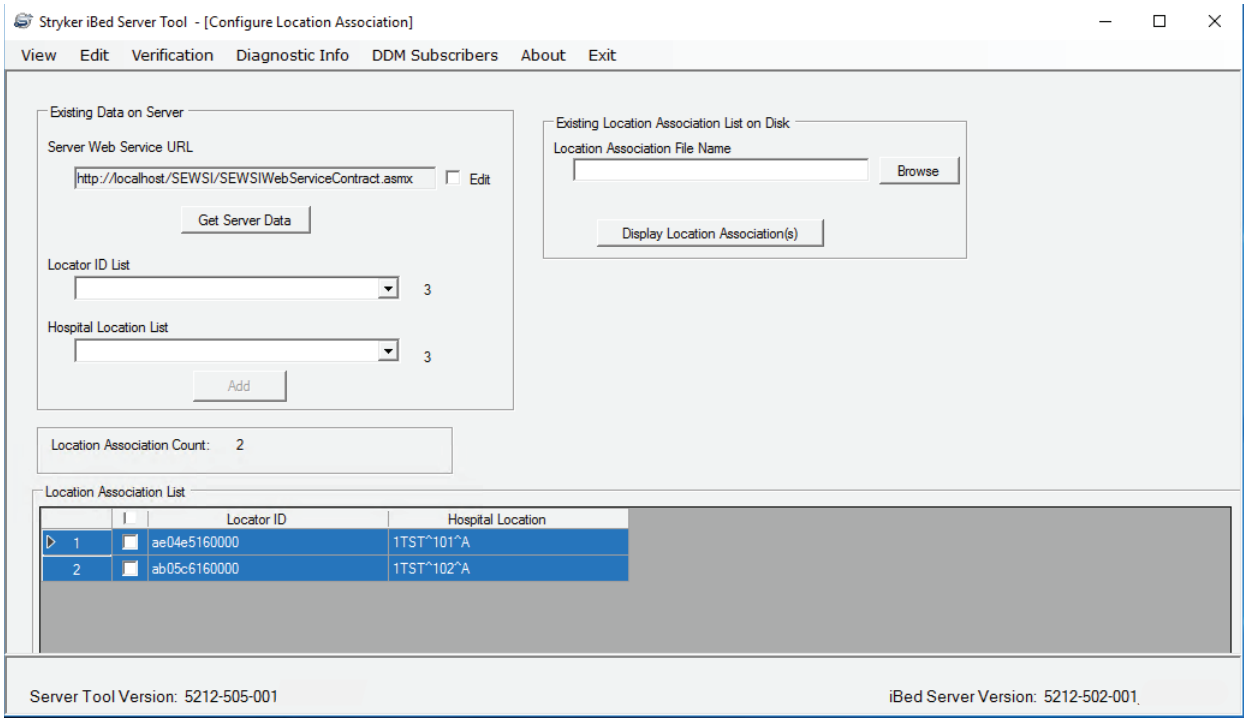


Figure 56 – Upload Location Association

8. Select **OK** in the **Alert** window to confirm that the Locator ID List, Hospital Location List, and Location Association List are uploaded to the server.
9. To verify the lists in the **iBed Server Tool** window, select **View→iBed Server**.

   Note - Allow time for synchronization before you check the **Master Device URL List**.

Adding more Stryker interfaces

Integrating Engage

Note - Only the Stryker Wireless Implementation Team can install this software.

To integrate Engage, follow the installation steps found in the SD-227 available from the Stryker quality system.

Integrating Smart Equipment Management (SEM)

Note - Only the Stryker Wireless Implementation Team can install this software.

To integrate SEM, follow the installation steps found in the SD-227 available from the Stryker quality system.

Integrating Vision

Note - Only the Stryker Wireless Implementation Team can install this software.

To integrate Vision, follow the installation steps found in the SD-227 and M0000017526 available from the Stryker quality system.

Adding a third-party interface

Integrating Rauland Responder® 5

Note - Only the Stryker Wireless Implementation Team can install this software.

To integrate **Rauland Responder** 5, follow the installation steps found in the SD-180 available from the Stryker quality system.

Configuring the wireless router (Stryker device configuration)

Note - iBed Server 2.0 and higher wireless clients authenticate with AES encryption only. Below is an example of configuring a LINKSYS EA6350 router.

To configure the wireless router for Stryker devices:

1. Enter the router's administrative menu to configure the router for use.
2. In the **Basic** tab, edit the 2.4 GHz and 5 GHz Wireless Settings so that they match (Figure 57).

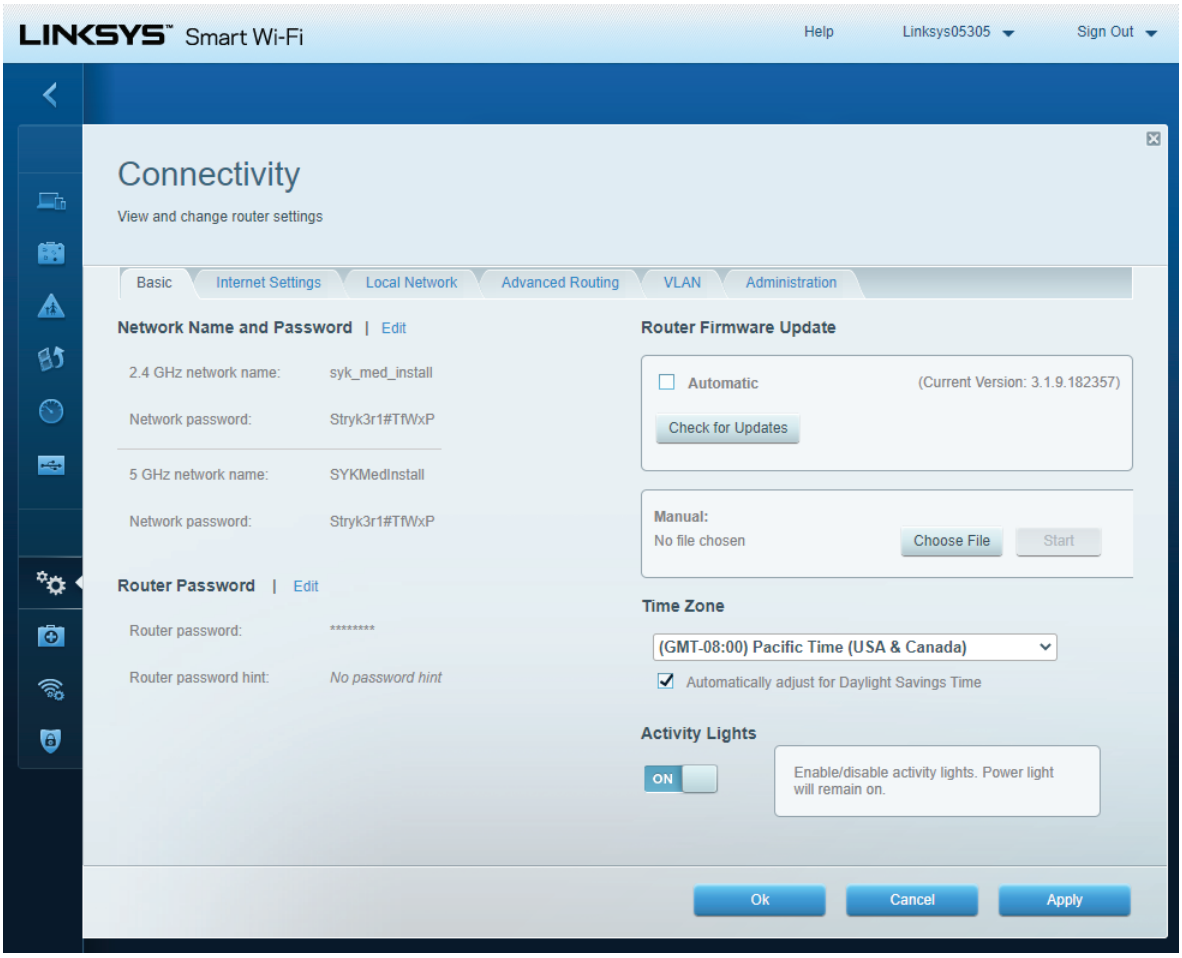


Figure 57 – Basic tab

3. In the **Local Network** tab, verify that the router is set for DHCP (Figure 58).

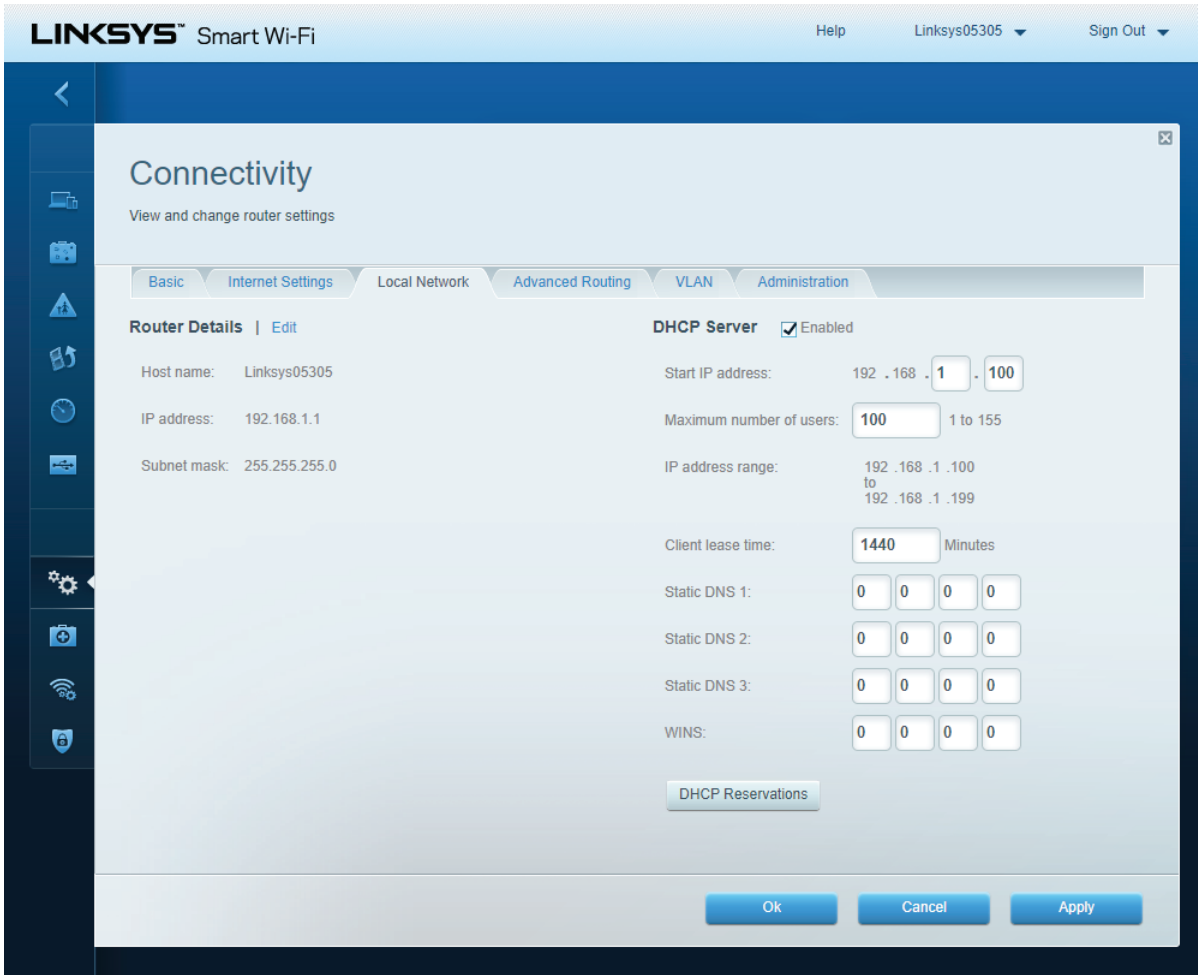


Figure 58 – Local Network tab

4. Select **Apply**.

Configuring the wireless network connection settings

Applies to any Stryker product with the wireless option.

Note - You must have a laptop and a router configured for Stryker defaults.

1. Plug in the router configured for Stryker defaults (*Configuring the wireless router (Stryker device configuration)* (page 34)).
2. Plug the power cord of the product into the wall outlet. Make sure that the wireless option is turned on.
3. Connect the laptop to the syk_med_install SSID that the configured router is broadcasting.
4. Open the **iBed Wireless Configuration Tool**.
5. On the product, enter the **Connectivity Info** menu by accessing the service menu on the footboard. See the appropriate product maintenance manual.
6. Scroll down to the IP address that the router provided for the product.
7. Enter the product IP address in the **Wireless Device URL/IP** box (Figure 59).

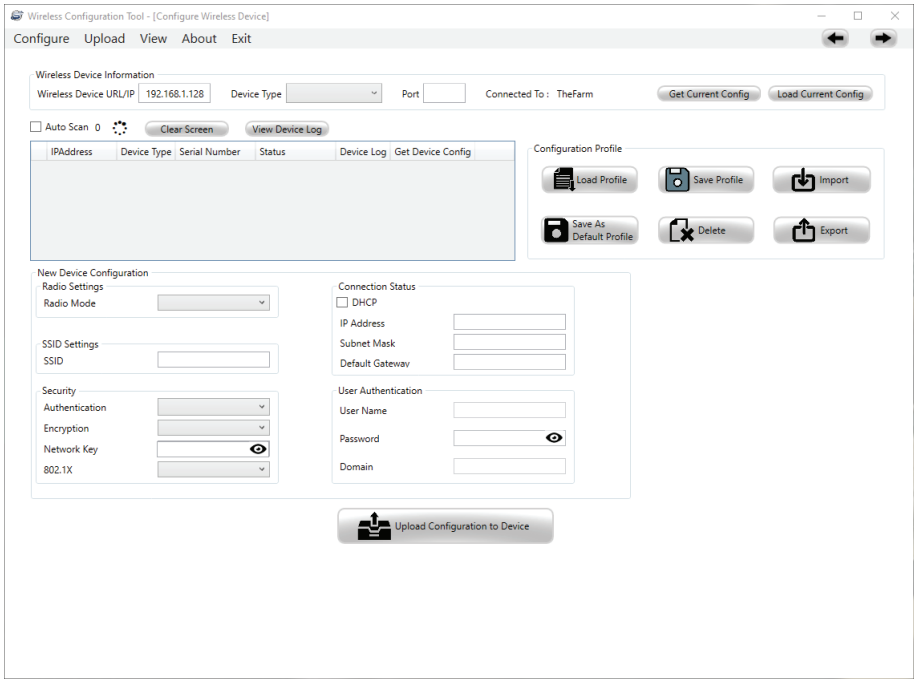


Figure 59 – Wireless Device URL

8. Select **Get Current Config**. The product's wireless default settings are retrieved and connect to the device. The information is shown in the left column of the tool.
9. Select **OK** to confirm the retrieval.
10. Enter the facility network information. Make sure that you fill in the appropriate blanks in the right column of the tool.
11. Select the **Radio Mode** for the facility requirements.
12. Select **Upload Configuration to Device**.

    Note - If the radio does not connect, check the settings entered into the column on the right. If they are incorrect, reset the radio defaults. Repeat the configuration process.

Resetting the wireless module to factory default settings (Med-Surg bed)

Tools required:

- Large paper clip

Procedure:

1. Raise the product to the highest height position.
2. Insert the large paperclip into the reset hole (A) on the bottom side of the wireless module (B) (Figure 60).
3. Hold the large paper clip inside the reset hole for five seconds.

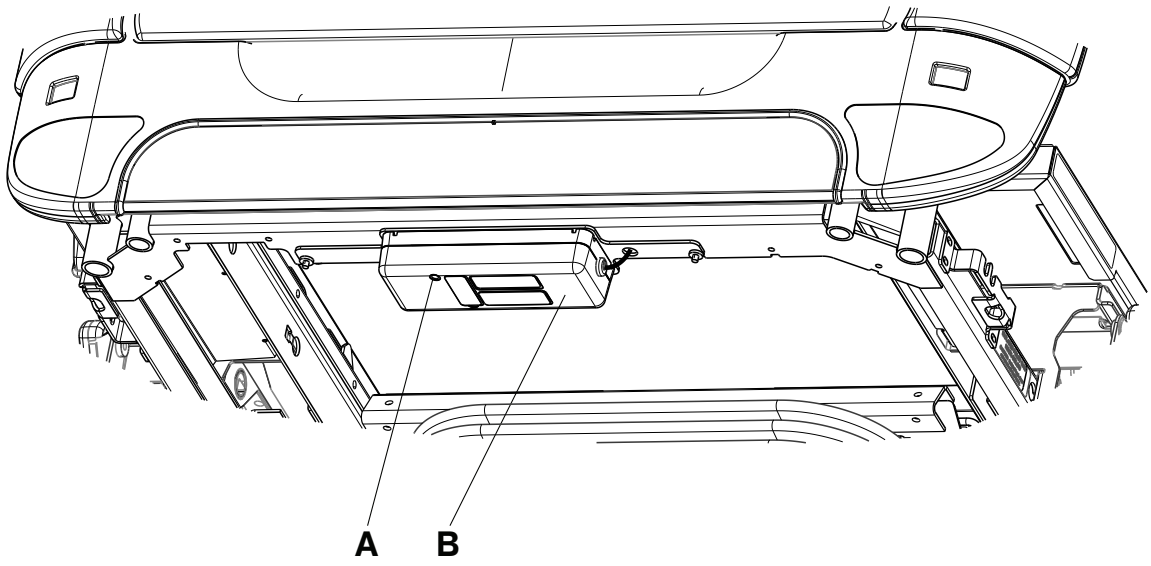


Figure 60 – Wireless module

Resetting the wireless module to factory default settings (Model FL27 InTouch)

- For InTouch 2.1-4.0, complete steps 1–5.
- For InTouch 5.0 or higher, complete step 1 to reset the Wi-Fi.

Tools required:

- Appropriate FL27 InTouch Maintenance Manual

Procedure:

1. See the appropriate FL27 InTouch Maintenance Manual for steps to access the **Configuration** menu. For InTouch 2.1-4.0, see Figure 61. For InTouch 5.0 or higher, see Figure 63.
2. Select **Wi-Fi Configuration** (A) (Figure 61).
3. Select the **Advanced** tab (B) (Figure 62).
4. Select **Reset** (C) (Figure 62).
5. Select **Save**.

InTouch 2.1-4.0

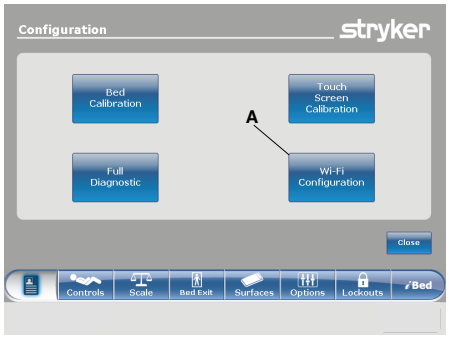


Figure 61 – InTouch Configuration Menu

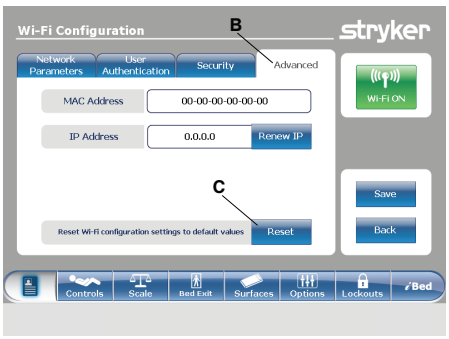


Figure 62 – InTouch Wi-Fi Configuration menu

InTouch 5.0 or higher

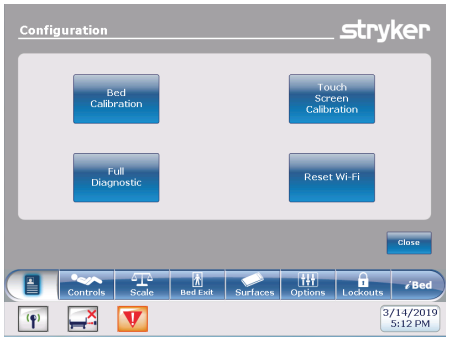


Figure 63 – InTouch Wi-Fi Reset

Resetting the wireless module to factory default settings (Model 3009 ProCuity)

Procedure:

1. Enter the service menu and select **Connectivity** (A).

   Note - See the Model 3009 ProCuity Maintenance Manual for steps to access the service menu.

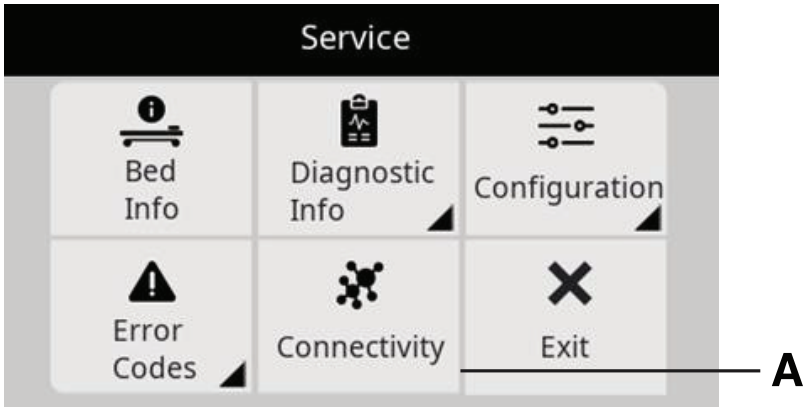


Figure 64 – ProCuity service menu

2. Select **Wi-Fi**.
3. Select **Reset Wi-Fi**.

Troubleshooting

Basic

Problem	Possible cause	Solution
Cannot verify the iBed Server Tool	The Web Service URL is incorrect.	Make sure that the URL in the **Web Service URL** box is correct. 1. If the URL is incorrect, enter the following URL into the **Web Service URL** box (*Verify Stryker iBed Server Tool installation* (page 28)):**http://localhost/SEWSI/SEWSIWebServiceContract.asmx**. 2. Select **Verify Server**.
	The Heartbeat service is not active.	1. Make sure that the Heartbeat service is running. 1.1. If the Heartbeat service has not started, start the service, restart the server, and then reverify the iBed Server Application.
	The IIS Manager does not have the required Default Web Sites.	1. Make sure that the IIS Manager has the required Default Web Sites. 1.1. Navigate to **Internet Information Services (IIS) Manager**. 1.2. Navigate to **Web Sites > Default Web Site** to verify that the three web sites are listed: CHAP / SERVERSCHEMA / SEWSI. 1.3. If the Default Web Site is not listed, reinstall the iBed Server Application.

Problem	Possible cause	Solution
Cannot see the product in the iBed Server Application	The MAC address does not have the IP address or DNS name of the product.	1. If the troubleshooting steps in the appropriate product maintenance manual were followed: 1.1. Use the MAC address from the product and verify the wireless module's IP address or DNS name with IT. 1.2. Ping the wireless module from the server machine using the Command Prompt (ping **IP address or DNS name**). 1.3. Press **Enter**. 1.3.1. If you receive four responses, then the product is on the wireless network. 1.3.2. If you receive no response, make sure that the wireless module on the product.
Problem	**Possible cause**	**Solution**
Cannot see a product in the Server Tools under the Device Location List, but the product shows under the connected device URL List	The device was not added to the device list.	1. Using the server tool, select **Verify Device Directly**. 2. Select **Get Existing Devices**, and then select the device in question. 3. Add the device to the **Device List**. 4. Select the device from **Device List** then select **Verify Devices**. 5. Check the **Connection Status** once it responds. 5.1. If there is a response, the device is communicating on the wireless network.

Problem	Possible cause	Solution
	The serial number in the CPU and the serial number on the product specification label do not match.	1. Identify the product serial number that is stored in the CPU. Match the serial number label on the product. **Note** - If there are two matching serial numbers in the device list, the server recognizes the first device that logs on to the server. 2. To find the product's serial number, put the product into the product configuration mode. Navigate to the **Serial Number > Current SN** to verify the serial number. 3. If the serial number does not match, go to the **Edit SN** menu to edit the serial number, and then save.
Problem	**Possible cause**	**Solution**
Cannot see a location	The Locator ID was entered incorrectly.	1. Using the iBed Locator Association Tool, select **View Current Location Associations**. 2. Select **Get Location Associations** from the server. 3. Look through the **Hospital Location** and verify the Locator ID. **Note** - The Locator ID is alphanumeric and case-sensitive. Use lower case to enter the Locator ID letters, or the server will not recognize the locator. 3.1. If the Locator ID is incorrect, use the **Update** function to update the error. 3.2. If the Locator ID is missing, see *Adding locator IDs and hospital locations* (page 31).

Problem	Possible cause	Solution
Third party does not receive product status information	Incorrect URL entered for the SEWSI or Port 80 is blocked.	1. Make sure that the SEWSI **web.config** file has the correct URL. 1.1. Navigate to the directory where the iBed server tool is installed. 1.1.1. Navigate to the SEWSI folder and open the **web.config** file. 1.1.2. Find the line that contains **ServerURL=.** 1.1.3. Make sure that the local host was replaced with the IP of the server. **Note** - Do not use a DNS name. 2. Make sure that **Port 80** is not blocked. 2.1. **Port 80** needs to be open between the Stryker server and products (bidirectional) and the Stryker server and any third-party servers (bidirectional). 2.2. If **Port 80** is blocked, work with IT to open the port. 3. Search SEWSI logs to make sure that there are no communication failures. Find messages generated for the third party.

Advanced

Connectivity issues

View total device counts to identify drops.

Note - Navigate to the directory where the iBed Server Tool is installed and open the LOGS folder.

1. Find **StrykerMainenanceService_logfile.txt**.
2. Highlight several of the **StrykerMainenanceService_logfile.txt** files. The log files can occur if there was an outage.
   a. Right-click and select **Edit with Notepad++.**
3. In Notepad++, press **Ctrl+F** to open a **Find Window**.
   a. Enter the string “[Total Connected Devices Count excluding server = xx]” and select **Find in All Opened Documents** to search.
   b. The **Find Result** pane in Notepad++ populates with the log lines as a result of your search (Figure 65).

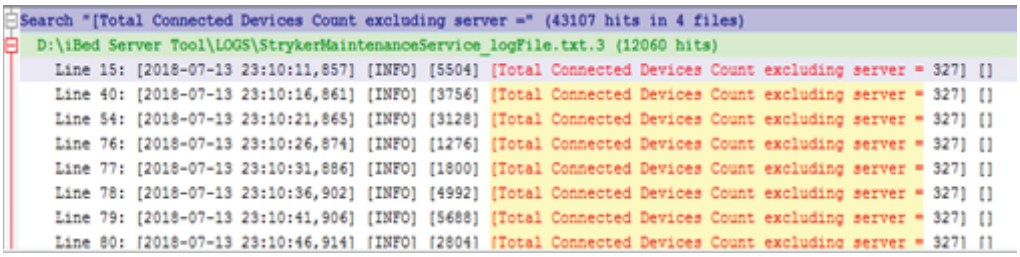


Figure 65 – Total device counts

c. Review the list to locate the drop in the number of connected devices and the duration of time the devices were offline.

Note - Work with the local IT department to investigate.

Third-party communication issues

Search SEWSI log files for third-party messages.

1. Open the iBed Server Tool.
2. Navigate to the subscription list tab.

   Note - When you search for messages from a product, make sure that you use the correct Device ID.
3. Copy the subscription ID for a device that is going to the correct third party.

   a. Verify the subscriber URL to find messages to a specific third party.
4. Navigate to the directory where iBed Server Tool is installed.

   a. Open the **LOGS** folder.

   b. Find **SEWSI_logfile.txt**.
5. For a specific timeframe, search for the modified date in Windows Explorer. Highlight many **SEWSI_logfile.txt** files.
6. Right-click the highlighted files and select **Edit with Notepad++**.
7. Press **Ctrl+F** to open a **Find** window.

   a. Paste the subscription ID copied in step 3 into the **Find** window.

   b. Select **Find in all opened documents**.

   c. The **Find result** pane opens in Notepadd ++ with all messages that contain the **Subscriber ID**.
8. Start the XML message from the **Find** pane to open the file to that line.

   a. The XML messages start with **<?xml version=”1.0” encoding=utf-8”?>**.

   Note - Example message with the payload XML data highlighted: <?xml version="1.0" encoding="utf-8"?><soap:Envelope xmlns:soap="http://schemas.xmlsoap.org/soap/envelope/" xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance" xmlns:xsd="http://www.w3.org/2001/XMLSchema"><soap:Body><ReceiveSubscriptionRequest xmlns="http://SEWSI.ServiceContracts/2008/09"><SubscriberID>C3000-000-000_180415201155204742</SubscriberID>**<PayloadXML><device id="3000-000-000_180415201"><BedHeightIn>27</BedHeightIn><LastLoggedWeightLb>102.900009</LastLoggedWeightLb><BedExitAlarming>false</BedExitAlarming></device></PayloadXML><TimeStamp>2018-07-16T11:59:14.3410647-04:00</TimeStamp>**</ReceiveSubscriptionRequest></soap:Body></soap:Envelope>] []

Device not connecting to server

Search for duplicate serial numbers (devices newer than GW1).

1. Open the iBed Server Tool.
2. Navigate to the **Client Diagnostic Info** tab.

3. Select the far left blank cell of the header to highlight the entire table.
   a. Copy and paste the data into a **Microsoft Excel** spreadsheet.
4. Highlight the **Client ID** column.
5. In the **Home** tab of the ribbon, select **Conditional Formatting**.
   a. Select **Highlight Cell Rules→Duplicate Values**.
   b. Select **OK** to highlight duplicates in red.
   c. Highlight the row above where the data was pasted, select the **Data** tab, and select **Filter**.

   Note - Any cells highlighted (except **Network Exception/Timeouts**) are duplicate serial numbers that you need to resolve.

Connectivity issues of one or more devices

Not receiving a specific product status over port 80.

Verify communication from devices to the server with SOAP UI.

Note - To complete this procedure, a Stryker supplied project file is required.

1. Open **SOAP UI**.
2. In the **Projects** pane, expand the **SEWSI** folder.
3. Select **ConnectivityMock** to open the **ConnectivityMock** window (Figure 66).

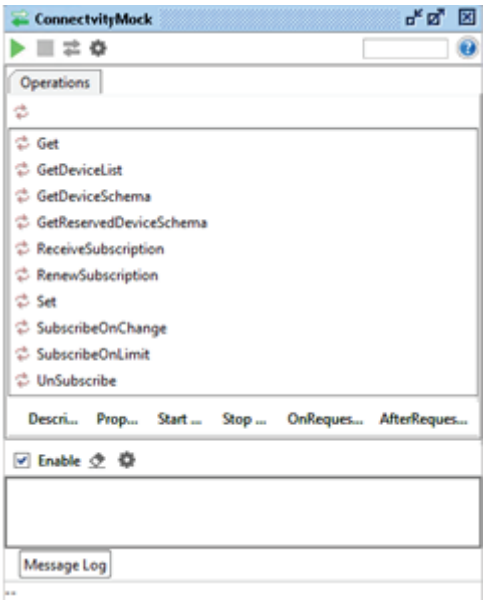


Figure 66 – Connectivity Mock

4. Select the gear icon to edit settings for Mock Third-party.
   a. Modify the host URL to the IP address of the server where SOAP UI is running (Figure 67).

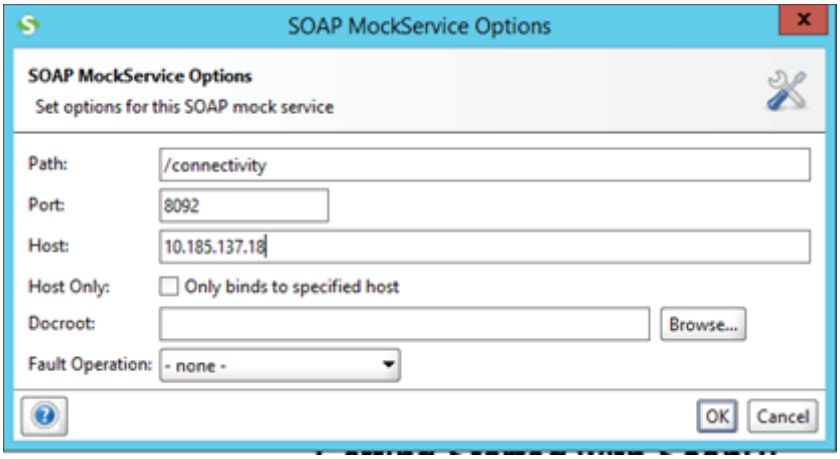


Figure 67 – SOAP UI

b. Select **OK** to save.

5. Select the green **Play** icon to start the Mock Third-party Service.
6. Select the green arrows to open the service webpage to verify connection.

   a. Copy the URL of the webpage to the clipboard.

7. In the **Projects** pane, expand **SEWSIWebServiceContract**.

   a. Expand the **SubscribeOnChange**.

   b. Double-click **VTF - Sub 3 (72 hour)**.

   c. Modify the Subscriber URL with the URL from step 3 (Figure 68).



Figure 68 – VTF - Sub 3 (72 hour)

d. Change the Device ID to the Device ID being searched for (Figure 68).

e. Select the **Play** icon in the **VTF - Sub 3 (72 hour)** window.

8. In the **ConnectivityMock** window, messages appear if the ports are open and the server is able to communicate with the device (Figure 69).

   Note - If messages do not appear, port 80 may be closed or the **WebServiceURL** in the **SEWSI web.config** file may be incorrect.

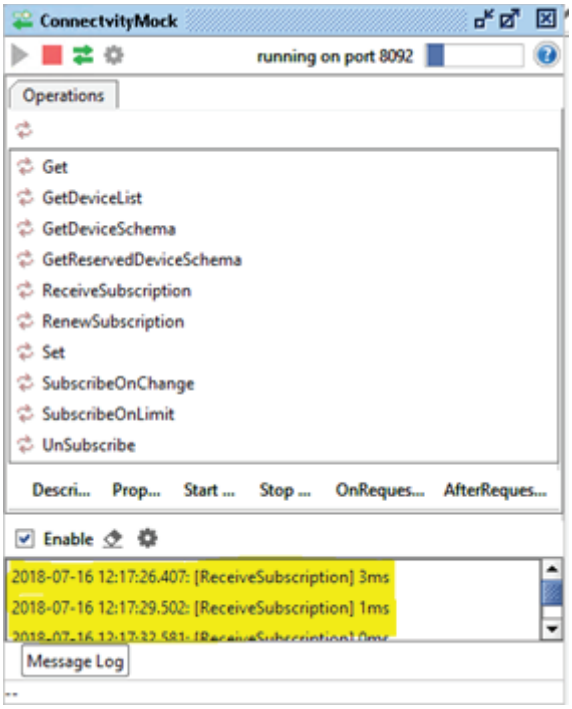


Figure 69 – Message Log

9. Double-click the message to view the XML generated (Figure 70).

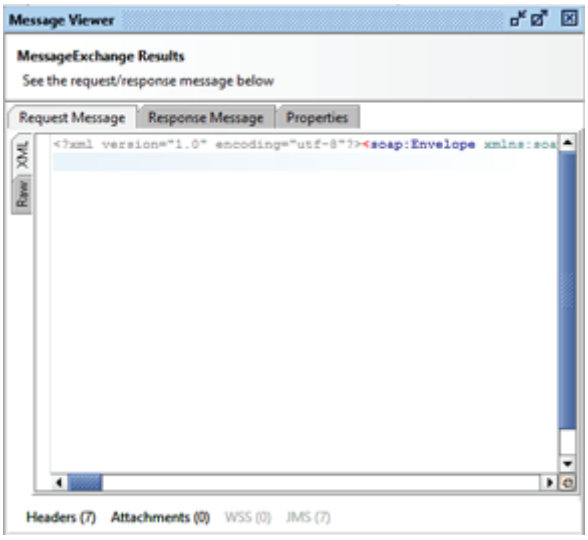


Figure 70 – Message Viewer

Cannot communicate with device

Verify communication with the device over the port using **TELNET** are open.

1. Open a **command** prompt.
2. Enter the command **telnet <IPAddress> <Port>**, where the **IP Address** is the address of the device and the **Port** is the port number for verification (Figure 71).

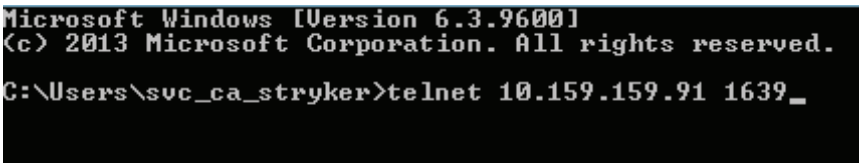


Figure 71 – Command prompt

- A blank box with a blinking cursor indicates that the port is open.
- **Connecting to** indicates that the port is closed or the device is offline (Figure 72).

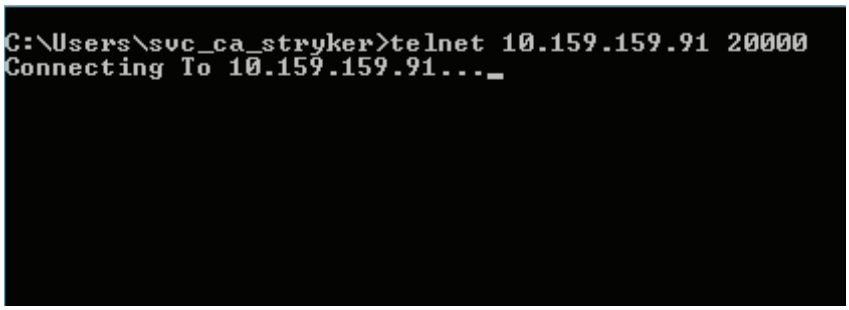


Figure 72 – Connecting

Note - Only use **TELNET** for a device that is online and pingable.

Cannot communicate with device (DNS only)

Verify the Hostname with **NSLOOKUP**.

1. Open a **command** prompt.
2. Enter the command **nslookup <IPAddress>** where the **IP Address** is the address of the device for **DNS entry** verification.
   - A reply with the **hostname** and **IP address** indicates success (Figure 73).

   Note - The first line is the **DNS** server name and IP address. The second line is the device hostname/IP.

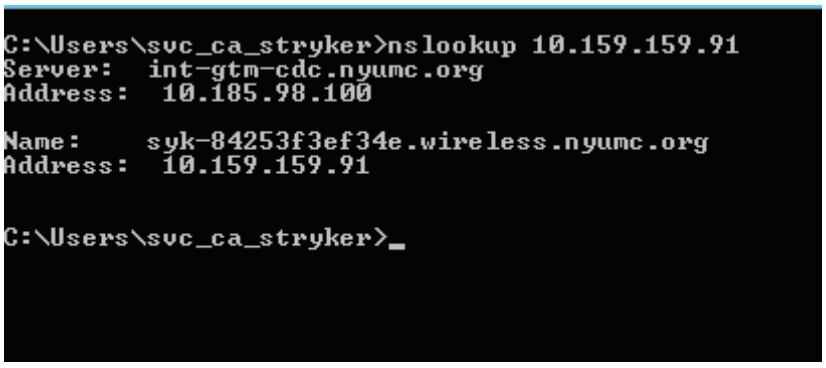


Figure 73 – DNS success

- A reply that states **<DNSServerName> can't find <IPAddress>** indicates failure (Figure 74).

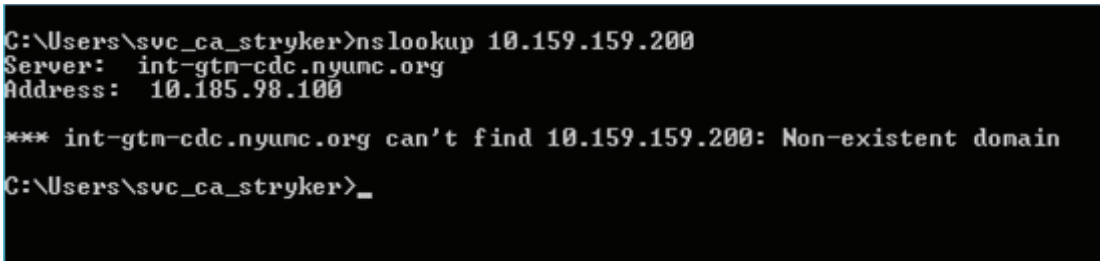


Figure 74 – DNS failure

3. To verify a reverse lookup, enter the command **nslookup <hostname>** where the **hostname** is the device you are verifying the DNS entry for.

   Note - The reply from the server must match the reply from step 2.

Smart Equipment Management option – troubleshooting

1. To verify the **Device Data Manager Utility**:
   - Select **Start** from Windows.
   - Enter **StrykerDeviceDataManagerRegistration** in the search box.
   - Make sure that the **StrykerDeviceDataManagerRegistration** utility displays in the search results.
2. To verify the iBed Server Tool:
   - Locate the machine where the Stryker iBed Server Application is installed. Open the **iBed Server Tool**.
   - Select the **Subscription List** tab. Make sure that the **Device ID** and **Subscription ID** columns are populated.
   - Make sure that the server has a general subscription and each device has both a general and alarm subscription (Figure 75).

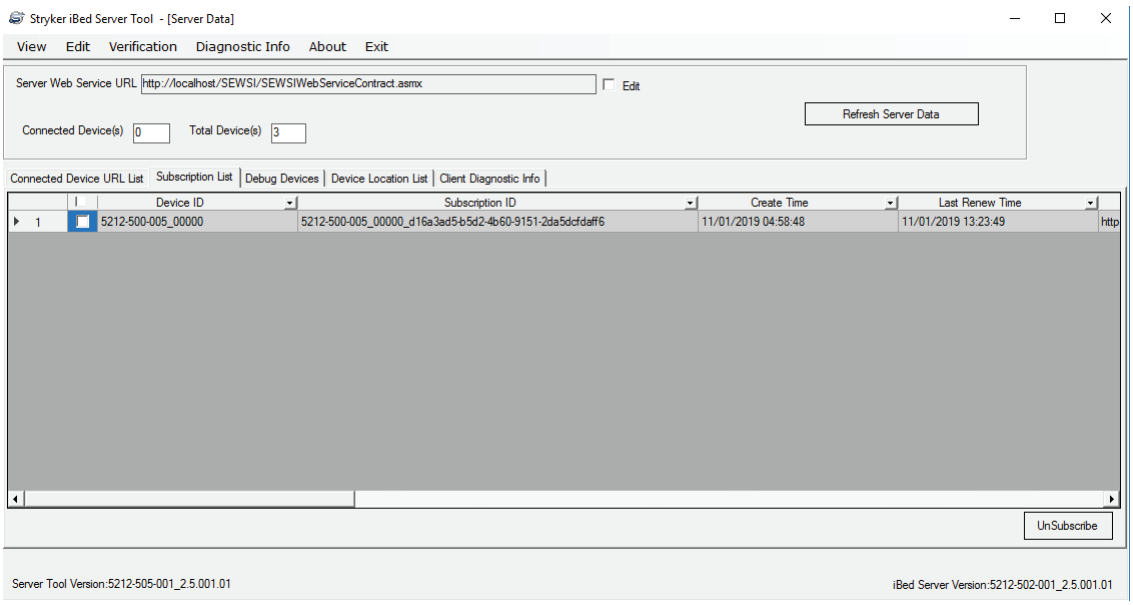


Figure 75 – General subscription

- Make sure that the **Subscriber URL** column displays the same URL shown in the **Web.config** file of the Device Data Manager (Figure 76 and Figure 77).

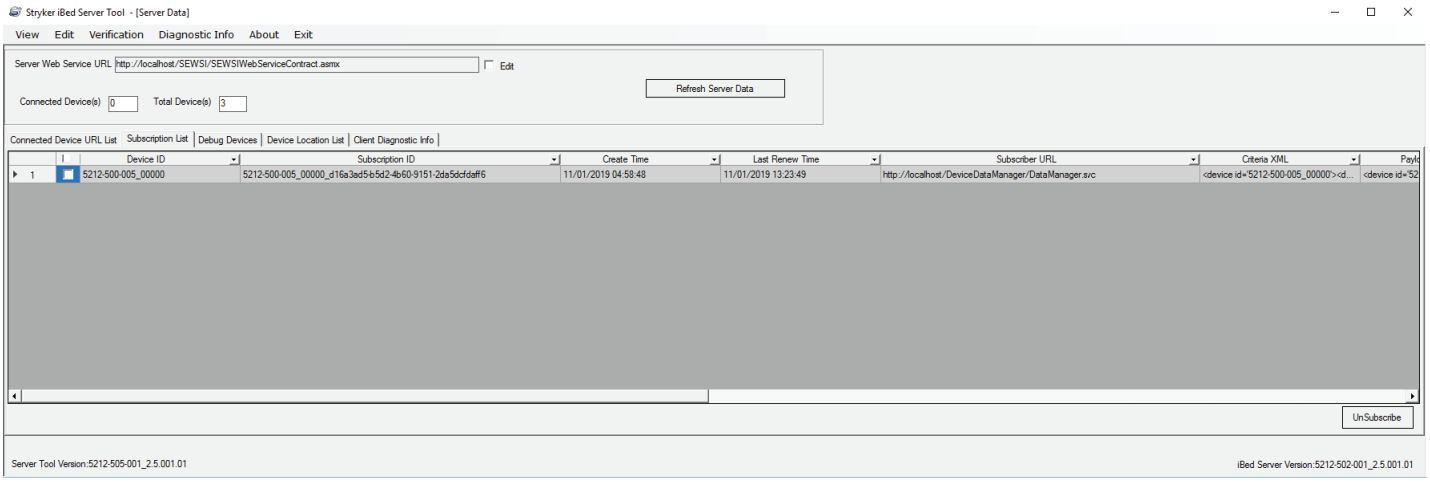


Figure 76 – Subscription List

```
appSettings>
   <add key="SEWSI_URL" value="http://10.117.40.238/SEWSI/SEWSIWebServiceContract.asmx"></add>
   <add key="CHAP_URL" value="http://10.117.40.238/CHAP/CHAPWebServiceContract.asmx"></add>
   <add key="SUBSCRIBERURL" value="http://10.117.40.238/DeviceDataManager/DataManager.svc"></add>
   <add key="IserverIP" value="10.117.40.238"></add>
   <add key="IsLifenet" value="true"></add>
   <add key="LifenetRegistrationUrl" value="https://api-ng-dev.physio-labs.com/bedagents/?api-version=1.0"></add>
   <add key="LifenetAgentUrl" value="/bedagents/{0}?api-version=1.0"></add>
   <add key="LifenetBedUrl" value="/beds/{0}?api-version=1.0"></add>
   <add key="LifeNetUserName" value="Test"></add>
```

Figure 77 – Web.config file

3. To verify the server data in the Device Data Manager log file:

   - Search for a string **"DeviceID=<SerialNumber> JsonContent="** in the log file (Figure 78)

     Note - Replace **<SerialNumber>** with a serial number in the **Web.config** file.

```
[2017-11-23 11:51:07,355] [DEBUG] [19364] [Entering function LifenetDataManager::UploadDataToCloud] []
[2017-11-23 11:51:07,394] [INFO] [19364] [In LifenetDataManager DeviceID = 1234567890 JsonContent=
{"GatewaySerial":"1234567890","GatewayModel":"5212-500-005_00000","IPAddress":"10.50.113.78","SoftwareVersion":"1.0.0.2","Description":"TestHospital","TotalDevices":6}]
[2017-11-23 11:51:07,470] [DEBUG] [19364] [Leaving function IServerManager::ParseSubscribedDataStream] []
```

Figure 78 – Example: DeviceID = 1234567890 JsonContent=

   - Search for a string **"Data Uploaded for Server successfully!"** in the log file (Figure 79)

```
[2017-05-22 13:33:07,487] [INFO] [3624] [No change detected in server data returning] []
[2017-05-22 13:33:07,503] [INFO] [15340] [Data Upload Response for deviceID = :3000-000-000_DeviceS11Pal43 content = ] []
[2017-05-22 13:33:07,503] [INFO] [15340] [Data Uploaded successfully for DeviceID = 3000-000-000_DeviceS11Pal43] []
[2017-05-22 13:33:07,518] [INFO] [16072] [Data Upload Response for deviceID = :247703F4B422 content = ] []
[2017-05-22 13:33:07,518] [INFO] [16072] [Data Uploaded for Server successfully!] [
[2017-05-22 13:33:07,612] [INFO] [16072] [Starting request processing for SubscriptionID = C3000-000-000_DeviceS11Pal78_201705221317313380] []
[2017-05-22 13:33:07,737] [INFO] [15340] [Data Upload Response for deviceID = :3000-000-000_DeviceS11Pal138 content = ] []
[2017-05-22 13:33:07,737] [INFO] [15340] [Data Uploaded successfully for DeviceID = 3000-000-000_DeviceS11Pal138] []
[2017-05-22 13:33:07,737] [INFO] [16072] [Time taken for deserilization (ms) = 0] []
[2017-05-22 13:33:07,752] [INFO] [6156] [DeviceID = 3000-000-000_DeviceS11Pal78 JsonContent=
```

Figure 79 – Data uploaded in log file

4. To verify the connected devices in the log file:

   - Search for a string **"DeviceID = <deviceID> JsonContent="** in the log file (Figure 80)

     Note - Replace **<deviceID>** with the device ID of the connected device.

[2017-12-05 14:13:26,222] [INFO] [10152] [In LifenetDataManager DeviceID = 3000-000-000_DeviceS1 JsonContent= {"ActiveDeviceError":true,"ActiveDeviceErrorInformation":"load cell error","DeviceErrorLog1":"FR LoadCell Error","DeviceErrorLog2":"FRSR Switch Error","DeviceErrorLog3":"HRSR Switch Error","DeviceErrorLog4":"FLSR Switch Error","DeviceErrorLog5":"FLSR Switch Error","DeviceErrorLog6":"FLSR Switch Error","DeviceErrorLog7":"FRSR Switch Error","DeviceErrorLog8":"FRSR Switch Error","DeviceErrorLog9":"FR LoadCell Error","DeviceErrorLog10":"FR LoadCell Error","IPAddress":"172.156.10.11","MACAddress":"pqrst","NetworkAddress":"http://localhost/device1/service.asmx/Interface","SoftwareVersion":"1.0","PatientPresent":false,"RSSI":"20","LowBedHeight":false,"HRSiderailUp":true,"HLSiderailUp":true,"FRSiderailUp":true,"FLSiderailUp":true,"BrakeOn":true,"BedExitArmed":false,"LBSArmed":false,"BedExitAlarming":false,"LBSAlarming":false,"BrakeAlarming":false,"Online":true,"ConnectionUptime":1564.4642602,"SerialNumber":"3000-000-000_DeviceS1","Model":"Med-Surg"}] []

Figure 80 – Example: DeviceID = 3000-000-000_DeviceS1 JsonContent=

- Search for a string **"Data Uploaded successfully for DeviceID = <deviceID>"** in the log file (Figure 81)

  Note - Replace **<deviceID>** with the device ID of the connected device.

```
[2017-12-05 13:47:56,425] [INFO] [12688] [Connection to Lifenet established successfully. Data uploaded successfully for d
[2017-12-05 13:47:56,425] [DEBUG] [12688] [Leaving function LifenetDataManager::UploadDataToCloud] []
[2017-12-05 13:47:56,425] [INFO] [12688] [Device data successfully uploaded for 3000-000-000_DeviceS1 in Lifenet] []
[2017-12-05 13:47:56,425] [DEBUG] [12688] [Leaving function LifenetDeviceStatusManager::UploadDeviceData] []
[2017-12-05 13:47:56,425] [DEBUG] [12688] [Leaving function LifenetDeviceStatusManager::ProcessData] []
[2017-12-05 13:47:56,425] [INFO] [00440] [Connection to Lifenet established successfully. Data Uploaded successfully for de
```

Figure 81 – Example: Data Uploaded successfully for 3000-000-000_DeviceS1 in LIFENET

Email alerts

The iBed Server Application generates emails for the following scenarios:

Email information	Scenario
Email Subject: Stryker iBed Server Alert **Email Body:** 2015-04-20 00:24:59,298 [2964] ERROR Stryker.IServer. BusinessLogic.SEWSI.RuleManager. EMailToAdminForLowBatteryStatus - SEND EMAIL: Stryker room locator f5d5b2130000 in room 205 has a low battery. Currently connected to device ID 3000-000-000_ 130316141.	Low Battery Status is true for the BBID mapped with a location
Email Subject: Stryker iBed Server Alert **Email Body:** 2015-04-20 00:35:51,784 [2328] ERROR Stryker.IServer. BusinessLogic.SEWSI.RuleManager. EMailToAdminForLowBatteryStatus - SEND EMAIL: Stryker room locator f5d5b2130000 is not in the location list and has a low battery, update the location and association lists as required. Currently connected to device ID 3000-000-000_130316141.	Low Battery Status is true for a BBID which is not mapped to any room or the BBID is missing
Email Subject: Stryker iBed Server Alert **Email Body:** 2015-04-20 00:45:22,254 [2328] ERROR Stryker.IServer. BusinessLogic.SEWSI.RuleManager. EmailToAdminForMissingBBID - SEND EMAIL: Stryker room locator f5d5b2130000 is not in the location list and does not have an association to a room, update or create the location association as required. Currently connected to device ID 3000-000-000_130316141.	BBID is sent in the subscription payload but it is not present in the "BBIDList.xml" file

Email information	Scenario
Email Subject: Stryker iBed Server Alert **Email Body:** 2015-04-20 00:48:02,395 [2328] ERROR Stryker.IServer. BusinessLogic.SEWSI.RuleManager. EmailToAdminForMissingBBID - SEND EMAIL: Stryker room locator f5d5b2130000 is in the location list but is not associated to a room, update the location association as required. Currently connected to device ID 3000-000-000_ 130316141.	BBID is sent in payload and it is present in “BBIDList.xml” file but is not present in “DeviceBBIdLocationAssciation. xml” file
Email Subject: Stryker iBed Server Alert **Email Body:** 2015-04-20 00:50:52,536 [2328] ERROR Stryker.IServer. BusinessLogic.SEWSI.RuleManager. EmailToAdminForMissingBBID - SEND EMAIL: Stryker room locator f5d5b2130000 is in the location list but is associated to an undefined room, update the location association as required. Currently connected to device ID 3000-000-000_130316141.	BBID is sent in payload and it is present in “BBIDList.xml” file and in “DeviceBBIdLocationAssciation.xml” file but the location for that BBID is missing in “DeviceBBIdLocationAssciation.xml” file
Email Subject: **Stryker iBed Server Urgent Alert** **Email Body:** Application Health Check Failed at Step 1 -> iBedServer is unable to access the database. Please restart the MS-SQL database. After restart, if the message continues, please contact Stryker support.	When DB is down
Email Subject: **Stryker iBed Server Urgent Alert** **Email Body:** Application Health Check Failed at Step 2 -> The MS-SQL database is corrupt. Following Tables are missing in Database ->DeviceConnectionInfoList. Please contact Stryker support to rebuild. Application Health Check Failed at Step 3 -> iBedServer is unable to access SEWSI. Please restart the World Wide Web Publishing Service and StrykerSEWSIHeartbeatservice. After restart, if the message continues, please contact Stryker support.	DeviceConnectionInfoList table does not exist
Email Subject: **Stryker iBed Server Urgent Alert** **Email Body:** Application Health Check Failed at Step 2 -> The MS-SQL database is corrupt. Following Tables are missing in Database ->MasterSubscriptionInfo. Please contact Stryker support to rebuild.	MasterSubscriptionInfo table does not exist

Email information	Scenario
Email Subject: **Stryker iBed Server Urgent Alert** **Email Body:** Application Health Check Failed at Step 2 -> The MS-SQL database is corrupt. Following Logins are missing in Database ->NT AUTHORITY\LOCAL SERVICE. Please contact Stryker support to rebuild.	LOCAL SERVICE does not exist
Email Subject: **Stryker iBed Server Urgent Alert** **Email Body:** Application Health Check Failed at Step 2 -> The MS-SQL database is corrupt. Following Logins are missing in Database ->NT AUTHORITY\NETWORK SERVICE. Please contact Stryker support to rebuild. Application Health Check Failed at Step 3 -> iBedServer is unable to access SEWSI. Please restart the World Wide Web Publishing Service and StrykerSEWSIHeartbeatservice. After restart, if the message continues, please contact Stryker support.	NETWORK SERVICE does not exist
Email Subject: **Stryker iBed Server Urgent Alert** **Email Body:** Application Health Check Failed at Step 3 -> iBedServer is unable to access SEWSI. Please restart the World Wide Web Publishing Service and StrykerSEWSIHeartbeatservice. After restart, if the message continues, please contact Stryker support. Application Health Check Failed at Step 4 -> StrykerSEWSIHeartbeatservice is not running. Please restart StrykerSEWSIHeartbeatservice. After restart, if the message continues, please contact Stryker support.	Both SEWSI and HB services are down
Email Subject: **Stryker iBed Server Urgent Alert** **Email Body:** Application Health Check Failed at Step 2 -> The MS-SQL database is corrupt. Following Tables are missing in Database ->MasterSubscriptionInfo. Please contact Stryker support to rebuild. Application Health Check Failed at Step 3 -> iBedServer is unable to access SEWSI. Please restart the World Wide Web Publishing Service and StrykerSEWSIHeartbeatservice. After restart, if the message continues, please contact Stryker support. Application Health Check Failed at Step 4 -> StrykerSEWSIHeartbeatservice is not running. Please restart StrykerSEWSIHeartbeatservice. After restart, if the message continues, please contact Stryker support.	Both SEWSI and HB services are down and the MasterSubscriptionInfo table does not exist

Email information	Scenario
Email Subject: **Stryker iBed Server Urgent Alert** **Email Body:** Application Health Check Failed at Step 3 -> iBedServer is unable to access SEWSI. Please restart the World Wide Web Publishing Service and StrykerSEWSIHeartbeatservice. After restart, if the message continues, please contact Stryker support. Application Health Check Failed at Step 4 -> StrykerSEWSIHeartbeatservice is not running. Please restart StrykerSEWSIHeartbeatservice. After restart, if the message continues, please contact Stryker support.	HB is down
Email Subject: **Stryker iBed Server Urgent Alert** **Email Body:** iBed Server is unable to communicate with Stryker clients. Please check the server/network configuration. If the message continues, please contact Stryker Technical Support.	No devices are detected
Email Subject: **Stryker iBed Server Urgent Alert** **Email Body:** Total number of clients connected to iBed Server has gone below <configured threshold>. Please check the server/ network configuration. If the message continues, please contact Stryker Technical Support.	Number of connected devices drops below the configured threshold value
Email Subject: **Stryker iBed Server Urgent Alert** **Email Body:** The following errors with Third-party Communication has been recorded in last 1 hour. <Error>	Error with the Third-party Communications

Stryker Corporation or its divisions or other corporate affiliated entities own, use or have applied for the following trademarks or service marks: **Engage, iBed, InTouch, ProCuity, Stryker**. All other trademarks are trademarks of their respective owners or holders.

Stryker Medical
3800 E. Centre Avenue
Portage, MI 49002
USA

5212-409-001 Rev AC.0 2025-05
WCR: AC.2