

iBed® Server v2

Installation/Configuration Manual

REF 5212

Connected Hospital®



Symbols

	General warning
	Caution
	Manufacturer
	Direct current
	Alternating current

Table of Contents

Warning/Caution/Note Definition	2
Summary of safety precautions	3
Introduction	4
Indications for use	4
iBed Server software	4
System requirements and recommendations	4
Device connection requirements	5
Contact information	6
Installation	7
Server configuration	7
Windows Server 2008	7
Windows Server 2012	17
iBed Server application	29
iBed Wireless Configuration Tool	36
Editing Windows configuration	37
Configuring the Internet Information Services (IIS) Manager for iBed Server	38
Verify iBed Server	40
Setup	42
Adding devices (clients) to the Master Device List	42
Adding iBed Locator IDs and hospital locations	43
Adding an additional Stryker interface	45
Smart Equipment Management (SEM)	45
Adding a third-party interface	50
Integrating Rauland Responder® 5	50
Configuring the wireless router (Stryker device configuration)	51
Configuring wireless network connection settings	53
Resetting the wireless module to factory default settings (Med-Surg bed)	54
Resetting the wireless module to factory default settings (Model FL27 InTouch)	55
Troubleshooting	56
Basic	56
Advanced	59
Connectivity issues (total device counts)	59
Third party communication issues	60
Device not connecting to server	61
Connectivity issues to one / multiple devices	61
Cannot communicate with device (verify ports are open)	63
Cannot communicate with device (DNS only)	64
Smart Equipment Management (option) troubleshooting	65
Email alerts	68

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.

Summary of safety precautions

Always read and strictly follow the warnings and cautions listed on this page. Service only by qualified personnel.

CAUTION

- Before proceeding with this installation, make sure that a previous version of the **iBed** Server application is not currently installed on the target system. If a previous version was installed, uninstall the software. If you attempt to install the application on a system where a previous version was installed, the installer behavior may be unpredictable.
 - Before proceeding with this installation, make sure that a previous version of the **iBed** Wireless configuration tool application is not currently installed on the target system. If a previous version was installed, uninstall the software. If you attempt to install the application on a system where a previous version was installed, the installer behavior may be unpredictable.
-

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.

Indications for use

The intended use for the **iBed®** Wireless (with **iBed** Awareness) is to assist clinical staff to monitor bed parameters on specific Stryker beds. The desired bed parameters are set by operators at the bedside. The **iBed** Wireless software is only intended for use with specifically enabled Stryker beds that have been verified and validated with the **iBed** Wireless software, and is not intended to provide bed status information for non-Stryker beds. The **iBed** Wireless software is not intended to communicate any patient status information, nor to permanently store any type of data. The **iBed** Wireless with **iBed** Awareness System is not intended to provide automated treatment decisions or as a substitute for professional healthcare judgment. The **iBed** Wireless with **iBed** Awareness System is not a replacement or substitute for vital signs monitoring or alert equipment. All patient medical diagnosis and treatment are to be performed under direct supervision and oversight of an appropriate healthcare professional.

iBed Server software

The included **iBed** Server installation CD (5212-501-001) contains the software required for the **iBed** Server installation.

Note - Before uninstalling the application, copy the following files to the **Public Documents** folder. The files will import to the new application. Using the **iBed** Server Tool, configure the Master Device List and the Locator Associations.

Install directory\Stryker\iBedServerApplication\Data

BBIDList.xml

DeviceURLs.xml

DeviceBBIDLocationAssociation.xml

HospitalLocationList.xml

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

System requirements and recommendations

Note

- If minimum system requirements are not met, system performance will be impacted.
- Apply relevant software patches annually.

Hardware:

Minimum requirements for the **iBed** Server hardware is dependent on the number of beds connected to the system.

1 - 300 connected beds:

- 2.x GHz processor or higher with a total of 4 cores
- Memory: 8 GB RAM
- Hard Drive: 150 GB

301 - 600 connected beds:

- 2.x GHz processor or higher with a total of 8 cores
- Memory: 16 GB RAM

- Hard Drive: 150 GB

601 - 800 connected beds:

- 2.x GHz processor or higher with a total of 16 cores
- Memory: 32 GB RAM
- Hard Drive: 150 GB

801 - 1,000 connected beds:

- 2.x GHz processor or higher with a total of 24 cores
- Memory: 32 GB RAM
- Hard Drive: 150 GB

1,001 - 1,300 connected beds:

- 2.x GHz processor or higher with a total of 32 cores
- Memory: 64 GB RAM
- Hard Drive: 150 GB

Note

- For systems that have over 1,300 connected beds, add a core for every 50 additional beds.
- Two server environments are recommended for the **iBed** Wireless System: TEST and PROD
- The **iBed** Wireless System is supported in either physical or virtual environments.

Software:

Windows Server 2008 R2 / 2012 R2

- Add Roles
 - Web Server (IIS) (Installed)
 - Roles Services
 - Application development
 - ASP.NET (Installed)
 - ASP (Installed)
 - Management tools
 - IIS Management Console (Installed)
- Features
 - .NET Framework 4.5 (or higher) features (Installed)
 - WCF Services
 - HTTP Activation
- All current Microsoft High Priority Updates (Installed) and optional update for .NET Framework 4.5 (or higher)

Additional configuration or setup may be required depending on equipment and other variables. If you have difficulties during installation, setup, configuration, or while attempting to establish a connection between the **iBed** Server and Stryker wireless clients, contact Stryker Technical Support at 1-800-327-0770.

Device connection requirements

Note - You are required to use the DNS naming convention for each Stryker device if the devices can travel to multiple sub-nets.

- DHCP connections using a reserved IP address for each device via its MAC address
- Static connections using static IP address for each device via its MAC address
- DNS naming convention using each device host name that is hard-coded to the device (Host name example = SYK-82453f21f0c2 [SYK device 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

E-mail: medicaliBedWirelessSupport@stryker.com

Installation

Server configuration

Windows Server 2008

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

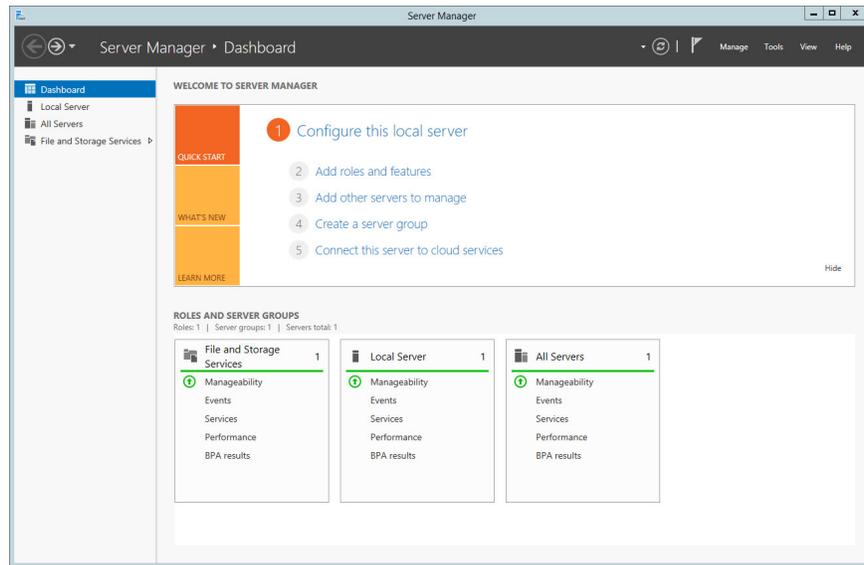


Figure 1 – Add Roles and Features

3. Click the **Next** button in the **Add Roles and Features Wizard** (Figure 2).

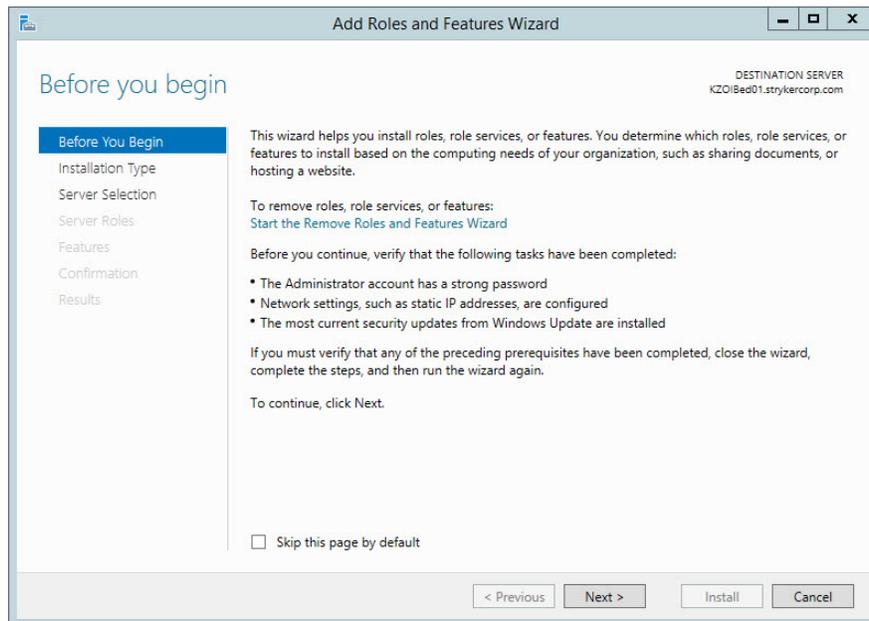


Figure 2 – Add Roles and Features Wizard

4. In the **Installation Type** step, select the **Role-based or feature-based installation** if not already selected and click **Next** (Figure 3).

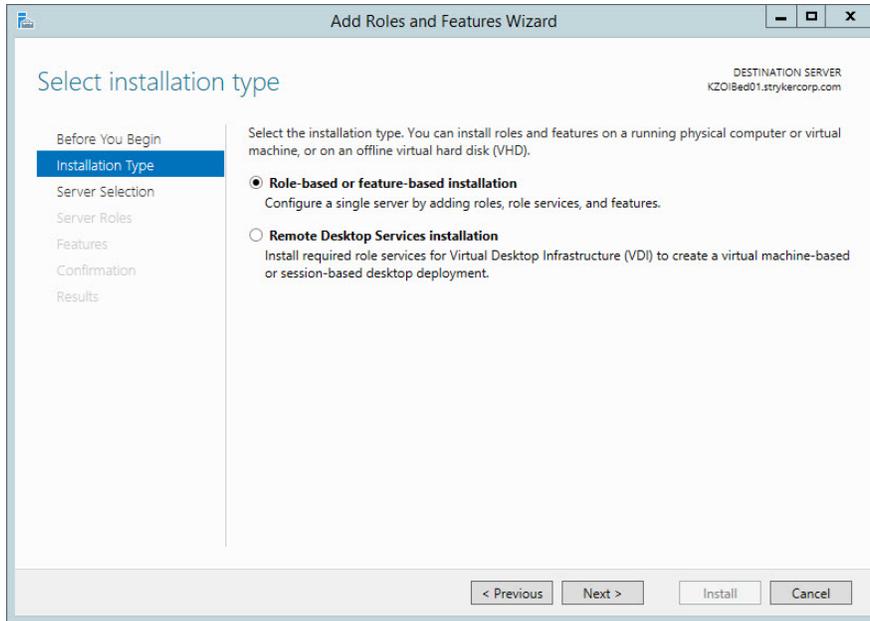


Figure 3 – Installation Type

5. In the **Server Selection** step, click **Select a server from the server pool** and make sure that the server is correct in the **Server Pool** box and click **Next** (Figure 4).

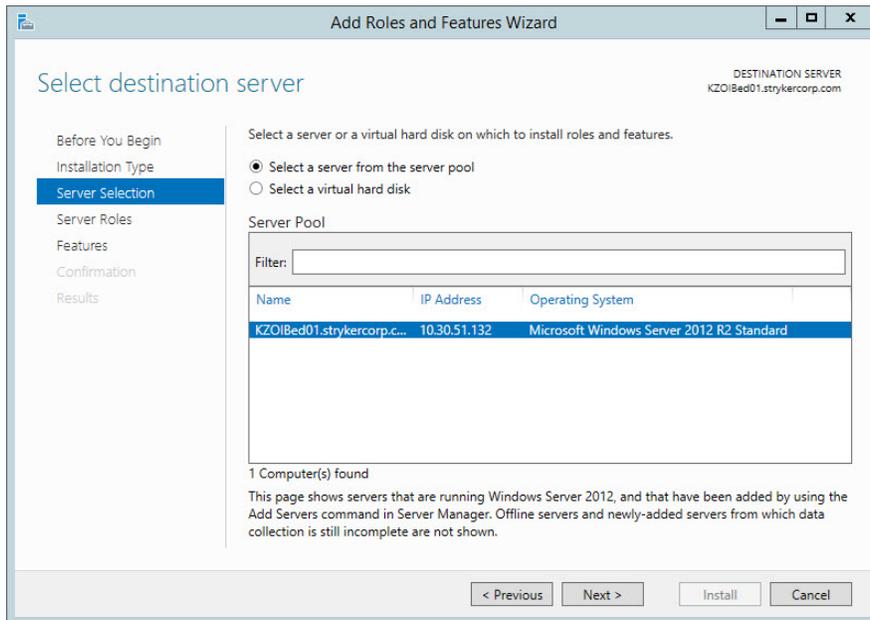


Figure 4 – Server Selection

6. In the **Server Roles** step, scroll through the options in the **Roles** box and select **Web Server (IIS)** (Figure 5).

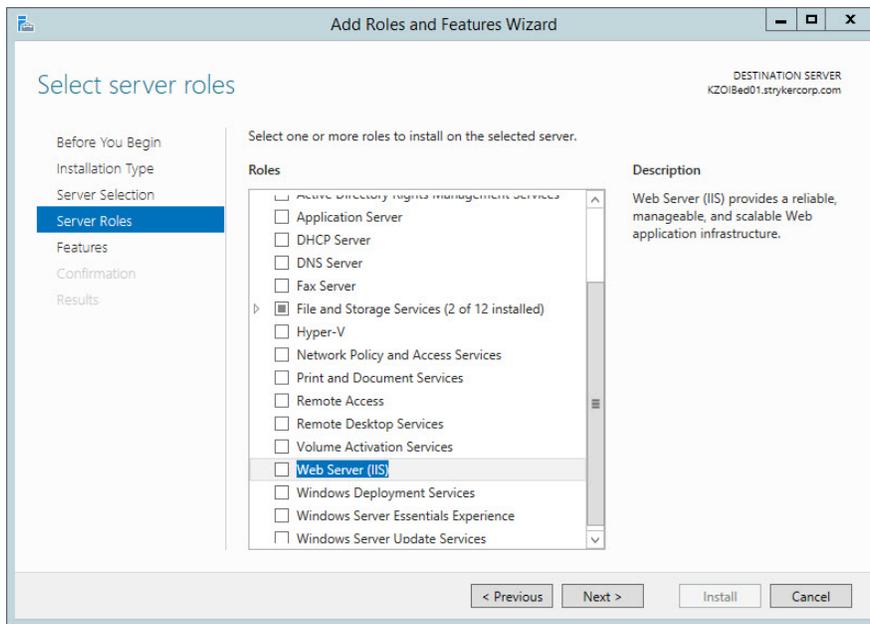


Figure 5 – Web Server (IIS)

7. In the pop-up, **Add features that are required for Web Server (IIS)**, click the **Add Features** button (Figure 6).

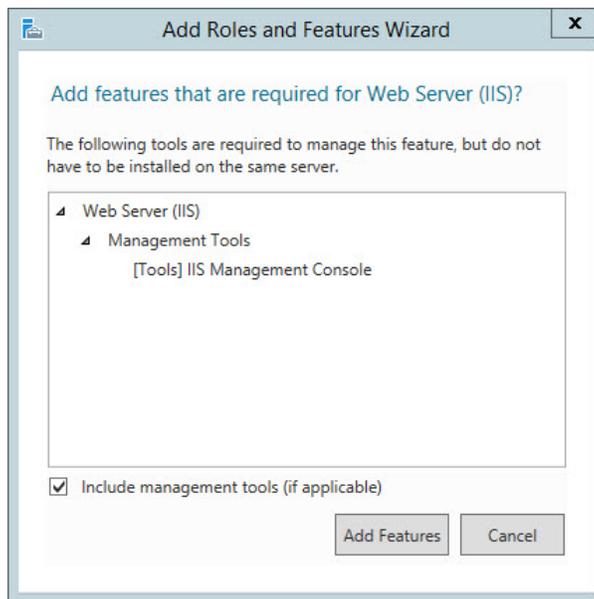


Figure 6 – Add features

8. In the **Server Roles** step, click the **Next** button (Figure 7).

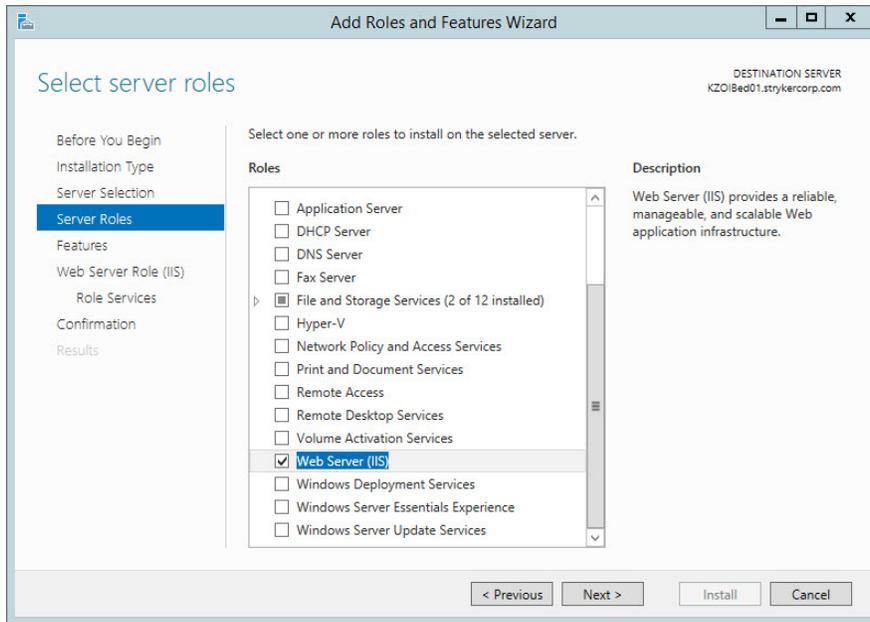


Figure 7 – Server confirmation

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

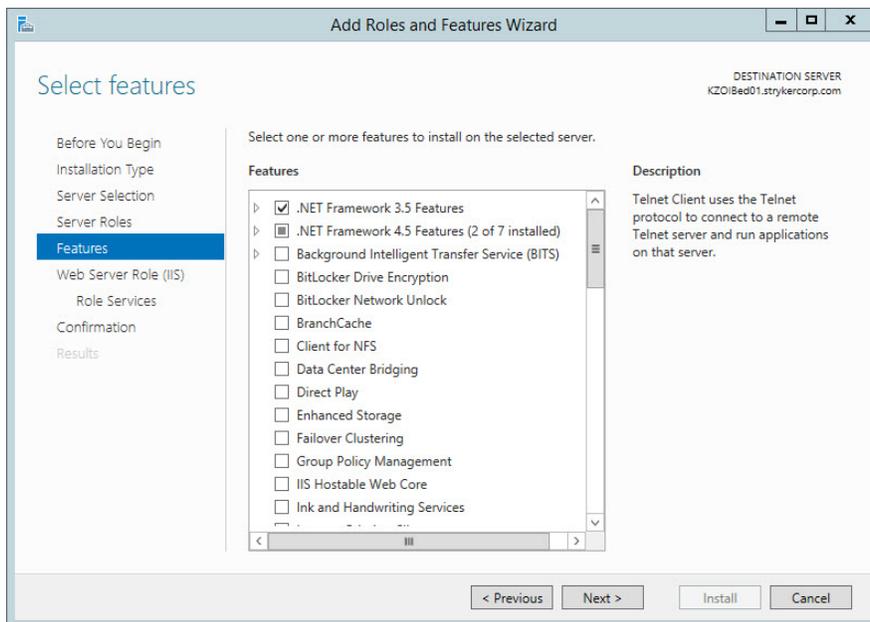


Figure 8 – Features selection

10. In the **Web Server Role (IIS)** step, click the **Next** button (Figure 9).

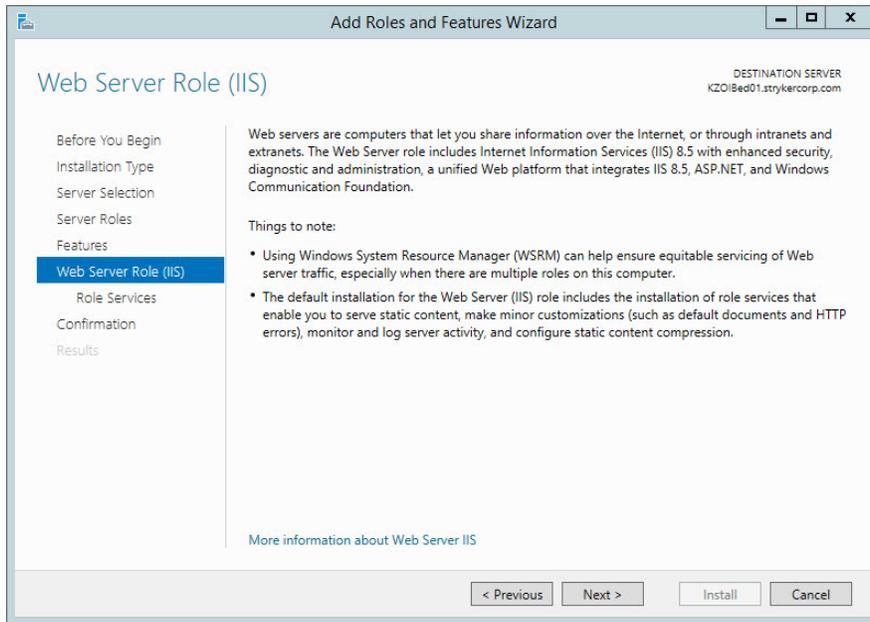


Figure 9 – Web Server Role (IIS)

11. In the **Role Services** step, click the **Next** button (Figure 10).

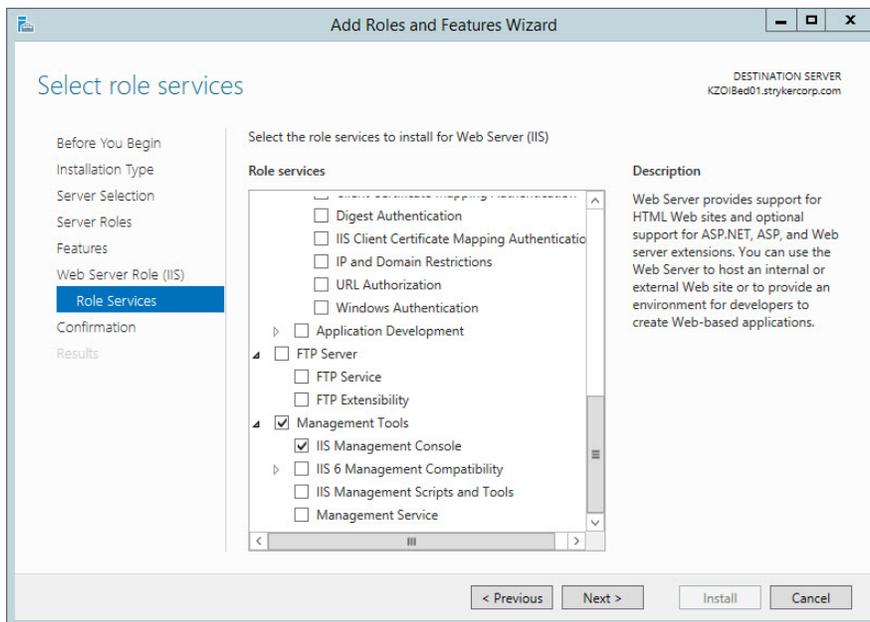


Figure 10 – Role Services

12. In the **Confirmation** step, click the **Install** button to start the installation of the role and features (Figure 11).

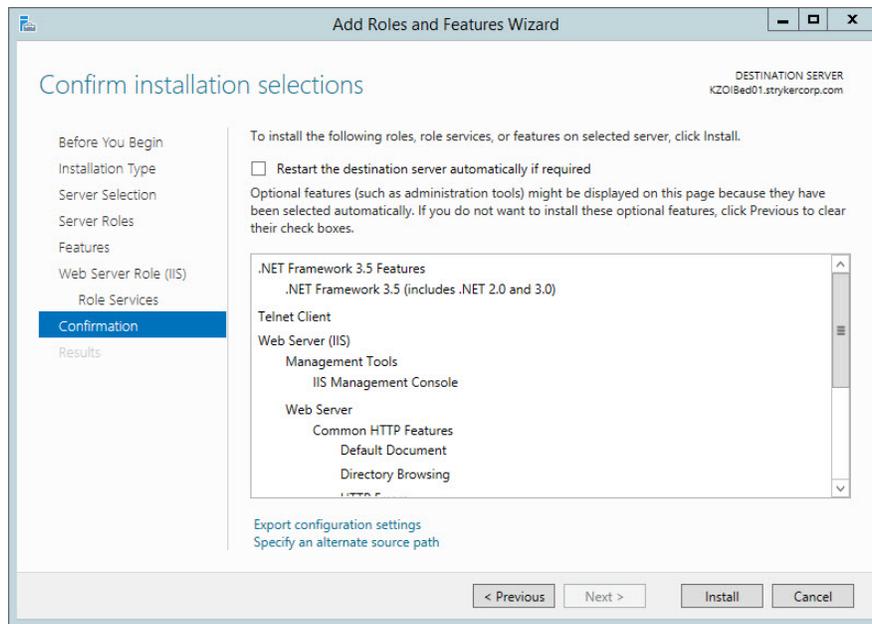


Figure 11 – Install confirmation

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

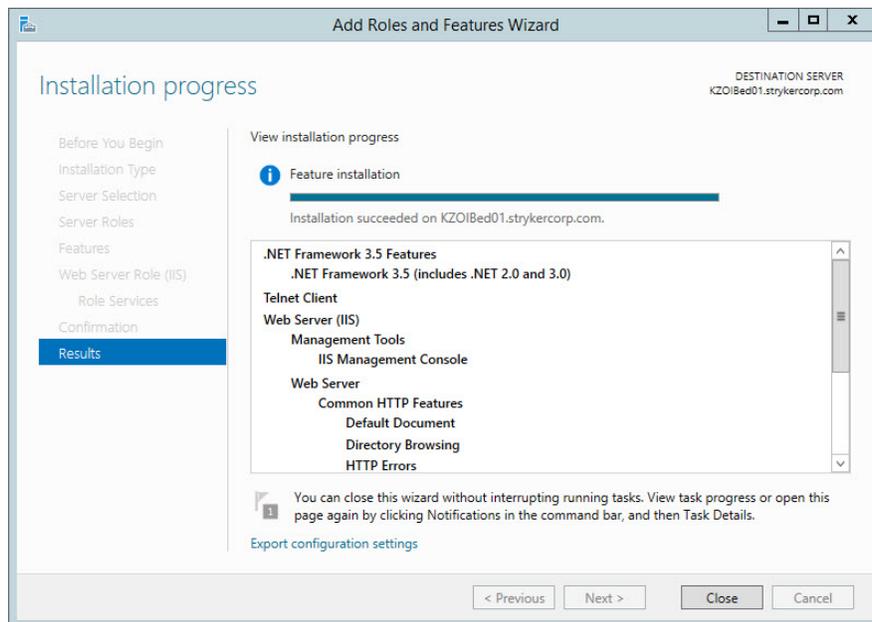


Figure 12 – Completed installation

14. Click on the **Add roles and features** link (Figure 13).

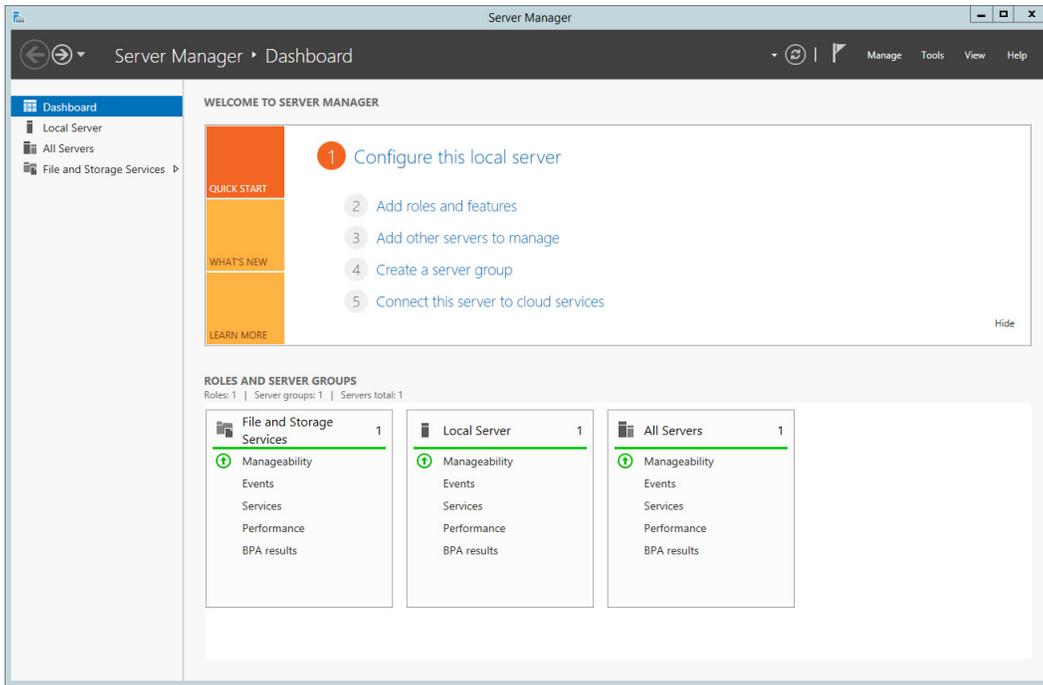


Figure 13 – Add roles and features

15. Click the **Next** button in the **Add Roles and Features Wizard** (Figure 14).

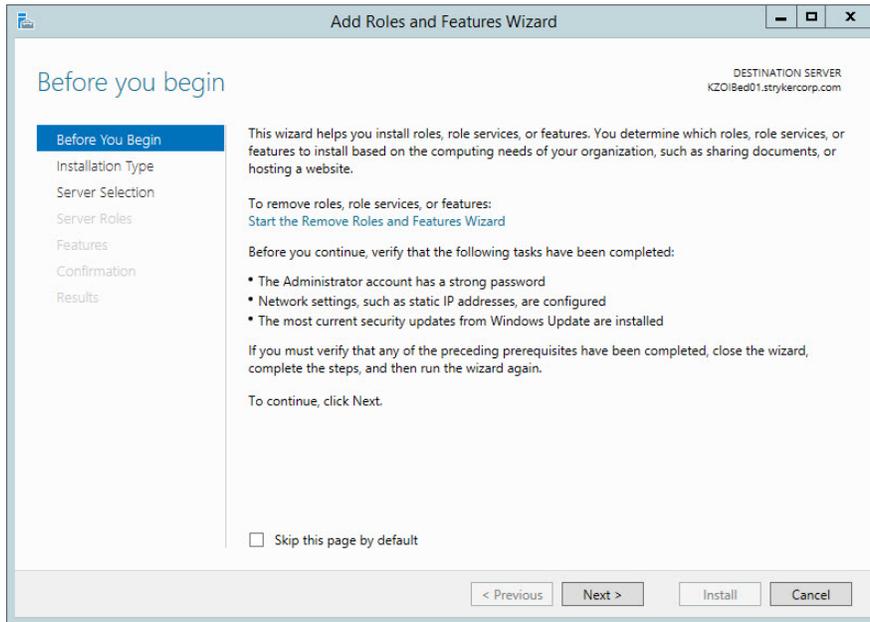


Figure 14 – Add Roles and Features Wizard

16. In the **Installation Type** step, select the **Role-based or feature-based installation** and click **Next** (Figure 15).

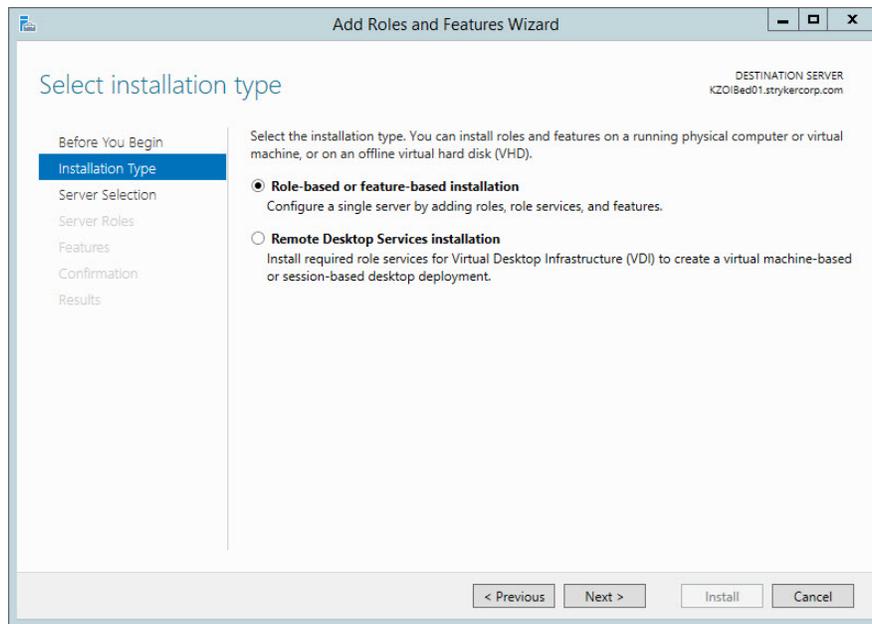


Figure 15 – Installation Type

17. In the **Server Selection** step, click **Select a server from the server pool** and verify that the server is correct in the **Server Pool** box and click **Next** (Figure 16).

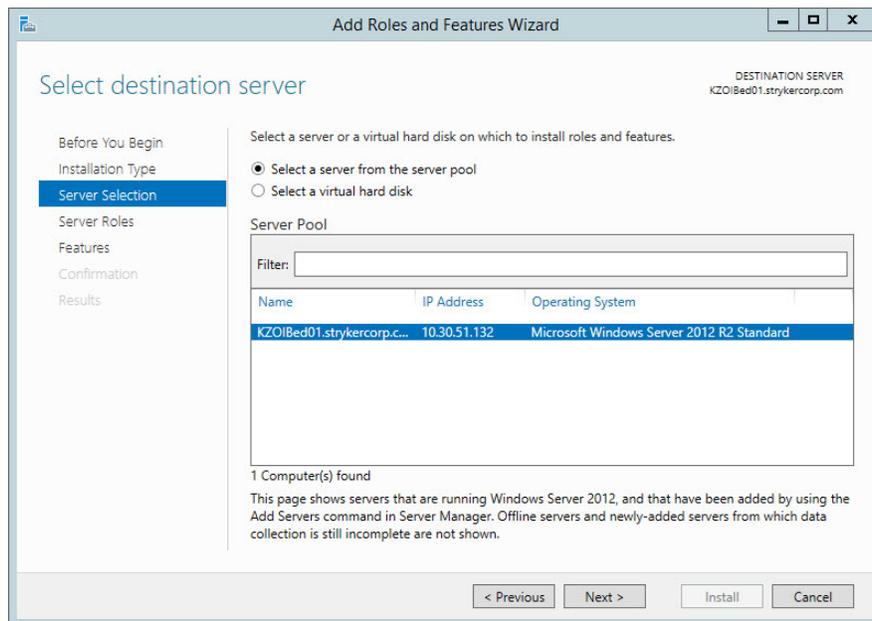


Figure 16 – Server selection

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

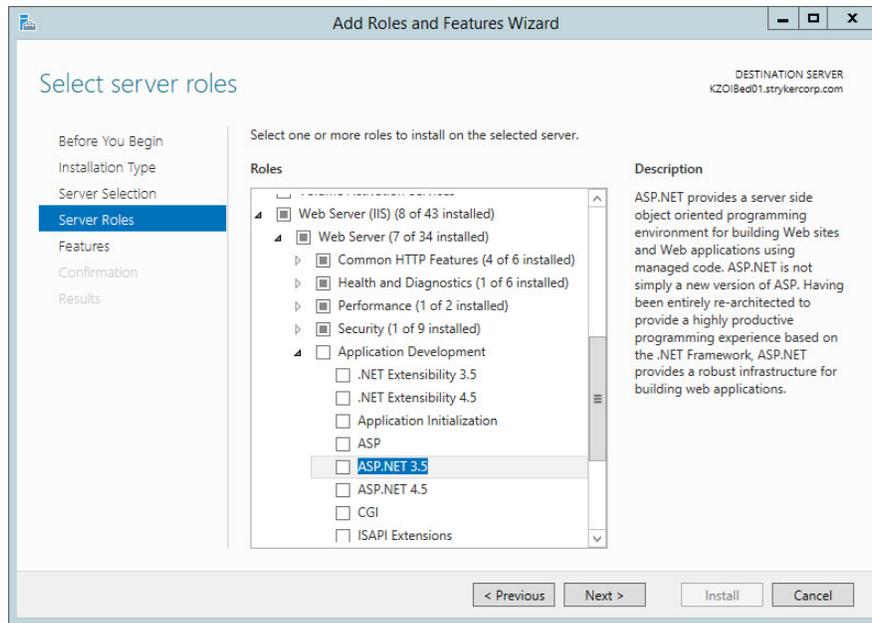


Figure 17 – Server Roles

19. In the pop-up window, click **Add Features** (Figure 18).

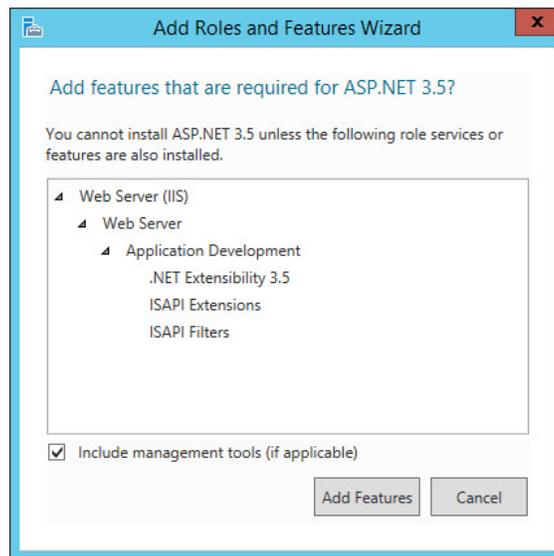


Figure 18 – Add Features

20. In the **Server Roles** step, select **ASP** and click **Next** (Figure 19).

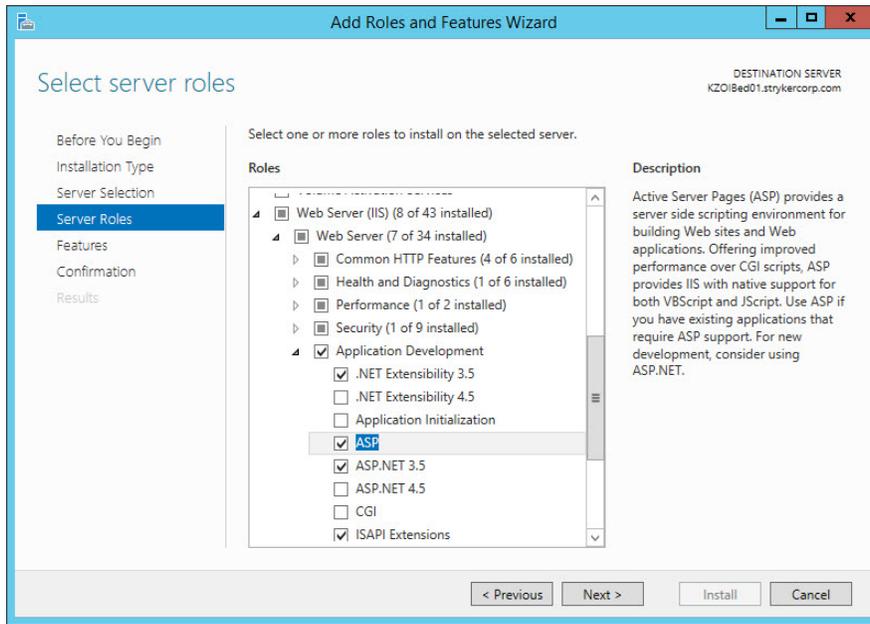


Figure 19 – ASP role

21. In the **Features** step, click **Next** (Figure 20).

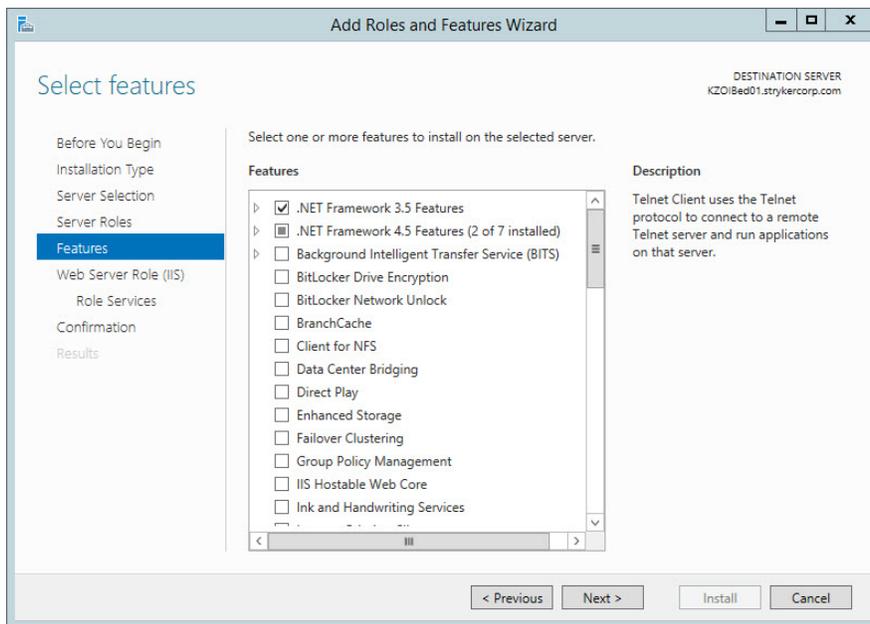


Figure 20 – Features selection

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

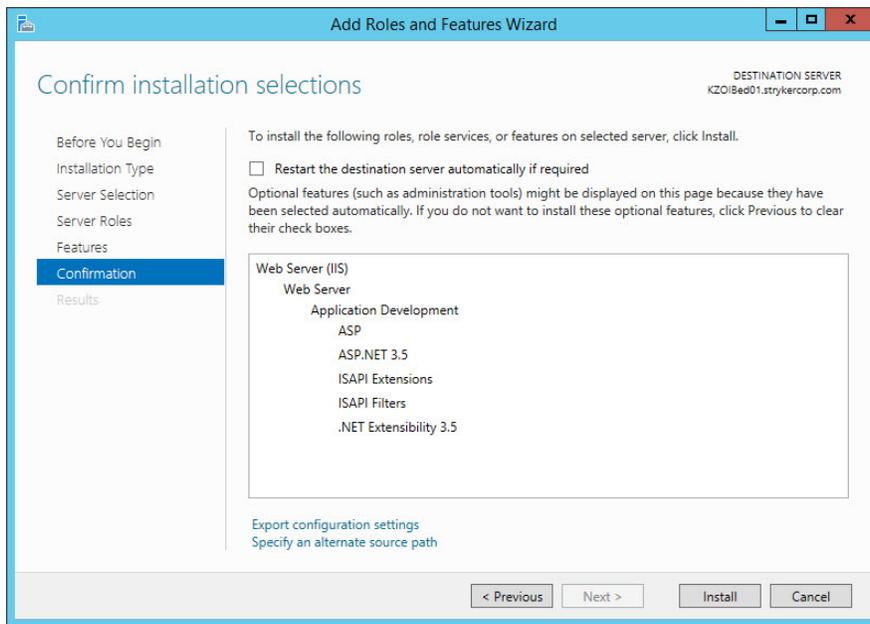


Figure 21 – Confirm installation

23. When installation is complete, click the **Close** button (Figure 22).

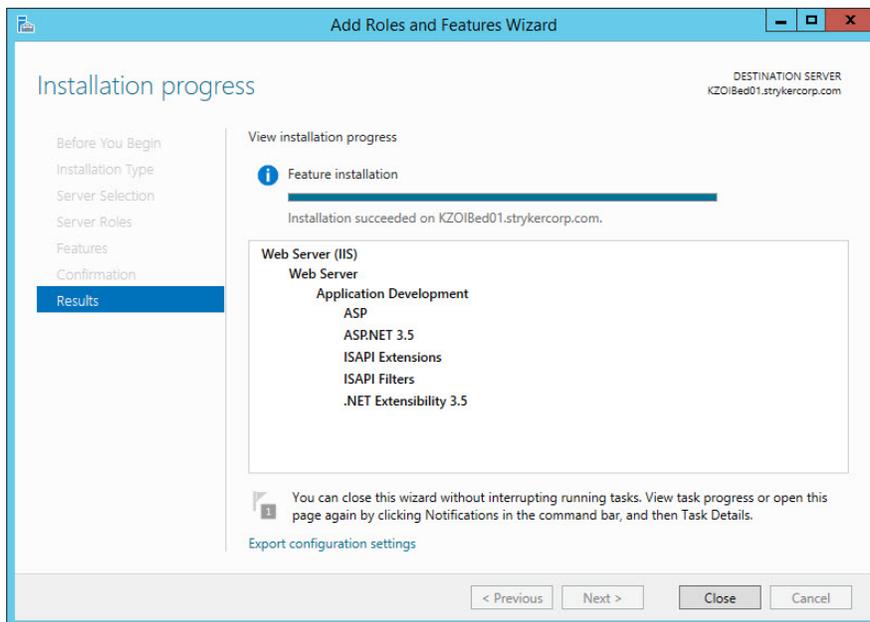


Figure 22 – Installation complete

24. Restart the server.

25. Run **Windows Update** to look for any important and optional updates and install them. Restart the server if required.

Windows Server 2012

1. In the **Server Manager** navigate to the Dashboard.

2. Click on the **Add roles and features** link (Figure 23).

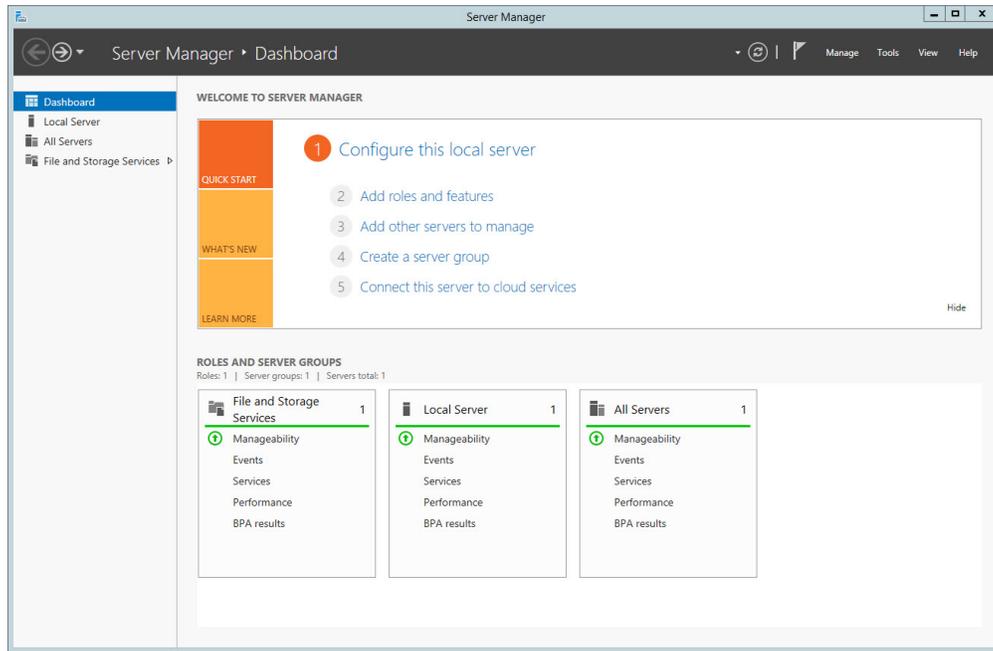


Figure 23 – Add roles and features

3. Click the **Next** button in the **Add Roles and Features Wizard** (Figure 24).

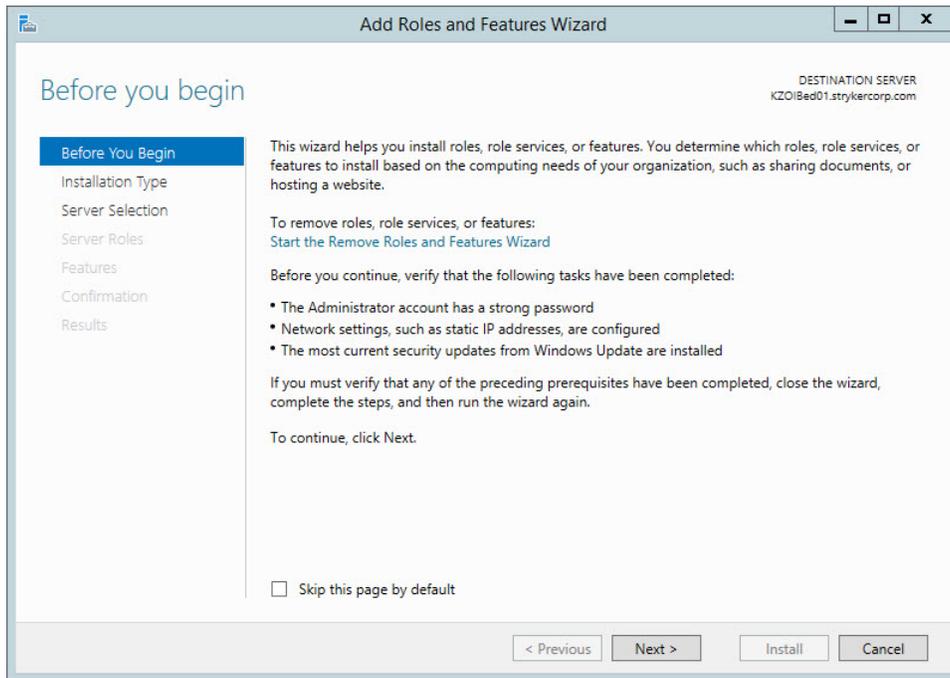


Figure 24 – Add Roles and Features Wizard

4. In the **Installation Type** step, select the **Role-based or feature-based installation** if not already selected and click **Next** (Figure 25).

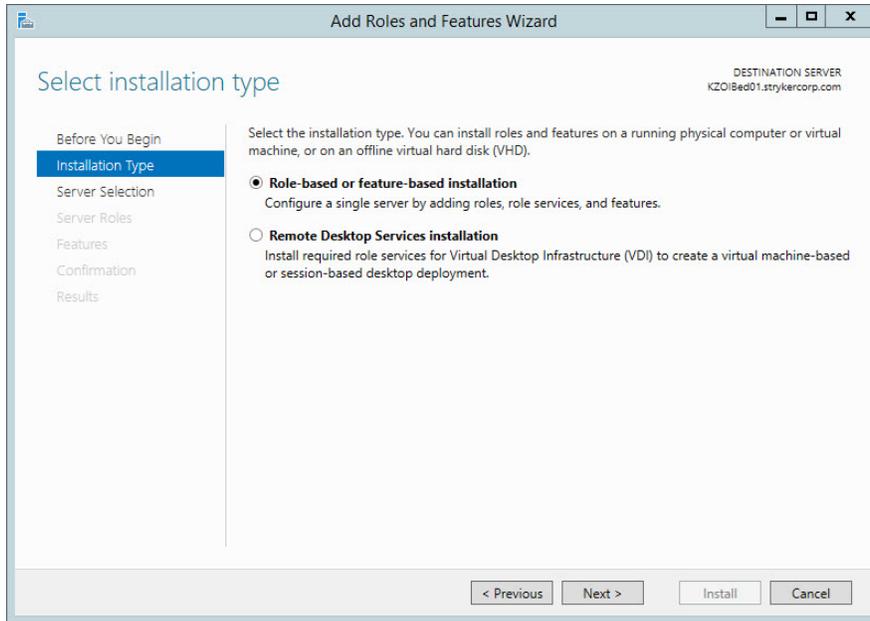


Figure 25 – Installation Type

5. In the **Server Selection** step, click **Select a server from the server pool** and make sure that the server is correct in the **Server Pool** box and click **Next** (Figure 26).

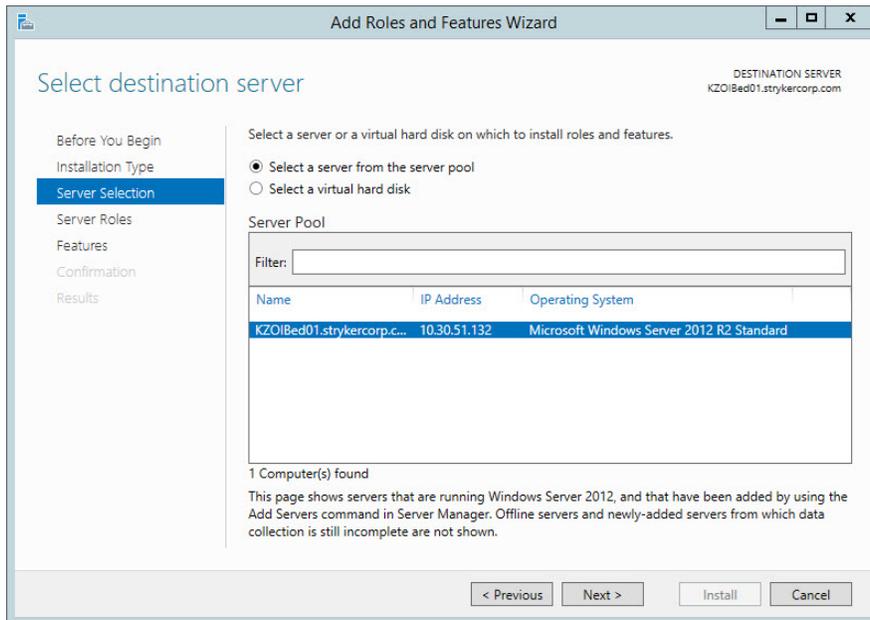


Figure 26 – Server Selection

6. In the **Server Roles** step, scroll through the options in the **Roles** box and select **Web Server (IIS)** (Figure 27).

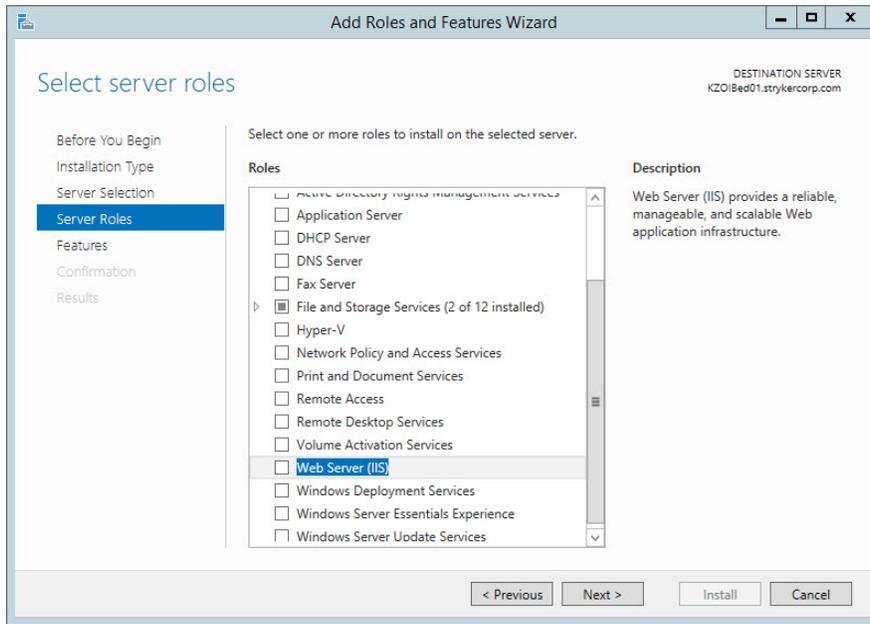


Figure 27 – Web Server (IIS)

7. In the pop-up, **Add features that are required for Web Server (IIS)**, click the **Add Features** button (Figure 28).

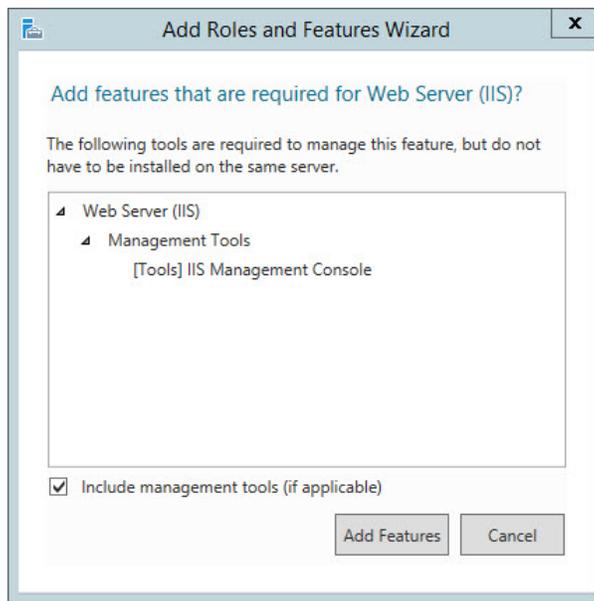


Figure 28 – Add Features

8. In the **Server Roles** step, click the **Next** button (Figure 29).

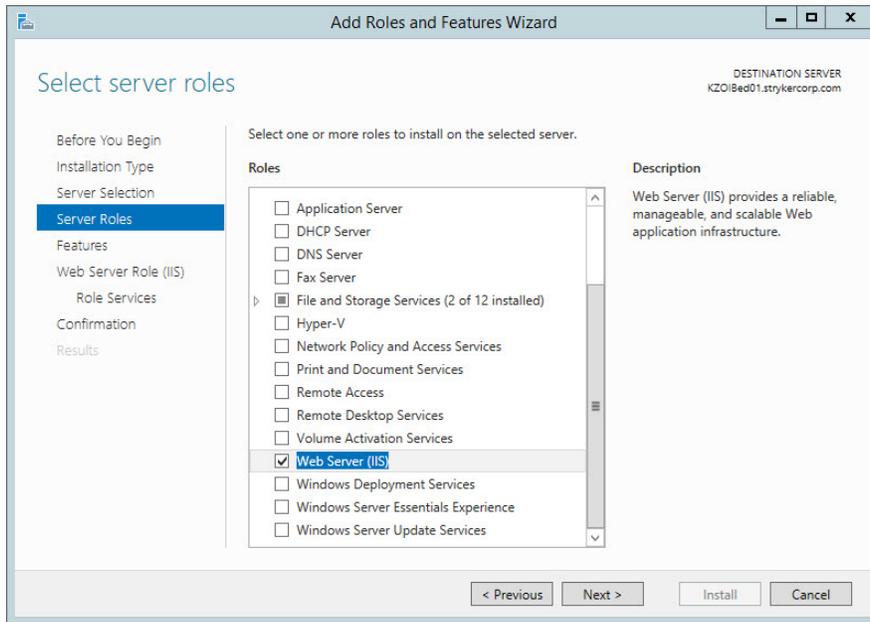


Figure 29 – Server confirmation

9. In the **Features** step, select **.NET Framework 3.5 Features** and **Telnet Client** in the **Features** box (Figure 30).

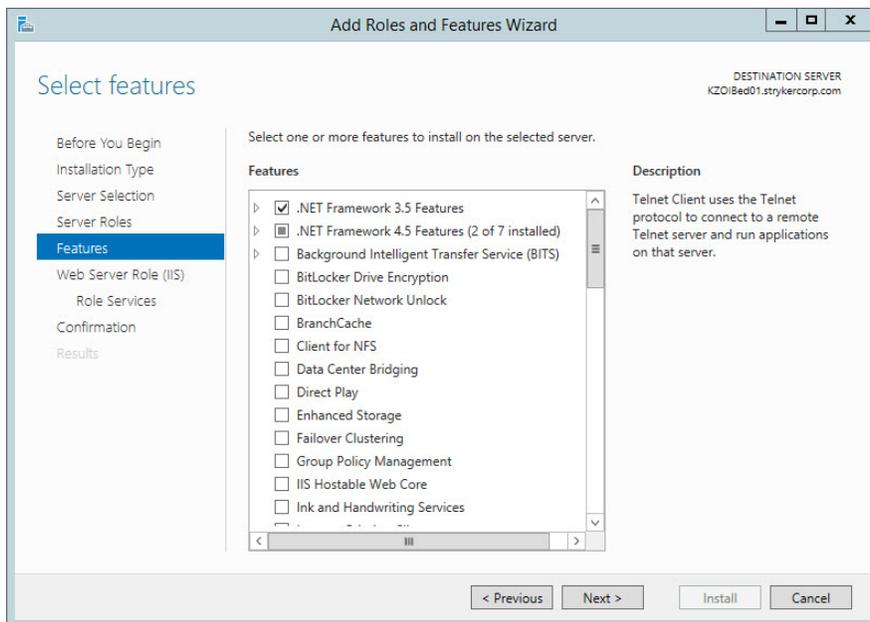


Figure 30 – Features selection

10. In the **Web Server Role (IIS)** step, click the **Next** button (Figure 31).

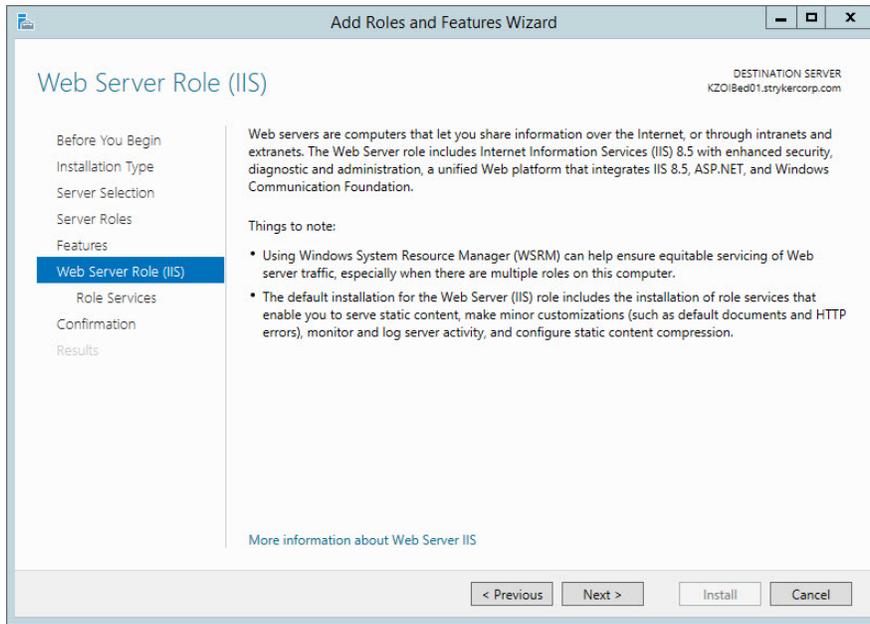


Figure 31 – Web Server Role (IIS)

11. In the **Role Services** step, click the **Next** button (Figure 32).

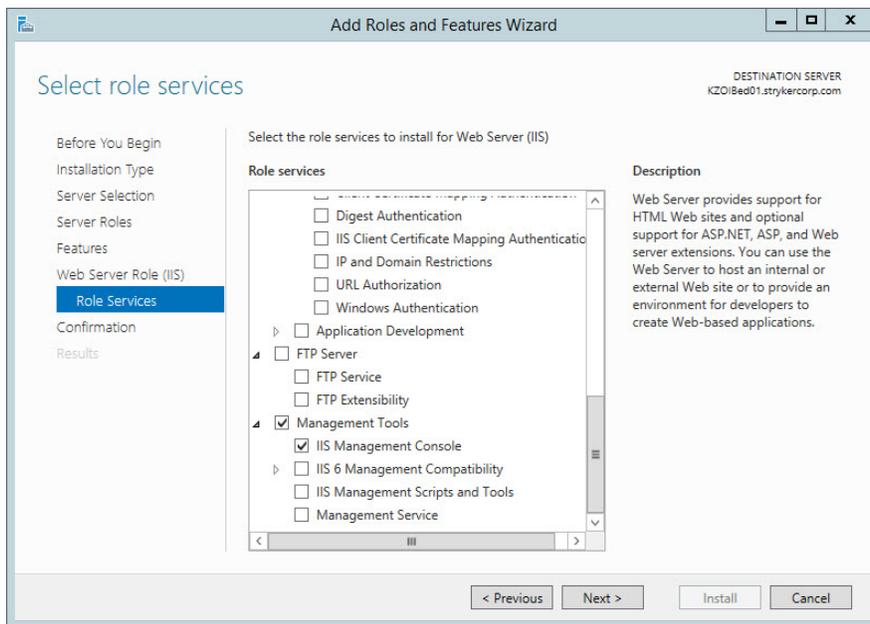


Figure 32 – Role Services

12. In the **Confirmation** step, click the **Install** button to start the installation of the role and features (Figure 33).

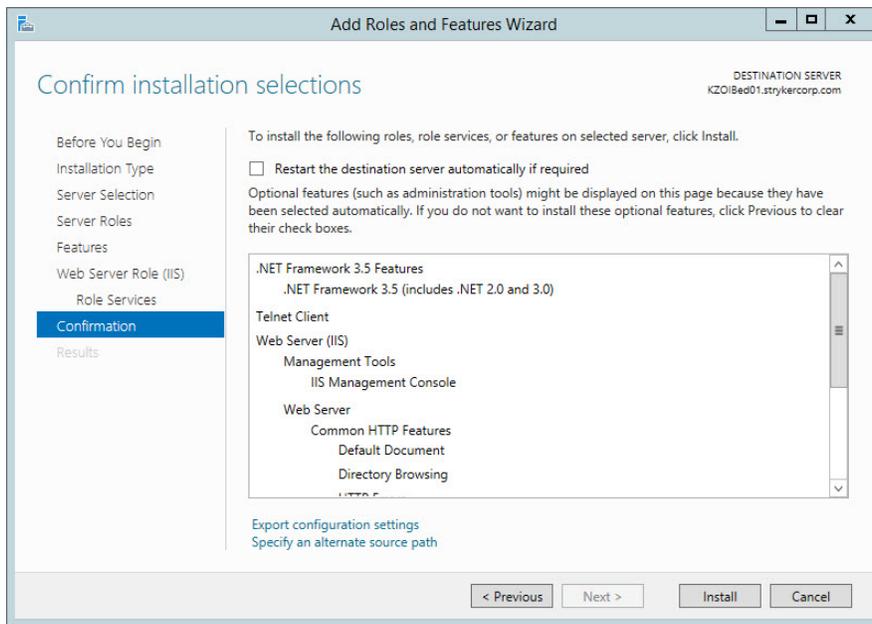


Figure 33 – Install confirmation

13. When the installation is finished, click the **Close** button (Figure 34).

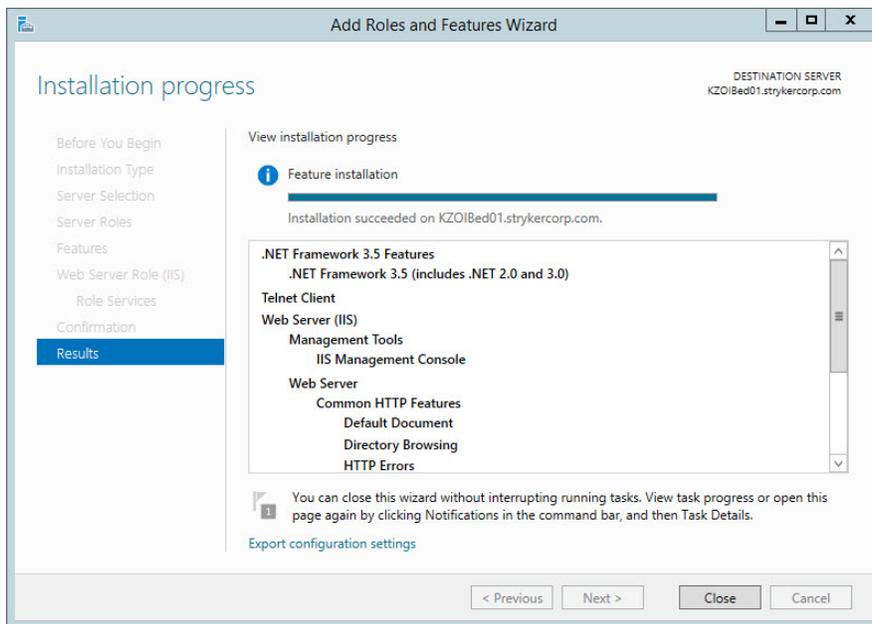


Figure 34 – Completed installation

14. Click on the **Add roles and features** link (Figure 35).

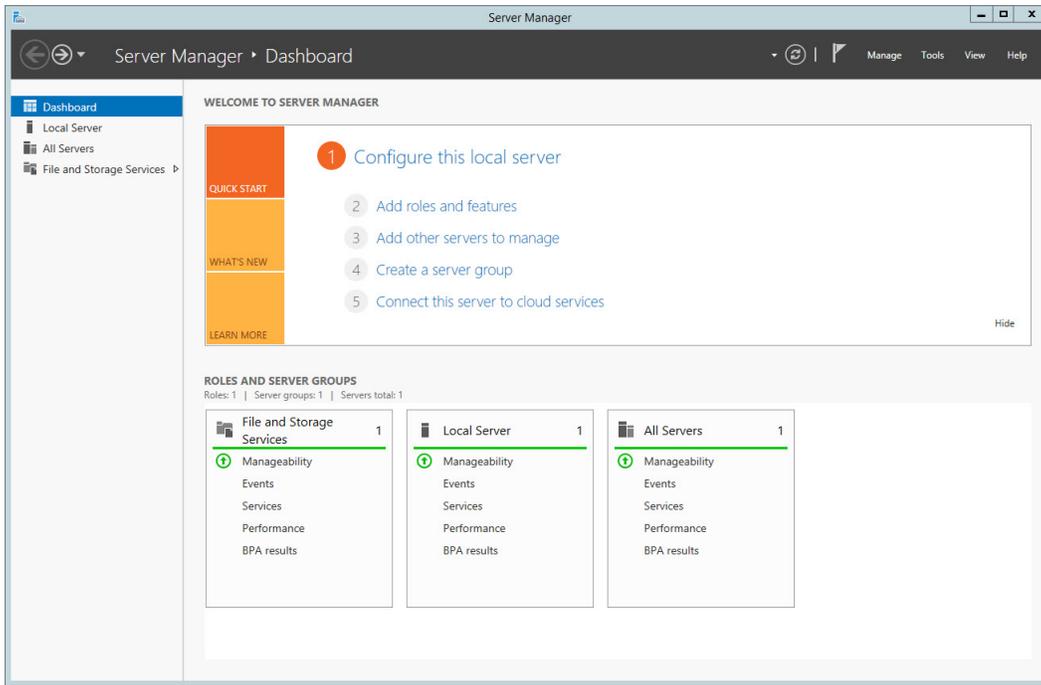


Figure 35 – Add roles and features

15. Click the **Next** button in the **Add Roles and Features Wizard** (Figure 36).

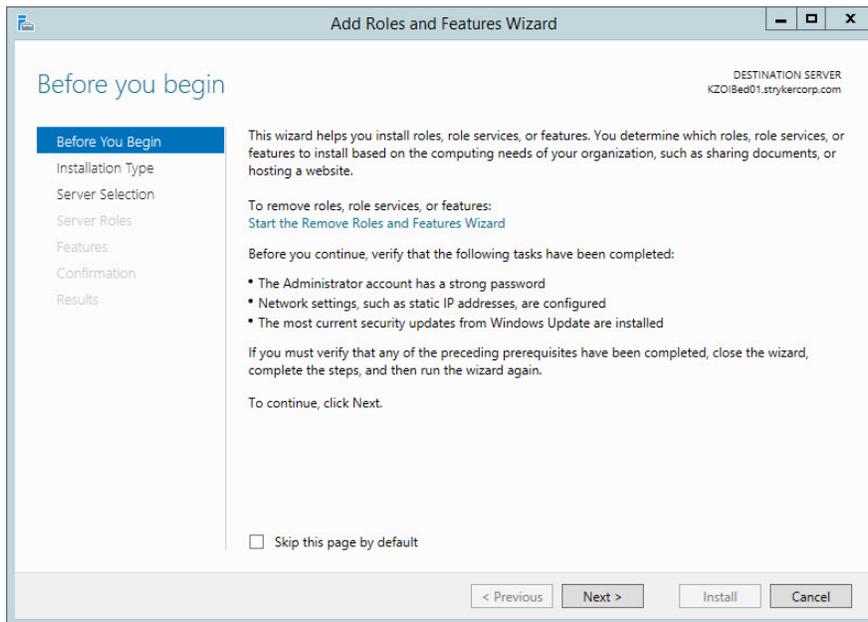


Figure 36 – Add Roles and Features Wizard

16. In the **Installation Type** step, select the **Role-based or feature-based installation** and click **Next** (Figure 37).

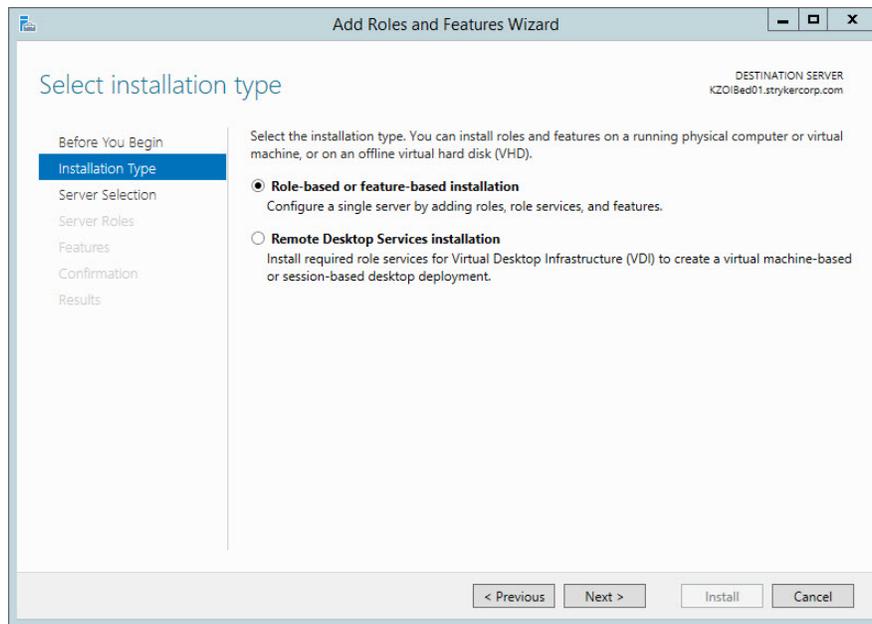


Figure 37 – Installation Type

17. In the **Server Selection** step, click **Select a server from the server pool** and verify that the server is correct in the **Server Pool** box and click **Next** (Figure 38).

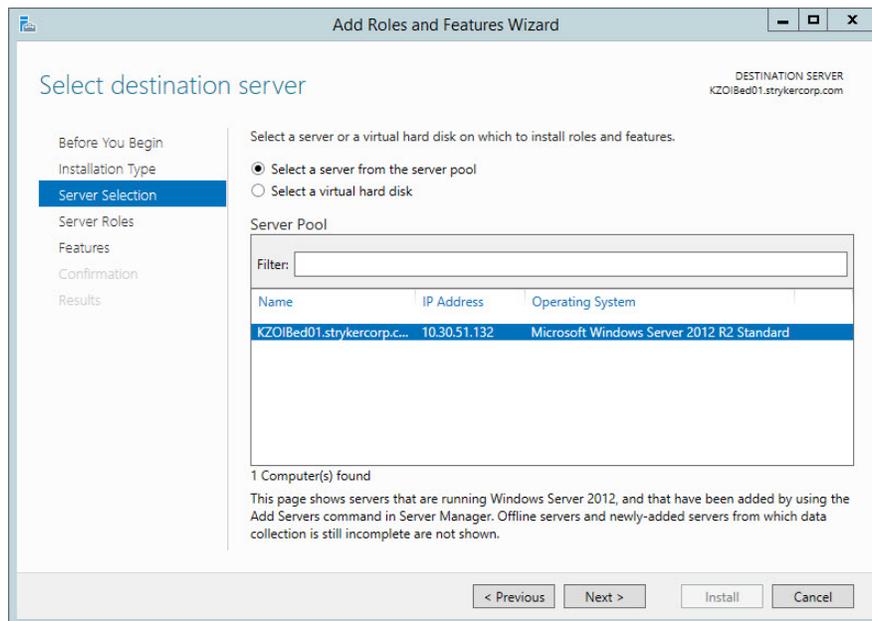


Figure 38 – Server Selection

18. In the **Server Roles** step in the **Roles** box, expand the **Web Server (IIS)** heading, **Web Server** heading, and then **Application Development**. Select **ASP.NET 3.5** and click **Next** (Figure 39).

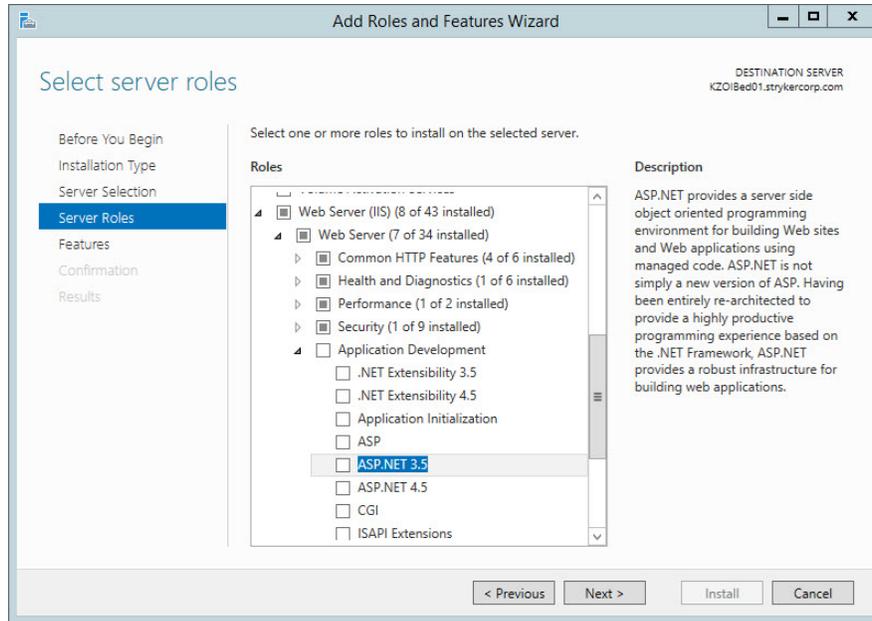


Figure 39 – Server Roles

19. In the pop-up window, click **Add Features** (Figure 40).

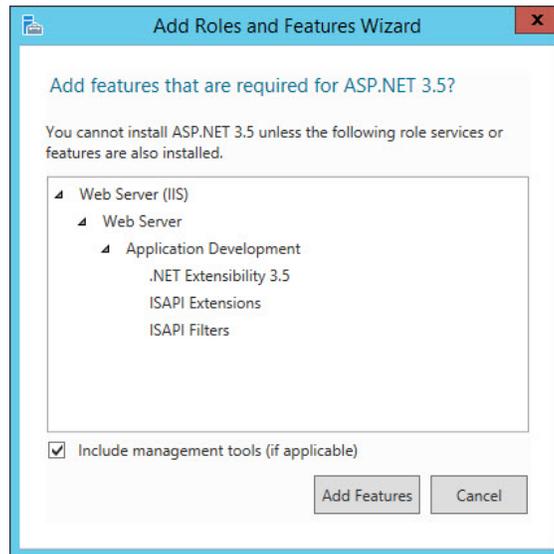


Figure 40 – Add Features

20. In the **Server Roles** step, select **ASP** and click **Next** (Figure 41).

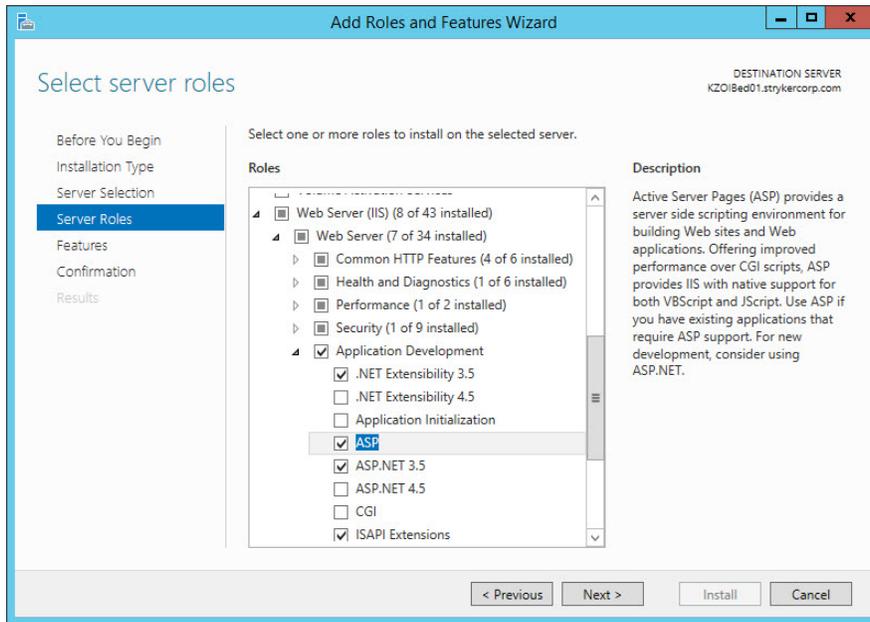


Figure 41 – ASP

21. In the **Features** step, click **Next** (Figure 42).

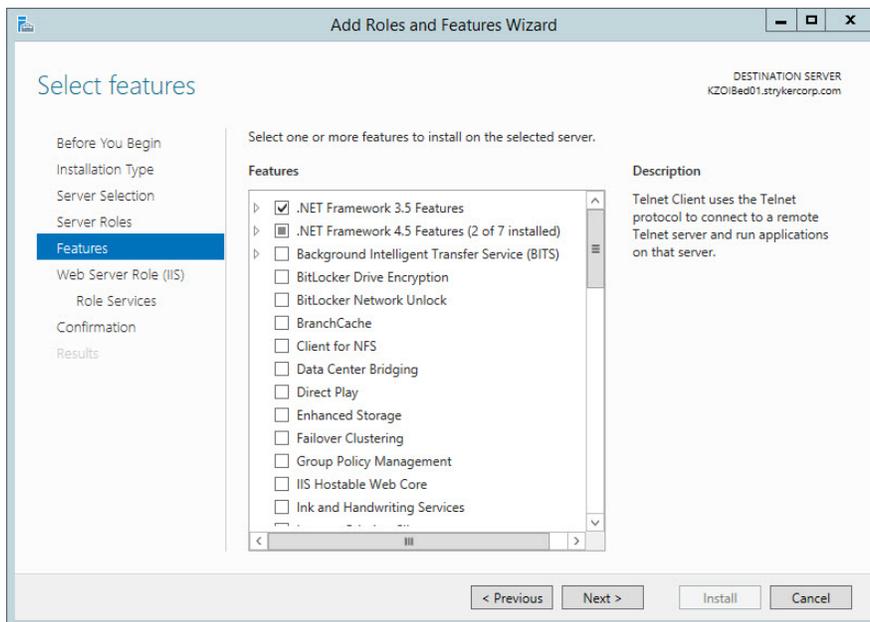


Figure 42 – Features selection

22. In the **Confirm installation selections** step, click **Install** (Figure 43).

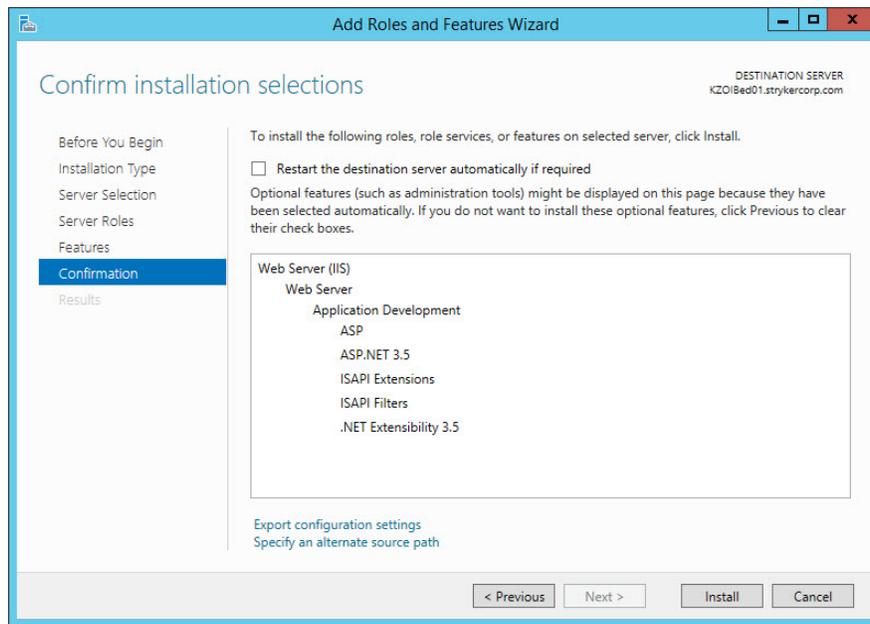


Figure 43 – Confirm installation

23. When installation is complete, click the **Close** button (Figure 44).

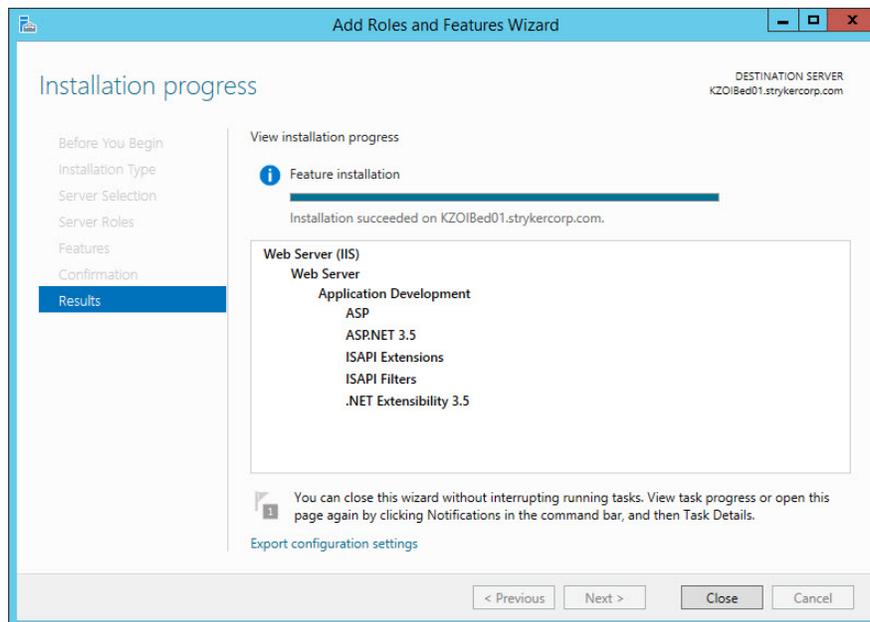


Figure 44 – Installation complete

24. Restart the server.

25. Run **Windows Update** to look for any important and optional updates and install them. Restart the server if required.

iBed Server application

CAUTION - Before proceeding with this installation, make sure that a previous version of the **iBed** Server application is not currently installed on the target system. If a previous version was installed, uninstall the software. If you attempt to install the application on a system where a previous version was installed, the installer behavior may be unpredictable.

1. Begin the **iBed** Server Application installation by right clicking the **5212-502-001 Server Application Setup.exe** file and select **Run as Administrator**.
2. If Microsoft SQL Server 2012 Express is not already installed, the **InstallShield Wizard requirements** window will open. Click the **Install** button (Figure 45).

Note - If Microsoft SQL Server 2012 Express is already installed, go to step 11.

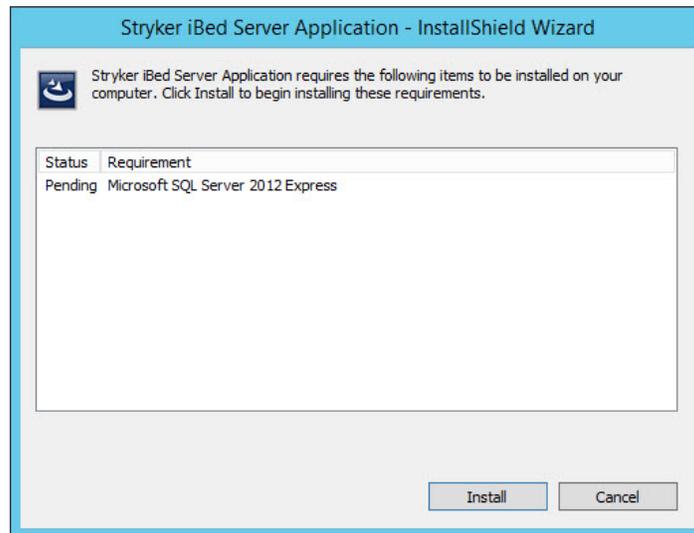


Figure 45 – Microsoft SQL service

3. Click the **Yes** button in the confirmation pop-up to start the SQL Server installation (Figure 46).

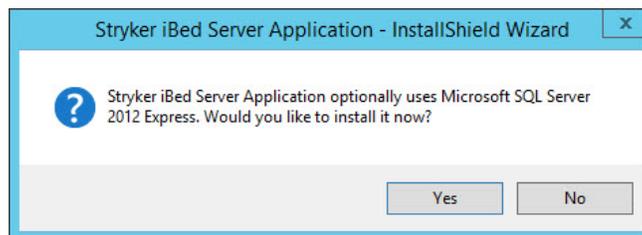


Figure 46 – SQL confirmation

4. Select **I accept the license terms** box and then click the **Next** button (Figure 47).

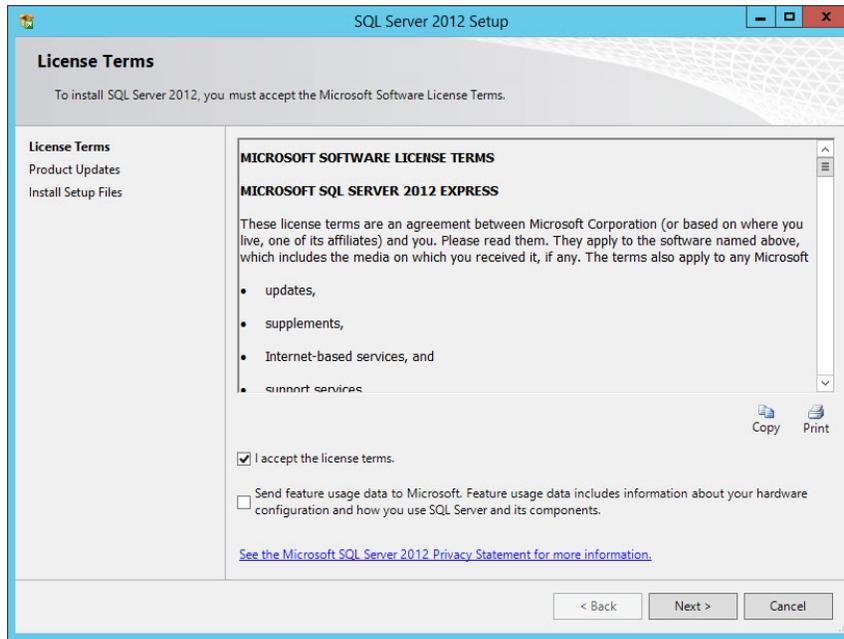


Figure 47 – SQL license

5. In the **Feature Selection** step, 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 and then click **Next** (Figure 48).

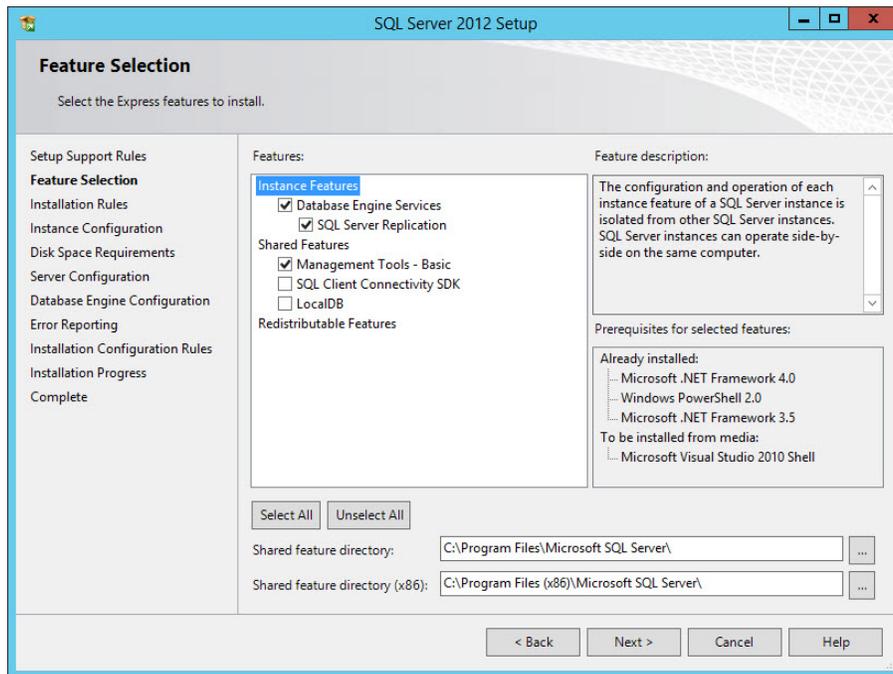


Figure 48 – SQL features

6. In the **Instance Configuration** step, click **Next** (Figure 49).

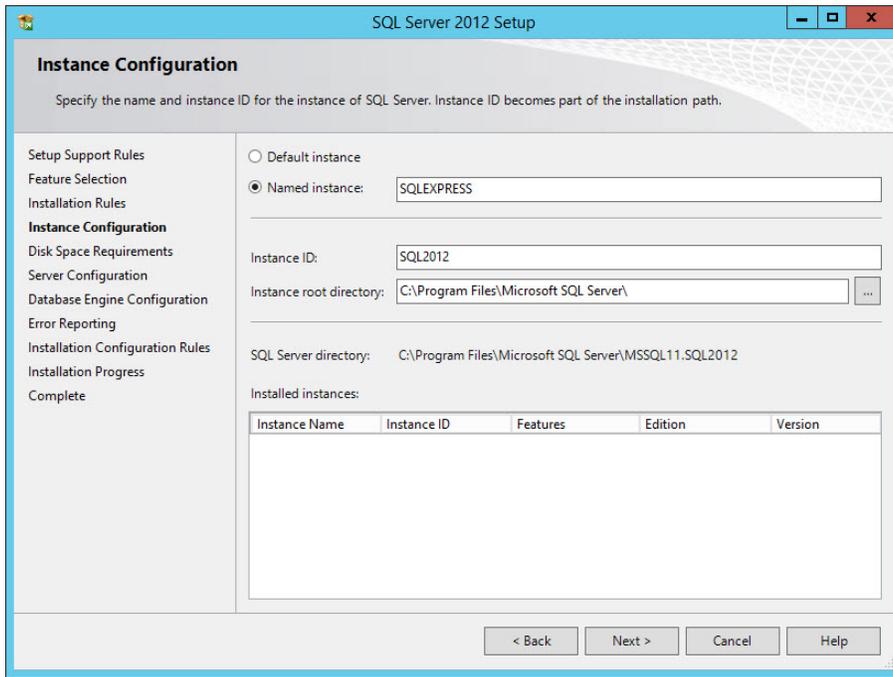


Figure 49 – Instance Configuration

7. In the **Server Configuration** step, click **Next** (Figure 50).

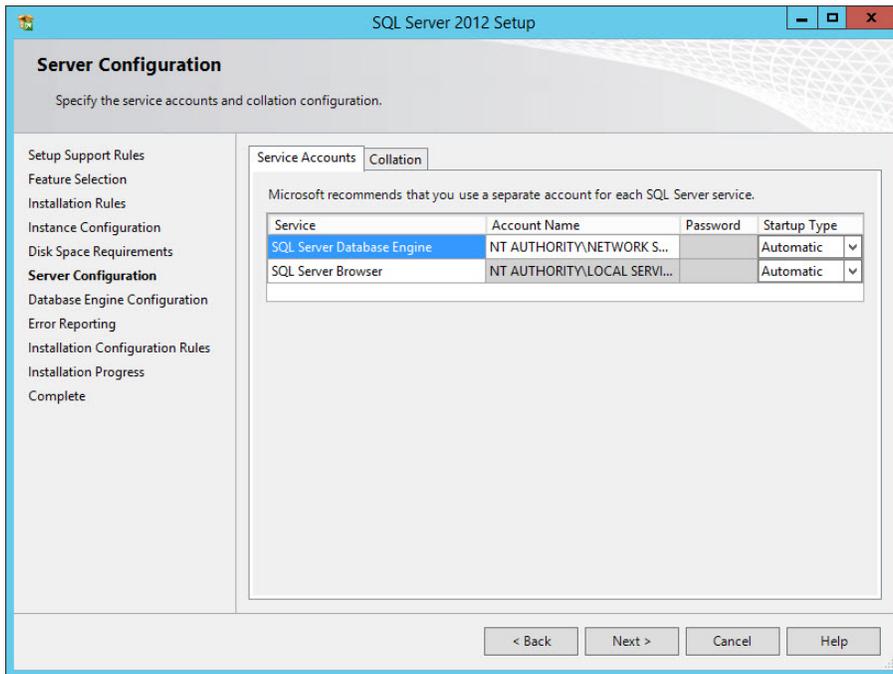


Figure 50 – Server Configuration

8. In the **Database Engine Configuration** step, click **Next** (Figure 51).

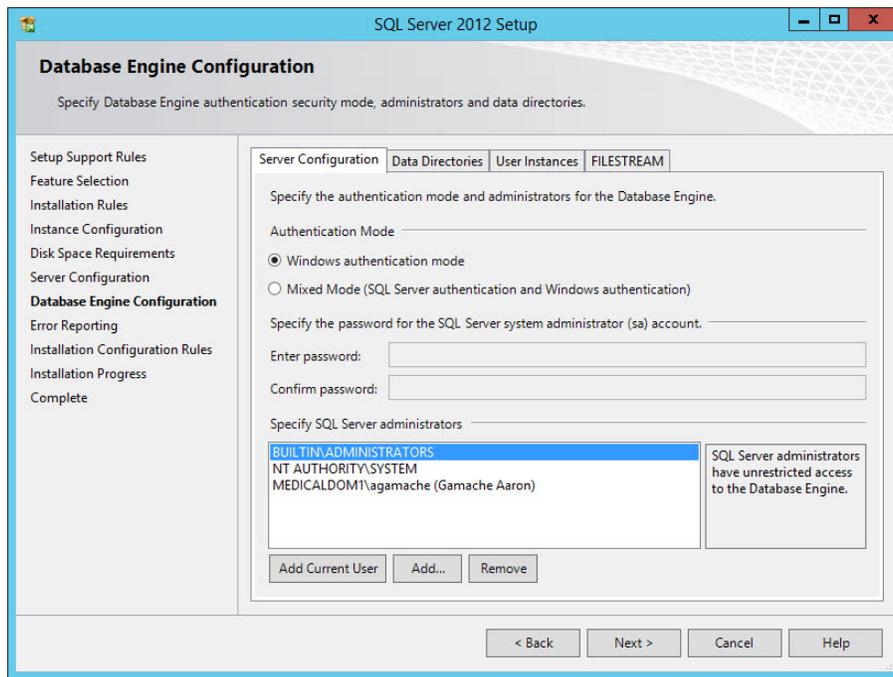


Figure 51 – Database Engine Configuration

9. In the **Error Reporting** step, click **Next** to start the SQL Server 2012 install process (Figure 52).

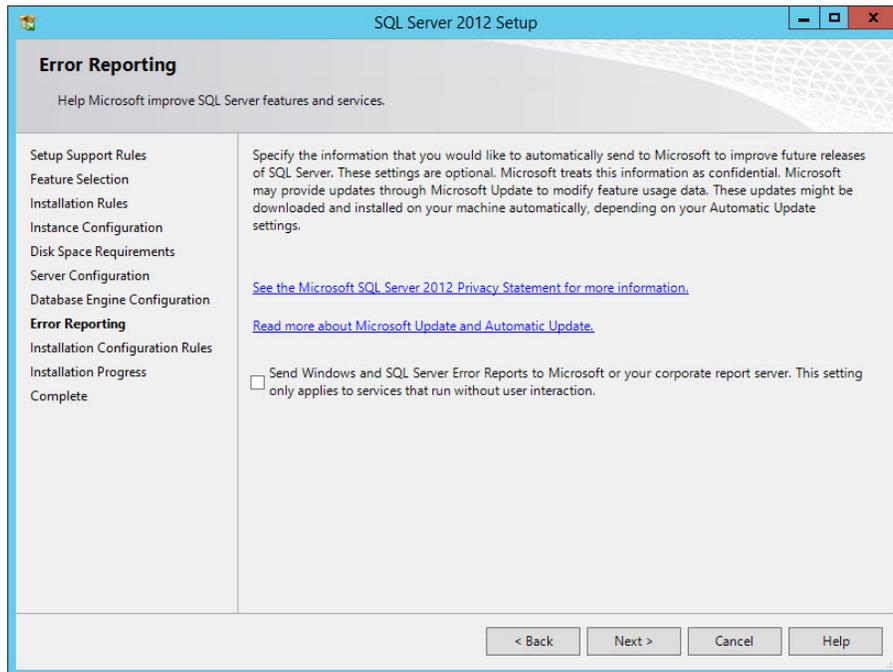


Figure 52 – Error Reporting

10. When installation is complete, click **Close** in the **Complete** window which will start the **iBed Server Application** installation (Figure 53).

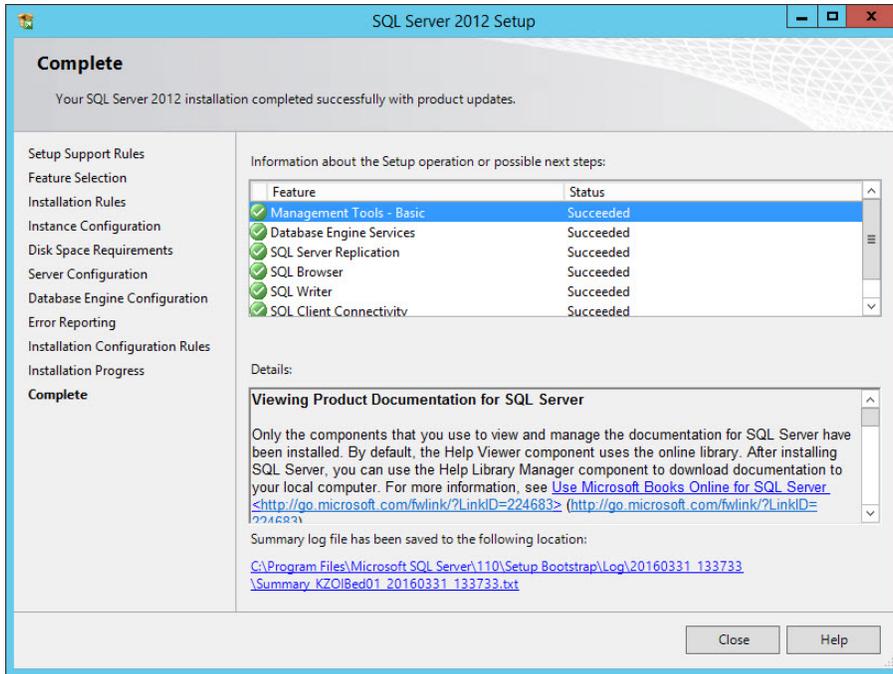


Figure 53 – SQL server install complete

11. In the **InstallShield Wizard** window, click **Next** (Figure 54).

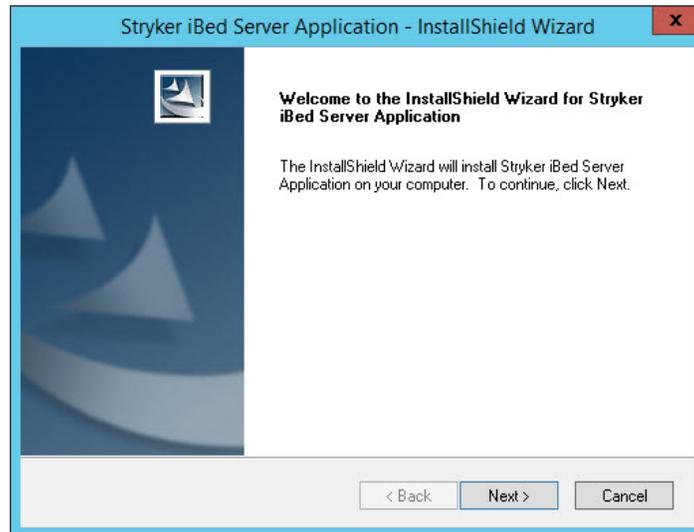


Figure 54 – InstallShield Wizard

12. In the **iBed Server Application** system configuration window, enter the sites information and click **Next** (Figure 55).

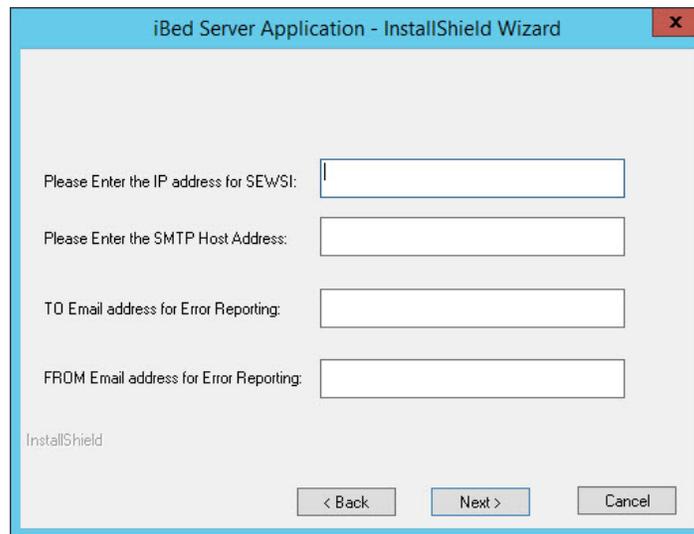


Figure 55 – Application configuration

13. The **Choose Destination Location** screen will appear (Figure 56).

- a. If using the default location, click **Next**.
- b. If using a different location, click **Change** and then **Next** to confirm.

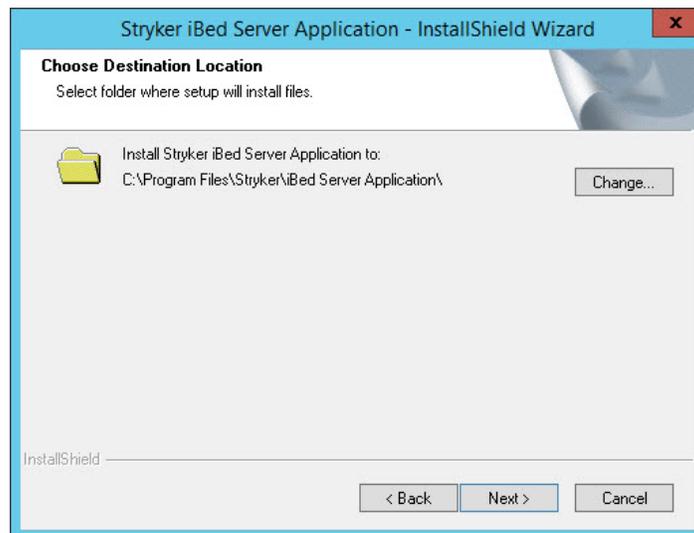


Figure 56 – Choose Destination Location

14. The **Select Program Folder** screen will appear (Figure 57).

- a. If using the default folder, click **Next**.
- b. If using a different folder, create a different folder name and click **Next**.

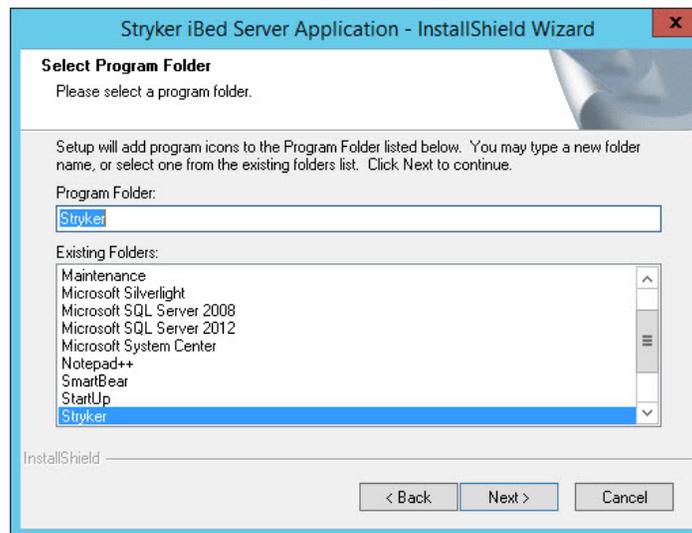


Figure 57 – Select Program Folder

15. Click **Install** to begin the installation (Figure 58).

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

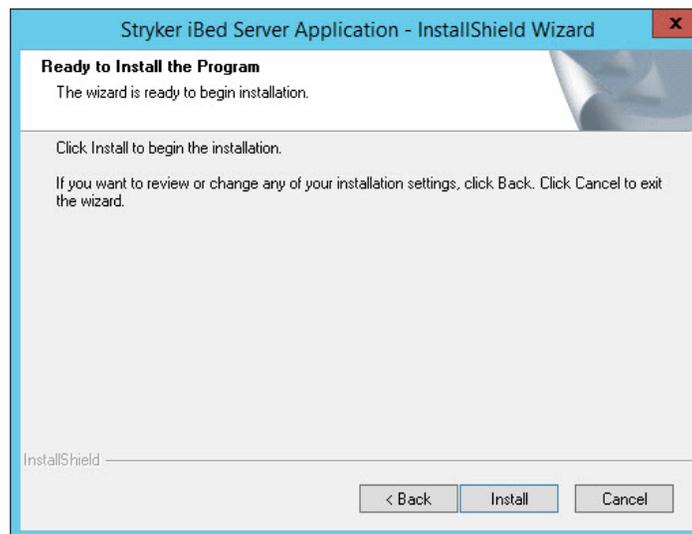


Figure 58 – Install iBed Server

16. Click **Finish** to exit the **InstallShield Wizard** (Figure 59).



Figure 59 – Finish

iBed Wireless Configuration Tool

CAUTION - Before proceeding with this installation, make sure that a previous version of the **iBed** Wireless configuration tool application is not currently installed on the target system. If a previous version was installed, uninstall the software. If you attempt to install the application on a system where a previous version was installed, the installer behavior may be unpredictable.

1. Run the **iBed** Wireless Configuration Tool by double-clicking the **5212-503-001 iBed Wireless configuration tool Setup.exe** file on the source location.
2. In the **InstallShield Wizard** screen, click **Next** (Figure 60).

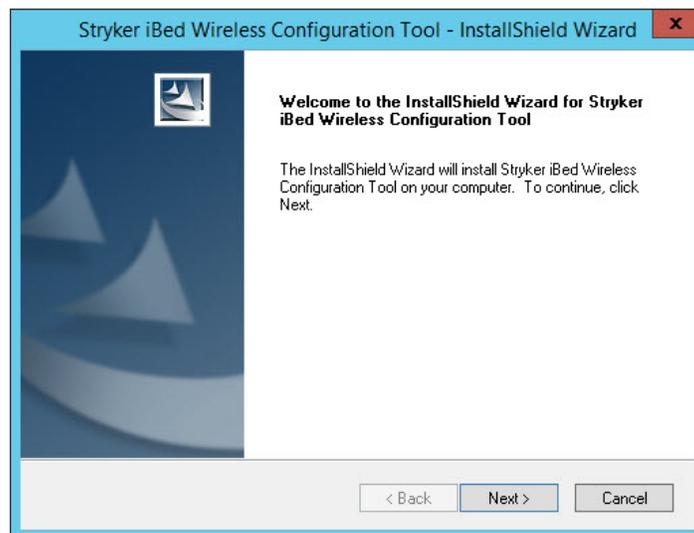


Figure 60 – InstallShield Wizard

3. The **Choose Destination Location** screen will appear (Figure 61).
 - a. If using the default location, click **Next**.
 - b. If using a different location, click **Change** and then **Next** to confirm.

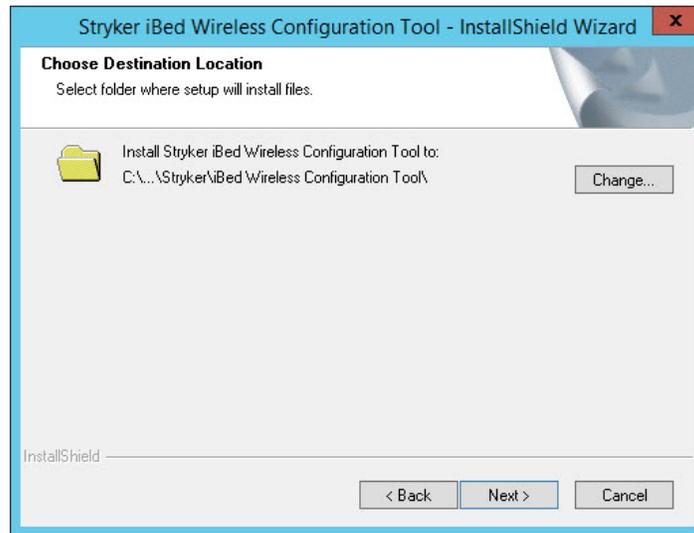


Figure 61 – Choose Destination Location

4. Click **Finish** to exit the **InstallShield Wizard** (Figure 62).

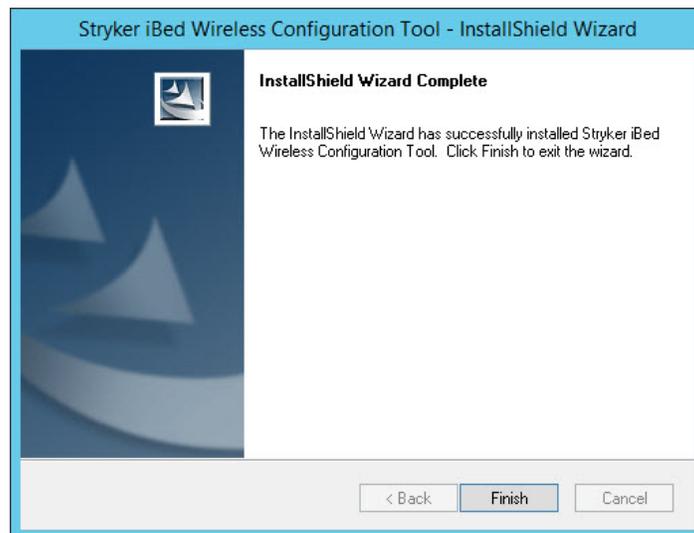


Figure 62 – Finish

Editing Windows configuration

1. Browse to the machine.config file.
 - C:\Windows\Microsoft.NET\Framework\v2.0.50727\CONFIG\ machine.config (32 bit)
 - C:\Windows\Microsoft.NET\Framework64\v2.0.50727\CONFIG\ machine.config (64 bit)
2. To edit the previous file to increase the thread count for the .NET Framework, replace `<processModel autoConfig="false"` with `<processModel autoConfig="false" maxWorkerThreads="1000" maxIoThreads="1000" minWorkerThreads="50" minIoThreads="50"/>`.

3. Browse to: **C:\Program Files (x86)\Stryker\iBed Server Application\HB\SEWSI.HeartBeatWindowsService.exe.config**.
4. To increase the available ports (TCP connections):
 - a. Execute using a command prompt: `netsh int ipv4 set dynamicport tcp start=1025 num=64510`

Configuring the Internet Information Services (IIS) Manager for iBed Server

1. Go to the **Internet Information Services (IIS) Manager**.
 - a. Expand the **Connections** tree and **Sites** folder.
 - b. In the **Connections** pane, click **Application Pools** (Figure 63).
 - c. In the **Application Pools** pane, select **DefaultAppPool** (Figure 63).
 - d. In the **Actions** pane, click **Recycling** (Figure 63).

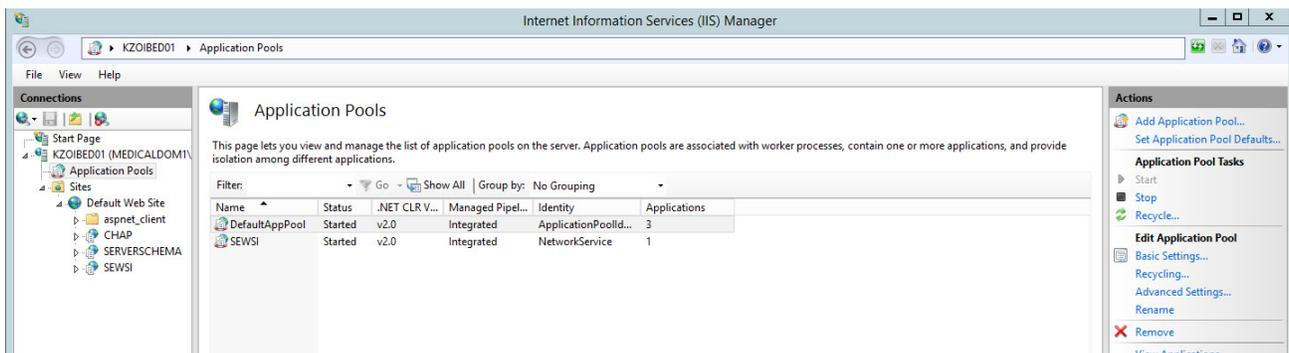


Figure 63 – Disabling recycling conditions

- e. Disable Recycling by clearing any selected boxes (Figure 64).
- f. Click **Next**, and then click **Finish**.

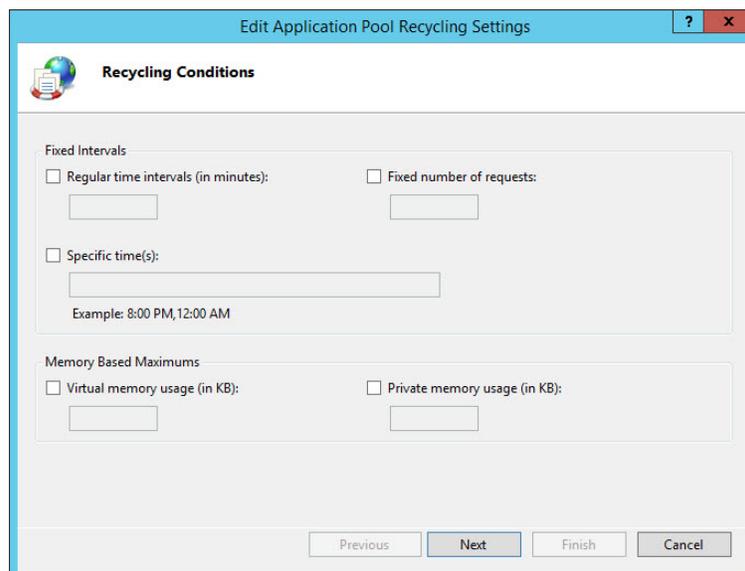


Figure 64 – Recycling Conditions

2. Make sure that all Application Pools (Default and SEWSI) are using v2.0 .NET Framework (Figure 63).
3. In the **Connections** pane, click **Default Web Site**.

4. In the **Actions** pane under **Manage Website / Configure**, click **Limits** (Figure 65).

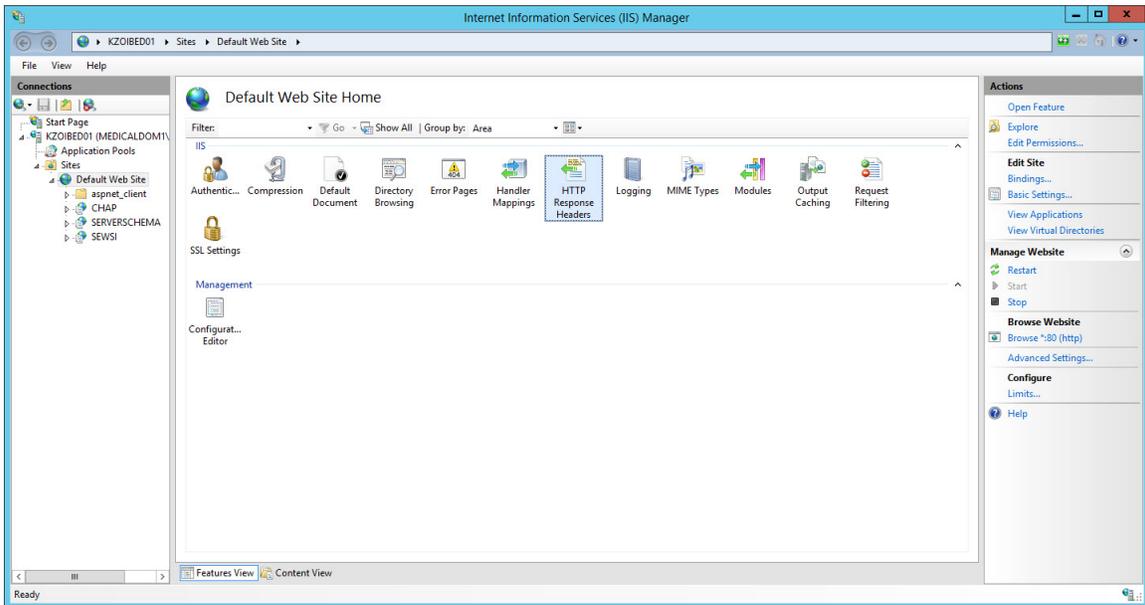


Figure 65 – Limits

5. In the **Connection Limits** area, change the **Connection time-out (in seconds)**: to 8, and then click **OK** (Figure 66).

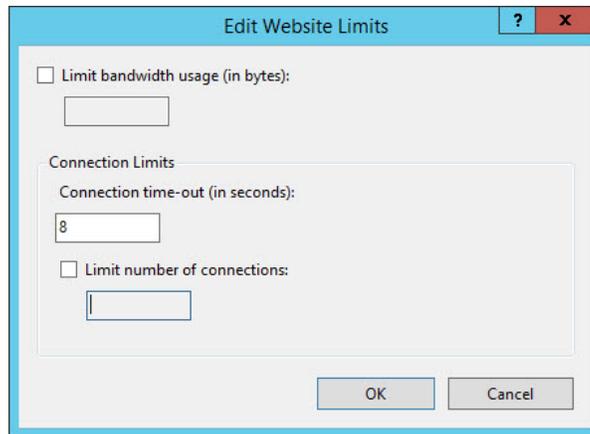


Figure 66 – Connection time-out

6. Exit the Internet Information Services (IIS) Manager.

Verify iBed Server

To verify iBed Server:

1. Open the **Stryker iBed Server Tool** by either double-clicking the **iBed Server Tools Suite** shortcut  located on your desktop, or by clicking **Start > All Programs > Stryker > iBed Server Tools** (Figure 67).

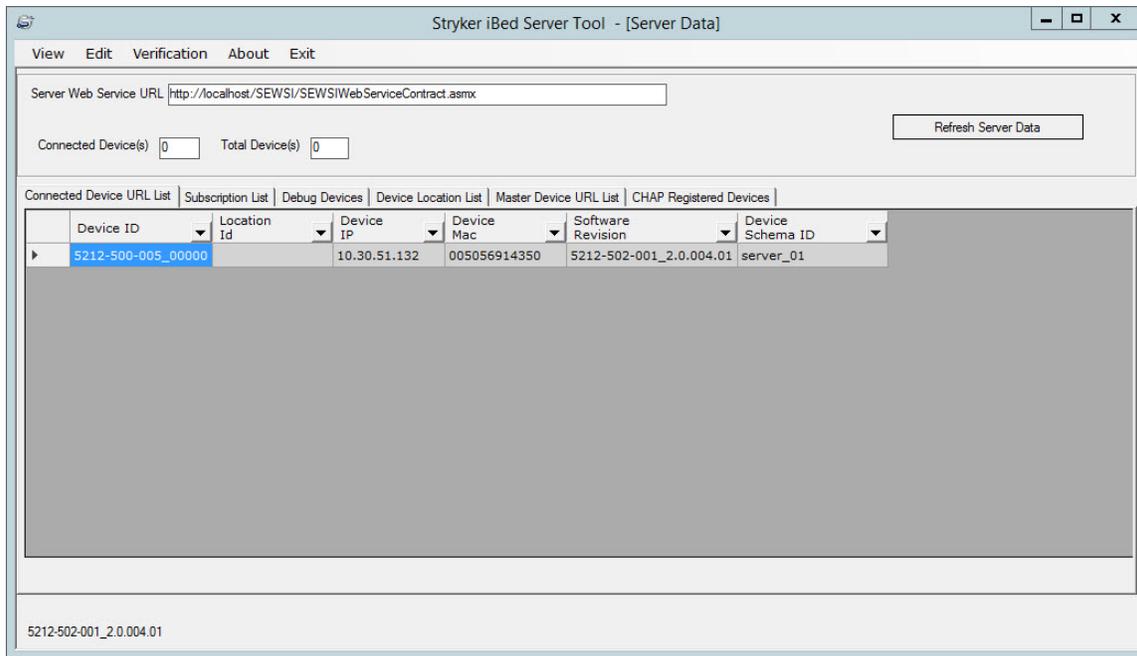


Figure 67 – Stryker iBed Server Tool

2. Click **Verification>Server** in the task bar.
3. In the **iBed Server Verification** window, click **Verify Server** (Figure 68).

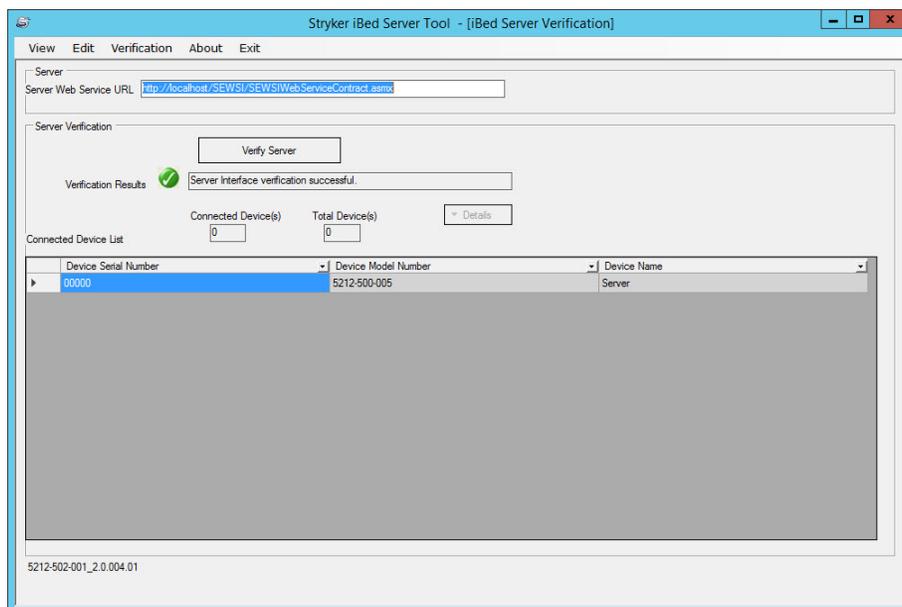


Figure 68 – Verify iBed Server

- a. If the server interface verification is successful, the system returns a green check (Figure 68).

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

Note - Before you continue installing **iBed** Server, you must resolve this error. To resolve the error, return to the beginning of the installation process and make sure that all steps were executed properly. For further troubleshooting details, see *Troubleshooting* (page 56).

4. Proceed to *Adding devices (clients) to the Master Device List* (page 42).

Setup

Adding devices (clients) to the Master Device List

1. Open the **iBed Server Tool** by either double-clicking the **iBed Server Tools Suite** shortcut  located on your desktop, or by clicking **Start > All Programs > Stryker > iBed Server Tools > iBed Server Tools**.
2. In the **iBed Server Tool** window, click **Edit>Master Device List** (Figure 69).

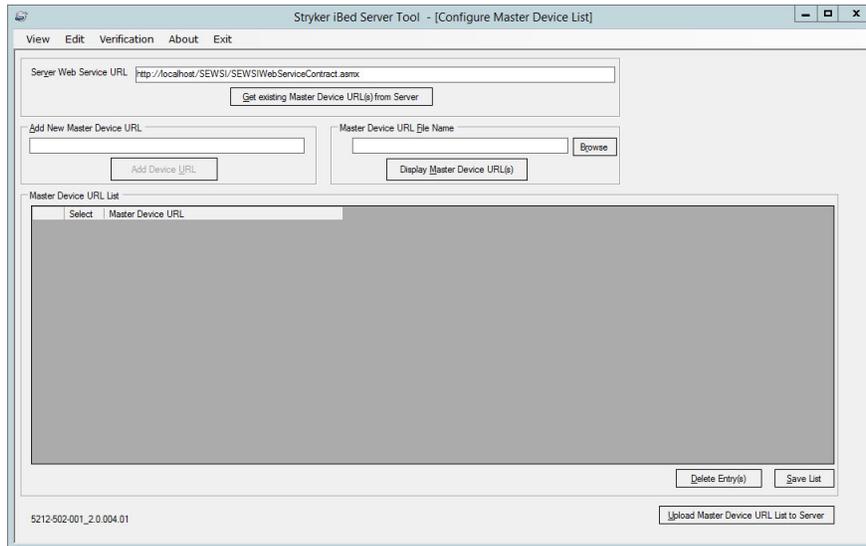


Figure 69 – Edit Master Device List

3. In the **Add New Device URL** box, type in the URL of the device and then click **Add Device URL** (example: `http://10.32.56.101:1639` or `http://syk-84253f2356a.stryker.com:1639`) (Figure 70).

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

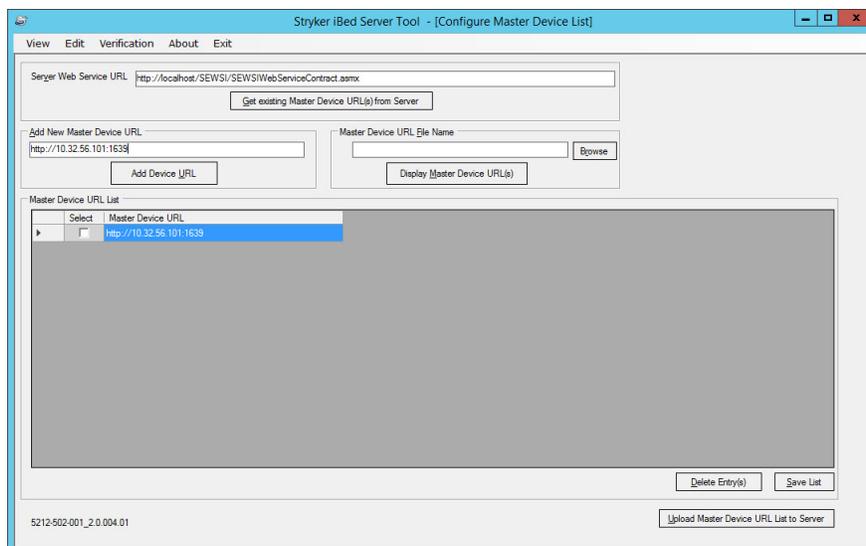


Figure 70 – Add Device URL

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

- Once all new devices are in the list, click the **Select All** box of the **Master Device URL List** and then click the **Upload Master Device URL List to the Server** button (Figure 71).

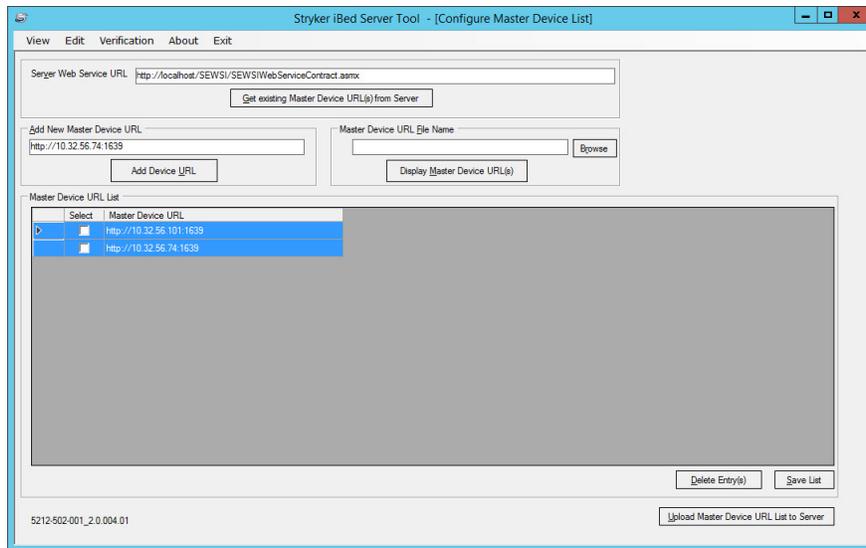


Figure 71 – Master Device URL List

- Click the **OK** button in the **Alert** window confirming that the **Master Device URL List** was uploaded to the server.
- To make sure that the **Master Device URL List** uploaded, go to the **iBed Server Tool** window and click **View>iBed Server**.

Note - Allow time for synchronization before you make sure that the **Master Device URL List** was uploaded.

Adding iBed Locator IDs and hospital locations

- Open the **iBed Server Tool** by either double-clicking the **iBed Server Tools Suite** shortcut  located on your desktop, or by clicking **Start > All Programs > Stryker > iBed Server Tools > iBed Server Tools**.
- In the **iBed Server Tool** window, click **Edit>Location Association** (Figure 72).

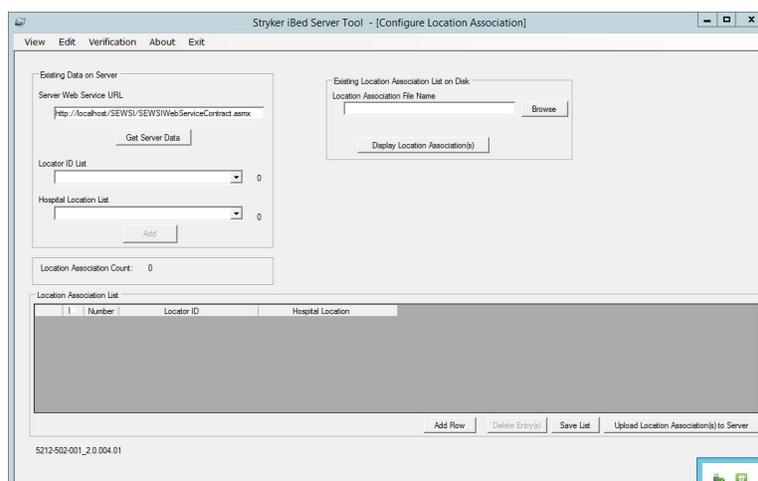


Figure 72 – Location Association

- In the **Location Association List** box, click in the **Locator ID** box and type the ID from the Locator (Figure 73).

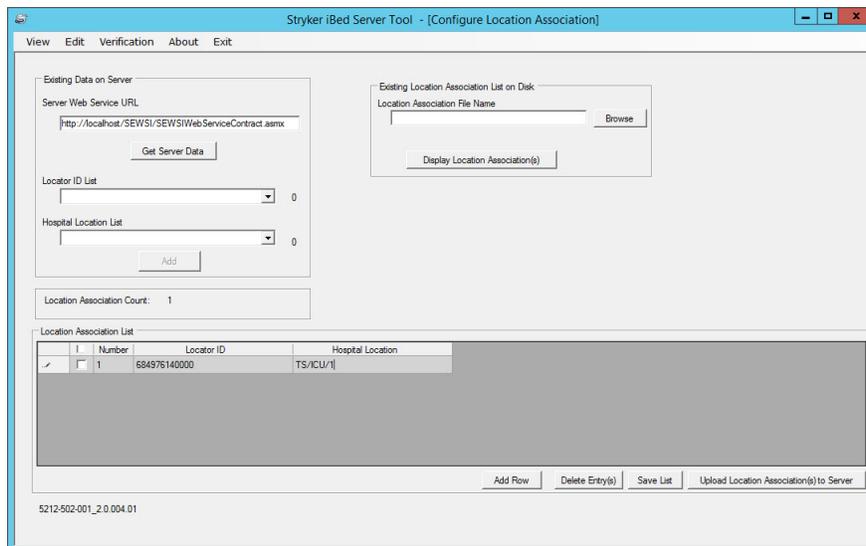


Figure 73 – Add Location Association

- In the **Location Association List** box, click in the **Hospital Location** box and type the Hospital Location (Figure 73).
Note - The Hospital Location is normally formatted using the location HL7 alias name.
- To add another association, click the **Add Row** button (Figure 73).
- Repeat steps 3 and 4 until all new Locator IDs and Hospital Locations have been entered.
- Once all new location associations have been made, click the upper left **Select All** box of the Location Association List, and then click **Upload Location Association(s) to Server** (Figure 74).

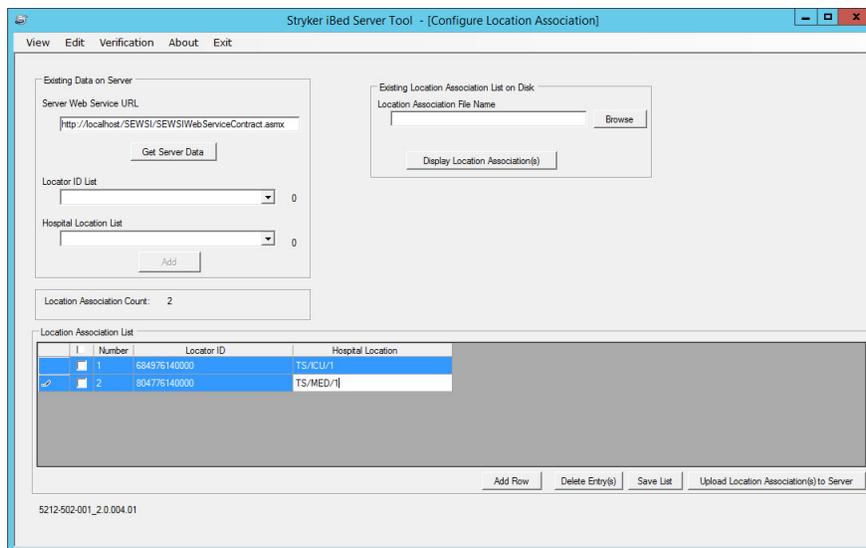


Figure 74 – Upload Location Association

- Click the **OK** button in the **Alert** window to confirm that the Locator ID List, Hospital Location List, and Location Association List have been successfully uploaded to the server.
- To verify in the **iBed Server Tool** window, click **View>iBed Server**.

Note - Allow time for synchronization before you make sure that the Master Device URL List was uploaded.

Adding an additional Stryker interface

Smart Equipment Management (SEM)

Note - If the facility has an existing LIFENET account, navigate to **Account Definition** and check the **Smart Equipment Management** box under **Features**.

Creating a LIFENET® account

Note - Make sure that the facility does not have a pre-existing LIFENET account. If they do not, continue to step 1.

1. In an internet browser window, go to <https://www.lifenetsystems.com/> to reach the LIFENET website.
2. Click on the **Account** tab and click **Accounts** in the drop down list (Figure 75).

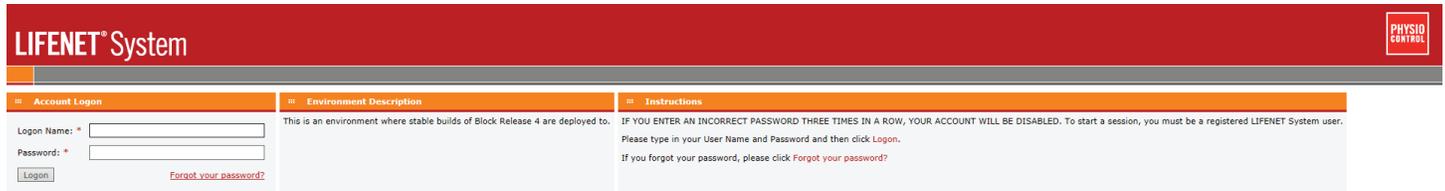


Figure 75 – LIFENET create account

3. To create a new account, click **Add Account** (Figure 76).

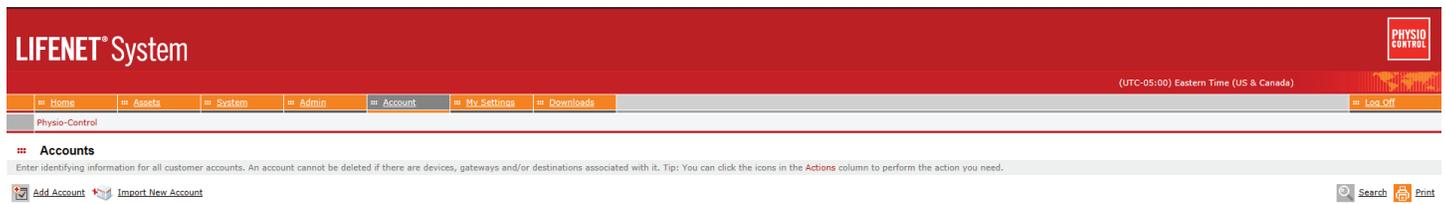


Figure 76 – Add Account

4. Submit information for all of the required fields:

a. Add Account (Figure 77)

Figure 77 – Add Account

b. Account Address (Figure 78)

Figure 78 – Account Address

c. Account Definition (Figure 79)

Note - Make sure that you select the following: LIFENET, Live, Hospital, Expiration Date, Smart Equipment Management, and Other Devices

Figure 79 – Account Definition

d. Account Configuration

Note - This step can be skipped.

e. Account Administrator (Figure 80)

Priority	Type	Phone Number
Primary Phone	Work Phone	<input type="text"/>
Secondary Phones	No Records Found	Add a phone number

Priority	Type	E-Mail Address
Primary E-Mail Address	Work E-Mail	<input type="text"/>
Secondary E-Mail Addresses	No Records Found	Add an e-mail address

Figure 80 – Account Administrator

f. Notes

Note - This step can be skipped.

5. Click **Done** which will prompt an email to be sent to the newly created Account Administrator. This email will contain a link to the SEM home page and a temporary password that needs to be changed before installing the SEM Device Data Manager (Figure 81).

Figure 81 – SEM home page

Installing the Stryker SEM Device Data Manager

1. Upload the Stryker SEM Device Data Manager install file (5212-504-001) onto the Stryker server where the **iBed** Server Application is installed.
2. Begin the Stryker SEM Device Data Manager installation by right clicking the **5212-504-001 Device Data Manager** file and select **Run as Administrator**.

3. In the **Stryker SEM Device Data Manager - InstallShield Wizard** window, click **Next** (Figure 82).

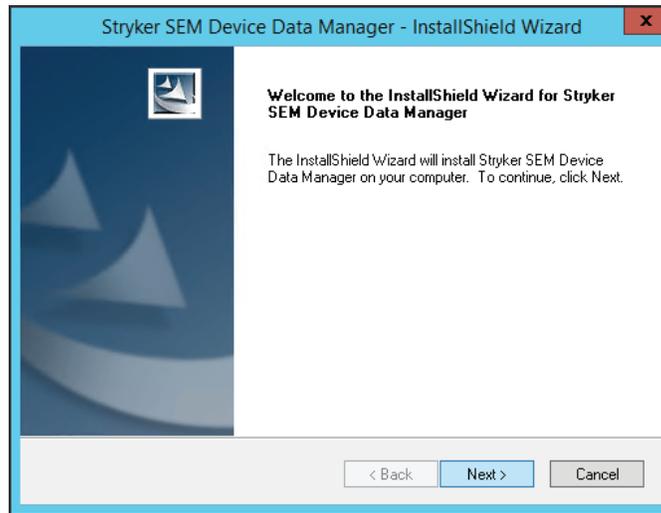


Figure 82 – InstallShield Wizard

4. In the **Stryker SEM Device Data Manager - InstallShield Wizard** window, enter the following values and click **Next** (Figure 83).

- *i*Server IP address: IP address of the machine where the *i*Server is installed
- Hospital name: Name of the hospital
- Agent Serial Number: Enter the MAC address of the server machine where the SEM Device Data Manager is installed
- **LIFENET** UserName - Username that is used to register Device Data Manager with **LIFENET**
- **LIFENET** Password - Password that is used to register Device Data Manager with **LIFENET**
- **LIFENET** URL - The URL for registering the Device Data Manager installed at the hospital with **LIFENET**

Note - The **LIFENET** user name and password are located in the email sent to the Account Administrator in *Creating a LIFENET® account* (page 45).

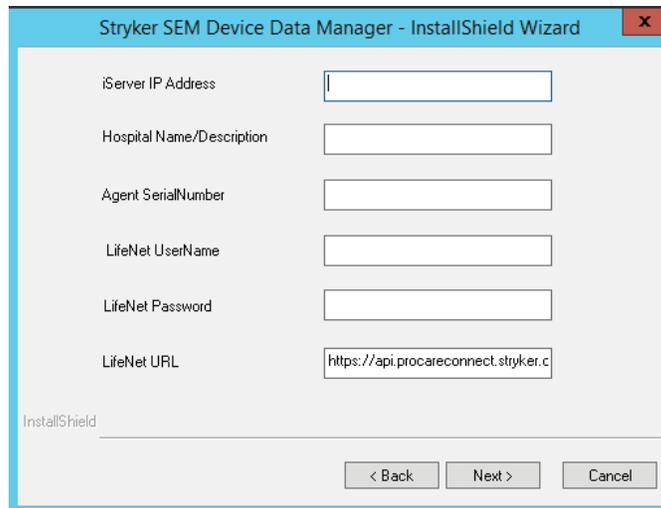


Figure 83 – Field values

5. In the **Choose Destination Location** step, click **Next** to install the SEM Device Data Manager files to the default location or click **Change** to select a different destination folder (Figure 84).

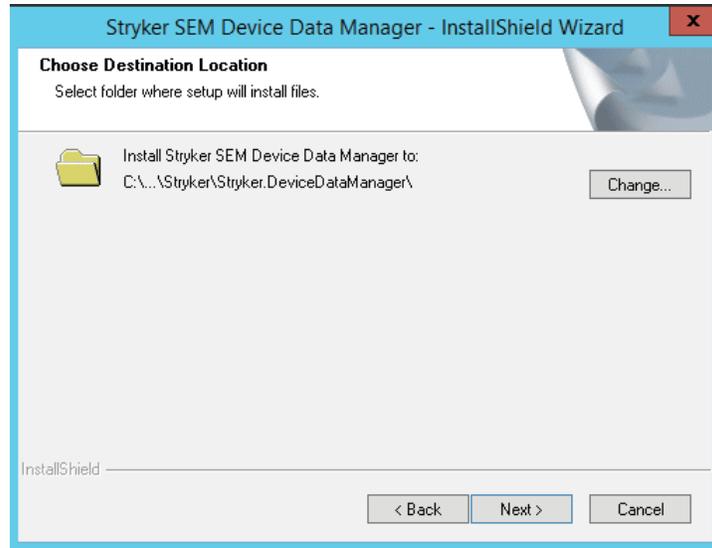


Figure 84 – Choose Destination Location

6. Click **Finish** to close the **Stryker SEM Device Data Manager - InstallShield Wizard** window (Figure 85).

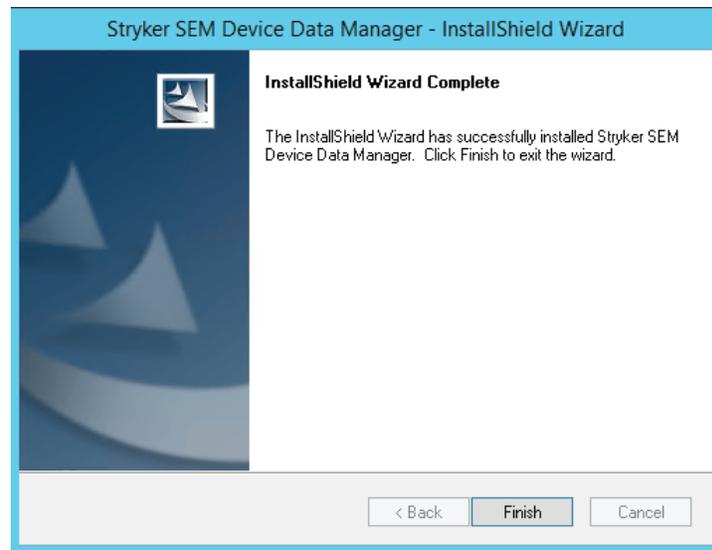


Figure 85 – InstallShield Wizard Complete

Verifying the Stryker SEM Device Data Manager is installed

1. In Windows, click **Start**.
2. Enter **run** in the search box.
3. In the run window, enter **inetmgr**.
4. Expand **Connections** in the left panel.
5. Under **Sites** navigate to and click **DeviceDataManager** (Figure 86).

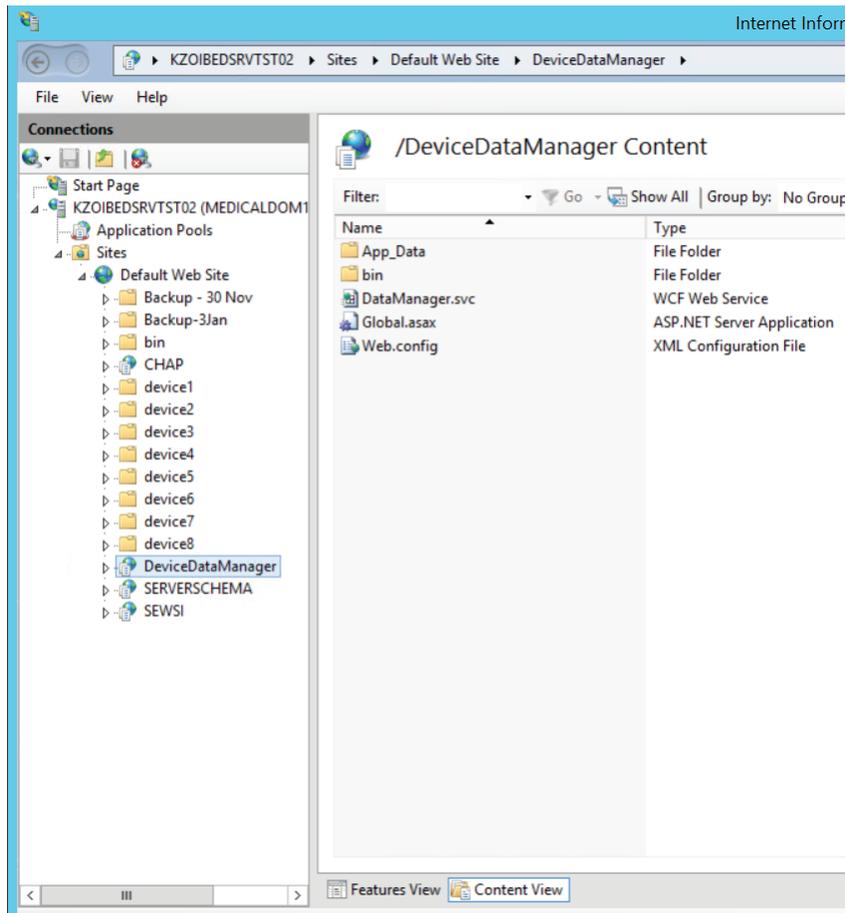


Figure 86 – DeviceDataManager

6. Right click on **DataManager.svc** and click **Browse**.
7. A browser window should open to the Data Manager Service web page.

Adding a third-party interface

Integrating Rauland Responder® 5

Note - This installation to be performed by Stryker personnel only.

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

Configuring the wireless router (Stryker device configuration)

Note - *iBed* Server 1.0 wireless clients only authenticate with TKIP encryption and *iBed* Server 2.0 wireless clients only authenticate with AES encryption. Below is an example of configuring a LINKSYS N600 E2500 router.

To configure the wireless router for Stryker devices:

1. Enter the router's admin menu to configure the router for use.
2. In the **Setup/Basic Setup** tab, verify the router is set for DHCP (Figure 87).

The screenshot displays the Linksys E2500 Basic Setup page. The top navigation bar includes 'Setup', 'Wireless', 'Security', 'Storage', 'Access Policy', 'Applications & Gaming', 'Administration', and 'Status'. The 'Setup' section is expanded to show 'Basic Setup', 'VLAN Setup', 'IPv6 Setup', 'DDNS', 'MAC Address Clone', and 'Advanced Routing'. The 'Basic Setup' page is divided into several sections: 'Language' (English), 'Internet Setup' (Automatic Configuration - DHCP), 'Network Setup' (Router Address), 'DHCP Server Setting', 'Time Settings' (Time Zone), and 'Reboot'. The DHCP Server Setting section is highlighted, showing the 'DHCP Server' is 'Enabled'. The 'Start IP Address' is 192.168.1.100, and the 'Maximum Number of Users' is 100. The 'IP Address Range' is 192.168.1.100 to 199. The 'Client Lease Time' is 0 minutes. The 'Static DNS' and 'WINS' fields are all set to 0.0.0.0. The 'Time Zone' is set to '(GMT-05:00) Eastern Time (USA & Canada)' and the 'Automatically adjust clock for daylight saving changes' checkbox is checked. The 'Reboot' button is visible at the bottom.

Figure 87 – Basic Setup

3. In the **Wireless/Basic Wireless Settings** tab, configure the 2.4 GHz and 5 GHz Wireless Settings so they match Figure 88.

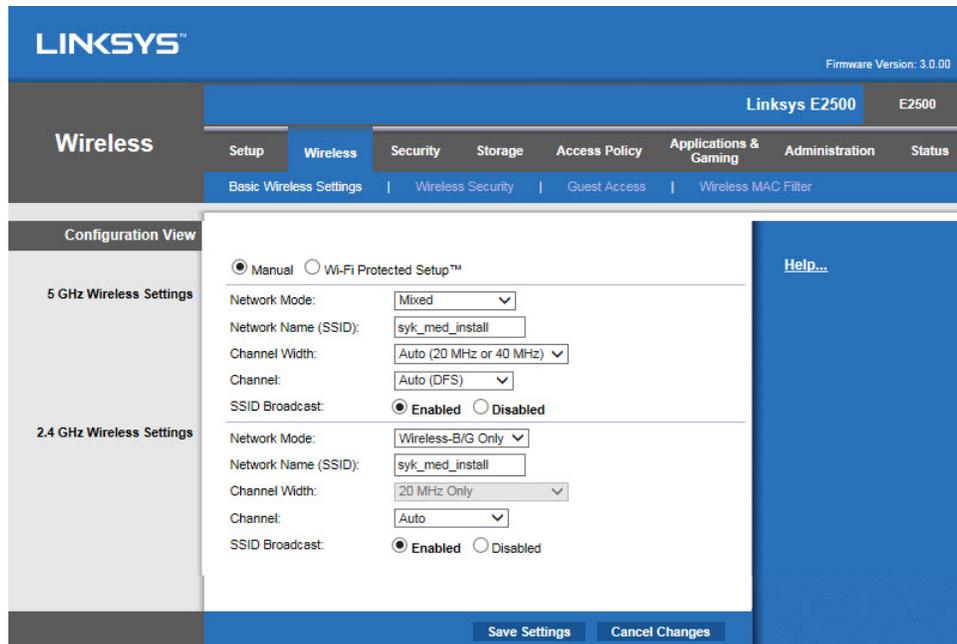


Figure 88 – Basic Wireless Settings

4. In the **Wireless/Wireless Security** tab, configure the 2.4 GHz and 5 GHz Wireless Security Settings so they match Figure 89.

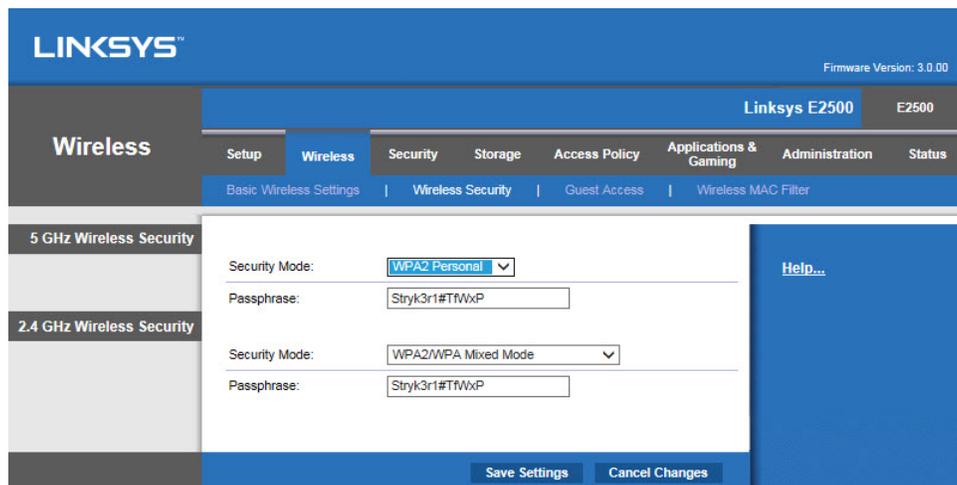


Figure 89 – Wireless Security

5. Click the **Save Settings** button.

Configuring wireless network connection settings

Applies to Gateway 1 (3002 **Secure**® II, 3002 / 3005 **S3**®), Gateway 2 (3002 / 3005 **S3**), and Gateway 3 (2131 / 2141 **InTouch**®).

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 51)).
2. Plug the power cord of the bed into the wall outlet and make sure that the wireless option is turned on.
3. Connect the laptop to the syk_med_install SSID which the configured router is broadcasting.
4. Open the **iBed Wireless Configuration Tool**.
5. On the bed, 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 which the router provided for the bed.
7. Enter the bed IP address in the **Wireless Device URL/IP** box (Figure 90).

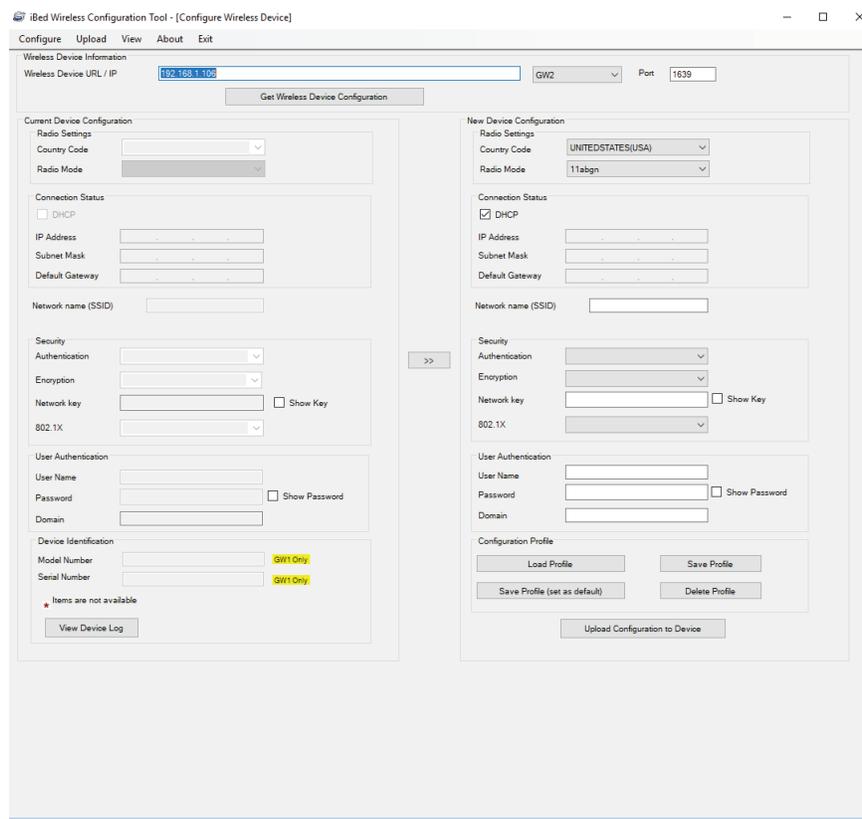


Figure 90 – Wireless Device URL

8. Click the **Get Wireless Device Configuration** button. This will retrieve the bed wireless default settings and connect to the bed, which is shown in the left column of the tool.
9. Click the **OK** button of the retrieval confirmation.
10. Enter the facility network information and make sure that you fill in all of the appropriate blanks in the right column of the tool.
11. Select the **Radio Mode** for the facility requirements.
12. Click the **Upload Configuration to Device** button.

Note - If the radio does not connect, make sure that you check the settings entered into the column on the right. If they are incorrect, the radio will need to be reset to defaults and then 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 its highest position.
2. Using a large paper clip, insert it into the reset hole (A) on the bottom side of the wireless module (B).
3. Hold the large paper clip inside the reset hole for five seconds.

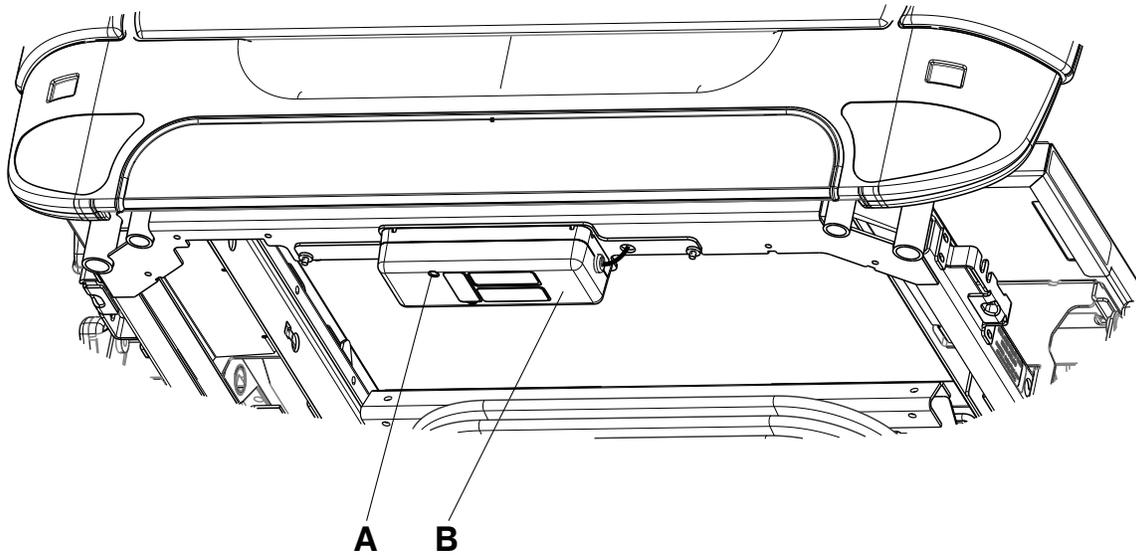


Figure 91 – Wireless module

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

Note - For InTouch 2.1-4.0, follow all of the steps below. For InTouch 5.0 or higher, see step 1 to reset Wi-Fi.

Tools required:

- Appropriate FL27 InTouch maintenance manual

Procedure:

1. Use the appropriate FL27 InTouch maintenance manual to access the **Configuration** menu (For InTouch 2.1-4.0 see Figure 92. For InTouch 5.0 or higher, see Figure 94).
2. Tap **Wi-Fi Configuration** (A) (Figure 92).
3. Tap the **Advanced** tab (A) (Figure 93).
4. Tap **Reset** (B) (Figure 93).
5. Tap **Save**.

InTouch 2.1 - 4.0

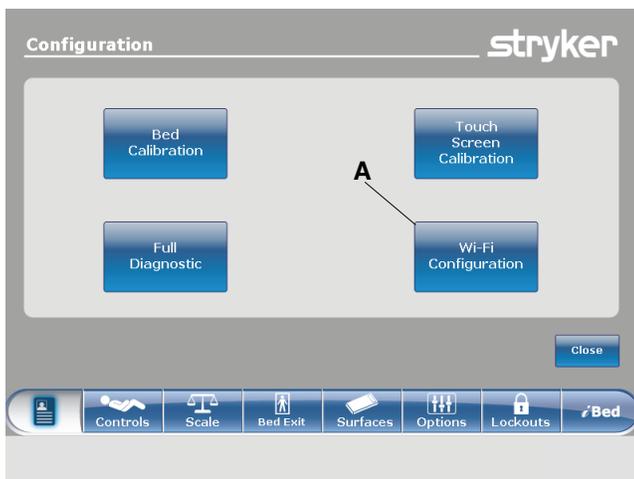


Figure 92 – InTouch Configuration Menu

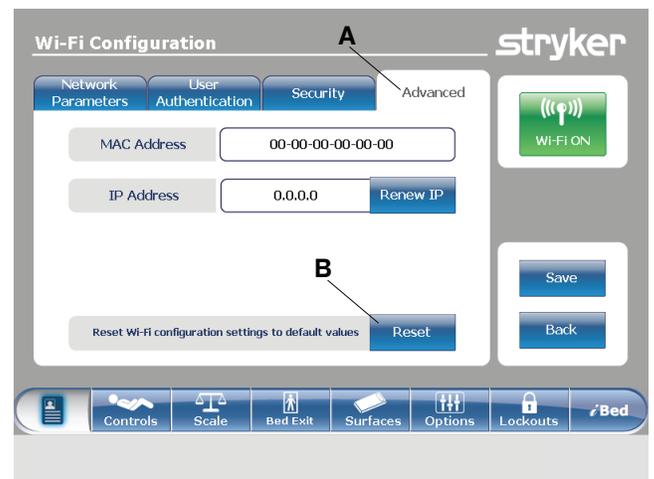


Figure 93 – InTouch Wi-Fi Configuration menu

InTouch 5.0 or higher

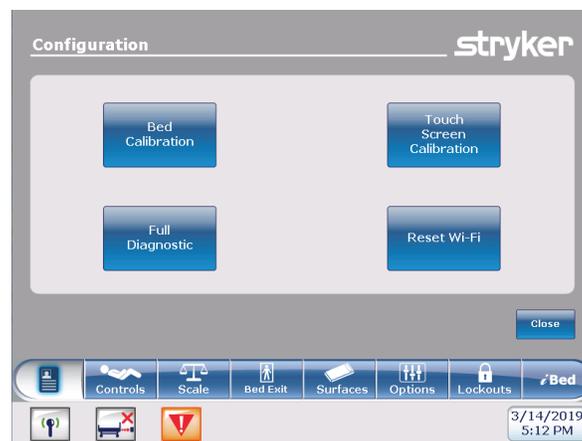


Figure 94 – InTouch Wi-Fi Reset

Troubleshooting

Basic

Problem	Possible cause	Solution
Cannot verify the iBed Server Tool	The Web Service URL is incorrect.	<p>Make sure the URL in the Web Service URL box is correct.</p> <ol style="list-style-type: none">1. If the URL is incorrect, enter the following URL into the Web Service URL box (<i>Verify iBed Server</i> (page 40)): http://localhost/SEWSI/SEWSIWebServiceContract.asmx.2. Click Verify Server.
	The Heartbeat service is not active.	<ol style="list-style-type: none">1. Make sure that the Heartbeat service is running.<ol style="list-style-type: none">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 all of the required Default Web Sites.	<ol style="list-style-type: none">1. Make sure that the IIS Manager has all of the required Default Web Sites.<ol style="list-style-type: none">1.1. Go 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
<p>Cannot see the device in the iBed Server application</p>	<p>The MAC address does not have the bed's IP address or DNS name.</p>	<ol style="list-style-type: none"> 1. If the troubleshooting steps in the appropriate bed maintenance manual were followed: <ol style="list-style-type: none"> 1.1. Use the MAC address from the bed and verify with IT what wireless module's IP address or DNS name is. 1.2. Ping the wireless module from the server machine using the Command Prompt (ping IP address or DNS name :1639). 1.3. Press Enter. <ol style="list-style-type: none"> 1.3.1. If you receive four (4) responses, then the bed is on the wireless network. 1.3.2. If you receive no response, check the wireless module on the bed.
Problem	Possible cause	Solution
<p>Cannot see a device in the Server Tools under the Device Location List, but the device shows under the connected device URL List</p>	<p>The device was not added to the device list.</p>	<ol style="list-style-type: none"> 1. Using the server tool, select Verify Device Directly. 2. Click Get Existing Device(s), and then select the device in question. 3. Add it to the Device List. 4. In the Device List, select the device, and then click Verify Device(s). 5. Check the Connection Status once it responds. <ol style="list-style-type: none"> 5.1. If there is a response, the device is communicating properly on the wireless network.

Problem	Possible cause	Solution
	<p>The serial number in the CPU and the serial number on the bed specification label do not match.</p>	<ul style="list-style-type: none"> • Identify the bed serial number that is stored in the CPU. It should match the serial number on the serial label on the bed. <p>Note - If there are two matching serial numbers in the device list, the server will only recognize the first device that logs on to the server.</p> <ul style="list-style-type: none"> • To find the bed's serial number, put the bed into the Bed Configuration mode and navigate to Serial Number > Current SN to verify the serial number. • 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
<p>Cannot see a location</p>	<p>The Locator ID was entered incorrectly.</p>	<ol style="list-style-type: none"> 1. Using the iBed Locator Association Tool, select View Current Location Associations. 2. Click Get Location Associations from server. 3. Look through the Hospital Location and verify the Locator ID. <p>Note - The Locator ID is alphanumeric and case sensitive. You must use lower case to enter the Locator ID letters, or the server will not recognize the locator.</p> <ol style="list-style-type: none"> 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 <i>Adding iBed Locator IDs and hospital locations</i> (page 43).

Problem	Possible cause	Solution
<p>Third party does not receive bed status information</p>		<ol style="list-style-type: none"> 1. Make sure the SEWSI web.config file has the correct Web URL.. <ol style="list-style-type: none"> 1.1. Navigate to the directory where the iBed Server Tool is installed. <ol style="list-style-type: none"> 1.1.1. Navigate to the SEWSI folder and open the web.config file. 1.1.2. Find the line which contains ServerURL= <ol style="list-style-type: none"> 1) Make sure the local host was replaced with the IP of the server <p>Note - This cannot be a DNS name.</p> 2. Make sure Port 80 is not blocked. <ol style="list-style-type: none"> 2.1. Port 80 needs to be open between the Stryker server and products (bi-directional), and the Stryker server and any third-party servers (bi-directional) (LINK HERE). 2.2. If Port 80 is blocked, work with IT to open the port. 3. Search SEWSI logs to make sure there are no communication failures. Find messages generated for the third-party (LINK HERE)

Advanced

Connectivity issues (total device counts)

View total device counts to identify drops.

- Navigate to the directory where iBed Server Tools is installed and open the LOGS folder.
 1. Find **StrykerMainenanceService_logfile.txt**.
 2. Highlight several of the **StrykerMainenanceService_logfile.txt** files during the time when there may have been an outage.
 - a. Right click and select **Edit with Notepad++**.
 3. In **Notepad++** press **Ctrl+F** to open a find window.
 - a. Search for the below string and select **Find in All Opened Documents**.

Note - [Total Connected Devices Count excluding server =

- b. The **Find Result** pane in **Notepad++** will populate with the lines of the selected log files (Figure 95).

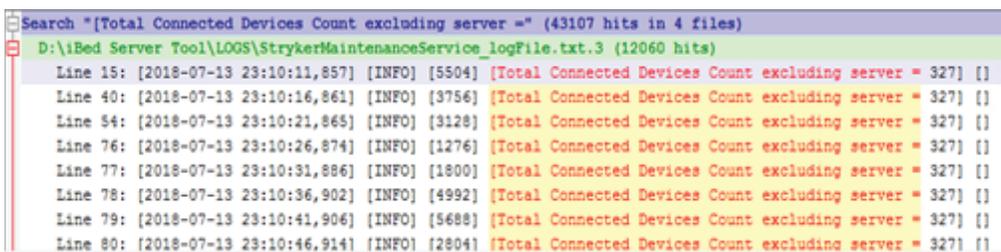


Figure 95 – Total device counts

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

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 which is going to the correct third party.
 - a. Verify 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. To search for messages in a specific timeframe, highlight multiple **SEWSI_logfile.txt** in that range based on the date modified in Windows Explorer.
 - a. Right click the highlighted files and select **Edit with Notepad++**.
6. Press **Ctrl+F** to open a find window.
 - a. Paste the **Subscription ID** copied in step 3.
 - b. Select **Find in all opened documents**.
 - c. The Find result pane will open with all messages containing the **Subscriber ID**.
7. Click the XML message from the Find pane to open the file to that line.
 - a. XML messages will start in format `<?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. Click the far left blank cell of the header to highlight the entire table.
 - a. Copy and paste the data in **Microsoft Excel**.
4. Highlight the **Client ID** column.
5. In the **Home** tab of the ribbon, click **Conditional Formatting**.
 - a. Highlight **Cells Rules - Duplicate Values**.
 - b. Click **OK** to highlight duplicates in red.
 - c. Highlight the row above where the data was pasted, click the **Data** tab, and select **Filter**.

Any cells highlighted (except **Network Exception / Timeouts**) are duplicate serial numbers which need to be resolved.

Connectivity issues to one / multiple devices

Not receiving specific bed status over port 80.

- Verify communication from devices to the server with SOAP UI.

Note - Requires Stryker supplied project file.

1. Open **SOAP UI**.
2. In the **Projects** pane, expand the **SEWSI** folder.
3. Click **Connectivity Mock** to open **Connectivity Mock** window (Figure 96).

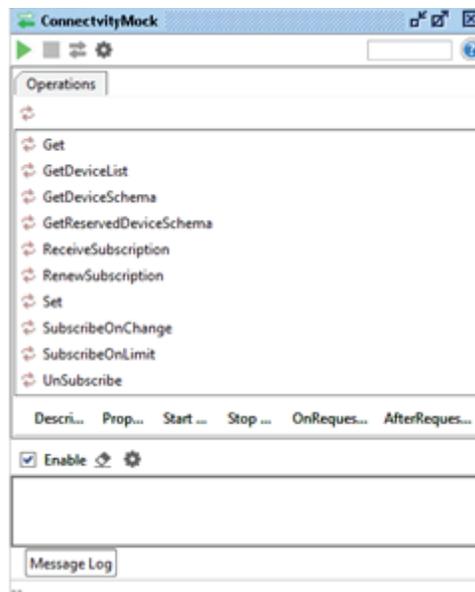


Figure 96 – Connectivity Mock

4. Click the gear icon to edit settings for Mock Third Party.
 - a. Modify host URL to the IP address of the server where SOAP UI is running (Figure 97).

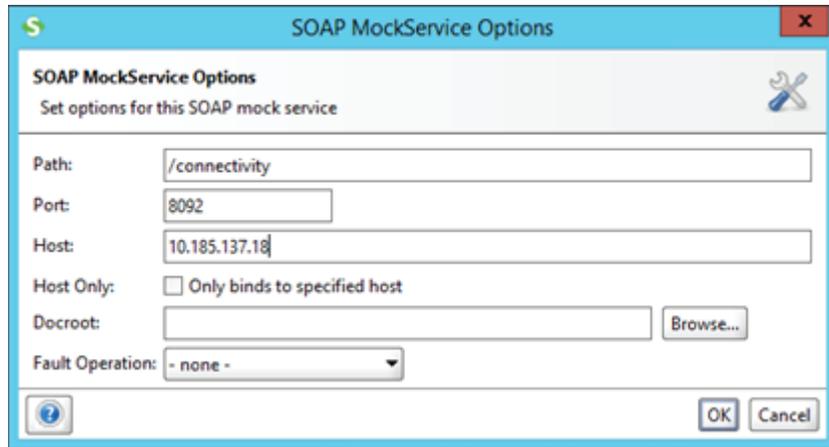


Figure 97 – SOAP UI

- b. Click **OK** to save.
5. Click the green **Play** icon to start the Mock Third Party Service.
6. Click the green arrows to open the service webpage to verify.
 - a. Copy the URL of the webpage to the clipboard
7. In the Projects Pane, expand **SEWSIWebServiceContract**.
 - a. Expand **SubscribeOnChange**.
 - b. Double click **VTF - Sub 3 (72 hour)**.
 - c. Modify the Subscriber URL with the URL from step 3.3.1 (Figure 98).

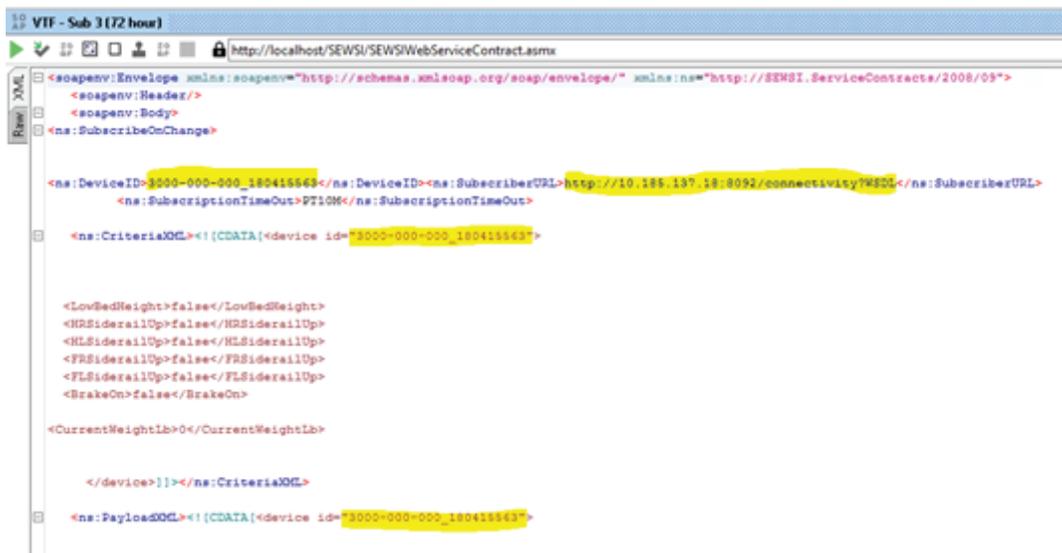


Figure 98 – VTF - Sub 3 (72 hour)

- d. Change the Device ID to the Device ID being searched for (Figure 98).
 - e. Click the Play icon in **VTF - Sub 3 (72 hour)** window.

8. In the **ConnectivityMock** window, you will begin to see messages appear in the message log if the ports are open and the server is able to communicate with the device (Figure 99).

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

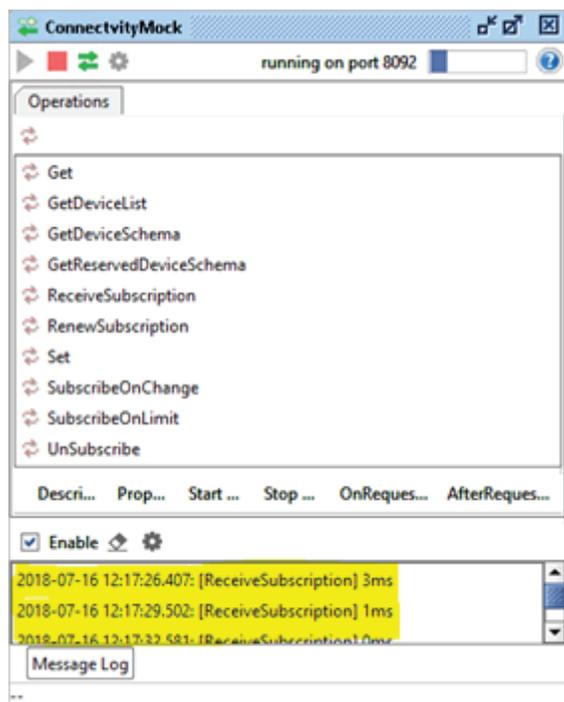


Figure 99 – Message Log

9. Double click a message to view the XML generated (Figure 100).

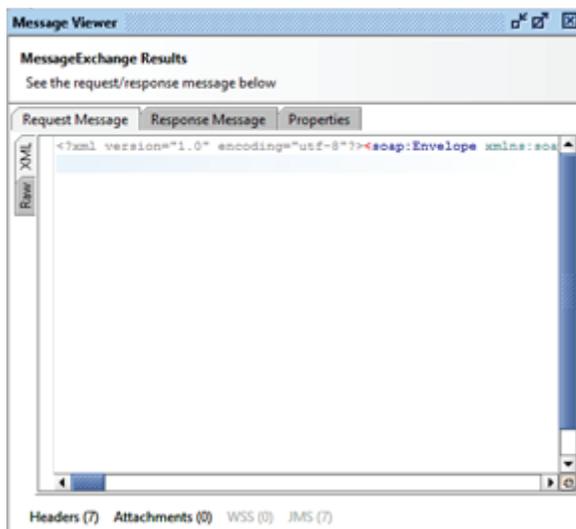


Figure 100 – Message Viewer

Cannot communicate with device (verify ports are open)

Verify communication with device over port using TELNET.

1. Open a **command** prompt.

2. Enter the command **telnet <IPAddress> <Port>**, where **IP Address** is the address of the device and **Port** is the port number for verification (Figure 101).

```
Microsoft Windows [Version 6.3.9600]
(c) 2013 Microsoft Corporation. All rights reserved.
C:\Users\svc_ca_stryker>telnet 10.159.159.91 1639_
```

Figure 101 – 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 102).

```
C:\Users\svc_ca_stryker>telnet 10.159.159.91 20000
Connecting To 10.159.159.91..._
```

Figure 102 – Connecting

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

Cannot communicate with device (DNS only)

Verify Hostname with NSLOOKUP

1. Open a **command** prompt.
2. Enter the command **nslookup <IPAddress>** where **IP Address** is the address of the device for **DNS entry** verification.
 - A reply with the **hostname** and **IP address** indicates success (Figure 103).

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

```
C:\Users\svc_ca_stryker>nslookup 10.159.159.91
Server: int-gtm-cdc.nyumc.org
Address: 10.185.98.100

Name: syk-84253f3ef34e.wireless.nyumc.org
Address: 10.159.159.91

C:\Users\svc_ca_stryker>_
```

Figure 103 – DNS success

- A reply that states <DNSServerName> can't find <IPAddress> indicates failure (Figure 104).

```
C:\Users\svc_ca_stryker>nslookup 10.159.159.200
Server:  int-gtm-cdc.nyumc.org
Address: 10.185.98.100

*** int-gtm-cdc.nyumc.org can't find 10.159.159.200: Non-existent domain
C:\Users\svc_ca_stryker>_
```

Figure 104 – DNS failure

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

Note - The server reply should be the same as seen in step 2.

Smart Equipment Management (option) troubleshooting

1. To verify **Device Data Manager Utility**:

- In Windows, click **Start**.
- Enter **StrykerDeviceDataManagerRegistration** in the search box.
- Make sure that the **StrykerDeviceDataManagerRegistration** utility is displayed in the search results.

2. To verify in **iBed Server Tool**:

- Locate the machine where the Stryker **iBed Server** application is installed and open the **iBed Server Tool**.
- Click the **Subscription List** tab and 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 105).

Connected Device	URL List	Subscription List	Debug Devices	Device Location List	Master Device URL List	CHAP Registered Devices	Client Diagnostic Info
		Device ID			Subscription ID		Create Time
1	<input type="checkbox"/>	5212-500-005_00000			5212-500-005_00000_3af0fc22-ade0-4542-9ddf-386bfd20a045		12/7/2017 8:39:41 PM
▶ 2	<input checked="" type="checkbox"/>	3000-000-000_DeviceW1			C3000-000-000_DeviceW1_201712072039427036		12/7/2017 8:39:42 PM
3	<input type="checkbox"/>	3000-000-000_DeviceW1			C3000-000-000_DeviceW1_Alarms201712072039427036		12/7/2017 8:39:42 PM
4	<input type="checkbox"/>	3000-000-000_DeviceW2			C3000-000-000_DeviceW2_201712072039425276		12/7/2017 8:39:42 PM
5	<input type="checkbox"/>	3000-000-000_DeviceW2			C3000-000-000_DeviceW2_Alarms201712072039426806		12/7/2017 8:39:42 PM
6	<input type="checkbox"/>	3000-000-000_DeviceW3			C3000-000-000_DeviceW3_201712072039423646		12/7/2017 8:39:42 PM
7	<input type="checkbox"/>	3000-000-000_DeviceW3			C3000-000-000_DeviceW3_Alarms201712072039423626		12/7/2017 8:39:42 PM

Figure 105 – 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 106 and Figure 107).

Subscription ID	Create Time	Last Renew Time	Subscriber URL
5212-500-005_00000_3af0fc22-ade0-4542-9ddf-386bfd20a045	12/7/2017 8:39:41 PM	12/7/2017 8:39:41 PM	http://10.117.40.238/DeviceDataManager/DataManager.svc
C3000-000-000_DeviceW1_201712072039427036	12/7/2017 8:39:42 PM	12/7/2017 8:39:42 PM	http://10.117.40.238/DeviceDataManager/DataManager.svc
C3000-000-000_DeviceW1_Alarms201712072039427036	12/7/2017 8:39:42 PM	12/7/2017 8:39:42 PM	http://10.117.40.238/DeviceDataManager/DataManager.svc
C3000-000-000_DeviceW2_201712072039425276	12/7/2017 8:39:42 PM	12/7/2017 8:39:42 PM	http://10.117.40.238/DeviceDataManager/DataManager.svc
C3000-000-000_DeviceW2_Alarms201712072039426806	12/7/2017 8:39:42 PM	12/7/2017 8:39:42 PM	http://10.117.40.238/DeviceDataManager/DataManager.svc
C3000-000-000_DeviceW3_201712072039423646	12/7/2017 8:39:42 PM	12/7/2017 8:39:42 PM	http://10.117.40.238/DeviceDataManager/DataManager.svc
C3000-000-000_DeviceW3_Alarms201712072039423626	12/7/2017 8:39:42 PM	12/7/2017 8:39:42 PM	http://10.117.40.238/DeviceDataManager/DataManager.svc

Figure 106 – 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-nq-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 107 – Web.config file

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

- Search for string “DeviceID=<SerialNumber> JsonContent=” in the log file (Figure 108)

Note - Replace <SerialNumber> with 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 108 – Example: DeviceID = 1234567890 JsonContent=

- Search for string “Data Uploaded for Server successfully!” in the log file (Figure 109)

```

1 [2017-05-22 13:33:07,487] [INFO] [3624] [No change detected in server data returning] []
2 [2017-05-22 13:33:07,503] [INFO] [15340] [Data Upload Response for deviceID = :3000-000-000_DeviceS11Pal43 content = ] []
3 [2017-05-22 13:33:07,503] [INFO] [15340] [Data Uploaded successfully for DeviceID = 3000-000-000_DeviceS11Pal43] []
4 [2017-05-22 13:33:07,518] [INFO] [16072] [Data Upload Response for deviceID = :247703F4B422 content = ] []
5 [2017-05-22 13:33:07,518] [INFO] [16072] [Data Uploaded for Server successfully!] []
6 [2017-05-22 13:33:07,612] [INFO] [16072] [Searching request processing for SubscriptionID = C3000-000-000_DeviceS11Pal178_201705221317313380] []
7 [2017-05-22 13:33:07,737] [INFO] [15340] [Data Upload Response for deviceID = :3000-000-000_DeviceS11Pal138 content = ] []
8 [2017-05-22 13:33:07,737] [INFO] [15340] [Data Uploaded successfully for DeviceID = 3000-000-000_DeviceS11Pal138] []
9 [2017-05-22 13:33:07,737] [INFO] [16072] [Time taken for deserialization (ms) = 0] []
0 [2017-05-22 13:33:07,752] [INFO] [6156] [DeviceID = 3000-000-000_DeviceS11Pal178 JsonContent=

```

Figure 109 – Data uploaded in log file

4. To verify connected devices in the log file:

- Search for string “DeviceID = <deviceID> JsonContent=” in the log file (Figure 110)

Note - Replace <deviceID> with 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 110 – Example: DeviceID = 3000-000-000_DeviceS1 JsonContent=

- Search for string “Data Uploaded successfully for DeviceID = <deviceID>” in the log file (Figure 111)

Note - Replace <deviceID> with 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] [10152] [Connection to Lifenet established successfully. Data uploaded successfully for d
```

Figure 111 – Example: Data Uploaded successfully for 3000-000-000_DeviceS1 in LIFENET

Email alerts

The following email alerts may be generated by the *iBed* server application.

Email info	Scenario
<p>Email Subject: Stryker iBed Server Alert</p> <p>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.</p>	<p>Low Battery Status is true for the BBID mapped with a location</p>
<p>Email Subject: Stryker iBed Server Alert</p> <p>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.</p>	<p>Low Battery Status is true for a BBID which is not mapped to any room or the BBID is missing</p>
<p>Email Subject: Stryker iBed Server Alert</p> <p>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.</p>	<p>BBID is sent in the subscription payload but it is not present in the "BBIDList.xml" file</p>
<p>Email Subject: Stryker iBed Server Alert</p> <p>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.</p>	<p>BBID is sent in payload and it is present in "BBIDList.xml" file but not present in "DeviceBBIDLocationAssociation.xml" file</p>

Email info	Scenario
<p>Email Subject: Stryker iBed Server Alert</p> <p>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.</p>	<p>BBID is sent in payload and it is present in "BBIDList.xml" file and in "DeviceBBIdLocationAssciation.xml" file but location for that BBID is missing in "DeviceBBIdLocationAssciation.xml" file</p>
<p>Email Subject : Stryker iBed Server Urgent Alert</p> <p>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.</p>	<p>When DB is down</p>
<p>Email Subject: Stryker iBed Server Urgent Alert</p> <p>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.</p>	<p>DeviceConnectionInfoList table doesn't exist</p>
<p>Email Subject: Stryker iBed Server Urgent Alert</p> <p>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.</p>	<p>MasterSubscriptionInfo table doesn't exist</p>
<p>Email Subject: Stryker iBed Server Urgent Alert</p> <p>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.</p>	<p>LOCAL SERVICE doesn't exist</p>

Email info	Scenario
<p>Email Subject: Stryker iBed Server Urgent Alert</p> <p>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.</p> <p>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.</p>	<p>NETWORK SERVICE doesn't exist</p>
<p>Email Subject: Stryker iBed Server Urgent Alert</p> <p>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.</p> <p>Application Health Check Failed at Step 4 -> StrykerSEWSIHeartbeatservice is not running. Please restart StrykerSEWSIHeartbeatservice. After restart, if the message continues, please contact Stryker support.</p>	<p>Both SEWSI and HB services are down</p>
<p>Email Subject: Stryker iBed Server Urgent Alert</p> <p>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.</p> <p>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.</p> <p>Application Health Check Failed at Step 4 -> StrykerSEWSIHeartbeatservice is not running. Please restart StrykerSEWSIHeartbeatservice. After restart, if the message continues, please contact Stryker support.</p>	<p>Both SEWSI and HB services are down and MasterSubscriptionInfo table doesn't exist</p>

Email info	Scenario
<p>Email Subject: Stryker iBed Server Urgent Alert</p> <p>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.</p> <p>Application Health Check Failed at Step 4 -> StrykerSEWSIHeartbeatservice is not running. Please restart StrykerSEWSIHeartbeatservice. After restart, if the message continues, please contact Stryker support.</p>	<p>HB is down</p>
<p>Email Subject: Stryker iBed Server Urgent Alert</p> <p>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.</p>	<p>No devices are detected</p>
<p>Email Subject: Stryker iBed Server Urgent Alert</p> <p>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.</p>	<p>Number of connected devices drops below the configured threshold value</p>
<p>Email Subject: Stryker iBed Server Urgent Alert</p> <p>Email Body: The following errors with Third Party Communication has been recorded in last 1 hour. <Error></p>	<p>Error with third party</p>

stryker[®]



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