Druck

4Sight2

Calibration Management Software

Installation Manual 123M3140 Revision F

1. Introduction

The 4Sight2 Calibration software is a web based calibration management tool that helps you maintain and control your calibration environment to the highest standards of metrology. You can use the software for these tasks:

- Manage the calibration of all the measurement devices for a specified business location
- Setup a schedule of calibration work for technicians
- Upload and download data to and from the Druck portable calibrators(DPI620 Genii, DPI611 and DPI612) that have a USB communication function
- Manage the calibration records for devices that are not supported by a portable calibrator (Manual Data Entry)
- Inspect your calibration history records. You can also make a permanent record of each calibration certificate. For example: For ISO 9000 quality control procedures.
- Control automated calibrations using Druck Pressure Controllers (PACE 1000, 5000 & 6000), Portable Calibrators (DPI620 Genii, DPI611 and DPI612) and Temperature Calibrators (DryTC165, DryTC 650, LiquidTC165 & LiquidTC255)

1.1 Target Audience

1.1.1 Administrators

An administrator is responsible for the installation and configuration of the 4Sight2 software. After initial installation of 4Sight2 a single administrative account will be available. From this account new Users can be created, and Groups/Permission Sets assigned. Administrative users have read and write access to all of 4Sight2's features.

1.1.2 Supervisor

A supervisor has the responsibility of asset and calibration management. They have the ability to create and update assets within the 4Sight2 Enterprise, including Plants, Locations, Tags and Devices. They are responsible for linking documents to assets, such as Plant processes and device datasheets. Supervisors can create test procedures to be used during calibration, as well as schedule procedures and monitor the health of devices. Supervisors have the necessary permissions to approve calibrations.

1.1.3 Technicians

Technicians are responsible for performing calibrations. Calibrations can either be Portable, Manual or Automated, and is the technician's role to perform the relevant calibration type on a device. Once a calibration has been performed technicians can review the results and complete calibrations to then be approved by a supervisor.

1.1.4 Auditor

An auditor is responsible for inspecting reports. It may be mandatory in some Plants to conduct audits as a regulatory requirement.

2. System Requirements

The minimum system requirements to install 4Sight2 application in Server and Client machines are listed below:

2.1 Application Server

Operating System	Windows 10, Windows Server 2012 R2, Windows Server 2016, Windows Server 2019
Updates	All Windows Updates fully installed
Processor	Quad Core
RAM	8GB or greater (32GB Recommended)
Disk space	1TB
Network Speed	10Mbps

2.2 Client Work station

Operating System	Windows 10, Windows Server 2012 R2, Windows Server 2016, Windows Server 2019
Browser	Google Chrome V80+, Microsoft Edge V80, Firefox V74
Adobe Reader	Adobe Acrobat Reader DC Version 2015.017.20050 +
RAM	8GB or greater
Processor	Dual Core
Disk space	600GB
Network Speed	10Mbps

2.3 Local Installation

Operating System	Windows 10, Windows Server 2012 R2, Windows Server 2016, Windows Server 2019
Updates	All Windows Updates fully installed
Adobe Reader	Adobe Acrobat Reader DC Version 2015.017.20050 +
Processor	Dual Core
RAM	16GB or greater (32GB recommended)
Disk space	500GB or greater disk space
Browser	Google Chrome V80+, Microsoft Edge V80, Firefox V74

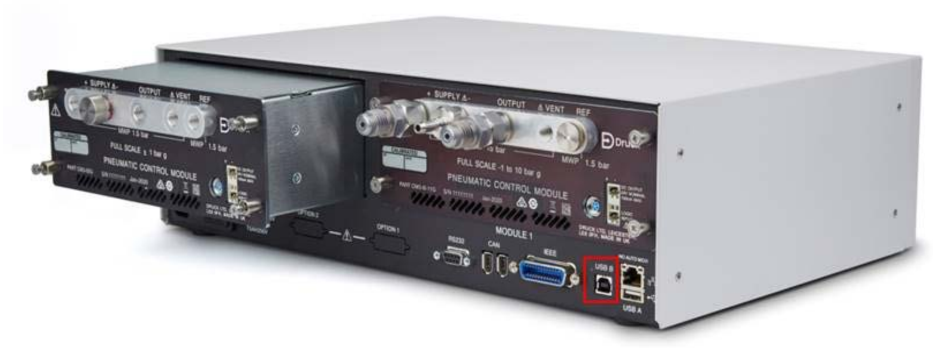
2.4 4Sight2 Supported Firmware

For the latest information about supported firmware, refer the link below:

https://www.bakerhughes.com/druck/test-and-calibration-instrumentation/calibration-management-software-4sight2

or

For PACE, Insert the USB B for 4Sight2 Communication as indicated in the image below:



4Sight2 Installation

3. 4Sight2 Installation

To install 4Sight2 firstly copy the 4Sight2 Setup zip to your desktop and extract the files from the zip. From the set-up file select the 4Sight2 executable.

Note: Following antivirus software are used for scanning 4Sight2 and Comm Server installs,

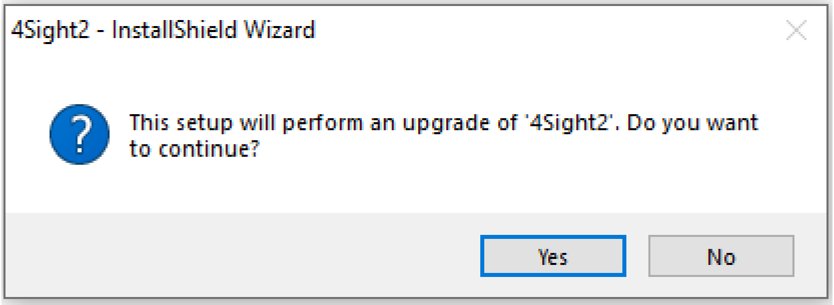
- McAfee VirusScan Enterprise + AntiSpyware Enterprise Version number: 8.8.0
- Symantec Endpoint Protection Version number: 14.3.558

Once you have run the setup executable the InstallShield wizard will start. The InstallShield wizard contains two stages of 4Sight2 installation:

1. Database Installation
2. Web Application Installation

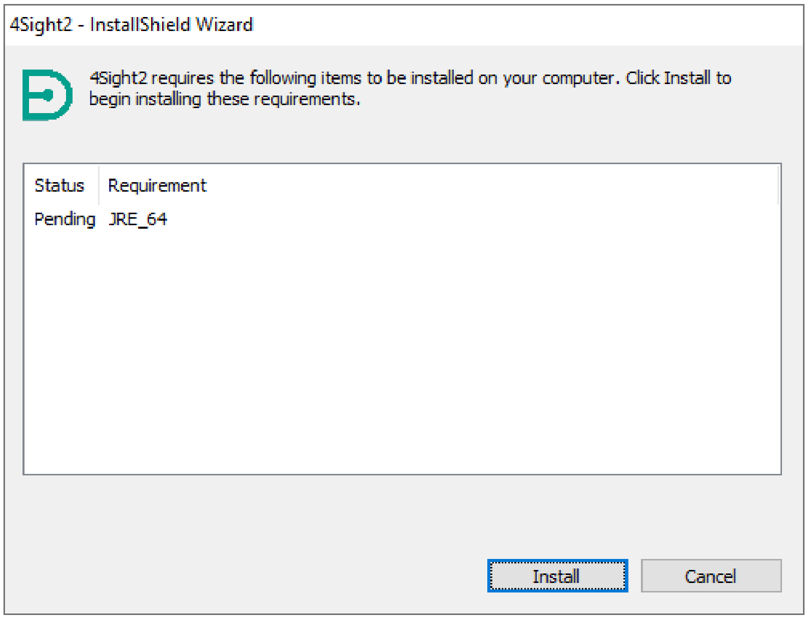
Follow the instruction from the InstallShield Wizard or use the following two sections to walk through the installation process.

1. If 4Sight2 is already installed on the machine, then the installation wizard will prompt you to perform an upgrade to a recent version. Click **Yes** to perform the recent upgrade.



This setup will perform an upgrade of '4Sight2'. Do you want to continue?

2. If 4Sight2 is installed for the first time on the machine, then the installation wizard will display the below screen. Select **Install** and the listed items displayed will be installed.

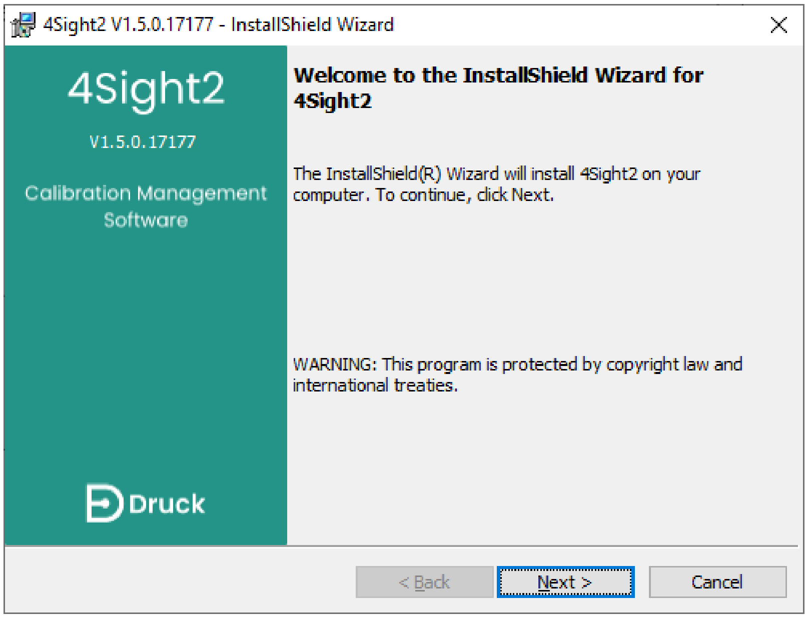


4Sight2 - InstallShield Wizard

4Sight2 requires the following items to be installed on your computer. Click Install to begin installing these requirements.

Status	Requirement
Pending	JRE_64

3. Once installation of any prerequisite items is complete, the InstallShield Wizard Welcome screen will be displayed. Click **Next** to continue.



4Sight2 V1.5.0.17177 - InstallShield Wizard

Welcome to the InstallShield Wizard for 4Sight2

The InstallShield(R) Wizard will install 4Sight2 on your computer. To continue, click Next.

WARNING: This program is protected by copyright law and international treaties.

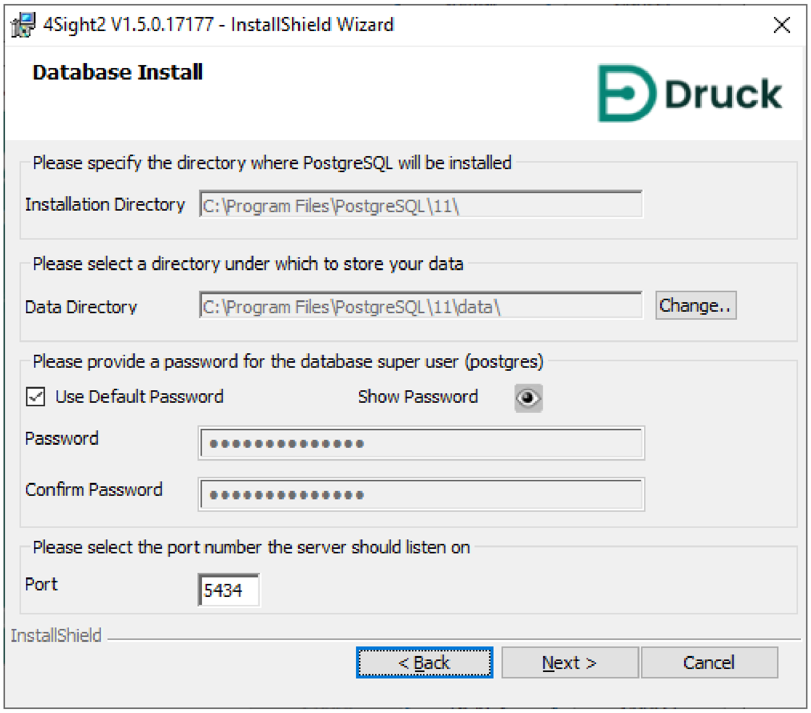
3.1 Database Installation

4Sight2 application uses a PostgreSQL database. Instructions are given below on how to install the PostgreSQL database and what to do if a PostgreSQL database is already installed.

3.2 PostgreSQL Installation

Follow this procedure if a PostgreSQL database is not installed on the machine.

1. If there is no instance of the PostgreSQL database installed on the machine, then the installation wizard will display the below screen.



4Sight2 V1.5.0.17177 - InstallShield Wizard

Database Install

Please specify the directory where PostgreSQL will be installed

Installation Directory: C:\Program Files\PostgreSQL\11\

Please select a directory under which to store your data

Data Directory: C:\Program Files\PostgreSQL\11\data\

Please provide a password for the database super user (postgres)

☑ Use Default Password

Password: •••••••••••••••

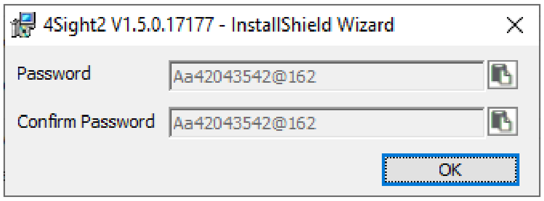
Confirm Password: •••••••••••••••

Please select the port number the server should listen on

Port: 5434

Installation Directory: Select the directory where PostgreSQL application can be installed.
Data Directory: Select the directory where the PostgreSQL database can be stored.
Password/ Confirm Password: Enter the password of the PostgreSQL database super user. This prompted only in case if PostgreSQL database is installed first time.
Note: This password will be required to access the database contents after the installation.
Port: This is the port address of the PostgreSQL database to satisfy application request.
Note: If the port number is already occupied, contact the IT team. User can also change the port number, which needs to be noted down to launch the application later.

Important: The user must make note of the database password. Loss of password information may result in denial of access or data loss. Uncheck the User Default Password checkbox to update the database super user password. If you wish to keep the default password or view the new password entered select the 👁 (Show Password) icon. To copy the password to the clip board, use the 📋 (Copy to Clipboard) icon.

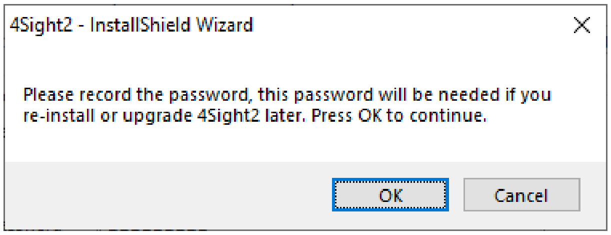


4Sight2 V1.5.0.17177 - InstallShield Wizard

Password: Aa42043542@162

Confirm Password: Aa42043542@162

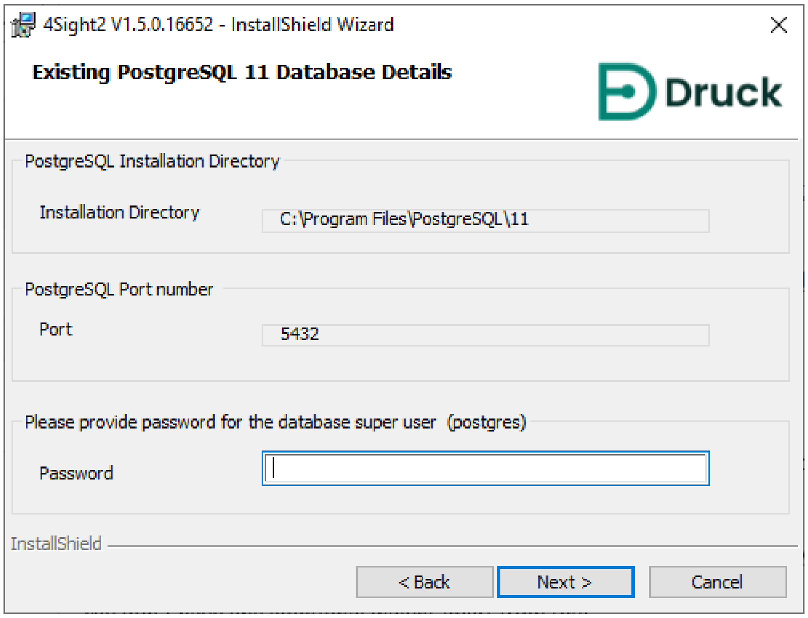
You will then be prompted to record the password again by the installer. Select **OK** once you have made a note of the password.



4Sight2 - InstallShield Wizard

Please record the password, this password will be needed if you re-install or upgrade 4Sight2 later. Press OK to continue.

2. This step will be shown to the user only in case the PostgreSQL database is already installed.



4Sight2 V1.5.0.16652 - InstallShield Wizard

Existing PostgreSQL 11 Database Details

PostgreSQL Installation Directory

Installation Directory: C:\Program Files\PostgreSQL\11

PostgreSQL Port number

Port: 5432

Please provide password for the database super user (postgres)

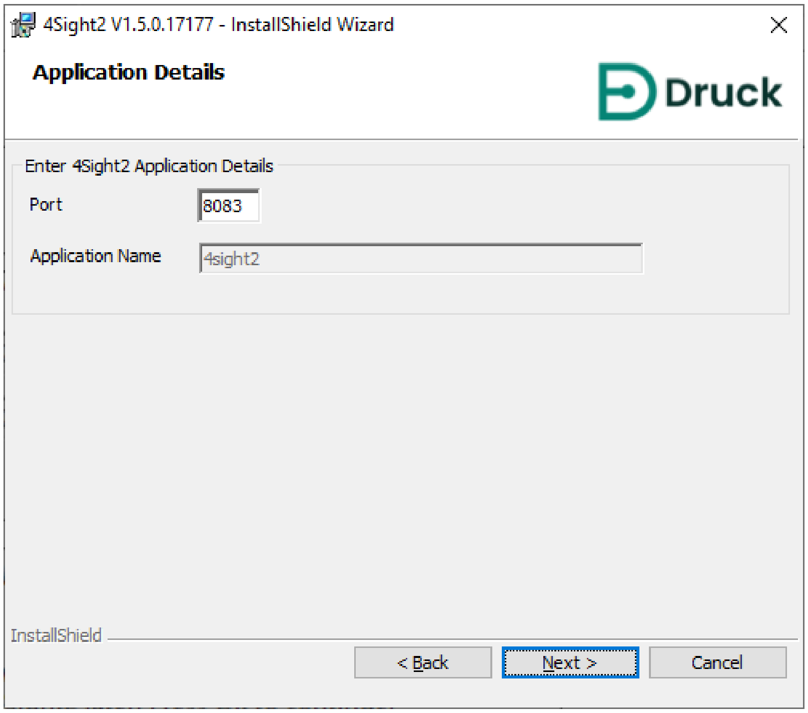
Password:

Installation Directory: This is to specify the path where the PostgreSQL is already installed. It is read-only information.

Password: This is to confirm the PostgreSQL database super user password.

Port: This is to specify the port number that PostgreSQL database is using to execute the db. request.

3. In the Application Details window, enter the below details



4Sight2 V1.5.0.17177 - InstallShield Wizard

Application Details

Enter 4Sight2 Application Details

Port: 8083

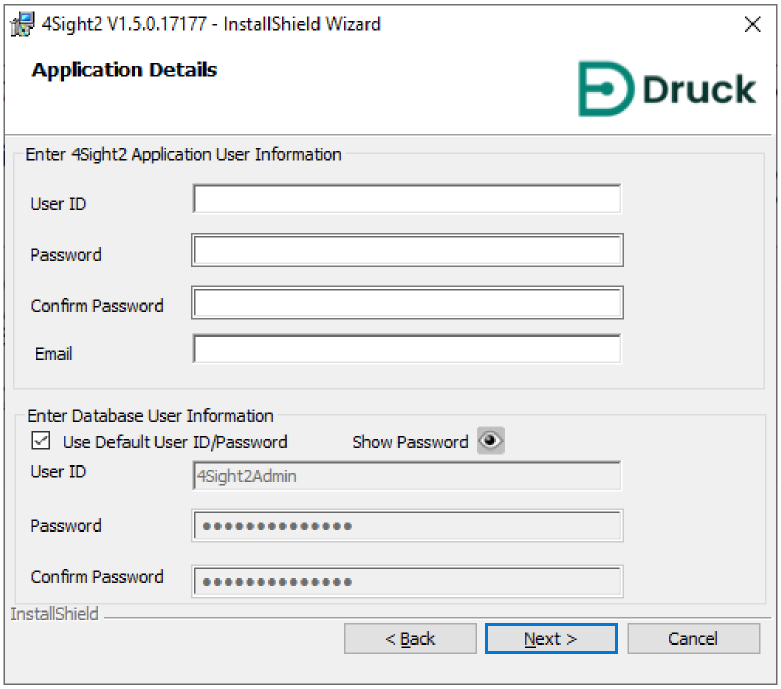
Application Name: 4sight2

Port: Enter the Tomcat web server port that is used by the 4Sight2 web application to respond to HTTP request.

Application Name: Enter the application Context path you will use to connect to the 4Sight2 application in your browser. By default, this is 4sight2.

Note: If the port number is already occupied, contact the IT team. User can also change the port number, which needs to be noted down to launch the application later.

4. Select **Next** and the Application User Information screen will be displayed.



4Sight2 V1.5.0.17177 - InstallShield Wizard

Application Details

Enter 4Sight2 Application User Information

User ID

Password

Confirm Password

Email

Enter Database User Information

☑ Use Default User ID/Password   Show Password

User ID: 4Sight2Admin

Password: ••••••••••••••

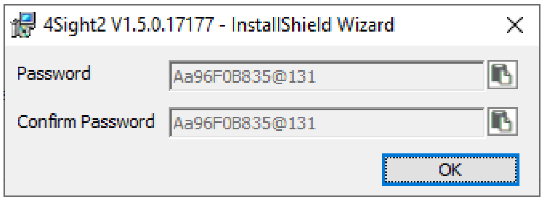
Confirm Password: ••••••••••••••

Application User Information: This section is to enter the super user name and password for accessing the 4Sight2 application.

Note: This password will be required to access the 4Sight2 application upon installation.

Database User Information: This section is to enter the database user name and password that will be used by the 4Sight2 application to communicate with PostgreSQL database.

⚠ **Important:** The user must make note of the database password. Loss of password information may result in denial of access or data loss. Uncheck the User Default Password checkbox to update the database super user password. If you wish to keep the default password or view the new password entered select the 👁 (Show Password) icon. To copy the password to the clip board, use the 📋 (Copy to Clipboard) icon.

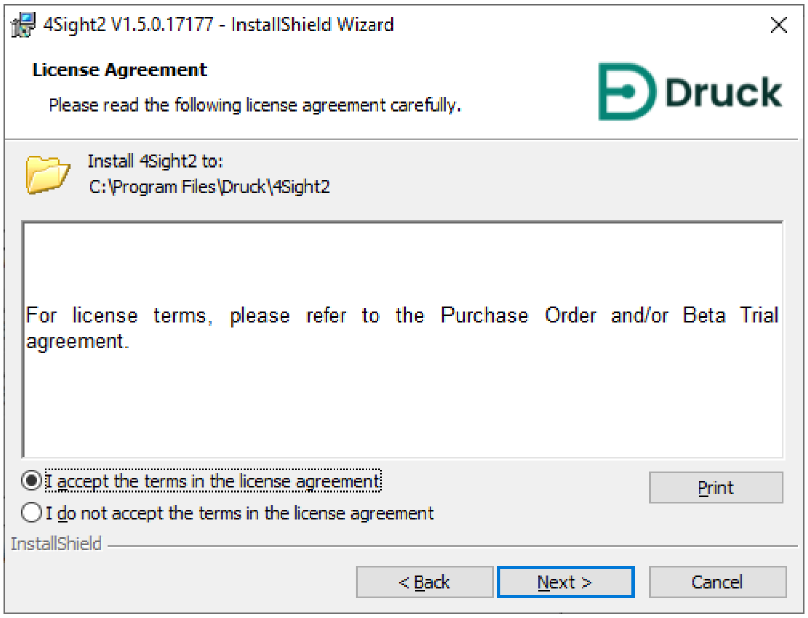


4Sight2 V1.5.0.17177 - InstallShield Wizard

Password: Aa96F0B835@131

Confirm Password: Aa96F0B835@131

5. After the license terms and condition are read, select the "I agree to the License terms and conditions." radio button and then click **Next**.



4Sight2 V1.5.0.17177 - InstallShield Wizard

License Agreement

Please read the following license agreement carefully.

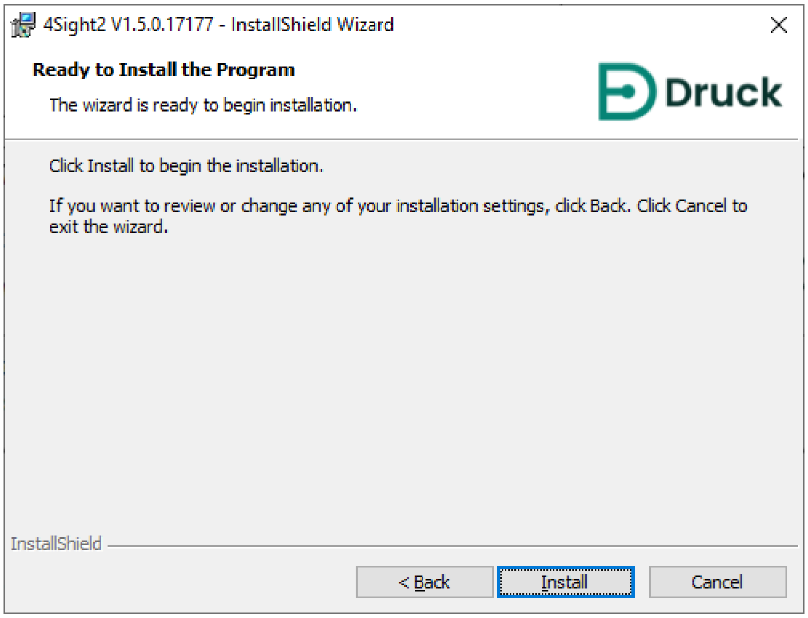
Install 4Sight2 to:
C:\Program Files\Druck\4Sight2

For license terms, please refer to the Purchase Order and/or Beta Trial agreement.

● I accept the terms in the license agreement

○ I do not accept the terms in the license agreement

6. Click **Install** to begin the installation. All the software packages related to the 4Sight2 application and the database will be installed.



4Sight2 V1.5.0.17177 - InstallShield Wizard

Ready to Install the Program

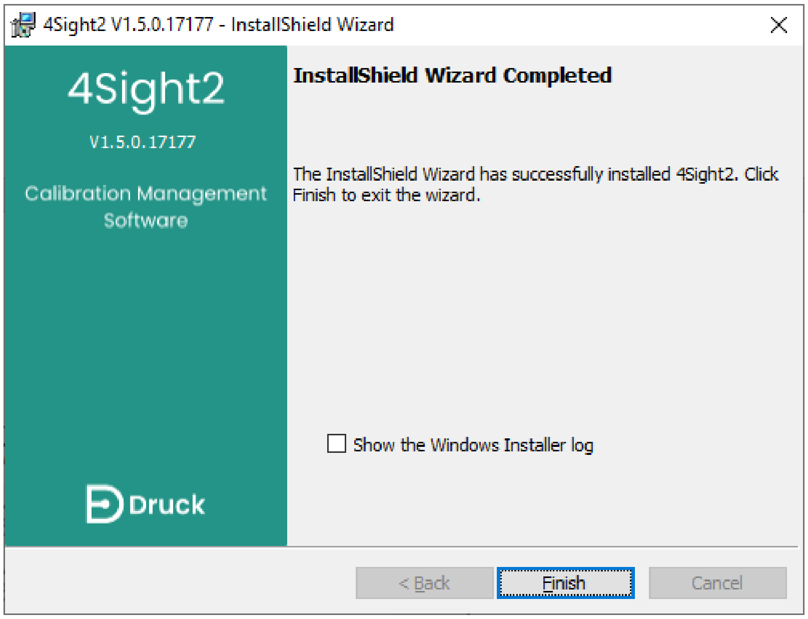
The wizard is ready to begin installation.

Click Install to begin the installation.

If you want to review or change any of your installation settings, click Back. Click Cancel to exit the wizard.

Congratulations the 4Sight2 application has now been setup.

7. Click **Finish** button to close the window and follow instructions in the next section to login to 4Sight2 application.



4Sight2 V1.5.0.17177 - InstallShield Wizard

InstallShield Wizard Completed

The InstallShield Wizard has successfully installed 4Sight2. Click Finish to exit the wizard.

□ Show the Windows Installer log

To log in to 4Sight2 on the server locally, go to

http://ComputerName or IPAddress:PortNo/ApplicationName

- **ComputerName –** The name of the PC where the 4Sight2 application has been installed. This can be located by right clicking on this PC and selecting properties.
- **IPAddress** – The IP address of the PC where the 4Sight2 application has been installed. This can be located by running 'ipconfig' in a Windows command window.

- **PortNo -** The number that was entered into the Tomcat Port Number field during application installation.
- **ApplicationName -** The name that was entered in the Application Name field during application installation.

4Sight2 Test Equipment Communicator Installation

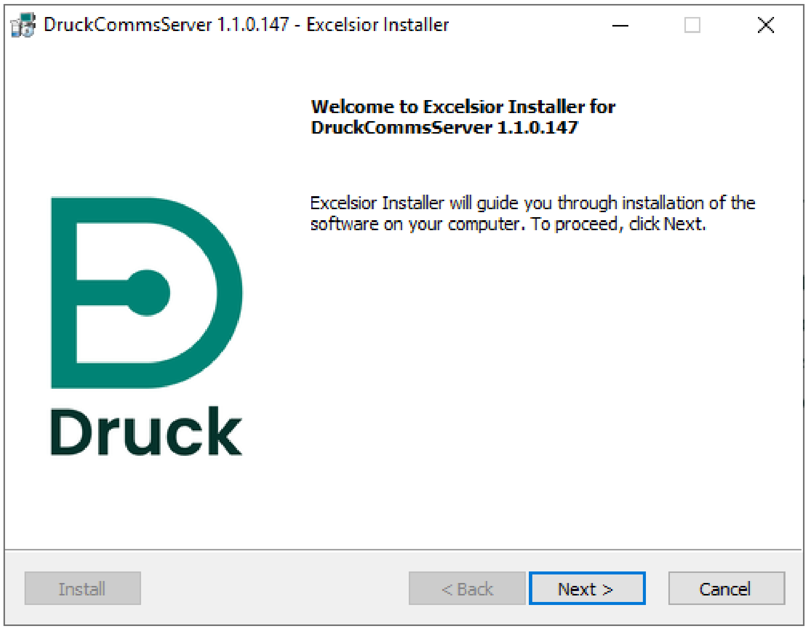
4. 4Sight2 Test Equipment Communicator Installation

1. The Test Equipment Communicator provides the means for your Druck instruments to communicate with the 4Sight2 application. The Test Equipment Communicator can either be installed from the 4Sight2 set up folder or can be downloaded via 4Sight2 initial device communication. If the Test Equipment Communicator is not available in the set-up file, once the 4Sight2 application is running and a range has been created, navigate to Calibration > Portable using the 4Sight2 menu as an administrative user, see 4Sight2 User Manual for navigation and range creation help. Select the refresh button next to the test equipment dropdown. If the Test Equipment Communicator is not running, you will see the following message:

   Unable to Communicate with Test Equipment

   Download the Test Equipment communicator package. After downloading, unzip and run setup.exe to install. For installation instructions or troubleshooting refer to the Installation Manual. Please contact Administrator for assistance.

2. Select **Download** to obtain the Test Equipment Communicator set up file.
3. The Test Equipment Communicator set up files will appear as a CommsServerInstall Zip file. Once the Comms Server Zip has downloaded, the same steps can be followed pre and post 4Sight2 installation.
4. Extract the files from the Comms Server Zip file and double click the setup.exe file to run the installer.
5. The DruckCommsServer installer will be displayed. Follow the instructions in the installer or follow this guide.

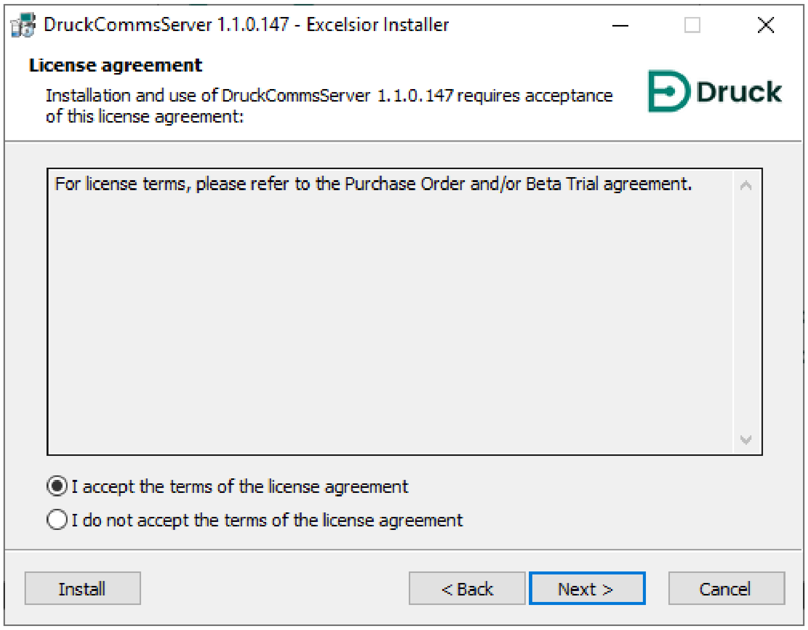


DruckCommsServer 1.1.0.147 - Excelsior Installer

Welcome to Excelsior Installer for DruckCommsServer 1.1.0.147

Excelsior Installer will guide you through installation of the software on your computer. To proceed, click Next.

6. Select **Next** to display the License agreement screen, read through the terms then select **I accept the terms of the license agreement**, then **Next** to continue.



DruckCommsServer 1.1.0.147 - Excelsior Installer

License agreement

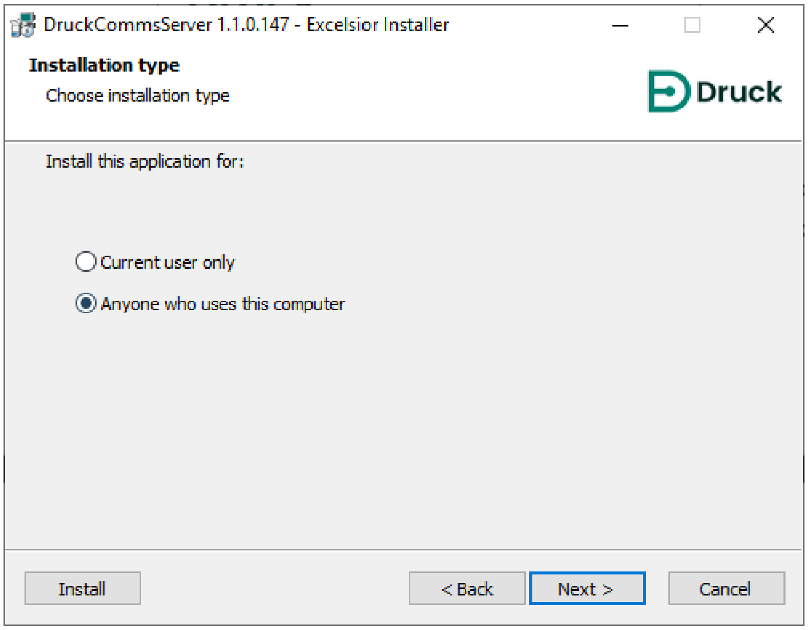
Installation and use of DruckCommsServer 1.1.0.147 requires acceptance of this license agreement:

For license terms, please refer to the Purchase Order and/or Beta Trial agreement.

● I accept the terms of the license agreement

○ I do not accept the terms of the license agreement

7. From the Installation type screen, select whether you want to install the CommsServer for all user of this PC or the current user only.



DruckCommsServer 1.1.0.147 - Excelsior Installer

Installation type

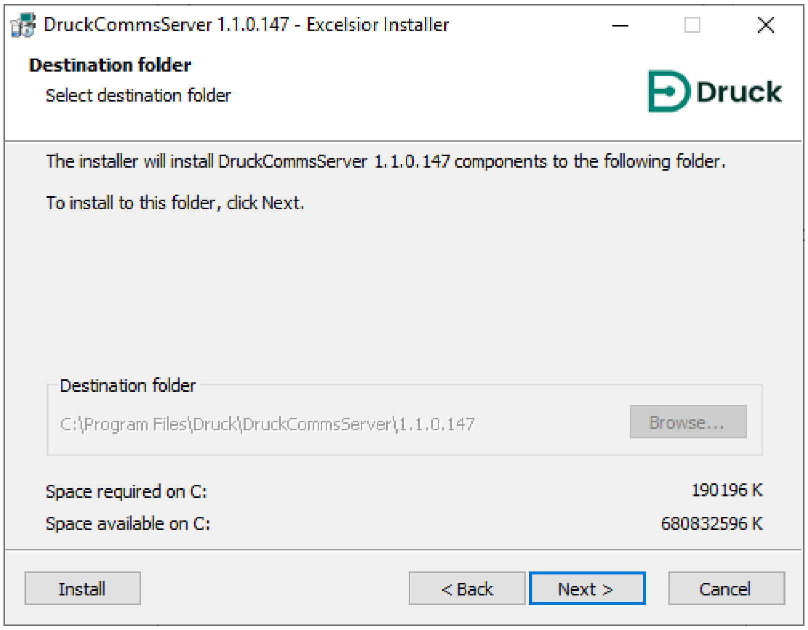
Choose installation type

Install this application for:

○ Current user only

● Anyone who uses this computer

8. The Destination folder screen displays the folder in which the DruckCommsServer will be installed. By default, this is C:\Program Files\Druck\DruckCommsServer\[application_version]



DruckCommsServer 1.1.0.147 - Excelsior Installer

Destination folder

Select destination folder

The installer will install DruckCommsServer 1.1.0.147 components to the following folder.

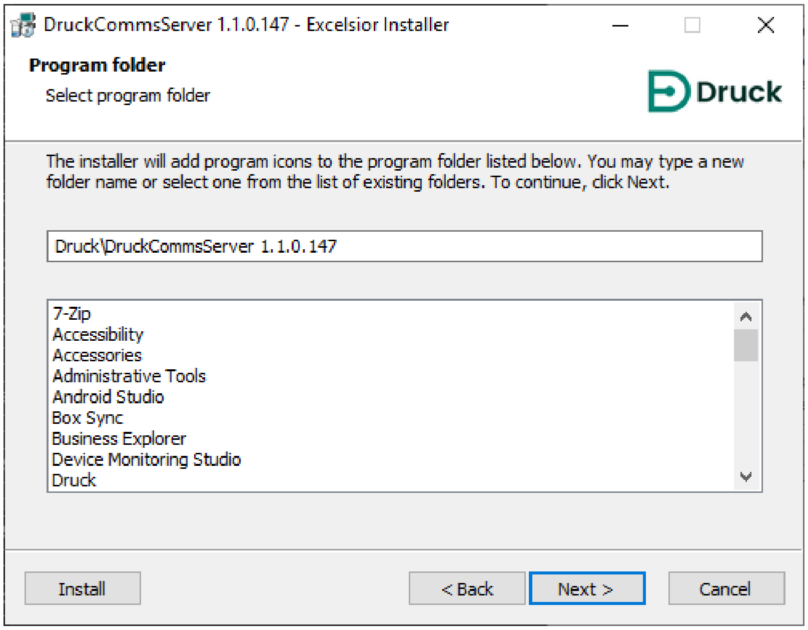
To install to this folder, click Next.

Destination folder: C:\Program Files\Druck\DruckCommsServer\1.1.0.147

Space required on C: 190196 K

Space available on C: 680832596 K

9. The Program Folder screen allows you to select where installer adds the program icon to the program folder.



DruckCommsServer 1.1.0.147 - Excelsior Installer

Program folder

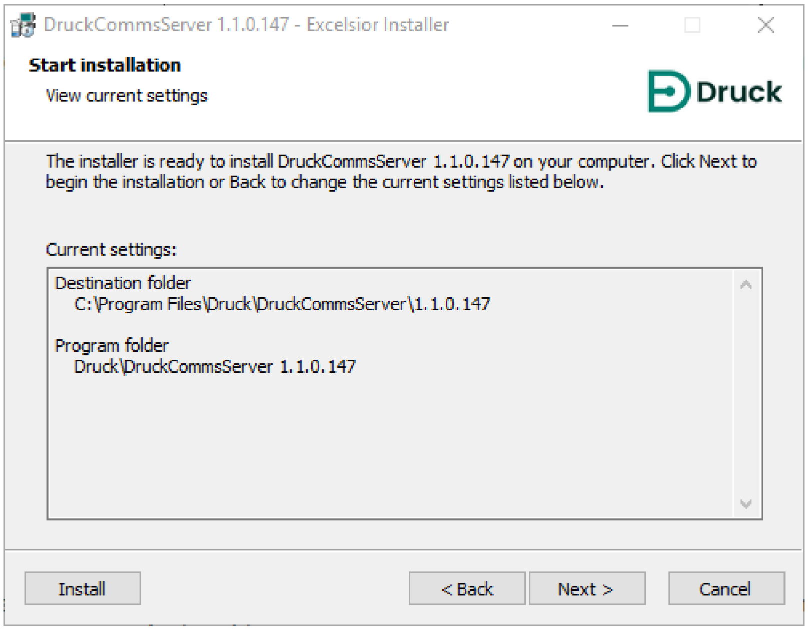
Select program folder

The installer will add program icons to the program folder listed below. You may type a new folder name or select one from the list of existing folders. To continue, click Next.

Druck\DruckCommsServer 1.1.0.147

7-Zip
Accessibility
Accessories
Administrative Tools
Android Studio
Box Sync
Business Explorer
Device Monitoring Studio
Druck

10. The start installation screen will then be displayed, select **Next** to start installation.



DruckCommsServer 1.1.0.147 - Excelsior Installer

Start installation

View current settings

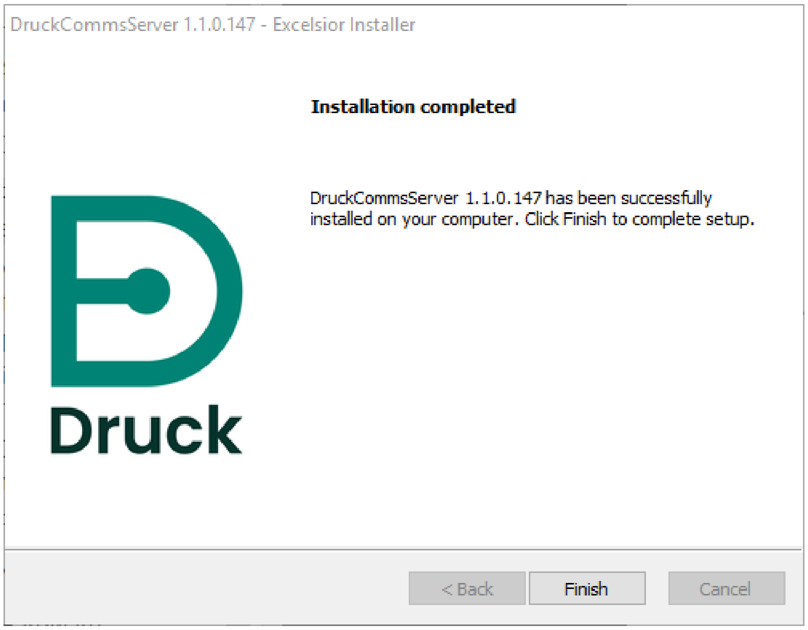
The installer is ready to install DruckCommsServer 1.1.0.147 on your computer. Click Next to begin the installation or Back to change the current settings listed below.

Current settings:

Destination folder
C:\Program Files\Druck\DruckCommsServer\1.1.0.147

Program folder
Druck\DruckCommsServer 1.1.0.147

11. Once Installation has completed, select **Finish**.

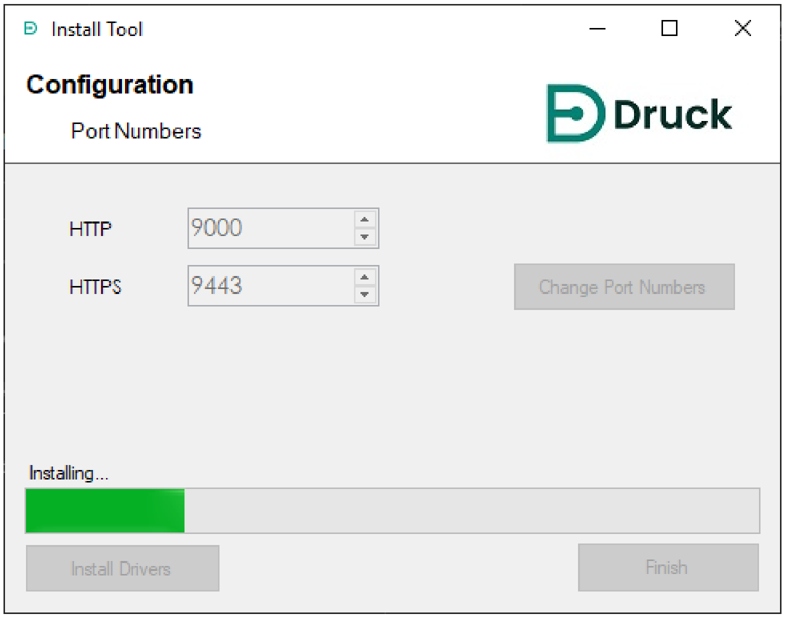


DruckCommsServer 1.1.0.147 - Excelsior Installer

Installation completed

DruckCommsServer 1.1.0.147 has been successfully installed on your computer. Click Finish to complete setup.

12. Next, the CommsServer install tool application will be displayed to install the additional drivers that are required.



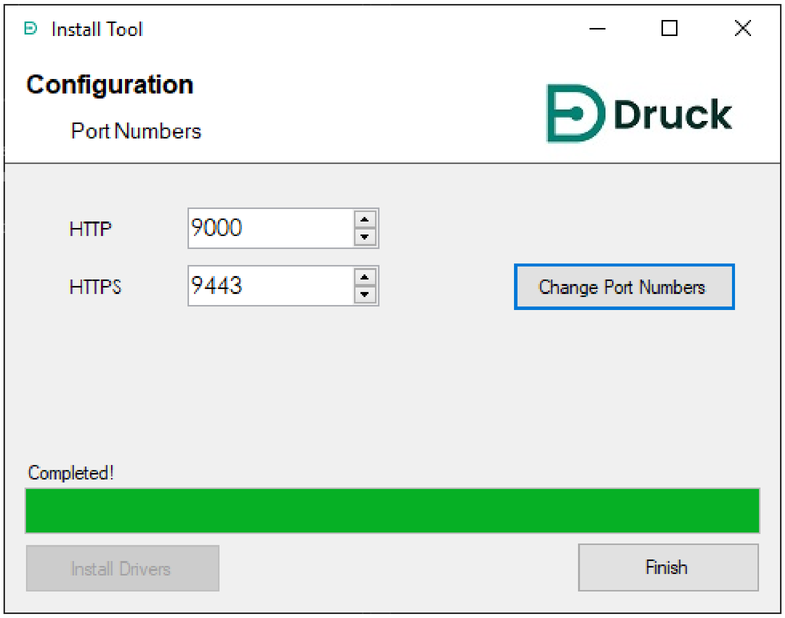
HTTP 9000

HTTPS 9443

Installing...

13. If you are unsure if alternative port number are being used by 4Sight2, please contact your administrative user

Note: The install tool can be run separately after install to reconfigure these port numbers. .



HTTP 9000

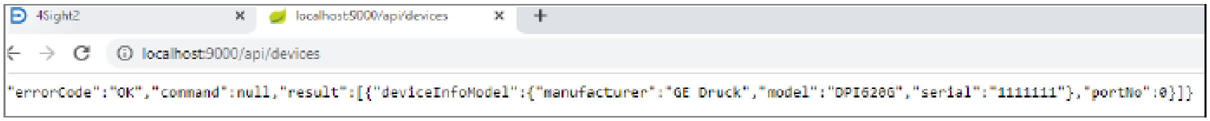
HTTPS 9443

Completed!

14. Test the Test Equipment Communicator installation by typing the following URL into your web browser:

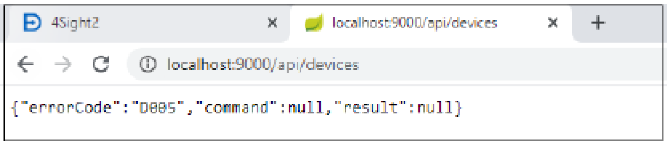
    http:/localhost:[http port number used above default 9000]/api/devices

The web browser should display list of any device you have connected:



```
"errorCode":"OK","command":null,"result":[{"deviceInfoModel":{"manufacturer":"GE Druck","model":"DPI620G","serial":"1111111"},"portNo":0}]}
```

If no devices are connected you should see the following



```
{"errorCode":"D005","command":null,"result":null}
```

Note: Drivers required for temperature calibrators will not be configured automatically. See section 4.3 Temperature Calibrator Driver Configuration

15. If device driver installation is unsuccessful, use the steps in the next section to manually configure the necessary drivers.

4.1 Manual Driver Configuration

IT security policy settings may prevent Druck drivers from auto-configuring on installation. This will be apparent if 4Sight2 is unable to communicate with the various equipment.

For the latest information, https://www.bakerhughes.com/druck/test-and-calibration-instrumentation/calibration-management-software-4sight2

or

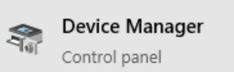
To resolve this issue, the Druck drivers may be configured manually. Please consult your local IT representative if you are unsure about this or require further assistance.

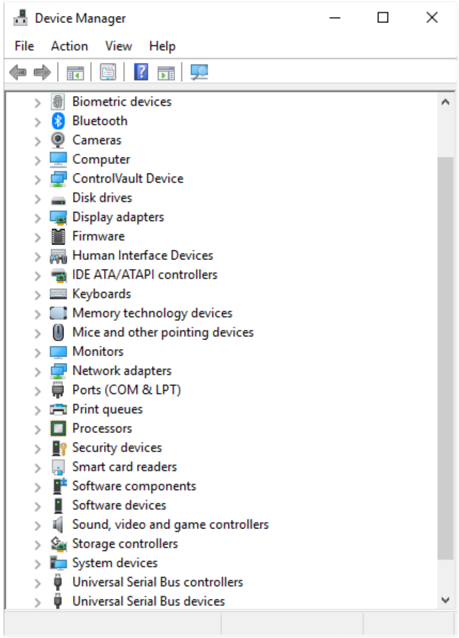
4.1.1 Prerequisites

To install the drivers, you need 4Sight2 application installed or accessible on/from the machine. Make sure you can login to 4Sight2 application from the computer before attempting to install the drivers.

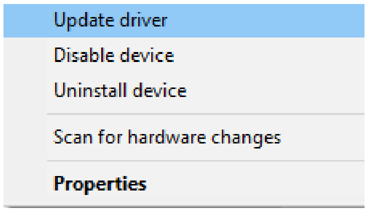
To install the driver manually perform the following steps,

1. On the Desktop, search for Device Manager and run.

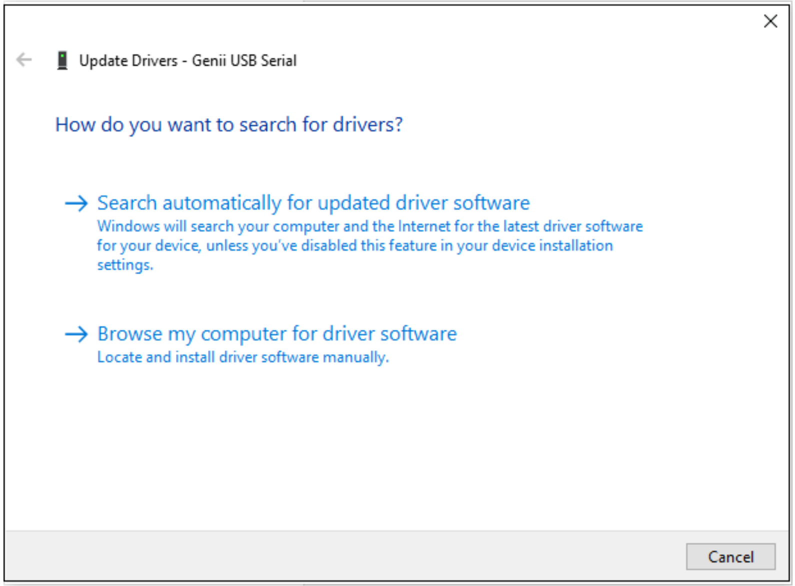




2. Scroll through the list of USB devices to find the devices that are not configured (Unknown Device or Other devices). Right click and select **Update Driver**.



3. Select **Browse my computer for driver software**.



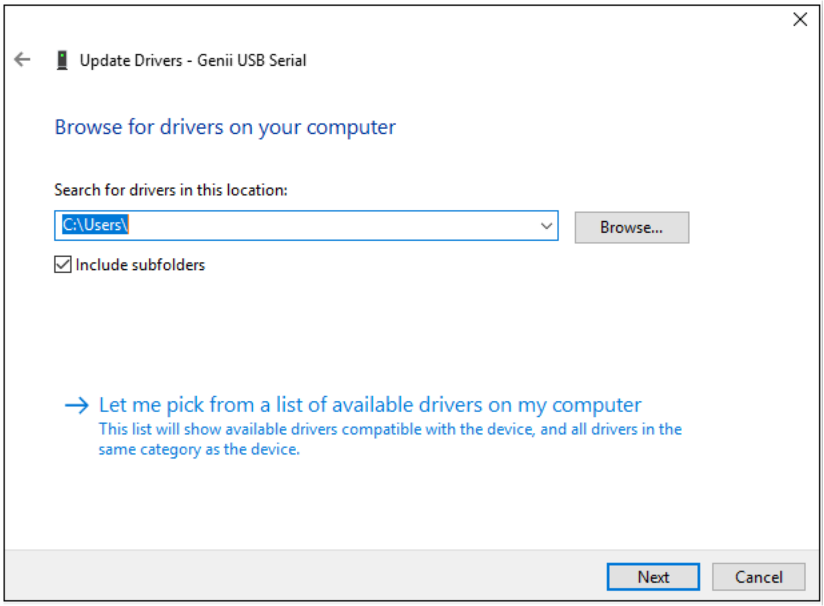
Update Drivers - Genii USB Serial

How do you want to search for drivers?

→ Search automatically for updated driver software
Windows will search your computer and the Internet for the latest driver software for your device, unless you've disabled this feature in your device installation settings.

→ Browse my computer for driver software
Locate and install driver software manually.

4. Select **Let me pick from a list of available drivers** on my computer.



Update Drivers - Genii USB Serial

Browse for drivers on your computer

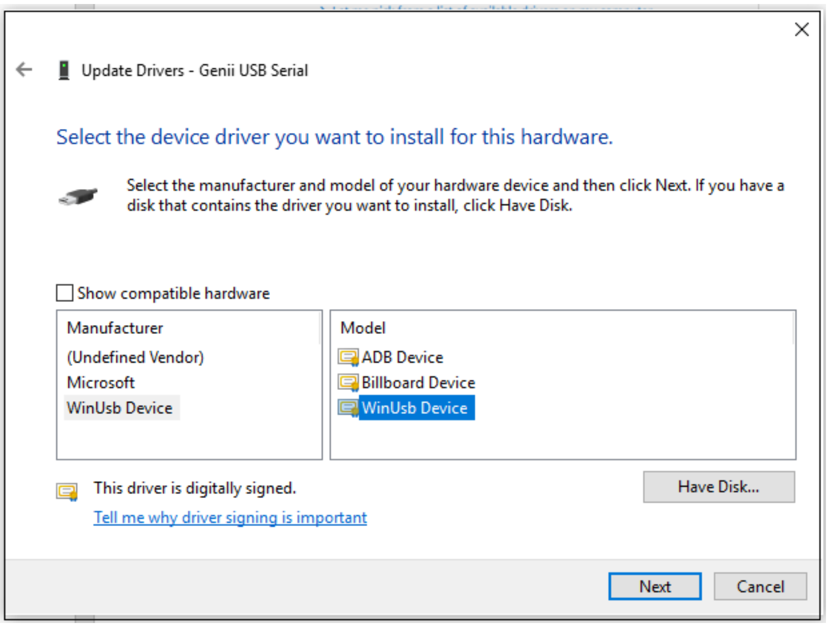
Search for drivers in this location:

C:\Users\

☑ Include subfolders

→ Let me pick from a list of available drivers on my computer
This list will show available drivers compatible with the device, and all drivers in the same category as the device.

5. Uncheck **Show compatible hardware** and select **WinUsb Device** for Manufacture and **WinUsb Device** for Model.



Update Drivers - Genii USB Serial

Select the device driver you want to install for this hardware.

Select the manufacturer and model of your hardware device and then click Next. If you have a disk that contains the driver you want to install, click Have Disk.

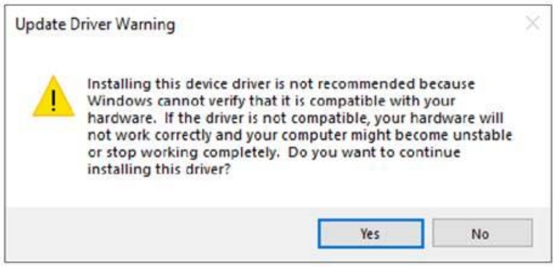
□ Show compatible hardware

Manufacturer	Model
(Undefined Vendor)	ADB Device
Microsoft	Billboard Device
WinUsb Device	WinUsb Device

This driver is digitally signed.

Tell me why driver signing is important

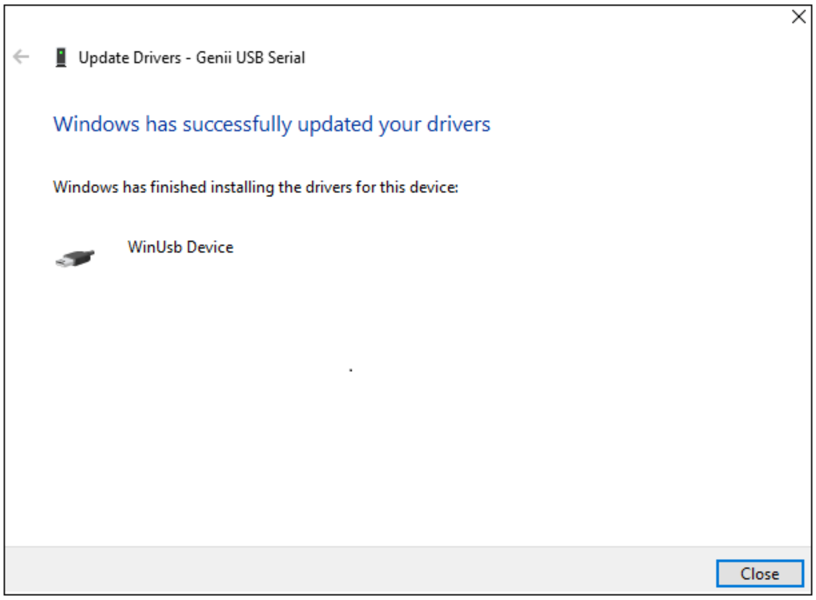
6. The following Warning will be displayed. Click **Yes**.



Update Driver Warning

Installing this device driver is not recommended because Windows cannot verify that it is compatible with your hardware. If the driver is not compatible, your hardware will not work correctly and your computer might become unstable or stop working completely. Do you want to continue installing this driver?

7. Windows has successfully updated your drivers will display.



Update Drivers - Genii USB Serial

Windows has successfully updated your drivers

Windows has finished installing the drivers for this device:

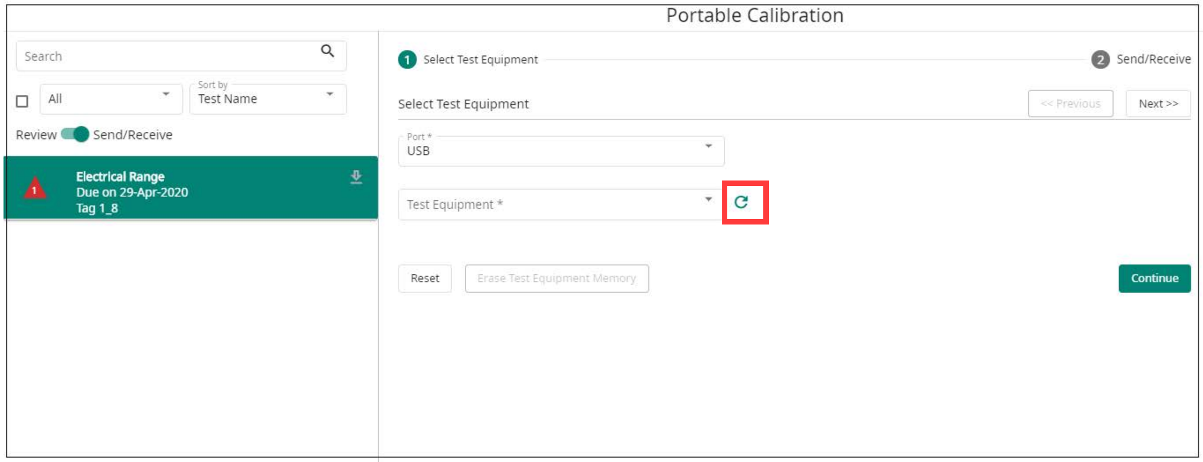
WinUsb Device

Repeat the above steps for each category of device when you connect the device for the first time.

For example, if you connect a PACE and Genii for the first time, you may have to repeat the above steps for PACE and Genii separately the first time. All further instances of all PACEs and Genii's should work without the need to perform these settings. However, if you connect a different category of device later such as a DPI611/612, you will need to repeat the steps again for this category of device.

4.2 Testing the Test Equipment Communicator

1. Login to 4Sight2 as a Technician.
2. Go to **Assets >> Worklist.**
3. Select one or more ranges and assign them to either Portable or Automated calibration work-flow.
4. Click on **Refresh** button.



Portable Calibration

Electrical Range
Due on 29-Apr-2020
Tag 1_8

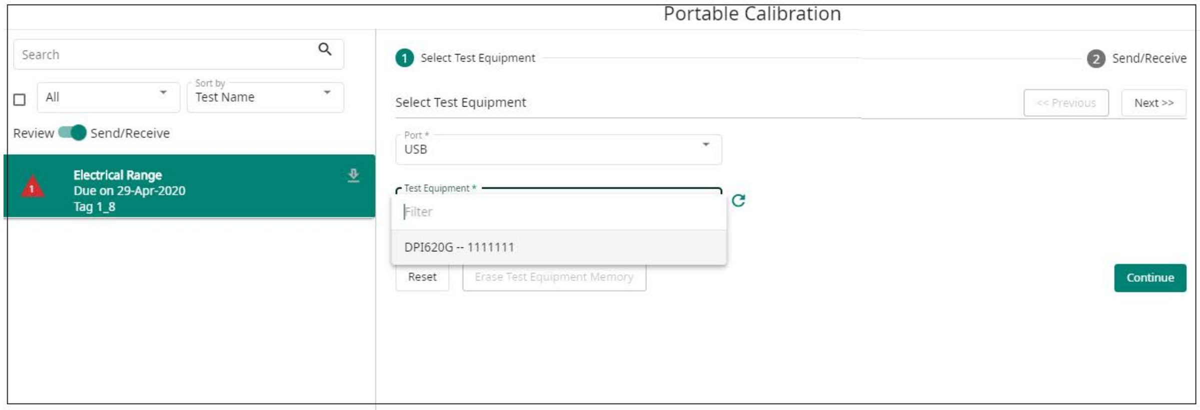
1 Select Test Equipment — 2 Send/Receive

Select Test Equipment

Port *: USB

Test Equipment *

5. Click on **Test Equipment** drop down. If you see the connected device in the list, then the Test Equipment Communicator is configured correctly.



Portable Calibration

Electrical Range
Due on 29-Apr-2020
Tag 1_8

1 Select Test Equipment — 2 Send/Receive

Select Test Equipment

Port *: USB

Test Equipment *

Filter

DPI620G -- 1111111

4.3 Temperature Calibrator Driver Configuration

In order to allow the Temperature Calibrator to communicate with 4Sight2 an FTDI driver must be installed.

1. Download the FTDI driver using this link: https://www.ftdichip.com/Drivers/VCP.htm.
2. Extract the downloaded file from the zip and save the file to a known location on your machine.
3. Navigate the windows Device Manager on your machine.
4. Select Ports (COM & LPT) from the list of devices, to view the temperature calibrator.
5. Right click the temperature calibrator and select update drivers.
6. Select Browse my computer for driver software.
7. Select Browse next to the search box titled Search for drivers in this location.
8. Select the folder extracted folder containing the driver download.
9. Select Next and then close.
10. The driver will now be installed.
11. To test communication with a temperature calibrator in 4Sight2, navigate automated calibration and check that the temperature calibrator can be selected as an Input Controller. Alternatively, re-run Step 14 from section 4.

Deployment Guide

5. Deployment Guide

5.1 Deployment Architecture

Typical architecture includes 4Sight2 web application and UAA (User Authentication and Authorization) server running inside the Tomcat Web Server with the PostgreSQL database running on the same machine.

The Browser Client Web Application will connect to the 4Sight2 server which in turn stores and retrieves the information from the PostgreSQL database.

5.2 Physical Deployment

We assume that the user installing 4Sight2 has Cyber Security Measures already in place meeting the user security policies, including the following:

- The server is placed in a secure location with physical limited access control.
- Server access control is protected with limited authorize access.
- Server network is protected with the firewall to allow limited access to the well-known applications only on known ports
- The applications run in their own context and have access to database and file systems in their own folder only.

5.3 Network

The clients are connected using Web Browsers, either through Ethernet connections or via a wireless network. There could be potential latency on the wireless network depending on the wireless bandwidth and number of devices connected.

It is advisable to disable or remove any browser plugins and extensions installed on the browser.

4Sight2 webserver should not be exposed to Internet, any access needed must be provided via Intranet or VPN.

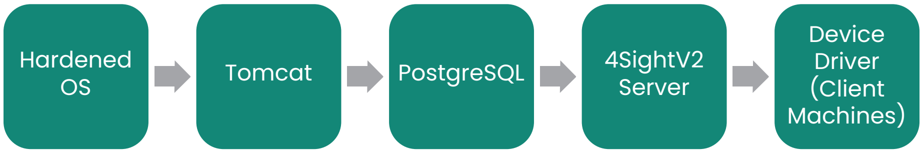
5.4 Deployment Sequence

PostgreSQL, Tomcat and Java Runtime are prerequisites to the 4Sight2 application. PostgreSQL is installed as a separate package while others are packaged along with the application. So if PostgreSQL is already installed on the user machine then we just need the Superuser password to connect and configure it.

The installation requires Windows administrator rights on the machine. Before the installation, the user must have the PostgreSQL superuser password. The Application administrator username & password and Database username & password.

PostgreSQL superuser password is required for creating the database and other structures inside the PostgreSQL server. The Application administrator is the first user of the application. They are responsible for creating other users and assigning them different roles. The Database user has access to 4Sight2 and UAA database. These username credentials are used for accessing the database.

The application is published on a machine port. The default port is 8083, and the user can change the port at the time of installation or later. The default application context in Tomcat is 4Sight2.



Follow the Operating System hardening procedure as per Microsoft or CIS guidelines to harden the OS. The installation procedure will guide the user to install PostgreSQL before installing the 4Sight2 server.

The Test Equipment Communicator is installed on the client machines when test equipment is connected via USB ports. If the Test Equipment Communicator is not already installed on the machine, the user is prompted to download the Test Equipment Communicator from the 4Sight2 server and install it on the machine. The Test Equipment Communicator listens to port 9000 and can only communicate on secure layer.

5.5 Post-Deployment Tasks

5.5.1 Adding User and Groups

The administrator is responsible for creating different users like Supervisor, Senior Technician, Technician, and Auditor in the application. The administrator can assign them to different built-in default groups. If more control or finer granularity of access is required, then administrator can create custom groups and assign specific access to them.

5.5.2 Default passwords

We are using the hardcoded default password for tomcat user in the file "C:\Program Files\Druck\4Sight2\<<latest folder number>>\apache-tomcat\conf\tomcat-user.xml".

It is recommended to change the default password and to always use a password which adheres to password best practices.

```
<role rolename="tomcat"/>
<user username="tomcat" password="P@55w0rd" roles="tomcat"/>
</tomcat-users>
```

Best practices have been implemented to ensure this application is secure. To achieve additional security please perform the following tasks:-

The configuration files and folders are protected with only Service and Systems having access rights by default. Therefore before attempting to perform the tasks below, the admin user only has read/write access to the C:\Program Files\Druck\4Sight2\<<latest folder number>>\apache-tomcat\conf folder, so open the command prompt with admin user credentials.

5.5.3 Secure Communications

This section provides instructions to configure 4sight2 in a secure mode (aka SSL mode) using a self-signed certificate. Please read the assumptions and terms and conditions defined in the 4Sight2 application before proceeding. A self-signed certificate is one way of enabling SSL in 4Sight2. Alternatively, a third-party CA certificate can be purchased from many vendors such as Symantec, Digicert and so on.

Note: By just enabling SSL does not necessarily make your application secure. This is one of the most common practices towards building a secure web application.

5.5.3.1 Assumptions and Warnings

Following assumptions are made for the below instructions to work:

⚠ OpenSSL for Windows software is required for generating Self-Signed Certificates. 4Sight2 assumes that your organisations, regional and national laws and regulatory guidelines allow you to use OpenSSL software.

- Keytool is a Key and Certificate management utility provided by Java which is used to generate various components involved in https configuration. 4Sight2 assumes that your organisations, regional and national laws and regulatory guidelines allow you to use Keytool utility.
- You need administrative privileges to perform below configurations. For more information on getting administrative rights, contact your local IT department.
- Below steps require basic understanding about computer process therefore ideally it is recommended that these steps be performed by or under the guidance of local IT.
- The content presented in this document such as host names, passwords, URLs and folder paths are for reference only. Ensure you modify the commands accordingly before execution.
- The following sections cover two scenarios. One is the Server and Client are on the same machine and the second the Server and Client are on different machines (i.e. A multiple Client scenario).

5.5.3.2 Steps to configure 4Sight2 Application in Https

1. Stop 4Sight2 from Windows Services
2. Open command prompt in **Admin Mode**
3. Navigate to the below folder within the 4Sight2 installation directory by executing command below,

   ```
   cd "C:\Program Files\Druck\4Sight2\<<latest folder number>>\apache-tomcat\conf"
   ```

4. Check if keytool is present by running the following command in the command prompt : **Keytool** -?

   If not, then Set environment path to JRE bin within 4Sight2 installation folder as shown below. Update the correct path based on installation folder.

   ```
   C:\Program Files\Druck\4Sight2\<<latest folder number>>\jre\bin
   Set "Path=%Path%;C:\Program Files\Druck\4Sight2\<<latest folder number>>\jre\bin"
   ```

5. For creating new certificate skip to point 6, otherwise if a certificate already exists do the following:

   a. Check if certificate file 4Sight.jks exists in java keystore

   ```
   keytool -list -alias <<hostname>> -storepass <<KeyPassword>> -keystore 4Sight.jks
   ```

   b. If certificate already installed, remove it,

   ```
   keytool -delete -noprompt -alias <<hostname>> -storepass <<KeyPassword>> -keystore 4Sight.jks
   ```

   c. Check and delete if 4SightV2PublicKey.cer exists,

   ```
   del "../../app/Certificate/4SightV2PublicKey.cer"
   ```

   d. Check certificate already exists in cacert of java.

   ```
   keytool -list -alias <<hostname>> -storepass changeit -keystore "../../jre/lib/security/cacerts"
   ```

   e. Delete certificate if exists in java store.

```
keytool -delete -noprompt -alias <<hostname>> -storepass changeit -keystore "../../
jre/lib/security/cacerts" -file "../../app/Certificate/4SightV2PublicKey.cer"
```

6. Create new certificate by executing below:

```
keytool -genkey -trustcacerts -keyalg "RSA" -keysize 2048 -validity 1095 -keypass
<<KeyPassword>> -alias <<hostname>> -keystore 4Sight.jks -storepass <<StorePassword>> -
dname "CN=%COMPUTERNAME%, OU=<<Organization Unit>>, O=<<Organization>>,
L=<<Location>>, S=<<State>>, C=<<Country Initial>>" -ext eku:critical=sa
```

7. Export the certificate to the file 4SightV2PublicKey.cer (Do not change name or path)

```
keytool -export -alias <<hostname>> -keystore 4Sight.jks -storepass <<StorePassword>> -
storetype JKS -file "C:\Program Files\Druck\4Sight2\<<latest folder
number>>\app\Certificate\4SightV2PublicKey.cer"
```

Once the command has successfully executed a message stating: "Certificate stored in file C:\Program Files\Druck\4Sight2\<<latest folder number>>\app\Certificate\4SightV2PublicKey.cer" will be displayed.

8. Import certificate into java CACert file.

```
keytool -import -noprompt -trustcacerts -alias <<hostname>> -storepass changeit -keystore
"../../jre/lib/security/cacerts" -file ../../app/Certificate/4SightV2PublicKey.cer
```

After successful command execute a message stating "Certificate was added to keystore" will be displayed.

9. Make entry of the certificate into Tomcat configuration file

   a. Open the server.xml file from below location.

   ```
   C:\Program Files\Druck\4Sight2\<<latest folder number>>\apache-
   tomcat\conf\server.xml"
   ```

   b. Make the following entry in server.xml.

   ```
   <Connector port="8443" protocol="org.apache.coyote.http11.Http11NioProtocol"
   maxThreads="150" SSLEnabled="true" sslProtocol="TLSv1.2" keystoreFile="conf/
   4Sight.jks"
   keystorePass="<<KeyPassword>>" keyAlias="tomcat" scheme="https" secure="true"
   clientAuth="false" />
   ```

   c. Comment the following section to disable http connections.

   ```
   <connectionTimeout="20000" maxSwallowSize="104857600" port="8083"
   protocol="HTTP/1.1" redirectPort="8443" relaxedPathChars="&quot;[\]^`{|}+"
   relaxedQueryChars="&quot;[\]^`{|}+"/>
   ```

Note: Application will not work if you do not comment this part.

10. At this point the 4Sight2 application Https configuration is complete.
11. To test the configurations done above, re-start 4Sight2 Service in Windows Service.
12. Open google chrome, clear browser cache and restart the browser.
13. Enter following URL in browser: https://<<host-name>>:8443/4sight2

- It may take longer time to load the URL the first time.
- Screen stating, "Your connection is not private" will be displayed
- Click on **Advanced** button >> **Proceed to XX** link.
- If you do not see 4sight2 screen, click **Reload** button.
- You will be redirected to 4sight2 page.

- There will be an "Not Secure" error in address bar which will eventually go away after registering certificate in mmc.

Not secure | ~~https~~://[redacted]:8443/4sight2/

5.5.3.3 Steps to configure DruckCommsServer in Https if Installed on the Server Machine

Replace values in << >> with suitable data before executing the command.

1. Stop DruckCommsServer from Windows Services.
2. Open command prompt in **Admin Mode**.
3. Check if keytool is present by running the following command in the command prompt: **Keytool -?**

   If not, then Set environment path to JRE bin within 4Sight2 installation folder as shown below. Update the correct path based on installation folder.

   ```
   C:\Program Files\Druck\4Sight2\<<latest folder number>>\jre\bin
   Set "Path=%Path%;C:\Program Files\Druck\4Sight2\<<latest folder number>>\jre\bin"
   ```
4. Navigate to the below folder within the DruckCommServer installation directory by executing command below,

   ```
   cd " C:\Program Files\Druck\DruckCommsServer\<< Communication Service version >>"
   ```
5. Check if a certificate already exists do the following:

   a. Check certificate already exists in cacert of java.

   ```
   keytool -list -alias tomcat -storepass changeit -keystore cacerts
   ```

   b. Delete certificate if exists in java store.

   ```
   keytool -delete -noprompt -alias tomcat -storepass changeit -keystore cacerts
   ```

   c. Delete the preconfigured certs from CommsServer that comes with default

   ```
   del 4Sight.jks
   del 4SightV2DeviceMngr.pfx
   ```
6. Create new certificate by executing below:

   ```
   keytool -genkey -trustcacerts -keyalg "RSA" -keysize 2048 -validity 1095 -keypass
   <<KeyPassword>> -alias tomcat -keystore CommServer.jks -storepass <<StorePassword>>
   dname "CN=localhost, OU=<<Organization Unit>>, O=<<Organization>>, L=<<Location>>,
   S=<<State>>, C=<<Country Initial>>" -ext eku:critical=sa
   ```
7. Export the certificate to the file DruckCommServer.cer

   ```
   keytool -export -alias tomcat -keystore CommServer.jks -storepass <<StorePassword>> -
   storetype JKS -file DruckCommServer.cer
   ```

   Once the command has successfully executed a message stating:
   "Certificate stored in file DruckCommServer.cer " will be displayed.
8. Import comm server certificate into java CACert file.

   ```
   keytool -import -noprompt -trustcacerts -alias tomcat -storepass changeit -keystore
   cacerts -file DruckCommServer.cer
   ```

   After successful command execute a message stating "Certificate was added to keystore" will be displayed.

9. Import 4Sight certificate into java CACert file.

   keytool -import -noprompt -trustcacerts -alias <<server hostname>> -storepass changeit -keystore cacerts -file "C:\Program Files\Druck\4Sight2\<<latest folder number>>\app\Certificate\4SightV2PublicKey.cer"
   After successful command execute a message stating "Certificate was added to keystore" will be displayed.

10. Edit the key-store password for application.properties in DruckCommsServer.

    Open this file:
    C:\Program Files\Druck\DruckCommsServer\<<Communication Service Version>>\application.properties and change the following line:
    keystore = CommServer.jks
    key-store.password= << StorePassword >>
    Note: **<< StorePassword >>** referring to the **StorePassword** used in step 6.

11. Restart 4Sight2 and DruckCommsServer services.

5.5.3.4 Steps to Configure DruckCommsServer in HTTPs if Installed on a Client Machine

1. Keytool utility is packaged with Java so you can install Java on your machine or check for availability of java keytool directly without installation of Java.
2. Stop DruckCommsServer from Windows Services.
3. Open command prompt in **Admin Mode**.
4. Check if keytool is present by running the following command in the command prompt: **Keytool -?**

   If not, then Set environment path to JRE bin if you installed java on machine or can set path to keytool as shown below.
   Update the correct path based on installation folder.
   C:\Program Files\Java\<< Java version >>\bin
   Set Path=%Path%; "C:\Program Files\Java\<< Java version >>\bin"

5. Get the **4SightV2PublicKey.cer** file from Server machine where 4Sight application installed. This file is located on server as below,

   C:\Program Files\Druck\4Sight2\<<latest folder number>>\app\Certificate\4SightV2PublicKey.cer

6. Copy this **4SightV2PublicKey.cer** into following path:

   C:\Program Files\Druck\DruckCommsServer\<< Communication Service version >>

7. Now Follow steps 4 to 8 in section 5.5.3.3.
8. Import 4Sight certificate into java CACert file.

   keytool -import -noprompt -trustcacerts -alias <<server hostname>> -storepass changeit -keystore cacerts -file 4SightV2PublicKey.cer
   After successful command execute a message stating "Certificate was added to keystore" will be displayed.

9. Now Follow steps 10 to 11 in section 5.5.3.3.

5.5.3.5 Steps to generating Self-signed certificate for 4Sight2

1. Download and install Open SSL for Windows.
2. Stop 4Sight2 services from Windows Services.
3. Create a new folder called **4Sight2Certificate** inside C drive.

   You can choose any location or folder name provided you have administrative access to that folder.
4. Create a new file inside above folder in notepad and save the file as **openssl-ca.cnf**

   copy below contents to the file and save the file.

```
HOME          = .
RANDFILE       = $ENV::HOME/.rnd

############################################################
############
[ ca ]
default_ca    = CA_default     # The default ca section

[ CA_default ]
base_dir      = .
certificate   = $base_dir/cacert.pem   # The CA certifcate
private_key   = $base_dir/cakey.pem    # The CA private key
new_certs_dir = $base_dir              # Location for new certs after signing
database      = $base_dir/index.txt    # Database index file
serial        = $base_dir/serial.txt   # The current serial number

unique_subject = no  # Set to 'no' to allow creation of
                # several certificates with same subject.

default_days     = 1000        # How long to certify for
default_crl_days = 30          # How long before next CRL
default_md       = sha256      # Use public key default MD
preserve         = no          # Keep passed DN ordering

x509_extensions = ca_extensions # The extensions to add to the cert

email_in_dn     = no           # Don't concat the email in the DN
copy_extensions = copy         # Required to copy SANs from CSR to cert

############################################################
############
[ req ]
default_bits       = 4096
default_keyfile    = cakey.pem
distinguished_name = ca_distinguished_name
x509_extensions    = ca_extensions
string_mask        = utf8only
############################################################
############
[ ca_distinguished_name ]
countryName         = Country Name (2 letter code)
countryName_default = US

stateOrProvinceName         = State or Province Name (full name)
stateOrProvinceName_default = Maryland

localityName             = Locality Name (eg, city)
localityName_default     = Baltimore
```

```
organizationName          = Organization Name (eg, company)
organizationName_default    = Test CA, Limited

organizationalUnitName       = Organizational Unit (eg, division)
organizationalUnitName_default = Server Research Department

commonName       = [Company Name]
commonName_default = Test CA

emailAddress       = Email Address
emailAddress_default = test@example.com

########################################################
############
[ ca_extensions ]

subjectKeyIdentifier   = hash
authorityKeyIdentifier = keyid:always, issuer
basicConstraints       = critical, CA:true
keyUsage             = keyCertSign, cRLSign

########################################################
############
[ signing_policy ]
countryName           = optional
stateOrProvinceName    = optional
localityName          = optional
organizationName       = optional
organizationalUnitName = optional
commonName            = supplied
emailAddress          = optional

########################################################
############
[ signing_req ]
subjectKeyIdentifier   = hash
authorityKeyIdentifier = keyid,issuer
basicConstraints       = CA:FALSE
keyUsage             = digitalSignature, keyEncipherment
```

Note: Update **[Company Name]** above and save the file. This is the certificate issuers name that will appear in management console.

5. Create a new file inside above folder in notepad and save the file as **openssl-server.cnf** copy below contents to the file and save the file.

```
HOME          = .
RANDFILE       = $ENV::HOME/.rnd

########################################################
############
[ req ]
default_bits      = 2048
default_keyfile    = serverkey.pem
distinguished_name = server_distinguished_name
req_extensions     = server_req_extensions
string_mask        = utf8only

########################################################
############
[ server_distinguished_name ]
countryName        = Country Name (2 letter code)
countryName_default = US

stateOrProvinceName        = State or Province Name (full name)
stateOrProvinceName_default = MD

localityName        = Locality Name (eg, city)
localityName_default = Baltimore

organizationName          = Organization Name (eg, company)
organizationName_default    = Test Server, Limited

commonName          = [Hostname of server]
commonName_default   = Test Server

emailAddress        = Email Address
emailAddress_default = test@example.com

########################################################
############
[ server_req_extensions ]

subjectKeyIdentifier = hash
basicConstraints     = CA:FALSE
keyUsage           = digitalSignature, keyEncipherment
subjectAltName       = @alternate_names
nsComment          = "OpenSSL Generated Certificate"

########################################################
############
[ alternate_names ]
```

```
DNS.1 = [Hostname of server]

# IPv4 localhost
IP.1     = [IP Address of server]

# IPv6 localhost
IP.2     = ::1
```

Note: Update Hostname and IPv4 address above and save the file.

6. Open command prompt with Administrative privileges.
7. Navigate to 4Sight2Certificate folder by executing below,

   ```
   cd "<<full path to 4Sight2Certificate >>"
   ```

8. Set OpenSSL bin folder path variable by executing below command.

   ```
   Set path=%path%;"<<bin folder of openssl>>"
   ```

   Example default path:

   ```
   Set Path=%Path%;"C:\Program Files\OpenSSL-Win64\bin"
   ```

9. Set JRE bin folder path variable by executing below command. Note: below path may be different.

   ```
   Set path=%path%;"C:\Program Files\Druck\4Sight2\<<latest folder number>>\jre\bin"
   ```

10. Execute below command to generate cacert.pem and cakey.pem files

    ```
    openssl req -x509 -config openssl-ca.cnf -newkey rsa:4096 -days <<Number of days>> -sha256 -nodes -out cacert.pem -outform PEM
    ```

    Enter correct certificate data when prompted for e.g. country, state etc.

11. Execute below commands to generate servercert.csr and serverkey.pem files

    ```
    openssl req -config openssl-server.cnf -newkey rsa:2048 -days <<Number of days>> -sha256 -nodes -out servercert.csr -outform PEM
    ```

    Enter correct certificate date when prompted for e.g. country, state etc.

12. Create a new file in notepad and name it as index.txt. Save the file in 4Sight2Certificate folder.
13. Create a new file in notepad and name it as serial.txt. Save the file in 4Sight2Certificate folder.

    Open the file and enter **01** Save and close the file.

14. Execute below command to generate new certificates in the files servercert.pem and serverkey.pem.

    ```
    openssl ca -config openssl-ca.cnf -policy signing_policy -extensions signing_req -out servercert.pem -infiles servercert.csr
    ```

    Enter Y to commit the changes. you will see Database updated after successfully execution.

15. Package existing key files to PFX format by executing below command.

    ```
    openssl pkcs12 -export -in servercert.pem -inkey serverkey.pem -certfile cacert.pem -name "<<hostname>>" -out <<hostname>>.p12
    ```

    you will be prompted to enter password twice.

16. Convert PFX store into Java key store sorted by JRE bin location referred above i.e. tomcat/config path.

```
keytool -importkeystore -srckeystore <<hostname>>.p12 -srcstoretype PKCS12 -destkeystore "C:\Program Files\Druck\4Sight2\<<latest folder number>>\apache-tomcat\conf\4Sight.jks"   -deststoretype jks
```

Note: Keep password same for both stores. Make sure you point to 4Sight.jks present in config folder of tomcat as shown above.
You will be prompted to enter destination keystore password and source keystore password. After successful command execution you will see "Import command completed: 1 entries successfully imported" message.

17. Export certificate from java key store to file at:

    C:\Program Files\Druck\4Sight2\<<latest folder number>>\app\Certificate\4SightV2PublicKey.cer

    ```
    keytool -export -alias <<hostname>>  -keystore  "C:\Program Files\Druck\4Sight2\<<latest folder number>>\apache-tomcat\conf\4Sight.jks" -storePass “<<password>>” -storetype JKS -file "C:\Program Files\Druck\4Sight2\<<latest folder number>>\app\Certificate\4SightV2PublicKey.cer"
    ```

    Note: Make sure you point to 4Sight.jks present in config folder of tomcat as shown above.
    You will get Certificate stored in file message after successful execution,

18. Import certificate file into cacerts folder within 4sight2 installation directory.

    Note: path may vary depending up on installation directory and 4sight2 version

    ```
    keytool -import -noprompt -trustcacerts -alias <<hostname>> -storepass changeit -keystore "C:\Program Files\Druck\4Sight2\<<latest folder number>>\jre\lib\security\cacerts" -file "C:\Program Files\Druck\4Sight2\<<latest folder number>>\app\Certificate\4SightV2PublicKey.cer"
    ```

    Note: for some reason the alias you are trying to create already exists, run below command to first delete it and then execute above to create a new alias:

    ```
    keytool -delete -noprompt -trustcacerts -alias <<hostname>> -storepass changeit -keystore "C:\Program Files\Druck\4Sight2\<<latest folder number>>\jre\lib\security\cacerts" -file "C:\Program Files\Druck\4Sight2\<<latest folder number>>\app\Certificate\4SightV2PublicKey.cer"
    ```

    you will receive "Certificate was added to keystore" message after successful execution of this command.

19. Make the following change in server.xml file (exist in C:\Program Files\Druck\4Sight2\<<latest folder number>>\apache-tomcat\conf).

    a. Make the following entry in server.xml.

    ```
    <Connector port="8443"
    protocol="org.apache.coyote.http11.Http11NioProtocol"
    maxThreads="150"
    SSLEnabled="true"
    sslProtocol="TLSv1.2"
    keystoreFile="conf/4Sight.jks"
    keystorePass="<<KeyPassword>>"
    keyAlias="<<Host name>>"
    scheme="https"
    secure="true"
    clientAuth="false" />
    ```

b. Comment the following section to disable http connections.

```
<connectionTimeout="20000" maxSwallowSize="104857600" port="8083"
protocol="HTTP/1.1" redirectPort="8443" relaxedPathChars="&quot;[\]^`{|}+"
relaxedQueryChars="&quot;[\]^`{|}+"/>
```

20. This completes the https configuration for 4Sight2. So now Start the 4sight2 service from windows services.

5.5.3.6 Steps to Configure Self-Signed Certificate for DruckCommsServer if Installed on Server Machine

Here we assumed that you are successfully converted 4sight2 application into HTTPs by executing steps in section 5.5.3.5 and you already have files below in **4Sight2Certificate** folder:

- openssl-server.cnf
- openssl-ca.cnf
- cacert.pem
- cakey.pem
- index.txt
- serial.txt
- 4SightV2PublicKey.cer (This file can be located into C:\Program Files\Druck\4Sight2\<<latest folder number>>\app\Certificate folder)

1. Create a new folder as **CommserverCertificate** and copy the files above and make changes as below:

- openssl-server.cnf

  Under **req** section change the **default_keyfile** value as "**DruckCommServerCertKey.pem**".

    - Under **server_distinguished_name** change the **commonName** value to "**localhost**".
    - Under **alternate_names** change the **DNS.1** value to "**localhost**".
    - Under **alternate_names** change the **IP.1** value to "**127.0.0.1**"
    - Save the file.
- openssl-ca.cnf. (Do not change anything inside)
- cacert.pem. (Do not change anything inside)
- index.txt (Delete all the contents inside, make it empty file)
- serial.txt (Delete all the contents inside and make only entry of 01 inside)

2. Stop the DruckCommsServer service from Windows Services.
3. Open command prompt with Administrative privileges.
4. Navigate to **CommserverCertificate** folder by executing below,

```
cd "<<full path to CommserverCertificate >>"
```

5. Set OpenSSL bin folder path variable by executing below command.

```
Set path=%path%;"<<bin folder of openssl>>"
```

   Example default path:

```
Set Path=%Path%;"C:\Program Files\OpenSSL-Win64\bin"
```

6. Set JRE bin folder path variable by executing below command. Note: below path may be different,

```
Set path=%path%;"C:\Program Files\Druck\4Sight2\<<latest folder number>>
\jre\bin"
```

7. After finish this, create a Comm Server certificate request by following command

   ```
   openssl req -config openssl-server.cnf -newkey rsa:2048 -sha256 -nodes -out
   DruckCommServer.csr -outform PEM
   ```

   After this command executes, you will have a request in **DruckCommServer.csr** and a private key in **DruckCommServerCertKey.pem**

8. Then, perform the following to sign the csr request with your ca:

   ```
   openssl ca -config openssl-ca.cnf -policy signing_policy -extensions signing_req -out
   DruckCommServerCert.pem -infiles DruckCommServer.csr
   ```

9. After this, Create an PFX file with alias **tomcat** for comm server by following command,

   ```
   openssl pkcs12 -export -in DruckCommServerCert.pem -inkey
   DruckCommServerCertKey.pem -certfile cacert.pem -name "tomcat" -out
   DruckCommServer.pfx
   ```

10. Convert the PFX store into Java keystore using keytool

    Note: Keep the password same for both the keystore.

    ```
    keytool -importkeystore -srckeystore DruckCommServer.pfx -srcstoretype PKCS12 -
    destkeystore CommServer.jks -deststoretype jks
    ```

11. Now import the certificate into cacert .

    a. Now delete the existing tomcat alias which comes with installation by default

    ```
    keytool -delete -noprompt -trustcacerts -alias tomcat -storepass changeit -keystore
    "C:\Program Files\Druck\DruckCommsServer\<< Communication Service version
    >>\cacerts"
    ```

    b. After deleting existing alias tomcat then import the certificate into cacerts by,

    ```
    keytool -import -noprompt -trustcacerts -alias tomcat -storepass changeit -keystore
    "C:\Program Files\Druck\DruckCommsServer\<< Communication Service version
    >>\cacerts" -file DruckCommServerCert.pem
    ```

12. Now we need to import 4sight public key into comm server cacert for communication authentication so to do that execute below command,

    ```
    keytool -import -noprompt -trustcacerts -alias <<4sight server hostname>> -storepass
    changeit -keystore "C:\Program Files\Druck\DruckCommsServer\<< Communication
    Service version >>\cacerts" -file "C:\Program Files\Druck\4Sight2\<<latest folder number>>
    \app\Certificate\4SightV2PublicKey.cer"
    ```

13. After finish all above You will have **DruckCommServer.pfx** and **CommServer.jks** in current **CommserverCertificate** folder.

    Copy those files and paste it into "C:\Program Files\Druck\DruckCommsServer\<< Communication Service version >>\" directory. And edit the **application.properties** from same location, Change the property's value as below

    a. **Keystore = CommServer.jks**

    b. **key-store.password = <<KeystorePassword>>**

    c. **key-store.type=JKS**

5.5.3.6.1 Installing Certificate in Windows for 4sight and DruckCommsServer

1. Open Run and enter "mmc" hit Enter.
2. Go to File and select Add/Remove snap-ins.
3. From Left side menu select certificates. Press Add then select Computer account >> Next >> Finish. Then click on Ok.

4. Expand certificates (Local computer) section. Expand Trusted Root Certification Authorities.

   In that right click on Certificates folder >> All tasks >> Import.

   Select the cacert.pem >> next >> finish.

   So, our custom CA authority get installed successfully under trusted authority.

After performing all these steps start the DruckCommsServer service.

5.5.3.7 Steps to Configure Self-Signed Certificate for DruckCommsServer if Installed on a Client Machine

To convert DruckCommsServer into HTTPs, you need to have java keytool and OpenSSL utility.

1. Keytool utility is packaged with Java so you can install Java on your machine or check for availability of java keytool directly without installation of Java.
2. Download and install OpenSSL for Windows.
3. Set OpenSSL bin folder path variable by executing below command.

   Set path=%path%;"<<bin folder of openssl>>"
   Example default path:
   Set Path=%Path%;"C:\Program Files\OpenSSL-Win64\bin"

4. Set JRE bin folder path variable by executing below command.

   C:\Program Files\Java\<< Java version >>\bin
   Set Path=%Path%; "C:\Program Files\Java\<< Java version >>\bin"

5. Stop DruckCommsServer service from Windows Services.
6. Create a new folder called **CommserverCertificate** inside C drive or any other drive as you want.
7. Get the 4sight2 public certificate file **4SightV2PublicKey.cer** from server machine which is located on path C:\Program Files\Druck\4Sight2\<<latest folder number>>\app\Certificate directory and copy this file into **CommserverCertificate** folder.
8. Now create **openssl-server.cnf** and **openssl-ca.cnf** by following steps 4 and 5 from section 5.5.3.5 and create index.txt and serial.txt by following steps 12 and 13 into **CommserverCertificate** folder.
9. Now you will have Five files in CommServerCertificate folder

   a. openssl-server.cnf
   b. openssl-ca.cnf
   c. index.txt
   d. serial.txt
   e. 4SightV2PublicKey.cer

10. Open command prompt with Administrative privileges.

    Navigate to CommserverCertificate folder by executing below,
    cd "<<full path to CommserverCertificate >>"

11. Execute below command to generate cacert.pem and cakey.pem files.

    openssl req -x509 -config openssl-ca.cnf -newkey rsa:4096 -sha256 -nodes -out cacert.pem -outform PEM
    Enter correct certificate data when prompted for e.g. country, state etc

12. Now change the content of files in **CommserverCertificate** folder by executing step 1 from section 5.5.3.6.
13. Now executes the steps from 7 to 11 from the 5.5.3.6.

14. Now we need to import 4sight public key into comm server cacert for communication authentication so to do that execute below command,

    keytool -import -noprompt -trustcacerts -alias <<4sight server hostname>> -storepass changeit -keystore "C:\Program Files\Druck\DruckCommsServer\<< Communication Service version >>\cacerts" -file 4SightV2PublicKey.cer

15. After finish all above You will have **DruckCommServer.pfx** and **CommServer.jks** in current **CommserverCertificate** folder.

    Copy those files and paste it into **"C:\Program Files\Druck\DruckCommsServer\<< Communication Service version >>\"** directory. And edit the **application.properties** from same location, Change the property's value as below

    a. Keystore = CommServer.jks

    b. key-store.password = <<KeystorePassword>>

    c. key-store.type=JKS

5.5.3.7.1 Installing certificate in Windows for DruckCommsServer.

1. Open Run and enter "mmc" hit Enter.
2. Go to File and select Add/Remove snap-ins.
3. From Left side menu select certificates. Press Add then select Computer account >> Next >> Finish. Then click on Ok.
4. Expand certificates (Local computer) section. Expand Trusted Root Certification Authorities.

   In that right click on Certificates folder >> All tasks >> Import.

   Select the cacert.pem >> next >> finish.

   So, our custom CA authority get installed successfully under trusted authority.

After performing all these steps start the DruckCommsServer service.

If you just want to check whether DruckCommsServer is successfully converted into https, then in google chrome tab just open the following link: **https://localhost:9443/api/devicemanager/version** (Please put your comm server port number if you have changed but default one is 9443)

5.5.3.8 Validating Certificate in 4Sight2

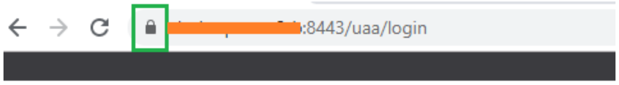
1. Re-start the Server PC.
2. Re-start the 4Sight2 and DruckCommsServer services from Windows Services Open
3. Open google chrome, clear browser cache and re-start google chrome. Make sure no other instances of google chrome are running.
4. Enter below URL in the address bar, hit enter.

   Https://<<Server hostname>>:8443/4sight2.

   Note: you need to use hostname in above URL

5. You should be displayed the login screen with the correct HTTPS URL.

   Note: the red error has disappeared from the address bar. If the link is still not secure, then restart your computer and go to step 3.



[redacted]:8443/uaa/login

4Sight2 Installation FAQs

6. 4Sight2 Installation FAQs

6.1 Setup & Installation

Question 1: I have a multi-site organisation spanning across different regions in the world globally. What is the best way to setup 4Sight2?

Answer: It depends on how you maintain and run these sites. If all sites are maintained and run from a central IT hub, you can install single 4Sight2 license centrally. All sites can access 4Sight2 over the network or LAN. On the other hand, if you have child businesses that are separate entities self-run and managed, you can buy multiple 4Sight2 licenses.

Question 2: If I buy multiple 4Sight2 licenses, will there be any communication between them?

Answer: No. Each 4Sight2 license is an isolated separate software with its own application installation and database. There is no communication between separate installations. Contact 4Sight2 team for further clarity or to discuss any special requirements.

Question 3: How can I download 4Sight2?

Answer: You can easily download 4Sight2 from the company website. Below is the link.

https://info.bakerhughesds.com/4sight2-software-trial-LP.html

OR

you can call the sales offices and raise a purchase order. You should then receive the demo version on a USB stick.

Question 4: Can I install 4Sight2 on a non-windows operating system?

Answer: No. 4Sight2 is only supported for windows platform.

Question 5: I have downloaded and installed 4Sight2? How do I access 4Sight2?

Answer: 4Sight2 is a web-based software. Therefore, no icon is generated on your desktop or computer when you install 4Sight2. To access 4Sight2,

- Open Google Chrome, paste below URL in the address bar and press enter,
- If 4Sight2 installed on the same computer, use, http://localhost:<application_port_number> / 4sight2If 4Sight2 installed on a different computer in the same network, use,

  http://<Computer name OR IP address>:<application_port_number>/4sight2
- Create Bookmark in Google chrome for future reference.

Question 6: 4Sight2 installer failing to locate Postgres Database files

Please ensure the installer has been extracted to a local location and the executable is being run from the Disk 1 folder. Ensure the local location to which the installer has been extracted does not have a long pathname as this can also result in failure to find the installer prerequisite files.

Question 7: What happens If upgrade process is canceled at any stage during upgrade ?

Answer: At any stage if admin cancel the upgrade process then it will rollback to 1.4 version and should be up and working. Admin needs to again start the upgrade process to perform upgrade successfully.

Question 8: While installing 4Sight2 application if user gets this message “Please enter valid port number. To know valid port numbers please refer installation manual”

Answer: Following is the range of invalid ports, choose valid port to continue with the installation

- Port 0 to 1024 are reserved for TCP connection
- List of unsafe ports are - 2049, 3659, 4045, 6000, 6665-6669, 65535

Question 9: 4Sight2 with https is not working in the system

Answer: Follow the syntax for domain name of the computer where the 4sight2 application is going to be installed

```
<domain> ::= <subdomain>
                <subdomain> ::= <label> | <subdomain> "." <label>
                                    <label> ::= <letter> [ [ <ldh-str> ] <let-dig> ]
<ldh-str> ::= <let-dig-hyp> | <let-dig-hyp> <ldh-str>
<let-dig-hyp> ::= <let-dig> | "-"
<let-dig> ::= <letter> | <digit>
<letter> ::= any one of the 52 alphabetic characters A through Z in
upper case and a through z in lower case
<digit> ::= any one of the ten digits 0 through 9
```

Note: Upper and lower case letters are allowed in domain names. Two names with the same spelling but different case are treated as identical.

6.2 Test Equipment Communicator FAQs

Question 1: I have completed all of the steps in the installation manual and still cannot see my device in the list.

Answer: If you still cannot find the Test equipment in the list after performing these steps, re-install the 4Sight2 drivers again. To do that, go to **Control Panel >> Programs and Features**, uninstall DruckCommsServer from the list. Install the Test Equipment Communicator again.

Question 2:. I get an error, '**No Devices Found**'

Answer: To resolve the issue,

- Make sure you have physically connected the device correctly using USB cable. To check this, go to device manager locate your device in the list. You should ideally find your device under Universal Serial Bus devices section. If you see your device under Other devices, you need to perform above settings to make your device a USB device.
- Make sure your device is in communications or comms mode. See step 1 above.
- Make sure the driver path is correctly pointed to C:\Windows\INF... See step 2 above.

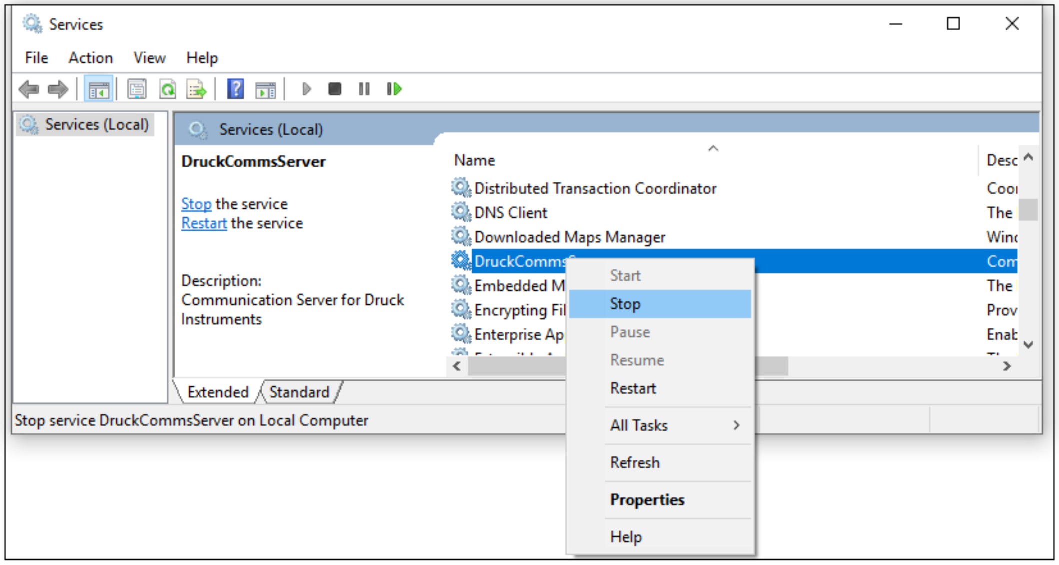
Question 3: I get an error, ‘**Internal Server Error**’ when I click on refresh or click on the

test equipment from the list.,

Answer: To resolve this issue,

- Go to Windows Services (also known as Services),

- Right click on **DruckCommsServer** Service from the list and click **Restart**.



Description:
Communication Server for Druck Instruments

Stop service DruckCommsServer on Local Computer

- Go to 4Sight2 >> Click on **Refresh** button. You should see the device in the list.

Question 4: I get an error, '**Communications Error**'.

Answer: Sometimes the software cannot communicate with the device properly due to several reasons such as loose USB contact, device getting hung up, device busy performing other tasks, server busy executing other tasks and so on. Click on the Refresh button again and the issue must go away (try this 2-3 times)

However, if you still get this error consistently and persistently, try below steps,

- Reboot your Device (Genii / PACE), make sure it is safe to do so and the device isn't in the middle of a critical operation. Try again. Also make sure the device is still physically connected.

If above step does not work, follow instructions in step 3 above and restart **DruckCommsServer** Service.

Installation Troubleshooting

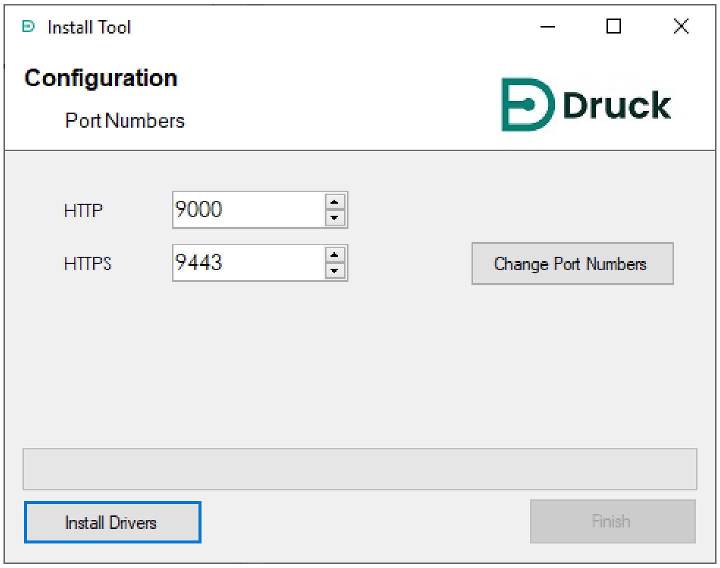
7. Installation Troubleshooting

7.1 Test Equipment Communication Issues

If upon using 4Sight2 to communicate with test equipment you may find no test equipment is being returned, although you have checked that the Test Equipment communicator is return json string upon a direct call to the communicator. This may be due to one of two main issues:

- The port numbers have been configured incorrectly - please contact your administrative user to find out which ports 4Sigth2 is using to contact the Test Equipment Communicator.

  Once you know which ports you should be using navigate to C:\Program Files\Druck\DruckCommsServer\[Version] and run the CommsServerInstallTool.exe



HTTP 9000

HTTPS 9443

Edit the port numbers and then click the **Change Port Numbers** button. Wait while the service restarts. The port numbers have now changed. Select the **Finish** button.

- The Test Equipment Communicator is not configured for Https, but 4Sight2 is.

  Contact your administrator to install a self-signed certificate for the Test Equipment Communicator.

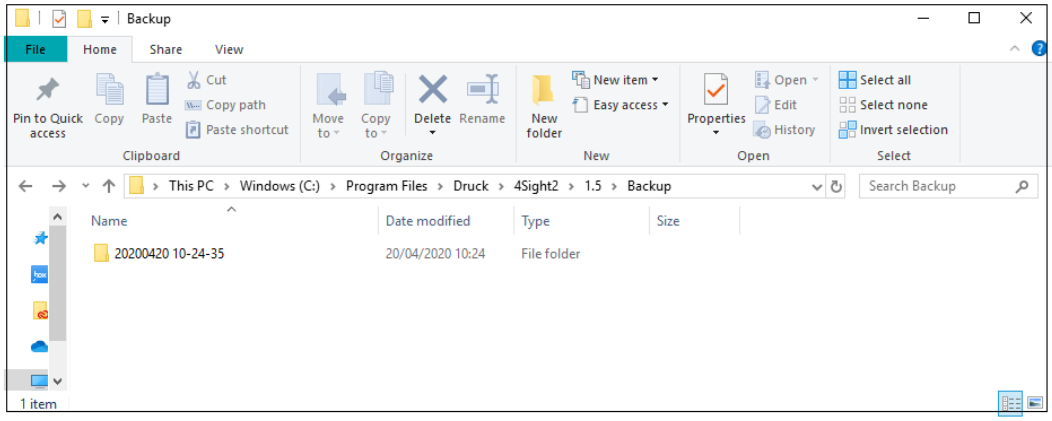
7.2 Postgres Database Backup

Refer to 4Sight2 user manual - 123M3138 for information on postgres database backup.

7.3 Postgres Database Restore

Assuming you already have performed a database backup using the 4Sight Application.

The 4Sight application (Version 1.4 & above) provides an interface for initiating a backup (user initiated / scheduled). This operation creates files in the backup folder inside the 4Sight installation directory on the server. Each backup initiated creates a new folder within the backup folder with the name in the format YYYYMMDDHHSS (Year, Month, Date, Hour & Second) depending upon the date & time when the backup completed successfully.



Name	Date modified	Type	Size
20200420 10-24-35	20/04/2020 10:24	File folder	

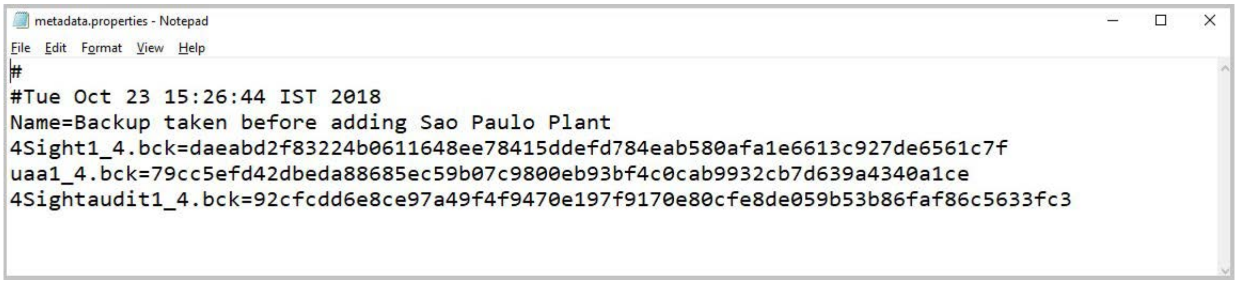
It is a recommended practice to backup the contents of the backup folder on a separate media

Each folder has 5 files.

1. 4Sight<APPLICATION_VERSION>.bck
2. 4Sightaudit<APPLICATION_VERSION>.bck
3. uaa<APPLICATION_VERSION>.bck
4. metadata.properties
5. status.json

The *.bck files have a suffix with the 4Sight application version. Please ensure that you restore a database that matches the exact version of your application. Higher / lower version of database are not supported by the application. Note that the version contains an underscore (_) and not period (.) e.g. 1_4 & not 1.4. When using the below commands in the Steps for Restore, kindly ensure that you replace the <APPLCATION_VERSION> with the correct version of 4Sight that has been installed.

The metadata.properties file contains the name of the backup as entered during the backup initiation.



```
#
#Tue Oct 23 15:26:44 IST 2018
Name=Backup taken before adding Sao Paulo Plant
4Sight1_4.bck=daeabd2f83224b0611648ee78415ddefd784eab580afa1e6613c927de6561c7f
uaa1_4.bck=79cc5efd42dbeda88685ec59b07c9800eb93bf4c0cab9932cb7d639a4340a1ce
4Sightaudit1_4.bck=92cfcdd6e8ce97a49f4f9470e197f9170e80cfe8de059b53b86faf86c5633fc3
```

SHA 256 Check

In a backup, there are 3 files - one for each database, with the extension .bck. The metadata.properties file contains the SHA 256 of each of the backup files.

1. Open a command prompt as Administrator & change directory to the folder containing the selected backup files.
2. Use the below commands to calculate the SHA256 of each file

```
certutil -hashfile 4Sight<APPLICATION_VERSION>.bck SHA256
certutil -hashfile 4Sightaudit<APPLICATION_VERSION>.bck SHA256
certutil -hashfile uaa<APPLICATION_VERSION>.bck SHA256
```

3. Before continuing with the steps to restore, check that the SHA 256 of each file matches the SHA 256 mentioned in the metadata file. Backup file is valid for restore if checksum from command prompt and checksum from metatdata file are exactly same. Continue with the Steps for restore only if they are the same.

7.4 Steps for Restore:

1. Login into the 4Sight server as Administrator.
2. Find the port on which the Postgres Database is running. It can be found in the property spring.datasource.url inside the <4Sight INSTALLATION DIRECTORY>\apache-tomcat\webapps\application.properties file. Use a Notepad running as Administrator to open this file. It is the number just before the 4Sight**<APPLICATION_VERSION>**
3. Login into the psql command utility from a command prompt running as Administrator, using the postgres user

```
C:\Program Files\PostgreSQL\11\bin\psql" --port=<DB_PORT> postgres postgres
```

4. The database user used by the application can be found in the property spring.datasource.username inside the <4Sight INSTALLATION DIRECTORY>\apache-tomcat\webapps\application.properties file. Use a Notepad running as Administrator to open this file.
5. Delete *_temp databases if they exists & then create the empty *_temp databases by running the below commands in the psql prompt

```
DROP DATABASE IF EXISTS "4Sight<APPLICATION_VERSION>_temp";
CREATE DATABASE "4Sight<APPLICATION_VERSION>_temp"  WITH TEMPLATE template0 OWNER
"<DB_USER>" LC_COLLATE = "C" LC_CTYPE = "C" TABLESPACE =
"4Sight_<APPLICATION_VERSION>_4Sight";
DROP DATABASE IF EXISTS "4Sightaudit<APPLICATION_VERSION>_temp";
CREATE DATABASE "4Sightaudit<APPLICATION_VERSION>_temp"  WITH TEMPLATE template0
OWNER "<DB_USER>" LC_COLLATE = "C" LC_CTYPE = "C" TABLESPACE =
"4Sight_<APPLICATION_VERSION>_4Sightaudit";
DROP DATABASE IF EXISTS "uaa<APPLICATION_VERSION>_temp";
CREATE DATABASE "uaa<APPLICATION_VERSION>_temp"  WITH TEMPLATE template0 OWNER
"<DB_USER>" LC_COLLATE = "C" LC_CTYPE = "C" TABLESPACE =
"4Sight_<APPLICATION_VERSION>_uaa";
```

Change the Database owner of the above 3 databases to this user. Note that the username is case sensitive.

```
ALTER DATABASE "4Sight<APPLICATION_VERSION>_temp" OWNER TO "<DB_USER>";
ALTER DATABASE "4Sightaudit<APPLICATION_VERSION>_temp" OWNER TO "<DB_USER>";
ALTER DATABASE "uaa<APPLICATION_VERSION>_temp" OWNER TO "<DB_USER>";
```

6. Check the metadata.properties files of the backups & decide upon which backup you need to restore.
7. Open another command prompt as Administrator & change directory to the folder containing the above selected backup files.

   Restore the database from the *.bck files to *_temp databases using the below commands. If prompted for a password, enter the postgres super user's password.
   "C:\Program Files\PostgreSQL\11\bin\pg_restore" --port=**<DB_PORT>** --no-owner --username=postgres --dbname=4Sight**<APPLICATION_VERSION>**_temp -n public --role=**<DB_USER>** 4Sight**<APPLICATION_VERSION>**.bck

   "C:\Program Files\PostgreSQL\11\bin\pg_restore" --port=**<DB_PORT>** --no-owner --username=postgres --dbname=4Sightaudit**<APPLICATION_VERSION>**_temp -n public --role=**<DB_USER>** 4Sightaudit**<APPLICATION_VERSION>**.bck

   "C:\Program Files\PostgreSQL\11\bin\pg_restore" --port=**<DB_PORT>** --no-owner --username=postgres --dbname=uaa**<APPLICATION_VERSION>**_temp -n public --role=**<DB_USER>** uaa**<APPLICATION_VERSION>**.bck
8. Delete the *_old databases if they exist by running the below commands in the psql prompt.

   DROP DATABASE IF EXISTS "4Sight**<APPLICATION_VERSION>**_old";
   DROP DATABASE IF EXISTS "4Sightaudit**<APPLICATION_VERSION>**_old";
   DROP DATABASE IF EXISTS "uaa**<APPLICATION_VERSION>**_old";
9. Stop the 4Sight service & pgadmin applications if any are open.
10. Rename the existing 4Sight databases to *_old by running the below commands in the psql prompt.

    ALTER DATABASE "4Sight**<APPLICATION_VERSION>**" RENAME TO "4Sight**<APPLICATION_VERSION>**_old";
    ALTER DATABASE "4Sightaudit**<APPLICATION_VERSION>**" RENAME TO "4Sightaudit**<APPLICATION_VERSION>**_old";
    ALTER DATABASE "uaa**<APPLICATION_VERSION>**" RENAME TO "uaa**<APPLICATION_VERSION>**_old";
11. Rename the *_temp databases to 4Sight databases by running the below commands in the psql prompt.

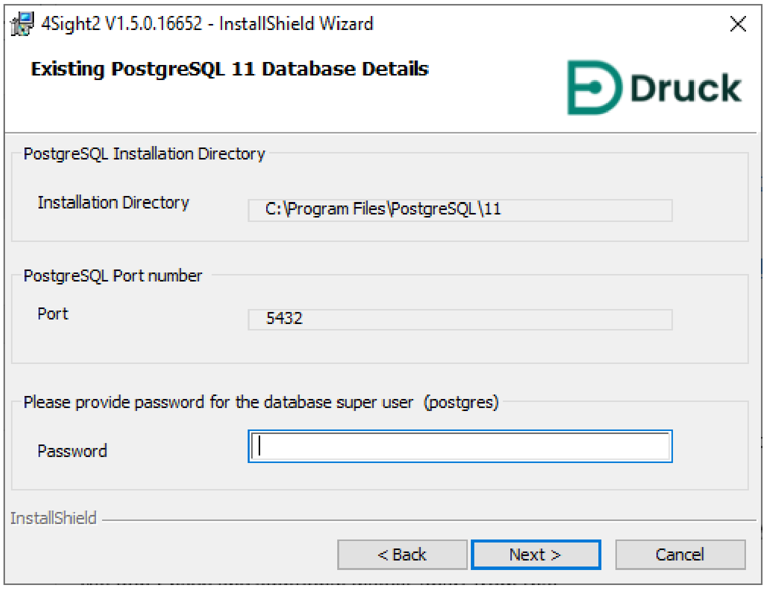
    ALTER DATABASE "4Sight**<APPLICATION_VERSION>**_temp" RENAME TO "4Sight**<APPLICATION_VERSION>**";
    ALTER DATABASE "4Sightaudit**<APPLICATION_VERSION>**_temp" RENAME TO "4Sightaudit**<APPLICATION_VERSION>**";
    ALTER DATABASE "uaa**<APPLICATION_VERSION>**_temp" RENAME TO "uaa**<APPLICATION_VERSION>**";
12. Start the 4Sight Service & try logging in as Administrator. Note that the password of the Administrator at the time of taking the backup has to be used to login now.

7.5 How to recover from a 4Sight2 Machine Crash?

Assumptions: User has taken a backup of the 4Sight2 database before the crash.

User already knows the username and password for both application and database.

1. Setup the machine with supporting OS and Drivers.
2. Install 4Sight2 on the machine.
3. While installing the application, provide the same username and password as previously given for the both application and Postgres database.



4Sight2 V1.5.0.16652 - InstallShield Wizard

Existing PostgreSQL 11 Database Details

PostgreSQL Installation Directory

Installation Directory: C:\Program Files\PostgreSQL\11

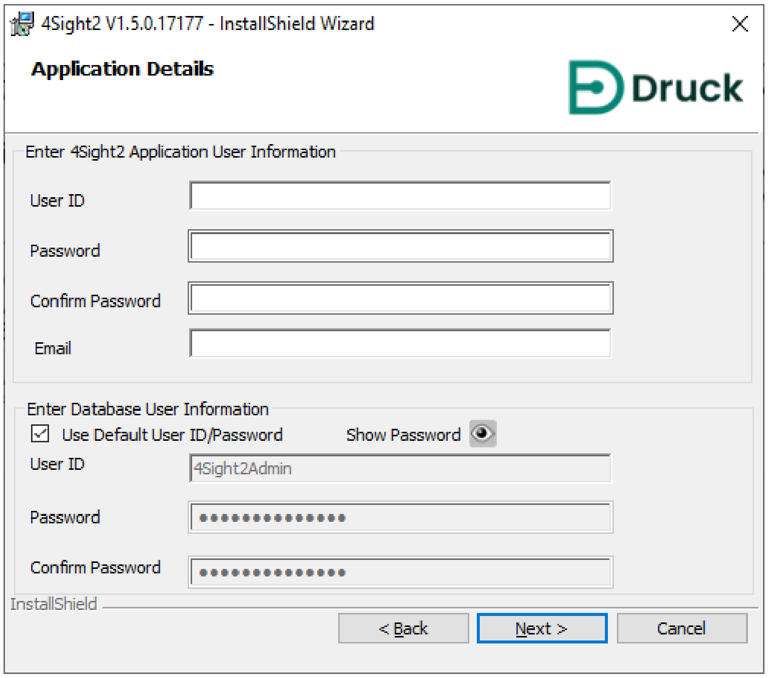
PostgreSQL Port number

Port: 5432

Please provide password for the database super user (postgres)

Password:

Password same as previous Install



4Sight2 V1.5.0.17177 - InstallShield Wizard

Application Details

Enter 4Sight2 Application User Information

User ID:

Password:

Confirm Password:

Email:

Enter Database User Information

☑ Use Default User ID/Password Show Password

User ID: 4Sight2Admin

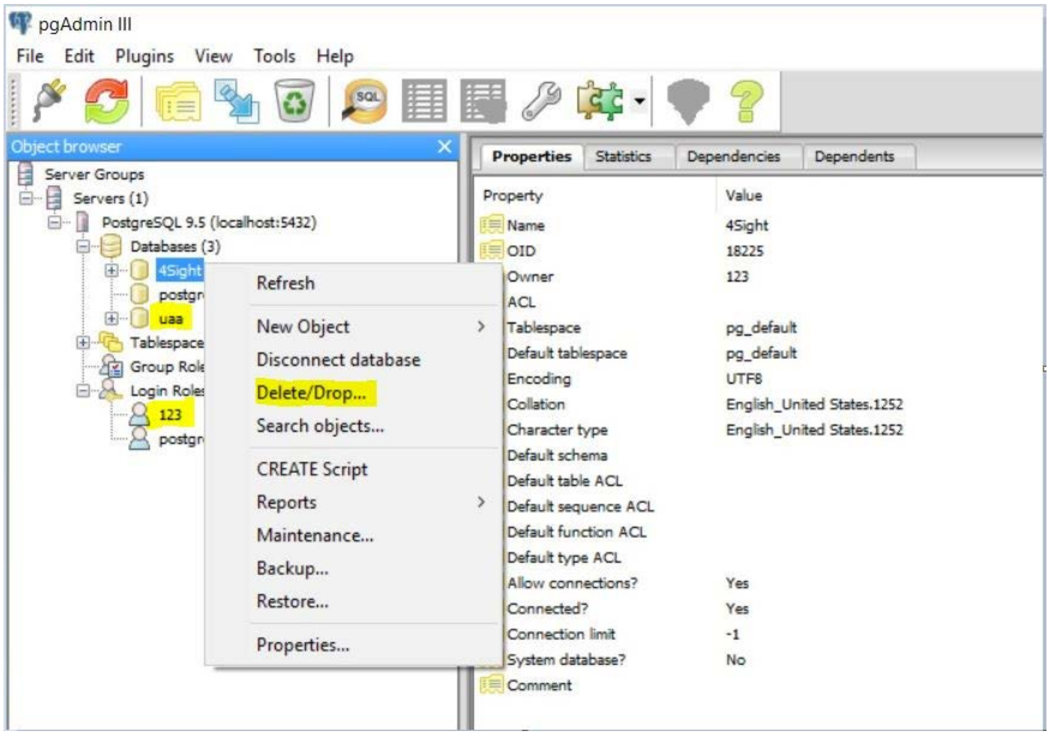
Password: ●●●●●●●●●●●●●●

Confirm Password: ●●●●●●●●●●●●●●

Complete all the fields as previous install

4. After successfully installing the application, drop the default database created while installing application from pgAdmin (Right click on database & select Delete/Drop). If you are getting an

error while dropping database, then restart the Postgres service and try the same after refreshing.



Property	Value
Name	4Sight
OID	18225
Owner	123
ACL	
Tablespace	pg_default
Default tablespace	pg_default
Encoding	UTF8
Collation	English_United States.1252
Character type	English_United States.1252
Default schema	
Default table ACL	
Default sequence ACL	
Default function ACL	
Default type ACL	
Allow connections?	Yes
Connected?	Yes
Connection limit	-1
System database?	No
Comment	

5. After successfully dropping the database and user. Follow these steps to restore the database as mentioned above from command prompt.
6. Now you have successfully restored database, open the application from browser and review the same.

7.6 Installation failure scenario:

Below table explains the various failure scenario's during installation and their remedy actions.

Error Message	Scenario	Remedy/Action to take
"Insufficient disk space available to install 4Sight2 application. Please ensure a minimum of 4096 MB is available. Free Space : available MB.	Failure due to hard disk size issue (If there is no required space at the start of upgrade)	Admin need to free space in respective drive and then try Upgrade process again.
"Deployment fail while Migrating database"	Failure due to hard disk size issue (If there is not sufficient space after upgrade started successfully)	Admin need to free space in respective drive and then try Upgrade process again.

Error Message	Scenario	Remedy/Action to take
"Installation failed while migrating Database. Please reinstall 4sight2”	Failure due to data Integrity at copy data base	Admin need to contact Customer help desk if this occurs. Data integrity reason captured in logs at location.[C:\Users\[Username]\App Data\Local\Temp\logs]
"Installation failed while migrating Database. Please reinstall 4sight2”	Failure due to data Integrity at schema update stage	Admin need to contact Customer help desk if this occurs. Data integrity reason captured in logs at location.C:\Program Files\Druck\4Sight2\<<latest folder number>>\logs
“Failed to locate existing 4Sight2 service. Please ensure existing 4Sight2 version is installed on this machine and the service is running"	This failure happens If installer unable to get the state of the service"	Admin needs to ensure that 4Sight2 service is up and running
"Failed to start the 4Sight2 service. Please ensure the 4Sight2 service is present and running”	Failure if application corrupted, some files are deleted or port is in use by other application or user has stopped the service etc.	If admin succeed to get the service state and if it is not running for any reason(e.g. application corrupted, some files are deleted or port is in use by other application or user has stopped the service etc.) then system try to start the service. If service is not able to start than admin need to contact customer support to fix the problem.
"Upgrade of 4Sight2 application is supported from version 1.3 onwards. For earlier version upgrade support please contact Customer Care."	Upgrade will not happen if older than 1.3 version is installed.	Upgrade is only possible from 1.3 to higher version.
Installer has detected another minor version of PostgreSQL 11. Installer will not continue. Refer to 4Sight2 Installation manual for more details	4Sight2 cannot continue the 4Sight2 installation as same PostgreSQL version (variant) exists on target machine	Possible options 1. User can choose another machine 2. User backup existing application which is using Postgres version 11.3, un-install and deploy that application on other machine. Un-install Postgres and re-start 4Sight2 Installation
Installation failed while upgrading database. Please reinstall 4Sight2. Refer to 4Sight2 Installation manual for more details	Some internal error might have happened during the upgrade, user can attempt re-install	If problem persists, User can share installation logs for more understanding

7.7 General Causes of Error

Below are commonly observed problems associated with 4sight2 communication with the Druck equipment via USB.

- Physical connection is loose or wobbly
- Worn cables / ports
- Poor quality USB adaptors
- Overloaded USB adaptors / ports
- Devices kept running for long time thereby causing them to go in hibernate or sleep mode
- Devices not in communications mode
- Driver software not installed or upgraded. You need same version of 4Sight2 application and the drivers to establish communication with the hardware.
- Devices have very old firmware versions.

7.8 Uninstalling 4Sight2

Follow these instructions if you require installation of a new copy of 4Sight2, a new version of 4Sight2 or need to uninstall 4Sight2 due to issues occurring during installation.

⚠ Uninstallation of the PostgreSQL database component will delete the 4Sight2 database resulting in loss of data. A backup will not be created automatically by the following steps, so make sure you have created a manual backup before proceeding and saved this backup in an alternative location to the 4Sight2 installs folder. Refer to the Postgres Database backup and restore section of this manual.

If you choose to uninstall just 4Sight2 application and keep the database, please refer to the 4Sight2 installation part of this manual. You will require the credentials for database superuser upon re-installation. Do not attempt to perform an uninstall if you do not know these credentials.

If you wish to upgrade your 4Sight2 version without uninstalling the database, please **DO NOT** follow these instructions.

1. Go to the Control panel >> Programs and Features
2. Right Click on 4Sight2 and select Uninstall.
3. Follow the instructions in the Uninstall wizard
4. Right Click on PostgreSQL 11 and select Uninstall
5. Follow the instructions in the Uninstall wizard
6. Uninstalling PostgreSQL does not delete the data folder. You need to do this manually. Delete the data folder which can be found at C:\Program Files\PostgreSQL\11\
   a. If you wish to delete the entire PostgreSQL folder, make sure any backup files, scripts are moved from the bin folder before proceeding
   b. By default 4Sight2 database backups are created and saved at the following location: C:\Program Files\PostgreSQL\11\bin
7. It is recommended to restart the computer if possible.
8. 4Sight2 is now successfully uninstalled.

7.9 Secure Communications Trouble shooting

1. Command 'command name' is not recognized as an internal or external command. E.g. 'key-tool' is not recognized as an internal or external command,

- If you get an error like this, that means in the current folder that you are in, command prompt cannot find reference to the specified command.

  To solve this error, use the below command to point to the correct folder.
  Set Path=%Path%;"<<full path of the location where the command is>>"
  Example, in above error related to keytool, you need to set path to below,
  Set "Path=%Path%;C:\Program Files\Druck\4Sight2\<<latest folder number>>\jre\bin"

2. Bad IP address

- If you get an error message which this text, this means the IP Address or Hostname in either openssl-ca.cnf or openssl-server.cnf files are incorrect. Note: you may need to correct this at multiple places in these files and re-execute the steps again.

3. No such file or directory...

- If you get an error message with this text, this means the command you have executed probably refers to a filename that is not correct. Check the command for any filenames errors and also check if the file with that name is present in the folder and re-run the commands. You may either have to correct the filename in the command or follow steps to generate the missing files.

- This error can occur for index.txt and serial.txt files because in certain cases the file extension gets appended to the name twice for e.g. intex.txt.txt.

  Simply edit the file and save it without the .txt extension. Make sure file has one .txt extension.

Best Practices

8. Best Practices

Server Hardening

The server environment should be hardened as per Microsoft or CIS guidelines.

8.1 Tomcat

- Install Tomcat in secure folder where only admin or LocalService has access, such as *C:\Program Files(x86)*
- Install Tomcat as a service running in LocalService account.
- Remove everything from WebApp, remove the default unwanted applications.
- Replace Default error page, such as 404, 403, 500 etc
- Enforce HTTPS, enable SSL.
- Management application should run on SSL.
- User individual log file for each web application.
- Remove Server banner.
- Enable Access logging.
- Change Shutdown port and command.

8.2 PostgreSQL

- All the high privilege account like pgdba, postgres, depesz should be allowed to local login only.
- Make sure sequence is correct in pg-hba.conf file so that the correct users get right access
- Configure the pg-hba.conf so that server can be connected only from the local machine and not through the network.

8.3 Firewall Best Practices

Here are some of the firewall best practices which are recommended for use with 4Sight2:

8.3.1 Policy

1. Firewall configuration should be consistent with the Organization Security Policy.
2. Always use Least privilege policy. Deny all by default. Allow specific traffic (using source, destination and port)
3. Place Specific rules first and use explicit drop rules.
4. Log all the actions, specifically failure attempts for audit trail

8.3.2 Resources

1. Monitor memory utilization
2. Monitor CPU utilization
3. Monitor Bandwidth utilization.
4. Limit the number of application running on the Firewall machine

8.3.3 Installation and Maintenance

1. Limit Physical Access to the firewall machine
2. Use unique user id for administration

3. Follow strict account policy on the machine
4. Patch operating systems, application software, firmware etc. regularly.
5. Archive rule base, configuration and logs regularly. Document all rules and changes made in a source control.
6. Perform regular tests.
7. Remove unused rule when service is decommissioned.
8. Audit and review the rules on a regular basis.
9. Monitory security advisories on a regular basis

8.3.4 Additional Security

1. Use Statefull inspections.
2. Use Proxies
3. Use Application level inspection and filtering.

8.3.5 Internal Protection

1. Have Acceptable Usage Policy
2. Personal Firewall for each user
3. Host Based intrusion prevention
4. Network Monitoring
5. Content Filtering
6. Access Control on each computer and application.

Office Locations

Headquarters

Leicester, UK
Phone: +44 (0) 116 2317233
Email: gb.sensing.sales@bakerhughes.com

Australia

Springfield Central
Phone: +61 414191649

China

Beijing
Phone: +86 180 1929 3751
Email: fan.kai@bakerhughes.com

China

Guangzhou
Phone: +86 173 1081 7703
Email: dehou.zhang@bakerhughes.com

China

Shanghai
Phone +86 135 6492 6586
Email: hensen.zhang@bakerhughes.com

France

Toulouse
Phone: +33 562 888 250
Email: sensing.FR.cc@bakerhughes.com

Germany

Frankfurt
Phone: +49 (0) 69-22222-973
Email: sensing.de.cc@bakerhughes.com

India

Bangalore
Phone: +91 9986024426
Email: aneesh.madhav@bakerhughes.com

Italy

Milan
Phone: +39 02 36 04 28 42
Email: csd.italia@bakerhughes.com

Japan

Tokyo
Phone: +81 3 6890 4538
Email: gesitj@bakerhughes.com

Netherlands

Hoevelaken
Phone: +31 334678950
Email: nl.sensing.sales@bakerhughes.com

Russia

Moscow
Phone: +7 915 3161487
Email: aleksey.khamov@bakerhughes.com

UAE

Abu Dhabi
Phone: +971 528007351
Email:suhel.aboobacker@bakerhughes.com

USA

Boston
Phone: 1–800-833-9438
Email: ccpressureusa@bakerhughes.com

Services and Support Locations

Tech Support

Global
Email:
drucktechsupport@bakerhughes.com

Brazil

Campinas
Phone: +55 11 3958 0098, +55 19 2104 6983
Email: mcs.services@bakerhughes.com

China

Changzhou
Phone: +86 400 818 1099
Email: service.mcchina@bakerhughes.com

France

Toulouse
Phone: +33 562 888 250
Email: sensing.FR.cc@bakerhughes.com

India

Pune
Phone: +91 213 5620426
Email:
mcsindia.inhouseservice@bakerhughes.com

Japan

Tokyo
Phone: +81 3 3531 8711
Email: service.druck.jp@bakerhughes.com

UAE

Abu Dhabi
Phone: +971 2 4079381
Email: gulfservices@bakerhughes.com

UK

Leicester
Phone: +44 (0) 116 2317107
Email: sensing.grobycc@bakerhughes.com

USA

Billerica
Phone: +1 (281) 542-3650
Email: namservice@bakerhughes.com

Baker Hughes