Druck

4Sight2

Software de gestión de calibración

Manual de instalación 123M3140 Revisión F

Índice

1. Introducción

El software de calibración 4Sight2 es una herramienta de gestión de calibración basada en la web que ayuda a mantener y controlar el entorno de calibración conforme a las mejores prácticas de metrología. Puede utilizar el software para realizar estas tareas:

- Gestionar la calibración de todos los dispositivos de medición de unas instalaciones determinadas.
- Elaborar un programa de trabajos de calibración para los técnicos.
- Cargar y descargar datos en calibradores portátiles Druck (DPI620 Genii, DPI611 y DPI612) con función de comunicación USB.
- Gestionar los registros de calibración de dispositivos no compatibles con calibradores portátiles (entrada de datos manual).
- Revisar sus registros históricos de calibración. También puede mantener un registro permanente de cada certificado de calibración. Por ejemplo: Para procedimientos de control de calidad ISO 9000.
- Controlar las calibraciones automatizadas utilizando controladores de presión Druck (PACE 1000, 5000 y 6000), calibradores portátiles (DPI620 Genii, DPI611 y DPI612) y calibradores de temperatura (DryTC165, DryTC 650, LiquidTC165 y LiquidTC255).

1.1 Destinatarios del producto

1.1.1 Administradores

Los administradores son responsables de la instalación y configuración del software 4Sight2. Tras la instalación inicial de 4Sight2, solo habrá una cuenta administrativa. Dicha cuenta permite crear nuevos usuarios y asignar grupos y conjuntos de permisos. Los usuarios administrativos tienen acceso de lectura y escritura a todas las características de 4Sight2.

1.1.2 Supervisores

Los supervisores son responsables de la gestión de activos y calibraciones. Pueden crear y actualizar archivos en la Empresa 4Sight2, incluyendo Plantas, Ubicaciones y Dispositivos. Se encargan de vincular documentos a activos, como procesos de plantas y hojas de características de dispositivos. Los supervisores pueden crear procedimientos de prueba que se utilizarán durante la calibración, además de programar procedimientos y supervisar el estado de los dispositivos. Disponen de los permisos necesarios para aprobar calibraciones.

1.1.3 Técnicos

Los técnicos son responsables de llevar a cabo las calibraciones. Una calibración puede ser Portátil, Manual o Automatizada. El técnico se encarga de realizar el tipo de calibración correspondiente en un dispositivo. Una vez realizada la calibración, los técnicos pueden revisar el resultado y finalizarla para que la apruebe un supervisor.

1.1.4 Auditores

Los auditores son responsables son responsables de inspeccionar los informes. En algunas plantas, las auditorías son obligatorias por razones de cumplimiento normativo.

2. Requisitos del sistema

Los requisitos mínimos del sistema para instalar la aplicación 4Sight2 en máquinas cliente y servidor se detallan a continuación:

2.1 Servidor de la aplicación

Sistema operativo	Windows 10, Windows Server 2012 R2, Windows Server 2016, Windows Server 2019
Actualizaciones	Todas las actualizaciones de Windows deben estar instaladas
Procesador	Cuatro núcleos
RAM	8 GB o superior (se recomiendan 32 GB)
Espacio en disco	1 TB
Velocidad de red	10 Mbps

2.2 Estación de trabajo cliente

Sistema operativo	Windows 10, Windows Server 2012 R2, Windows Server 2016, Windows Server 2019
Navegador	Google Chrome V80+, Microsoft Edge V80, Firefox V74
Adobe Reader	Adobe Acrobat Reader DC Versión 2015.017.20050 +
RAM	8 GB o superior
Procesador	Dos núcleos
Espacio en disco	600GB
Velocidad de red	10 Mbps

2.3 Instalación local

Sistema operativo	Windows 10, Windows Server 2012 R2, Windows Server 2016, Windows Server 2019
Actualizaciones	Todas las actualizaciones de Windows deben estar instaladas
Adobe Reader	Adobe Acrobat Reader DC Versión 2015.017.20050 +
Procesador	Dos núcleos
RAM	16GB o superior (se recomiendan 32GB)
Espacio en disco	500 GB como mínimo de espacio en disco
Navegador	Google Chrome V80+, Microsoft Edge V80, Firefox V74

2.4 Firmware compatible con 4Sight2

Para obtener la información más reciente sobre el firmware compatible, consulte el siguiente enlace:

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

o

Para PACE, inserte el USB B para 4Sight2 Communication como se indica en la imagen a continuación:

Instalación de 4Sight2

3. Instalación de 4Sight2

Para instalar 4Sight2, copie primero el archivo ZIP de instalación de 4Sight2 en el escritorio y extraiga su contenido. En el archivo de instalación, seleccione el ejecutabla de 4Sight2.

Nota: Se utiliza el siguiente software antivirus para analizar las instalaciones de 4Sight2 y Comm Server,

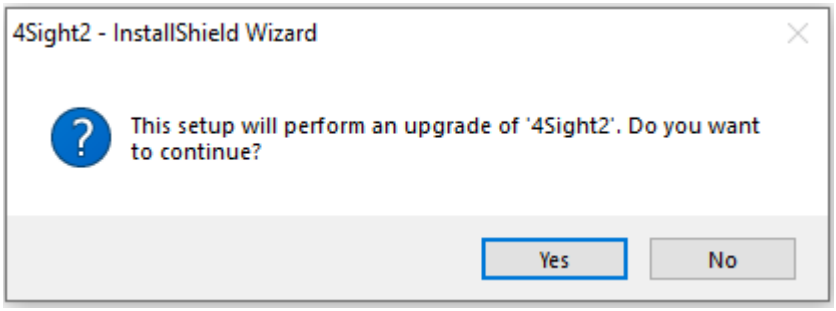
- McAfee VirusScan Enterprise + AntiSpyware Enterprise Versión: 8.8.0
- Symantec Endpoint Protection Versión: 14.3.558

Una vez ejecutado el programa de instalación, se iniciará el asistente InstallShield. El asistente InstallShield consta de dos etapas para instalar 4Sight2:

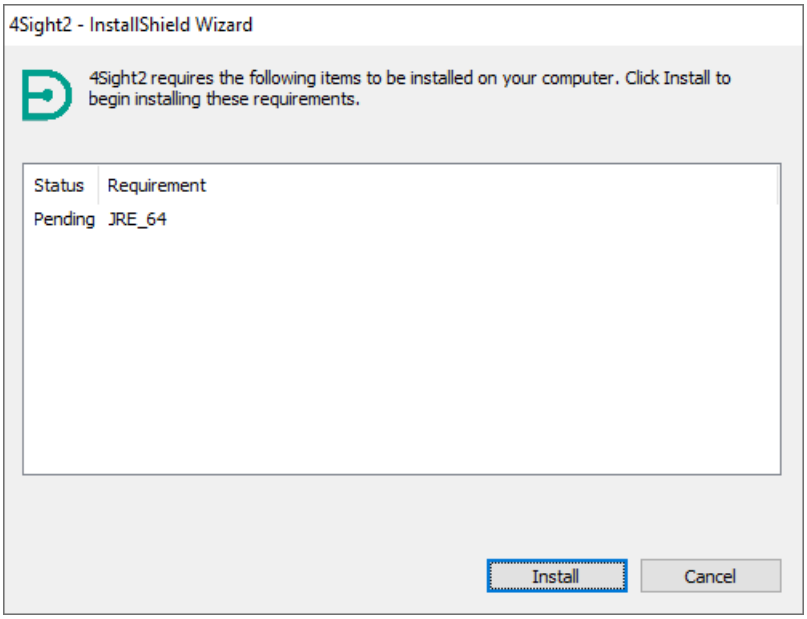
1. Instalación de la base de datos
2. Instalación de la aplicación web

Siga las instrucciones del asistente InstallShield o las dos secciones siguientes para llevar a cabo el proceso de instalación.

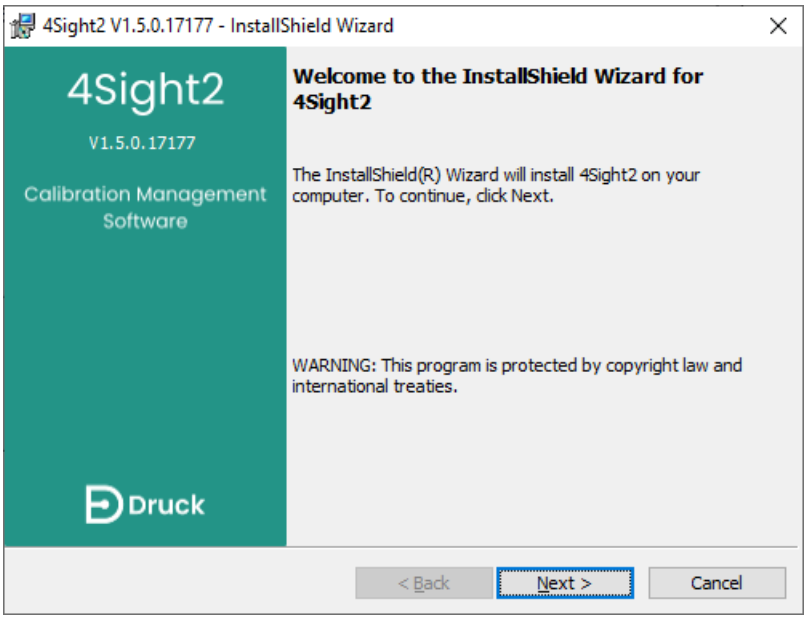
1. Si 4Sight2 ya está instalado en la máquina, el asistente de instalación le pedirá que lleve a cabo una actualización a una versión reciente. Haga clic en **Sí** para llevar a cabo la actualización.



2. Si 4Sight2 se instala por primera vez en la máquina, el asistente de instalación presentará la pantalla siguiente. Seleccione **Instalar** para instalar los elementos que aparecen en la lista.



3. Una vez instalados todos los elementos necesarios, aparecerá la pantalla Bienvenida al asistente de instalación InstallShield. Haga clic en **Siguiente** para continuar.



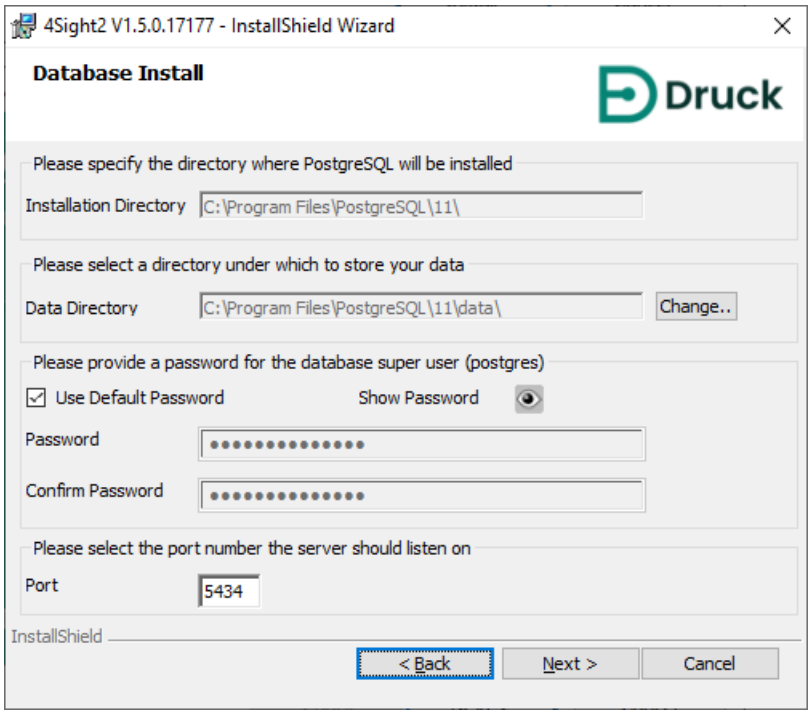
3.1 Instalación de la base de datos

La aplicación 4Sight2 utiliza una base de datos PostgreSQL. Las siguientes instrucciones indican cómo instalar la base de datos PostgreSQL y cómo proceder si ya hay instalada una base de datos PostgreSQL.

3.2 Instalación de PostgreSQL

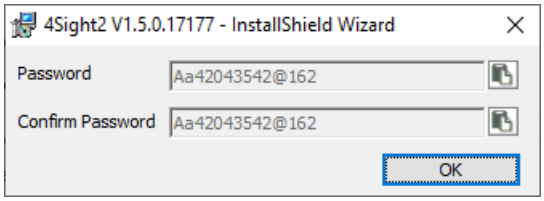
Siga este procedimiento si no hay una base de datos PostgreSQL instalada en la máquina.

1. Si no hay ninguna instancia de la base de datos PostgreSQL instalada en la máquina, el asistente de instalación presentará la pantalla siguiente.

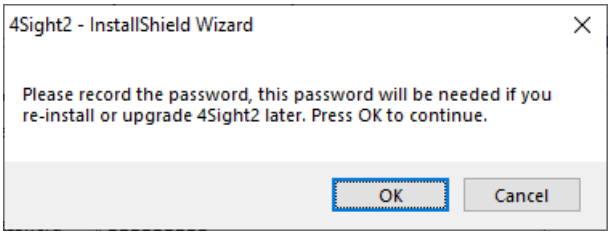


Directorio de instalación: Seleccione el directorio en el que se instalará la aplicación PostgreSQL.
Directorio de datos: Seleccione el directorio en el que se almacenarán los datos de la aplicación PostgreSQL.
Contraseña/Confirmar contraseña: Introduzca la contraseña del superusuario de la base de datos PostgreSQL. Sólo deberá hacerlo si instala la base de datos PostgreSQL por primera vez.
Nota: Esta contraseña será necesaria para acceder al contenido de la base de datos después de la instalación.
Puerto: Es la dirección del puerto de la base de datos PostgreSQL a través del cual se atenderán las solicitudes de la aplicación.
Nota: Si el número de puerto a está ocupado, contacte con el equipo de TI. El usuario también puede cambiar el número de puerto, pero deberá anotarlo para iniciar después la aplicación.

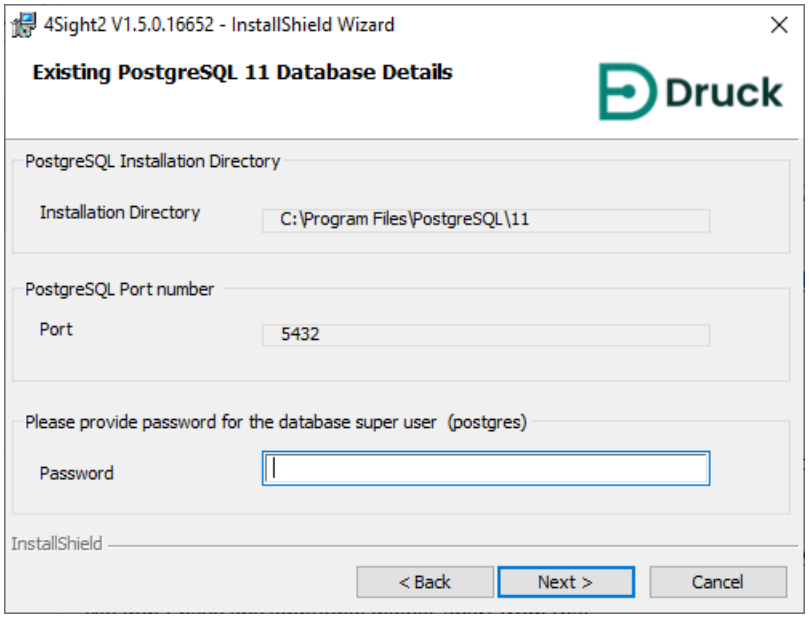
Importante: El usuario debe tomar nota de la contraseña de la base de datos. La pérdida de la contraseña puede conllevar la denegación de acceso o la pérdida de datos. Desactive la casilla de verificación Contraseña predeterminada de usuario para actualizar la contraseña de superusuario de la base de datos. Si desea mantener la contraseña predeterminada o ver la nueva contraseña introducida, seleccione el icono (Mostrar contraseña). Para copiar la contraseña al portapapeles, utilice el icono (Copiar al portapapeles).



A continuación, el instalador le pedirá que registre de nuevo la contraseña. Seleccione **Aceptar** cuando haya anotado la contraseña.

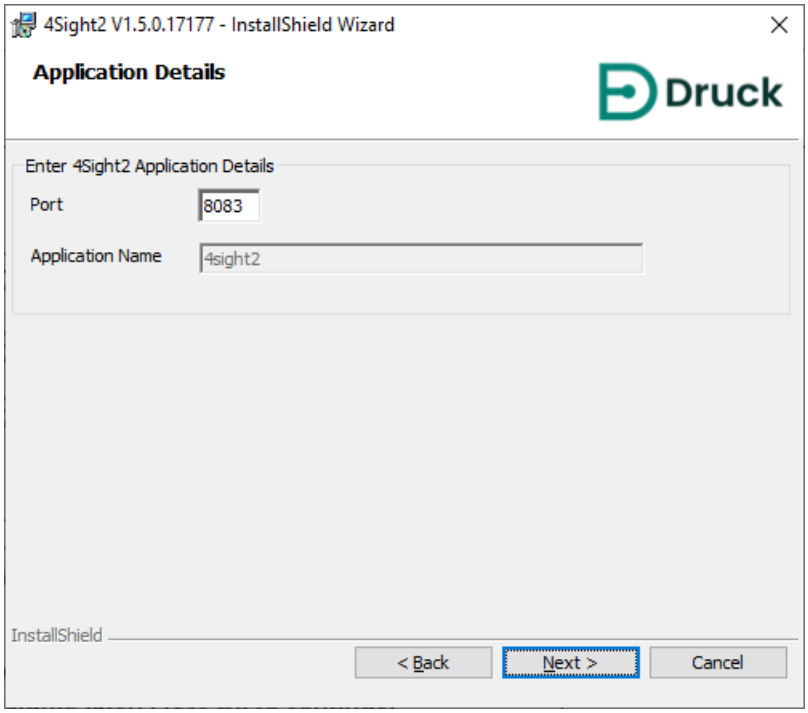


2. Este paso solo se mostrará si la base de datos PostgreSQL ya está instalada.



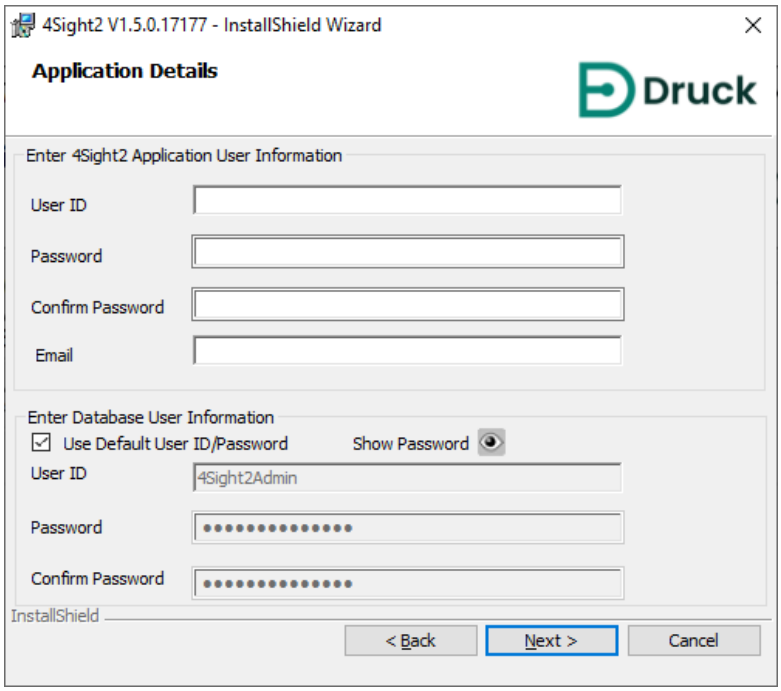
Directorio de instalación: Este campo indica la ruta en la que está instalada la base de datos PostgreSQL. La información es de sólo lectura.
Contraseña: Este campo permite confirmar la contraseña del superusuario de la base de datos PostgreSQL.
Puerto: Este campo permite especificar el número de puerto que utiliza la aplicación PostgreSQL para ejecutar la solicitud db.

3. En la ventana Detalles de la aplicación, introduzca los siguientes datos.



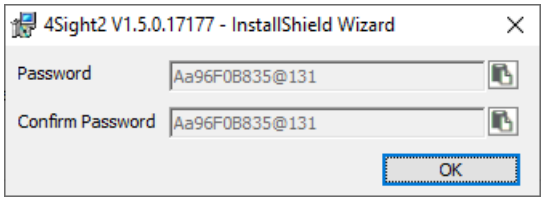
Puerto: Introduzca el puerto del servidor web Tomcat utilizado por la aplicación web 4Sight2 para responder a las solicitudes HTTP.
Nombre de la aplicación: Introduzca la ruta de acceso a la aplicación que permitirá conectarse a la aplicación 4Sight2 desde el navegador web. De forma predeterminada, es 4sight2.
Nota: Si el número de puerto a está ocupado, contacte con el equipo de TI. El usuario también puede cambiar el número de puerto, pero deberá anotarlo para iniciar después la aplicación.

4. Seleccione **Siguiente** para acceder a la pantalla Información del usuario de la aplicación.

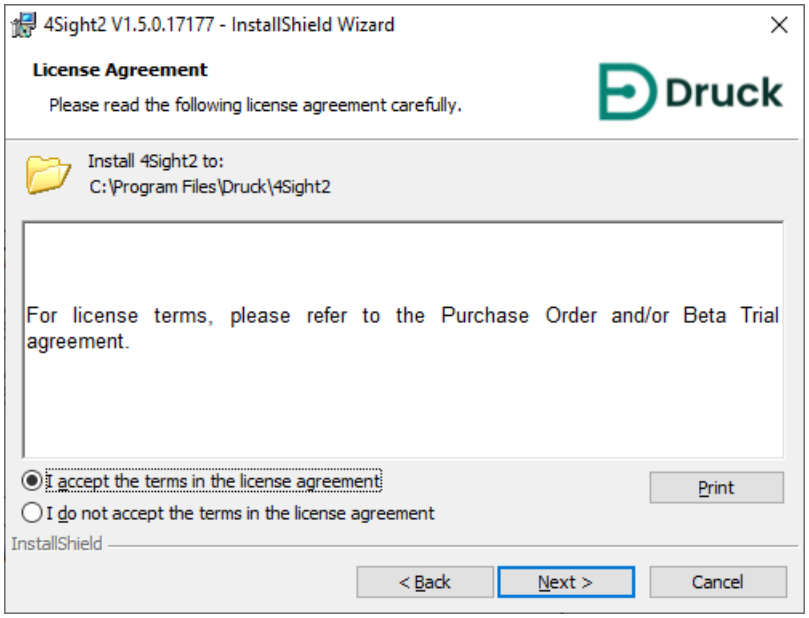


Información del usuario de la aplicación: Esta sección permite introducir el nombre y la contraseña del superusuario para acceder a la aplicación 4Sight2.
Nota: Esta contraseña será necesaria para acceder al contenido de la aplicación 4Sight2 después de la instalación.
Información del usuario de la base de datos: Esta sección permite introducir el nombre de usuario y la contraseña que utilizará la aplicación 4Sight2 para comunicarse con la base de datos PostgreSQL.

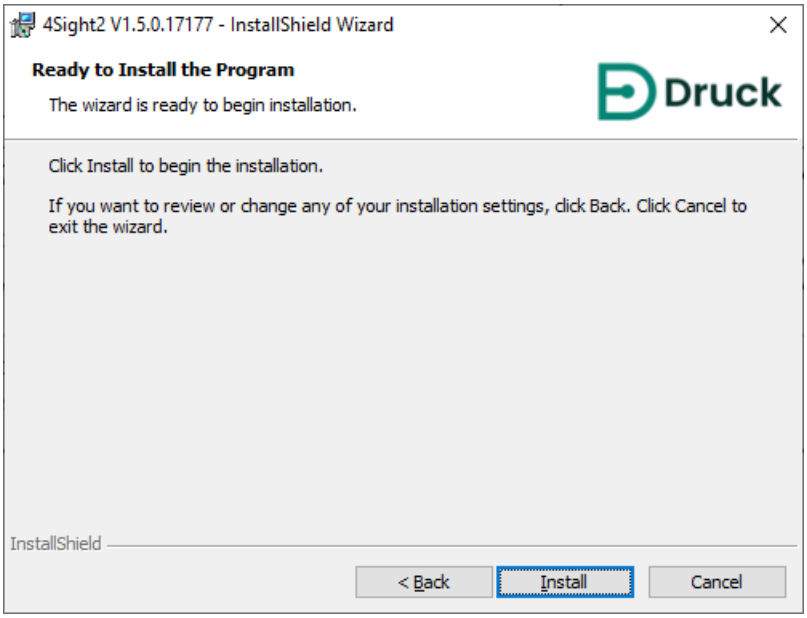
Importante: El usuario debe tomar nota de la contraseña de la base de datos. La pérdida de la contraseña puede conllevar la denegación de acceso o la pérdida de datos. Desactive la casilla de verificación Contraseña predeterminada de usuario para actualizar la contraseña de superusuario de la base de datos. Si desea mantener la contraseña predeterminada o ver la nueva contraseña introducida, seleccione el icono (Mostrar contraseña). Para copiar la contraseña al portapapeles, utilice el icono (Copiar al portapapeles).



5. Una vez haya leído las condiciones de la licencia, seleccione el botón de radio “Acepto la licencia y las condiciones.” y haga clic en **Siguiente**.

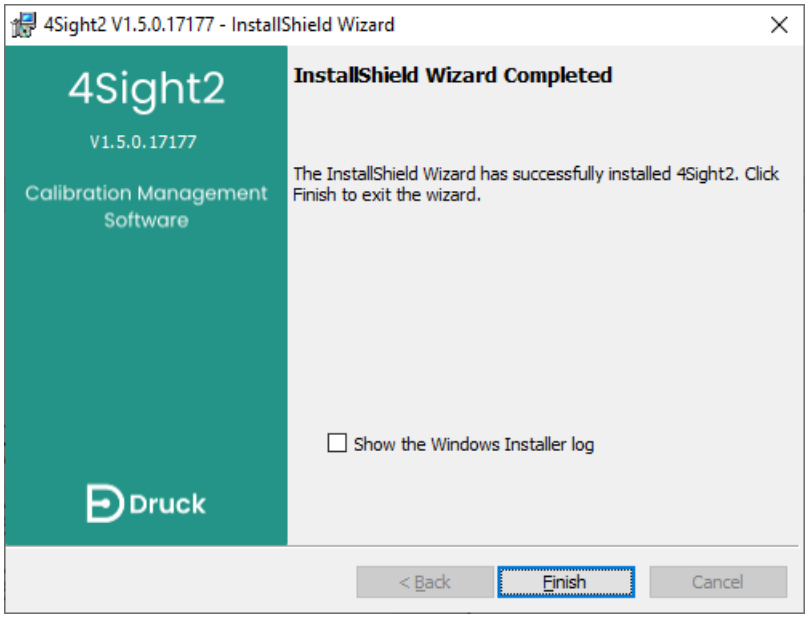


6. Haga clic en **Instalar** para iniciar la instalación. Se instalarán todos los paquetes de software relacionados con la aplicación 4Sight2 y la base de datos.



Enhorabuena, la aplicación 4Sight2 se ha instalado.

7. Haga clic en el botón **Terminar** para cerrar la ventana y siga las instrucciones de la siguiente sección para iniciar sesión en la aplicación 4Sight2.



Para iniciar sesión en 4Sight2 de forma local en el servidor, acceda a

http://Nombre o dirección IP del ordenador:Nro. de puerto/Nombre de la aplicación

- **Nombre del ordenador:** El nombre del PC en el que se ha instalado la aplicación 4Sight2. Para encontrarlo, puede hacer clic con el botón secundario en Este PC y seleccionar las propiedades.
- **Dirección IP:** La dirección IP del PC en el que se ha instalado la aplicación 4Sight2. Para encontrarla, puede ejecutar 'ipconfig' desde el símbolo del sistema de Windows.
- **Nro. de puerto:** El número introducido en el campo Número de puerto Tomcat durante la instalación de la aplicación.
- **Nombre de la aplicación:** El nombre introducido en el campo Nombre de la aplicación durante la instalación de la aplicación.

Instalación de 4Sight2 Test Equipment Communicator

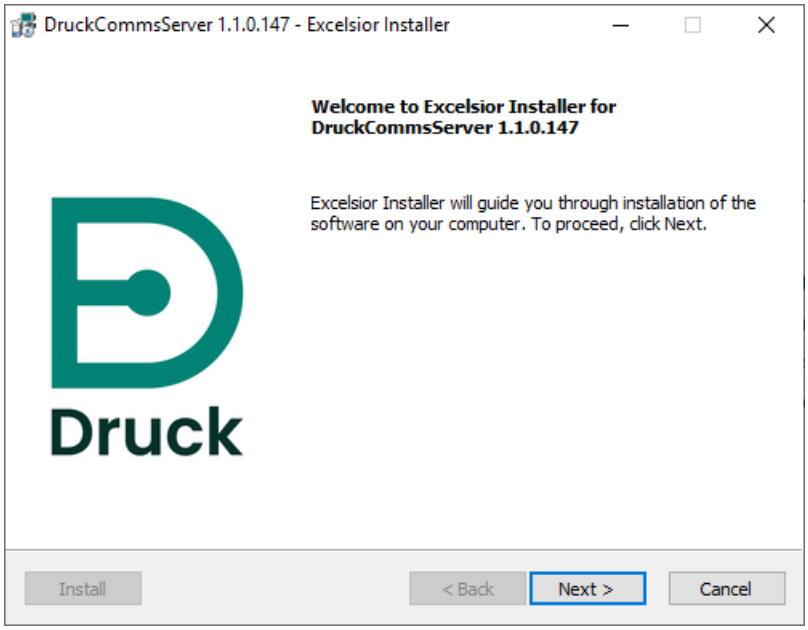
4. Instalación de 4Sight2 Test Equipment Communicator

1. Test Equipment Communicator proporciona los medios para que los instrumentos Druck se comuniquen con la aplicación 4Sight2. Se puede instalar desde la carpeta de instalación de 4Sight2 o bien descargarse durante la comunicación inicial del dispositivo con 4Sight2. Si Test Equipment Communicator no está disponible en el archivo de instalación, una vez se esté ejecutando la aplicación y se haya creado un rango, acceda a Calibración > Portátil a través del menú 4Sight2 como usuario administrativo. Consulte el manual del usuario de 4Sight2 para obtener información sobre la navegación y la creación de rangos. Seleccione el botón de actualización, situado junto a la lista desplegable de equipos de prueba. Si el comunicador del equipo de prueba no se está ejecutando, aparecerá el siguiente mensaje de error:

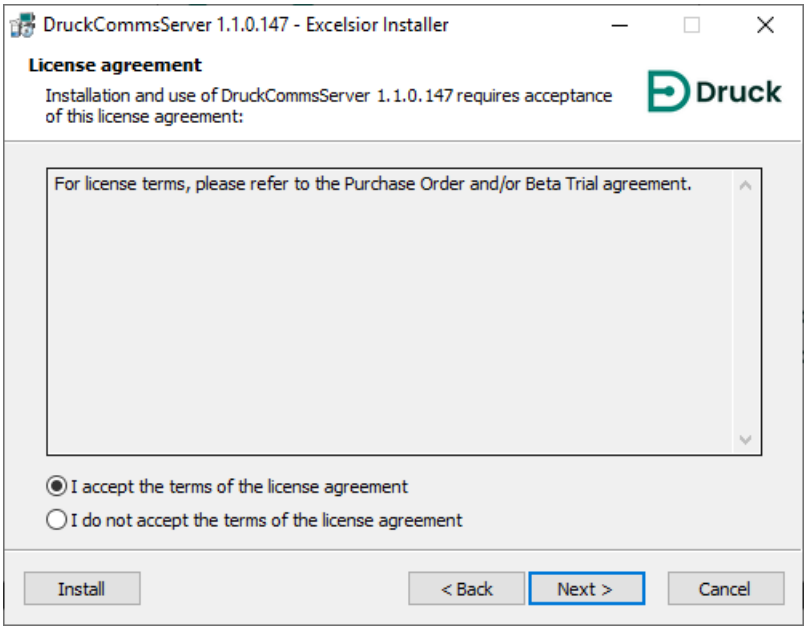
   No se puede establecer la comunicación con el equipo de prueba

   Descargue el paquete Test Equipment Communicator. Una vez realizada la descarga, descomprima y ejecute setup.exe para instalarlo. Para ver las instrucciones de instalación o resolución de problemas, consulte el manual de instalación. Contacte con el administrador si necesita ayuda.

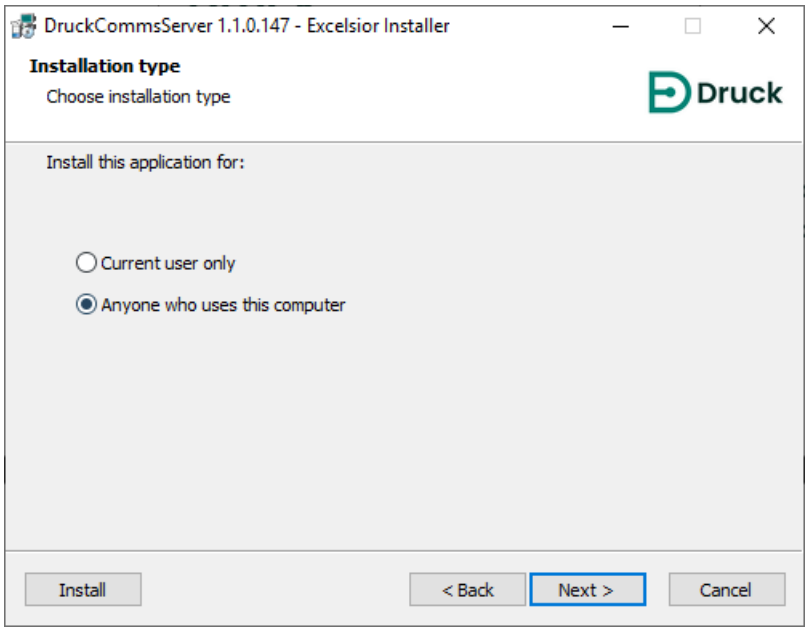
2. Seleccione **Descargar** para obtener el archivo de instalación de Test Equipment Communicator.
3. Los archivos de instalación de Test Equipment Communicator están incluidos en el archivo ZIP CommsServerInstall. Una vez descargado el archivo ZIP de Comms Server, los mismos pasos son válidos antes y después de la instalación de 4Sight2.
4. Extraiga los archivos del archivo ZIP de Comms Server y haga doble clic en el archivo setup.exe para ejecutar el instalador.
5. Aparecerá el instalador de DruckCommsServer. Siga las indicaciones del instalador o las de esta guía.



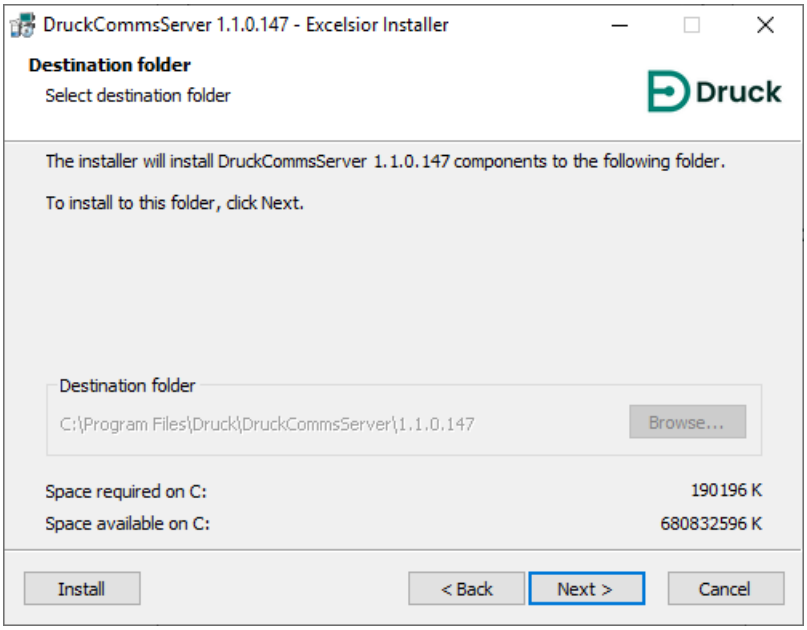
6. Seleccione **Siguiente** para acceder a la pantalla del acuerdo de licencia, lea las condiciones y seleccione **Acepto las condiciones del acuerdo de licencia** y, a continuación, **Siguiente** para continuar.



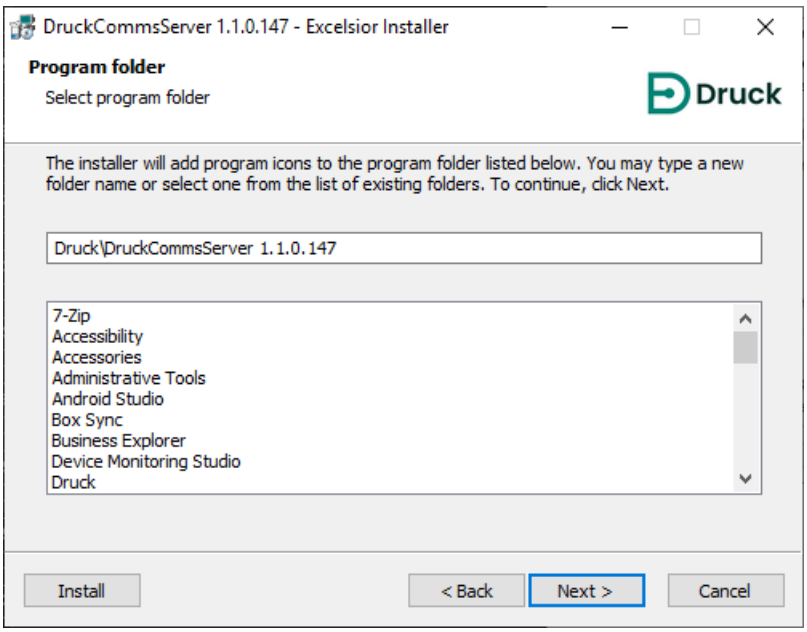
7. En la pantalla Tipo de instalación, seleccione si desea instalar CommsServer para todos los usuarios del PC o solo para el usuario actual.



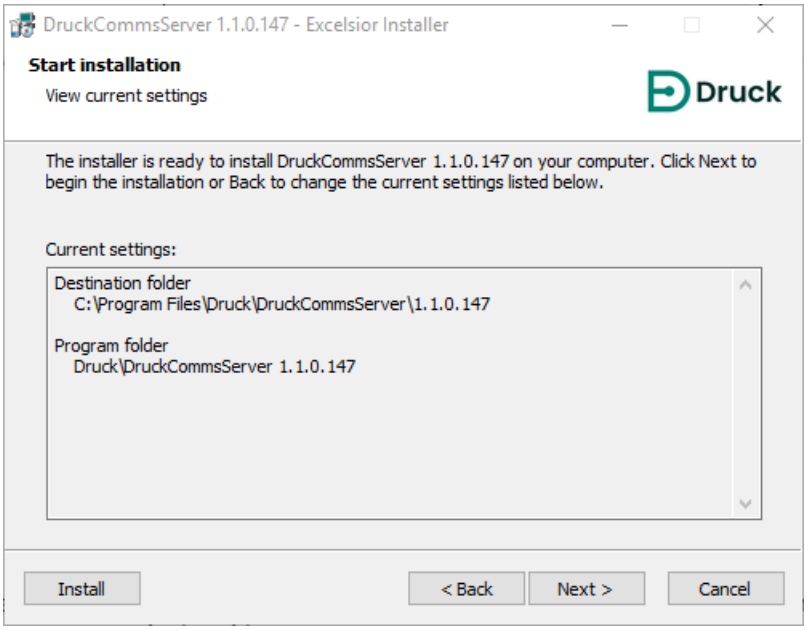
8. La pantalla Carpeta de destino muestra la carpeta en la que se instalará DruckCommsServer. De forma predeterminada, es C:\Program Files\Druck\DruckCommsServer\[versión_aplicación]



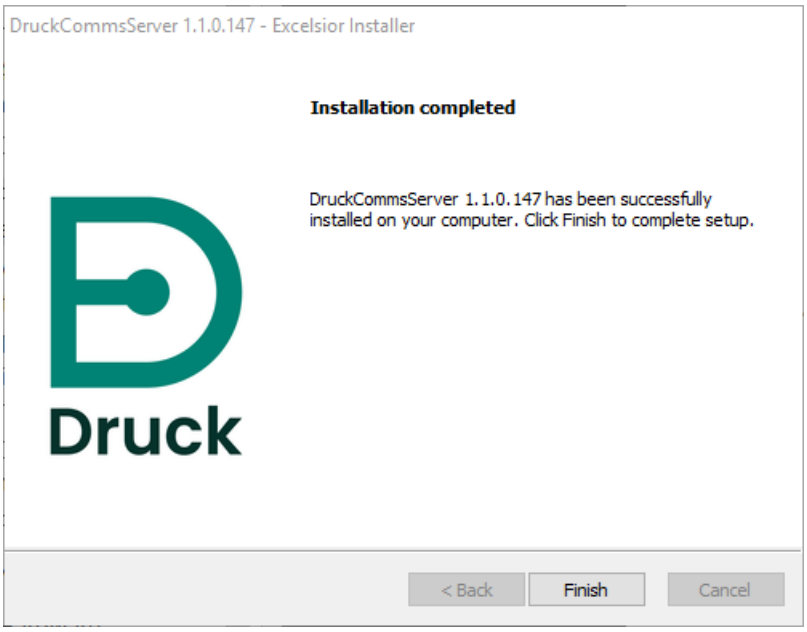
9. La pantalla Carpeta de programa permite seleccionar la ubicación en la que el instalador añadirá el icono de programa a la carpeta de programa.



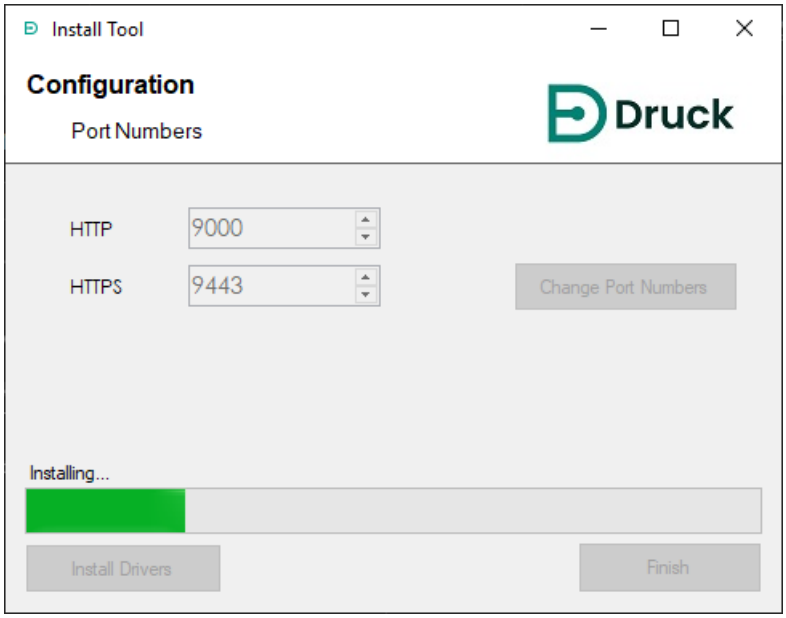
10. Al principio se mostrará la pantalla de instalación. Seleccione **Siguiente** para iniciar la instalación.



11. Una vez finalizada la instalación, seleccione **Finalizar**.

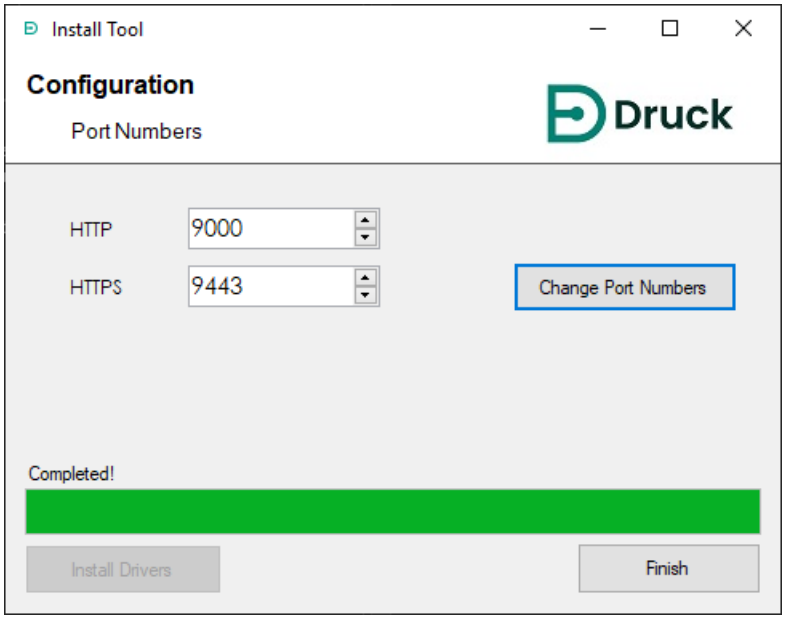


12. A continuación, aparecerá la herramienta de instalación de CommsServer para instalar los controladores adicionales necesarios.



13. En caso de dudas sobre si 4Sight2 utiliza un número de puerto alternativo, contacte con el usuario alternativo.

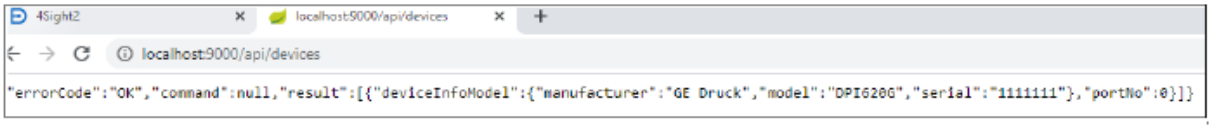
Nota: La herramienta de instalación se puede ejecutar por separado después de instalar o reconfigurar los números de puerto.



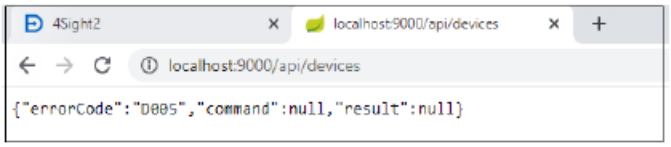
14. Para probar la instalación de Test Equipment Communicator, escriba la siguiente URL en el navegador web:

    http:/localhost:[número de puerto http utilizado superior a 9000]/api/devices

El navegador web debe mostrar la lista de dispositivos conectados:



Si no hay ningún dispositivo conectado, debe aparecer lo siguiente.



Nota: Los controladores que necesitan los calibradores de temperatura no se configurarán automáticamente. Consulte la sección 4.3 Configuración de controladores para calibradores de temperatura.

15. Si la instalación del calibrador del dispositivo no tiene éxito, siga los pasos de la sección siguiente para configurarlos.

4.1 Configuración manual de controladores

La configuración de la política de seguridad de TI puede impedir que los controladores de Druck se configuren automáticamente durante la instalación. Esto será evidente si 4Sight2 no puede comunicarse con los siguientes equipos:

Para la información más reciente, https://www.bakerhughes.com/druck/test-and-calibration-instrumentation/calibration-management-software-4sight2

o

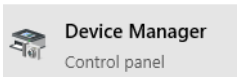
Para solucionar este problema, los controladores de Druck pueden configurarse manualmente. Consulte con el responsable de TI local si no está seguro al respecto o necesita más ayuda.

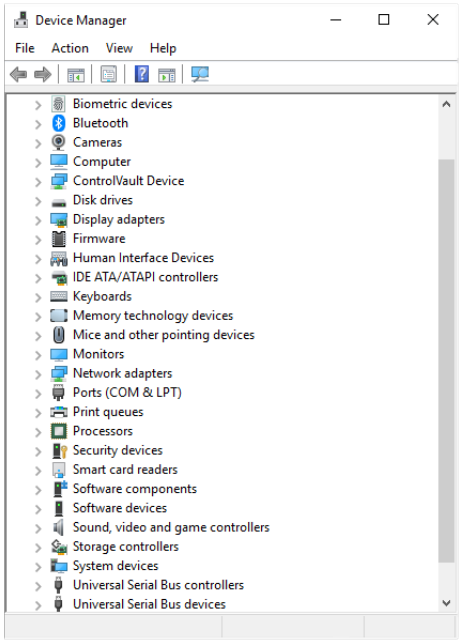
4.1.1 Requisitos previos

Para instalar los controladores, la aplicación 4Sight2 debe estar instalada o ser accesible desde la máquina. Asegúrese de tener acceso a la aplicación 4Sight2 desde el ordenador antes de instalar los controladores.

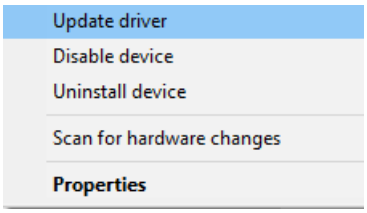
Para instalar manualmente el controlador, lleve a cabo los pasos siguientes.

1. En el escritorio, busque el Administrador de dispositivos y ejecútelo.

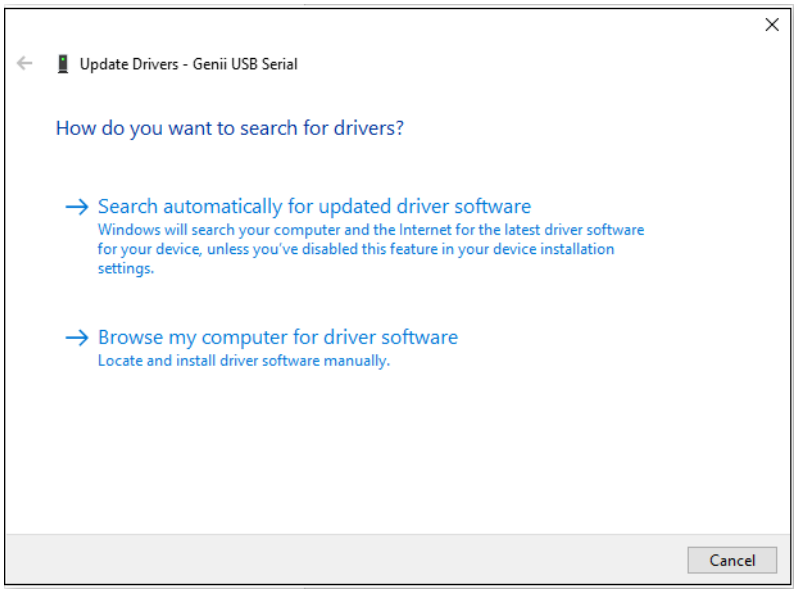




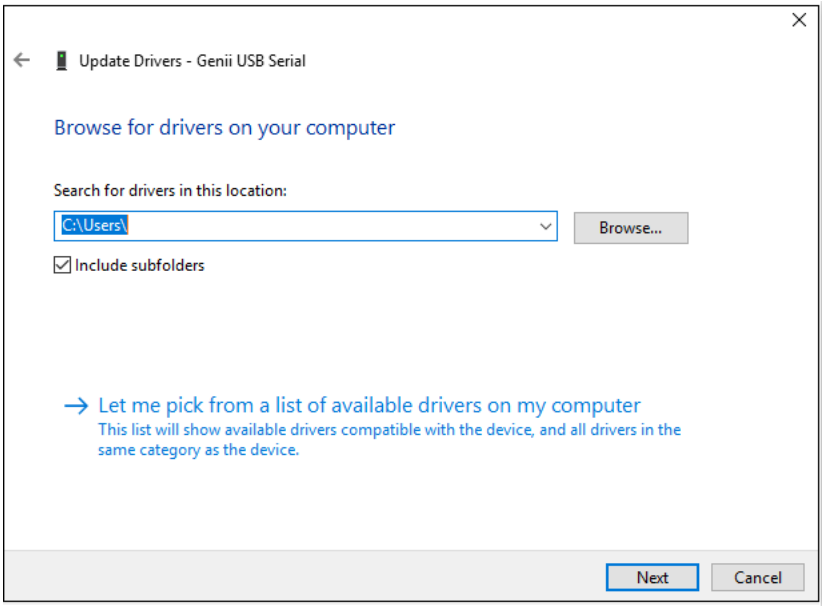
2. Recorra la lista de dispositivos USB para hallar los dispositivos que no están configurados (Dispositivo desconocido u Otros dispositivos). Haga clic con el botón derecho y seleccione **Actualizar controlador**.



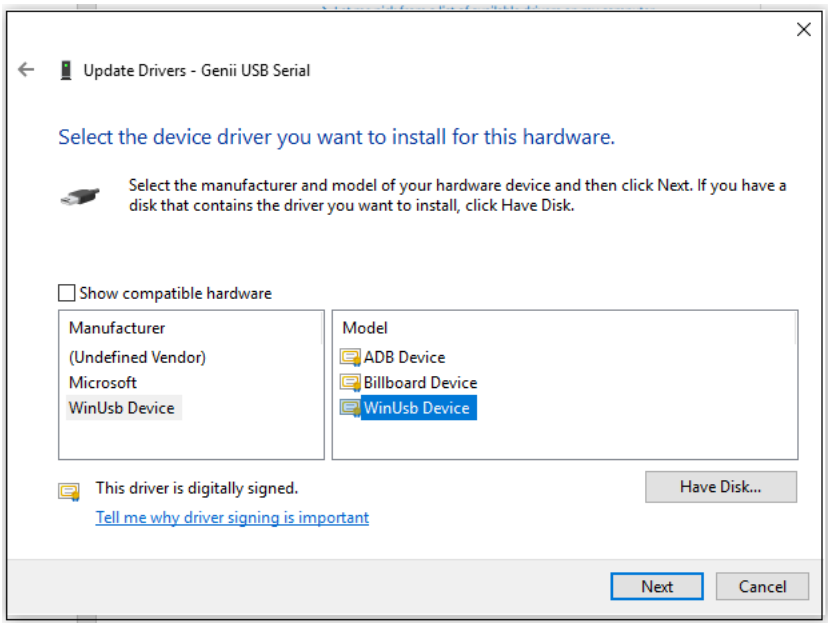
3. Seleccione **Buscar software de controlador en el equipo**.



4. Seleccione **Elegir en una lista de controladores disponibles en el equipo**.

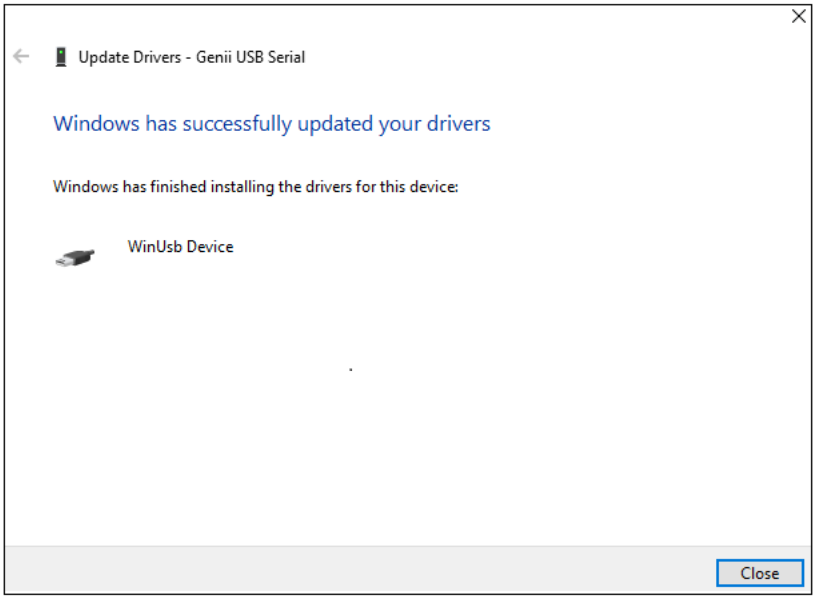


5. Desactive **Mostrar hardware compatible** y seleccione **Dispositivo WinUsb** en Fabricante y **Dispositivo WinUsb** en Modelo.



6. Aparecerá el aviso siguiente. Haga clic en **Sí**.

7. Aparecerá un mensaje para indicar que Windows ha actualizado los controladores correctamente.

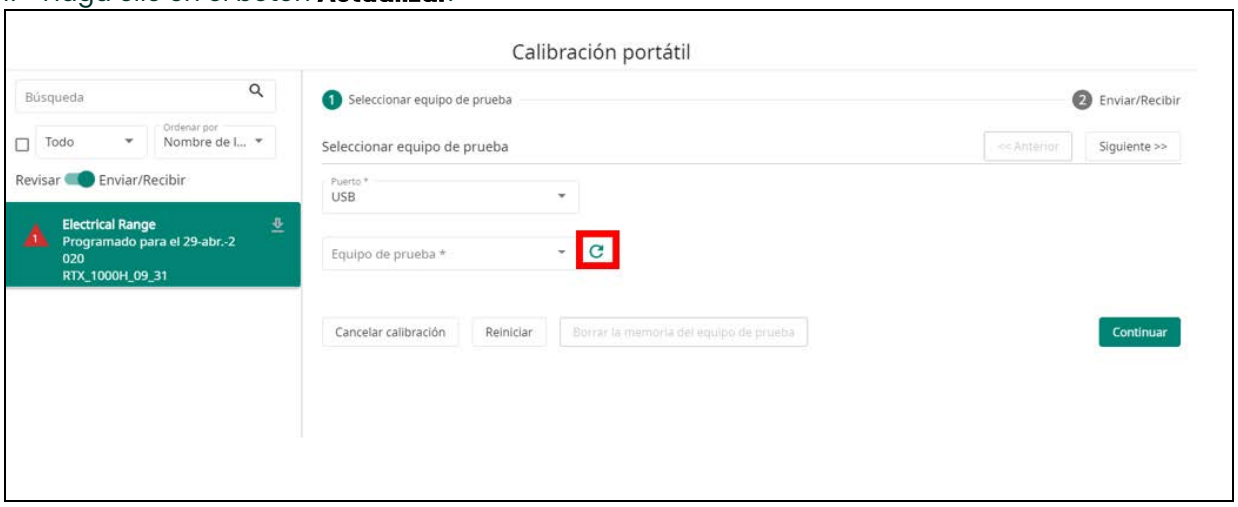


Repita los pasos anteriores para cada categoría de dispositivo cuando conecte el dispositivo por primera vez.

Por ejemplo, si conecta por primera vez un dispositivo PACE y Genii, puede que deba repetir por separado los pasos anteriores para PACE y Genii. Todas las instancias posteriores de PACE y Genii funcionarán normalmente sin necesidad de realizar estos ajustes. No obstante, si conecta posteriormente una categoría de dispositivo diferente, como DPI611/612, deberá repetir estos pasos.

4.2 Prueba de Test Equipment Communicator

1. Inicie sesión en 4Sight2 cómo técnico.
2. Acceda a **Activos >> Lista de trabajo**.
3. Seleccione uno o varios rangos y asígnelos al flujo de trabajo Portátil o Calibración automatizada.
4. Haga clic en el botón **Actualizar**.



5. Haga clic en la lista desplegable **Equipos de prueba**. Si el equipo conectado aparece en la lista, Test Equipment Communicator está configurado correctamente.

4.3 Configuración de controladores para calibradores de temperatura

Para que un calibrador de temperatura se comunique con 4Sight2, es preciso instalar un controlador FTDI.

1. Utilice el siguiente enlace para descargar el controlador FTDI: https://www.ftdichip.com/Drivers/VCP.htm.
2. Extraiga el archivo descargado en formato ZIP y guárdelo en una ubicación conocida de la máquina.
3. Ejecute el Administrador de dispositivos de Windows en la máquina.
4. Selecciona Puertos (COM y LPT) en la lista de dispositivos para ver el calibrador de temperatura.
5. Haga clic con el botón derecho en el calibrador de temperatura y seleccione la opción de actualización de controladores.
6. Seleccione Buscar software de controlador en el equipo.
7. Seleccione Buscar, junto al cuadro de búsqueda denominado Buscar controladores en esta ubicación.
8. Seleccione la carpeta de extracción que contiene la descarga del controlador.
9. Seleccione Siguiente y cierre la ventana.
10. El controlador quedará instalado.
11. Para probar la comunicación con un calibrador de temperatura en 4Sight2, acceda a la calibración automatizada y compruebe si se puede seleccionar el calibrador como controlador de entrada. Alternativamente, repita el procedimiento desde el paso 15 de la sección 4.

Guía de despliegue

5. Guía de despliegue

5.1 Arquitectura de despliegue

La arquitectura habitual incluye la aplicación web 4Sight2 y un servidor UAA (autenticación y autorización de usuarios) que se ejecuta en un servidor web Tomcat con la base de datos PostgreSQL ejecutándose en la misma máquina.

La aplicación web cliente del navegador se conectará al servidor 4Sight2, que a su vez almacena y recupera la información desde la base de datos PostgreSQL.

5.2 Despliegue físico

Se da por sentado que el usuario que instala 4Sight2 ya ha implantado medidas de ciberseguridad conforme a las directivas de seguridad del cliente, incluidas las siguientes:

- El servidor debe estar en una ubicación segura con control de acceso limitado físicamente.
- El control de acceso al servidor debe estar protegido por un acceso con autorización limitada.
- La red del servidor está protegida por el firewall para limitar el acceso a las aplicaciones conocidas sólo a través de los puertos conocidos.
- Las aplicaciones funcionan en su propio contexto y sólo tienen acceso a la base de datos y los sistemas de archivos de su propia carpeta.

5.3 Red

Los clientes se conectan con navegadores web, a través de conexiones Ethernet o de una red inalámbrica. Podría haber una latencia en la red inalámbrica, dependiendo del ancho de banda y del número de dispositivos conectados.

Se recomienda desactivar o retirar los complementos y extensiones que estén instalados en el navegador.

El servidor web 4Sight2 no debe estar expuesto a Internet. Todo acceso se deberá facilitar a través de una intranet o VPN.

5.4 Secuencia de despliegue

PostgreSQL, Tomcat y Java Runtime son requisitos previos para la aplicación. PostgreSQL se instala como paquete independiente, mientras que el resto se instala conjuntamente con la aplicación. Si PostgreSQL ya está instalado en la máquina del usuario, sólo es necesario introducir la contraseña del superusuario para conectarse y configurarlo.

La instalación requiere derechos de administrador de Windows en la máquina. Antes de la instalación, el usuario debe tener la contraseña de superusuario de PostgreSQL. También son necesarios el nombre de usuario y contraseña del administrador de la aplicación y el nombre de usuario y contraseña de la base de datos.

La contraseña de superusuario de PostgreSQL es necesaria para crear la base de datos y otras estructuras en el servidor PostgreSQL. El administrador de la aplicación es el primer usuario de la misma. Es responsable de crear otros usuarios y de asignarles roles. El usuario de la base de datos tiene acceso a 4Sight2 y la base de datos UAA. Las credenciales de este nombre de usuario se utilizan para acceder a la base de datos.

La aplicación se publica en un puerto de la máquina. El número de puerto predeterminado es 8083, pero el usuario puede cambiarlo durante la instalación o más tarde. El contexto predeterminado de la aplicación en Tomcat es 4Sight2.

Siga las instrucciones del procedimiento de protección del sistema operativo de Microsoft o CIS. El procedimiento de instalación le guiará para instalar PostgreSQL antes del servidor 4Sight2.

Test Equipment Communicator se instala en las máquinas cliente cuando un equipo de prueba se conecta a través de los puertos USB. Si Test Equipment Communicator aún no está instalado en la máquina, el usuario deberá descargarlo del servidor 4Sight2 e instalarlo. Test Equipment Communicator escucha el puerto 9000 y sólo se puede comunicar en el nivel seguro.

5.5 Tareas posteriores al despliegue

5.5.1 Añadir usuarios y grupos

El administrador es responsable de crear los distintos usuarios de la aplicación: supervisor, técnico superior, técnico, auditor... y de asignarles a distintos grupos predeterminados. Si se requiere mayor control o granularidad sobre el acceso, el administrador puede crear grupos personalizados y asignarles un acceso específico.

5.5.2 Contraseñas predeterminadas

Utilizamos la contraseña predeterminada codificada de forma rígida para el usuario de tomcat en el archivo "C:\Program Files\Druck\4Sight2\<<latest folder number>>\apache-tomcat\conf\tomcat-user.xml".

Se recomienda cambiar la contraseña predeterminada y utilizar siempre una contraseña que siga las buenas prácticas.

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

Se han aplicado las mejores prácticas para reforzar la seguridad de la aplicación. Si desea obtener mayor seguridad, lleve a cabo las siguientes tareas:

Los archivos y carpetas de configuración están protegidos, Servicio y Sistemas son las únicas cuentas que tienen derechos de acceso de forma predeterminada. Por tanto, antes de realizar las tareas descritas a continuación, el usuario admin solo tiene acceso de lectura y escritura a la carpeta C:\Program Files\Druck\4Sight2\<<latest folder number>>\apache-tomcat\conf, por lo que es necesario abrir el símbolo del sistema con las credenciales del usuario admin.

5.5.3 Comunicación segura

En esta sección se facilitan instrucciones para configurar 4sight2 en modo seguro (modo aka SSL) mediante un certificado autofirmado. Lea detenidamente los supuestos y las condiciones que se definen en la aplicación 4Sight2 antes de proceder. Un certificado autofirmado es un medio para habilitar SSL en 4Sight2. Alternativamente, puede comprar un certificado CA de terceros a proveedores como Symantec, Digicert, etc.

Nota: La simple habilitación de SSL no hace necesariamente que su aplicación sea segura. Se trata de una de las formas más habituales de crear una aplicación web segura.

5.5.3.1 Supuestos y advertencias

Los siguientes supuestos son importantes para el buen funcionamiento de las instrucciones que se detallan a continuación:

El software OpenSSL for Windows es necesario para generar certificados autofirmados. 4Sight2 entiende que las organizaciones y legislaciones regionales y nacionales del cliente le permiten utilizar el software OpenSSL.

- Keytool es una utilidad de gestión de claves y certificados ofrecida por Java que se utiliza para generar distintos componentes que interfieren en la configuración https. 4Sight2 entiende que las organizaciones y legislaciones regionales y nacionales del cliente le permiten utilizar la utilidad Keytool.
- Necesitará privilegios administrativos para realizar las configuraciones que se describen a continuación. Para obtener más información sobre cómo obtener derechos administrativos, contacte con su departamento de informática.
- Los pasos siguientes requieren conocimientos básicos de los procesos informáticos. Se recomienda realizar tales pasos bajo la supervisión del departamento de informática.
- El contenido que se presenta en este documento, como nombres de host, contraseñas, URL y rutas a carpetas, tiene carácter ilustrativo. Asegúrese de modificar los comandos en consecuencia antes de su ejecución.
- Las secciones siguientes abarcan dos escenarios. Uno de ellos es en que el cliente y el servidor residen en la misma máquina. En el segundo, el cliente y el servidor residen en máquinas distintas (escenario de varios clientes).

5.5.3.2 Pasos para la configuración de la aplicación 4Sight2 en Https

1. Detenga 4Sight2 en los servicios de Windows
2. Abra el símbolo del sistema en **modo de administrador**.
3. Navegue hasta la siguiente carpeta, situada bajo el directorio de instalación de 4Sight2. Para ello ejecute el comando siguiente:

   cd "C:\Program Files\Druck\4Sight2\<<latest folder number>>\apache-tomcat\conf"
4. Compruebe si keytool está presente ejecutando el siguiente comando desde el símbolo del sistema: **Keytool** -?

   De no ser así, establezca la ruta de acceso de entorno a JRE bin en la carpeta de instalación de 4Sight2 como se muestra a continuación. Actualice la ruta de acceso correcta en función de la carpeta de inatalación.

   C:\Program Files\Druck\4Sight2\<<latest folder number>>\jre\bin
   Set "Path=%Path%;C:\Program Files\Druck\4Sight2\<<latest folder number>>\jre\bin"
5. Para crear el nuevo certificado, siga en el paso 6. En caso contrario, si ya existe un certificado, siga estos pasos:

   a. Compruebe si ya existe el archivo de certificado de 4Sight.jks en el almacén de claves de java.

   keytool -list -alias <<nombre de host>> -storepass <<ContraseñaDeClave>> -keystore 4Sight.jks

   b. Si el certificado ya está instalado, elimínelo.

keytool -delete -noprompt -alias <<nombre de host>> -storepass <<ContraseñaDeClave>> -keystore 4Sight.jks

c. Compruebe si existe el archivo 4SightV2PublicKey.cer y, en caso afirmativo, elimínelo.
del "../../app/Certificate/4SightV2PublicKey.cer"

d. Compruebe si el certificado ya existe en el cacert de java.
keytool -list -alias <<nombre de host>> -storepass changeit -keystore "../../jre/lib/security/cacerts"

e. Elimine el certificado si existe en el almacén de java.
keytool -delete -noprompt -alias <<nombre de host>> -storepass changeit -keystore "../../jre/lib/security/cacerts" -file "../../app/Certificate/4SightV2PublicKey.cer"

6. Cree el nuevo certificado con la siguiente instrucción:

   keytool -genkey -trustcacerts -keyalg "RSA" -keysize 2048 -validity 1095 -keypass <<ContraseñaDeClave>> -alias <<nombre de host>> -keystore 4Sight.jks -storepass <<ContraseñaDeAlmacenamiento>> -dname "CN=%COMPUTERNAME%, OU=<<Unidad Organizativa>>, O=<<Organización>>, L=<<Ubicación>>, S=<<Estado>>, C=<<InicialDePaís>>" -ext eku:critical=sa

7. Exporte el certificado al archivo 4SightV2PublicKey.cer (no cambie el nombre del archivo ni la ruta).

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

   Una vez ejecutado el comando correctamente, se mostrará el mensaje "Certificado guardado en el archivo C:\Program Files\Druck\4Sight2\<<latest folder number>>\app\Certificate\4SightV2PublicKey.cer".

8. Importe el certificado al archivo java CACert.

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

Una vez ejecutado el comando correctamente, aparecerá el mensaje "El certificado se ha añadido al almacén de claves".

9. Cree la entrada del certificado en el archivo de configuración de Tomcat.

   a. Abra el archivo server.xml en la ubicación siguiente.
   C:\Program Files\Druck\4Sight2\<<latest folder number>>\apache-tomcat\conf\server.xml"

   b. Cree la siguiente entrada en server.xml.
   <Connector port="8443" protocol="org.apache.coyote.http11.Http11NioProtocol" maxThreads="150" SSLEnabled="true" sslProtocol="TLSv1.2" keystoreFile="conf/4Sight.jks"
   keystorePass="<<ContraseñaDeClaveKeyPassword>>" keyAlias="tomcat" scheme="https" secure="true" clientAuth="false" />

   c. Comente la siguiente sección para inhabilitar las conexiones http.
   <connectionTimeout="20000" maxSwallowSize="104857600" port="8083" protocol="HTTP/1.1" redirectPort="8443" relaxedPathChars=""[\]^`{|}+" relaxedQueryChars="&quot;[\]^`{|}+"/>

Nota: La aplicación no funcionará si no hace este comentario.

10. Llegado este punto, la configuración Https de la aplicación 4Sight2 habrá finalizado.
11. Para comprobar las configuraciones realizadas, reinicie el servicio 4Sight2 en Windows Service.
12. Abra Google Chrome, borre la caché del navegador y reinicie el navegador.
13. Escriba la siguiente URL en el navegador: https://<<nombre de host>>:8443/4sight2

- La primera vez, el tiempo de carga de la URL puede ser superior.
- Aparecerá una pantalla con el siguiente mensaje "Su conexión no es privada".
- Haga clic en el botón **Avanzado** >> **Seguir en XX**.
- Si no aparece la pantalla 4sight2, haga clic en el botón**Volver a cargar**.
- Volverá a la página de 4sight2.
- Aparecerá un error "No seguro" en la barra de direcciones que puede que desaparezca después de registrar el certificado en mmc.

5.5.3.3 Pasos para configurar DruckCommsServer en Https si se ha instalado en el equipo servidor

Reemplace los valores en << >> con datos adecuados antes de ejecutar el comando.

1. Detenga DruckCommsServer2 en los servicios de Windows.
2. Abra el símbolo del sistema en **modo de administrador**.
3. Compruebe si keytool está presente ejecutando el siguiente comando desde el símbolo del sistema: **Keytool -?**

   De no ser así, establezca la ruta de acceso de entorno a JRE bin en la carpeta de instalación de 4Sight2 como se muestra a continuación.
   Actualice la ruta de acceso correcta en función de la carpeta de instalación.
   C:\Program Files\Druck\4Sight2\<<latest folder number>>\jre\bin
   Set "Path=%Path%;C:\Program Files\Druck\4Sight2\<<latest folder number>>\jre\bin"
4. Navegue hasta la siguiente carpeta, situada en el directorio de instalación de DruckCommServer. Para ello ejecute el comando siguiente:

   cd " C:\Program Files\Druck\DruckCommsServer\<<VersiónDeCommunicationService>>"
5. Siga estos pasos para comprobar si ya existe un certificado.

   a. Compruebe si el certificado ya existe en el cacert de java.
   keytool -list -alias tomcat -storepass changeit -keystore cacerts

   b. Elimine el certificado si existe en el almacén de java.
   keytool -delete -noprompt -alias tomcat -storepass changeit -keystore cacerts

   c. Elimine los certificados preconfigurados de CommsServer incluidos de forma predeterminada.
   del 4Sight.jks
   del 4SightV2DeviceMngr.pfx
6. Cree el nuevo certificado con la siguiente instrucción:

   keytool -genkey -trustcacerts -keyalg "RSA" -keysize 2048 -validity 1095 -keypass <<ContraseñaClave>> -alias tomcat -keystore CommServer.jks -storepass

<<ContraseñaAlmacén>> dname "CN=localhost, OU=<<Unidad de organización>>, O=<<Organización>>, L=<<Ubicación>>, S=<<Estado>>, C=<<Inicial del país>>" -ext eku:critical=sa

7. Exporte el certificado al archivo DruckCommServer.cer

   keytool -export -alias tomcat -keystore CommServer.jks -storepass <<ContraseñaAlmacén>> -storetype JKS -file DruckCommServer.cer
   Una vez ejecutado el comando correctamente, se mostrará el mensaje "Certificado almacenado en el archivo DruckCommServer.cer".

8. Importe el certificado de Comm Server al archivo java CACert.

   keytool -import -noprompt -trustcacerts -alias tomcat -storepass changeit -keystore cacerts -file DruckCommServer.cer
   Una vez ejecutado el comando correctamente, aparecerá el mensaje "El certificado se ha añadido al almacén de claves".

9. Importe el certificado de 4Sight al archivo java CACert.

   keytool -import -noprompt -trustcacerts -alias <<nombre de host del servidor>> -storepass changeit -keystore cacerts -file "C:\Program Files\Druck\4Sight2\<<latest folder number>>\app\Certificate\4SightV2PublicKey.cer"
   Una vez ejecutado el comando correctamente, aparecerá el mensaje "El certificado se ha añadido al almacén de claves".

10. Edite la contraseña del almacén de claves para application.properties en DruckCommsServer.

    Abra el siguiente archivo:
    C:\Program Files\Druck\DruckCommsServer\<<VersiónDeCommunicationService>\application.properties y cambie la siguiente línea:
    keystore = CommServer.jks
    key-store.password= << ContraseñaAlmacén >>
    Nota: **<< ContraseñaAlmacén >>** es el valor **ContraseñaAlmacén** utilizado en el paso 6.

11. Reinicie los servicios 4Sight2 y DruckCommsServer.

5.5.3.4 Pasos para configurar DruckCommsServer en HTTPs si se ha instalado en un equipo cliente

1. La utilidad Keytool está incluida en Java y permite instalar Java en un equipo o comprobar directamente la disponibilidad de java keytool sin necesidad de instalar Java.
2. Detenga DruckCommsServer2 en los servicios de Windows.
3. Abra el símbolo del sistema en **modo de administrador**.
4. Compruebe si keytool está presente ejecutando el siguiente comando desde el símbolo del sistema: **Keytool -?**

   Si no lo está, establezca la ruta de acceso de entorno a JRE bin si Java se ha instalado en la máquina o establézcala a keytool, como se muestra a continuación.
   Actualice la ruta de acceso correcta en función de la carpeta de instalación.
   C:\Program Files\Java\<< Versión Java >>\bin
   Set Path=%Path%; "C:\Program Files\Java\<< Versión Java >>\bin"

5. Obtenga el archivo **4SightV2PublicKey.cer** del equipo servidor en el que se ha instalado la aplicación 4Sight. El archivo se encuentra en la siguiente ubicación del servidor:

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

6. Copie **4SightV2PublicKey.cer** a la ruta siguiente:
   C:\Program Files\Druck\DruckCommsServer\<< Versión Communication Service >>
7. Siga los pasos 4-8 de la sección 5.5.3.3.
8. Importe el certificado de 4Sight al archivo java CACert.
   keytool -import -noprompt -trustcacerts -alias <<nombre de host servidor>> -storepass changeit -keystore cacerts -file 4SightV2PublicKey.cer
   Una vez ejecutado el comando correctamente, aparecerá el mensaje "El certificado se ha añadido al almacén de claves".
9. Siga los pasos 10-11 de la sección 5.5.3.3.

5.5.3.5 Pasos para generar un certificado autofirmado para 4Sight2

1. Descargue e instale Open SSL for Windows.
2. Detenga 4Sight2 en los servicios de Windows.
3. Cree una nueva carpeta con el nombre **4Sight2Certificate** en la unidad C.
   Puede elegir cualquier ubicación o nombre de carpeta siempre que cuente con acceso administrativo a la misma.
4. Utilice el Bloc de notas para crear un nuevo archivo en la carpeta y guárdelo como **openssl-ca.cnf**.
   Copie el contenido siguiente al archivo y guárdelo.

```
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
```

Nota: Actualice el **[Company Name]** arriba y guarde el archivo. Este es el nombre del emisor del certificado que aparecerá en la consola de administración.

5. Utilice el Bloc de notas para crear un nuevo archivo en la carpeta y guárdelo como **openssl-server.cnf**.

Copie el contenido siguiente al archivo y guárdelo.

```
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
```

Nota: Actualice el nombre de host (Host name of server) y la dirección IPv4 (IP Address of server) y guarde el archivo.

6. Abra el símbolo del sistema con privilegios administrativos.
7. Acceda a la carpeta 4Sight2Certificate con el siguiente comando.

   cd "<<ruta de acceso completa a 4Sight2Certificate >>"
8. Establezca la variable de ruta de acceso a la carpeta OpenSSL bin con el siguiente comando.

   Set path=%path%;"<<carpeta bin de openssl>>"

   Ejemplo de ruta de acceso predeterminada:

   Set Path=%Path%;"C:\Program Files\OpenSSL-Win64\bin"
9. Establezca la variable de ruta de acceso a la carpeta JRE bin con el siguiente comando. Nota: La ruta de acceso puede ser otra.

   Set path=%path%;"C:\Program Files\Druck\4Sight2\<<latest folder number>>\jre\bin"
10. Ejecute el comando siguiente para generar los archivos cacert.pem y cakey.pem:

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

    Introduzca los datos correctos del certificado cuando lo pida el sistema (país, estado, etc.).
11. Ejecute los comandos siguientes para generar los archivos servercert.csr y serverkey.pem:

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

    Introduzca los datos correctos del certificado cuando lo pida el sistema (país, estado, etc.).
12. Utilice el Bloc de notas para crear un nuevo archivo con el nombre index.txt. Guarde el archivo en la carpeta 4Sight2Certificate.
13. Utilice el Bloc de notas para crear un nuevo archivo con el nombre serial.txt. Guarde el archivo en la carpeta 4Sight2Certificate.

    Abra el archivo y escriba **01**. Guarde y cierre el archivo.
14. Ejecute el comando siguiente para generar nuevos certificados en los archivos servercert.pem y serverkey.pem.

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

    Escriba Y para aplicar los cambios. Se mostrará la base de datos actualizada después de la ejecución.
15. Ejecute el comando siguiente para crear un paquete de los archivos de clave existentes en formato PFX.

    openssl pkcs12 -export -in servercert.pem -inkey serverkey.pem -certfile cacert.pem -name "<<nombre de host>>" -out <<nombre de host>>.p12

    Se le pedirá que introduzca dos veces la contraseña.

16. Convierta el almacén PFX en almacén de claves Java ordenado por la ubicación JRE bin indicada anteriormente (tomcat/config path).

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

    Nota: Utilice la misma contraseña para los dos almacenes. Asegúrese de señalar al archivo 4Sight.jks presente en la carpeta config de tomcat como se ha mostrado anteriormente.
    Se le pedirá que introduzca la contraseña del almacén de claves de destino y la contraseña del almacén de claves de origen. Una vez ejecutado correctamente el comando, aparecerá el mensaje "Comando de importación finalizado: Se ha importado correctamente 1 entrada".

17. Exporte el certificado del almacén de claves java al siguiente archivo:

    C:\Program Files\Druck\4Sight2\<<latest folder number>>\app\Certificate\4SightV2PublicKey.cer
    keytool -export -alias <<nombre de host>> -keystore "C:\Program Files\Druck\4Sight2\<<latest folder number>>\apache-tomcat\conf\4Sight.jks" -storePass "<<contraseña>>" -storetype JKS
    -file "C:\Program Files\Druck\4Sight2\<<latest folder number>>\app\Certificate\4SightV2PublicKey.cer"

    Nota: Asegúrese de señalar al archivo 4Sight.jks presente en la carpeta config de tomcat como se ha mostrado anteriormente.
    Una vez ejecutado correctamente el comando, se mostrará el mensaje Certificado almacenado en el archivo.

18. Importe el archivo de certificado a la carpeta cacerts, ubicada en el directorio de instalación de 4sight2.

    Nota: La ruta de acceso puede variar en función del directorio de instalación y de la versión de 4sight2.

    keytool -import -noprompt -trustcacerts -alias <<nombre de host>> -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"

    Nota: Por alguna razón, el alias que intenta crear ya existe. Ejecute el comando siguiente para borrarlo primero y ejecute después el comando anterior para crear un alias nuevo.

    keytool -delete -noprompt -trustcacerts -alias <<nombre de host>> -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"

    Una vez ejecutado correctamente el mensaje, aparecerá el mensaje "El certificado se ha añadido al almacén de claves".

19. Haga el siguiente cambio en el archivo server.xml file (en C:\Program Files\Druck\4Sight2\<<latest folder number>>\apache-tomcat\conf).

    a. Cree la siguiente entrada en 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. Comente la siguiente sección para inhabilitar las conexiones http.
<connectionTimeout="20000" maxSwallowSize="104857600" port="8083"
protocol="HTTP/1.1" redirectPort="8443" relaxedPathChars=""[\]^`{|}+"
relaxedQueryChars=""[\]^`{|}+"/>

20. Se ha completado la configuración de https para 4Sight2. Inicie ahora el servicio 4sight2 desde los servicios de Windows.

5.5.3.6 Pasos para configurar un certificado autofirmado para DruckCommServer si se ha instalado en un equipo servidor

Como premisa, se entiende que ha convertido correctamente la aplicación 4sight2 a HTTPs ejecutando los pasos de la sección 5.5.3.5 y que los archivos siguientes ya están en la carpeta **4Sight2Certificate**:

- openssl-server.cnf
- openssl-ca.cnf
- cacert.pem
- cakey.pem
- index.txt
- serial.txt
- 4SightV2PublicKey.cer (este archivo puede estar en la carpeta C:\Program Files\Druck\4Sight2\<<latest folder number>>\app\Certificate)

1. Cree una nueva carpeta **CommserverCertificate** y copie los archivos anteriores. Realice los cambios siguientes:

- openssl-server.cnf

  En la sección **req**, cambie el valor de **default_keyfile** a "**DruckCommServerCertKey.pem**".

  - En **server_distinguished_name**, cambie el valor de **commonName** a "**localhost**".
  - En **alternate_names**, cambie el valor de **DNS.1** a "**localhost**".
  - En **alternate_names**, cambie el valor de **IP.1** a "**127.0.0.1**"
  - Guarde el archivo.
- openssl-ca.cnf. (No cambie su contenido)
- cacert.pem. (No cambie su contenido)
- index.txt (Elimine todo su contenido hasta que quede vacío)
- serial.txt (Elimine todo su contenido hasta que quede solo la entrada 01)

2. Detenga el servicio Druck CommsServer en los servicios de Windows.
3. Abra el símbolo del sistema con privilegios administrativos.
4. Acceda a la carpeta **CommserverCertificate** con el siguiente comando.

   cd "<<ruta de acceso completa a CommserverCertificate >>"

5. Establezca la variable de ruta de acceso a la carpeta OpenSSL bin con el siguiente comando.

   Set path=%path%;"<<carpeta bin de openssl>>"

   Ejemplo de ruta de acceso predeterminada:

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

6. Establezca la variable de ruta de acceso a la carpeta JRE bin con el siguiente comando. Nota: La ruta de acceso puede ser otra.

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

7. Una vez finalizada esta operación, ejecute el siguiente comando para crear una solicitud de certificado de Comm Server.

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

   Una vez ejecutado este comando, dispondrá de una solicitud en **DruckCommServer.csr** y de una clave privada en **DruckCommServerCertKey.pem**.

8. A continuación, ejecute este comando para registrar la solicitud de csr en su ca:

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

9. A continuación, cree un archivo PFX con alias **tomcat** para comm server con el siguiente comando,

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

10. Convierta el almacén PFX en almacén de claves Java con keytool.

    Nota: Utilice la misma contraseña para el almacén de claves.

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

11. A continuación, importe el certificado a cacert.

    a. Elimine el alias de tomcat existente (incluido de forma predeterminada con la instalación).

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

    b. Una vez eliminado el alias de tomcat existente, importe el certificado a cacerts con el comando siguiente:

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

12. Llegado este punto, es necesario importar la clave pública de 4sight al cacert de CommServer para autenticar la comunicación. Para ello, ejecute el comando siguiente:

    keytool -import -noprompt -trustcacerts -alias <<Nombre de host del servidor 4sight>> -storepass changeit -keystore "C:\Program Files\Druck\DruckCommsServer\<< Versión de Communication Service >>\cacerts" -file "C:\Program Files\Druck\4Sight2\<<latest folder number>>\app\Certificate\4SightV2PublicKey.cer"

13. Una vez completados estos pasos, los archivos **DruckCommServer.pfx** y **CommServer.jks** estarán en la carpeta **CommserverCertificate** actual.

Copie estos archivos y péguelos en el directorio "C:\Program Files\Druck\DruckCommsServer\<< Versión de Communication Service >>\". Edite **application.properties** en la misma ubicación para cambiar el valor de la propiedad como se indica a continuación:

a. Keystore = CommServer.jks

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

c. key-store.type=JKS

5.5.3.6.1 Instalación del certificado en Windows para 4sight y DruckCommsServer

1. Abra Ejecutar y escriba "mmc". Pulse Intro.
2. Acceda a Archivo y seleccione Agregar/Eliminar complementos.
3. En el menú de la izquierda, seleccione Certificados. Pulse Agregar y seleccione Cuenta de equipo >> Siguiente >> Terminar. Haga clic en Aceptar.
4. Expanda la sección de certificados (equipo local). Expanda Entidades de certificación raíz de confianza.

   Haga clic con el botón secundario en Carpeta de certificados >> Todas las tareas >> Importar.

   Seleccione cacert.pem >> Siguiente >> Terminar.

   Nuestra entidad CA personalizada se instala correctamente en una entidad de confianza.

Una vez completados todos estos pasos, inicie el servicio DruckCommsServer.

5.5.3.7 Pasos para configurar un certificado autofirmado para DruckCommServer si se ha instalado en un equipo cliente

Para convertir DruckCommsServer a HTTPs, debe disponer de las utilidades java keytool y OpenSSL.

1. La utilidad Keytool está incluida en Java y permite instalar Java en un equipo o comprobar directamente la disponibilidad de java keytool sin necesidad de instalar Java.
2. Descargue e instale OpenSSL for Windows.
3. Establezca la variable de ruta de acceso a la carpeta OpenSSL bin con el siguiente comando.

   Set path=%path%;"<<carpeta bin de openssl>>"

   Ejemplo de ruta de acceso predeterminada:

   Set Path=%Path%;"C:\Program Files\OpenSSL-Win64\bin"
4. Establezca la variable de ruta de acceso a la carpeta JRE bin con el siguiente comando.

   C:\Program Files\Java\<< Versión Java >>\bin

   Set Path=%Path%; "C:\Program Files\Java\<< Versión Java >>\bin"
5. Detenga el servicio DruckCommsServer en los servicios de Windows.
6. Cree una nueva carpeta llamada **CommserverCertificate** en la unidad C o en cualquier otra unidad.
7. Obtenga el archivo de certificado público **4SightV2PublicKey.cer** del archivo servidor, ubicado en C:\Program Files\Druck\4Sight2\<<latest folder number>>\app\Certificate, y cópielo a la carpeta **CommserverCertificate**.
8. Cree los archivos **openssl-server.cnf** y **openssl-ca.cnf**. Para ello, siga los pasos 4 y 5 de la sección 5.5.3.5 y cree index.txt y serial.txt siguiendo los pasos 12 y 13 en la carpeta **CommserverCertificate**.
9. Ahora, la carpeta CommServerCertificate contendrá cinco archivos.

   a. openssl-server.cnf

   b. openssl-ca.cnf

   c. index.txt

d. serial.txt
e. 4SightV2PublicKey.cer

10. Abra el símbolo del sistema con privilegios administrativos.

    Acceda a la carpeta CommserverCertificate con el siguiente comando.
    cd "<<ruta de acceso completa a CommserverCertificate >>"

11. Ejecute el comando siguiente para generar los archivos cacert.pem y cakey.pem:

    openssl req -x509 -config openssl-ca.cnf -newkey rsa:4096 -sha256 -nodes -out cacert.pem -outform PEM
    Introduzca los datos correctos del certificado cuando lo pida el sistema (país, estado, etc.).

12. Cambie el contenido de los archivos de la carpeta **CommserverCertificate**. Para ello, siga el paso 1 de la sección 5.5.3.6.

13. Ejecute los pasos 7-11 de la sección 5.5.3.6.

14. Llegado este punto, es necesario importar la clave pública de 4sight al cacert de CommServer para autenticar la comunicación. Para ello, ejecute el comando siguiente:

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

15. Una vez completados estos pasos, los archivos **DruckCommServer.pfx** y **CommServer.jks** estarán en la carpeta **CommserverCertificate** actual.

    Copie estos archivos y péguelos en el directorio "C:\Program Files\Druck\DruckCommsServer\<< Versión de Communication Service >>\". Edite **application.properties** en la misma ubicación para cambiar el valor de la propiedad como se indica a continuación:

    a. Keystore = CommServer.jks
    b. key-store.password = << ContraseñaAlmacénClaves >>
    c. key-store.type=JKS

5.5.3.7.1 Instalación del certificado en Windows para DruckCommsServer

1. Abra Ejecutar y escriba "mmc". Pulse Intro.
2. Acceda a Archivo y seleccione Agregar/Eliminar complementos.
3. En el menú de la izquierda, seleccione Certificados. Pulse Agregar y seleccione Cuenta de equipo >> Siguiente >> Terminar. Haga clic en Aceptar.
4. Expanda la sección de certificados (equipo local). Expanda Entidades de certificación raíz de confianza.

   Haga clic con el botón secundario en Carpeta de certificados >> Todas las tareas >> Importar.
   Seleccione cacert.pem >> Siguiente >> Terminar.
   Nuestra entidad CA personalizada se instala correctamente en una entidad de confianza.

Una vez completados todos estos pasos, inicie el servicio DruckCommsServer.

Si solo quiere comprobar si DruckCommsServer se ha convertido correctamente a https, abra el siguiente enlace en la ficha Google Chrome: **https://localhost:9443/api/devicemanager/version** (Introduzca el número de puerto de su servidor de comunicaciones si es distinto al predeterminado: 9443)

5.5.3.8 Validación del certificado en 4Sight2

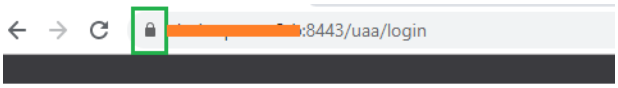
1. Reinicie el PC servidor.
2. Reinicie los servicios 4Sight2 y DruckCommsServer esde servicios de Windows.

3. Abra Google Chrome, borre la caché del navegador y reinicie Google Chrome. Asegúrese de que no haya otras instancias de Google Chrome activas.
4. Escriba la URL siguiente en la barra de direcciones y pulse Inro.

   Https://<<Nombre de host del servidor>>:8443/4sight2.

   Nota: Utilice el nombre de host de la URL anterior.
5. Aparecerá la pantalla de inicio de sesión con la URL HTTPS correcta.

   Nota: El error rojo ha desaparecido de la barra de direcciones. Si el enlace sigue sin ser seguro, reinicie el equipo y vuelva al paso 3.



Preguntas frecuentes sobre la instalación de 4Sight2

6. Preguntas frecuentes sobre la instalación de 4Sight2

6.1 Configuración e instalación

Pregunta 1: Mi organización consta de varios centros en distintas zonas del mundo. ¿Cuál es la mejor forma de configurar 4Sight2?

Respuesta: Depende de cómo mantenga y opere los centros. Si todos los centros se mantienen y operan desde un departamento informático centralizado, puede instalar centralmente una sola licencia de 4Sight2. Todos los centros podrán acceder a 4Sight2 a través de la red o de una LAN. Por otra parte, si tiene filiales con gestión independiente, puede adquirir varias licencias 4Sight2.

Pregunta 2: Si adquiero varias licencias de 4Sight2, ¿habrá comunicación entre ellas?

Respuesta: No. Cada licencia de 4Sight2 es un software aislado e independiente con su propia instalación y base de datos. No hay comunicación entre las distintas instalaciones. Contacte con el equipo de 4Sight2 para obtener más información o para hablar sobre sus necesidades concretas.

Pregunta 3: ¿Cómo puedo descargar 4Sight2?

Respuesta: Puede descargar fácilmente 4Sight2 desde el sitio web de la empresa. El enlace se indica a continuación.

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

O

Llame a una oficina comercial y haga un pedido. Recibirá una versión de demostración en una unidad USB.

Pregunta 4: ¿Puedo instalar 4Sight2 en un sistema operativo que no sea Windows?

Respuesta: No. 4Sight2 solo es compatible con la plataforma Windows.

Pregunta 5: Acabo de descargar e instalar 4Sight2. ¿Cómo puedo acceder a 4Sight2?

Respuesta: 4Sight2 es una aplicación basada en la web. Por tanto, no se genera ningún icono en el escritorio ni el ordenador durante su instalación. Para acceder a 4Sight2:

- Abra Google Chrome, pegue la URL siguiente en la barra de dirección y pulse Enter.
- Si 4Sight2 está instalado en el mismo ordenador, utilice http://localhost:<número_puerto_aplicación> /4sight2 Si 4Sight2 está instalado en otro ordenador de la misma red, utilice

  http://<Nombre O dirección IP del ordenador>:<número_puerto_aplicación>/4sight2
- Cree un marcador en Google Chrome para futuras consultas.

Pregunta 6: El instalador de 4Sight2 no puede encontrar los archivos de la base de datos Postgres.

Asegúrese de que el instalador se haya extraído a una ubicación local y de que el archivo se esté ejecutando desde la carpeta Disco 1. Asegúrese de que la ubicación local en la que se haya extraído el instalador no tenga un nombre de ruta muy largo, ya que podría dar lugar a fallos a la hora de encontrar los archivos necesarios.

Pregunta 7: ¿Qué sucede si el proceso de actualización se cancela en cualquier punto?

Respuesta: Si el administrador cancela el proceso de actualización en cualquier punto, se volverá a la versión 1.4, que debería quedar plenamente operativa. El administrador deberá reiniciar el proceso de actualización para finalizar correctamente la actualización.

Pregunta 8: Durante la instalación de la aplicación 4Sight2, si el usuario recibe el mensaje "Introduzca un número de puerto válido. Para determinar los números de puerto válidos, consulte el manual de instalación."

Respuesta: A continuación, se indica el rango de puertos no válidos. Elija un puerto válido para continuar con la instalación.

- Los puertos 0 a 1024 están reservados para la conexión TCP.
- Lista de puertos no seguros: 2049, 3659, 4045, 6000, 6665-6669, 65535

Pregunta 9: 4Sight2 con https no funciona en el sistema

Respuesta: Siga la sintaxis del nombre de dominio del ordenador en el que se vaya a instalar la aplicación 4Sight2.

<dominio> ::= <subdominio>

<subdominio> ::= <etiqueta> | <subdominio> "." <etiqueta>

<etiqueta> ::= <letra> [[<ldh-str>] <let-dig>]

<ldh-str> ::= <let-dig-hyp> | <let-dig-hyp> <ldh-str>

<let-dig-hyp> ::= <let-dig> | "-"

<let-dig> ::= <letra> | <dígito>

<letra> ::= cualquiera de los 52 caracteres alfabéticos (A-Z) en

mayúsculas o minúsculas

<dígito> ::= cualquiera de los 10 dígitos (0-10)

Nota: Se admiten mayúsculas y minúsculas en nombres de dominio. Dos nombres con los mismos caracteres pero diferencia de minúsculas y mayúsculas se tratarán idénticamente.

6.2 Preguntas frecuentes sobre Test Equipment Communicator

Pregunta 1: He seguido todos los pasos del manual de instalación pero sigo sin ver mi dispositivo en la lista.

Respuesta: Si no logra ver el Equipo de prueba en la lista después de seguir estos pasos, reinstale los controladores de 4Sight2. Para ello, acceda a **Panel de control >> Programas y características** y desinstale DruckCommsServer. Instale de nuevo Test Equipment Communicator.

Pregunta 2:. Aparece el error '**No se encontraron dispositivos**'.

Respuesta: Para solucionar el problema:

- Asegúrese de haber conectado físicamente el dispositivo con el cable USB. Para ello, acceda al administrador de dispositivos y localice el dispositivo en la lista. Normalmente, el dispositivo

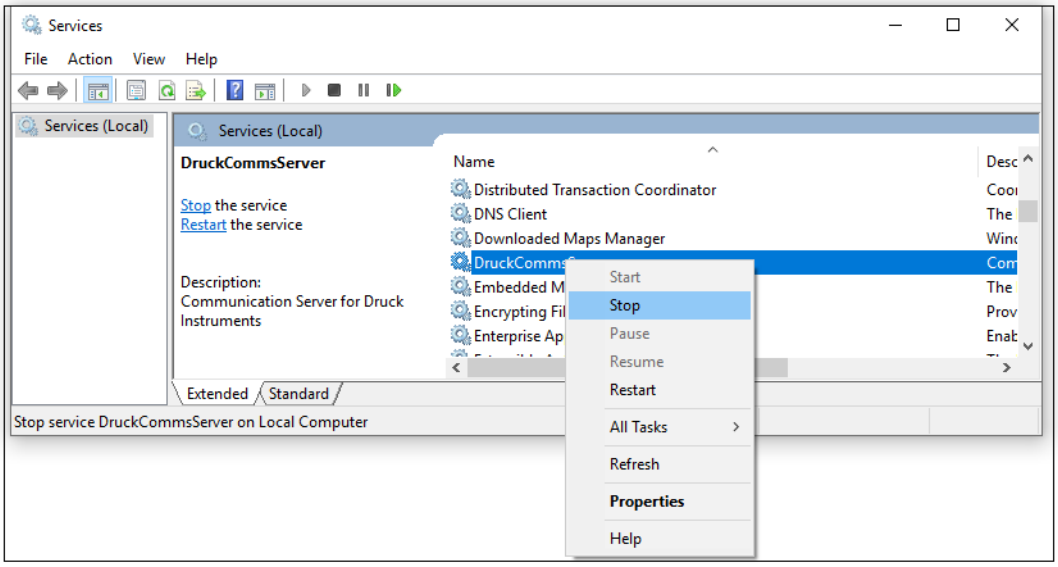
estará en la sección de dispositivos Bus serie universal. Si el dispositivo aparece bajo Otros dispositivos, deberá realizar los ajustes anteriores para configurarlo como dispositivo USB.

- Asegúrese de que el dispositivo esté en modo de comunicaciones o comms. Consulte el paso 1.
- Asegúrese de que la ruta del dispositivo dirija correctamente a C:\Windows\INF... Consulte el paso 2.

Pregunta 3: Aparece el error '**Error interno del servidor**' cuando actualizo o hago clic en el equipo de prueba que figura en la lista.

Respuesta: Para solucionar el problema:

- Acceda a Servicios de Windows (Servicios).
- Haga clic con el botón derecho en el servicio **DruckCommsServer** de la lista y, después, en **Reiniciar**.



- Acceda a 4Sight2 y haga clic en el botón **Actualizar**. Aparecerán los procedimientos en la lista.

Pregunta 4: Aparece el error '**Error de comunicaciones**'.

Respuesta: En ocasiones, el software no puede comunicarse correctamente con el dispositivo por distintas razones: mal contacto del cable USB, dispositivo en mal estado, dispositivo ocupado realizando otras tareas, servidor ocupado, etc. Haga clic de nuevo en el botón Actualizar para resolver el problema (pruebe 2 o 3 veces).

Si el error persiste, siga estos pasos:

- Reinicie el dispositivo (Genii / PACE). Asegúrese antes de que sea seguro hacerlo y de que no esté ejecutando ninguna operación crítica. Inténtelo de nuevo. Asegúrese también de que el dispositivo esté físicamente conectado.

Si estos pasos no resuelven el problema, siga las instrucciones del paso 3 y reinicie el servicio **DruckCommsServer**.

Resolución de problemas de instalación

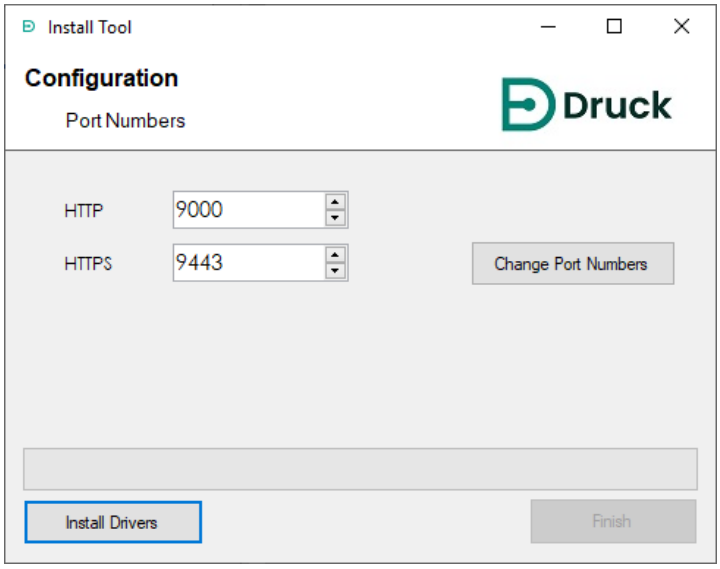
7. Resolución de problemas de instalación

7.1 Problemas de comunicación con el equipo de prueba

Durante el uso de 4Sight2 para comunicar con un equipo de prueba, puede suceder que no se detecte equipo alguno aunque se haya comprobado que Test Equipment Communicator devuelve la cadena json tras una llamada directa al comunicador. Por lo general, este problema tiene una de dos causas:

- Los números de puerto se han configurado incorrectamente. Contacte con el usuario administrativo para determinar los puertos que utiliza 4Sigth2 para contactar con Test Equipment Communicator.

  Cuando sepa los puertos correctos, acceda a C:\Program Files\Druck\DruckCommsServer\[Versión] y ejecute CommsServerInstallTool.exe.



Modifique los números de puerto y haga clic en el botón **Cambiar números de puerto**. Espere a que el servicio se reinicie. Los números de puerto habrán cambiado. Pulse el botón **Finalizar**.

- Test Equipment Communicator no está configurado para Https, pero 4Sight2 sí.

  Contacte con el administrador para instalar un certificado autofirmado para Test Equipment Communicator.

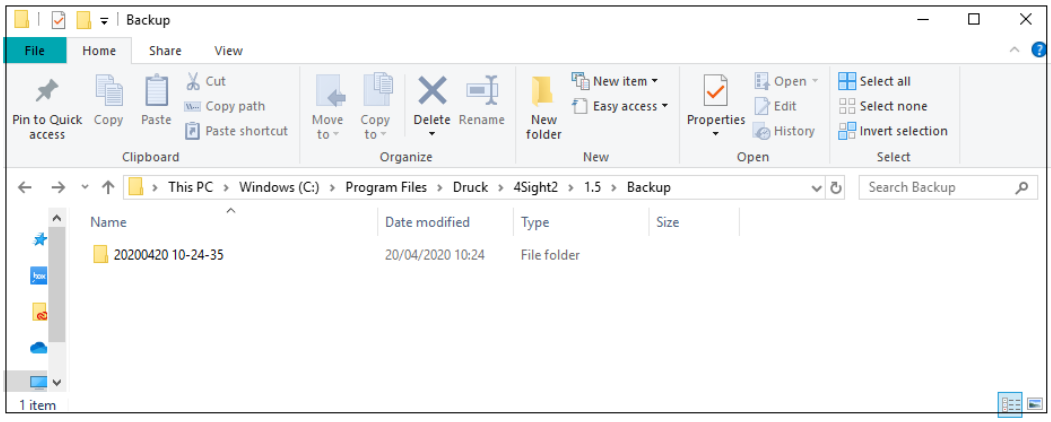
7.2 Copia de seguridad de la base de datos Postgres

Consulte el manual del usuario de 4Sight2 (123M3138) para obtener información sobre la copia de seguridad de la base de datos Postgres.

7.3 Restauración de la base de datos Postgres

Debe haber hecho previamente una copia de seguridad de la base de datos con la aplicación 4Sight.

La aplicación 4Sight (versión 1.4 o posterior) dispone de una interfaz para hacer una copia de seguridad (iniciada por el usuario o programada). Esta operación crea archivos en la carpeta de copias de seguridad del directorio de instalación de 4Sight en el servidor. Cada copia de seguridad iniciada crea una nueva carpeta en la de copias de seguridad con nombre en formato AAAAMMDDHHSS (año, mes, día hora y segundo) para indicar la fecha y la hora de finalización de la copia.



Se recomienda hacer una copia de seguridad del contenido de la carpeta de copias de seguridad en un soporte aparte.

Cada carpeta contiene 5 archivos.

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

Los archivos *.bck tienen un prefijo que corresponde a la versión de la aplicación 4Sight. Asegúrese de restaurar una base de datos que coincida con la versión exacta de la aplicación. La aplicación no admite bases de datos de otras versiones. Tenga en cuenta que la versión contiene un guión bajo (_) en lugar de un punto (.); p. ej., 1_4 y no 1.4. Cuando utilice los siguientes comandos en Pasos para la restauración, asegúrese de sustituir <VERSIÓN_APLICACIÓN> por la versión correcta de la aplicación 4Sight instalada.

El archivo metadata.properties contiene el nombre de la copia de seguridad introducido durante el inicio del proceso.

Comprobación de SHA 256

Una copia de seguridad consta de 3 archivos con extensión .bck, uno para cada base de datos. El archivo metadata.properties contiene el SHA 256 de cada uno de los archivos de la copia de seguridad.

1. Abra una ventana de símbolo del sistema como Administrador y cambie de directorio para acceder a la carpeta que contiene los archivos de la copia de seguridad seleccionada.
2. Utilice los comandos siguientes para calcular el SHA 256 de cada archivo.

   certutil -hashfile 4Sight**<VERSIÓN_APLICACIÓN>**.bck SHA256
   certutil -hashfile 4Sightaudit**<VERSIÓN_APLICACIÓN>**.bck SHA256
   certutil -hashfile uaa**<VERSIÓN_APLICACIÓN>**.bck SHA256

3. Antes de seguir con los pasos para la restauración, compruebe que el SHA 256 de cada archivo coincida con el indicado en el archivo de metadatos. El archivo de la copia de seguridad es válido si la suma de comprobación devuelta por el comando coincide exactamente con la del archivo de metadatos. No siga con los pasos para la restauración si no son idénticas.

7.4 Pasos para la restauración:

1. Inicie sesión como administrador en el servidor 4Sight como.
2. Busque el puerto en el que se ejecuta la base de datos Postgres. Lo encontrará en la propiedad spring.datasource.url, en el archivo <DIRECTORIO DE INSTALACIÓN DE 4Sight>\apache-tomcat\webapps\application.properties. Utilice una instancia de Notepad que se ejecute en modo Administrador para abrir el archivo. Es el número que se encuentra justo antes de 4Sight**<VERSIÓN_APLICACIÓN>**
3. Inicie sesión en la utilidad de comandos psql desde una ventana de símbolo del sistema que se ejecute en modo Administrador. Utilice el usuario de postgres

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

4. Encontrará el usuario de la base de datos utilizado por la aplicación en la propiedad spring.datasource.username, en el archivo <DIRECTORIO DE INSTALACIÓN DE 4Sight>\apache-tomcat\webapps\application.properties. Utilice una instancia de Notepad que se ejecute en modo Administrador para abrir el archivo.
5. Elimine las bases de datos *_temp, si las hay, y cree las bases de datos *_temp vacías ejecutando los siguientes comandos en la ventana de símbolo del sistema de psql:

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

   Asigne a este usuario como propietario de las 3 bases de datos anteriores. En el nombre de usuario, se distingue entre mayúsculas y minúsculas.

ALTER DATABASE "4Sight**<VERSIÓN_APLICACIÓN>**_temp" OWNER TO "**<USUARIO_BD>**";
ALTER DATABASE "4Sightaudit**<VERSIÓN_APLICACIÓN>**_temp" OWNER TO "**<USUARIO_BD>**";
ALTER DATABASE "uaa**<VERSIÓN_APLICACIÓN>**_temp" OWNER TO "**<USUARIO_BD>**";

6. Compruebe los archivos metadata.properties de las copias de seguridad y decida cuál de las copias de seguridad necesita restaurar.
7. Abra otra ventana de símbolo del sistema como Administrador y cambie de directorio para acceder a la carpeta que contiene los archivos de la copia de seguridad seleccionada.

   Restaure la base de datos desde los archivos *.bck a las bases de datos *_temp con los comandos siguientes. Si se le pide una contraseña, introduzca la de superusuario de Postgres.
   "C:\Program Files\PostgreSQL\11\bin\pg_restore" --port=**<PUERTO_BD>** --no-owner --username=postgres --dbname=4Sight**<VERSIÓN_APLICACIÓN>**_temp -n public --role=**<USUARIO_BD>** 4Sight**<VERSIÓN_APLICACIÓN>**.bck

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

   "C:\Program Files\PostgreSQL\11\bin\pg_restore" --port=**<PUERTO_BD>** --no-owner --username=postgres --dbname=uaa**<VERSIÓN_APLICACIÓN>**_temp -n public --role=**<USUARIO_BD>** uaa**<VERSIÓN_APLICACIÓN>**.bck
8. Elimine las bases de datos *_old, si las hay, ejecutando los siguientes comandos en la ventana de símbolo del sistema de psql:

   DROP DATABASE IF EXISTS "4Sight**<VERSIÓN_APLICACIÓN>**_old";
   DROP DATABASE IF EXISTS "4Sightaudit**<VERSIÓN_APLICACIÓN>**_old";
   DROP DATABASE IF EXISTS "uaa**<VERSIÓN_APLICACIÓN>**_old";
9. Detenga las aplicaciones Servicio 4Sight y pgadmin si están abiertas.
10. Elimine las bases de datos *_old, si las hay, ejecutando los siguientes comandos en la ventana de símbolo del sistema de psql:

    ALTER DATABASE "4Sight**<VERSIÓN_APLICACIÓN>**" RENAME TO "4Sight**<VERSIÓN_APLICACIÓN>**_old";
    ALTER DATABASE "4Sightaudit**<VERSIÓN_APLICACIÓN>**" RENAME TO "4Sightaudit**<VERSIÓN_APLICACIÓN>**_old";
    ALTER DATABASE "uaa**<VERSIÓN_APLICACIÓN>**" RENAME TO "uaa**<VERSIÓN_APLICACIÓN>**_old";
11. Cambie el nombre de las bases de datos *_temp a bases de datos 4Sight ejecutando los siguientes comandos en la ventana de símbolo del sistema de psql:

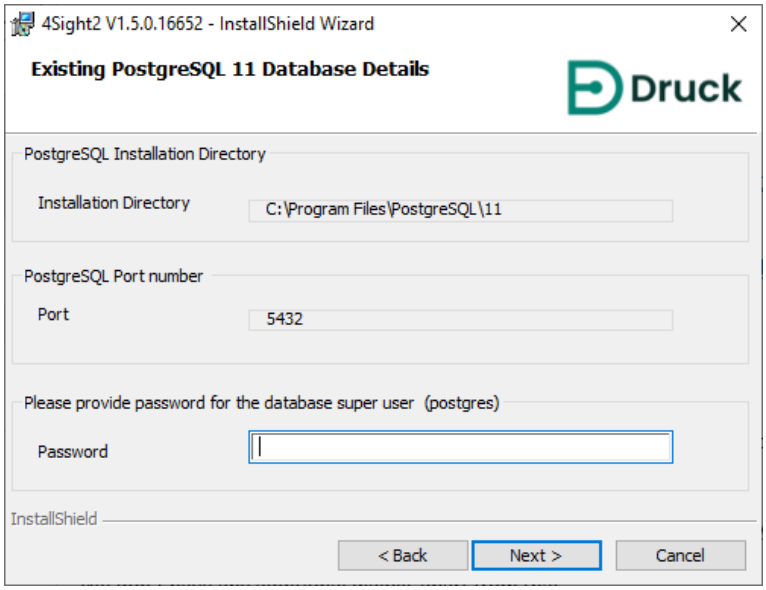
    ALTER DATABASE "4Sight**<VERSIÓN_APLICACIÓN>**_temp" RENAME TO "4Sight**<VERSIÓN_APLICACIÓN>**";
    ALTER DATABASE "4Sightaudit**<VERSIÓN_APLICACIÓN>**_temp" RENAME TO "4Sightaudit**<VERSIÓN_APLICACIÓN>**";
    ALTER DATABASE "uaa**<VERSIÓN_APLICACIÓN>**_temp" RENAME TO "uaa**<VERSIÓN_APLICACIÓN>**";
12. Inicie Servicio 4Sight e intente iniciar sesión como administrador. Tenga en cuenta que deberá utilizar la contraseña del administrador usada en el momento de hacer la copia de seguridad para iniciar sesión ahora.

7.5 ¿Cómo recuperarse de un fallo de la máquina 4Sight2?

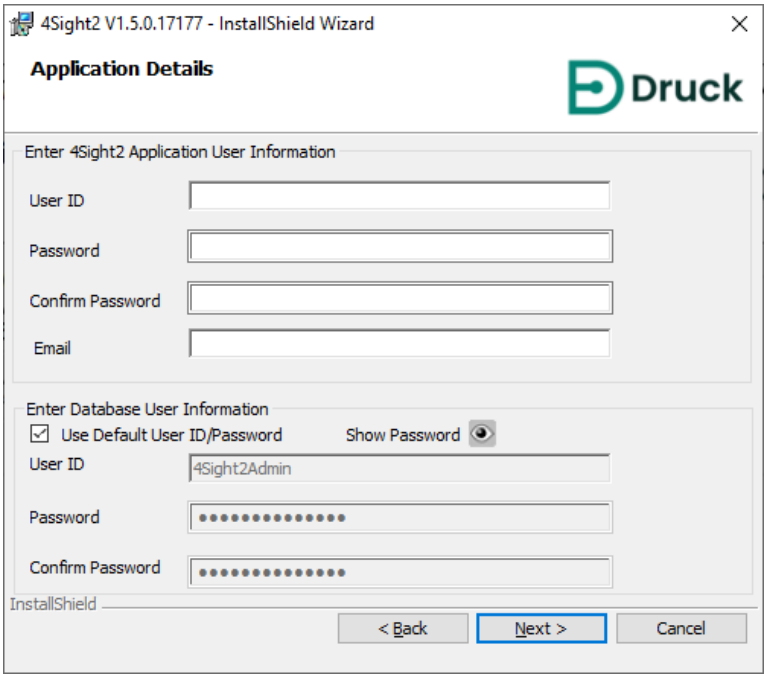
Supuestos: El usuario ha hecho una copia de seguridad de la base de datos 4Sight2 antes del fallo.

El usuario conoce el nombre de usuario y la contraseña para acceder a la aplicación y la base de datos.

1. Configure la máquina con un sistema operativo y controladores compatibles.
2. Instale 4Sight2 en la máquina.
3. Cuando instale la aplicación, utilice el mismo nombre de usuario y contraseña que utilizó previamente paa la aplicación y la base de datos Postgres.

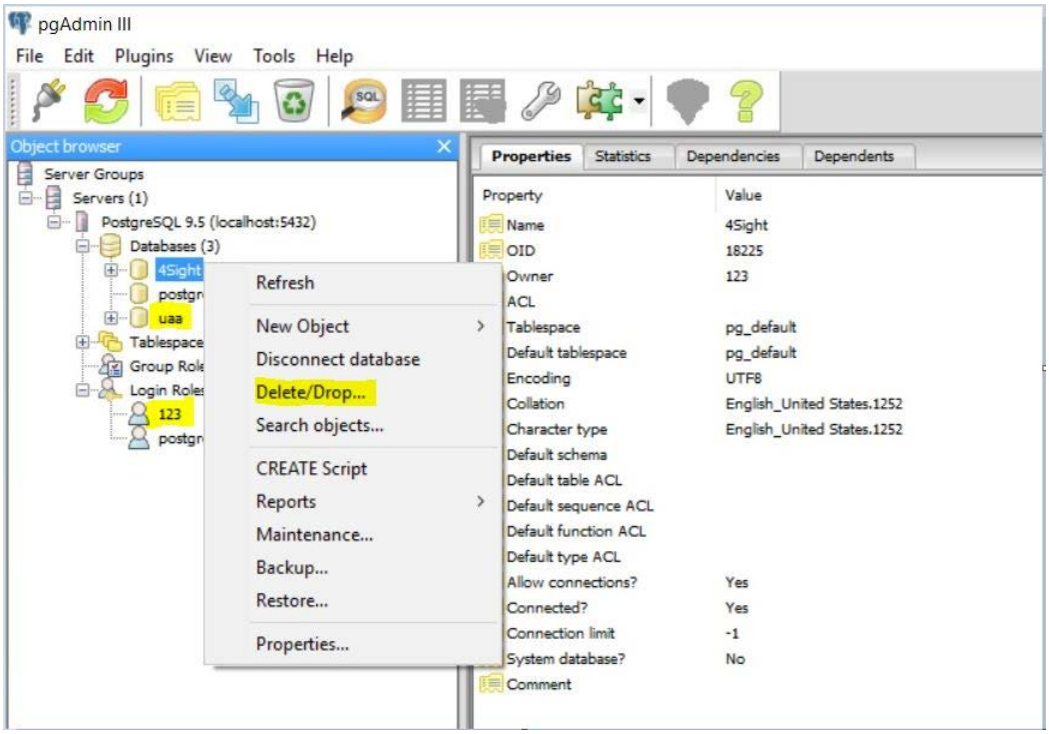


Utilice la misma contraseña de la instalación anterior.



Cumplimente todos los campos como en la instalación anterior.

4. Una vez instalada correctamente la aplicación, traslade la base de datos predeterminada creada durante la instalación de la aplicación desde pgAdmin (haga clic con el botón derecho en la base de datos y seleccione Eliminar/Soltar). Si se produce un error mientras traslada la base de datos, reinicie el servicio Postgres e inténtelo de nuevo después de actualizar.



5. Una vez trasladados correctamente la base de datos y el usuario: Siga estos pasos para restaurar la base de datos según las instrucciones anteriores desde una ventana de símbolo del sistema.
6. Ya ha restaurado correctamente la base de datos. Abra la aplicación desde el navegador y compruébelo.

7.6 Escenario de fallo de la instalación:

En la tabla siguiente se explican los distintos escenarios de fallo durante la instalación y sus soluciones.

Mensaje de error	Escenario	Solución/Acción necesaria
"Insufficient disk space available to install 4Sight2 application. Please ensure a minimum of 4096 MB is available. Free Space : available MB."	Fallo debido a un problema de tamaño del disco duro (cuando no hay espacio suficiente en disco al iniciar la actualización).	El administrador debe liberar espacio en la unidad y repetir el proceso de actualización.

Mensaje de error	Escenario	Solución/Acción necesaria
"Deployment fail while Migrating database"	Fallo debido a un problema de tamaño del disco duro (cuando no hay espacio suficiente en disco después de iniciar la actualización correctamente).	El administrador debe liberar espacio en la unidad y repetir el proceso de actualización.
"Installation failed while migrating Database. Please reinstall 4sight2"	Fallo debido a la integridad de los datos al copiar la base de datos.	En este caso, el administrador debe contactar con el centro de atención al cliente. Motivo de integridad de datos capturado en los registros en la posición. [C:\Users\[NombreUsuario]\App Data\Local\Temp\logs]
"Installation failed while migrating Database. Please reinstall 4sight2"	Fallo debido a la integridad de datos en la fase de actualización del esquema.	En este caso, el administrador debe contactar con el centro de atención al cliente. Motivo de integridad de datos capturado en los registros en la posición. 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"	Este fallo se produce cuando el instalador no puede obtener el estado del servicio.	El administrador debe comprobar que el servicio 4Sight2 funcione correctamente.
"Failed to start the 4Sight2 service. Please ensure the 4Sight2 service is present and running"	Fallo debido a daños en la aplicación. Faltan archivos, otra aplicación está utilizando el puerto, el usuario ha detenido el servicio, etc.	Si el administrador obtiene el estado del servicio y este no funciona por alguna razón (aplicación dañada, faltan archivos, otra aplicación está utilizando el puerto, el usuario ha detenido el servicio, etc.), el sistema intenta iniciar el servicio. Si no se puede iniciar el servicio, el administrador debe contactar con el centro de atención al cliente para resolver el problema.
"Upgrade of 4Sight2 application is supported from version 1.3 onwards. For earlier version upgrade support please contact Customer Care."	La actualización no se llevará a cabo si la versión instalada es anterior a la 1.3.	Solo es posible actualizar a partir de la versión 1.3.

Mensaje de error	Escenario	Solución/Acción necesaria
Installer has detected another minor version of PostgreSQL 11. Installer will not continue. Refer to 4Sight2 Installation manual for more details	La instalación de 4Sight2 no puede continuar porque existe la misma versión de PostgreSQL (variante) en el equipo de destino.	Opciones posibles: 1. El usuario puede elegir otra máquina. 2. El usuario hace una copia de seguridad de la aplicación existente que utiliza Postgres versión 11.3, desinstala la aplicación y la instala en otra máquina. Desinstale Postgres y reinicie la instalación de 4Sight2.
Installation failed while upgrading database. Please reinstall 4Sight2. Refer to 4Sight2 Installation manual for more details	Puede que se haya producido un error interno durante la actualización. El usuario puede intentar repetir la instalación.	Si el problema persiste, consulte los registros de instalación para obtener más información.

7.7 Causas generales de error

A continuación, se describen distintos problemas habituales que afectan a la comunicación con equipos Druck a través de USB.

- La conexión física se ha aflojado o es poco firme.
- Cables o puertos desgastados.
- Adaptadores USB de baja calidad.
- Adaptadores o puertos USB sobrecargados.
- Los dispositivos han estado funcionando durante mucho tiempo y han pasado al modo de hibernación o suspensión.
- Los dispositivos no están en modo de comunicación.
- No se ha instalado o actualizado el software del controlador. Necesita la misma versión de la aplicación 4Sight2 y los controladores para establecer la comunicación con el hardware.
- Las versiones de firmware de los dispositivos son muy antiguas.

7.8 Desinstalación de 4Sight2

Siga estas instrucciones si necesita instalar una copia nueva o una versión nueva de 4Sight2 o si desea desinstalar 4Sight2 debido a problemas durante la instalación.

La desinstalación del componente de la base de datos PostgreSQL eliminará la base de datos 4Sight2 y provocará la pérdida de información. Con este procedimiento, no se creará automáticamente una copia de seguridad, por lo que deberá asegurarse de hacerla manualmente antes de continuar y guardarla en una ubicación alternativa a la carpeta de instalación de 4Sight2. Consulte la sección Copia de seguridad y restauración de la base de datos Postgres de este manual.

Si decide desinstalar la aplicación 4Sight2 y mantener la base de datos, consulte las instrucciones de instalación de 4Sight2 de este manual. Necesitará disponer de credenciales de superusuario de base de datos para la reinstalación. No intente desinstalar si no dispone de ellas.

Si desea actualizar la versión de 4Sight2 sin desinstalar la base de datos, **NO** siga estas instrucciones.

1. Acceda a Panel de control >> Programas y características.
2. Haga clic con el botón secundario en 4Sight2 y seleccione Desinstalar.
3. Siga las instrucciones del asistente de desinstalación.
4. Haga clic con el botón secundario en PostgreSQL 11 y seleccione Desinstalar.
5. Siga las instrucciones del asistente de desinstalación.
6. La desinstalación de PostgreSQL no elimina la carpeta de datos. Deberá hacerlo manualmente. Elimine la carpeta de datos, ubicada en C:\Program Files\PostgreSQL\11\.
    a. Si desea eliminar toda la carpeta de PostgreSQL, asegúrese de mover previamente todos los archivos de copia de seguridad y de secuencia de comandos desde la carpeta bin.
    b. Las copias de seguridad de la base de datos 4Sight2 se crean y guardan de forma predeterminada en la siguiente ubicación: C:\Program Files\PostgreSQL\11\bin
7. Se recomienda reiniciar el ordenador.
8. La desinstalación de 4Sight2 ha concluido.

7.9 Resolución de problemas de comunicación segura

1. El comando 'nombre de comando' no se reconoce como comando interno o externo. Por ejemplo, 'keytool' no se reconoce como comando interno o externo.

- Si obtiene un error similar a este, indica que el símbolo del sistema no puede encontrar el comando especificado en la carpeta actual.

  Para resolverlo, utilice el comando siguiente para dirigirse a la carpeta correcta.

  Set Path=%Path%;"<<ruta de acceso completa a la carpeta que contiene el comando>>"

  Por ejemplo en el error anterior del comando keytool, establezca la ruta siguiente:

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

2. Dirección IP incorrecta

- Si obtiene este mensaje de error, indica que la dirección IP o el nombre de host del archivo openssl-ca.cnf u openssl-server.cnf es incorrecto. Nota: Puede ser necesario corregir el problema en varios puntos de estos archivos y volver a ejecutar los pasos.

3. No existe tal archivo o directorio...

- Si obtiene este mensaje de error, indica que el comando ejecutado puede hacer referencia a un nombre de archivo incorrecto. Compruebe si el comando contiene nombres de archivo incorrectos y si el archivo con el nombre está presente en la carpeta. Vuelva a ejecutar los comandos. Puede ser necesario corregir el nombre de archivo en el comando o seguir los pasos para generar los archivos que falten.
- Este error se puede producir con los archivos index.txt y serial.txt, porque en algunos casos la extensión de archivo se añade dos veces al nombre (p. ej., intex.txt.txt).

  Edite el archivo y guárdelo sin la extensión .txt. Asegúrese de que el archivo solo tenga una extensión .txt.

Buenas prácticas

8. Buenas prácticas

Protección del servidor

El entorno del servidor debe estar protegido de acuerdo con las directrices de Microsoft o CIS.

8.1 Tomcat

- Instale Tomcat en una carpeta segura a la que sólo pueda acceder admin o LocalService, como *C:\Program Files(x86).*
- Instale Tomcat como servicio que se ejecuta en la cuenta LocalService.
- Elimine todos los elementos almacenados en WebApp y las aplicaciones predeterminadas no deseadas.
- Restablezca la página de error predeterminada; por ejemplo, 404, 403, 500, etc.
- Exija HTTPS y habilite SSL.
- La aplicación de administración debe ejecutarse sobre SSL.
- Archivo de registro individual de usuario para cada aplicación web.
- Elimine el banner del servidor.
- Habilite el acceso al registro.
- Cambie el puerto y el comando de apagado.

8.2 PostgreSQL

- Todas las cuentas con privilegios elevados, como pgdba, postgres y depesz, deben tener únicamente permiso de inicio de sesión local.
- Asegúrese de que la secuencia sea correcta en el archivo pg-hba.conf para que cada usuario obtenga los derechos correctos.
- Configure pg-hba.conf de forma que el la conexión al servidor pueda establecerse únicamente desde la máquina local, y no a través de la red.

8.3 Buenas prácticas para el firewall

A continuación, recomendamos varias buenas prácticas para el firewall de 4Sight2:

8.3.1 Directiva

1. La configuración del firewall debe ser coherente con las directivas de seguridad de la organización.
2. Utilice siempre una directiva de privilegios mínimos. Deniegue todo de forma predeterminada. Permita tráfico específico (con origen, destino y puerto).
3. Sitúe primero las reglas específicas y utilice reglas de caída explícitas.
4. Registre todas las acciones, particularmente los intentos de fallo para la traza de auditoría.

8.3.2 Recursos

1. Supervise el uso de memoria.
2. Supervise el uso de la CPU.
3. Supervise el uso del ancho de banda.
4. Limite el número de aplicaciones que se ejecutan en la máquina del firewall.

8.3.3 Instalación y mantenimiento

1. Limite el acceso físico a la máquina del firewall.
2. Utilice un identificador de usuario único para la administración.
3. Siga directivas de cuentas estrictas en la máquina.
4. Aplique parches con regularidad a los sistemas operativos, aplicaciones, firmware, etc.
5. Archive con regularidad las bases de reglas, configuraciones y registros. Documente todas las reglas y los cambios realizados en un control de fuentes.
6. Realice pruebas regulares.
7. Elimine las reglas inutilizadas cuando llegue la retirada del servicio.
8. Audite y revise las reglas regularmente.
9. Supervise con regularidad las asesorías de seguridad.

8.3.4 Seguridad adicional

1. Utilice inspecciones con estado.
2. Utilice proxies.
3. Utilice inspección y filtrado a nivel de aplicación.

8.3.5 Protección interna

1. Aplique una directiva de uso aceptable.
2. Utilice un firewall personal para cada usuario.
3. Prevenga las instrucciones en cada host.
4. Supervise la red.
5. Filtre los contenidos.
6. Active el control de acceso en cada ordenador y aplicación.

Oficinas

Sede central

Leicester, RU
Teléfono: +44 (0) 116 2317233
Correo electrónico:
gb.sensing.sales@bakerhughes.com

Alemania

Fráncfort
Teléfono: +49 (0) 69-22222-973
Correo electrónico:
sensing.de.cc@bakerhughes.com

Australia

Springfield Central
Teléfono: 1300 171 502
Correo electrónico: custcare.au@ge.com

China

Beijing
Teléfono: +86 180 1929 3751
Correo electrónico:
fan.kai@bakerhughes.com

China

Guangzhou
Teléfono: +86 173 1081 7703
Correo electrónico:
dehou.zhang@bakerhughes.com

China

Shanghái
Teléfono:+86 135 6492 6586
Correo electrónico:
hensen.zhang@bakerhughes.com

EAU

Abu Dhabi
Teléfono: +971 528007351
Correo electrónico:
suhel.aboobacker@bakerhughes.com

EE. UU.

Boston
Teléfono: 1-800-833-9438
Correo electrónico:
custcareboston@bhge.com

Francia

Toulouse
Teléfono: +33 562 888 250
Correo electrónico:
sensing.FR.cc@bakerhughes.com

India

Bangalore
Teléfono: +91 9986024426
Correo electrónico:
aneesh.madhav@bakerhughes.com

Italia

Milán
Teléfono: +39 02 36 04 28 42
Correo electrónico:
csd.italia@bakerhughes.com

Japón

Tokio
Teléfono: +81 3 6890 4538
Correo electrónico:
gesitj@bakerhughes.com

Países Bajos

Hoevelaken
Teléfono: +31 334678950
Correo electrónico:
nl.sensing.sales@bakerhughes.com

Rusia

Moscú
Teléfono: +7 915 3161487
Correo electrónico:
aleksey.khamov@bakerhughes.com

Servicios y asistencia

Asistencia técnica

Global
Correo electrónico:
mstechsupport@bakerhughes.com

Brasil

Campinas
Teléfono: +55 11 3958 0098, +55 19 2104 6983
Correo electrónico:
mcs.services@bakerhughes.com

China

Changzhou
Teléfono: +86 400 818 1099
Correo electrónico:
service.mcchina@bakerhughes.com

EAU

Abu Dhabi
Teléfono: +971 2 4079381
Correo electrónico:
gulfservices@bakerhughes.com

EE. UU.

Billerica
Teléfono: +1 (281) 542-3650
Correo electrónico:
namservice@bakerhughes.com

Francia

Toulouse
Teléfono: +33 562 888 250
Correo electrónico:
sensing.FR.cc@bakerhughes.com

India

Pune
Teléfono: +91 213 5620426
Correo electrónico:
mcsindia.inhouseservice@bakerhughes.com

Japón

Tokio
Teléfono: +81 3 3531 8711
Correo electrónico:
service.druck.jp@bakerhughes.com

Reino Unido

Leicester
Teléfono: +44 (0) 116 2317107
Correo electrónico:
sensing.grobycc@bakerhughes.com

123M3140 Revisión F | Español

Baker Hughes