Druck

4Sight2

Software de gestão da calibragem

Manual de instalação 123M3140 Revisão F

Índice

1. Introdução

O software de calibragem 4Sight2 é uma ferramenta baseada na web para gestão da calibragem, que ajuda a manter e a controlar o ambiente da calibragem nos mais elevados padrões de metrologia. Pode utilizar o software nas seguintes tarefas:

- Gestão da calibragem de todos os dispositivos de medição para uma determinada localização na empresa
- Configuração de um programa de trabalhos de calibragem para técnicos
- Carregamento e transferência de dados de e para os calibradores portáteis da Druck (DPI620 Genii, DPI611 e DPI612) que têm uma funcionalidade de comunicação por USB
- Gestão dos registos de calibragem dos dispositivos que não são suportados por um calibrador portátil (introdução manual de dados)
- Inspecione os registos do seu histórico de calibragens. Também pode efetuar um registo permanente de cada certificado de calibragem. Por exemplo: Para os procedimentos de controlo de qualidade ISO 9000.
- Controle as calibragens automatizadas com os controladores de pressão da Druck (PACE 1000, 5000 e 6000), os calibradores portáteis (DPI620 Genii, DPI611 e DPI612) e os calibradores de temperatura (DryTC165, DryTC 650, LiquidTC165 e LiquidTC255)

1.1 Público-alvo

1.1.1 Administradores

Um administrador é responsável pela instalação e configuração do software 4Sight2. Depois da instalação inicial da 4Sight2, ficará disponível uma única conta administrativa. A partir desta conta, podem ser criados novos utilizadores e podem ser atribuídos grupos/definições de permissão. Os administradores têm acesso de leitura e escrita a todas as funcionalidades da 4Sight2.

1.1.2 Supervisor

O supervisor é responsável por gerir os elementos e a calibragem. O supervisor tem a capacidade de criar e atualizar os elementos da 4Sight2 Enterprise, incluindo Fábricas, Localizações, Identificações e Dispositivos. É ainda responsável por associar documentos aos elementos, tais como os processos das fábricas e as folhas de dados dos dispositivos. Os supervisores podem criar procedimentos de teste que serão utilizados durante a calibragem, assim como procedimentos de agendamento e monitorização do estado dos dispositivos. Os supervisores têm as permissões necessárias para aprovar as calibragens.

1.1.3 Técnicos

Os técnicos são responsáveis pela execução das calibragens. As calibragens podem ser Portáteis, Manuais ou Automatizadas e é da responsabilidade do técnico efetuar o tipo de calibragem relevante num dispositivo. Depois de efetuar a calibragem, os técnicos podem analisar os resultados e concluir as calibragens que serão posteriormente aprovadas por um supervisor.

1.1.4 Auditor

Um auditor é responsável pela inspeção dos relatórios. Em algumas fábricas, pode ser obrigatória a realização de auditorias.

2. Requisitos do sistema

Os requisitos mínimos do sistema para instalar a aplicação 4Sight2 no servidor e nas máquinas cliente são os seguintes:

2.1 Servidor da aplicação

Sistema operativo	Windows 10, Windows Server 2012 R2, Windows Server 2016, Windows Server 2019
Atualizações	Todas as atualizações do Windows totalmente instaladas
Processador	Quad Core
RAM	8 GB ou superior (recomendado 32 GB)
Espaço no disco	1 TB
Velocidade da rede	10 Mbps

2.2 Estação de trabalho do cliente

Sistema operativo	Windows 10, Windows Server 2012 R2, Windows Server 2016, Windows Server 2019
Browser	Google Chrome V80+, Microsoft Edge V80, Firefox V74
Adobe Reader	Adobe Acrobat Reader Versão DC 2015.017.20050 +
RAM	8 GB ou superior
Processador	Dual Core
Espaço no disco	600 GB
Velocidade da rede	10 Mbps

2.3 Instalação local

Sistema operativo	Windows 10, Windows Server 2012 R2, Windows Server 2016, Windows Server 2019
Atualizações	Todas as atualizações do Windows totalmente instaladas
Adobe Reader	Adobe Acrobat Reader Versão DC 2015.017.20050 +
Processador	Dual Core
RAM	16 GB ou mais (recomendado 32 GB)
Espaço no disco	500 GB ou mais de espaço no disco
Browser	Google Chrome V80+, Microsoft Edge V80, Firefox V74

2.4 Firmware suportado pela 4Sight2

Para obter as informações mais recentes sobre o firmware suportado, consulte o link abaixo:

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

ou

Para PACE, insira o USB B para comunicação 4Sight2 conforme indicado na imagem abaixo:

Instalação da 4Sight2

3. Instalação da 4Sight2

Para instalar a 4Sight2, copie primeiro o ficheiro de configuração .zip da 4Sight2 para o seu ambiente de trabalho e extraia os ficheiros. A partir do ficheiro de configuração, selecione o ficheiro executável da 4Sight2.

Nota: É utilizado o seguinte software antivírus para analisar as instalações do 4Sight2 e Comm Server,

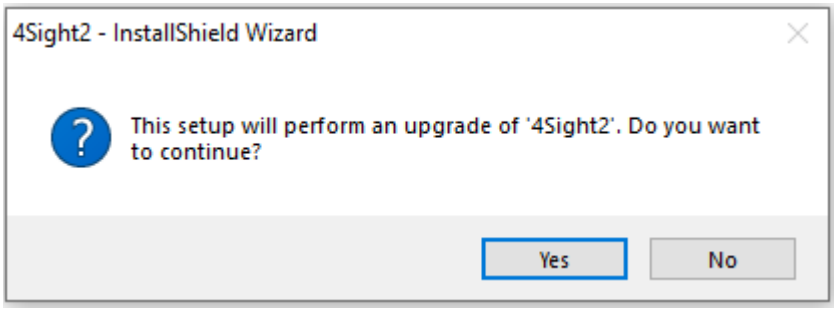
- McAfee VirusScan Enterprise + AntiSpyware Enterprise Número de versão: 8.8.0
- Symantec Endpoint Protection Número de versão: 14.3.558

Depois de executar o ficheiro de configuração, surge o assistente InstallShield. O assistente InstallShield inclui duas fases da instalação da 4Sight2:

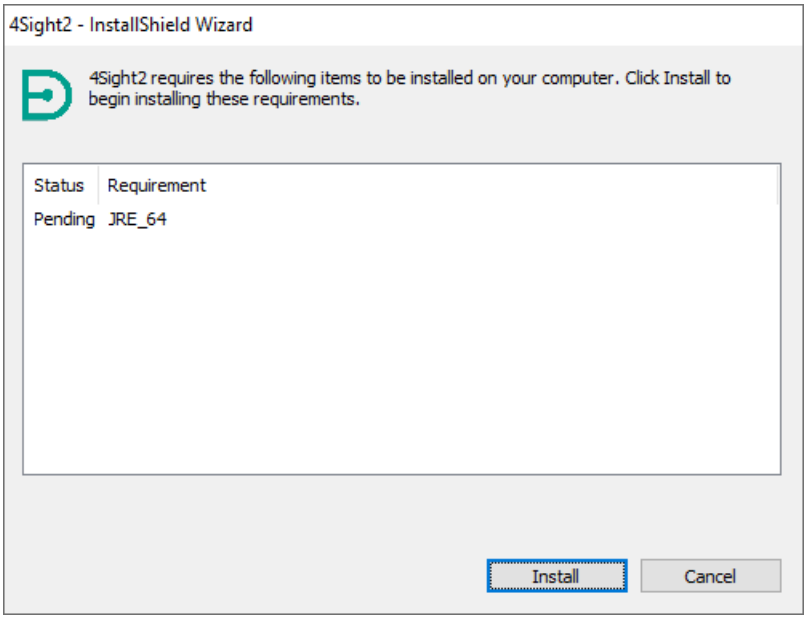
1. Instalação da base de dados
2. Instalação da aplicação na Internet

Siga as instruções do assistente InstallShield ou leia as duas secções seguintes para acompanhar o processo de instalação.

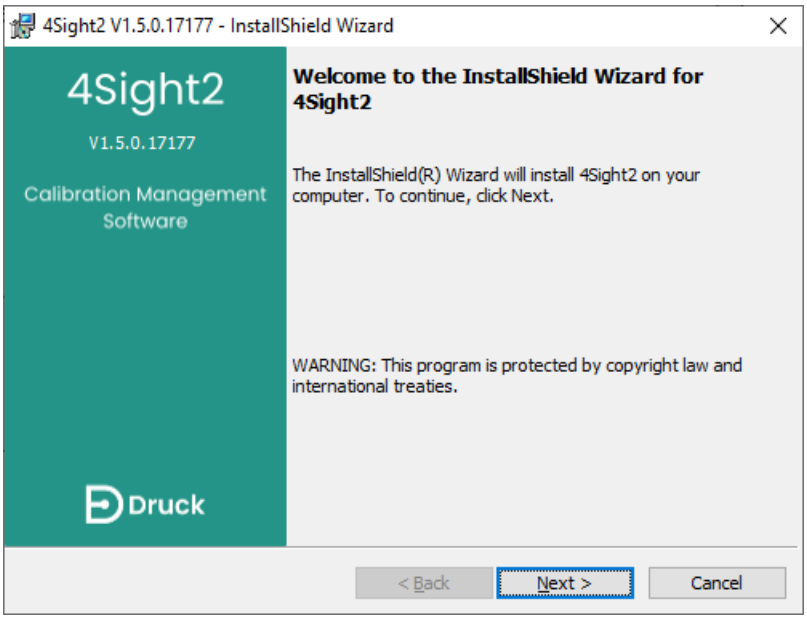
1. Se a 4Sight2 já se encontrar instalada na máquina, o assistente de instalação irá solicitar-lhe que efetue uma atualização para uma versão mais recente. Clique em **Sim** para atualizar para a versão mais recente.



2. Se a 4Sight2 for instalada pela primeira vez na máquina, o assistente de instalação apresenta o ecrã abaixo. Selecione **Instalar** e serão apresentados numa lista os itens que devem ser instalados.



3. Depois de concluir a instalação de qualquer pré-requisito, será apresentado o ecrã Bem-vindo ao assistente InstallShield. Clique em **Seguinte** para continuar.



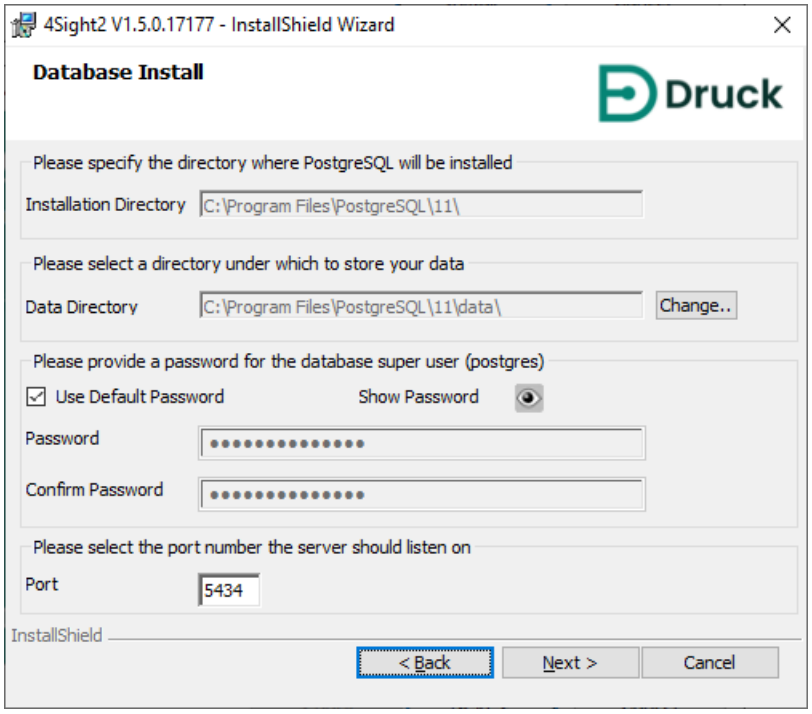
3.1 Instalação da base de dados

A aplicação 4Sight2 utiliza uma base de dados PostgreSQL. Em seguida, são fornecidas as instruções sobre como instalar a base de dados PostgreSQL e como proceder se a base de dados PostgreSQL já estiver instalada.

3.2 Instalação da PostgreSQL

Siga este procedimento se a base de dados PostgreSQL não estiver instalada na máquina.

1. Se a base de dados PostgreSQL não estiver instalada na máquina, o assistente de instalação irá apresentar o ecrã abaixo.



Diretório de instalação: Selecione o diretório em que a aplicação PostgreSQL pode ser instalada.

Diretório dos dados: Selecione o diretório em que a base de dados PostgreSQL pode ser armazenada.

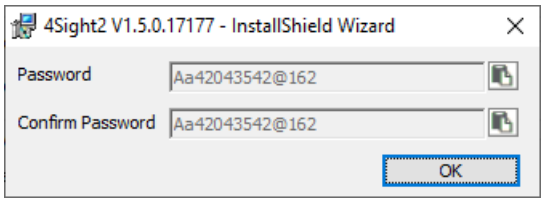
Palavra-passe/Confirmar palavra-passe: Escreva a palavra-passe do superutilizador da base de dados PostgreSQL. Isto acontece apenas na primeira instalação da base de dados PostgreSQL.

Nota: Esta palavra-passe é pedida para aceder aos conteúdos da base de dados depois da instalação.

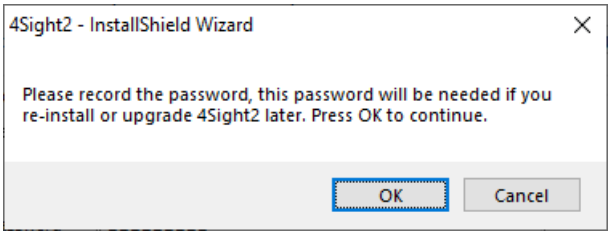
Porta: Este é o endereço da porta da base de dados PostgreSQL pedido para a aplicação.

Nota: Se o número da porta já estiver ocupado, contacte a equipa de TI. O utilizador também pode alterar o número da porta e deve anotá-lo para iniciar a aplicação mais tarde.

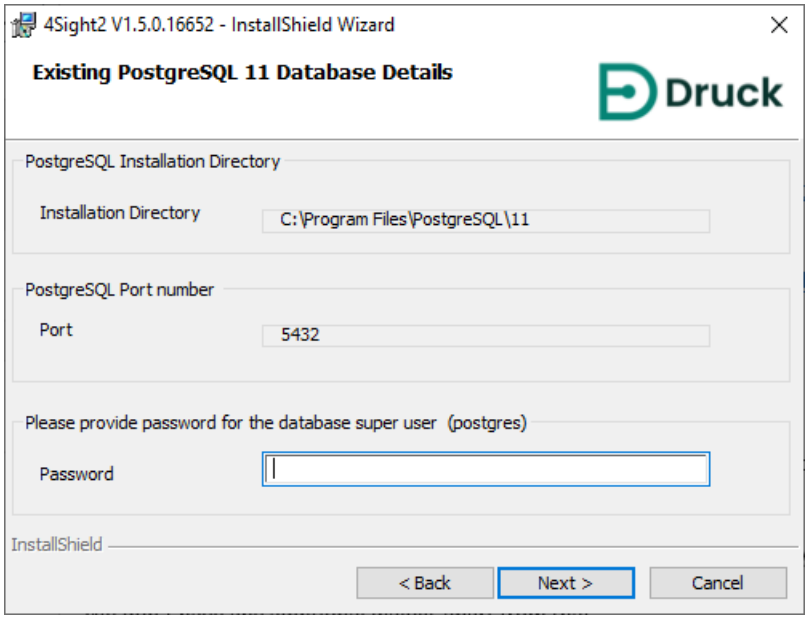
Importante: O utilizador deve anotar a palavra-passe da base de dados. A perda das informações da palavra-passe pode implicar negação de acesso ou perda de dados. Desmarque a caixa de verificação Palavra-passe do utilizador predefinida para atualizar a palavra-passe do superutilizador para a base dados. Se pretender manter a palavra-passe predefinida ou ver a nova palavra-passe introduzida, selecione o ícone (Mostrar palavra-passe). Para copiar a palavra-passe para a área de transferência, utilize o ícone (Copiar para a área de transferência).



Ser-lhe-á então pedido que grave novamente a palavra-passe com o instalador. Selecione **OK** assim que tiver anotado a palavra-passe.

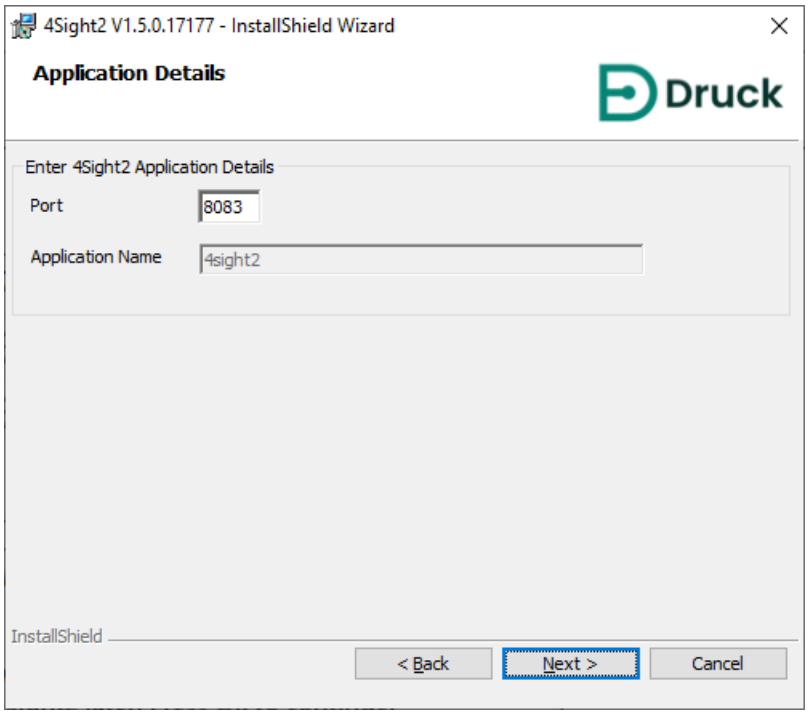


2. Este passo só será mostrado ao utilizador se a base de dados PostgreSQL já estiver instalada.



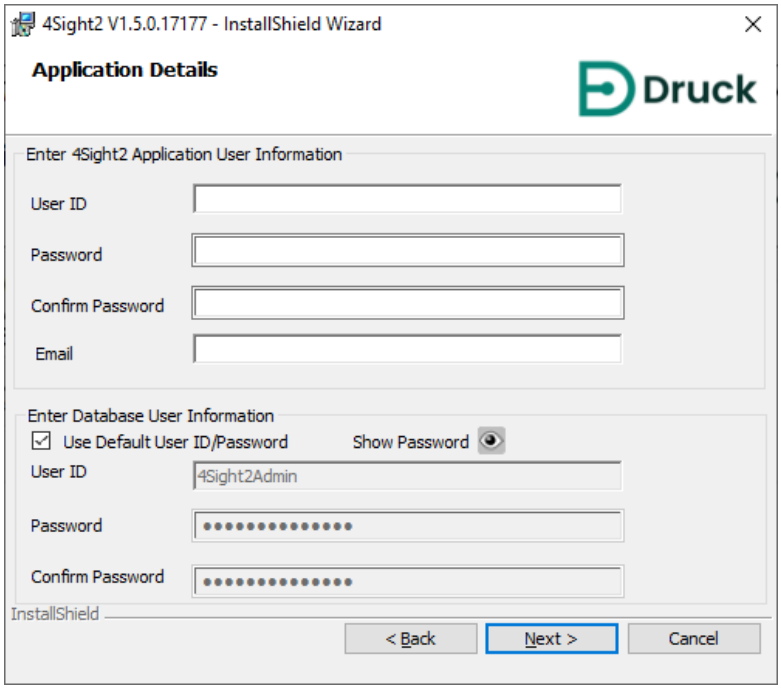
Diretório de instalação: Este especifica o caminho da localização de instalação do PostgreSQL. Trata-se de uma informação só de leitura.
Palavra-passe: Esta serve para confirmar a palavra-passe de superutilizador da base de dados PostgreSQL.
Porta: Esta especifica o número da porta utilizado pela base de dados PostgreSQL para executar o pedido db.

3. Na janela Detalhes da aplicação, introduza os seguintes detalhes



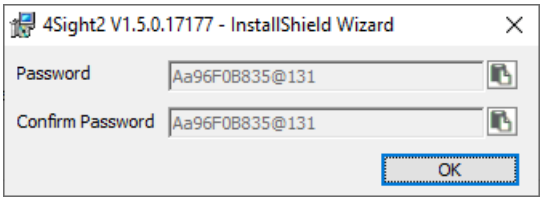
Porta: Indique a porta do servidor web Tomcat que é utilizada pela aplicação web 4Sight2 para responder a pedidos de HTTP.
Nome da aplicação: Indique o caminho do contexto da aplicação que irá utilizar no seu browser para se ligar à aplicação 4Sight2. Por predefinição, o nome é 4sight2.
Nota: Se o número da porta já estiver ocupado, contacte a equipa de TI. O utilizador também pode alterar o número da porta e deve anotá-lo para iniciar a aplicação mais tarde.

4. Selecione **Seguinte** e verá o ecrã Utilizador da aplicação.

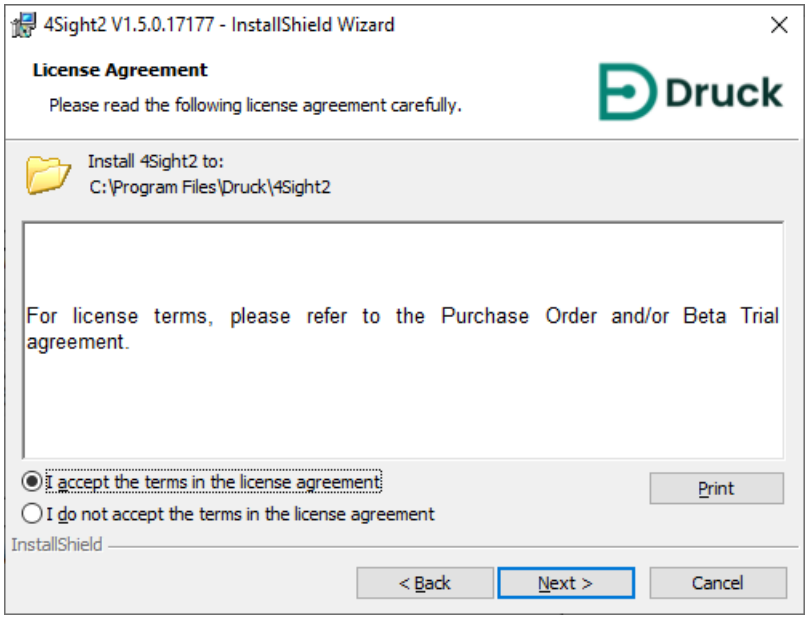


Informações sobre o utilizador da aplicação: Esta secção serve para indicar o nome e a palavra-passe de superutilizador para aceder à aplicação 4Sight2.
Nota: Esta palavra-passe é necessária para aceder à aplicação 4Sight2 depois da instalação.
Informações sobre o utilizador da base de dados: Esta secção serve para indicar o nome e a palavra-passe do utilizador da base de dados que serão utilizados pela aplicação 4Sight2 para comunicar com a base de dados PostgreSQL.

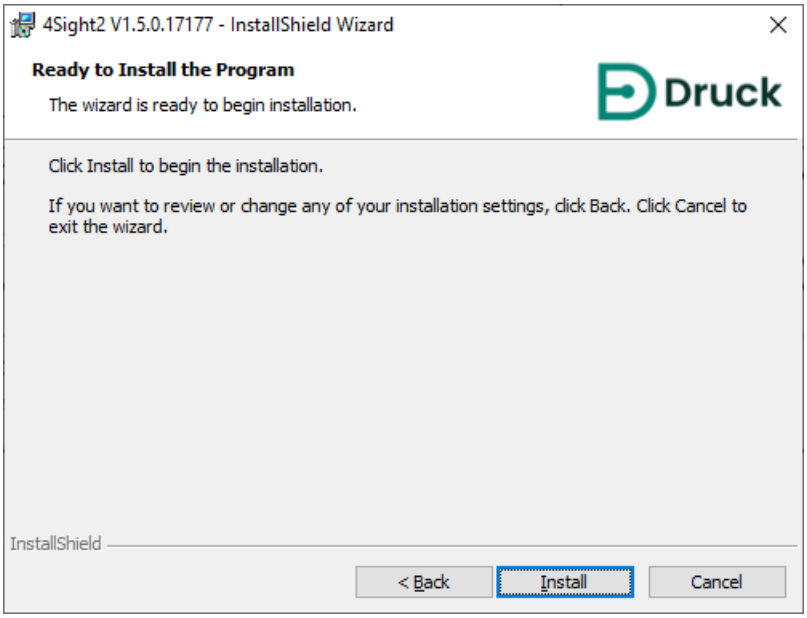
Importante: O utilizador deve anotar a palavra-passe da base de dados. A perda das informações da palavra-passe pode implicar negação de acesso ou perda de dados. Desmarque a caixa de verificação Palavra-passe do utilizador predefinida para atualizar a palavra-passe do superutilizador para a base dados. Se pretender manter a palavra-passe predefinida ou ver a nova palavra-passe introduzida, selecione o ícone (Mostrar palavra-passe). Para copiar a palavra-passe para a área de transferência, utilize o ícone (Copiar para a área de transferência).



5. Depois de ler os termos e condições da licença, selecione o botão de opção "I accept the terms in the licence agreement." e, em seguida, clique em **Seguinte**.

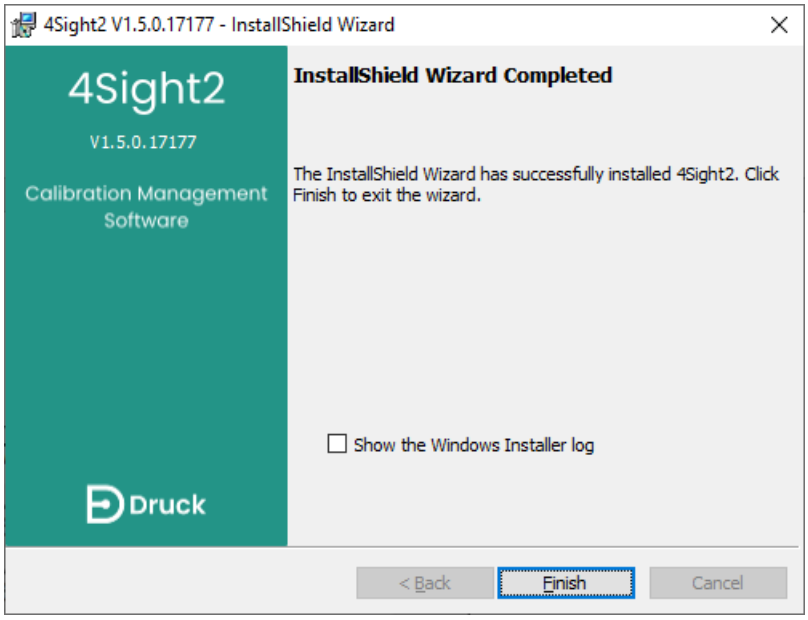


6. Clique em **Instalar** para iniciar a instalação. Todos os pacotes de software relacionados com a aplicação 4Sight2 e com a base de dados serão instalados.



Parabéns! A aplicação 4Sight2 está agora configurada.

7. Clique no botão **Concluir** para fechar a janela e siga as instruções da secção seguinte para iniciar sessão na aplicação 4Sight2.



Para iniciar sessão no servidor local da 4Sight2, vá para

http://ComputerName or IPAddress:PortNo/ApplicationName

- **ComputerName –** O nome do PC onde a aplicação 4Sight2 foi instalada. Este pode ser localizado ao clicar com o botão direito do rato neste PC e ao selecionar Propriedades.
- **IPAddress** – O endereço IP do PC onde a aplicação 4Sight2 foi instalada. Este pode ser localizado ao executar "ipconfig" numa janela de comandos do Windows.

- **PortNo -** O número que foi indicado no campo Número de Porta do Tomcat durante a instalação da aplicação.
- **ApplicationName -** O nome que foi indicado no campo Nome da Aplicação durante a instalação da aplicação.

Instalação do comunicador do equipamento de teste da 4Sight2

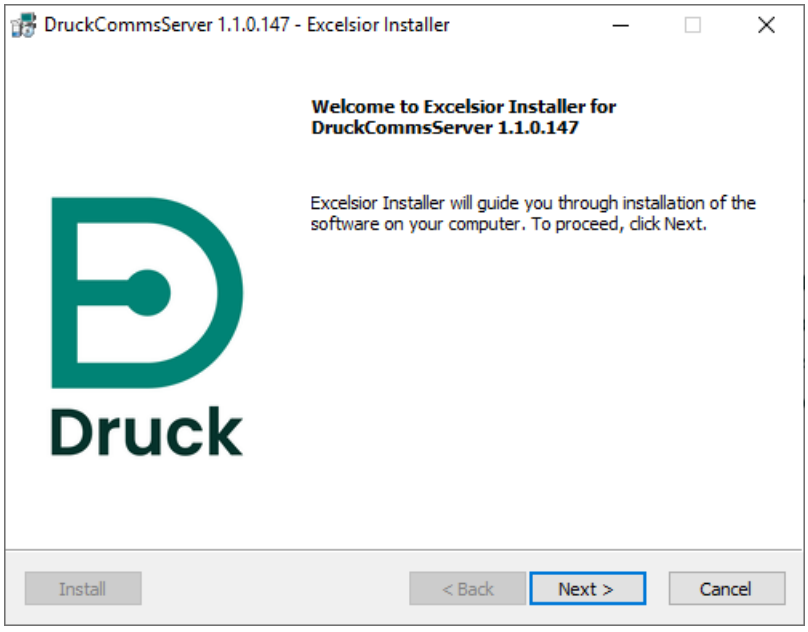
4. Instalação do comunicador do equipamento de teste da 4Sight2

1. O comunicador do equipamento de teste fornece os meios para que os seus instrumentos da Druck comuniquem com a aplicação 4Sight2. O comunicador do equipamento de teste pode ser instalado a partir da pasta de configuração da 4Sight2 ou pode ser transferido através da comunicação do dispositivo inicial da 4Sight2. Se o comunicador do equipamento de teste não estiver disponível no ficheiro de configuração, assim que a aplicação 4Sight2 estiver a funcionar e tiver sido criado um intervalo, aceda como administrador às opções Calibragem > Portátil no menu 4Sight2 para ajuda na navegação e na criação de intervalos. Selecione o botão de atualização junto ao menu pendente do equipamento de teste. Se o comunicador do equipamento de teste não estiver a funcionar, verá a seguinte mensagem:

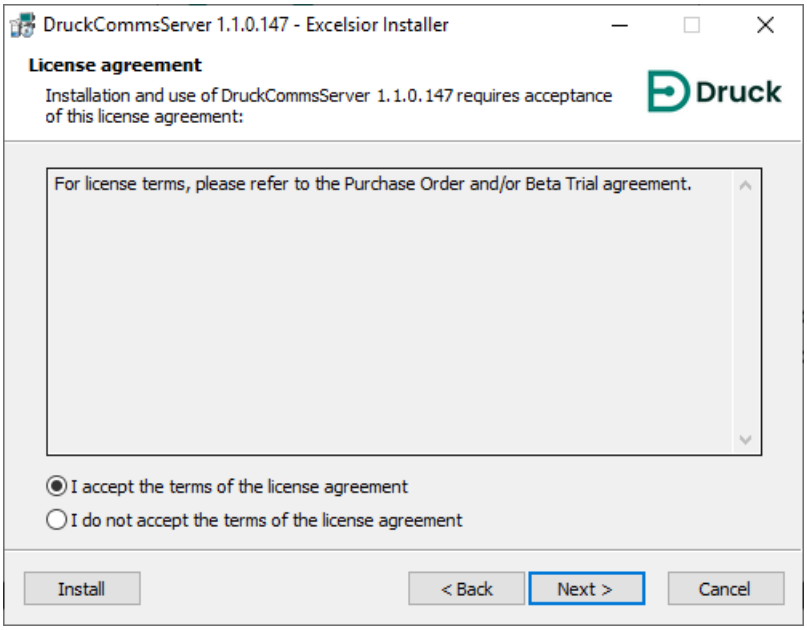
   Impossível comunicar com o equipamento de teste

   Transfira o pacote do comunicador do equipamento de teste. Depois de o transferir, descompacte-o e execute o ficheiro setup.exe para efetuar a instalação. Para as instruções de instalação ou para deteção e resolução de problemas, consulte o manual de instalação. Contacte o administrador se necessitar de assistência.

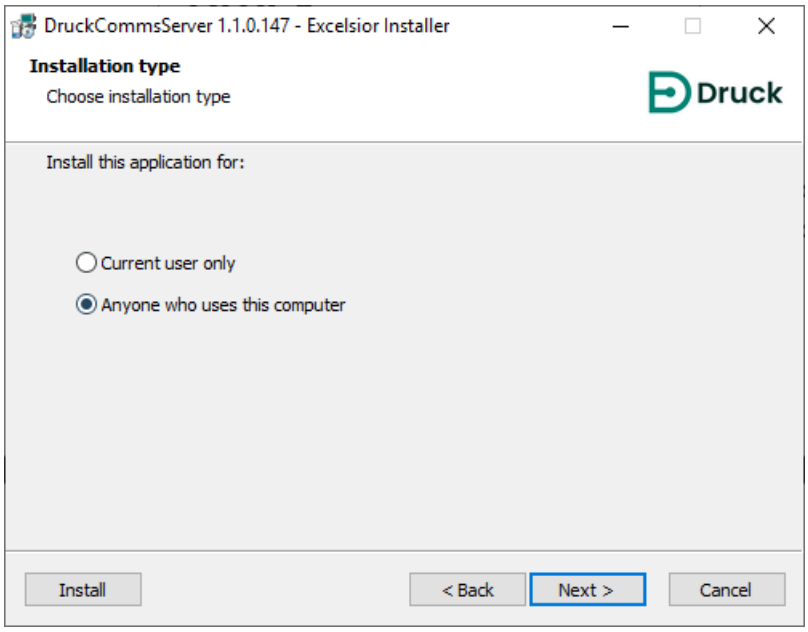
2. Selecione **Transferir** para obter o ficheiro de configuração do comunicador do equipamento de teste.
3. O ficheiro de configuração do comunicador do equipamento de teste é o ficheiro CommsServerInstall.zip. Quando tiver transferido o ficheiro CommsServerInstall.zip, pode executar os mesmos passos antes e depois da instalação da 4Sight2.
4. Extraia os ficheiros do ficheiro CommsServer.zip e clique duas vezes no ficheiro setup.exe para executar o instalador.
5. Será apresentado o instalador DruckCommsServer. Siga as instruções do instalador ou siga este guia.



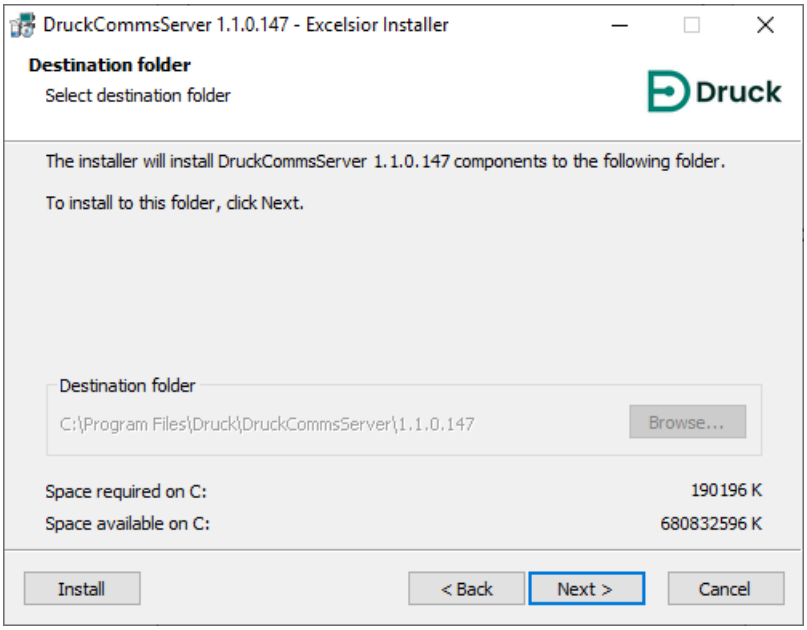
6. Selecione **Seguinte** para visualizar o ecrã Acordo de licença, leia os respetivos termos e selecione **I accept the terms of the license agreement** e, em seguida, clique em **Seguinte** para continuar.



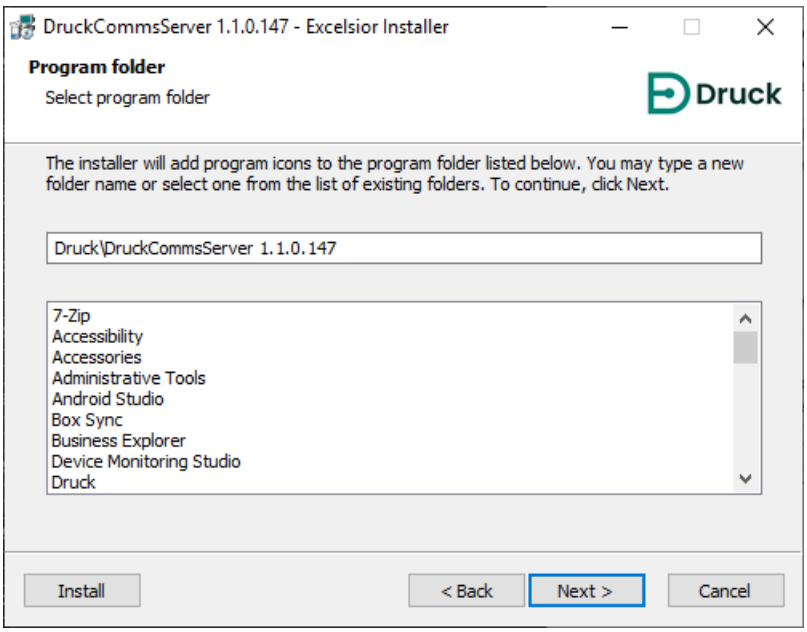
7. No ecrã Tipo de instalação, selecione se pretende instalar o CommsServer para todos os utilizadores deste PC ou apenas para o utilizador atual.



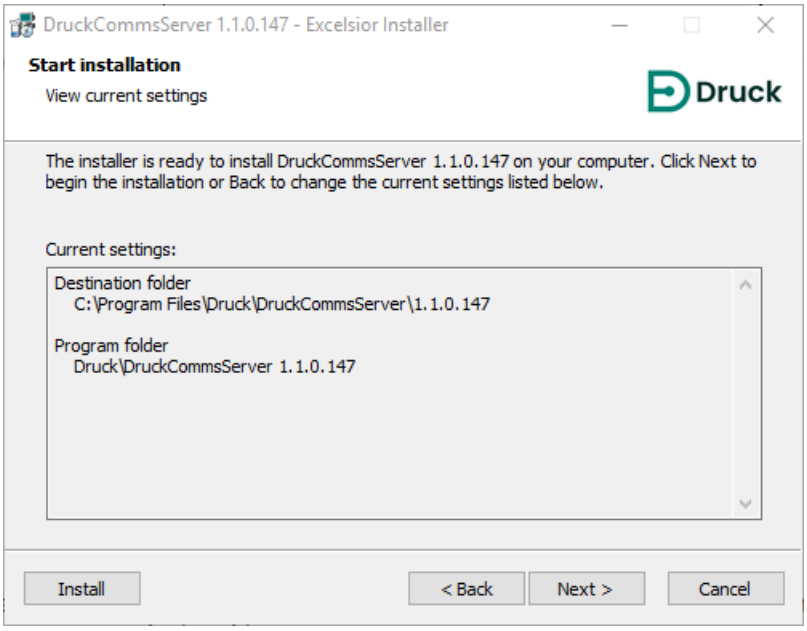
8. O ecrã Pasta de destino apresenta a pasta na qual o ficheiro DruckCommsServer será instalado. Por predefinição, a pasta encontra-se em C:\Programas\Druck\DruckCommsServer\[versão_aplicação]



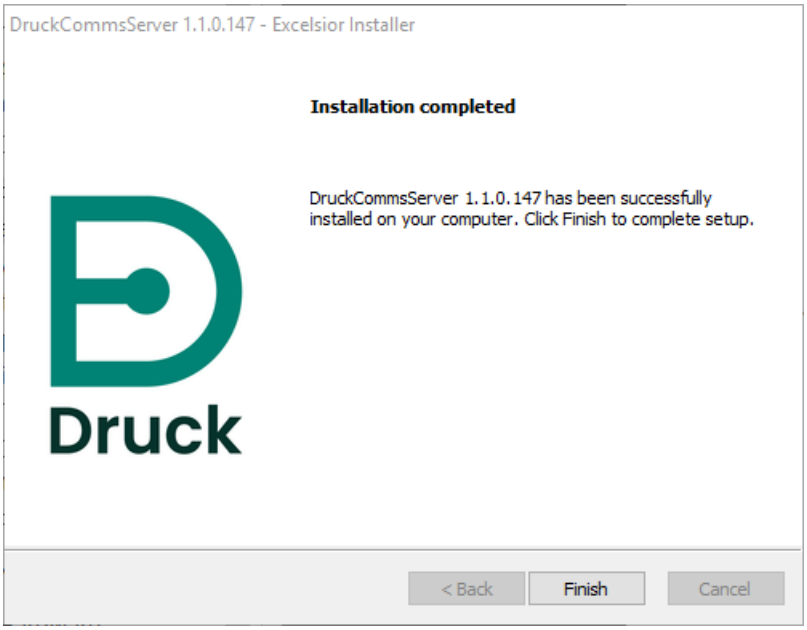
9. O ecrã Pasta do programa permite-lhe selecionar a localização onde o instalador adiciona o ícone do programa à pasta do programa.



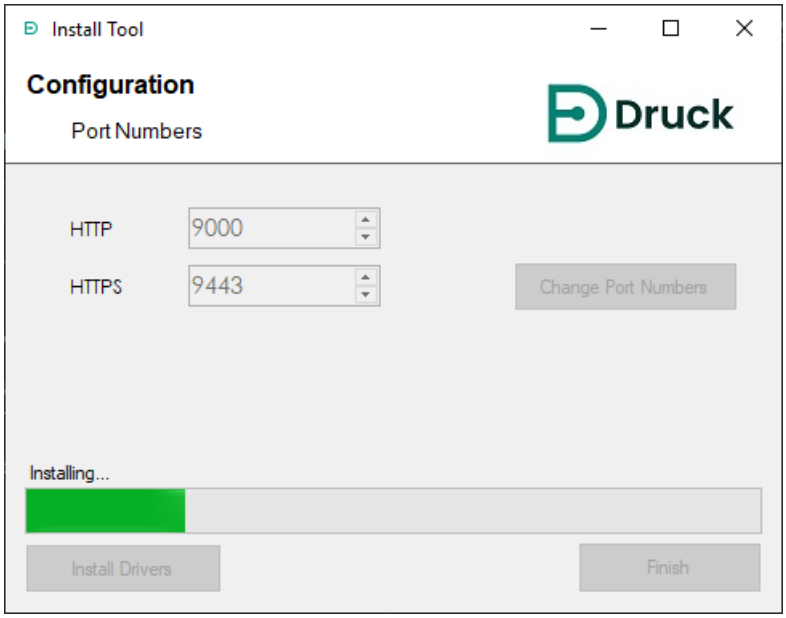
10. O ecrã Iniciar instalação é então apresentado. Selecione **Seguinte** para iniciar a instalação.



11. Depois de concluir a instalação, selecione **Concluir**.

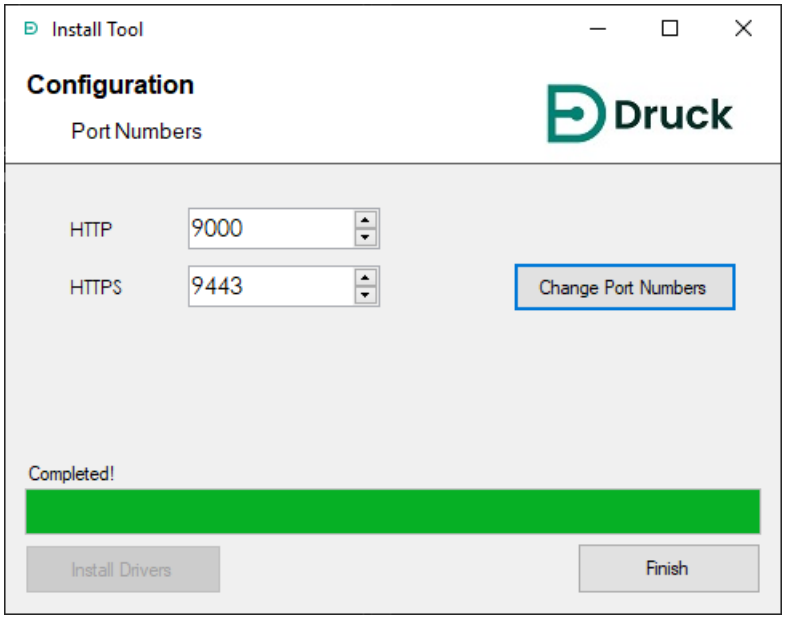


12. Em seguida, será apresentada a aplicação da ferramenta de instalação CommsServer para instalar os controladores adicionais exigidos.



13. Se não souber qual o número de porta alternativo que está a ser utilizado pela 4Sight2, contacte o seu utilizador administrativo

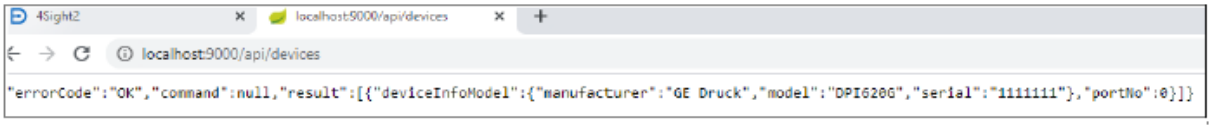
Nota: A ferramenta de instalação pode ser executada em separado após a instalação para voltar a configurar esses números de portas.



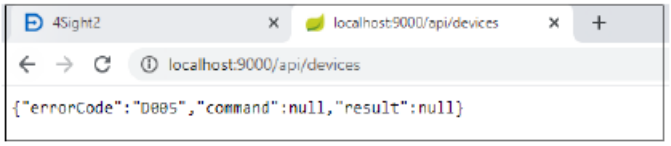
14. Teste a instalação do comunicador do equipamento de teste, digitando o seguinte URL no seu browser da web:

    http:/anfitriãolocal:[número da porta http utilizado acima da predefinição 9000]/api/dispositivos

O browser da web deve apresentar uma lista de todos os dispositivos que tem ligados:



Se não estiver ligado nenhum dispositivo, deverá ver o seguinte



Nota: Os controladores exigidos para os calibradores de temperatura não serão automaticamente configurados. Consulte a secção 4.3 Configuração dos controladores dos calibradores de temperatura

15. Se a instalação do controlador do dispositivo não tiver sido efetuada com sucesso, execute os passos da secção seguinte para configurar manualmente os controladores necessários.

4.1 Configuração manual do controlador

As definições da política de segurança das TI podem impedir que os controladores da Druck configurem automaticamente a instalação. Isso acontecerá se o 4Sight2 não conseguir se comunicar com os vários equipamentos.

Para as informações mais recentes https://www.bakerhughes.com/druck/test-and-calibration--instrumentation/calibration-management-software-4sight2

ou

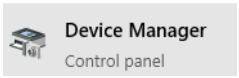
Para resolver este problema, os controladores da Druck podem ser manualmente configurados. Consulte o seu representante local de TI se tiver dúvidas sobre este problema ou se pretender obter assistência.

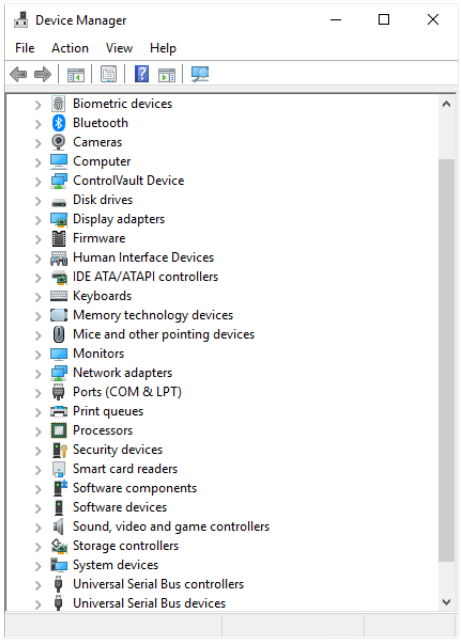
4.1.1 Pré-requisitos

Para instalar os controladores, a aplicação 4Sight2 terá de ser instalada ou terá de estar acessível na máquina. Antes de tentar instalar os controladores, certifique-se de que inicia sessão na aplicação 4Sight2 a partir do computador.

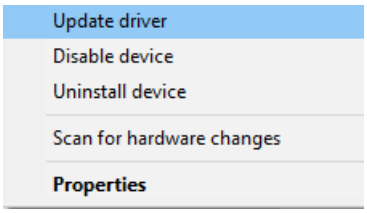
Para a instalação manual dos controladores, execute os seguintes passos:

1. No ambiente de trabalho, procure o gestor de dispositivos e execute-o.

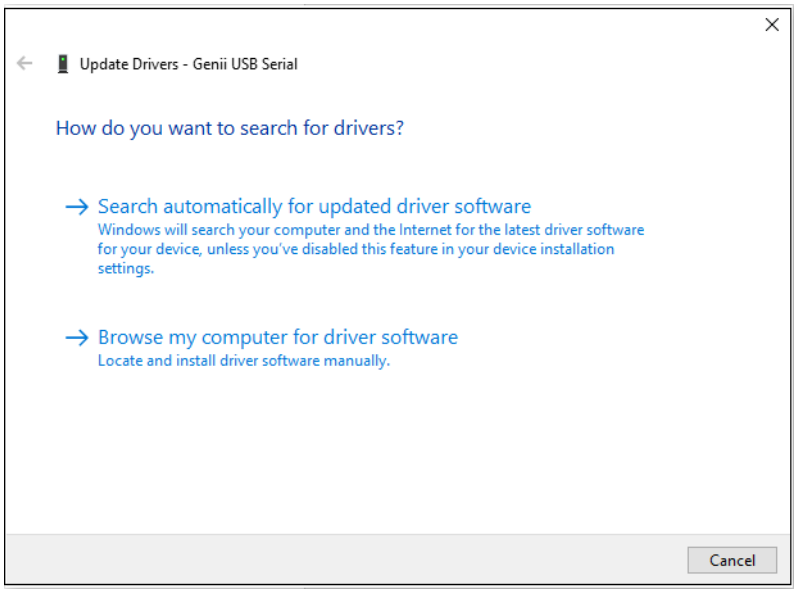




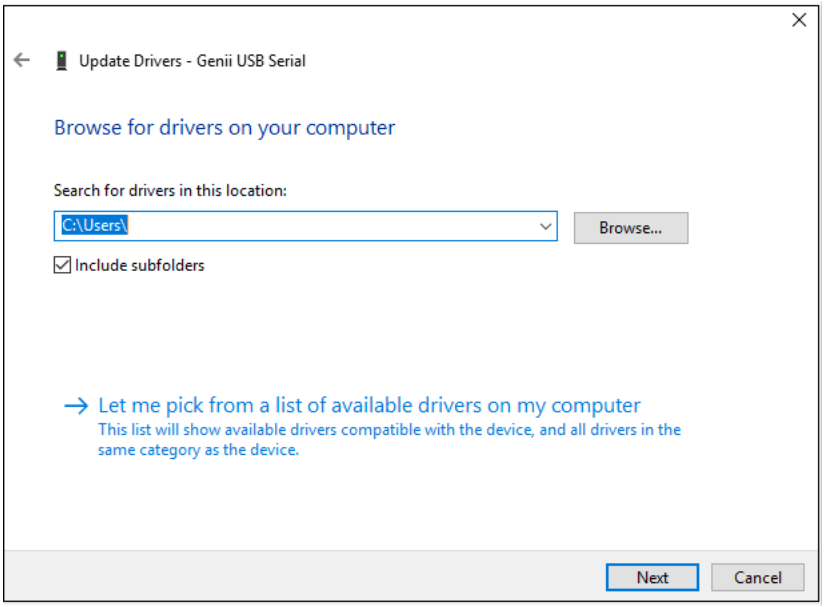
2. Percorra a lista dos dispositivos USB para encontrar os dispositivos que não estão configurados (Dispositivo desconhecido ou Outros dispositivos). Clique com o botão direito do rato e selecione **Atualizar controlador**.



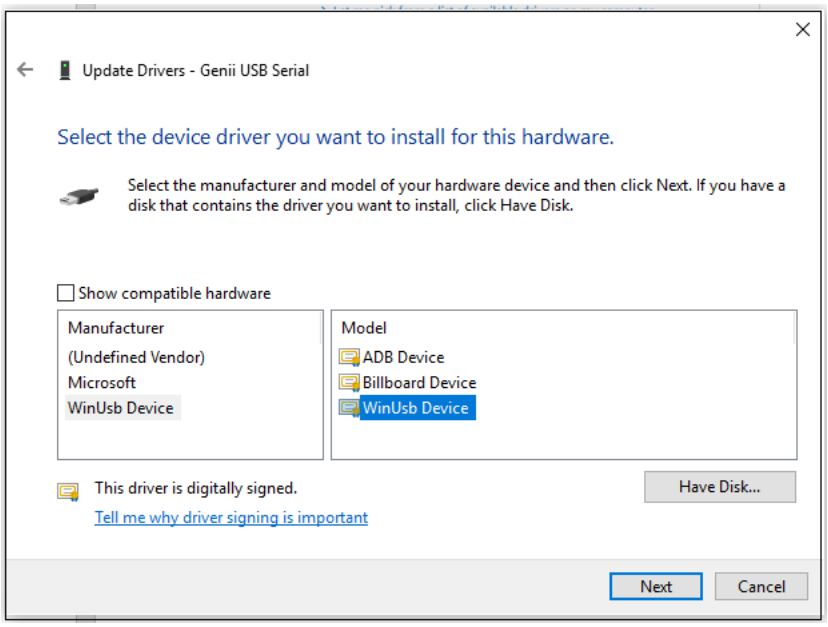
3. Selecione **Procurar o software do controlador no meu computador**.



4. Selecione **Escolher os controladores disponíveis a partir de uma lista** no meu computador.

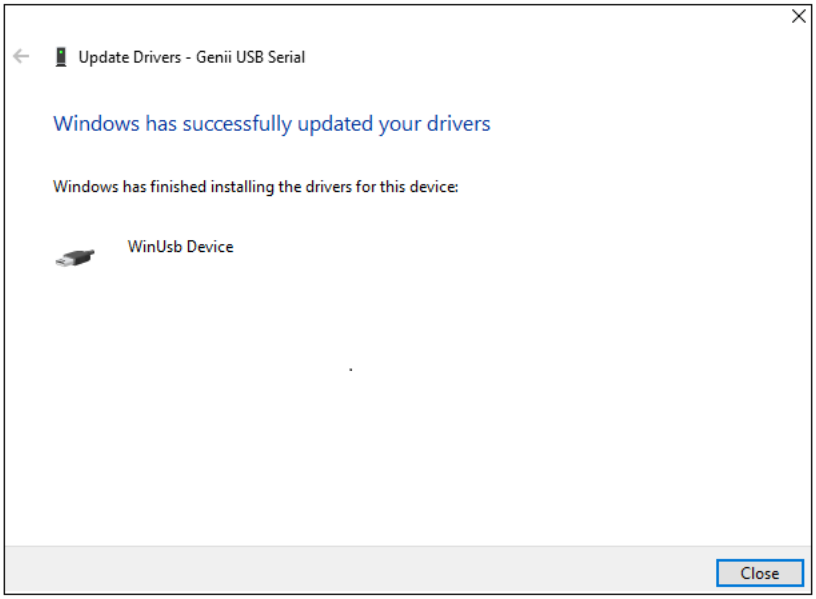


5. Desmarque **Mostrar hardware compatível** e selecione **Dispositivo WinUsb** para o Fabrico e **Dispositivo WinUsb** para o Modelo.



6. Será apresentado o seguinte aviso. Clique em **Sim**.

7. Será apresentado o ecrã que indica que o Windows atualizou com sucesso os seus controladores.

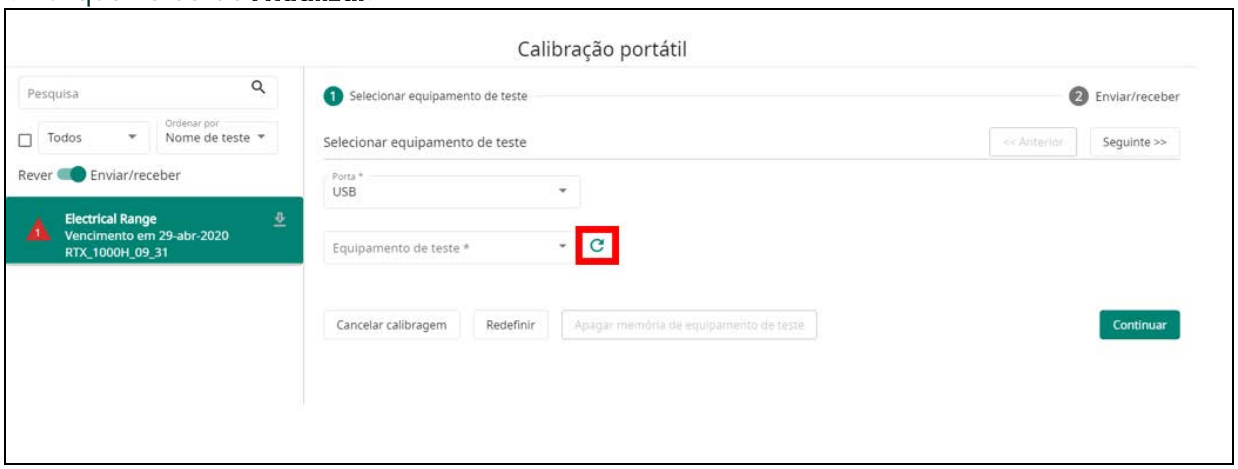


Repita os passos de cima para cada categoria de dispositivo quando ligar o dispositivo pela primeira vez.

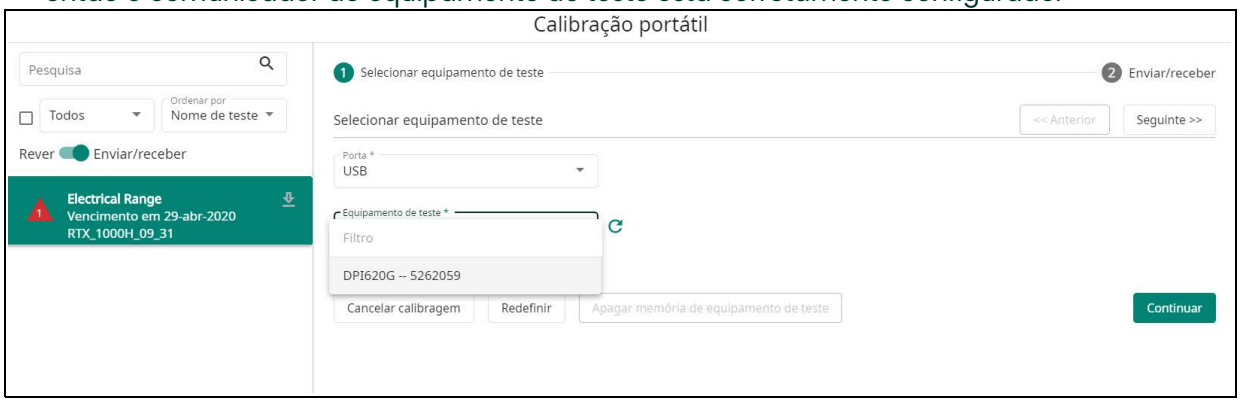
Por exemplo, se ligar um PACE e um Genii pela primeira vez, poderá ter de repetir os passos acima para o PACE e para o Genii em separado. Sempre que colocar novamente qualquer PACE ou Genii em funcionamento, já não terá de os configurar. Contudo, se ligar mais tarde uma categoria de dispositivo diferente (como um DPI611/612), terá de repetir os passos para esta categoria de dispositivo.

4.2 Testar o comunicador do equipamento de teste

1. Inicie sessão na 4Sight2 na qualidade de técnico.
2. Aceda a **Elementos >> Lista de trabalho.**
3. Selecione um ou mais intervalos e atribua-os ao fluxo de trabalho da calibragem Portátil ou Automatizada.
4. Clique no botão **Atualizar**.



5. Clique no menu pendente **Equipamento de teste**. Se encontrar na lista o dispositivo ligado, então o comunicador do equipamento de teste está corretamente configurado.



4.3 Configuração do controlador do calibrador da temperatura

Para permitir que o calibrador da temperatura comunique com a 4Sight2, tem de ser instalado um controlador FTDI.

1. Transfira o controlador FTDI através desta ligação: https://www.ftdichip.com/Controladores/VCP.htm.
2. Extraia o ficheiro transferido do ficheiro .zip e guarde-o numa localização conhecida na sua máquina.
3. Aceda ao gestor de dispositivos do Windows na sua máquina.
4. Selecione as Portas (COM e LPT) na lista de dispositivos para ver o calibrador da temperatura.
5. Clique com o botão direito do rato no calibrador de temperatura e selecione Atualizar controladores.
6. Selecione Procurar o software do controlador no meu computador.
7. Selecione Procurar junto à caixa de pesquisa com o título Procurar controladores nesta localização.
8. Selecione a pasta extraída que contém o controlador transferido.
9. Selecione Seguinte e feche.
10. O controlador será instalado agora.
11. Para testar a comunicação com um calibrador da temperatura na 4Sight2, aceda à calibragem automatizada e verifique se o calibrador da temperatura pode ser selecionado como Controlador de entrada. Em alternativa, volte a executar o passo 14 da secção 4.

Guia de implementação

5. Guia de implementação

5.1 Arquitetura de implementação

A arquitetura típica inclui a aplicação web 4Sight2 e o servidor UAA (Autenticação e Autorização do Utilizador), que são executados no servidor web Tomcat com a base de dados PostgreSQL em execução na mesma máquina.

A aplicação web Browser Client ligar-se-á ao servidor da 4Sight2, que, por sua vez, armazena e recupera as informações da base de dados PostgreSQL.

5.2 Implementação física

Assumimos que o utilizador que instala a 4Sight2 já implementou medidas de cibersegurança em conformidade com as políticas de segurança dos utilizadores, incluindo o seguinte:

- O servidor é colocado numa localização segura com controlo de acesso físico limitado.
- O controlo de acesso ao servidor está protegido com acesso autorizado limitado.
- A rede de servidores está protegida por uma firewall que permite o acesso limitado a aplicações bem conhecidas apenas em portas conhecidas
- As aplicações são executadas no seu próprio contexto e têm acesso à base de dados e aos sistemas de ficheiros apenas na sua própria pasta.

5.3 Rede

Os clientes são ligados por browsers da Internet, seja através de uma ligação Ethernet ou através de redes sem fios. Pode existir uma latência na rede sem fios, dependendo da banda larga sem fios e do número de dispositivos ligados.

É aconselhável desativar ou remover quaisquer plugins e extensões de browser que estejam instalados no próprio browser.

O servidor web 4Sight2 não deve ser exposto à Internet e qualquer acesso necessário tem de fornecido via Intranet ou VPN.

5.4 Sequência de implementação

PostgreSQL, Tomcat e Java Runtime são pré-requisitos para a aplicação 4Sight2. O PostgreSQL é instalado individualmente enquanto os outros são instalados juntamente com a aplicação. Assim, se o PostgreSQL já estiver instalado na máquina do utilizador, basta introduzir a palavra-passe do superutilizador para efetuar a ligação e a configuração do sistema.

A instalação necessita dos direitos de administrador do Windows na máquina. Antes da instalação, o utilizador deve ter consigo a palavra-passe de superutilizador do PostgreSQL. O nome de utilizador e palavra-passe de administrador da aplicação e o nome de utilizador e palavra--passe da base de dados.

A palavra-passe de superutilizador do PostgreSQL é necessária para criar a base de dados e outras estruturas dentro do servidor do PostGreSQL. O administrador da aplicação é o primeiro utilizador da aplicação. Ele é responsável pela criação de outros utilizadores e por lhes atribuir funções diferentes. O utilizador da base de dados tem acesso às bases de dados da 4Sight2 e do UAA. As credenciais do nome de utilizador são usadas para aceder à base de dados.

A aplicação é publicada numa porta da máquina. A porta predefinida é a 8083 e o utilizador pode mudar essa porta no momento da instalação ou mais tarde. O contexto de aplicação predefinido no Tomcat é a 4Sight2.

Siga o procedimento de endurecimento do sistema operativo, de acordo com as diretrizes da Microsoft ou da CIS para esse mesmo fim. O procedimento de instalação explica ao utilizador como instalar a PostgreSQL antes de instalar o servidor da 4Sight2.

O comunicador do equipamento de teste é instalado nas máquinas do cliente quando o equipamento de teste estiver ligado através das portas USB. Se o comunicador do equipamento de teste ainda não estiver instalado na máquina, é pedido ao utilizador que transfira o comunicador do equipamento de teste a partir do servidor da 4Sight2 e o instale na máquina. O comunicador do equipamento de teste ouve a porta 9000 e apenas pode comunicar numa camada segura.

5.5 Tarefas de pós-implementação

5.5.1 Adicionar utilizadores e grupos

O administrador é responsável pela criação de diferentes utilizadores na aplicação, tais como o supervisor, o técnico sénior, o técnico e o auditor. O administrador pode atribuí-los a diferentes grupos predefinidos incorporados. Se for necessário mais controlo ou uma granularidade de acesso mais refinada, então o administrador pode criar grupos personalizados e atribuir-lhes um acesso específico.

5.5.2 Palavras-passe predefinidas

A 4Sight2 está a usar a palavra-passe predefinida codificada para o utilizador do Tomcat no ficheiro "C:\Programas\Druck\4Sight2\<<latest folder number>>\apache-tomcat\conf\tomcat--user.xml".

Deve mudar a palavra-passe predefinida e utilizar sempre uma palavra-passe que cumpra os procedimentos recomendados.

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

Os procedimentos recomendados foram implementados para garantir que esta aplicação é segura. Para maior segurança, execute as seguintes tarefas:

Os ficheiros e pastas de configuração estão protegidos de modo a que, por predefinição, apenas o serviço e os sistemas tenham direitos de acesso. Por isso, antes de tentar executar as tarefas descritas em seguida, o administrador apenas tem acesso de leitura/escrita na pasta C:\Programas\Druck\4Sight2\<<latest folder number>>\apache-tomcat\conf. Abra a linha de comandos com as credenciais de administrador.

5.5.3 Comunicações seguras

Esta secção fornece instruções sobre a configuração da 4Sight2 em modo seguro (ou seja, modo SSL) utilizando um certificado autoassinado. Leia os pressupostos e os termos e condições definidos na aplicação 4Sight2 antes de continuar. Um certificado autoassinado é uma forma de

ativar o SSL na 4Sight2. Alternativamente, um certificado CA de terceiros pode ser comprado a vários vendedores, como a Symantec, Digicert, etc.

Nota: A ativação de SSL, por si só, não torna a sua aplicação segura. Esta é uma das práticas mais comuns para criar uma aplicação web segura.

5.5.3.1 Pressupostos e avisos

Os seguintes pressupostos são necessários para as instruções em baixo surtirem efeito:

O software OpenSSL for Windows é necessário para gerar Certificados autoassinados. A 4Sight2 pressupõe que as suas organizações, leis nacionais e regionais e regulamentações lhe permitem utilizar o software OpenSSL.

- O Keytool é um utilitário de gestão de Chaves e Certificados providenciado através de Java que é utilizado para gerar várias componentes envolvidas na configuração de https. A 4Sight2 pressupõe que as suas organizações, leis nacionais e regionais e regulamentações lhe permitem utilizar o utilitário Keytool.
- Tem de ter privilégios administrativos para realizar as configurações indicadas a seguir. Para mais informações sobre a obtenção de direitos administrativos, contacte o seu departamento de TI local.
- Os passos em baixo requerem uma compreensão básica sobre o processo informático, por isso, recomenda-se que sejam realizados pelo departamento de TI local ou sob a sua orientação.
- Os conteúdos apresentados neste documento, como os nomes de anfitrião, palavras-passe, URLs e caminhos de pasta apenas servem de referência. Assegure que modifica os comandos em conformidade antes da execução.
- As seguintes secções cobrem dois cenários. Um é o de Servidor e Cliente na mesma máquina e o outro é o de Servidor e Cliente em máquinas diferentes (ou seja, um cenário de Clientes múltiplos).

5.5.3.2 Passos para configurar a Aplicação 4Sight2 em Https

1. Pare a 4Sight2 a partir dos Serviços do Windows
2. Abra a linha de comandos no **Modo de Administrador**
3. Navegue para pasta em baixo no diretório de instalação da 4Sight2 executando o comando em baixo,

   cd "C:\Programas\Druck\4Sight2\<<latest folder number>>\apache-tomcat\conf"
4. Verifique se o keytool está presente executando o comando seguinte na linha de comandos: **Keytool** -?

   Caso contrário, defina o caminho de ambiente para a reciclagem do JRE na pasta de instalação da 4Sight2, conforme mostrado em baixo. Atualize o caminho correto com base na pasta de instalação.

   C:\Programas\Druck\4Sight2\<<latest folder number>>\jre\bin
   Defina "Path=%Path%;C:\Programas\Druck\4Sight2\<<latest folder number>>\jre\bin"
5. Para criar um novo certificado, avance para o passo 6, caso contrário, se um certificado já existir, faça o seguinte:

   a. Verifique se o ficheiro de certificado 4Sight.jks existe no keystore de java

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

b. Se o certificado já estiver instalado, remova-o,
keytool -delete -noprompt -alias <<hostname>> -storepass <<KeyPassword>> -
-keystore 4Sight.jks

c. Verifique e elimine se existir 4SightV2PublicKey.cer,
del "../../app/Certificate/4SightV2PublicKey.cer"

d. Verifique se o certificado já existe no cacert de java.
keytool -list -alias <<hostname>> -storepass changeit -keystore "../../jre/lib/security/
cacerts"

e. Elimine o certificado se existir no arquivo java.
keytool -delete -noprompt -alias <<hostname>> -storepass changeit -keystore "../../
jre/lib/security/cacerts" -file "../../app/Certificate/4SightV2PublicKey.cer"

6. Crie um novo certificado executando o seguinte:

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

7. Exporte o certificado para o ficheiro 4SightV2PublicKey.cer (não altere o nome do ficheiro nem o caminho).

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

   Quando o comando tiver sido executado com sucesso, aparece a mensagem: "O certificado guardado no ficheiro
   C:\Programas\Druck\4Sight2\<<latest folder
   number>>\app\Certificate\4SightV2PublicKey.cer" será apresentado.

8. Importe o certificado para um ficheiro CACert em java.

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

Após uma execução do comando com sucesso, será apresentada a mensagem "O certificado foi adicionado a keystore".

9. Adicione o certificado no ficheiro de configuração do Tomcat

   a. Abra o ficheiro server.xml a partir do local em baixo.
   C:\Programas\Druck\4Sight2\<<latest folder number>>\apache-
   -tomcat\conf\server.xml"

   b. Introduza o seguinte comando no server.xml.
   <Connector port="8443" protocol="org.apache.coyote.http11.Http11NioProtocol"
   maxThreads="150" SSLEnabled="true" sslProtocol="TLSv1.2" keystoreFile="conf/
   4Sight.jks"
   keystorePass="<<KeyPassword>>" keyAlias="tomcat" scheme="https" secure="true"
   clientAuth="false" />

   c. Comente a secção seguinte para desativar as ligações http.
   <connectionTimeout="20000" maxSwallowSize="104857600" port="8083"
   protocol="HTTP/1.1" redirectPort="8443" relaxedPathChars=""[\]^`{|}+"
   relaxedQueryChars=""[\]^`{|}+"/>

Nota: A aplicação não funcionará se não comentar esta parte.

10. Neste ponto, a configuração de Https da 4Sight2 está concluída.
11. Para testar a configuração efetuada acima, reinicie o Serviço 4Sight2 nos Serviços do Windows.
12. Abra o Google Chrome, limpe a cache do browser e reinicie o browser.
13. Introduza o seguinte URL no browser: https://<<host-name>>:8443/4sight2

- O carregamento do URL pode demorar algum tempo na primeira vez.
- Será apresentado um ecrã com a mensagem "A sua ligação não é privada"
- Clique no botão **Avançadas** >> **Continuar para XX**.
- Se não for apresentado o ecrã 4sight2, clique no botão **Recarregar**.
- Será direcionado para a página da 4Sight2.
- Ocorrerá um erro "Inseguro" na barra de endereço que desaparecerá após registar o certificado no mmc.

5.5.3.3 Passos para configurar o DruckCommsServer em Https se instalado no computador servidor

Substitua os valores em << >> por dados adequados antes de executar o comando.

1. Pare o DruckCommsServer a partir dos Serviços do Windows.
2. Abra a linha de comandos no **Modo de Administrador**.
3. Verifique se o keytool está presente executando o comando seguinte na linha de comandos:
   Keytool -?

   Caso contrário, defina o caminho de ambiente para a reciclagem do JRE na pasta de instalação da 4Sight2, conforme mostrado em baixo.
   Atualize o caminho correto com base na pasta de instalação.
   C:\Programas\Druck\4Sight2\<<latest folder number>>\jre\bin
   Defina "Path=%Path%;C:\Programas\Druck\4Sight2\<<latest folder number>>\jre\bin"
4. Navegue para pasta em baixo no diretório de instalação do DruckCommServer executando o comando em baixo,
   cd " C:\Programas\Druck\DruckCommsServer\<< Communication Service version >>"
5. Se já existir um certificado, execute o seguinte:
   a. Verifique se o certificado já existe no cacert de java.
   keytool -list -alias tomcat -storepass changeit -keystore cacerts
   b. Elimine o certificado se existir no arquivo java.
   keytool -delete -noprompt -alias tomcat -storepass changeit -keystore cacerts
   c. Elimine os certs pré-configurados do CommsServer predefinido
   del 4Sight.jks
   del 4SightV2DeviceMngr.pfx
6. Crie um novo certificado executando o seguinte:
   keytool -genkey -trustcacerts -keyalg "RSA" -keysize 2048 -validity 1095 -keypass <<KeyPassword>> -alias tomcat -keystore CommServer.jks -storepass <<StorePassword>> dname "CN=localhost, OU=<<Organization Unit>>, O=<<Organization>>, L=<<Location>>, S=<<State>>, C=<<Country Initial>>" -ext eku:critical=sa

7. Exporte o certificado para o ficheiro DruckCommServer.cer

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

   Quando o comando tiver sido executado com sucesso, aparece a mensagem:
   Será apresentado "Certificado guardado no ficheiro DruckCommServer.cer ".

8. Importe o certificado comm server para um ficheiro java CACert.

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

   Após uma execução do comando com sucesso, será apresentada a mensagem "O certificado foi adicionado a keystore".

9. Importe o certificado 4Sight para um ficheiro java CACert.

   keytool -import -noprompt -trustcacerts -alias <<server hostname>> -storepass changeit --keystore cacerts -file "C:\Programas\Druck\4Sight2\<<latest folder number>>\app\Certificate\4SightV2PublicKey.cer"

   Após uma execução do comando com sucesso, será apresentada a mensagem "O certificado foi adicionado a keystore".

10. Edite a palavra-passe de key-store para application.properties no DruckCommsServer.

    Abra este ficheiro:
    C:\Programas\Druck\DruckCommsServer\<<Communication Service Version>>\application.properties e altere a seguinte linha:
    keystore = CommServer.jks
    key-store.password= << StorePassword >>
    Nota: **<< StorePassword >>** consultando a **StorePassword** utilizada no passo 6.

11. Reinicie os serviços 4Sight2 e DruckCommsServer.

5.5.3.4 Passos para configurar o DruckCommsServer em HTTPs se instalado no computador servidor

1. O utilitário Keytool inclui Java para poder instalar Java no seu computador ou verificar a disponibilidade do keytool java diretamente, sem instalação de Java.
2. Pare o DruckCommsServer a partir dos Serviços do Windows.
3. Abra a linha de comandos no **Modo de Administrador**.
4. Verifique se o keytool está presente executando o comando seguinte na linha de comandos:
   Keytool -?

   Caso contrário, defina o caminho de ambiente para a reciclagem do JRE se tiver instalado o java no computador ou defina o caminho para keytool conforme indicado em baixo.
   Atualize o caminho correto com base na pasta de instalação.
   C:\Programas\Java\<< Java version >>\bin
   Defina Path=%Path%; "C:\Programas\Java\<< Java version >>\bin"

5. Obtenha o ficheiro **4SightV2PublicKey.cer** a partir do computador servidor em que a aplicação 4Sight está instalada. Este ficheiro está localizado no servidor em baixo,

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

6. Copie **4SightV2PublicKey.cer** para o seguinte caminho:

   C:\Programas\Druck\DruckCommsServer\<< Communication Service version >>

7. Agora siga os passos 4 a 8 da secção 5.5.3.3.
8. Importe o certificado 4Sight para um ficheiro java CACert.

   keytool -import -noprompt -trustcacerts -alias <<server hostname>> -storepass changeit --keystore cacerts -file 4SightV2PublicKey.cer

   Após uma execução do comando com sucesso, será apresentada a mensagem "O certificado foi adicionado a keystore".
9. Agora siga os passos 10 a 11 da secção 5.5.3.3.

5.5.3.5 Passos para gerar um certificado autoassinado para a 4Sight2

1. Transfira e instale o Open SSL for Windows.
2. Pare os serviços 4Sight2 a partir dos Serviços do Windows.
3. Crie uma nova pasta com o nome **4Sight2Certificate** na unidade C.

   Pode escolher qualquer local ou nome de pasta desde que tenha acesso de administrador a essa pasta.
4. Crie um novo ficheiro na pasta de cima no bloco de notas e guarde o ficheiro como **openssl--ca.cnf**

   copie os conteúdos em baixo para o ficheiro e guarde o ficheiro.

```
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: Atualize o **[Company Name]** acima e salve o arquivo. Este é o nome do emissor do certificado que irá aparecem no console de gerenciamento.

5. Crie um novo ficheiro no bloco de notas na pasta de cima e guarde o ficheiro como **openssl--server.cnf**

   copie os conteúdos em baixo para o ficheiro e guarde o ficheiro.

```
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: Atualize o Nome do anfitrião e o endereço IPv4 de cima e guarde o ficheiro.

6. Abra a linha de comandos com privilégios de Administrador.
7. Navegue para a pasta 4Sight2Certificate executando o seguinte,

   cd "<<full path to 4Sight2Certificate >>"
8. Defina a variável do caminho da pasta de reciclagem OpenSSL executando o comando em baixo.

   Defina path=%path%;"<<bin folder of openssl>>"
   Exemplo do caminho predefinido:
   Defina Path=%Path%;"C:\Programas\OpenSSL-Win64\bin"
9. Defina a variável do caminho da pasta de reciclagem JRE executando o comando em baixo. Nota: o caminho em baixo pode ser diferente.

   Defina path=%path%;"C:\Programas\Druck\4Sight2\<<latest folder number>>\jre\bin"
10. Execute o comando em baixo para gerar os ficheiros cacert.pem e cakey.pem

    openssl req -x509 -config openssl-ca.cnf -newkey rsa:4096 -days <<Number of days>> -sha256 -nodes -out cacert.pem -outform PEM
    Introduza os dados de certificado corretos quando lhe for solicitado, por ex., o país, estado, etc.
11. Execute os comandos em baixo para gerar os ficheiros servercert.csr e serverkey.pem

    openssl req -config openssl-server.cnf -newkey rsa:2048 -days <<Number of days>> -sha256 -nodes -out servercert.csr -outform PEM
    Introduza os dados de certificado corretos quando lhe for solicitado, por ex., o país, estado, etc.
12. Crie um ficheiro novo no bloco de notas e atribua o nome index.txt. Guarde o ficheiro na pasta 4Sight2Certificate.
13. Crie um ficheiro novo no bloco de notas e atribua o nome serial.txt. Guarde o ficheiro na pasta 4Sight2Certificate.

    Abra o ficheiro e introduza **01** Guarde e feche o ficheiro.
14. Execute o comando em baixo para gerar novos certificados nos ficheiros servercert.pem e serverkey.pem.

    openssl ca -config openssl-ca.cnf -policy signing_policy -extensions signing_req -out servercert.pem -infiles servercert.csr
    Introduza Y para confirmar as alterações. Verá a base de dados atualizada após uma execução com sucesso.
15. Empacote os ficheiros chave existentes para o formato PFX executando o comando em baixo.

    openssl pkcs12 -export -in servercert.pem -inkey serverkey.pem -certfile cacert.pem -name "<<hostname>>" -out <<hostname>>.p12
    ser-lhe-á pedido para introduzir a palavra-passe duas vezes.

16. Converta o arquivo PFX para Java key store ordenado pelo local da reciclagem JRE referido acima, ou seja, o caminho tomcat/config.

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

    Nota: Mantenha a mesma palavra-passe para ambos os arquivos. Certifique-se de que indica 4Sight.jks presente na pasta config de tomcat, conforme indicado em cima.
    Ser-lhe-á pedido para introduzir a palavra-passe de keystore de destino e a palavra-passe de keystore de origem. Após uma execução do comando com sucesso, aparece a mensagem "Importação de comando concluída: 1 entrada importada com sucesso".

17. Exporte o certificado de keystore de java para ficheiro em:

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

    Nota: Certifique-se de que indica 4Sight.jks presente na pasta config de tomcat, conforme indicado em cima.
    Receberá a mensagem "Certificado guardado no ficheiro" após uma execução com sucesso,

18. Importe o ficheiro de certificado para a pasta cacerts no diretório de instalação da 4Sight2.

    Nota: o caminho pode variar consoante o diretório de instalação e a versão da 4Sight2
    keytool -import -noprompt -trustcacerts -alias <<hostname>> -storepass changeit -keystore "C:\Programas\Druck\4Sight2\<<latest folder number>>\jre\lib\security\cacerts" -file "C:\Programas\Druck\4Sight2\<<latest folder number>>\app\Certificate\4SightV2PublicKey.cer"

    Nota: por algum motivo, o alias que está a tentar criar já existe, execute o comando em baixo para eliminá-lo e, em seguida, execute o de cima para criar um novo alias:
    keytool -delete -noprompt -trustcacerts -alias <<hostname>> -storepass changeit -keystore "C:\Programas\Druck\4Sight2\<<latest folder number>>\jre\lib\security\cacerts" -file "C:\Programas\Druck\4Sight2\<<latest folder number>>\app\Certificate\4SightV2PublicKey.cer"

    Receberá a mensagem "O certificado foi adicionado a keystore" após uma execução com sucesso deste comando.

19. Efetue a seguinte alteração no ficheiro server.xml (existe em C:\Programas\Druck\4Sight2\<<latest folder number>>\apache-tomcat\conf).

    a. Introduza o seguinte comando no 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 a secção seguinte para desativar as ligações http.
<connectionTimeout="20000" maxSwallowSize="104857600" port="8083"
protocol="HTTP/1.1" redirectPort="8443" relaxedPathChars=""[\ ]^`{|}+"
relaxedQueryChars=""[\ ]^`{|}+"/>

20. Este passo conclui a configuração de https para a 4Sight2. Inicie agora o serviço 4sight2 a partir dos Serviços dos Windows.

5.5.3.6 Passos para configurar o certificado autoassinado para o DruckCommsServer se instalado no computador servidor

Aqui, pressupomos que converteu com sucesso a aplicação 4sight2 para HTTPs executando os passos da secção 5.5.3.5 e que já tem os ficheiros de baixo na pasta **4Sight2Certificate**:

- openssl-server.cnf
- openssl-ca.cnf
- cacert.pem
- cakey.pem
- index.txt
- serial.txt
- 4SightV2PublicKey.cer (Este ficheiro pode estar localizado na pasta C:\Programas\Druck\4Sight2\<<latest folder number>>\app\Certificate)

1. Crie uma nova pasta como **CommserverCertificate** e copie os ficheiros de cima e efetue as alterações conforme indicado em baixo:

- openssl-server.cnf

  Na secção **req**, altere o valor **default_keyfile** como "**DruckCommServerCertKey.pem**".
  - Em **server_distinguished_name**, altere o valor **commonName** para "**localhost**".
  - Em **alternate_names**, altere o valor **DNS.1** para "**localhost**".
  - Em **alternate_names**, altere o valor **IP.1** para "**127.0.0.1**"
  - Guarde o ficheiro.
- openssl-ca.cnf. (Não altere nada no interior)
- cacert.pem. (Não altere nada no interior)
- index.txt (Elimine todos os conteúdos no interior, transforme-o num ficheiro vazio)
- serial.txt (Elimine todos os conteúdos no interior e crie apenas a entrada de 01 no interior)

2. Pare o serviço DruckCommsServer nos Serviços do Windows.
3. Abra a linha de comandos com privilégios de Administrador.
4. Navegue para a pasta **CommserverCertificate** executando o seguinte,

   cd "<<full path to CommserverCertificate >>"
5. Defina a variável do caminho da pasta de reciclagem OpenSSL executando o comando em baixo.

   Defina path=%path%;"<<bin folder of openssl>>"
   Exemplo do caminho predefinido:

Defina Path=%Path%;"C:\Programas\OpenSSL-Win64\bin"

6. Defina a variável do caminho da pasta de reciclagem JRE executando o comando em baixo. Nota: o caminho em baixo pode ser diferente,

   Defina path=%path%;"C:\Programas\Druck\4Sight2\<<latest folder number>>\jre\bin"

7. Após este passo, crie um pedido de certificado Comm Server seguindo o comando

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

   Após a execução deste comando, terá um pedido em **DruckCommServer.csr** e uma chave privada em **DruckCommServerCertKey.pem**

8. Em seguida, realize o seguinte para assinar o pedido csr com o seu ca:

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

9. Em seguida, crie um ficheiro PFX com o alias **tomcat** para comm server seguindo o comando,

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

10. Converta o arquivo PFX para Java keystore utilizando o keytool

    Nota: mantenha a mesma palavra-passe para ambos os keystores.
    keytool -importkeystore -srckeystore DruckCommServer.pfx -srcstoretype PKCS12 -destkeystore CommServer.jks -deststoretype jks

11. Agora, importe o certificado para o cacert.

    a. Em seguida, elimine o alias tomcat incluído por predefinição com a instalação.
    keytool -delete -noprompt -trustcacerts -alias tomcat -storepass changeit -keystore "C:\Programas\Druck\DruckCommsServer\<< Communication Service version >>\cacerts"

    b. Após eliminar o alias tomcat existente, importe o certificado para o cacerts através de
    keytool -import -noprompt -trustcacerts -alias tomcat -storepass changeit -keystore "C:\Programas\Druck\DruckCommsServer\<< Communication Service version >>\cacerts" -file DruckCommServerCert.pem

12. Agora é necessário importar a chave pública da 4Sight2 para o comm server cacert para autenticação de comunicação, por isso, execute o comando em baixo,

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

13. No fim, terá **DruckCommServer.pfx** e **CommServer.jks** na pasta **CommserverCertificate** atual.

    Copie esses ficheiros e cole-os no diretório "C:\Programas\Druck\DruckCommsServer\<< Communication Service version >>\". Edite **application.properties** a partir do mesmo local e altere o valor da propriedade conforme indicado em baixo

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

5.5.3.6.1 Instalar o certificado no Windows para 4sight e DruckCommsServer

1. Abra Executar e introduza "mmc" e prima Enter.
2. Vá para Ficheiro e selecione Adicionar/Remover snap-ins.
3. No menu esquerdo, selecione os certificados. Prima Adicionar e selecionar a Conta do computador >> Seguinte >> Concluir. Em seguida, clique em Ok.
4. Expanda a secção de certificados (computador local). Expanda as Autoridades de Certificação de Raiz Fidedigna.

   Clique com o botão direito na pasta Certificados >> Todas as tarefas >> Importar.

   Selecione cacert.pem >> seguinte >> concluir.

   A nossa autoridade CA personalizada é instalada com sucesso como autoridade fidedigna.

Após estes passos, inicie o serviço DruckCommsServer.

5.5.3.7 Passos para configurar o certificado autoassinado para o DruckCommsServer se instalado num computador cliente

Para converter o DruckCommsServer para HTTPs, tem de ter o keytool java e de abrir o utilitário OpenSSL.

1. O utilitário Keytool inclui Java para poder instalar Java no seu computador ou verificar a disponibilidade do keytool java diretamente, sem instalação de Java.
2. Transfira e instale o OpenSSL for Windows.
3. Defina a variável do caminho da pasta de reciclagem OpenSSL executando o comando em baixo.

   Defina path=%path%;"<<bin folder of openssl>>"

   Exemplo do caminho predefinido:

   Defina Path=%Path%;"C:\Programas\OpenSSL-Win64\bin"

4. Defina a variável do caminho da pasta de reciclagem JRE executando o comando em baixo.

   C:\Programas\Java\<< Java version >>\bin
   Defina Path=%Path%; "C:\Programas\Java\<< Java version >>\bin"

5. Pare o serviço DruckCommsServer nos Serviços do Windows.
6. Crie uma nova pasta com o nome **CommserverCertificate** na unidade C ou outra unidade à sua escolha.
7. Obtenha o ficheiro de certificado público da 4Sight2 **4SightV2PublicKey.cer** a partir do computador servidor, localizado no caminho C:\Programas\Druck\4Sight2\<<latest folder number>>\app\Certificate e copie este ficheiro para a pasta **CommserverCertificate**.
8. Agora crie **openssl-server.cnf** e **openssl-ca.cnf** seguindo os passos 4 e 5 da secção 5.5.3.5 e crie o index.txt e serial.txt seguindo os passos 12 e 13 na pasta **CommserverCertificate**.
9. Tem agora cinco ficheiros na pasta CommServerCertificate
   a. openssl-server.cnf
   b. openssl-ca.cnf
   c. index.txt
   d. serial.txt
   e. 4SightV2PublicKey.cer
10. Abra a linha de comandos com privilégios de Administrador.

    Navegue para a pasta CommserverCertificate executando o seguinte
    cd "<<full path to CommserverCertificate >>"

11. Execute o comando em baixo para gerar os ficheiros cacert.pem e cakey.pem.

openssl req -x509 -config openssl-ca.cnf -newkey rsa:4096 -sha256 -nodes -out cacert.pem -outform PEM

Introduza os dados de certificado corretos quando lhe for solicitado, por ex., o país, estado, etc.

12. Agora altere o conteúdo dos ficheiros na pasta **CommserverCertificate** executando o passo 1 da secção 5.5.3.6.
13. Execute agora os passos 7 a 11 de 5.5.3.6.
14. Agora é necessário importar a chave pública da 4Sight2 para o comm server cacert para autenticação de comunicação, por isso, execute o comando em baixo,

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

15. No fim, terá **DruckCommServer.pfx** e **CommServer.jks** na pasta **CommserverCertificate** atual.

    Copie esses ficheiros e cole-os no diretório **"C:\Programas\Druck\DruckCommsServer\<< Communication Service version >>\"**. Edite **application.properties** a partir do mesmo local e altere o valor da propriedade conforme indicado em baixo

    a. Keystore = CommServer.jks

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

    c. key-store.type=JKS

5.5.3.7.1 Instalar o certificado no Windows para o DruckCommsServer.

1. Abra Executar e introduza "mmc" e prima Enter.
2. Vá para Ficheiro e selecione Adicionar/Remover snap-ins.
3. No menu esquerdo, selecione os certificados. Prima Adicionar e selecionar a Conta do computador >> Seguinte >> Concluir. Em seguida, clique em Ok.
4. Expanda a secção de certificados (computador local). Expanda as Autoridades de Certificação de Raiz Fidedigna.

   Clique com o botão direito na pasta Certificados >> Todas as tarefas >> Importar.

   Selecione cacert.pem >> seguinte >> concluir.

   A nossa autoridade CA personalizada é instalada com sucesso como autoridade fidedigna.

Após estes passos, inicie o serviço DruckCommsServer.

Se apenas deseja verificar se o DruckCommsServer é convertido com sucesso para https, no separador do Google Chrome, abra a seguinte ligação: **https://localhost:9443/api/devicemanager/version** (Introduza o seu número de porta comm server se o tiver alterado, mas a predefinição é 9443)

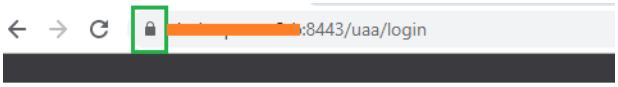
5.5.3.8 Validar o certificado na 4Sight2

1. Reinicie o computador servidor.
2. Reinicie os serviços 4Sight2 e DruckCommsServer a partir dos Serviços do Windows
3. Abra o Google Chrome, limpe a cache do browser e reinicie o Google Chrome. Certifique-se de que não estão a ser executadas outras instâncias do Google Chrome.
4. Introduza o URL de baixo na barra de endereço e prima enter.

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

   Nota: tem de utilizar o nome do anfitrião no URL de cima
5. Deve ser apresentado o ecrã de início de sessão com o URL HTTPS correto.

   Nota: o erro a vermelho desapareceu da barra de endereço. Se a ligação ainda não for segura, reinicie o seu computador e avance para o passo 3.



Perguntas mais frequentes sobre a instalação da 4Sight2

6. Perguntas mais frequentes sobre a instalação da 4Sight2

6.1 Configuração e instalação

Pergunta 1: Tenho uma organização com várias instalações em diferentes regiões do mundo. Qual é a melhor forma de configurar a 4Sight2?

Resposta: Depende de como mantém e gere estas instalações. Se todas as instalações forem mantidas e geridas a partir de uma plataforma de TI central, pode instalar uma licença individual da 4Sight2 a nível central. Todas as instalações podem aceder à 4Sight2 através da rede ou de LAN. Por outro lado, se tiver empresas subordinadas que sejam entidades separadas com gestão autónoma, pode adquirir várias licenças da 4Sight2.

Pergunta 2: Se eu comprar várias licenças da 4Sight2, haverá alguma comunicação entre as mesmas?

Resposta: Não. Cada licença da 4Sight2 é um software separado e isolado, com a sua própria instalação da aplicação e base de dados. Não existe comunicação entre instalações separadas. Contacte a equipa da 4Sight2 para mais esclarecimentos ou para discutir quaisquer requisitos especiais.

Pergunta 3: Como posso transferir a 4Sight2?

Resposta: Pode facilmente transferir a 4Sight2 a partir do web site da empresa. Abaixo é fornecida a ligação.

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

OU

Pode telefonar para os escritórios de vendas e efetuar uma encomenda. Deverá então receber a versão de demonstração numa pen USB.

Pergunta 4: Posso instalar a 4Sight2 num sistema operativo que não seja Windows?

Resposta: Não. A 4Sight2 apenas é suportada para a plataforma Windows.

Pergunta 5: Transferi e instalei a 4Sight2. Como acedo à 4Sight2?

Resposta: A 4Sight2 é um software baseado na web. Por conseguinte, não é criado qualquer ícone no seu ambiente de trabalho ou computador quando instala a 4Sight2. Para aceder à 4Sight2:

- Abra o Google Chrome, cole o URL abaixo na barra de endereço e prima Enter.
- Se a 4Sight2 estiver instalada no mesmo computador, utilize http://anfitriãolocal:<número_porta_aplicação>/4sight2. Se a 4Sight2 estiver instalada num computador diferente na mesma rede, utilize

  http://<Nome do computador OU Endereço IP>:<número_porta_aplicação>/4sight2
- Crie um marcador no Google Chrome para utilização futura.

Pergunta 6: Falha do instalador da 4Sight2 na localização dos ficheiros da base de dados Postgres

Certifique-se de que o instalador foi mudado para uma localização local e de que o ficheiro executável está a ser executado a partir da pasta Disco 1. Certifique-se de que a localização local para a qual o instalador foi movido não tem um nome de caminho longo, pois tal pode originar uma falha nos ficheiros do instalador.

Pergunta 7: O que acontece se o processo de atualização for cancelado em qualquer fase do processo?

Resposta: Se, em qualquer fase, o administrador cancelar o processo de atualização, a aplicação reverterá para a versão 1.4 e deverá ficar a funcionar. O administrador tem de iniciar novamente o processo de atualização para efetuar a atualização com sucesso.

Pergunta 8: Durante a instalação da aplicação 4Sight2, pode ser apresentada ao utilizador a mensagem "Introduza um número de porta válido. Para saber os números de porta válidos, consulte o manual de instalação."

Resposta: Em seguida, é indicado o intervalo de portas inválidas. Selecione uma porta válida para prosseguir com a instalação

- As portas 0 a 1024 são reservadas para a ligação TCP.
- Lista de portas inseguras: 2049, 3659, 4045, 6000, 6665-6669, 65535

Pergunta 9: A 4Sight2 com https não está a funcionar no sistema

Resposta: Respeite a sintaxe para o nome de domínio do computador onde a aplicação 4sight2 será instalada

<domain> ::= <subdomain>

<subdomain> ::= <label> | <subdomain> "." <label>

<label> ::= <letter> [[<ldh-str>] <let-dig>]

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

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

<let-dig> ::= <letter> | <digit>

<letter> ::= qualquer um dos 52 caracteres do alfabeto inglês de A a Z em

maiúscula e de a a z em minúscula

<digit> ::= qualquer um dos dez dígitos de 0 a 9

Nota: São permitidas letras em maiúscula e minúscula em nomes de domínio. Dois nomes com a mesma grafia, mas com maiúsculas e minúsculas diferentes, são tratados como idênticos.

6.2 Perguntas mais frequentes sobre o comunicador do equipamento de teste

Pergunta 1: Concluí todos os passos do manual de instalação e ainda não consigo visualizar o meu dispositivo na lista.

Resposta: Se ainda não consegue localizar o seu equipamento de teste na lista depois de executar estes passos, volte a instalar os controladores da 4Sight2. Para isso, aceda a **Painel de controlo >> Programas e funcionalidades** e desinstale o DruckCommsServer da lista. Instale novamente o comunicador do equipamento de teste.

Pergunta 2:. Deparei-me com o erro "**Nenhum dispositivo encontrado**"

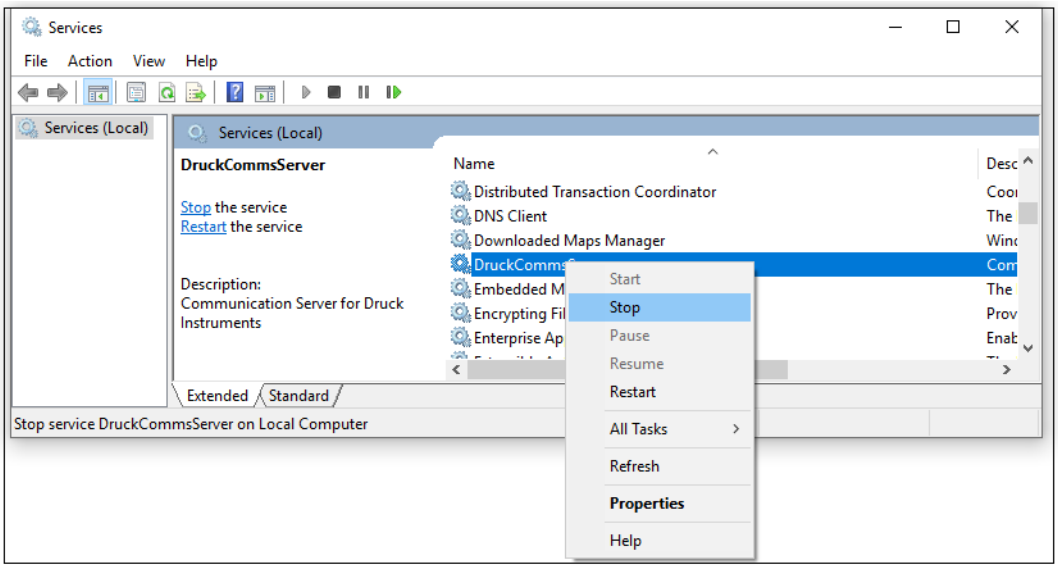
Resposta: Para resolver o problema,

- Certifique-se de que ligou física e corretamente o dispositivo com o cabo USB. Para verificar esta situação, aceda ao gestor de dispositivos para localizar o seu dispositivo na lista. Idealmente, deveria encontrar o seu dispositivo na secção de dispositivos Universal Serial Bus. Se encontrar o seu dispositivo em Outros dispositivos, terá de executar as definições mencionadas acima para que o seu dispositivo se torne num dispositivo USB.
- Certifique-se de que o seu dispositivo se encontra no modo de comunicações ou comms. Consulte o passo 1 acima.
- Certifique-se de que o caminho do controlador esta correctamente indicado em C:\Windows\INF... Consulte o passo 2 acima.

Pergunta 3: Deparei-me com o erro "**Erro de servidor interno**" quando cliquei no botão para atualizar ou quando cliquei no equipamento de teste apresentado na lista.

Resposta: Para resolver este problema,

- Aceda aos serviços do Windows (também denominado por Serviços),
- Clique com o botão direito no serviço **DruckCommsServer** apresentado na lista e clique em **Reiniciar**.



- Aceda a 4Sight2 >> Clique no botão **Atualizar**. Deverá ver os dispositivos na lista.

Pergunta 4: Deparei-me com o erro "**Erro de comunicações**".

Resposta: Por vezes o software não comunica corretamente com o dispositivo por vários motivos, como um contacto USB solto, um dispositivo que se desliga, um dispositivo ocupado a realizar outras tarefas, o servidor ocupado a executar outras tarefas, etc. Clique novamente no botão Atualizar e o problema deverá desaparecer (tente 2-3 vezes)

Contudo, se o erro persistir, tente executar os seguintes passos

- Reinicie o seu dispositivo (Genii/PACE). Certifique-se de que é seguro fazê-lo e de que o dispositivo não está a meio de uma operação crítica. Tente novamente. Certifique-se também de que o dispositivo está fisicamente ligado.

Se estes passos não resolverem o problema, siga as instruções no passo 3 acima e reinicie o serviço **DruckCommsServer**.

Resolução de problemas na instalação

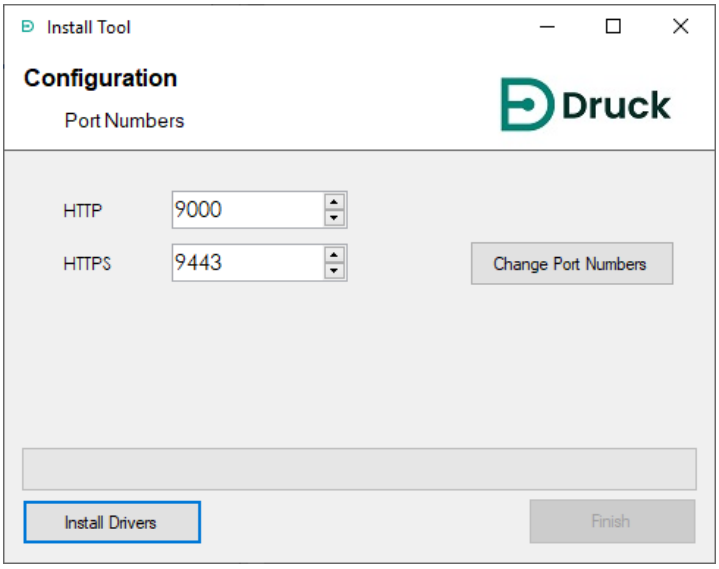
7. Resolução de problemas na instalação

7.1 Problemas de comunicação do equipamento de teste

Se, depois de utilizar a 4Sight2 para comunicar com o equipamento de teste, verificar que não é devolvido qualquer equipamento de teste, embora tenha verificado que o comunicador do equipamento de teste devolveu a cadeia de caracteres json depois de um contacto direto com o comunicador, isto pode dever-se a um de dois principais problemas:

- Os números de porta foram configurados de forma incorreta - contacte o seu administrador para saber quais as portas utilizadas pela 4Sigth2 para entrar em contacto com o comunicador do equipamento de teste.

  Quando souber que portas que deve utilizar, aceda a C:\Programas\Druck\DruckCommsServer\[Versão] e execute o ficheiro CommsServerInstallTool.exe



Edite os números das portas e, em seguida, clique no botão **Alterar números de porta**. Aguarde até que o serviço reinicie. Os números das portas foram agora alterados. Selecione o botão **Concluir**.

- O comunicador do equipamento de teste não está configurado para Https, mas a 4Sight2 está configurada para tal.

  Contacte o seu administrador para instalar um certificado autoassinado para o comunicador do equipamento de teste.

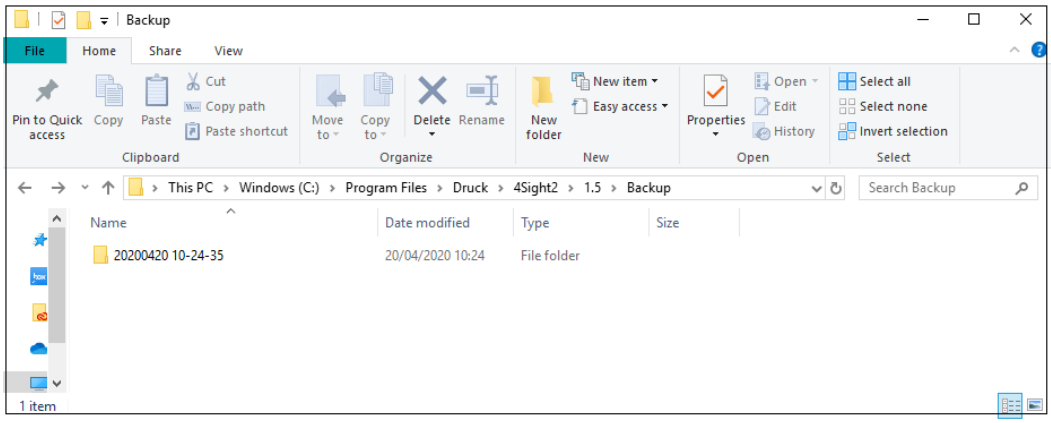
7.2 Cópia de segurança da base de dados Postgres

Consulte o manual do utilizador da 4Sight2 - 123M3138 para obter informações sobre a cópia de segurança da base de dados postgres.

7.3 Restauro da base de dados Postgres

Partindo do princípio de que já efetuou uma cópia de segurança da base de dados com a aplicação 4Sight.

A aplicação 4Sight (versão 1.4 e superiores) fornece uma interface para iniciar uma cópia de segurança (iniciada pelo utilizador/programada). Esta operação cria ficheiros na pasta de cópia de segurança existente no diretório de instalação da 4Sight no servidor. Cada cópia de segurança iniciada cria uma nova pasta dentro da pasta de cópia de segurança com o nome no formato AAAAMMDDHHSS (ano, mês, dia, hora e segundos), consoante a data e hora em que a cópia de segurança é concluída com sucesso.



É recomendado efetuar uma cópia de segurança do conteúdo da pasta de cópia de segurança num suporte de dados separado.

Cada pasta tem 5 ficheiros.

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

Os ficheiros *.bck têm um sufixo com a versão da aplicação 4Sight. Certifique-se de que restaura uma base de dados que corresponde à versão exata da sua aplicação. Versões superiores/ inferiores da base de dados não são suportadas pela aplicação. Tenha em atenção que a versão contém um caráter de sublinhado (_) e não um ponto (.), como, por ex., 1_4 e não 1.4. Ao utilizar os comandos indicados abaixo em Passos para restaurar, certifique-se de que substitui <VERSÃO_APLICAÇÃO> pela versão correta da 4Sight que foi instalada.

O ficheiro metadata.properties contém o nome da cópia de segurança, conforme indicado no início da cópia de segurança.

Verificação SHA 256

Numa cópia de segurança, existem 3 ficheiros - um para cada base de dados, com a extensão .bck. O ficheiro metadata.properties contém o SHA 256 de cada um dos ficheiros de cópia de segurança.

1. Abra uma linha de comandos como administrador e altere o diretório para a pasta que contém os ficheiros de cópia de segurança selecionados.
2. Utilize os comandos abaixo para calcular o SHA256 de cada ficheiro:

   certutil -hashfile 4Sight**<VERSÃO_APLICAÇÃO>**.bck SHA256
   certutil -hashfile 4Sightaudit**<VERSÃO_APLICAÇÃO>**.bck SHA256
   certutil -hashfile uaa**<VERSÃO_APLICAÇÃO>**.bck SHA256
3. Antes de prosseguir com os passos para restaurar, confirme se o SHA 256 de cada ficheiro corresponde ao SHA 256 mencionado no ficheiro de metadados. O ficheiro de cópia de segurança é válido para restauro se a soma de verificação da linha de comandos e a soma de verificação do ficheiro de metadados forem exatamente iguais. Avance para os passos para restaurar apenas se forem iguais.

7.4 Passos para restaurar:

1. Inicie sessão no servidor da 4Sight como administrador.
2. Localize a porta na qual a base de dados Postgres está a ser executada. Esta pode ser encontrada na propriedade spring.datasource.url no ficheiro <DIRETÓRIO DE INSTALAÇÃO DA 4Sight>\apache-tomcat\webapps\application.properties. Utilize um Bloco de notas executado no modo de administrador para abrir este ficheiro. É o número exatamente antes de 4Sight**<VERSÃO_APLICAÇÃO>.**
3. Inicie sessão no utilitário de linha de comandos psql a partir de uma linha de comandos executada no modo de administrador, com o utilizador da postgres.

   C:\Programas\PostgreSQL\11\bin\psql" --port=<PORTA_BD> postgres postgres
4. O utilizador da base de dados utilizado pela aplicação pode ser encontrado na propriedade spring.datasource.username no ficheiro <DIRETÓRIO DE INSTALAÇÃO DA 4Sight>\apache--tomcat\webapps\application.properties. Utilize um Bloco de notas executado no modo de administrador para abrir este ficheiro.
5. Elimine as bases de dados *_temp, se existirem, e, em seguida, crie as bases de dados *_temp vazias, executando os comandos abaixo na linha de comandos psql.

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

   Altere o proprietário da base de dados das 3 bases de dados acima para este utilizador. Tenha em atenção que o nome de utilizador é sensível a maiúsculas e minúsculas.

   ALTER DATABASE "4Sight**<VERSÃO_APLICAÇÃO>**_temp" OWNER TO "**<UTILIZADOR_BD>**";

ALTER DATABASE "4Sightaudit**<VERSÃO_APLICAÇÃO>**_temp" OWNER TO "**<UTILIZADOR_BD>**";
ALTER DATABASE "uaa**<VERSÃO_APLICAÇÃO>**_temp" OWNER TO "**<UTILIZADOR_BD>**";

6. Verifique os ficheiros metadata.properties das cópias de segurança e decida que cópia de segurança tem de restaurar.
7. Abra outra linha de comandos como administrador e altere o diretório para a pasta que contém os ficheiros de cópia de segurança selecionados acima.

   Restaure a base de dados a partir dos ficheiros *.bck para as bases de dados *_temp, utilizando os comandos indicados abaixo. Se lhe for solicitada uma palavra-passe, introduza a palavra-passe de superutilizador postgres.
   "C:\Programas\PostgreSQL\11\bin\pg_restore" --port=**<PORTA_BD>** --no-owner --
   -username=postgres --dbname=4Sight**<VERSÃO_APLICAÇÃO>**_temp -n public --
   -role=**<UTILIZADOR_BD>** 4Sight**<VERSÃO_APLICAÇÃO>**.bck

   "C:\Programas\PostgreSQL\11\bin\pg_restore" --port=**<PORTA_BD>** --no-owner --
   -username=postgres --dbname=4Sightaudit**<VERSÃO_APLICAÇÃO>**_temp -n public --
   -role=**<UTILIZADOR_BD>** 4Sightaudit**<VERSÃO_APLICAÇÃO>**.bck

   "C:\Programas\PostgreSQL\11\bin\pg_restore" --port=**<PORTA_BD>** --no-owner --
   -username=postgres --dbname=uaa**<VERSÃO_APLICAÇÃO>**_temp -n public --
   -role=**<UTILIZADOR_BD>** uaa**<VERSÃO_APLICAÇÃO>**.bck
8. Elimine as bases de dados *_old, se existirem, executando os comandos abaixo na linha de comandos psql.

   DROP DATABASE IF EXISTS "4Sight**<VERSÃO_APLICAÇÃO>**_old";
   DROP DATABASE IF EXISTS "4Sightaudit**<VERSÃO_APLICAÇÃO>**_old";
   DROP DATABASE IF EXISTS "uaa**<VERSÃO_APLICAÇÃO>**_old";
9. Pare as aplicações pgadmin e serviço da 4Sight, se alguma destas estiver aberta.
10. Mude o nome das bases de dados 4Sight existentes, executando os comandos abaixo na linha de comandos psql.

    ALTER DATABASE "4Sight**<VERSÃO_APLICAÇÃO>**" RENAME TO
    "4Sight**<VERSÃO_APLICAÇÃO>**_old";
    ALTER DATABASE "4Sightaudit**<VERSÃO_APLICAÇÃO>**" RENAME TO
    "4Sightaudit**<VERSÃO_APLICAÇÃO>**_old";
    ALTER DATABASE "uaa**<VERSÃO_APLICAÇÃO>**" RENAME TO "uaa**<VERSÃO_APLICAÇÃO>**_old";
11. Mude o nome das bases de dados *_temp para bases de dados 4Sight, executando os comandos abaixo na linha de comandos psql.

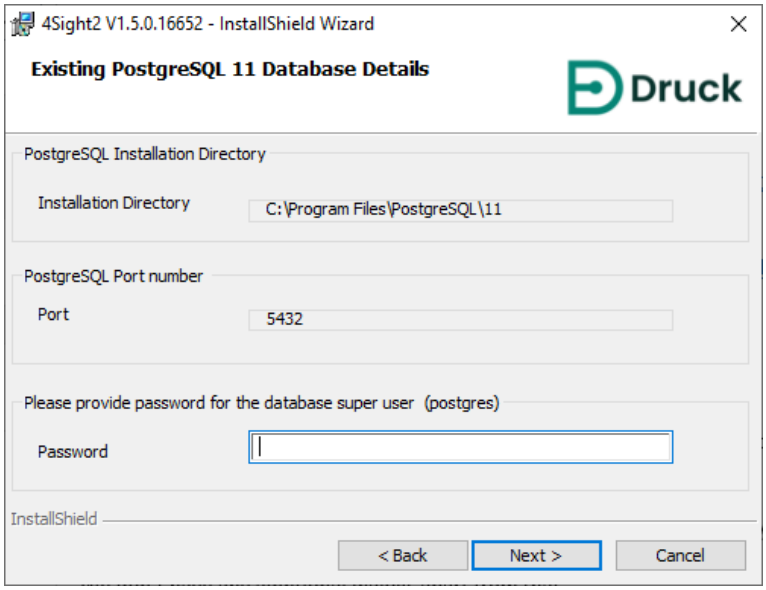
    ALTER DATABASE "4Sight**<VERSÃO_APLICAÇÃO>**_temp" RENAME TO
    "4Sight**<VERSÃO_APLICAÇÃO>**";
    ALTER DATABASE "4Sightaudit**<VERSÃO_APLICAÇÃO>**_temp" RENAME TO
    "4Sightaudit**<VERSÃO_APLICAÇÃO>**";
    ALTER DATABASE "uaa**<VERSÃO_APLICAÇÃO>**_temp" RENAME TO "uaa**<VERSÃO_APLICAÇÃO>**";
12. Inicie o serviço da 4Sight e tente iniciar sessão como administrador. Tenha em atenção que, para iniciar sessão agora, tem de ser utilizada a palavra-passe do administrador no momento em que foi efetuada a cópia de segurança.

7.5 Como recuperar de uma falha de sistema numa máquina com a 4Sight2?

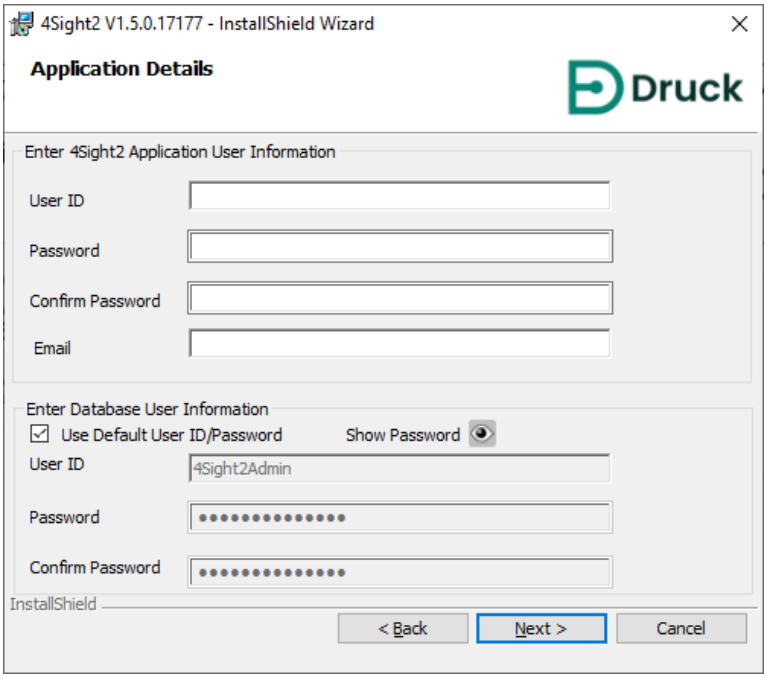
Suposições: O utilizador efetuou uma cópia de segurança da base de dados da 4Sight2 antes da falha de sistema.

O utilizador sabe o nome de utilizador e palavra-passe da aplicação e da base de dados.

1. Configure a máquina com o sistema operativo e os controladores compatíveis.
2. Instale a 4Sight2 na máquina.
3. Quando instalar a aplicação, forneça o mesmo nome de utilizador e palavra-passe que lhe foram anteriormente fornecidos para a aplicação e a base de dados Postgres.

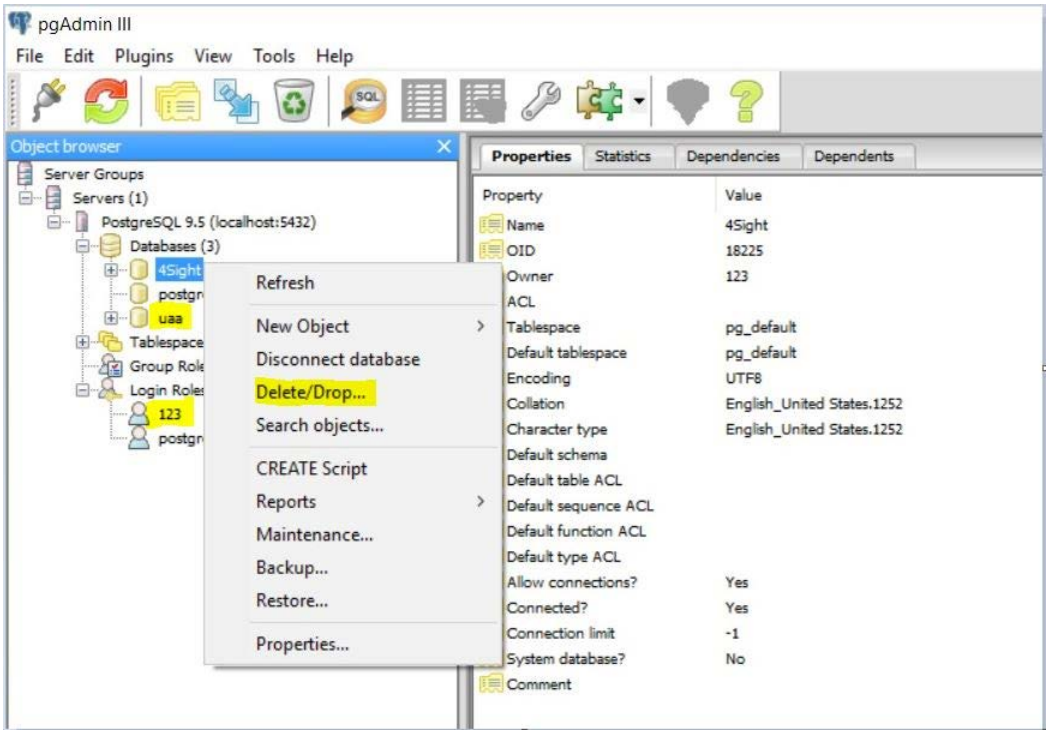


A palavra-passe é a mesma da instalação anterior



Preencha todos os campos tal como na instalação anterior

4. Após instalar com sucesso a aplicação, remova a base de dados predefinida criada ao instalar a aplicação a partir de pgAdmin (clique com o botão direito na base de dados e selecione Eliminar/remover). Se ocorrer um erro na remoção da base de dados, reinicie o serviço da Postgres e tente novamente depois de atualizar.



5. Depois de remover com sucesso a base de dados e o utilizador, execute estes passos para restaurar a base de dados conforme descrito acima a partir da linha de comandos.
6. Agora que restaurou com sucesso a base de dados, abra a aplicação a partir do browser e analise a base de dados.

7.6 Cenário de falha da instalação:

A tabela abaixo explica os vários cenários de falha durante a instalação e as respetivas soluções.

Mensagem de erro	Cenário	Solução/ação a executar
"Insufficient disk space available to install 4Sight2 application. Please ensure a minimum of 4096 MB is available. Free Space : available MB."	Falha devido a um problema de tamanho do disco rígido (se não existir espaço suficiente no início da atualização)	O administrador tem de libertar espaço na unidade relevante e, em seguida, tentar novamente o processo de atualização.
"Deployment fail while Migrating database"	Falha devido a um problema de tamanho do disco rígido (se não existir espaço suficiente depois de a atualização ter sido iniciada com sucesso)	O administrador tem de libertar espaço na unidade relevante e, em seguida, tentar novamente o processo de atualização.

Mensagem de erro	Cenário	Solução/ação a executar
"Installation failed while migrating Database. Please reinstall 4sight2"	Falha devido à integridade dos dados na cópia da base de dados	O administrador tem de contactar o suporte técnico se tal ocorrer. O motivo de integridade dos dados é captado em registos na localização [C:\Utilizadores\[Nome de utilizador]\ Dados da aplicação\Local\Temp\registos]
"Installation failed while migrating Database. Please reinstall 4sight2"	Falha devido à integridade dos dados na fase de atualização do esquema	O administrador tem de contactar o suporte técnico se tal ocorrer. O motivo de integridade dos dados é captado em registos na localização [C:\Programas\Druck\4Sight2\<<latest folder number>>\registos
"Failed to locate existing 4Sight2 service. Please ensure existing 4Sight2 version is installed on this machine and the service is running"	Esta falha ocorre se o instalador não for capaz de obter o estado do serviço	O administrador tem de assegurar que o serviço da 4Sight2 está a ser executado
"Failed to start the 4Sight2 service. Please ensure the 4Sight2 service is present and running"	Falha se a aplicação estiver corrompida, alguns ficheiros foram eliminados, a porta está a ser utilizada por outra aplicação ou o utilizador interrompeu o serviço, etc.	Se o administrador conseguir obter com sucesso o estado do serviço e se este não estiver a ser executado por algum motivo (por ex., aplicação corrompida, alguns ficheiros eliminados, porta em utilização por outra aplicação ou serviço interrompido pelo utilizador, etc.), deve tentar iniciar o serviço. Se não for possível iniciar o serviço, o administrador tem de contactar o suporte ao cliente para resolver o problema.
"Upgrade of 4Sight2 application is supported from version 1.3 onwards. For earlier version upgrade support please contact Customer Care."	A atualização não será efetuada se estiver instalada uma versão anterior à versão 1.3.	Apenas é possível efetuar uma atualização a partir da versão 1.3 para uma versão mais recente.
Installer has detected another minor version of PostgreSQL 11. Installer will not continue. Refer to 4Sight2 Installation manual for more details	A instalação da 4Sight2 não irá continuar, uma vez que já existe a mesma versão (variante) na máquina de destino	Possíveis opções 1. O utilizador pode escolher outra máquina 2. O utilizador pode efetuar uma cópia de segurança da aplicação existente (Postgres versão 11.3), desinstalá-la e instalar essa aplicação noutra máquina. Desinstalar a Postgres e reiniciar a instalação da 4Sight2

Mensagem de erro	Cenário	Solução/ação a executar
Installation failed while upgrading database. Please reinstall 4Sight2. Refer to 4Sight2 Installation manual for more details	Podem ter ocorrido alguns erros internos durante a atualização e o utilizador pode tentar reinstalar a aplicação	Se o problema persistir, o utilizador pode partilhar os registos da instalação para melhor compreensão do problema

7.7 Causas de erro comuns

Estes são alguns dos problemas normalmente observados e que estão associados à comunicação por USB da 4Sight2 com o equipamento da Druck.

- A ligação física é fraca ou instável
- Cabos/portas gastos
- Má qualidade dos adaptadores de USB
- Adaptadores/portas USB sobrecarregados
- Os dispositivos estão a funcionar há bastante tempo e, por isso, entram no modo de hibernação ou suspensão
- Os dispositivos não se encontram no modo de comunicação
- O software do controlador não está instalado nem atualizado. Para estabelecer comunicação com o hardware, necessita de ter a mesma versão da aplicação 4Sight2 e dos controladores.
- Os dispositivos possuem versões de firmware muito antigas.

7.8 Desinstalar a 4Sight2

Siga estas instruções se for necessário instalar uma nova cópia ou uma nova versão da 4Sight2 ou se for necessário desinstalar a 4Sight2 devido à ocorrência de problemas durante a instalação.

A desinstalação do componente da base de dados PostgreSQL irá eliminar a base de dados da 4Sight2, resultando numa perda de dados. Não será automaticamente gerada uma cópia de segurança através dos seguintes passos. Por isso, certifique-se de que criou manualmente uma cópia de segurança antes de continuar e de que gravou essa cópia numa localização alternativa à pasta da instalação da 4Sight2. Consulte a cópia de segurança da base de dados Postgres e restaure a secção deste manual.

Se optar por desinstalar apenas a aplicação 4Sight2 e pretender manter a base de dados, consulte a parte deste manual sobre a instalação da 4Sight2. Serão necessárias as credenciais do superutilizador para a base de dados após a reinstalação. Não tente desinstalar a aplicação se não souber as credenciais.

Se pretender atualizar a versão da 4Sight2 sem desinstalar a base de dados, **NÃO** siga estas instruções.

1. Aceda ao Painel de controlo >> Programas e funcionalidades
2. Clique com o botão direito na 4Sight2 e selecione Desinstalar.
3. Siga as instruções do assistente Desinstalar
4. Clique com o botão direito na PostgreSQL 11 e selecione Desinstalar
5. Siga as instruções do assistente Desinstalar

6. A desinstalação da PostgreSQL não elimina a pasta dos dados. Terá de o fazer manualmente. Elimine a pasta dos dados que está localizada em C:\Programas\PostgreSQL\11\
   a. Se pretender eliminar a totalidade da pasta da PostgreSQL, certifique-se de que coloca na pasta da reciclagem todos os ficheiros de cópia de segurança e scripts antes de continuar
   b. Por predefinição, as cópias de segurança da base de dados da 4Sight2 são criadas e guardadas na seguinte localização: C:\Programas\PostgreSQL\11\reciclagem
7. Recomendamos que reinicie o computador, se possível.
8. A 4Sight2 está agora desinstalada.

7.9 Resolução de problemas de Comunicação Segura

1. O comando 'command name' não é reconhecido como um comando interno ou externo. Por ex., 'keytool' não é reconhecido como comando interno ou externo,

- Se encontrar um erro como este, significa que na pasta em que está, a linha de comandos não encontra referência para o comando especificado.

  Para resolver este erro, utilize o comando de baixo para indicar a pasta correta.
  Defina Path=%Path%;"<<full path of the location where the command is>>"
  Exemplo, no erro em cima relacionado com keytool, tem de definir o caminho de baixo,
  Defina "Path=%Path%;C:\Programas\Druck\4Sight2\<<latest folder number>>\jre\bin"

2. Endereço IP Incorreto

- Se aparecer uma mensagem de erro com este texto, significa que o Endereço IP ou Nome do anfitrião nos ficheiros openssl-ca.cnf ou openssl-server.cnf está incorreto. Nota: pode ter de corrigir isto em vários locais nestes ficheiros e executar novamente os passos.

3. Ficheiro ou diretório não existe...

- Se aparecer uma mensagem de erro com este texto, significa que o comando que executou se refere provavelmente a num nome de ficheiro incorreto. Verifique o comando quanto a erros de nomes de ficheiro e se o ficheiro com esse nome está presente na pasta e execute novamente os comandos. Pode ter corrigir o nome do ficheiro no comando ou seguir os passos necessários para gerar os ficheiros em falta.
- Este erro pode ocorrer com ficheiros index.txt e serial.txt porque, em certos casos, a extensão do ficheiro é anexada ao nome duas vezes, por ex., intex.txt.txt.

  Basta editar o ficheiro e guardá-lo sem a extensão .txt. Certifique-se que o ficheiro tem uma extensão .txt.

Procedimentos recomendados

8. Procedimentos recomendados

Endurecimento do servidor

O ambiente do servidor deve ser endurecido de acordo com as diretrizes da Microsoft ou da CIS.

8.1 Tomcat

- Instale o Tomcat numa pasta segura a que apenas o administrador ou o serviço local tenha acesso, por exemplo, *C:\Programas(x86)*
- Instale o Tomcat como um serviço que é executado na conta do serviço local.
- Remova tudo da WebApp, remova as aplicações predefinidas que não pretende.
- Substitua a página de erro predefinida, por ex., 404, 403, 500, etc.
- Execute o HTTPS, ative o SSL.
- A aplicação de gestão deve ser executada no SSL.
- Ficheiro de registo individual do utilizador para cada aplicação da Internet.
- Remova o banner do servidor.
- Ative o registo de acesso.
- Altere a porta e o comando de encerramento.

8.2 PostgreSQL

- Todas as contas com privilégio elevado, tais como as contas pgdba, postgres e depesz, devem apenas poder iniciar sessão localmente.
- Certifique-se de que a sequência está correta no ficheiro pg-hba.conf para que os utilizadores certos consigam aceder
- Configure o ficheiro pg-hba.conf para que o servidor apenas possa apenas ser ligado a partir da máquina local e não através da rede.

8.3 Procedimentos recomendados para a firewall

Eis alguns dos procedimentos recomendados para a firewall durante a utilização da 4Sight2:

8.3.1 Política

1. A configuração da firewall deve estar em conformidade com a política de segurança da empresa.
2. Utilize sempre a política com menos privilégios. Por norma, negue tudo. Permita o fluxo de tráfego específico (utilizando a origem, o destino e a porta)
3. Estabeleça primeiro regras específicas e utilize regras de rejeição explícitas.
4. Registe todas as ações, especialmente as tentativas falhadas de registos de auditoria

8.3.2 Recursos

1. Utilização da memória do monitor
2. Utilização da CPU do monitor
3. Utilização da banda larga do monitor.
4. Limite o número de aplicações em curso na máquina com firewall

8.3.3 Instalação e manutenção

1. Limite o acesso físico à máquina com firewall
2. Utilize uma id exclusiva do utilizador para administração
3. Cumpra rigorosamente a política da conta na máquina
4. Atualize regularmente os sistemas operativos, o software da aplicação, o firmware, etc.
5. Arquive regularmente a base de regulamentos, a configuração e os registos. Documente todos os regulamentos e alterações efetuadas no controlo de uma origem.
6. Efetue testes com regularidade.
7. Remova os regulamentos não utilizados quando o serviço estiver fora de utilização.
8. Realize auditorias e reveja os regulamentos com regularidade.
9. Cumpra os avisos de segurança com regularidade

8.3.4 Segurança adicional

1. Utilize inspeções de estado.
2. Utilize proxys
3. Utilize as opçõess de inspeção e filtragem ao nível da aplicação.

8.3.5 Proteção interna

1. Disponha de uma política de utilização aceitável
2. Firewall pessoal para cada utilizador
3. Prevenção de intrusões baseadas no anfitrião
4. Monitorização da rede
5. Filtragem de conteúdos
6. Controlo do acesso em cada computador e aplicação.

Localização dos escritórios

Sede

Leicester, Reino Unido
Telefone: +44 (0) 116 2317233
E-mail: gb.sensing.sales@bakerhughes.com

Alemanha

Frankfurt
Telefone: +49 (0) 69-22222-973
E-mail: sensing.de.cc@bakerhughes.com

Austrália

Central de Springfield
Telefone: 1300 171 502
E-mail: custcare.au@ge.com

China

Guangzhou
Telefone: +86 173 1081 7703
E-mail: dehou.zhang@bakerhughes.com

China

Pequim
Telefone: +86 180 1929 3751
E-mail: fan.kai@bakerhughes.com

China

Xangai
Telefone +86 135 6492 6586
E-mail: hensen.zhang@bakerhughes.com

EAU

Abu Dhabi
Telefone: +971 528007351
E-mail:
suhel.aboobacker@bakerhughes.com

EUA

Boston
Telefone: 1-800-833-9438
E-mail: custcareboston@bhge.com

França

Toulouse
Telefone: +33 562 888 250
E-mail: sensing.FR.cc@bakerhughes.com

Índia

Bangalore
Telefone: +91 9986024426
E-mail: aneesh.madhav@bakerhughes.com

Itália

Milão
Telefone: +39 02 36 04 28 42
E-mail: csd.italia@bakerhughes.com

Japão

Tóquio
Telefone: +81 3 6890 4538
E-mail: gesitj@bakerhughes.com

Países Baixos

Hoevelaken
Telefone: +31 334678950
E-mail: nl.sensing.sales@bakerhughes.com

Rússia

Moscovo
Telefone: +7 915 3161487
E-mail: aleksey.khamov@bakerhughes.com

Localização dos centros de assistência e suporte

Assistência técnica

Global
E-mail: mstechsupport@bakerhughes.com

Brasil

Campinas
Telefone: +55 11 3958 0098, +55 19 2104 6983
E-mail: mcs.services@bakerhughes.com

China

Changzhou
Telefone: +86 400 818 1099
E-mail: service.mcchina@bakerhughes.com

EAU

Abu Dhabi
Telefone: +971 2 4079381
E-mail: gulfservices@bakerhughes.com

EUA

Billerica
Telefone: +1 (281) 542-3650
E-mail: namservice@bakerhughes.com

França

Toulouse
Telefone: +33 562 888 250
E-mail: sensing.FR.cc@bakerhughes.com

Índia

Pune
Telefone: +91 213 5620426
E-mail:
mcsindia.inhouseservice@bakerhughes.com

Japão

Tóquio
Telefone: +81 3 3531 8711
E-mail: service.druck.jp@bakerhughes.com

Reino Unido

Leicester
Telefone: +44 (0) 116 2317107
E-mail: sensing.grobycc@bakerhughes.com

123M3140 Revisão F | Português

Baker Hughes