Druck

4Sight2

Software de Gerenciamento de Calibração

Manual de Instalação – 123M3140 Revisão F

Índice

1. Introdução

O software de calibração 4Sight2 é uma ferramenta de gerenciamento de calibração baseada na web que ajuda você a manter e controlar seu ambiente de calibração com os mais altos padrões de metrologia. Você pode usar o software para essas tarefas para:

- Gerenciar a calibração de todos os dispositivos de medição para um local de negócio específico
- Estabelecer um cronograma de trabalho de calibração para os técnicos
- Carregar e descarregar dados dos calibradores portáteis Druck (DPI620 Genii, DPI611 e DPI612) que possuem uma função de comunicação USB
- Gerenciar os registros de calibração para dispositivos que não possuem um calibrador portátil (Entrada Manual de Dados)
- Inspecionar seus registros do histórico de calibração. Você também pode criar um registro permanente para cada certificado de calibração. Por exemplo: Para procedimentos de controle de qualidade ISO 9000.
- Controlar calibrações automatizadas utilizando Controladores de Pressão Druck (PACE 1000, 5000 e 6000), Calibradores Portáteis (DPI620 Genii, DPI611 e DPI612) e 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. Após a instalação inicial do 4Sight2, somente uma conta administrativa estará disponível. A partir desta conta, novos Usuários podem ser criados, e Grupos/Conjuntos de Permissão podem ser atribuídos. Os usuários administrativos têm acesso de leitura e escrita a todas as funcionalidades do 4Sight2.

1.1.2 Supervisor

O supervisor é responsável pela gestão de ativos e calibração. Eles têm a capacidade de criar e atualizar ativos dentro do 4Sight2 Enterprise, incluindo Fábricas, Localizações, Marcadores e Dispositivos. Eles são responsáveis por vincular documentos a ativos, como processos da fábrica e planilhas de dados de dispositivos. Os supervisores podem criar procedimentos de teste para serem utilizados durante a calibração, bem como agendar procedimentos e monitorar o estado dos dispositivos. Os supervisores dispõem das permissões necessárias para aprovar as calibrações.

1.1.3 Técnicos

Os técnicos são responsáveis por executar as calibrações. As calibrações podem ser Portáteis, Manuais ou Automatizadas, e é atribuição do técnico executar o tipo de calibração relevante em um dispositivo. Uma vez realizada a calibração, os técnicos podem rever os resultados e completar as calibrações para depois serem aprovados por um supervisor.

1.1.4 Auditor

Um auditor é responsável por inspecionar os relatórios. Em algumas fábricas, a realização de auditorias pode ser obrigatória e ser considerada uma exigência regulatória.

Copyright 2020. Druck Ltd, a Baker Hughes business

2. Requisitos de Sistema

Os requisitos mínimos de sistema para instalar o aplicativo 4Sight2 em máquinas Servidor e Cliente estão listados abaixo:

2.1 Servidor de Aplicações

Sistema Operacional	Windows 10, Windows Server 2012 R2, Windows Server 2016, Windows Server 2019
Atualizações	Todas as Atualizações do Windows foram instaladas
Processador	Quad Core
RAM	8 GB ou mais (recomenda-se 32 GB)
Espaço em disco	1 TB
Velocidade da rede	10 Mbps

2.2 Estação de Trabalho do Cliente

Sistema Operacional	Windows 10, Windows Server 2012 R2, Windows Server 2016, Windows Server 2019
Navegador	Google Chrome V80+, Microsoft Edge V80, Firefox V74
Adobe Reader	Adobe Acrobat Reader DC Versão 2015.017.20050 +
RAM	8GB ou mais
Processador	Dual Core
Espaço em disco	600 GB
Velocidade da rede	10 Mbps

2.3 Instalação Local

Sistema Operacional	Windows 10, Windows Server 2012 R2, Windows Server 2016, Windows Server 2019
Atualizações	Todas as Atualizações do Windows foram instaladas
Adobe Reader	Adobe Acrobat Reader DC Versão 2015.017.20050 +
Processador	Dual Core
RAM	16 GB ou mais (recomenda-se 32 GB)
Espaço em disco	500 Gb ou mais espaço em disco
Navegador	Google Chrome V80+, Microsoft Edge V80, Firefox V74

Copyright 2020. Druck Ltd, a Baker Hughes business

2.4 Firmware compatível com 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.

Copyright 2020. Druck Ltd, a Baker Hughes business

Instalação do 4Sight2

Copyright 2020. Druck Ltd, a Baker Hughes business

3. Instalação do 4Sight2

Para instalar o 4Sight2 primeiro, copie o zip do 4Sight2 Setup na sua área de trabalho e extraia os arquivos do zip. No arquivo de configuração, selecione o executável 4Sight2.

Observação: Os seguintes softwares antivírus são usados para a verificação das instalações do 4Sight2 e do Servidor de Comunicação,

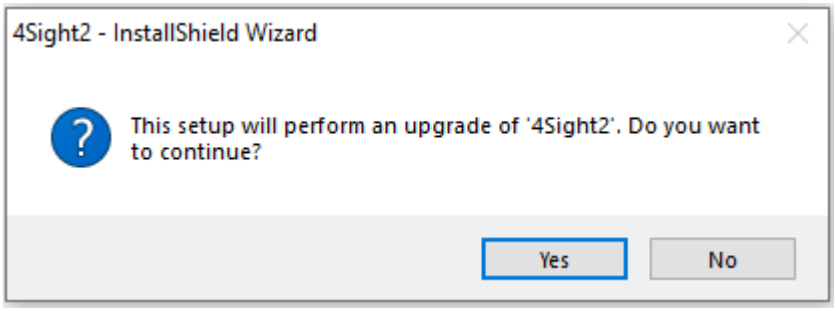
- McAfee VirusScan Enterprise + AntiSpyware Enterprise Número de versão: 8.8.0
- Symantec Endpoint Protection Número de versão: 14.3.558

Depois que você executar o executável de instalação, o Assistente InstallShield será iniciado. O assistente InstallShield possui duas etapas de instalação do 4Sight2:

1. Instalação de Banco de Dados
2. Instalação de Aplicativo da Web

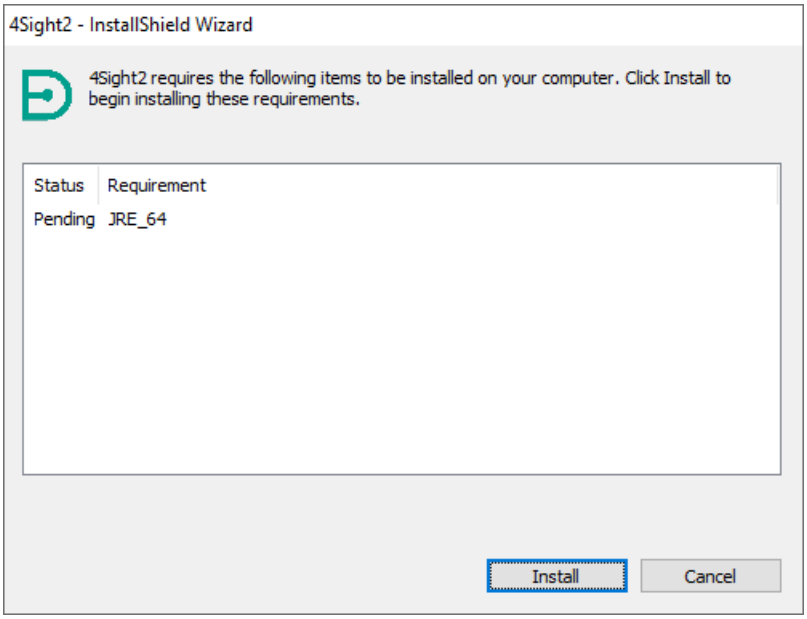
Siga as instruções do Assistente InstallShield ou use as duas seções a seguir para executar o processo de instalação.

1. Se o 4Sight2 já estiver instalado na máquina, o assistente de instalação vai solicitar que você execute uma atualização para uma versão recente. Clique em **Yes** (Sim) para aplicar a atualização recente.

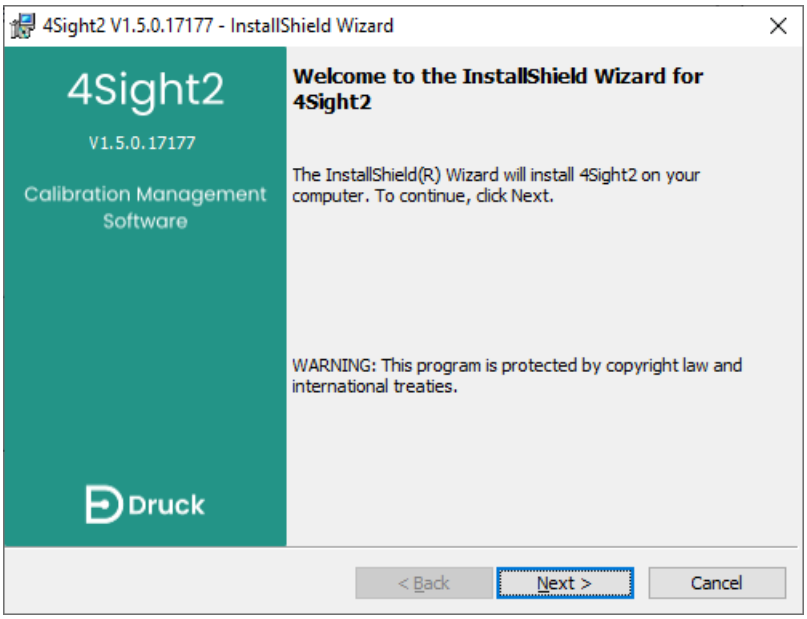


2. Se o 4Sight2 for instalado pela primeira vez na máquina, o assistente de instalação exibirá a tela abaixo. Selecione **Install** (Instalar) e os itens listados exibidos serão instalados.

Copyright 2020. Druck Ltd, a Baker Hughes business



3. Uma vez concluída a instalação de qualquer pré-requisito, será exibida a tela de boas-vindas do Assistente InstallShield. Clique em **Next** (Avançar) para continuar.



3.1 Instalação de Banco de Dados

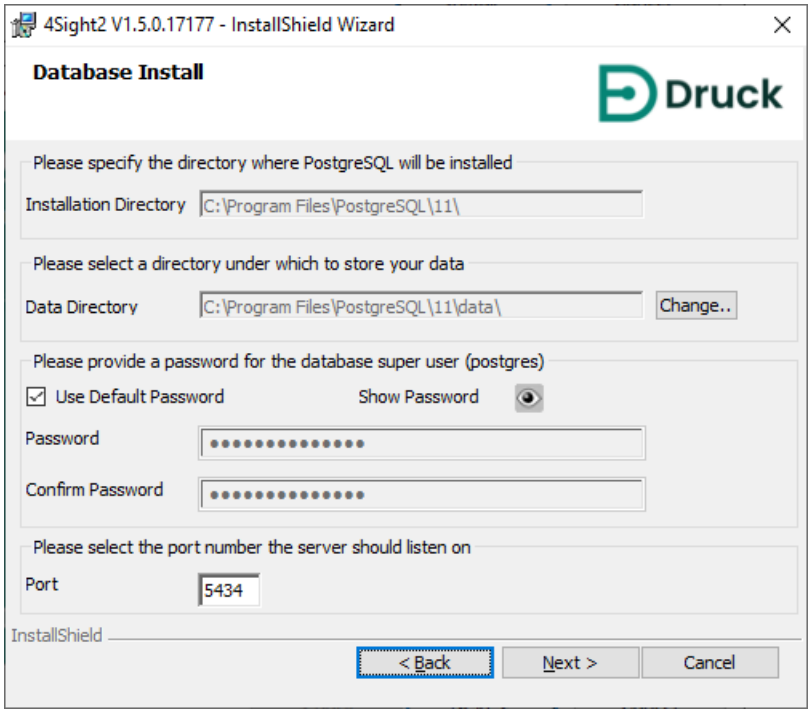
O aplicativo 4Sight2 utiliza um banco de dados PostgreSQL. A seguir são dadas instruções sobre como instalar o banco de dados PostgreSQL e o que fazer se um banco de dados PostgreSQL já estiver instalado.

Copyright 2020. Druck Ltd, a Baker Hughes business

3.2 Instalação do PostgreSQL

Siga este procedimento se um banco de dados PostgreSQL não estiver instalado na máquina.

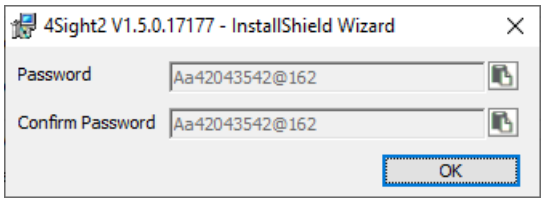
1. Se não houver nenhuma instância do banco de dados PostgreSQL instalada na máquina, o assistente de instalação exibirá a tela abaixo.



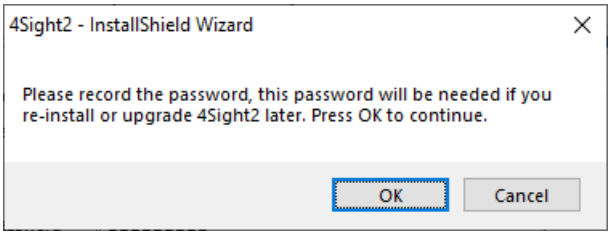
Installation Directory (Diretório de Instalação): Selecione o diretório onde o aplicativo PostgreSQL pode ser instalado.
Data Directory (Diretório de Dados): Selecione o diretório onde o banco de dados PostgreSQL pode ser instalado.
Password/ Confirm Password (Senha /Confirmar senha): Insira a senha de superusuário do banco de dados PostgreSQL. Isso só é necessário se o banco de dados PostgreSQL estiver sendo instalado pela primeira vez.
Observação: Esta senha será necessária para acessar o conteúdo do banco de dados após a instalação.
Port (Porta): Este é o endereço da porta do banco de dados do PostgreSQL para atender à solicitação do aplicativo.
Observação: Se o número da porta já estiver ocupado, entre em contato com a equipe de TI. O usuário também pode alterar o número da porta, que precisa ser anotado para lançar o aplicativo posteriormente.

Importante: O usuário deve anotar a senha do banco de dados. A perda de informação de senha pode resultar em negação de acesso ou perda de dados. Desmarque a caixa de seleção User Default Password (Senha Padrão do Usuário) para atualizar a senha do super usuário do banco de dados. Se você quiser manter a senha padrão ou visualizar a nova senha digitada, selecione o ícone Show Password (Mostrar Senha). Para copiar a senha para a área de transferência, use o ícone (Copiar para Área de Transferência).

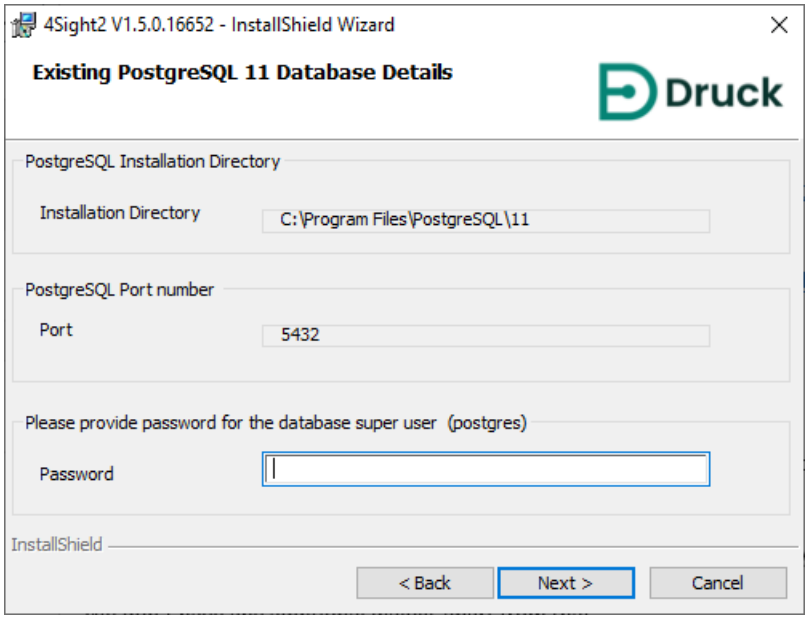
Copyright 2020. Druck Ltd, a Baker Hughes business



Você será então solicitado a registrar a senha novamente pelo instalador. Selecione **OK** depois de ter feito uma anotação da senha.



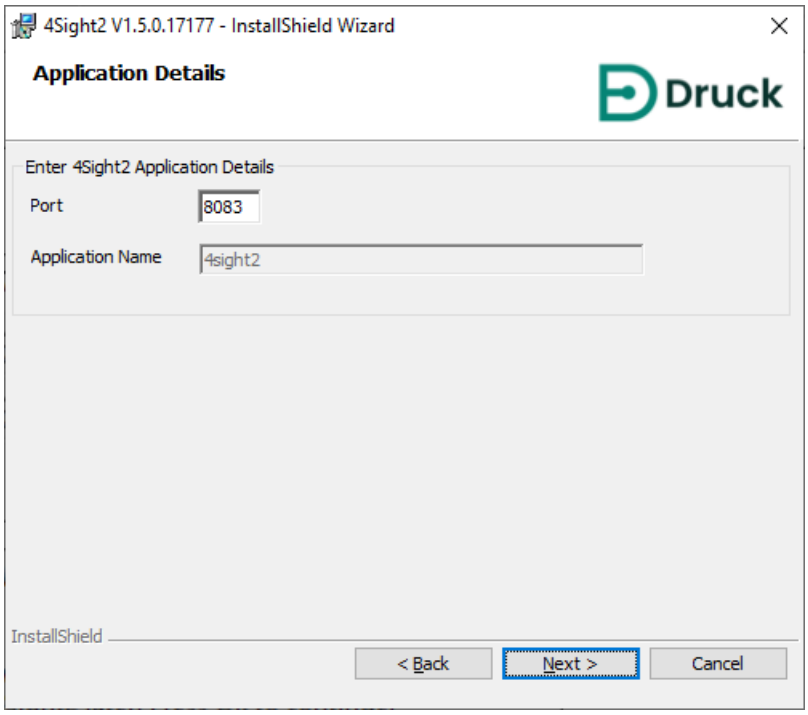
2. Este Passo será mostrado ao usuário somente no caso do banco de dados PostgreSQL já estar instalado.



Installation Directory (Diretório de Instalação): O objetivo é especificar o caminho onde o PostgreSQL já está instalado. É uma informação de leitura somente.
Password (Senha): Esta opção é para confirmar a senha do super usuário do banco de dados PostgreSQL.
Port (Porta): Esta opção é para especificar o número da porta que o banco de dados PostgreSQL está usando para executar a requisição db.

Copyright 2020. Druck Ltd, a Baker Hughes business

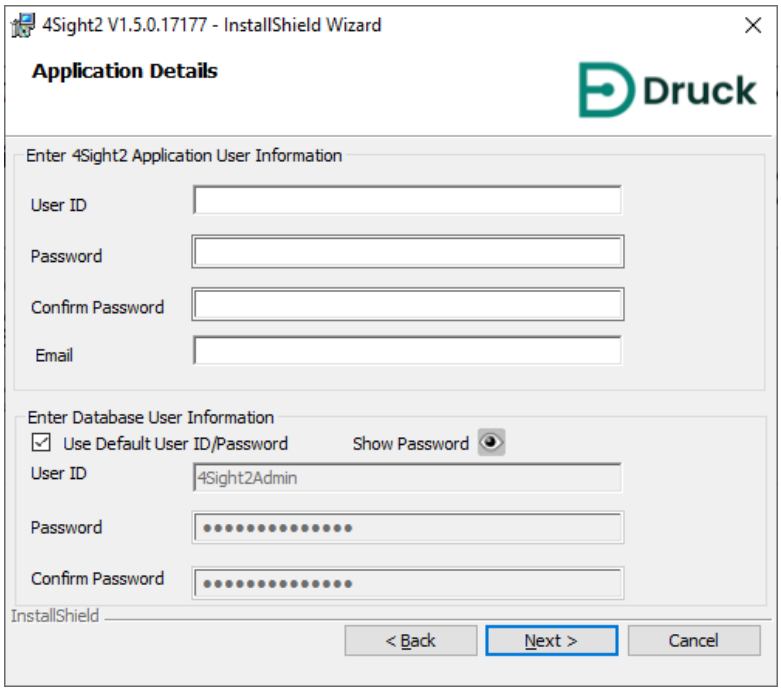
3. Na janela Application Details (Detalhes do Aplicativo), insira os detalhes abaixo.



Port (Porta): Entre na porta do servidor web Tomcat que é utilizada pelo aplicativo da web 4Sight2 para responder a uma solicitação HTTP.
Application Name (Nome do Aplicativo): Digite o caminho de contexto do aplicativo que você usará para se conectar ao aplicativo 4Sight2 no seu navegador. Por padrão, é o 4sight2.
Observação: Se o número da porta já estiver ocupado, entre em contato com a equipe de TI. O usuário também pode alterar o número da porta, que precisa ser anotado para lançar o aplicativo posteriormente.

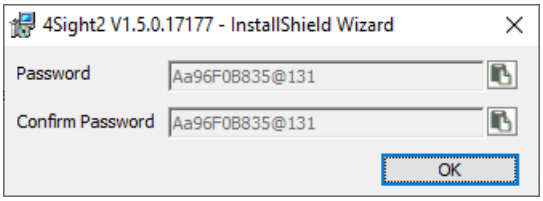
Copyright 2020. Druck Ltd, a Baker Hughes business

4. Selecione **Next** (Avançar) e será exibida a tela Application User Information (Informações do Usuário do Aplicativo).



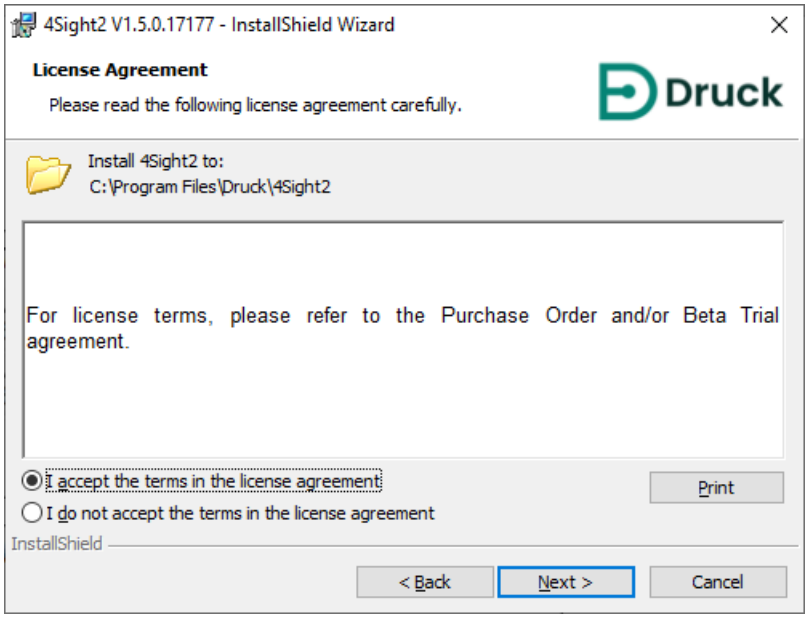
Application User Information (Informações de usuário do aplicativo): Esta seção é para inserir o nome e a senha do super usuário para acessar o aplicativo 4Sight2.
Observação: Esta senha será necessária para acessar o aplicativo 4Sight2 após a instalação.
Database User Information (Informações de usuário do banco de dados): Esta seção é para inserir o nome e a senha do usuário do banco de dados que será utilizado pelo aplicativo 4Sight2 para se comunicar com o banco de dados PostgreSQL.

Importante: O usuário deve anotar a senha do banco de dados. A perda de informação de senha pode resultar em negação de acesso ou perda de dados. Desmarque a caixa de seleção User Default Password (Senha Padrão do Usuário) para atualizar a senha do super usuário do banco de dados. Se você quiser manter a senha padrão ou visualizar a nova senha digitada, selecione o ícone Show Password (Mostrar Senha). Para copiar a senha para a área de transferência, use o ícone (Copiar para Área de Transferência).

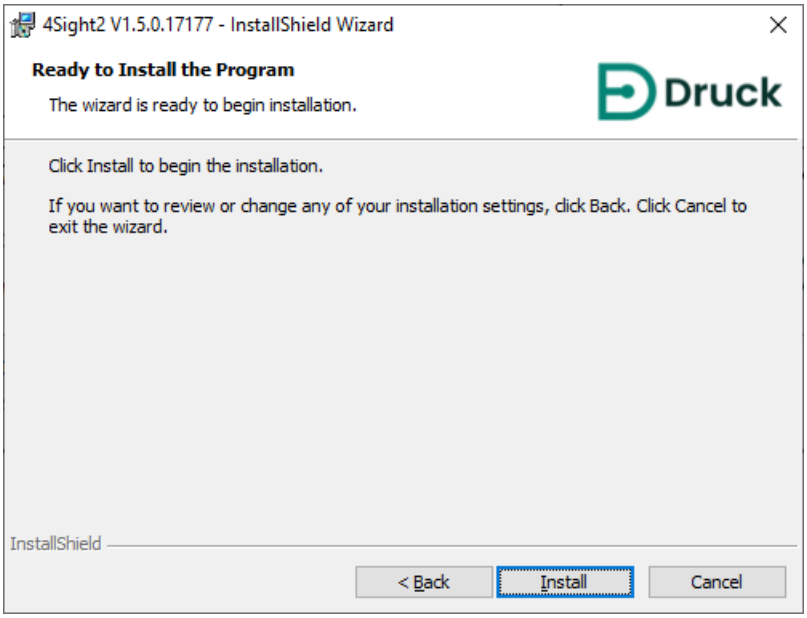


Copyright 2020. Druck Ltd, a Baker Hughes business

5. Após a leitura dos termos e condições da licença, selecione o botão "I agree to the License terms and conditions" (Eu concordo com os termos e condições) e depois clique em **Next** (Avançar).



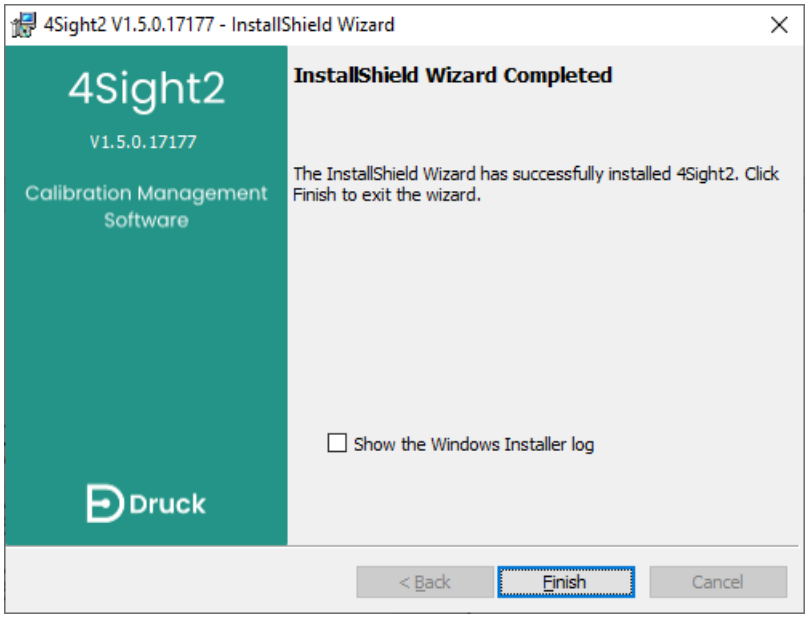
6. Clique em **Install** (Instalar) para iniciar a instalação. Todos os pacotes de software relacionados com o aplicativo 4Sight2 e o banco de dados serão instalados.



Copyright 2020. Druck Ltd, a Baker Hughes business

Parabéns, o aplicativo 4Sight2 foi agora configurado.

7. Clique no botão **Finish** (Concluir) para fechar a janela e seguir as instruções na próxima seção para fazer o login no aplicativo 4Sight2.



Para fazer o login o 4Sight2 no servidor local, acesse

http://NomeComputador ou EndereçoIP:NúmeroPorta/NomeAplicativo

- **NomeComputador –** O nome do PC onde o aplicativo 4Sight2 foi instalado. Ele pode ser localizado clicando-se com o botão direito do mouse sobre este PC e selecionando propriedades.
- **EndereçoIP –** O endereço IP do PC onde o aplicativo 4Sight2 foi instalado. Ele pode ser localizado executando 'ipconfig' em uma janela de comando do Windows.
- **NúmeroPorta –** O número que foi inserido no campo Tomcat Port Number (Número da Porta Tomcat) durante a instalação do aplicativo.
- **NomeAplicativo –** O nome que foi inserido no campo Application Name (Nome do Aplicativo) durante a instalação da aplicação.

Copyright 2020. Druck Ltd, a Baker Hughes business

Instalação do Comunicador de Equipamentos de Testes 4Sight2

Copyright 2020. Druck Ltd, a Baker Hughes business

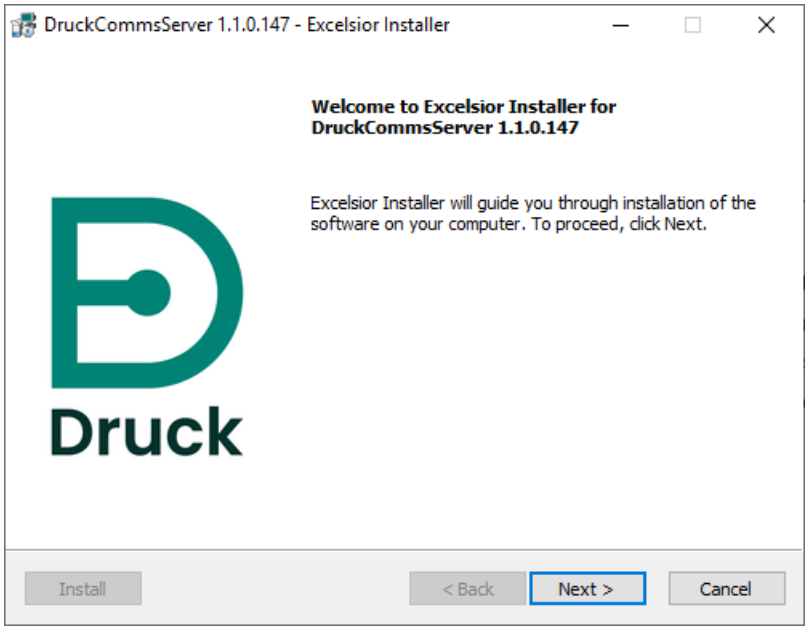
4. Instalação do Comunicador de Equipamentos de Testes 4Sight2

1. O Comunicador de Equipamentos de Teste fornece os meios para que seus instrumentos Druck se comuniquem com o aplicativo 4Sight2. O Comunicador do Equipamento de Teste pode ser instalado a partir da pasta de configuração do 4Sight2 ou pode ser baixado através da comunicação inicial do dispositivo 4Sight2. Se o Comunicador do Equipamento de Teste não estiver disponível no arquivo de configuração, uma vez que o aplicativo 4Sight2 esteja em execução e um intervalo tenha sido criado, navegue para Calibration (Calibração) > Portable (Portátil) usando o menu 4Sight2 como usuário administrativo, veja o Manual do Usuário do 4Sight2 para ajuda de navegação e criação de intervalo. Selecione o botão Refresh (Atualizar) ao lado do dropdown do equipamento de teste. Se o Comunicador do Equipamento de Teste não estiver funcionando, você verá a seguinte mensagem:

   Não foi possível estabelecer comunicação com o Equipamento de Teste

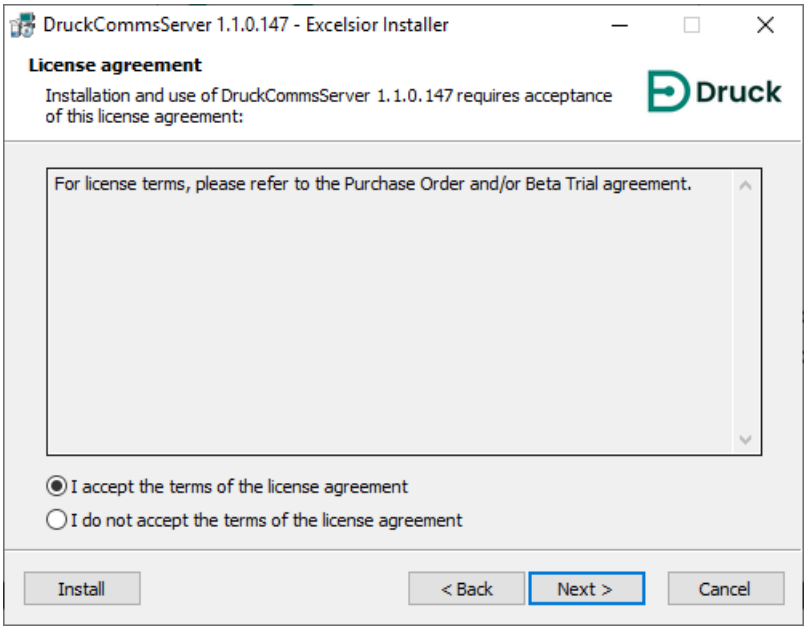
   Baixe o pacote do Comunicador do Equipamento de Teste. Após o download, descompacte e execute o setup.exe para instalar. Para instruções de instalação ou solução de problemas, consulte o Manual de Instalação. Entre em contato com o Administrador se precisar de assistência.

2. Selecione **Download** para obter o arquivo de configuração do Comunicador de Equipamento de Testes.
3. Os arquivos de configuração do Comunicador de Equipamento de Testes aparecerão como um CommsServerInstall.zip. Depois que o Comms Server Zip tiver baixado, os mesmos passos podem ser seguidos antes e depois da instalação do 4Sight2.
4. Extraia os arquivos do arquivo Zip do Comms Server e clique duas vezes no arquivo setup.exe para executar o instalador.
5. O instalador do DruckCommsServer será exibido. Siga as instruções no instalador ou siga este guia.

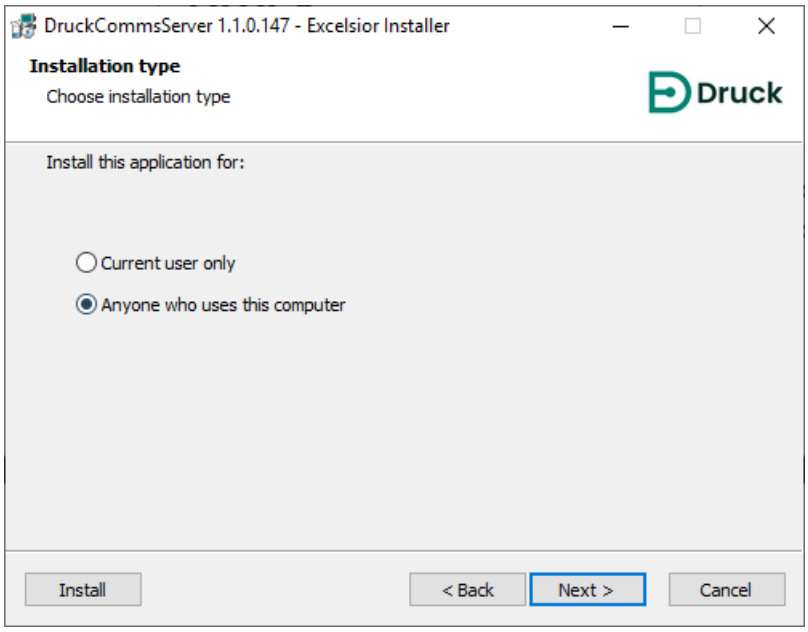


Copyright 2020. Druck Ltd, a Baker Hughes business

6. Selecione **Next** (Avançar) para continuar e exibir a tela de contrato de licença, leia os termos e selecione **I accept the terms of the license agreement**, (Eu aceito os termos do contrato de licença), depois clique em **Next** (Avançar) para continuar.

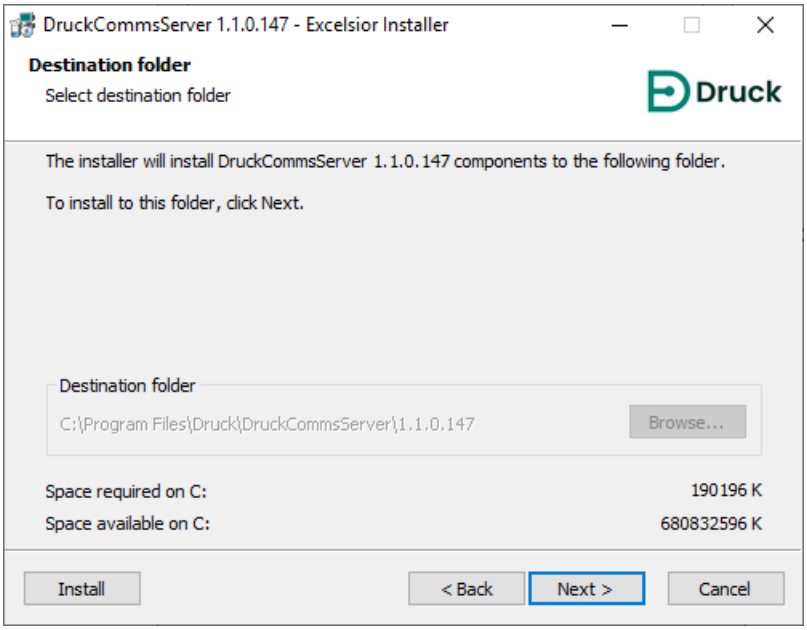


7. Na tela de tipo de Instalação, selecione se você deseja instalar o CommsServer para todos os usuários deste PC ou apenas para o usuário atual.

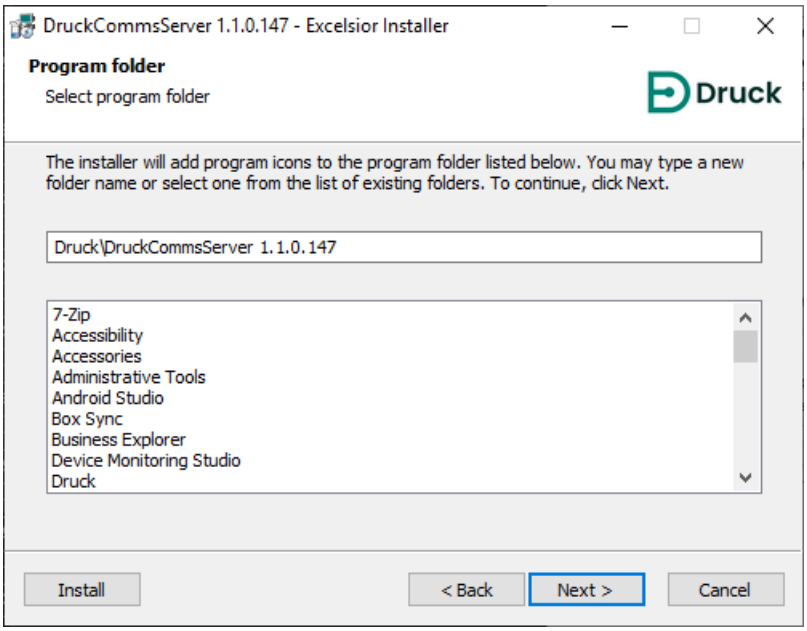


Copyright 2020. Druck Ltd, a Baker Hughes business

8. A tela da pasta Destino exibe a pasta em que o DruckCommsServer será instalado. Por padrão, é C:\Arquivos de Programas\Druck\DruckCommsServer\[versão_do_aplicativo]

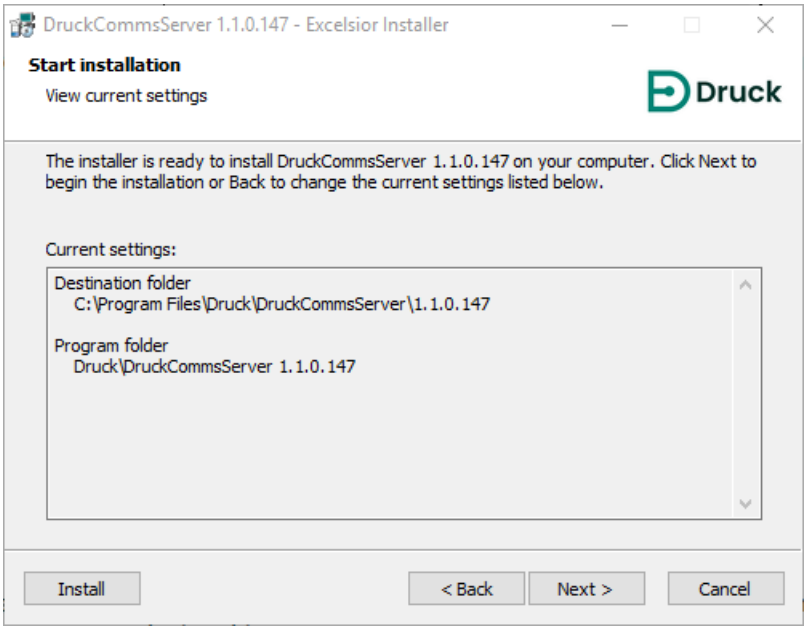


9. A tela Pasta de Programas permite que você selecione onde o instalador adiciona o ícone do programa à pasta do programa.

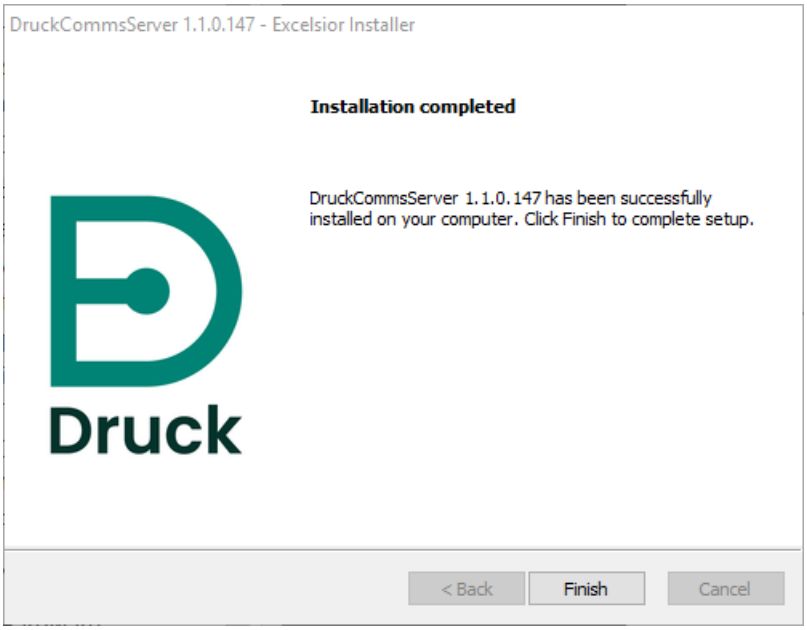


Copyright 2020. Druck Ltd, a Baker Hughes business

10. A tela de instalação inicial será exibida, selecione **Next** (Avançar) para iniciar a instalação.

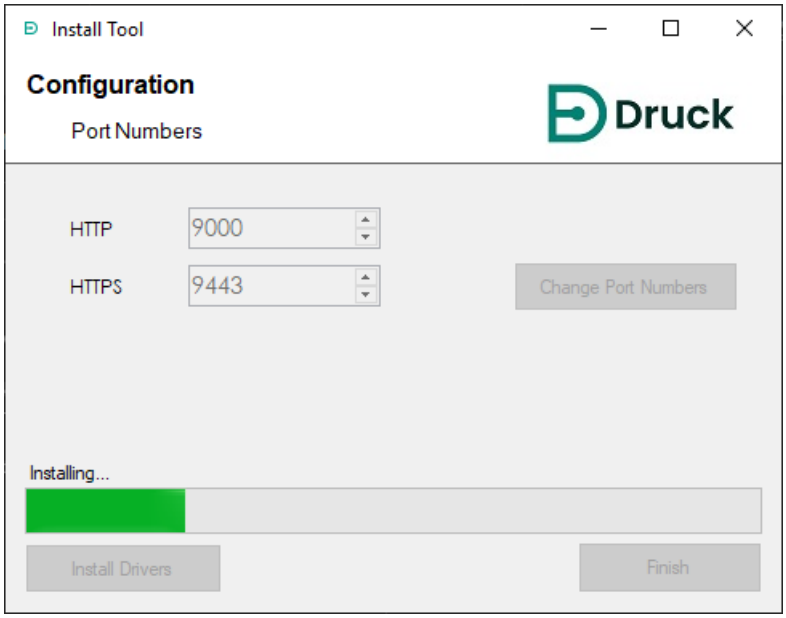


11. Depois que a Instalação for concluída, selecione **Finish** (Concluir).



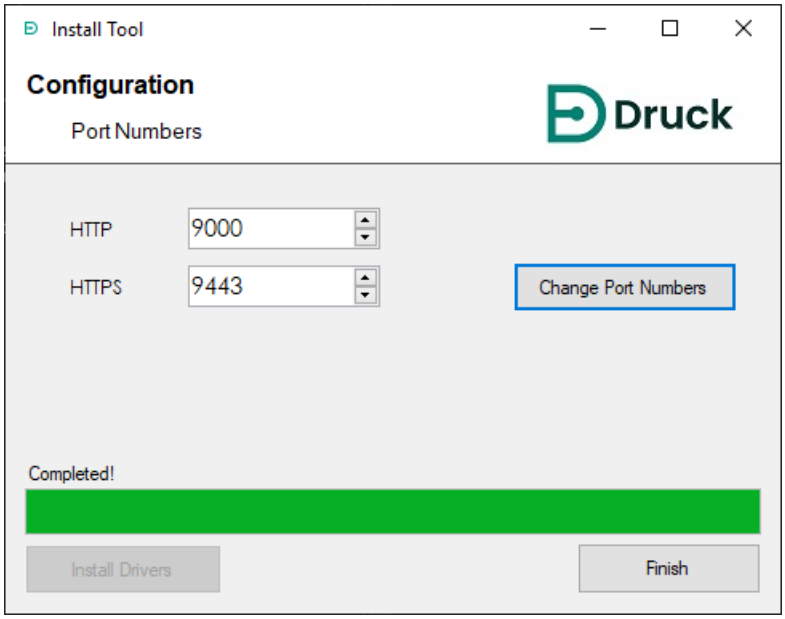
Copyright 2020. Druck Ltd, a Baker Hughes business

12. Em seguida, a ferramenta de instalação do CommsServer será exibida para instalar os drivers adicionais que foram necessários.



13. Se não tiver certeza se o número da porta alternativa está sendo usado pela 4Sight2, entre em contato com o seu usuário administrativo

Observação: A ferramenta de instalação pode ser executada separadamente após a instalação para reconfigurar estes números de porta.

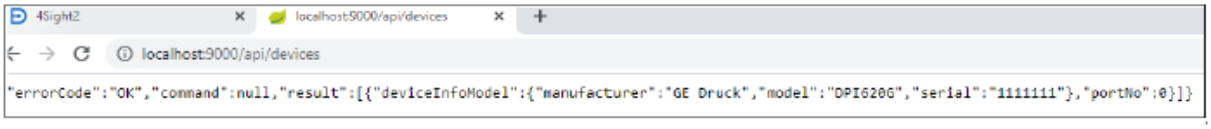


14. Teste a instalação do Comunicador do Equipamento de Teste, digitando a seguinte URL no seu navegador da Web:

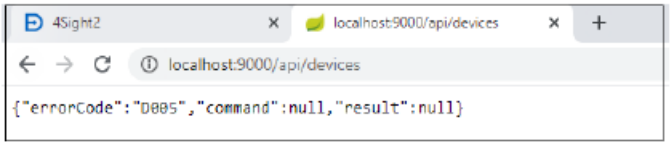
    http:/localhost:[http número de porta usado acima do padrão 9000]/api/devices

Copyright 2020. Druck Ltd, a Baker Hughes business

O navegador na web deve exibir a lista de qualquer dispositivo que você tenha conectado:



Se nenhum dispositivo estiver conectado, você deve ver o seguinte



Observação: Os drivers exigidos para calibradores de temperatura não serão configurados automaticamente. Veja a seção 4.3 Configuração do Driver do Calibrador de Temperatura

15. Se a instalação do driver do dispositivo não for bem sucedida, use os passos na próxima seção para configurar manualmente os drivers necessários.

4.1 Configuração Manual do Driver

As configurações da política de segurança de TI podem impedir que os drivers Druck se configurem automaticamente na instalação. Isso será aparente se o 4Sight2 não conseguir se comunicar com os seguintes 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 drivers Druck podem ser configurados manualmente. Consulte seu representante local de TI se você não tiver certeza sobre isso ou se precisar de mais assistência.

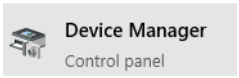
4.1.1 Pré-requisitos

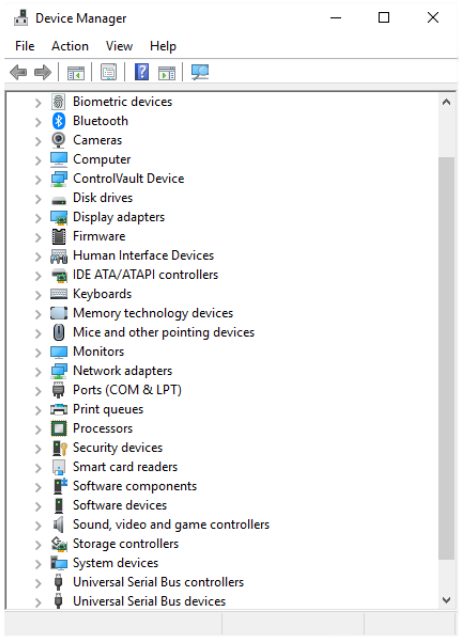
Para instalar os drivers, você precisa do aplicativo 4Sight2 instalado ou acessível na/da máquina. Certifique-se de que você possa fazer login no aplicativo 4Sight2 a partir do computador antes de tentar instalar drivers.

Copyright 2020. Druck Ltd, a Baker Hughes business

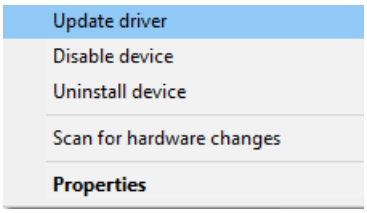
Para instalar o driver manualmente, complete as seguintes etapas:

1. No Desktop, procure pelo Gerenciador de Dispositivos e execute.



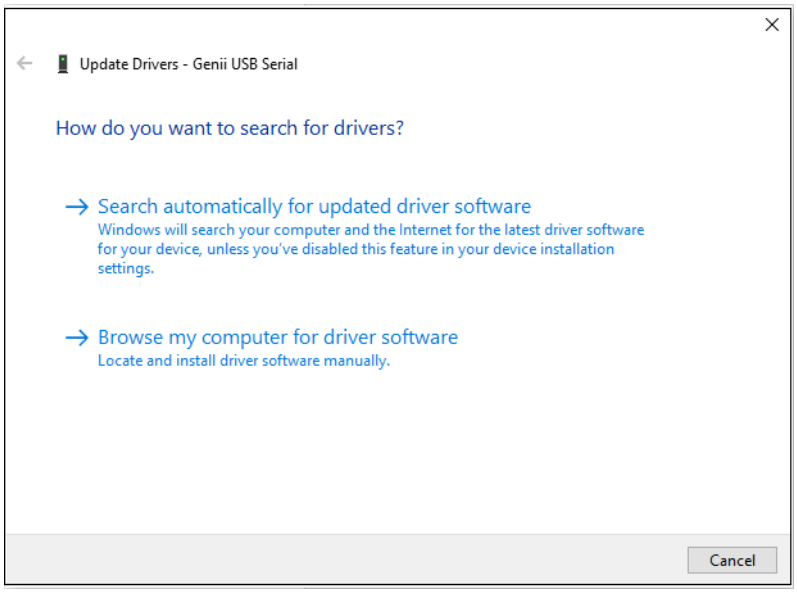


2. Percorra a lista de dispositivos USB para encontrar os dispositivos que não estão configurados (Dispositivo Desconhecido ou Outros dispositivos). Clique com o botão direito e selecione **Update Driver** (Atualizar driver).

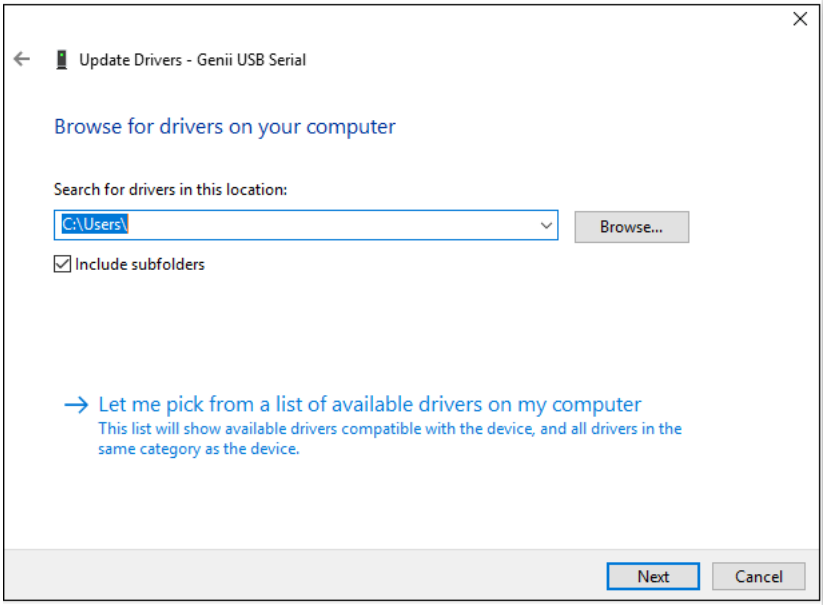


Copyright 2020. Druck Ltd, a Baker Hughes business

3. Selecione **Browse my computer for driver software** (Navegar meu computador para software de drivers).

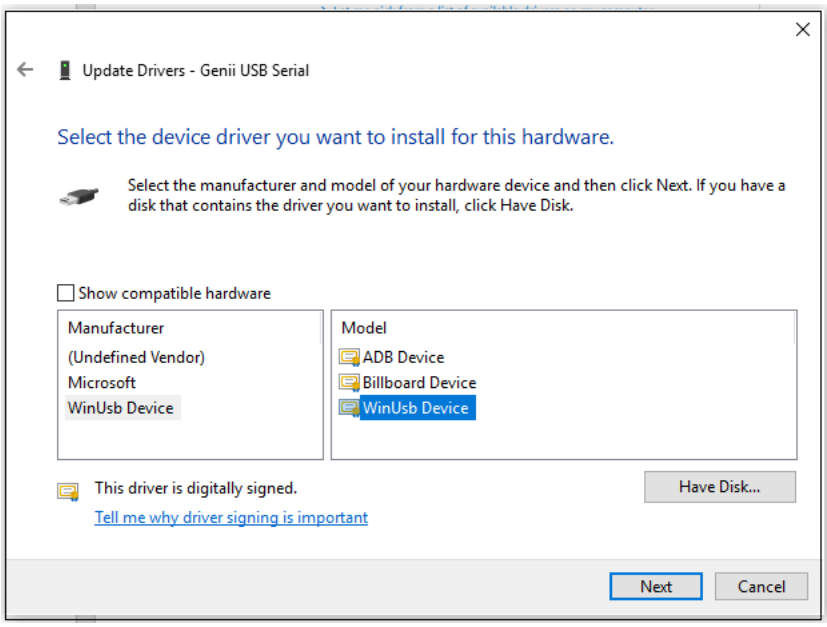


4. Selecione **Let me pick from a list of available drivers** (Permitir escolher de uma lista de drivers disponíveis) no meu computador.

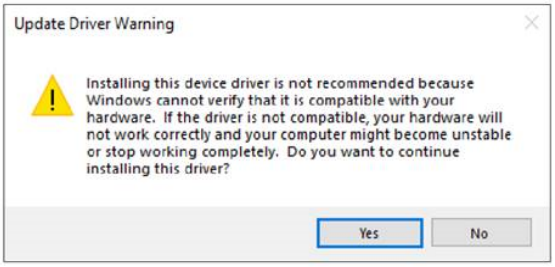


Copyright 2020. Druck Ltd, a Baker Hughes business

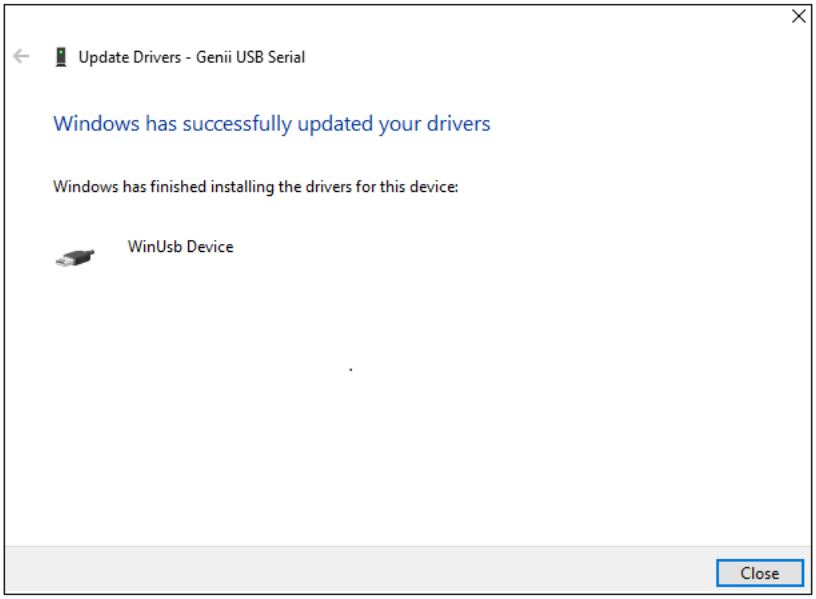
5. Cancele a seleção **Show compatible hardware** (Mostrar hardware compatível) e selecione **WinUsb Device** (Dispositivo WinUsb) para Manufatura e o **WinUsb Device** para Modelo.



6. A Advertência a seguir será exibida. Clique em **Yes** (Sim).



7. Será exibida a mensagem de que o Windows atualizou com sucesso seus drivers.



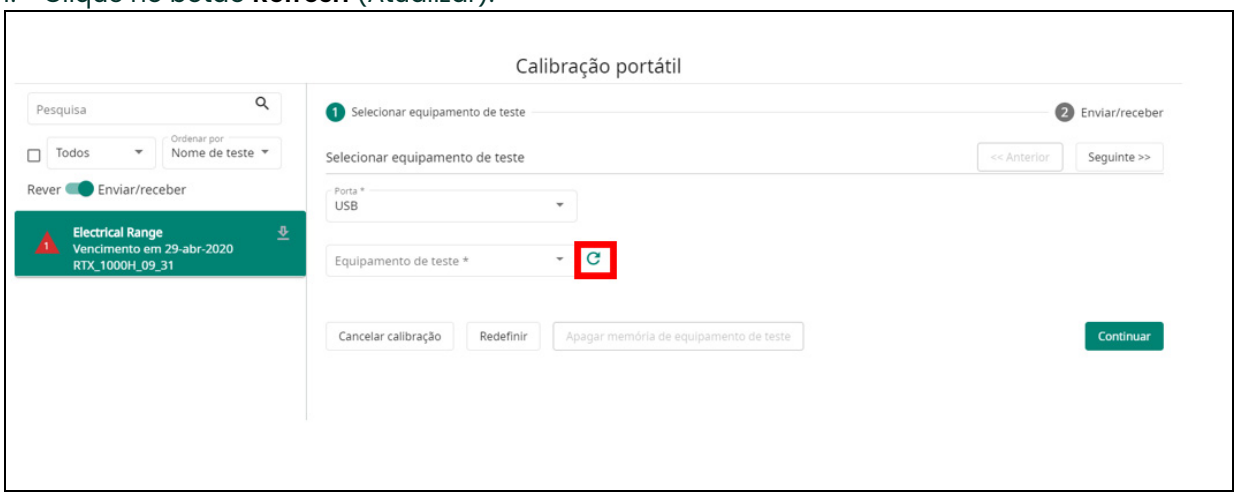
Copyright 2020. Druck Ltd, a Baker Hughes business

Repita os passos acima para cada categoria de dispositivo quando conectar o dispositivo pela primeira vez.

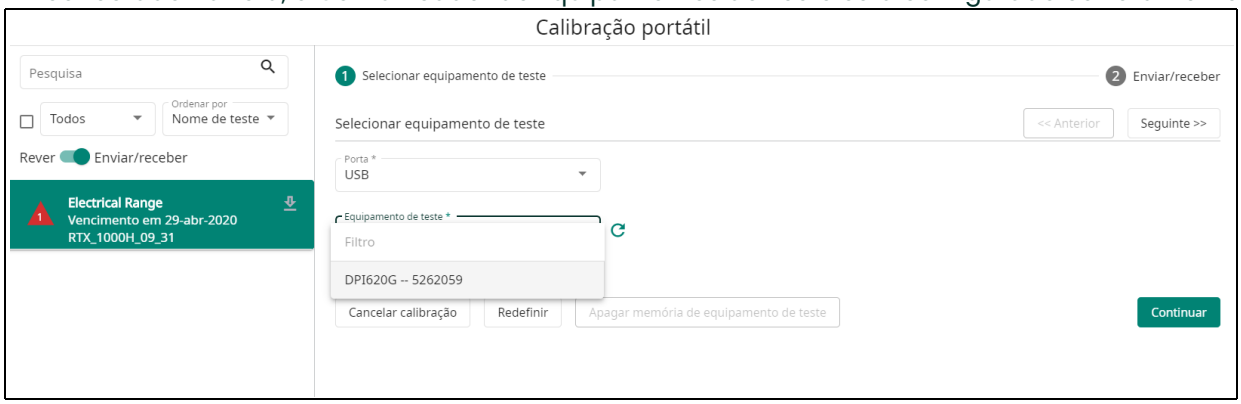
Por exemplo, se conectar um PACE e Genii pela primeira vez, você pode ter que repetir os passos acima para PACE e Genii separadamente na primeira vez. Todas as demais instâncias de todos os PACEs e Geniis devem funcionar sem a necessidade de realizar essas configurações. Entretanto, se você conectar uma categoria diferente de dispositivo posteriormente, como um DPI611/612, você precisará repetir os passos para esta categoria de dispositivo.

4.2 Testar o Comunicador de Equipamento de Teste

1. Faça o login no 4Sight2 como Técnico.
2. Vá para **Assets >> Worklist** (Ativos >> Lista de trabalho).
3. Selecione uma ou mais faixas e atribua ao fluxo de trabalho de calibração Portátil ou Automática.
4. Clique no botão **Refresh** (Atualizar).



5. Clique na lista suspensa **Test Equipment** (Testar Equipamento). Se você vir o dispositivo conectado na lista, o Comunicador de Equipamentos de Teste está configurado corretamente.



Copyright 2020. Druck Ltd, a Baker Hughes business

4.3 Configuração do Driver do Calibrador de Temperatura

Para que o Calibrador de Temperatura possa se comunicar com o 4Sight2, é preciso instalar um driver FTDI.

1. Baixe o driver FTDI usando este link: https://www.ftdichip.com/Drivers/VCP.htm.
2. Extraia o arquivo baixado do zip e salve em um local conhecido na sua máquina.
3. Navegue pelo Gerenciador de Dispositivos do Windows da sua máquina.
4. Selecione as Portas (COM e LPT) da lista de dispositivos, para visualizar o calibrador de temperatura.
5. Clique com o botão direito do mouse no calibrador de temperatura e selecione os drivers de atualização.
6. Selecione Browse my computer for driver software (Navegar meu computador para software de drivers).
7. Selecione Browse (Procurar) ao lado da caixa Search (Busca) para drivers neste local.
8. Selecione a pasta extraída da pasta contendo o download do driver.
9. Selecione Next (Avançar) e depois feche.
10. O driver não será instalado.
11. Para testar a comunicação com um calibrador de temperatura no 4Sight2, navegue pela calibração automática e verifique se o calibrador de temperatura pode ser selecionado como um Controlador de Entrada. Também é possível executar novamente o Passo 14 a partir da seção 4.

Copyright 2020. Druck Ltd, a Baker Hughes business

Guia de Implementação

Copyright 2020. Druck Ltd, a Baker Hughes business

5. Guia de Implementação

5.1 Arquitetura de Implementação

A arquitetura típica inclui o aplicativo da web 4Sight2 e o servidor UAA (Autenticação e Autorização de Usuário) operando no Servidor da Web Tomcat, com o banco de dados PostgreSQL executando na mesma máquina.

O Aplicativo Cliente do Navegador se conectará ao servidor 4Sight2 que, por sua vez, armazena e recupera as informações do banco de dados do PostgreSQL.

5.2 Implementação Física

Consideramos que o usuário que instala o 4Sight2 já implementou as Medidas Cibernéticas de Segurança em conformidade com as políticas de segurança do usuário, incluindo o seguinte:

- O servidor está em um local seguro com controle de acesso físico limitado.
- O controle de acesso ao servidor é protegido com autorização limitada de acesso.
- A rede do servidor é protegida com o firewall para permitir acesso limitado às aplicações conhecidas apenas em portas conhecidas.
- Os aplicativos são executados em seu próprio contexto e têm acesso a bancos de dados e sistemas de arquivos apenas na sua própria pasta.

5.3 Rede

Os clientes são conectados utilizando navegadores da Web, seja através de conexões Ethernet ou de uma rede sem fio. Pode haver latência na rede sem fio, dependendo da largura de banda e do número de dispositivos conectados.

É aconselhável desativar ou remover todos os plugins e extensões instalados no navegador.

O servidor da web do 4Sight2 não deve ser exposto à Internet, todo acesso necessário deve ser fornecido via Intranet ou VPN.

5.4 Sequência de Implementação

PostgreSQL, Tomcat e Java Runtime são pré-requisitos para o aplicativo 4Sight2. O PostgreSQL é instalado como um pacote separado enquanto outros são agrupados com o aplicativo. Se o PostgreSQL já estiver instalado na máquina do usuário, só precisamos da senha do Superusuário para conectá-lo e configurá-lo.

A instalação requer direitos de administrador do Windows na máquina. Antes da instalação, o usuário deve ter a senha de superusuário do PostgreSQL. O nome de usuário e a senha do administrador do aplicativo e o nome de usuário e a senha do banco de dados.

Para criar o banco de dados e outras estruturas dentro do servidor PostgreSQL, é necessário ter a senha de superusuário do PostgreSQL. O administrador do aplicativo é o primeiro usuário desse aplicativo. Eles são responsáveis por criar outros usuários e atribuir diferentes papéis. O usuário do Banco de Dados tem acesso ao banco de dados 4Sight2 e UAA. Essas credenciais de nome de usuário são usadas para acessar o banco de dados.

O aplicativo é publicado em uma porta da máquina. A porta padrão é 8083, e o usuário pode alterar a porta no momento da instalação ou posteriormente. O contexto de aplicativo padrão no Tomcat é o 4Sight2.

Copyright 2020. Druck Ltd, a Baker Hughes business

Siga o procedimento de fortalecimento do Sistema Operacional de acordo com as diretrizes da Microsoft ou CIS para endurecer o SO. O procedimento de instalação orientará o usuário a instalar o PostgreSQL antes de instalar o servidor 4Sight2.

O Comunicador de Equipamentos de Teste é instalado nas máquinas do cliente quando o equipamento de teste é conectado através de portas USB. Se o Comunicador de Equipamentos de Teste ainda não estiver instalado na máquina, o usuário é solicitado a baixá-lo do servidor 4Sight2 e instalá-lo na máquina. O comunicador do equipamento de teste ouve a porta 9000 e só pode se comunicar na camada segura.

5.5 Tarefas de Pós-Implementação

5.5.1 Adicionando Usuário e Grupos

O administrador é responsável por criar diferentes usuários como Supervisor, Técnico Sênior, Técnico e Auditor na aplicação. O administrador pode atribuí-los a diferentes grupos padrão incorporados. Se for necessário maior controle ou granularidade de acesso, o administrador pode criar grupos personalizados e atribuir um acesso específico a eles.

5.5.2 Senhas Padrão

Estamos usando a senha padrão codificada para o usuário do tomcat no arquivo "C:\Arquivos de Programas\Druck\4Sight2\<<latest folder number>>\apache-tomcatconf\tomcat-user.xml".

É recomendável alterar a senha padrão e usar sempre uma senha que siga as melhores práticas de senha.

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

As melhores práticas foram implementadas para garantir que este aplicativo seja seguro. Para obter segurança adicional, execute as seguintes tarefas:-

Os arquivos e pastas de configuração são protegidos apenas com serviços e sistemas que têm direitos de acesso por padrão. Portanto, antes de tentar executar as tarefas abaixo, o usuário admin só tem acesso de leitura/escrita à pasta C:\Arquivos de Programas\Druck\4Sight2\<<latest folder number>>\apache-tomcat\conf. Abra o prompt de comando com as credenciais do usuário admin.

5.5.3 Comunicação Segura

Esta seção fornece instruções para configurar o 4sight2 em um modo seguro (também conhecido como modo SSL) usando um certificado autoassinado. Leia as suposições e os termos e condições definidos no aplicativo 4Sight2 antes de prosseguir. Um certificado autoassinado é uma forma de habilitar o SSL no 4Sight2. Alternativamente, um certificado CA de terceiros pode ser adquirido de muitos outros fornecedores como a Symantec, a Digicert e assim por diante.

Observação: Ativar o SSL não necessariamente é suficiente para tornar sua aplicação segura. Esta é uma das práticas mais comuns para a construção de uma aplicação segura para web.

Copyright 2020. Druck Ltd, a Baker Hughes business

5.5.3.1 Suposições e Advertências

As seguintes suposições são feitas para as instruções abaixo funcionarem:

O software OpenSSL para Windows é necessário para gerar Certificados Autoassinados. O 4Sight2 pressupõe que as suas organizações, leis regionais e nacionais e diretrizes regulatórias permitem o uso do software OpenSSL.

- O Keytool é um utilitário de gerenciamento de chaves e certificados fornecido por Java, que é usado para gerar vários componentes envolvidos na configuração de https. O 4Sight2 pressupõe que suas organizações, leis regionais e nacionais e diretrizes regulatórias permitem o uso de utilitário Keytool.
- Você precisa de privilégios administrativos para executar as configurações abaixo. Para mais informações sobre como obter direitos administrativos, contate seu departamento de TI local.
- Os passos abaixo requerem um entendimento básico sobre o processo de computador, portanto, o ideal é que eles sejam executados pela TI local ou sob sua orientação.
- O conteúdo apresentado neste documento, como nomes de hosts, senhas, URLs e caminhos de pastas, é apenas para referência. Antes da execução, modifique os comandos conforme necessário.
- As seções a seguir cobrem dois cenários. Em um cenário, o Servidor e o Cliente estão na mesma máquina e, no segundo, o Servidor e o Cliente estão em máquinas diferentes (ou seja, um cenário de múltiplos Clientes).

5.5.3.2 Etapas para configurar o aplicativo 4Sight2 em https

1. Interrompa o 4Sight2 no Windows Services
2. Abra o prompt de comando em **Admin Mode** (Modo Admin)
3. Navegue até a pasta abaixo no diretório de instalação do 4Sight2 executando o comando abaixo

   cd "C:\Program Files\Druck\4Sight2\<<latest folder number>>\apache-tomcat\conf"
4. Verifique se o keytool está presente executando o seguinte comando no prompt de comando: **Keytool** -?

   Caso contrário, defina o caminho do ambiente para o compartimento JRE na pasta de instalação do 4Sight2, como mostrado abaixo. Atualize o caminho correto baseado na pasta de instalação.

   C:\Program Files\Druck\4Sight2\<<latest folder number>>\jre\bin
   Set "Path=%Path%;C:\Program Files\Druck\4Sight2\<<latest folder number>>\jre\bin"
5. Para criar um novo certificado, pule para o ponto 6. Caso contrário, se já existir um certificado, faça o seguinte:

   a. Verifique se o arquivo de certificado 4Sight.jks existe no keystore da Java.

   keytool -list -alias <<nome do host>> -storepass <<senha>> -keystore 4Sight.jks

   b. Se já estiver instalado o certificado, remova-o

   keytool -delete -noprompt -alias <<nome do host>> -storepass <<senha>> -keystore 4Sight.jks

   c. Verifique e exclua se o 4SightV2PublicKey.cer existe

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

   d. Verifique se o certificado já existe em CACert de Java.

Copyright 2020. Druck Ltd, a Baker Hughes business

keytool -list -alias <<nome do host>> -storepass changeit -keystore "../../jre/lib/security/cacerts"

e. Exclua o certificado se ele existir no armazenamento java.

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

6. Crie o novo certificado executando o comando abaixo:

   keytool -genkey -trustcacerts -keyalg "RSA" -keysize 2048 -validity 1095 -keypass <<Senha>> -alias <<Nome do Host>> -keystore 4Sight.jks -storepass <<Senha Armazenada>> -dname "CN=%COMPUTERNAME%, OU=<<Unidade de Organização>>, O=<<Organização>>, L=<<Localização>>, S=<<Estado>>, C=<<Inicial de País>>" -ext eku:critical=sa

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

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

   Se o comando for executado com sucesso, será exibida uma mensagem: "Certificate stored in file C:\Program Files\Druck\4Sight2\<<latest folder number>>\app\Certificate\4SightV2PublicKey.cer" (Certificado armazenado no arquivo C:\Program Files\Druck\4Sight2\<<latest folder number>>\app\Certificate\4SightV2PublicKey.cer).

8. Importe o certificado para o arquivo Java CACert.

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

Após o comando ser executado com sucesso, será exibida uma mensagem "Certificate was added to keystore" (Certificado foi adicionado ao keystore).

9. Insira o certificado no arquivo de configuração Tomcat

   a. Abra o arquivo server.xml a partir do local abaixo.

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

   b. Crie a seguinte entrada no server.xml.

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

   c. Comente a seguinte seção para desativar as conexões http.

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

Observação: O aplicativo não funciona se você não comentar esta parte.

10. Neste ponto, a configuração https do aplicativo 4Sight2 foi concluída.
11. Para testar as configurações realizadas acima, reinicie o Serviço 4Sight2 no Windows Service.
12. Abra o Google Chrome, limpe o cache do navegador e reinicie o navegador.

Copyright 2020. Druck Ltd, a Baker Hughes business

13. Insira a seguinte URL no navegador: https://<<nome do host>>:8443/4sight2

- Pode ser que demore mais tempo para carregar o URL na primeira vez.
- Será exibida a tela "Your connection is not private" (Sua conexão não é privada).
- Clique no botão **Advanced** (Avançado) >> link **Proceed to XX** (Ir para XX).
- Se você não vir a tela 4sight2, clique no botão **Reload** (Recarregar).
- Você será direcionado para a página 4sight2.
- Haverá um erro "Not Secure" (Não seguro) na barra de endereços, que desaparecerá após o registro do certificado em mmc.

5.5.3.3 Passos para configurar o DruckCommsServer em https se instalado na máquina do servidor

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

1. Interrompa o DruckCommsServer no Windows Services.
2. Abra o prompt de comandos em **Admin Mode** (Modo Admin).
3. Verifique se o keytool está presente, executando o seguinte comando no prompt de comandos: **Keytool -?**

   Caso contrário, defina o caminho do ambiente para o compartimento JRE na pasta de instalação do 4Sight2, como mostrado abaixo.
   Atualize o caminho correto baseado na pasta de instalação.
   C:\Program Files\Druck\4Sight2\<<latest folder number>>\jre\bin
   Set "Path=%Path%;C:\Program Files\Druck\4Sight2\<<latest folder number>>\jre\bin"
4. Navegue até a pasta abaixo no diretório de instalação do DruckCommServer executando o comando abaixo

   cd " C:\Program Files\Druck\DruckCommsServer\<< Versão de Serviço de Comunicação >>"
5. Verifique se já existe um Certificado e faça o seguinte:

   a. Verifique se o certificado já existe em CACert de Java.
   keytool -list -alias tomcat -storepass changeit -keystore cacerts

   b. Exclua o certificado se ele existir no armazenamento Java.
   keytool -delete -noprompt -alias tomcat -storepass changeit -keystore cacerts

   c. Elimine os certificados pré-configurados do CommsServer que vem como padrão
   del 4Sight.jks
   del 4SightV2DeviceMngr.pfx
6. Crie o novo certificado executando o comando abaixo:

   keytool -genkey -trustcacerts -keyalg "RSA" -keysize 2048 -validity 1095 -keypass <<Senha>> -alias tomcat -keystore CommServer.jks -storepass <<Senha Armazenamento>> dname "CN=localhost, OU=<<Unidade de Organização>>, O=<<Organização>>, L=<<Localização>>, S=<<Estado>>, C=<<Inicial de País>>" -ext eku:critical=sa
7. Exporte o certificado para o arquivo DruckCommServer.cer

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

Copyright 2020. Druck Ltd, a Baker Hughes business

Se o comando for executado com sucesso, será exibida uma mensagem: "Certificate stored in file DruckCommServer.cer" (Certificado armazenado no arquivo DruckCommServer.cer) será exibido.

8. Importe o certificado do servidor de comunicação para o arquivo java CACert.

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

   Após o comando ser executado com sucesso, será exibida uma mensagem "Certificate was added to keystore" (Certificado foi adicionado ao keystore).

9. Importe o certificado 4Sight para o arquivo java CACert.

   keytool -import -noprompt -trustcacerts -alias <<nome de host do servidor>> -storepass changeit -keystore cacerts -file "C:\Program Files\Druck\4Sight2\<<latest folder number>>\app\Certificate\4SightV2PublicKey.cer"

   Após o comando ser executado com sucesso, será exibida uma mensagem "Certificate was added to keystore" (Certificado foi adicionado ao keystore).

10. Edite a senha do armazenamento de chaves para aplication.properties no DruckCommsServer.

    Abra esse arquivo:
    C:\Program Files\Druck\DruckCommsServer\<<Versão do serviço de comunicação>>\application.properties e altere a seguinte linha:
    keystore = CommServer.jks
    Key-store.password=<<senha do armazenamento>>
    Observação: **<< Senha do armazenamento >>** referindo-se a **StorePassword** usado na etapa 6.

11. Reinicie os serviços do 4Sight2 e do DruckCommsServer.

5.5.3.4 Passos para Configurar o DruckCommsServer em HTPPS se Instalado na Máquina do Servidor

1. O utilitário Keytool é fornecido com Java, portanto, você pode instalar Java na sua máquina ou verificar a disponibilidade do keytool Java diretamente sem a instalação de Java.
2. Interrompa o DruckCommsServer no Windows Services.
3. Abra o prompt de comando em **Admin Mode** (Modo Admin).
4. Verifique se o keytool está presente executando o seguinte comando no prompt de comandos: **Keytool -?**

   Caso contrário, defina o caminho do ambiente para o compartimento JRE se você já instalou Java na máquina ou defina o caminho para o keytool conforme mostrado abaixo.
   Atualize o caminho correto baseado na pasta de instalação.
   C:\Program Files\Java\<< Versão Java >>\bin
   Set Path=%Path%; "C:\Program Files\Java\<< Versão Java >>\bin"

5. Obtenha o arquivo **4SightV2PublicKey.cer** da máquina do Servidor onde o aplicativo do 4Sight está instalado. Este arquivo está localizado no servidor como mostrado abaixo

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

6. Copie este **4SightV2PublicKey.cer** no caminho a seguir:

   C:\Program Files\Druck\DruckCommsServer\<< Versão de Serviço de Comunicação >>

Copyright 2020. Druck Ltd, a Baker Hughes business

7. Agora siga as etapas 4 a 8 na seção 5.5.3.3.
8. Importe o certificado 4Sight para o arquivo Java CACert.

   keytool -import -noprompt -trustcacerts -alias <<nome de host do servidor>> -storepass changeit -keystore cacerts -file 4SightV2PublicKey.cer

   Após o comando ser executado com sucesso, será exibida uma mensagem "Certificate was added to keystore" (Certificado foi adicionado ao keystore).
9. Agora siga as etapas 10 a 11 na seção 5.5.3.3.

5.5.3.5 Etapas para gerar certificado de autoassinatura para o 4Sight2

1. Baixe e instale o Open SSL para Windows.
2. Interrompa os serviços do 4Sight2 no Windows Services.
3. Crie uma nova pasta chamada **4Sight2Certificate** dentro da unidade C.

   Você pode escolher qualquer local ou nome de pasta desde que tenha acesso administrativo a essa pasta.
4. Crie um novo arquivo dentro da pasta acima no bloco de notas e salve esse arquivo como **openssl-ca.cnf**

   Copie o conteúdo abaixo para o arquivo e salve esse arquivo.

Copyright 2020. Druck Ltd, a Baker Hughes business

```
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
```

Copyright 2020. Druck Ltd, a Baker Hughes business

```
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
```

Observação: 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 arquivo dentro da pasta acima no bloco de notas e salve esse arquivo como **openssl-server.cnf**

Copie o conteúdo abaixo para o arquivo e salve esse arquivo.

Copyright 2020. Druck Ltd, a Baker Hughes business

```
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 ]
```

Copyright 2020. Druck Ltd, a Baker Hughes business

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

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

# IPv6 localhost
IP.2 = ::1

Observação: Atualize o nome do host e o endereço IPv4 acima e salve o arquivo.

6. Abra o prompt de comando com privilégios administrativos.
7. Vá para a pasta 4Sight2Certificate executando o comando abaixo

   cd "<<caminho completo para 4Sight2Certificate >>"
8. Defina a variável do caminho para a pasta do compartimento OpenSSL executando o comando abaixo.

   Set path=%path%;"<<pasta do openssl>>"

   Exemplo de caminho padrão:

   Set Path=%Path%;"C:\Program Files\OpenSSL-Win64\bin"
9. Defina a variável do caminho para pasta do compartimento JRE executando o comando abaixo. Observação: o caminho abaixo pode ser diferente.

   Set path=%path%;"C:\Program Files\Druck\4Sight2\<<latest folder number>>\jre\bin"
10. Execute o comando abaixo para gerar os arquivos 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

    Quando solicitado, insira os dados corretos do certificado referentes a país, estado, etc.
11. Execute os comandos abaixo para gerar os arquivos 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

    Insira a data correta do certificado quando solicitado para, por exemplo, país, estado, etc.
12. Crie um novo arquivo no bloco de notas e nomeie como index.txt. Salve o arquivo na pasta 4Sight2Certificate.
13. Crie um novo arquivo no bloco de notas e nomeie como serial.txt. Salve o arquivo na pasta 4Sight2Certificate.

    Abra o arquivo e insira **01** Salvar e fechar o arquivo.
14. Execute abaixo o comando para gerar novos certificados nos arquivos servercert.pem e serverkey.pem.

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

    Insira Y para aplicar as alterações. Você verá o banco de dados atualizado após uma execução bem-sucedida.
15. Agrupe arquivos de chaves existentes no formato PFX executando o comando abaixo.

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

    Você será solicitado a inserir a senha duas vezes.

Copyright 2020. Druck Ltd, a Baker Hughes business

16. Converta o armazenamento PFX em armazenamento de chaves Java classificadas conforme a localização do compartimento JRE citado acima, i.e. Tomcat/caminho de configuração.

    keytool -importkeystore -srckeystore <<nome do host>>.p12 -srcstoretype PKCS12 -destkeystore "C:\Program Files\Druck\4Sight2\<<latest folder number>>\apache--tomcat\conf\4Sight.jks"
    -deststoretype jks
    Observação: Mantenha as senhas iguais para os dois armazenamentos. Aponte para o 4Sight.jks presente na pasta de configuração tomcat como mostrado acima.
    Você será solicitado a fornecer a senha de armazenamento de chaves de destino e a senha de armazenamento de chaves de origem. Depois de executar o comando com sucesso, você verá a mensagem "Import command completed: 1 entries successfully imported" (Comando de importação concluído: 1 entrada importada com sucesso).

17. O certificado de exportação de armazenamento de chaves Java deve ser arquivado em:

    C:\Program Files\Druck\4Sight2\<<latest folder number>>\app\Certificate\4SightV2PublicKey.cer
    keytool -export -alias <<nome de host>> -keystore "C:\Program Files\Druck\4Sight2\<<latest folder number>>\apache-tomcat\conf\4Sight.jks" --storePass "<<senha>>"
    -storetype JKS -file "C:\Program Files\Druck\4Sight2\<<latest folder number>>\app\Certificate\4SightV2PublicKey.cer"
    Observação: Aponte para o 4Sight.jks presente na pasta de configuração de tomcat como mostrado acima.
    Você obtém a mensagem de certificado armazenado no arquivo após ele ser executado com sucesso.

18. Importe o arquivo de certificado na pasta cacerts no diretório de instalação 4Sight2.

    Observação: o caminho pode variar dependendo do diretório de instalação e da versão 4Sight2.
    keytool -import -noprompt -trustcacerts -alias <<nome do host>> -storepass changeit -keystore "C:\Program Files\Druck\4Sight2\<<latest folder number>>\jre\lib\security\cacerts" -file "C:\Program Files\Druck\4Sight2\<<latest folder number>>\app\Certificate\4SightV2PublicKey.cer"
    Nota: por alguma razão, o alias que você está tentando criar já existe, execute primeiro o comando abaixo para apagá-lo, e depois execute o comando acima para criar um novo alias:
    keytool -delete -noprompt -trustcacerts -alias <<nome do host>> -storepass changeit -keystore "C:\Program Files\Druck\4Sight2\<<latest folder number>>\jre\lib\security\cacerts" -file "C:\Program Files\Druck\4Sight2\<<latest folder number>>\app\Certificate\4SightV2PublicKey.cer"
    você receberá a mensagem "Certificate was added to keystore" (Certificado foi adicionado ao armazenamento de chaves) após a execução desse comando.

19. Faça a seguinte mudança no arquivo server.xml (em C:\Program Files\Druck\4Sight2\<<latest folder number>>\apache-tomcat\conf).

    a. Crie a seguinte entrada no server.xml.

    <Connector port="8443"
    protocol="org.apache.coyote.http11.Http11NioProtocol"
    maxThreads="150"
    SSLEnabled="true"

Copyright 2020. Druck Ltd, a Baker Hughes business

sslProtocol="TLSv1.2"
keystoreFile="conf/4Sight.jks"
keystorePass="<<KeyPassword>>"
keyAlias="<<Host name>>"
scheme="https"
secure="true"
clientAuth="false" />

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

20. Isso conclui a configuração de https para 4Sight2. Agora inicie o serviço 4sight2 de Windows Services.

5.5.3.6 Etapas para Configurar Certificado Autoassinado para DruckCommsServer se Instalado na Máquina do Servidor

Aqui consideramos que você converteu com sucesso o aplicativo 4sight2 em HTTPs executando as etapas na seção 5.5.3.5 e que você já tem os arquivos abaixo em **4Sight2Certificate**:

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

1. Crie uma nova pasta como **CommserverCertificate** e copie os arquivos acima. Depois, faça alterações como abaixo:

- openssl-server.cnf

  Na seção **req**, modifique o valor **default_keyfile** como "**DruckCommServerCertKey.pem**".
  - Em **server_distinguished_name**, modifique o valor **commonName** para "**localhost**".
  - Em **alternate_names**, modifique o valor **DNS.1** para "**localhost**".
  - Em **alternate_names**, modifique o valor **IP.1** para "**127.0.0.1**"
  - Salve o arquivo.
- openssl-ca.cnf. (Não modifique nada dentro do arquivo)
- cacert.pem (Não modifique nada dentro do arquivo)
- index.txt (Apagar todo o conteúdo do arquivo, esvaziá-lo)
- serial.txt (esvaziar todo o conteúdo interno e fazer apenas a entrada de 01 interna)

2. Interrompa o serviço DruckCommsServer do Windows Services.
3. Abra o prompt de comando com privilégios administrativos.
4. Vá para a pasta **CommserverCertificate** executando abaixo,
   cd "<<caminho completo para CommserverCertificate >>"

Copyright 2020. Druck Ltd, a Baker Hughes business

5. Defina a variável do caminho para a pasta do compartimento OpenSSL executando o comando abaixo.

   Set path=%path%;"<<pasta de openssl>>"

   Exemplo de caminho padrão:

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

6. Defina a variável do caminho para a pasta do compartimento JRE executando o comando abaixo. Observação: o caminho abaixo pode ser diferente,

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

7. Depois de concluir isso, crie uma solicitação de certificado Comm Server seguindo o comando

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

   Depois desse comando, você terá uma solicitação em **DruckCommServer.csr** e uma chave privada em **DruckCommServerCertKey.pem**

8. Depois, faça o seguinte para assinar a solicitação csr com seu ca:

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

9. Depois disso, crie um arquivo PFX com alias **tomcat** para o servidor de comunicação, seguindo o comando

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

10. Converta o armazenamento PFX em armazenamento de chaves Java usando a keytool

    Observação: mantenha senhas iguais para os dois armazenamentos de chaves.
    keytool -importkeystore -srckeystore DruckCommServer.pfx -srcstoretype PKCS12 -destkeystore CommServer.jks -deststoretype jks

11. Agora importe o certificado para o cacert.

    a. Depois exclua o alias tomcat existente, que vem com a instalação padrão
    keytool -delete -noprompt -trustcacerts -alias tomcat -storepass changeit -keystore "C:\Program Files\Druck\DruckCommsServer\<< Versão de Serviço de Comunicação >>\cacerts"

    b. Após excluir o tomcat de alias existente, importe o certificado para o cacerts por
    keytool -import -noprompt -trustcacerts -alias tomcat -storepass changeit -keystore "C:\Program Files\Druck\DruckCommsServer\<< Versão de Serviço de Comunicação >>\cacerts" -file DruckCommServerCert.pem

12. Precisamos importar a chave pública do 4sight para o cacert do servidor de comunicação para autenticar a comunicação. Para fazer isso, execute o comando abaixo

    keytool -import -noprompt -trustcacerts -alias <<nome de host do servidor 4sight>> -storepass changeit -keystore "C:\Program Files\Druck\DruckCommsServer\<< Versão de Serviço de Comunicação >>\cacerts" -file "C:\Program Files\Druck\4Sight2\<<latest folder number>>\app\Certificate\4SightV2PublicKey.cer"

13. Depois de concluir o passo acima, você terá **DruckCommServer.pfx** e **CommServer.jks** na pasta **CommserverCertificate** atual.

Copyright 2020. Druck Ltd, a Baker Hughes business

Copie esses arquivos e cole no diretório "C:\Program Files\Druck\DruckCommsServer\<< Versão de Serviço de Comunicação >>\". E edite **application.properties** a partir do mesmo local. Altere o valor da propriedade conforme mostrado abaixo

a. Keystore = CommServer.jks

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

c. key-store.type=JKS

5.5.3.6.1 Instalação do Certificado no Windows para 4sight e DruckCommsServer

1. Abra Run (Executar), insira "mmc" e pressione Enter.
2. Vá para File (Arquivo) e selecione Add/Remove snap-ins (Adicionar/Remover módulos adicionais).
3. No menu à esquerda, selecione os certificados. Pressione Add (Adicionar) e selecione Computer account (Conta de computador) >> Next (Avançar) >> Finish (Concluir). Em seguida, clique em OK.
4. Expanda a seção Certificates (Certificados) (computador local). Expanda as Autoridades Confiáveis de Certificação Raiz.

   À direita, clique na pasta Certificates (Certificados) >> Todas as Tarefas >> Importar.
   Selecione cacert.pem >> next (Avançar) >> finish (Concluir).
   Sendo assim, a Autoridade de Certificado CA personalizada é instalada com sucesso em autoridade confiável.

Depois de executar todas essas etapas, inicie o serviço DruckCommsServer.

5.5.3.7 Etapas para Configurar Certificado Autoassinado para DruckCommsServer se Instalado na Máquina Cliente

Para converter o DruckCommsServer em HTTPs, você precisa ter java keytool e o utilitário OpenSSL.

1. O utilitário Keytool é fornecido com Java, portanto, você pode instalar Java na sua máquina ou verificar a disponibilidade do keytool Java diretamente sem a instalação de Java.
2. Baixe e instale o OpenSSL para Windows.
3. Defina a variável do caminho para a pasta do compartimento OpenSSL executando o comando abaixo.

   Set path=%path%;"<<pasta de openssl>>"
   Exemplo de caminho padrão:
   Set Path=%Path%;"C:\Program Files\OpenSSL-Win64\bin"
4. Defina a variável do caminho para a pasta de compartimento JRE executando o comando abaixo.

   C:\Program Files\Java\<< Versão Java >>\bin
   Set Path=%Path%; "C:\Program Files\Java\<< Versão Java >>\bin"
5. Interrompa o serviço DruckCommsServer no Windows Services.
6. Crie uma nova pasta chamada **CommserverCertificate** na unidade C ou em qualquer outra unidade que você queira.
7. Obtenha o arquivo do certificado público do 4sight2 **4SightV2PublicKey.cer** do servidor localizado no caminho C:\Program Files\Druck\4Sight2\<<latest folder number>>\app\Certificate e copie o arquivo na pasta **CommserverCertificate**.
8. Agora crie **openssl-server.cnf** e **openssl-ca.cnf** seguindo as etapas 4 e 5 da seção 5.5.3.5 e crie index.txt e serial.txt seguindo as etapas 12 e 13 na pasta **CommserverCertificate**.
9. Agora você terá cinco arquivos na pasta CommServerCertificate.

Copyright 2020. Druck Ltd, a Baker Hughes business

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

10. Abra o prompt de comando com privilégios administrativos.

    Vá para a pasta CommserverCertificate executando o comando abaixo
    cd "<<full path to CommserverCertificate >>"

11. Execute o comando abaixo para gerar os arquivos cacert.pem e cakey.pem.

    openssl req -x509 -config openssl-ca.cnf -newkey rsa:4096 -sha256 -nodes -out cacert.pem -outform PEM
    Quando solicitado, insira os dados corretos do certificado, por exemplo, para país, estado, etc.

12. Agora, altere o conteúdo dos arquivos na pasta **CommserverCertificate** executando a etapa 1 da seção 5.5.3.6.

13. Agora execute as etapas de 7 a 11 a partir de 5.5.3.6.

14. Precisamos importar a chave pública do 4sight para o cacert do servidor de comunicação para autenticar a comunicação. Para fazer isso, execute o comando abaixo

    keytool -import -noprompt -trustcacerts -alias <<nome do host do servidor 4sight>> -storepass changeit -keystore "C:\Program Files\Druck\DruckCommsServer\<< Versão de Serviço de Comunicação >>\cacerts" -file 4SightV2PublicKey.cer

15. Depois de concluir o passo acima, você terá **DruckCommServer.pfx** e **CommServer.jks** na pasta **CommserverCertificate** atual.

    Copie esses arquivos e cole no diretório **"C:\Program Files\Druck\DruckCommsServer\<< Versão de Serviço de Comunicação >>\"**. E edite **application.properties** a partir do mesmo local. Altere o valor da propriedade conforme mostrado abaixo

    a. Keystore = CommServer.jks
    b. key-store.password = <<senha do armazenamento de chaves>>
    c. key-store.type=JKS

5.5.3.7.1 Instalação do certificado no Windows para DruckCommsServer.

1. Abra Run (Executar), insira “mmc” e pressione Enter.
2. Vá para File (Arquivo) e selecione Add/Remove snap-ins (Adicionar/Remover módulos adicionais).
3. No menu à esquerda, selecione os certificados. Pressione Add (Adicionar) e selecione Computer account (Conta de computador) >> Next (Avançar) >> Finish (Concluir). Em seguida, clique em OK.
4. Expanda a seção Certificates (Certificados) (computador local). Expanda as Autoridades Confiáveis de Certificação Raiz.

   À direita, clique na pasta Certificates (Certificados) >> All Tasks (Todas as tarefas) >> Import (Importar).
   Selecione cacert.pem >> next (Avançar) >> finish (Concluir).
   Dessa forma, a Autoridade de Certificado CA personalizada é instalada com sucesso em autoridade confiável.

Depois de executar todas essas etapas, inicie o serviço DruckCommsServer.

Se você quiser apenas verificar se o DruckCommsServer foi convertido com sucesso em https; na guia Google Chrome, basta abrir o seguinte link: **https://localhost:9443/api/devicemanager/**

Copyright 2020. Druck Ltd, a Baker Hughes business

version (Insira o número da porta do seu servidor de comunicação se tiver alterado, mas o padrão é 9443)

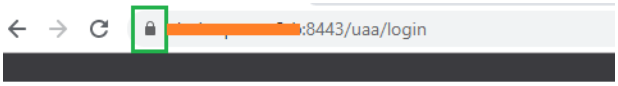
5.5.3.8 Validação do Certificado no 4Sight2

1. Reinicie o PC Servidor.
2. Reinicie os serviços do 4Sight2 e do DruckCommsServer a partir do Windows Services Open
3. Abra o Google Chrome, limpe o cache do navegador e reinicie o Google Chrome. Certifique-se de que não haja outras instâncias do Google Chrome em execução.
4. Insira o URL abaixo na barra de endereço, pressione Enter.

   Https://<<nome do host do servidor>>:8443/4sight2.

   Observação: você precisa usar o nome do host no URL acima.
5. Você deverá ver a tela de login com o URL HTTPS correto.

   Observação: o erro em vermelho desapareceu da barra de endereço. Se o link ainda não estiver seguro, reinicie o seu computador e vá para a etapa 3.



Copyright 2020. Druck Ltd, a Baker Hughes business

Perguntas Frequentes sobre a Instalação do 4Sight2

Copyright 2020. Druck Ltd, a Baker Hughes business

6. Perguntas Frequentes sobre a Instalação do 4Sight2

6.1 Configuração e Instalação

Pergunta 1: Tenho uma organização com múltiplas instalações que se estende por diferentes regiões do mundo. Qual é a melhor forma de configurar o 4Sight2?

Resposta: Depende de como você opera e mentém essas instalações. Se todos os sites forem mantidos e executados a partir de um hub central de TI, você pode instalar uma única licença 4Sight2 centralmente. Todos os sites podem acessar o 4Sight2 através da rede ou LAN. Por outro lado, se você tiver negócios secundários que sejam entidades separadas, autogerenciadas e administradas, você pode comprar várias licenças do 4Sight2.

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

Resposta: Não. Cada licença do 4Sight2 é um software separado e isolado com sua própria instalação de aplicação e banco de dados. Não há comunicação entre instalações separadas. Entre em contato com a equipe do 4Sight2 para maiores esclarecimentos ou para discutir quaisquer requisitos especiais.

Pergunta 3: Como posso baixar o 4Sight2?

Resposta: Você pode baixar facilmente o 4Sight2 do site da empresa. Abaixo temos o link.

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

OU

você pode ligar para os escritórios de vendas e obter um pedido de compra. Você deve receber a versão de demonstração em uma chave USB.

Pergunta 4: Posso instalar o 4Sight2 em um sistema operacional sem Windows?

Resposta: Não. O 4Sight2 só é suportado para plataforma Windows.

Pergunta 5: Fiz o download e instalei o 4Sight2? Como eu acesso o 4Sight2?

Resposta: O 4Sight2 é um software baseado na web. Portanto, nenhum ícone é gerado no seu desktop ou computador quando você instala o 4Sight2. Para acessar o 4Sight2,

- Abra o Google Chrome, cole abaixo da URL na barra de endereço e pressione Enter,
- Se o 4Sight2 estiver instalado no mesmo computador, use http://localhost:<número_porta_aplicativo> /4sight2. Se o 4Sight2 estiver instalado em um computador diferente na mesma rede, use,

  http://<Nome do computador OU endereço IP>:<número_porta_aplicativo>/4sight2
- Crie um marcado no Google Chrome para referência futura.

Pergunta 6: O instalador do 4Sight2 não consegue localizar os arquivos do banco de dados Postgres

Certifique-se de que o instalador foi extraído para um determinado local e o executável esteja sendo executado a partir da pasta Disco 1. Certifique-se de que o local para o qual o instalador foi extraído não tenha um caminho longo, pois isso também pode resultar na falha em encontrar os arquivos de pré-requisitos do instalador.

Copyright 2020. Druck Ltd, a Baker Hughes business

Pergunta 7: O que acontece se o processo de upgrade for cancelado em qualquer etapa durante o upgrade?

Resposta: A qualquer momento, se o administrador cancelar o processo de atualização, ele voltará para a versão 1.4 e deverá estar em funcionamento. O Admin precisa iniciar novamente o processo de atualização para realizar a atualização com sucesso.

Pergunta 8: Durante a instalação do aplicativo 4Sight2 se o usuário receber esta mensagem "Please enter valid port number. To know valid port numbers please refer installation manual" (Digite o número da porta válida. Para saber os número de porta válidos, consulte o manual de instalação).

Resposta: A seguir temos o intervalo de portas inválidas, escolha uma porta válida para continuar a instalação

- As Portas 0 a 1024 são reservadas para a conexão TCP
- A lista de portas inseguras são - 2049, 3659, 4045, 6000, 6665-6669, 65535

Pergunta 9: O 4Sight2 com https não está funcionando no sistema

Resposta: Siga a sintaxe do nome de domínio do computador onde a aplicação 4sight2 será instalada

<domínio> ::= <subdomínio>

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

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

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

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

<let-dig> ::= <letra> | <dígito>

<letra> ::= qualquer um dos 52 caracteres alfabéticos de A a Z em

maiúsculas e a até z em minúsculas

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

Observação: As letras maiúsculas e minúsculas são permitidas em nomes de domínio. Dois nomes com a mesma grafia, mas caso diferente, são tratados como idênticos.

6.2 Perguntas Frequentes de Comunicação do Equipamento de Teste

Pergunta 1: Eu completei todas as etapas do manual de instalação e ainda não consigo ver o meu dispositivo na lista.

Resposta: Se você ainda não encontrar o equipamento de Teste na lista após executar essas etapas, reinstale novamente os drivers do 4Sight2. Para fazer isso, vá para **Painel de Controles >> Programas e Recursos**, desinstale o DruckCommsServer da lista. Instale o Comunicador de Equipamento de Teste novamente.

Pergunta 2:. Eu recebo um erro, '**No Devices Found**' (Nenhum dispositivo encontrado)

Resposta: Para solucionar o problema,

- Conecte fisicamente o dispositivo corretamente usando o cabo USB. Para verificar isso, vá até o gerenciador de dispositivos, localizar seu dispositivo na lista. O ideal é que você encontre seu dispositivo na seção de Dispositivos USB. Se vir seu dispositivo em Other devices (Outros

Copyright 2020. Druck Ltd, a Baker Hughes business

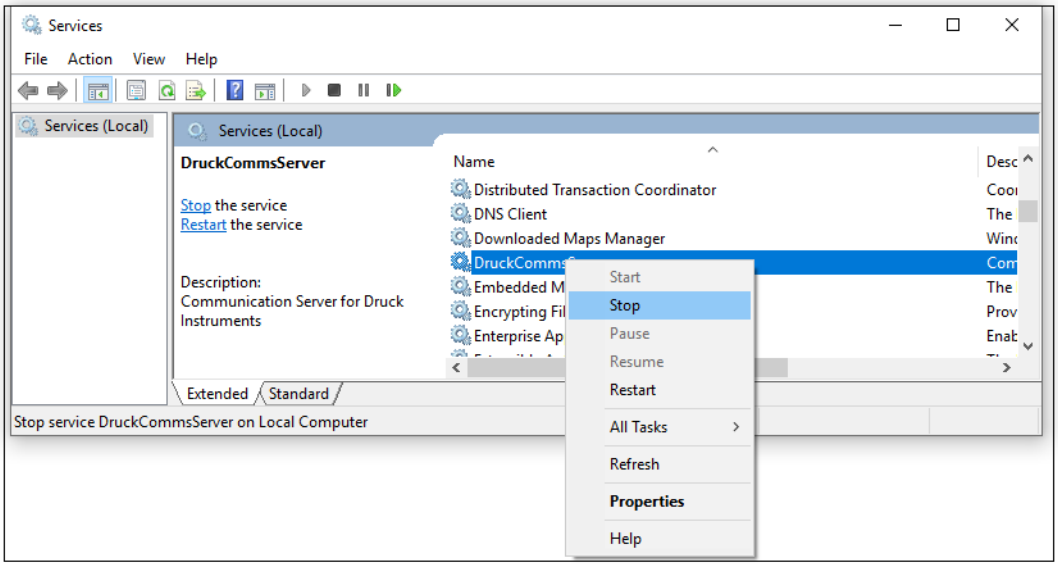
dispositivos), você precisa realizar as configurações acima para tornar seu dispositivo um dispositivo USB.

- Certifique-se de que seu dispositivo esteja no modo de comunicação ou comms. Veja a etapa 1 acima.
- Verifique se o caminho do motorista está corretamente apontado para C:\Windows\INF... Veja a etapa 2 acima.

Pergunta 3: Eu recebo um erro, '**Internal Server Error**' (Internal Server Error) quando clico em Refresh (Atualizar) ou clico no equipamento de teste da lista.

Resposta: Para solucionar esse problema,

- Vá para Windows Services (também conhecido como Serviços),
- Clique com o botão direito no Serviço **DruckCommsServer** na lista e clique em **Restart** (Reiniciar).



- Vá para 4Sight2 >> Clique no botão **Refresh** (Atualizar). Você deve ver o dispositivo na lista.

Pergunta 4: Eu recebo um erro, '**Communications Error**' (Erro de Comunicação).

Resposta: Às vezes, o software não consegue se comunicar corretamente com o dispositivo devido a vários motivos, tais como contato USB solto, dispositivo que fica pendurado, dispositivo ocupado executando outras tarefas, servidor ocupado executando outras tarefas e assim por diante. Clique novamente no botão Refresh (Atualizar) e o problema deve desaparecer (tente isso 2- 3 vezes).

No entanto, se você ainda assim obtiver esse erro de forma consistente e persistente, tente os passos abaixo,

- Reinicie seu dispositivo (Genii / PACE), certifique-se de que seja seguro e que o dispositivo não esteja no meio de uma operação crítica. Tente de novo. Verifique também se o dispositivo ainda está fisicamente conectado.

Se o passo acima não funcionar, siga as instruções do passo 3 acima e reinicie o Serviço **DruckCommsServer**.

Copyright 2020. Druck Ltd, a Baker Hughes business

Solução de Problemas de Instalação

Copyright 2020. Druck Ltd, a Baker Hughes business

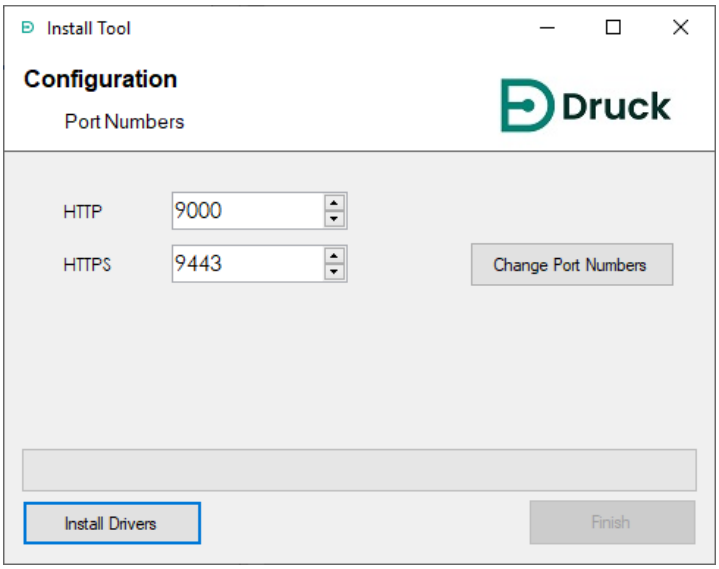
7. Solução de Problemas de Instalação

7.1 Problemas de Comunicação do Equipamento de Teste

Se ao usar o 4Sight2 para se comunicar com o equipamento de teste, você não receber retorno de nenhum equipamento de teste, embora você tenha verificado que o comunicador do equipamento de teste está retornando a string json após uma chamada direta para o comunicador. Isso pode estar ocorrendo por dois motivos principais:

- Os números das portas foram configurados incorretamente - entre em contato com seu usuário administrativo para saber quais portas a 4Sigth2 está utilizando para entrar em contato com o Comunicador de Equipamentos de Teste.

  Quando souber que portas você deve usar, vá para C:\Program Files\Druck\DruckCommsServer\[Versão] e execute o arquivo CommsServerInstallTool.exe



Edite os números de porta e, em seguida, clique no botão **Change Port Numbers** (Alterar Números de Portas). Aguarde enquanto o serviço reinicia. Os números de portas foram alterados. Selecione o botão **Finish** (Concluir).

- O Comunicador do Equipamentos de Teste não está configurado para Https, mas o 4Sight2 está.

  Entre em contato com seu administrador para instalar um certificado autoassinado para o Comunicador do Equipamento de Teste.

7.2 Backup do Banco de Dados Postgres

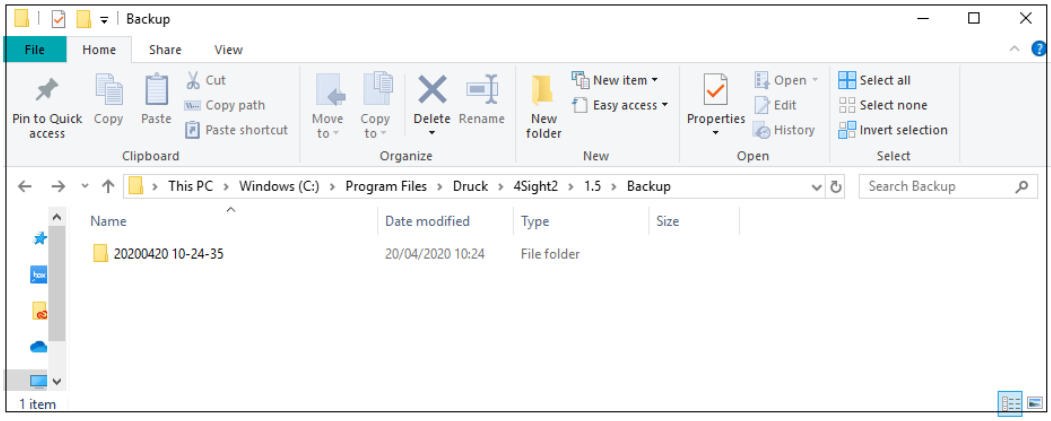
Consulte o manual do usuário do 4Sight2 - 123M3138 para informações sobre o backup do banco de dados postgres.

Copyright 2020. Druck Ltd, a Baker Hughes business

7.3 Restauração do Banco de Dados Postgres

Considerando que você já tenha realizado um backup do banco de dados usando o aplicativo 4Sight.

O aplicativo 4Sight (Versão 1.4 & acima) fornece uma interface para iniciar um backup (iniciado pelo usuário ou agendado). Esta operação cria arquivos na pasta de backup dentro do diretório de instalação do 4Sight no servidor. Cada backup iniciado cria uma nova pasta dentro da pasta de backup com o nome no formato AAAAMMDDHHSS (Ano, Mês, Data, Hora e Segundo) dependendo da data e hora em que o backup foi concluído com sucesso.



É uma prática recomendada fazer o backup do conteúdo da pasta de backup em uma mídia separada

Cada pasta tem 5 arquivos.

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

Os arquivos *.bck têm um sufixo com a versão do aplicativo 4Sight. Restaure um banco de dados que corresponda à versão exata de seu aplicativo. As versões superior / inferior da base de dados não são suportadas pela aplicação. Observe que a versão contém um sublinhado (_) e não um ponto (.), por exemplo, 1_4 e não 1.4. Ao utilizar os comandos abaixo nos Passos para Restauração, troque <VERSÃO_APLICATIVO> pela versão correspondente do 4Sight que foi instalada.

O arquivo metadata.properties contém o nome do backup conforme inserido durante a iniciação do backup.

Copyright 2020. Druck Ltd, a Baker Hughes business

Verificação do SHA 256

Em um backup, temos 3 arquivos - um para cada banco de dados, com a extensão .bck. O arquivo metadados.properties contém o SHA 256 de cada um dos arquivos de backup.

1. Abra um prompt de comando como Administrador e altere o diretório para a pasta que contém os arquivos de backup selecionados.
2. Use os comandos abaixo para calcular o SHA256 de cada arquivo

   certutil -hashfile 4Sight**<VERSÃO_APLICATIVO>.bck>**.bck SHA256
   certutil -hashfile 4Sightaudit**<VERSÃO_APLICATIVO>.bck>**.bck SHA256
   certutil -hashfile uaa**<VERSÃO_APLICATIVO>.bck>**.bck SHA256
3. Antes de prosseguir com as etapas de restauração, verifique se o SHA 256 de cada arquivo corresponde ao SHA 256 mencionado no arquivo de metadados. O arquivo de backup é válido para restauração se o checksum do prompt de comando e o checksum do arquivo metadados forem exatamente iguais. Continue com os Passos para restauração somente se eles forem iguais.

7.4 Etapas para Restauração:

1. Acesse o servidor 4Sight como Administrador.
2. Encontre a porta em que o Banco de Dados Postgres está rodando. Ela pode ser encontrada na porta spring.datasource.url dentro do arquivo <DIRETÓRIO DE INSTALAÇÃO DO 4Sight>\apache--tomcat\webapps\application.properties. Use um Bloco de Notas como Administrador para abrir este arquivo. É o número exibido logo antes de 4Sight**<VERSÃO_APLICATIVO>**
3. Como administrador, acesse o utilitário do comando psql a partir de um prompt de comando, usando o usuário postgres

   C:\Program Files\PostgreSQL\11\bin\psql" --port=<PORTA_BD> postgres postgres
4. O usuário de banco de dados usado pelo aplicativo pode ser encontrado na porta spring.datasource.url dentro do arquivo <DIRETÓRIO DE INSTALAÇÃO DO 4Sight>\apache--tomcat\webapps\application.properties. Use um Bloco de Notas como Administrador para abrir este arquivo.
5. Exclua os bancos de dados *_temp se eles existirem e depois crie os bancos de dados *_temp vazios executando os comandos abaixo no prompt do psql

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

   Mude o proprietário do Banco de Dados dos 3 bancos de dados acima para este usuário. Observe que o nome do usuário diferencia maiúsculas e minúsculas.

Copyright 2020. Druck Ltd, a Baker Hughes business

ALTER DATABASE "4Sight**<VERSÃO_APLICATIVO>**_temp" OWNER TO "**<USUÁRIO_BD>**";
ALTER DATABASE "4Sightaudit**<VERSÃO_APLICATIVO>**_temp" OWNER TO "**<USUÁRIO_BD>**";
ALTER DATABASE "uaa**<VERSÃO_APLICATIVO>**_temp" OWNER TO "**<USUÁRIO_BD>**";

6. Verifique os arquivos metadados.properties dos backups e decida qual backup você precisa restaurar.
7. Abra um outro prompt de comando como Administrador e altere o diretório para a pasta que contém os arquivos de backup selecionados.

   Restaure o banco de dados a partir dos arquivos *.bck para bancos de dados *_temp usando os comandos abaixo. Se for solicitada uma senha, digite a senha do super usuário do postgres.
   "C:\Program Files\PostgreSQL\11\bin\pg_restore" --port=**<PORTA_BD>** --no-owner --username=postgres --dbname=4Sight**<VERSÃO_APLICATIVO>.bck**_temp -n public --role=**<USUÁRIO_BD>** 4Sight**<VERSÃO_APLICATIVO>.bck**.bck

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

   "C:\Program Files\PostgreSQL\11\bin\pg_restore" --port=**<PORTA_BD>** --no-owner --username=postgres --dbname=uaa**<VERSÃO_APLICATIVO>.bck**_temp -n public --role=**<USUÁRIO_BD>** uaa**<VERSÃO_APLICATIVO>.bck**.bck
8. Exclua os bancos de dados *_old se eles existirem executando os comandos abaixo no prompt do psql

   DROP DATABASE IF EXISTS "4Sight**<VERSÃO_APLICATIVO>**_old";
   DROP DATABASE IF EXISTS "4Sightaudit**<VERSÃO_APLICATIVO>**_old";
   DROP DATABASE IF EXISTS "uaa**<VERSÃO_APLICATIVO>**_old";
9. Pare o serviço 4Sight e as aplicações pgadmin se alguma estiver aberta.
10. Renomeie os bancos de dados 4Sight para *_old executando os comandos abaixo no prompt do psql.

    ALTER DATABASE "4Sight**<VERSÃO_APLICATIVO>**" RENAME TO "4Sight**<VERSÃO_APLICATIVO>**_old";
    ALTER DATABASE "4Sightaudit**<VERSÃO_APLICATIVO>**" RENAME TO "4Sightaudit**<VERSÃO_APLICATIVO>**_old";
    ALTER DATABASE "uaa**<VERSÃO_APLICATIVO>**" RENAME TO "uaa**<VERSÃO_APLICATIVO>**_old";
11. Renomeie os bancos de dados *_temp para bancos de dados 4Sight executando os comandos abaixo no prompt do psql.

    ALTER DATABASE "4Sight**<VERSÃO_APLICATIVO>**_temp" RENAME TO "4Sight**<VERSÃO_APLICATIVO>**";
    ALTER DATABASE "4Sightaudit**<VERSÃO_APLICATIVO>**_temp" RENAME TO "4Sightaudit**<VERSÃO_APLICATIVO>**";
    ALTER DATABASE "uaa**<VERSÃO_APLICATIVO>**" RENAME TO "uaa**<VERSÃO_APLICATIVO>**";
12. Inicie o 4Sight Service e teste o login como Administrador. Observe que a senha do Administrador no momento de fazer o backup tem que ser usada para fazer o login agora.

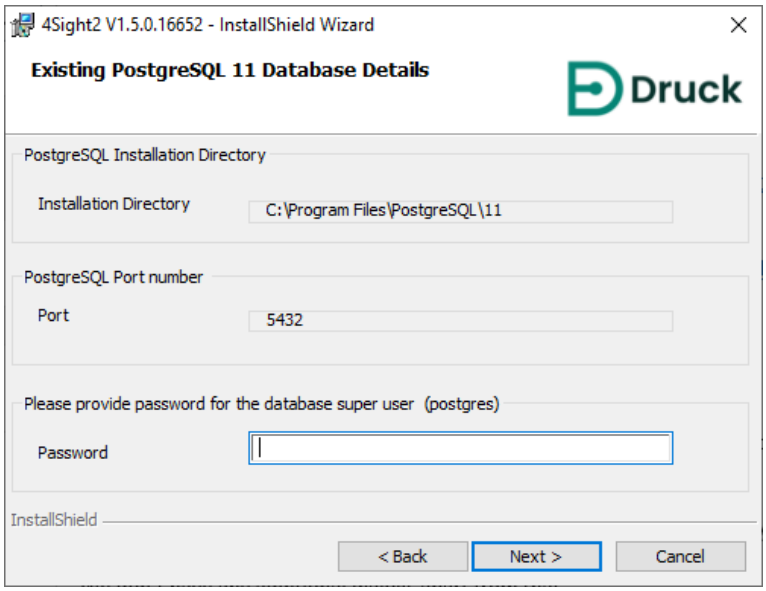
Copyright 2020. Druck Ltd, a Baker Hughes business

7.5 Como se recuperar de uma falha da máquina 4Sight2?

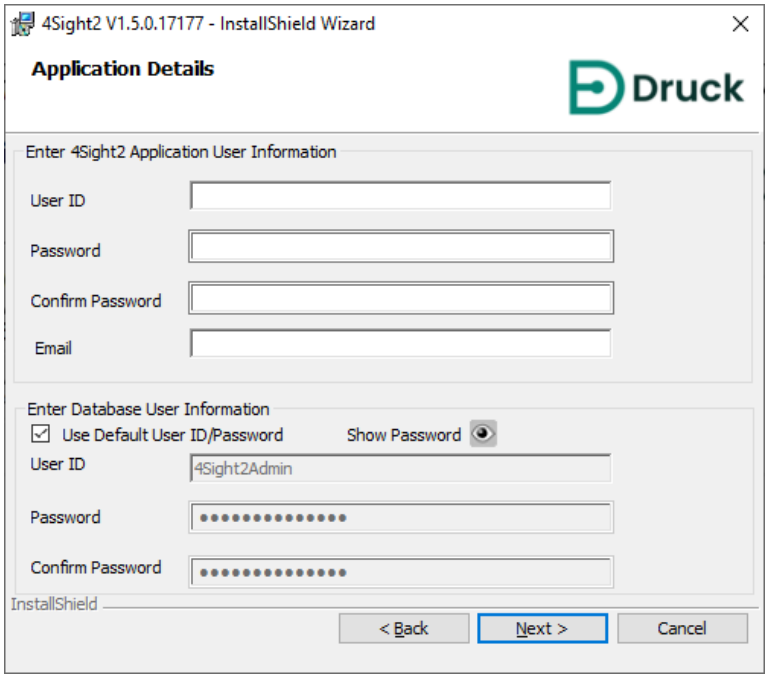
Pressupostos: O usuário fez um backup do banco de dados do 4Sight2 antes da falha.

O usuário já sabe o nome de usuário e a senha tanto do aplicativo quanto do banco de dados.

1. Configure a máquina com Sistema Operacional e Drivers de suporte.
2. Instale 4Sight2 na máquina.
3. Ao instalar o aplicativo, insira o mesmo nome de usuário e senha fornecidos anteriormente tanto para o aplicativo quanto para o banco de dados Postgres.



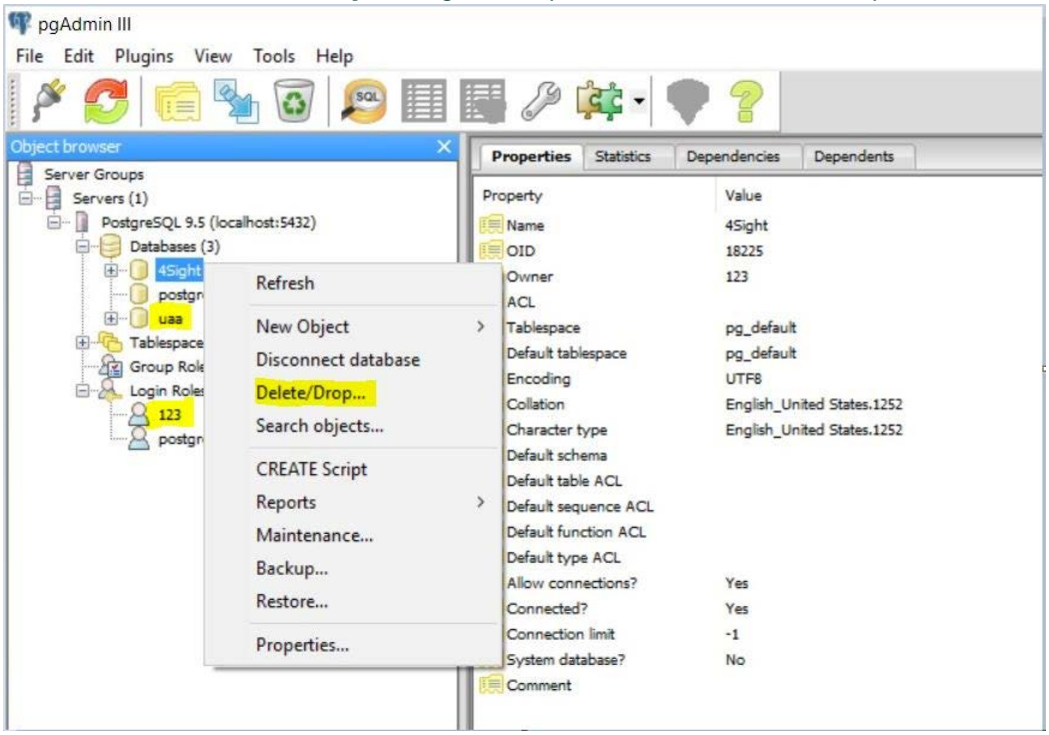
Senha igual à instalação anterior



Preencha todos os campos da mesma forma que na instalação anterior

Copyright 2020. Druck Ltd, a Baker Hughes business

4. Após instalar a aplicação com sucesso, solte o banco de dados padrão criado durante a instalação da aplicação do pgAdmin. Clique com o botão direito do mouse no banco de dados e selecione Delete (Excluir)/Drop (Soltar). Se você estiver recebendo um erro ao soltar o banco de dados, reinicie o serviço Postgres e repita a mesma tentativa após a atualização.



5. Depois de soltar o banco de dados e o usuário. Siga estes passos para restaurar o banco de dados como mencionado acima, a partir do prompt de comando.
6. Agora você restaurou o banco de dados com sucesso, abriu o aplicativo a partir do navegador e revisou o mesmo.

7.6 Cenário de falha na instalação:

A tabela abaixo explica os diversos cenários de falhas durante a instalação e suas ações corretivas.

Mensagem de Erro	Cenário	Correção/Ação necessária
"Insufficient disk space available to install 4Sight2 application. Please ensure a minimum of 4096 MB is available. Free Space : available MB."	Falha devido a problema de tamanho do disco rígido. Se não houver espaço necessário no início da atualização.	A administração precisa liberar espaço na respectiva unidade e depois tentar novamente o processo de Upgrade.
"Deployment fail while Migrating database"	Falha devido a problema no tamanho do disco rígido (se não houver espaço suficiente após o início do upgrade)	A administração precisa liberar espaço na respectiva unidade e depois tentar novamente o processo de Upgrade.

Copyright 2020. Druck Ltd, a Baker Hughes business

Mensagem de Erro	Cenário	Correção/Ação necessária
"Installation failed while migrating Database. Please reinstall 4sight2"	Falha devido à integridade dos dados na cópia do banco de dados	Admin precisa entrar em contato com o suporte ao cliente caso isso ocorra. Razão da integridade dos dados captada nos registros no local.[C:\Usuário\[Nome-de--usuário]\App Data\Local\Temp\logs]
"Installation failed while migrating Database. Please reinstall 4sight2"	Falha devido à integridade dos dados no estágio de atualização do esquema	O Admin precisa entrar em contato com o suporte ao cliente caso isso ocorra. Razão de integridade dos dados registrada nos logs no local.C:\Program Files\Druck\4Sight2\<<latest folder number>>\logs
"Failed to locate existing 4Sight2 service. Please ensure existing 4Sight2 version is installed on this machine and the service is running"	Esta falha acontece se o instalador não conseguir obter o estado do serviço".	A administração precisa garantir que o serviço 4Sight2 esteja pronto e funcionando
"Failed to start the 4Sight2 service. Please ensure the 4Sight2 service is present and running"	Falha ocorre se aplicativo estiver corrompido, alguns arquivos forem excluídos ou porta estiver em uso por outro aplicativo ou usuário tiver interrompido o serviço, etc.	Se o admin conseguir obter o estado do serviço e o sistema não estiver executando por qualquer razão (por exemplo, aplicativo corrompido, alguns arquivos excluídos ou porta em uso por outro aplicativo ou usuário interrompeu o serviço, etc.), o sistema tenta iniciar o serviço. Se o serviço não conseguir iniciar, a administração precisa entrar em contato com o suporte ao cliente para corrigir o problema.
"Upgrade of 4Sight2 application is supported from version 1.3 onwards. For earlier version upgrade support please contact Customer Care."	Não é possível atualizar se a versão instalada for anterior à versão 1.3.	A atualização só é possível a partir da versão 1.3 para uma versão posterior.
Installer has detected another minor version of PostgreSQL 11. Installer will not continue. Refer to 4Sight2 Installation manual for more details	O 4Sight2 não pode continuar a instalação do 4Sight2 porque a mesma versão (variante) do PostgreSQL já existe na máquina de destino.	Opções possíveis 1. Usuário pode escolher outra máquina. 2. Faça o backup do aplicativo existente que está usando o Postgres versão 11.3, desinstale e implante esse aplicativo em outra máquina. Desinstale o Postgres e reinicie a instalação do 4Sight2

Copyright 2020. Druck Ltd, a Baker Hughes business

Mensagem de Erro	Cenário	Correção/Ação necessária
Installation failed while upgrading database. Please reinstall 4Sight2. Refer to 4Sight2 Installation manual for more details	Pode ter ocorrido algum erro interno durante a atualização, o usuário pode tentar reinstalar	Se o problema persistir, o usuário pode compartilhar os logs de instalação para maior compreensão.

7.7 Causas Gerais de Erro

Apresentamos abaixo problemas comumente observados associados à comunicação do 4sight2 com o equipamento Druck via USB.

- A conexão física está frouxa ou instável
- Cabos/portas desgastados
- Adaptadores USB de má qualidade
- Portas/adaptadores USB sobrecarregados
- Os dispositivos permaneceram em funcionamento por muito tempo, o que fez com que eles entrassem em hibernação ou modo de suspensão.
- Dispositivos não estão no modos de Comunicação
- Software do driver não está instalado ou atualizado. Você precisa ter a mesma versão do aplicativo 4Sight2 e dos drivers para estabelecer comunicação com o hardware.
- Os dispositivos têm versões muito antigas de firmware.

7.8 Desinstalação do 4Sight2

Siga estas instruções se você precisar instalar uma nova cópia ou uma nova versão do 4Sight2, ou se precisar desinstalar o 4Sight2 devido a problemas ocorridos durante a instalação.

A desinstalação do componente de banco de dados PostgreSQL apaga o banco de dados 4Sight2 resultando em perda de dados. Um backup não será criado automaticamente seguindo esses passos, portanto certifique-se de que você criou um backup manual antes de prosseguir e salvou este backup em um local diferente da pasta de instalação do 4Sight2. Consulte a seção de backup e restauração do Banco de Dados Postgres deste manual.

Se você optar por desinstalar apenas o aplicativo 4Sight2 e manter o banco de dados, consulte a seção de instalação do 4Sight2 deste manual. Você precisará de credenciais de superusuário do banco de dados ao reinstalar. Não tente fazer uma desinstalação se você não possuir essas credenciais.

Se você quiser atualizar sua versão do 4Sight2 sem desinstalar o banco de dados, **NÃO** siga estas instruções.

1. Vá para Painel de Controle >> Aplicativos e Recursos.
2. Clique com o botão direito em 4Sight2 e selecione Desinstalar.
3. Siga as instruções do Assistente de Desinstalação.
4. Clique com o botão direito em PostgreSQL 11 e selecione Desinstalar.
5. Siga as instruções do Assistente de Desinstalação.

Copyright 2020. Druck Ltd, a Baker Hughes business

6. Desinstalar o PostgreSQL não exclui a pasta de dados. Você terá que fazer isso manualmente. Exclua a pasta de dados que pode ser encontrada em C:\Program Files\PostgreSQL\11\
   a. Se você quiser excluir a pasta inteira do PostgreSQL, certifique-se de que todos os arquivos de backup, scripts tenham sido removidos da pasta bin antes de prosseguir
   b. Por padrão, os backups do banco de dados 4Sight2 são criados e salvos neste local: C:\Arquivos de Programas\PostgreSQL\11\bin
7. É recomendável reiniciar o computador, se possível.
8. O 4Sight2 foi instalado com sucesso.

7.9 Solução de Problemas para Comunicação Segura

1. O comando 'nome do comando' não é reconhecido como um comando interno ou externo. Por exemplo, 'keytool' não é reconhecido como um comando interno ou externo,

- Se você receber um erro como este, isso significa que na pasta atual em que você está, o prompt de comando não pode encontrar referência ao comando especificado.

  Para resolver este erro, use o comando abaixo para apontar para a pasta correta.

  Set Path=%Path%;"<<caminho completo do local onde está o comando>>"

  Por exemplo, no erro acima relacionado com o keytool, você precisa definir o caminho para abaixo,

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

2. Bad IP address (Endereço IP com erro)

- Se você receber uma mensagem de erro com este texto, isso significa que o endereço IP ou o nome do host nos arquivos openssl-ca.cnf ou openssl-server.cnf estão incorretos. Nota: você pode precisar corrigir isso em vários lugares nestes arquivos e reexecutar os passos novamente.

3. No such file or directory...(Arquivou ou diretório não encontrado)

- Se você receber uma mensagem de erro com esse texto, isso significa que o comando que você executou provavelmente se refere a um nome de arquivo que não está correto. Verifique o comando para detectar erros de nomes de arquivos e também verifique se o arquivo com esse nome está presente na pasta e reexecute os comandos. Você pode ter que corrigir o nome do arquivo no comando ou seguir os passos para gerar os arquivos que faltam.
- Este erro pode ocorrer para arquivos index.txt e serial.txt porque, em certos casos, a extensão do arquivo é anexada ao nome duas vezes, por exemplo, intex.txt.txt.

  Basta editar o arquivo e salvá-lo sem a extensão .txt. Certifique-se de que o arquivo em uma extensão .txt.

Copyright 2020. Druck Ltd, a Baker Hughes business

Melhores Práticas

Copyright 2020. Druck Ltd, a Baker Hughes business

8. Melhores Práticas

Aumento da Resistência do Servidor

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

8.1 Tomcat

- Instale o Tomcat em uma pasta protegida, onde apenas o admin ou o LocalService tenha acesso, como *C:\Arquivos de Programas(x86)*
- Instale o Tomcat como um serviço em execução na conta LocalService.
- Remova tudo do WebApp, remova os aplicativos indesejados padrão.
- Substitua a página de erros padrão, tais como 404, 403, 500 etc
- Aplique HTTPS, habilite SSL.
- O aplicativo de gerenciamento deve ser executado em SSL.
- Arquivo de log individual do usuário para cada aplicação web.
- Remova o banner do servidor.
- Habilite o log de acesso.
- Altere a porta e o comando de desligamento.

8.2 PostgreSQL

- Todas as contas de alto privilégio como pgdba, postgres, depesz devem ser permitidas apenas para login local.
- Verifique se a sequência está correta no arquivo pg-hba.conf para que os usuários corretos tenham acesso correto.
- Configure o pg-hba.conf para que o servidor possa ser conectado somente a partir da máquina local, e não através da rede.

8.3 Melhores Práticas de Firewall

Apresentamos a seguir algumas das melhores práticas de firewall recomendadas para uso com o 4Sight2:

8.3.1 Política

1. A configuração do Firewall deve ser consistente com a Política de Segurança da Organização.
2. Use sempre a Política de Menos Privilégios. Por padrão, negue todos os privilégios. Permita tráfego específico (utilizando origem, destino e porta).
3. Estabeleça regras específicas primeiro e utilize regras explícitas de suspensão.
4. Registre todas as ações, especificamente tentativas falhas para trilha de auditoria.

8.3.2 Recursos

1. Monitore a utilização de memória
2. Monitore a utilização da CPU
3. Monitore a utilização da largura de banda.
4. Limitar o número de aplicativos em execução na máquina Firewall

Copyright 2020. Druck Ltd, a Baker Hughes business

8.3.3 Instalação e Manutenção

1. Limite o número de aplicativos em execução na máquina Firewall.
2. Use uma ID de usuário única para administração.
3. Siga uma política de conta rígida na máquina.
4. Aplique regularmente os patches de sistemas operacionais, aplicativos, firmware, etc.
5. Arquive base de regras, configuração e logs regularmente. Documente todas as regras e alterações feitas em um controle de fontes.
6. Execute autotestes.
7. Remova a regra não utilizada quando um serviço for desativado.
8. Faça auditorias e revise as regras regularmente.
9. Orientação de segurança monitorada regularmente

8.3.4 Segurança Adicional

1. Utilize inspeções stateful.
2. Utilize Proxies
3. Utilize inspeção e filtragem por Aplicação.

8.3.5 Proteção Interna

1. Tem uma política de uso aceitável
2. Firewall Pessoal para cada usuário
3. Prevenção de invasão baseada em host
4. Monitoramento da Rede
5. Filtragem de Conteúdo
6. Controle de acesso em cada computador e aplicativo.

Copyright 2020. Druck Ltd, a Baker Hughes business

Localizações de Escritório

Matrizes

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

Alemanha

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

Austrália

Springfield Central
Telefone: 1300 171 502
Email: custcare.au@ge.com

China

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

China

Pequim
Telefone: +86 180 1929 3751
Email: fan.kai@bakerhughes.com

China

Xangai
Telefone +86 135 6492 6586
Email: hensen.zhang@bakerhughes.com

EUA

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

França

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

Holanda

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

Índia

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

Itália

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

Japão

Tóquio
Telefone: +81 3 6890 4538
Email: gesitj@bakerhughes.com

Rússia

Moscou
Telefone: +7 915 3161487
Email: aleksey.khamov@bakerhughes.com

UAE

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

Localizações de Serviço e Suporte

Suporte Técnico

Global
Email: mstechsupport@bakerhughes.com

Brasil

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

China

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

EUA

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

França

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

Índia

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

Japão

Tóquio
Telefone: +81 3 3531 8711
Email: service.druck.jp@bakerhughes.com

Reino Unido

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

UAE

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

Copyright 2020 Druck, Baker Hughes Business. Este material contém uma ou mais marcas registradas da Baker Hughes Company e suas subsidiárias em um ou mais países. Todos os nomes de produtos e empresas de terceiros são marcas registradas de seus respectivos proprietários.
123M3140. Revisão F | Português (Brasil)

Baker Hughes