Druck

4Sight2

Logiciel de gestion d'étalonnage

Guide d'installation 123M3140 Révision F

Table des matières

1. Introduction

Le logiciel d'étalonnage 4Sight2 est un outil Web de gestion de l'étalonnage destiné à vous faciliter l'administration et le contrôle de votre environnement d'étalonnage selon les normes de métrologie les plus rigoureuses. Vous pouvez utiliser le logiciel pour les tâches suivantes :

- Gérer l'étalonnage de tous les appareils de mesure sur un emplacement spécifique de l'entreprise
- Définir un programme des travaux d'étalonnage à destination des techniciens
- Échanger les données avec les étalonneurs portatifs Druck (DPI620, DPI620 Genii, DPI611 et DPI612) qui disposent de fonctions de communication USB
- Gérer l'historique d'étalonnage des appareils qui ne sont pas pris en charge par un étalonneur portatif (saisie manuelle des données)
- Examiner vos historiques d'étalonnage. Vous pouvez aussi tenir un registre permanent de chaque certificat d'étalonnage. Par exemple : Pour les procédures de contrôle qualité ISO 9000.
- Piloter les étalonnages automatisés à l'aide des contrôleurs de pression Druck (PACE 1000, 5000 et 6000), des étalonneurs portatifs (DPI620 Genii, DPI611 et DPI612) et des étalonneurs de température (DryTC165, DryTC 650, LiquidTC165 et LiquidTC255)

1.1 Public visé

1.1.1 Administrateur

L'administrateur est chargé de l'installation et de la configuration du logiciel 4Sight2. Après la première installation de 4Sight2, il existe un seul compte administratif. Ce compte peut créer de nouveaux utilisateurs et affecter des groupes/ensembles de droits. Les utilisateurs administratifs ont des droits de lecture et d'écriture sur toutes les fonctionnalités de 4Sight2.

1.1.2 Superviseur

Un superviseur est chargé de la gestion des équipements et de leur étalonnage. Il peut créer et mettre à jour les actifs dans l'entreprise 4Sight2, notamment les usines, emplacements, tags et appareils. Il est chargé de rattacher aux actifs les documents tels que les process d'usine ou les fiches techniques d'appareil. Le superviseur peut créer des procédures d'essai à utiliser pendant l'étalonnage, et aussi planifier des procédures et surveiller l'état des appareils. Les superviseurs disposent des droits nécessaires pour approuver les étalonnages.

1.1.3 Technicien

Le technicien est chargé de réaliser les étalonnages. Les étalonnages peuvent être portatifs, manuels ou automatisés, et c'est au technicien qu'il incombe de réaliser le type d'étalonnage pertinent sur un appareil donné. Une fois qu'un étalonnage a été réalisé, le technicien peut en examiner les résultats et achever les étalonnages qui seront ensuite approuvés par un superviseur.

1.1.4 Auditeur

Un auditeur est chargé d'inspecter les rapports. Il se peut que, dans certaines usines, les audits doivent obligatoirement être menés par un auditeur.

2. Configuration système requise

La configuration minimum requise pour installer l'application 4Sight2 dans des machines serveur et client est la suivante :

2.1 Serveur d'application

Système d'exploitation	Windows 10, Windows Server 2012 R2, Windows Server 2016, Windows Server 2019
Mises à jour	Toutes les mises à jour Windows totalement installées
Processeur	Quadricoeur
Mémoire RAM	8 Go ou plus (32 Go recommandé)
Espace disque	1 To
Vitesse réseau	10Mbps

2.2 Poste de travail client

Système d'exploitation	Windows 10, Windows Server 2012 R2, Windows Server 2016, Windows Server 2019
Navigateur	Google Chrome V80+, Microsoft Edge V80, Firefox V74
Adobe Reader	Adobe Acrobat Reader DC version 2015.017.20050 +
Mémoire RAM	8 Go ou plus
Processeur	Bicoeur
Espace disque	600 Go
Vitesse réseau	10Mbps

2.3 Installation locale

Système d'exploitation	Windows 10, Windows Server 2012 R2, Windows Server 2016, Windows Server 2019
Mises à jour	Toutes les mises à jour Windows totalement installées
Adobe Reader	Adobe Acrobat Reader DC version 2015.017.20050 +
Processeur	Bicoeur
Mémoire RAM	16 Go ou plus (32 Go recommandé)
Espace disque	500 Go ou plus
Navigateur	Google Chrome V80+, Microsoft Edge V80, Firefox V74

2.4 Firmware 4Sight2 pris en charge

Pour les dernières informations sur les micrologiciels pris en charge, consultez le lien ci-dessous:
https://www.bakerhughes.com/druck/test-and-calibration-instrumentation/calibration-management-software-4sight2

ou

Pour PACE, insérez l'USB B pour la communication 4Sight2 comme indiqué dans l'image ci-dessous:

Installation de 4Sight2

3. Installation de 4Sight2

Pour installer 4Sight2, copiez d'abord le fichier d'installation zip de 4Sight2 sur votre bureau puis décompressez ce fichier. Dans le fichier d'installation, sélectionnez le fichier exécutable 4Sight2.

Remarque : Les logiciels antivirus ci-après sont utilisés pour les installations de 4Sight2 et du serveur de communication :

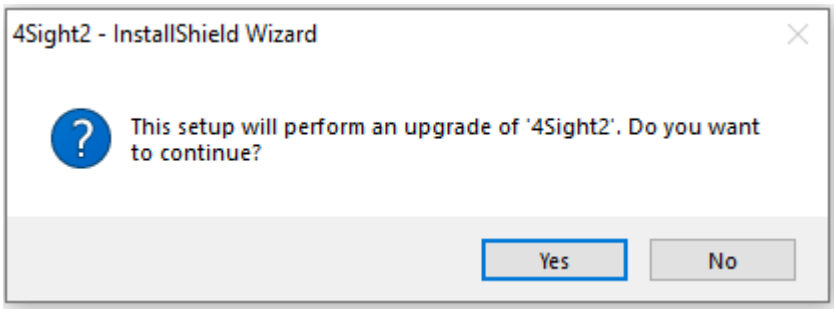
- McAfee VirusScan Enterprise + AntiSpyware Enterprise numéro de version : 8.8.0
- Symantec Endpoint Protection numéro de version : 14.3.558

Une fois que vous avez exécuté le fichier exécutable de configuration, l'assistant InstallShield démarre. L'assistant InstallShield réalise l'installation de 4Sight2 en deux temps :

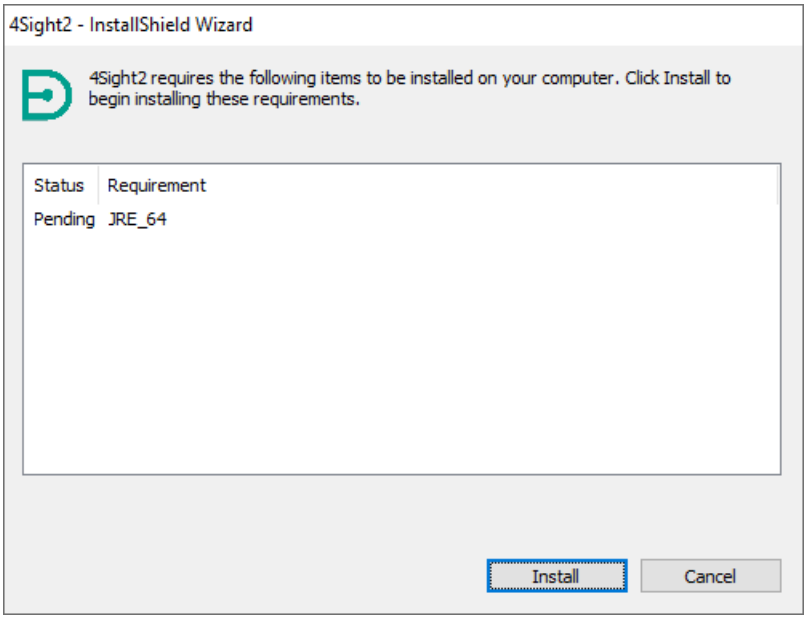
1. Installation de la base de données
2. Installation de l'application Web

Suivez les instructions affichées par l'assistant InstallShield ou consultez les deux sections ci-après pour être guidé dans le processus d'installation.

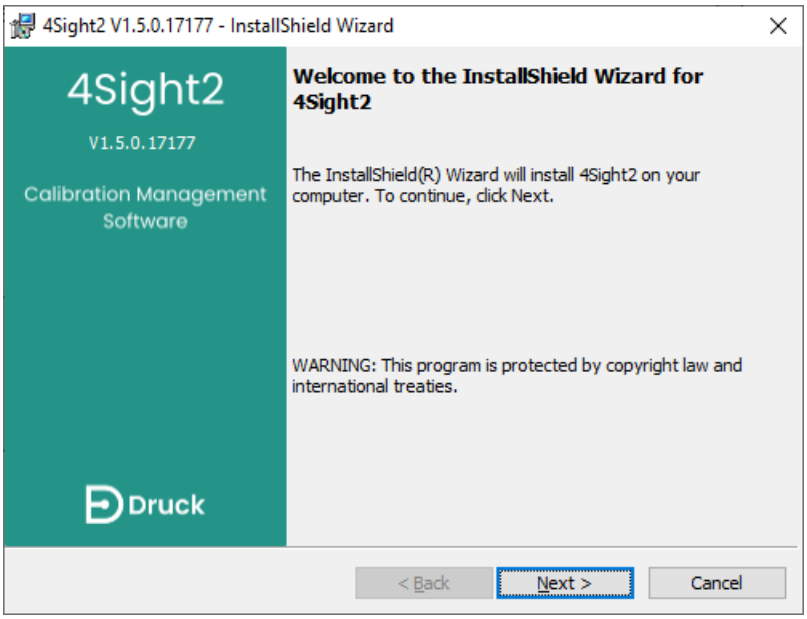
1. Si 4Sight2 est déjà installé sur la machine, l'assistant d'installation vous invite à procéder à une mise à niveau vers une version récente. Cliquez sur **Yes** (Oui) pour mettre à niveau.



2. S'il s'agit de la première installation de 4Sight2 sur la machine, l'assistant d'installation affiche l'écran ci-dessous. Sélectionnez **Install** (Installer) ; les éléments répertoriés qui sont affichés seront installés.



3. Une fois l'installation des éléments prérequis terminée, l'écran de bienvenue de l'assistant InstallShield s'affiche. Cliquez sur **Next** (Suivant) pour poursuivre.



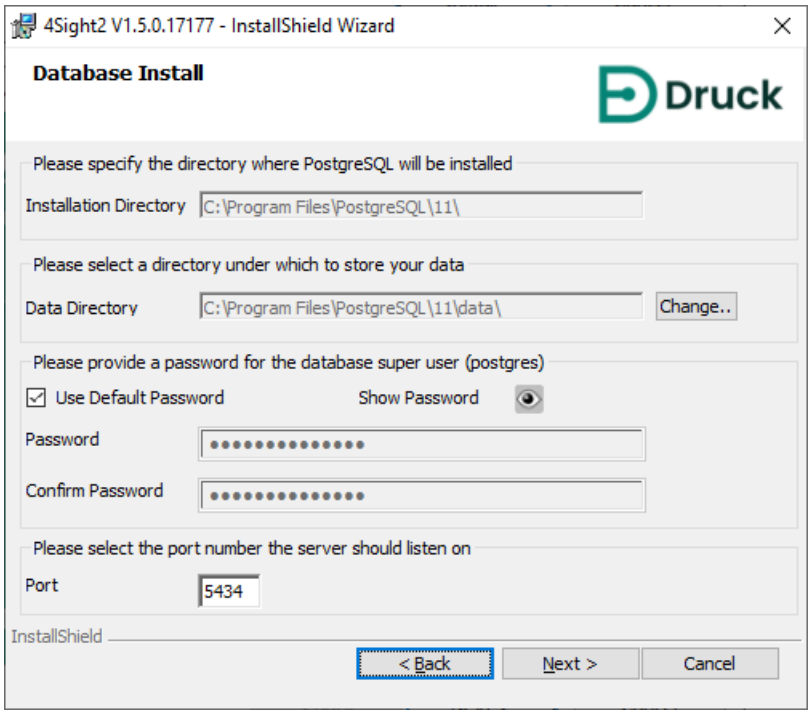
3.1 Installation de la base de données

L'application 4Sight2 utilise une base de données PostgreSQL. Les instructions ci-dessous expliquent comment installer la base de données PostgreSQL et que faire si une base de données PostgreSQL est déjà installée.

3.2 Installation de PostgreSQL

Suivez la procédure ci-après s'il n'y a pas de base de données PostgreSQL installée sur la machine.

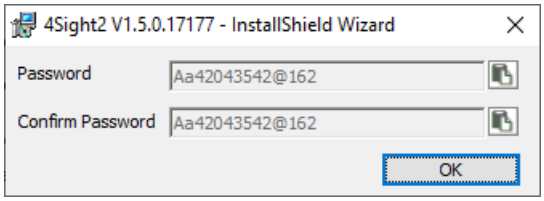
1. S'il n'y a pas d'instance de la base de données PostgreSQL installée sur la machine, l'assistant d'installation affiche l'écran ci-dessous.



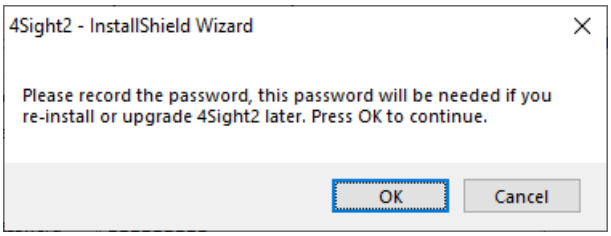
Installation Directory (Répertoire d'installation) : Sélectionnez le répertoire dans lequel l'application PostgreSQL peut être installée.
Data Directory (Répertoire de données) : Sélectionnez le répertoire dans lequel la base de données PostgreSQL peut être stockée.
Password/Confirm Password (Mot de passe/Confirmer mot de passe) : Saisissez le mot de passe du super-utilisateur de la base de données PostgreSQL. Cette invite est uniquement affichée à la première installation de la base de données PostgreSQL.
Remarque : Ce mot de passe sera requis pour accéder au contenu de la base de données après l'installation.
Port : C'est l'adresse du port auquel la base de données PostgreSQL répond aux requêtes de l'application.

Remarque : Si le numéro du port est déjà occupé, contactez le service informatique. L'utilisateur peut aussi changer le numéro du port, dont il faut prendre note en vue du lancement ultérieur de l'application.

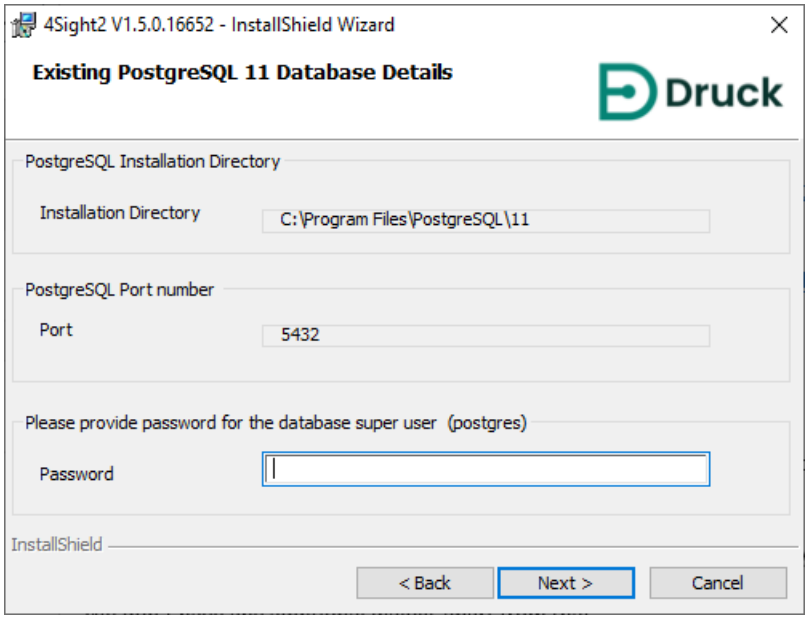
Important : L'utilisateur doit prendre note du mot de passe de la base de données. La perte du mot de passe peut donner lieu à un refus d'accès ou à la perte de données. Décochez la case User Default Password (Mot de passe utilisateur par défaut) pour actualiser le mot de passe du super utilisateur de la base de données. Si vous souhaitez conserver le mot de passe par défaut ou voir le nouveau mot de passe saisi, sélectionnez l'icône (Afficher mot de passe). Pour copier le mot de passe sur le presse-papier, utilisez l'icône (Copier sur presse-papier).



Le programme d'installation vous invitera de nouveau à prendre note du mot de passe. Sélectionnez **OK** lorsque vous avez pris note du mot de passe.

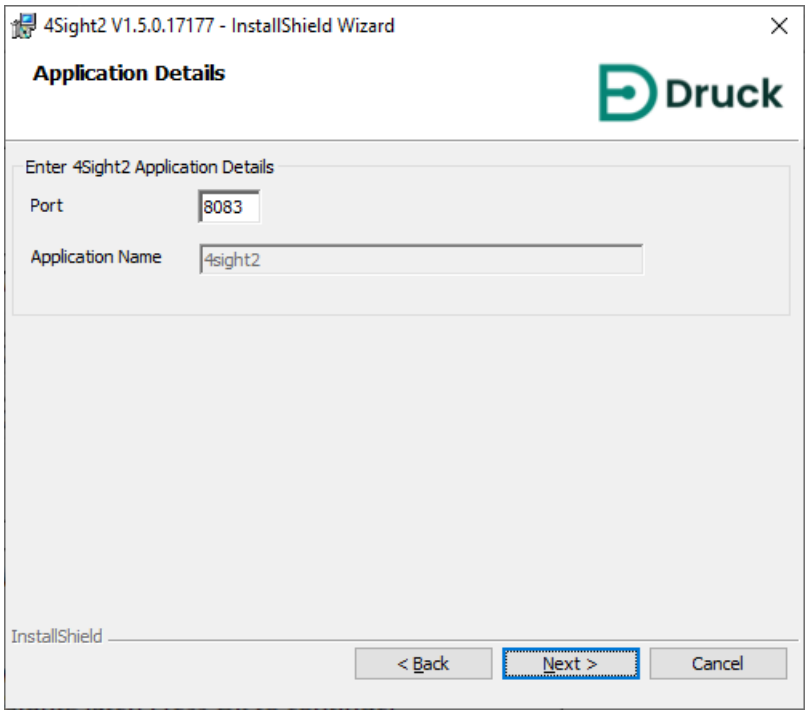


2. Cette étape est présentée à l'utilisateur uniquement dans le cas où la base de données PostgreSQL est déjà installée.



Répertoire d'installation : Il s'agit du chemin d'accès à la base de données PostgreSQL déjà installée. C'est une information à lecture seule.
Mot de passe : Il s'agit de confirmer le mot de passe du super-utilisateur de la base de données PostgreSQL.
Port : Il s'agit d'indiquer le numéro du port qu'utilise la base de données PostgreSQL pour exécuter la requête db.

3. Dans la fenêtre Application Details (Détails de l'application), saisissez les informations ci-après

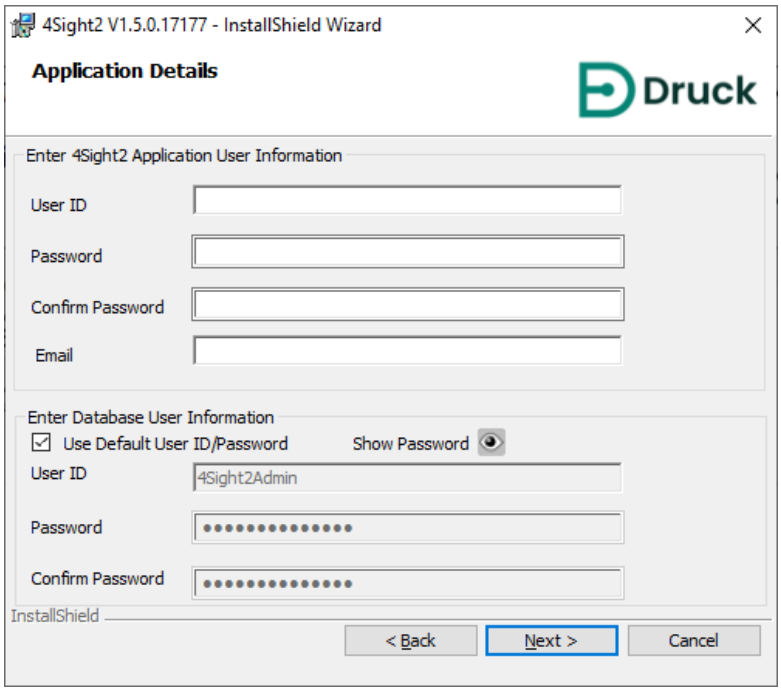


Port : Saisissez le port du serveur Web Tomcat qui est utilisé par l'application Web 4Sight2 pour répondre aux requêtes HTTP.

Application Name (Nom d'application) : Saisissez le chemin de contexte de l'application que vous utiliserez pour vous connecter à l'application 4Sight2 dans votre navigateur. Il s'agit de 4sight2, par défaut.

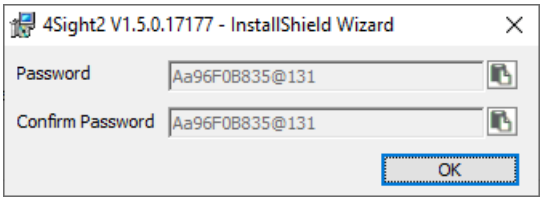
Remarque : Si le numéro du port est déjà occupé, contactez le service informatique. L'utilisateur peut aussi changer le numéro du port, dont il faut prendre note en vue du lancement ultérieur de l'application.

4. Sélectionnez **Next** (Suivant) ; l'écran d'information sur l'utilisateur de l'application s'affiche.

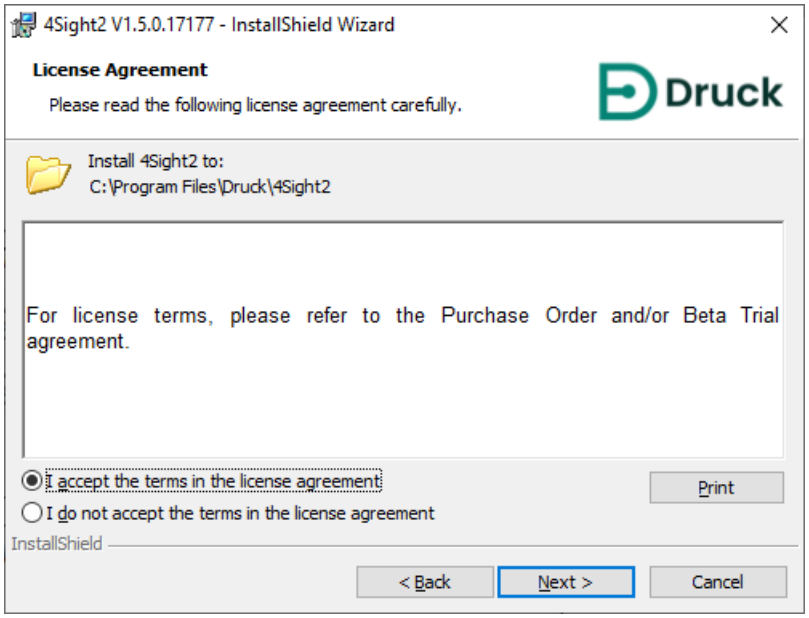


Informations d'utilisateur de l'application : Cette section concerne la saisie du nom et du mot de passe du super-utilisateur permettant d'accéder à l'application 4Sight2.
Remarque : Ce mot de passe sera requis pour accéder à l'application 4Sight2 après l'installation.
Informations d'utilisateur de la base de données : Cette section concerne la saisie du nom et du mot de passe d'utilisateur de la base de données, qui sera utilisé par l'application 4Sight2 pour communiquer avec la base de données PostgreSQL.

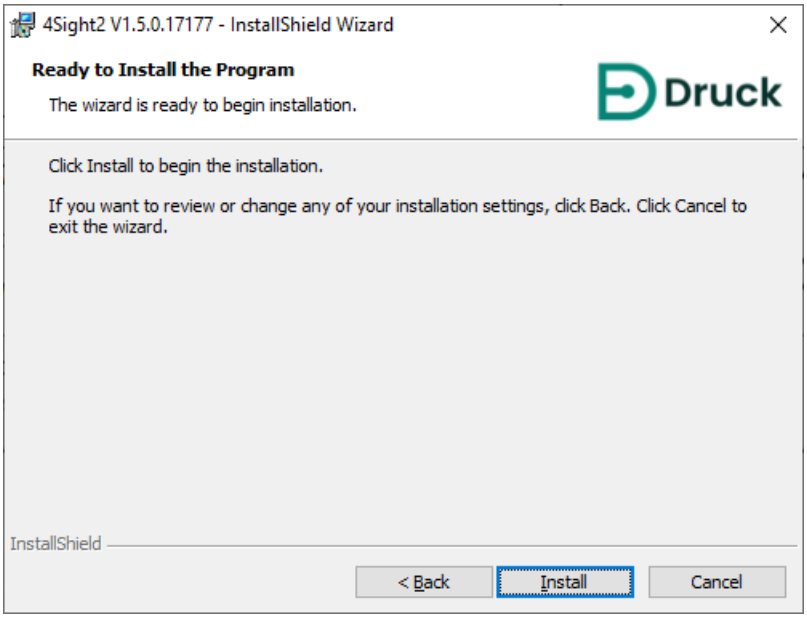
Important : L'utilisateur doit prendre note du mot de passe de la base de données. La perte du mot de passe peut donner lieu à un refus d'accès ou à la perte de données. Décochez la case User Default Password (Mot de passe utilisateur par défaut) pour actualiser le mot de passe du super utilisateur de la base de données. Si vous souhaitez conserver le mot de passe par défaut ou voir le nouveau mot de passe saisi, sélectionnez l'icône (Afficher mot de passe). Pour copier le mot de passe sur le presse-papier, utilisez l'icône (Copier sur presse-papier).



5. Après avoir lu les termes et conditions d'utilisation de la licence, cochez la case « J'accepte les conditions d'utilisation de la licence. » puis cliquez sur **Suivant**.

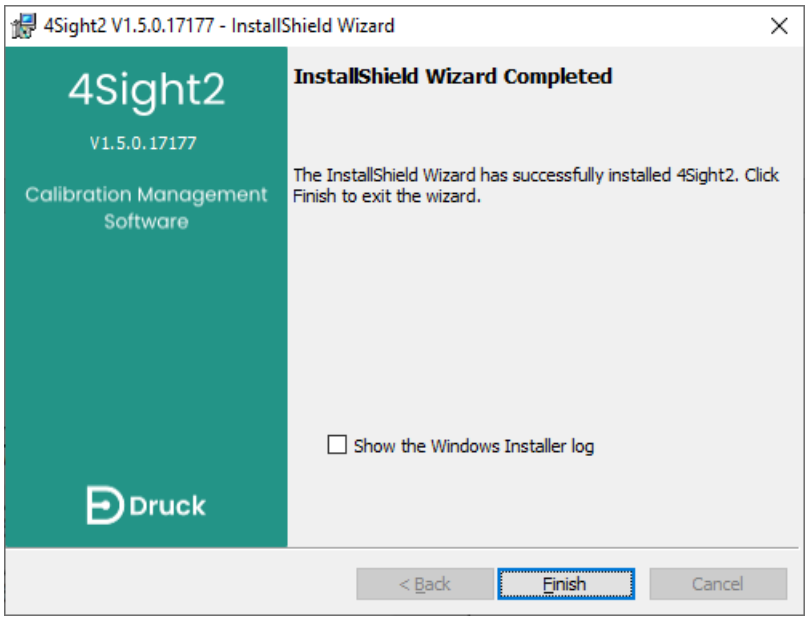


6. Cliquez sur **Installer** pour commencer l'installation. Tous les logiciels associés à l'application 4Sight2 et à la base de données seront installés.



Félicitations ! L'application 4Sight2 est maintenant installée.

7. Appuyez sur le bouton **Terminer** pour fermer la fenêtre et suivez les instructions figurant à la section suivante pour vous connecter à l'application 4Sight2.



Pour vous connecter à 4Sight2 sur le serveur local, allez à

http://NomOrdinateur ou AdresseIP:NoPort/NomApplication

- **NomOrdinateur –** Le nom du PC sur lequel l'application 4Sight2 est installée. Pour le localiser, faites un clic droit sur Ordinateur puis sélectionnez Propriétés.
- **IPAddress** – L'adresse IP du PC sur lequel l'application 4Sight2 a est installée. Pour le localiser, exécutez 'ipconfig' dans une invite de commande Windows.
- **NoPort –** Le numéro qui a été saisi dans le champ du numéro du port Tomcat pendant l'installation de l'application.
- **NomApplication –** Le nom qui a été saisi dans le champ du nom de l'application pendant l'installation de l'application.

Installation du communicateur d'appareil de test 4Sight2

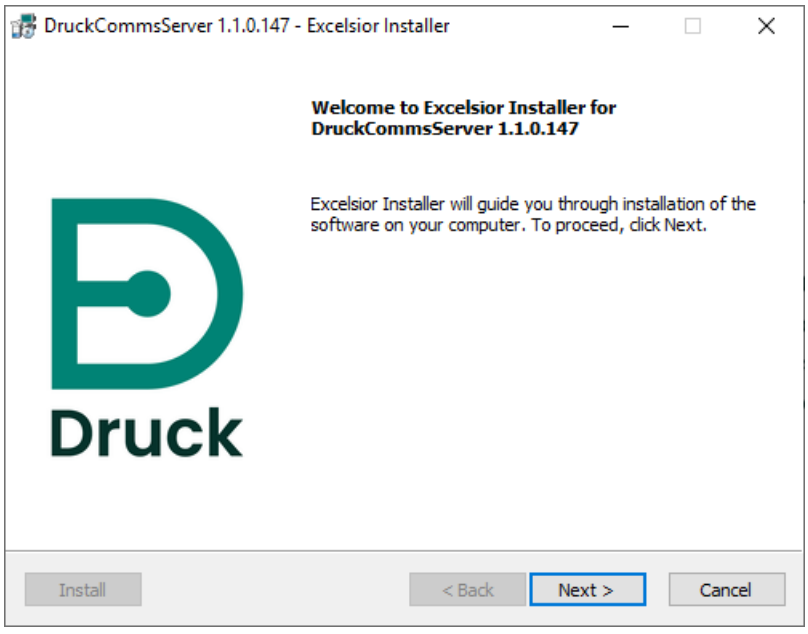
4. Installation du communicateur d'appareil de test 4Sight2

1. Le communicateur d'appareil de test permet à vos instruments Druck de communiquer avec l'application 4Sight2. Il peut soit être installé à partir du dossier d'installation de 4Sight2 soit être téléchargé via la communication initiale d'appareil 4Sight2. Si le communicateur d'appareil de test n'est pas disponible dans le fichier d'installation, procédez comme suit lorsque l'application 4Sight2 est ouverte et qu'une gamme a été créée : allez à Calibration > Portable (Étalonnage > Portatif) à l'aide du menu 4Sight2 en tant qu'utilisateur administratif, consultez le guide d'utilisation de 4Sight2 pour de l'aide sur la navigation et la création d'une gamme. Sélectionnez le bouton d'actualisation à côté de la liste déroulante des appareils de test. Si le communicateur d'appareil de test n'est pas en cours d'exécution, vous verrez le message suivant :

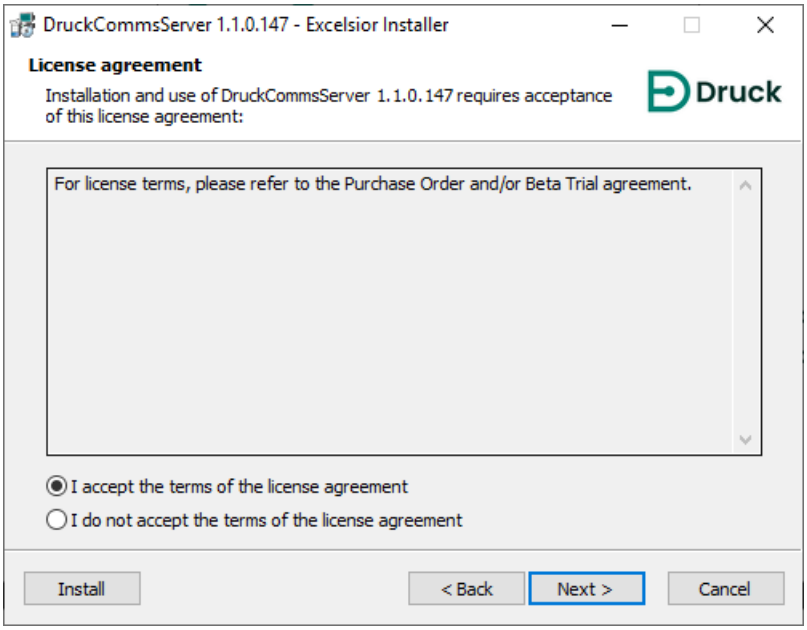
   Impossible de communiquer avec l'appareil de test

   Transférez le pack logiciel du communicateur d'appareil de test. Après le transfert, décompressez le pack et exécutez le fichier d'installation setup.exe. Pour les consignes d'installation et le dépannage en cas de problème d'installation, consultez le guide d'installation. Pour de l'aide, veuillez contacter l'administrateur.

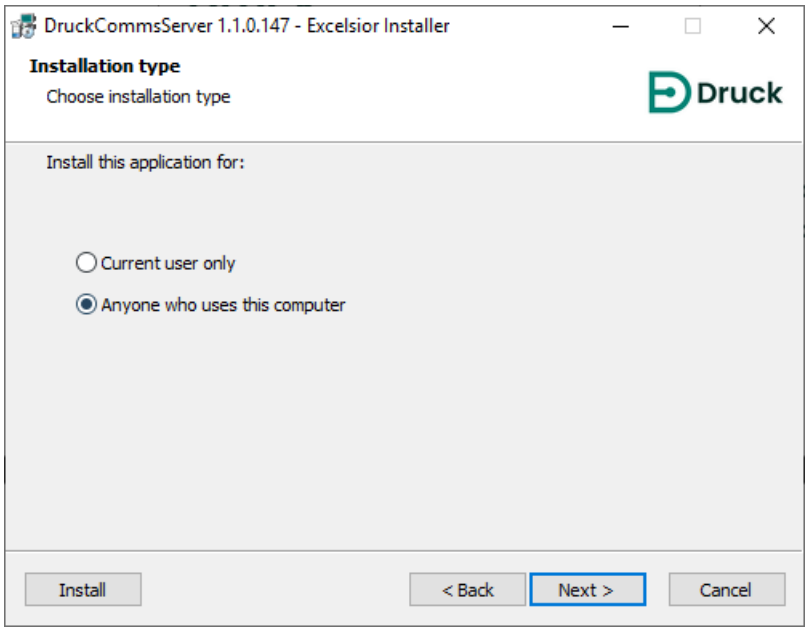
2. Sélectionnez **Download** (Télécharger) pour obtenir le fichier d'installation du communicateur d'appareil de test.
3. Les fichiers d'installation du communicateur d'appareil de test s'affichent sous la forme d'un fichier compressé CommsServerInstall Zip. Une fois le fichier Comms Server Zip téléchargé, procédez comme suit, que ce soit avant ou après l'installation de 4Sight2.
4. Extrayez les fichiers du fichier Comms Server Zip et double-cliquez sur le fichier setup.exe pour exécuter le programme d'installation.
5. Le programme d'installation DruckCommsServer s'affiche. Suivez les instructions affichées par le programme d'installation ou celles indiquées dans ce guide.



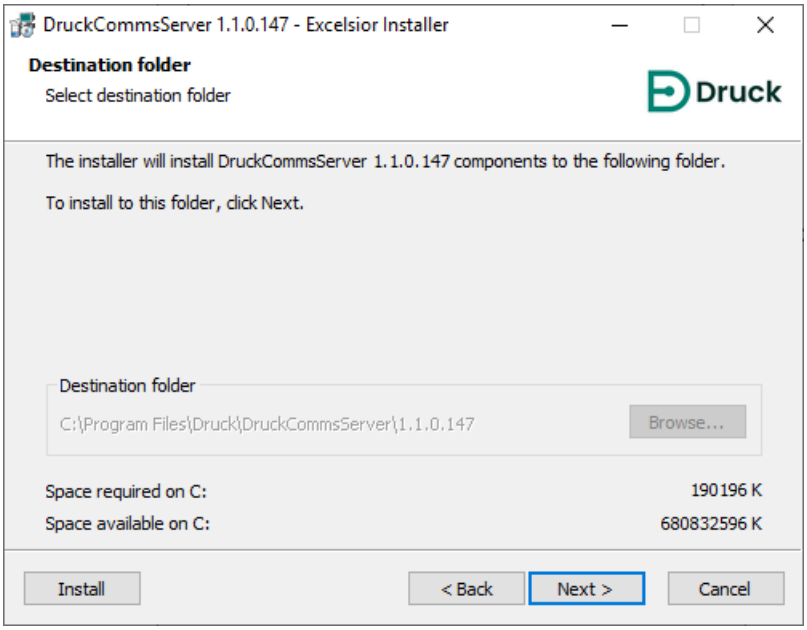
6. Sélectionnez **Next** (Suivant) pour afficher l'écran du contrat de licence, lisez attentivement les modalités, puis sélectionnez **I accept the terms of the license agreement** (J'accepte les modalités du contrat de licence) et **Next** (Suivant) pour continuer.



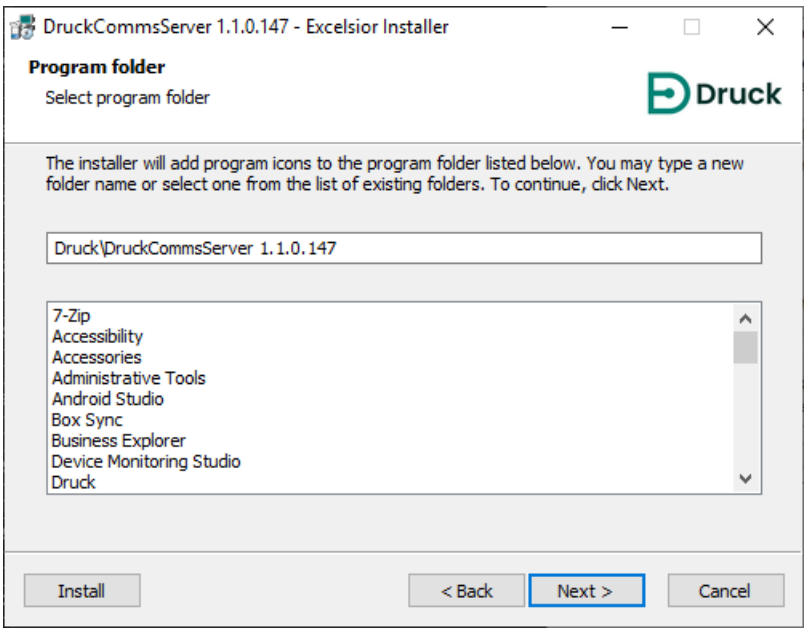
7. À l'écran du type d'installation (Installation type), indiquez si vous souhaitez installer CommsServer pour tous les utilisateurs de ce PC ou seulement pour l'utilisateur actuel.



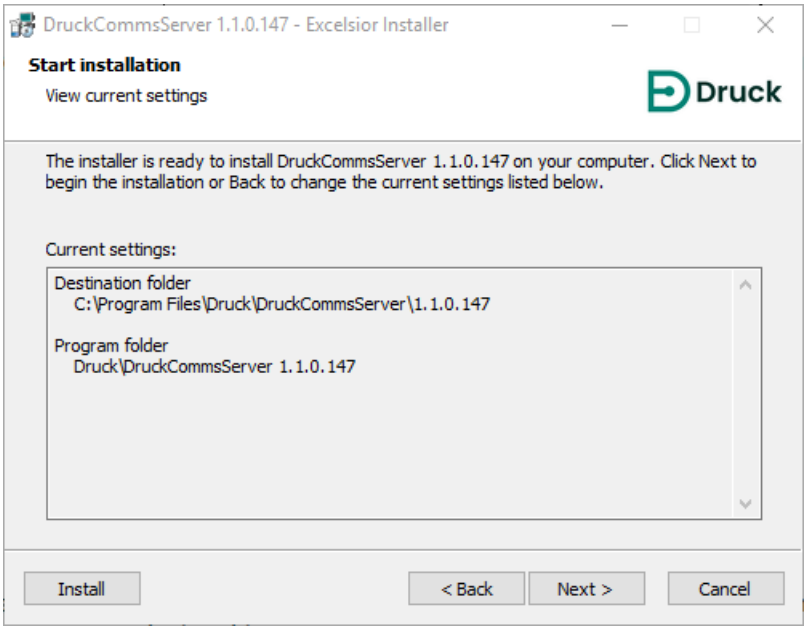
8. L'écran du dossier de destination (Destination folder) indique le dossier dans lequel DruckCommsServer sera installé. Par défaut, il s'agit de C:\Program Files\Druck\DruckCommsServer\[version_application]



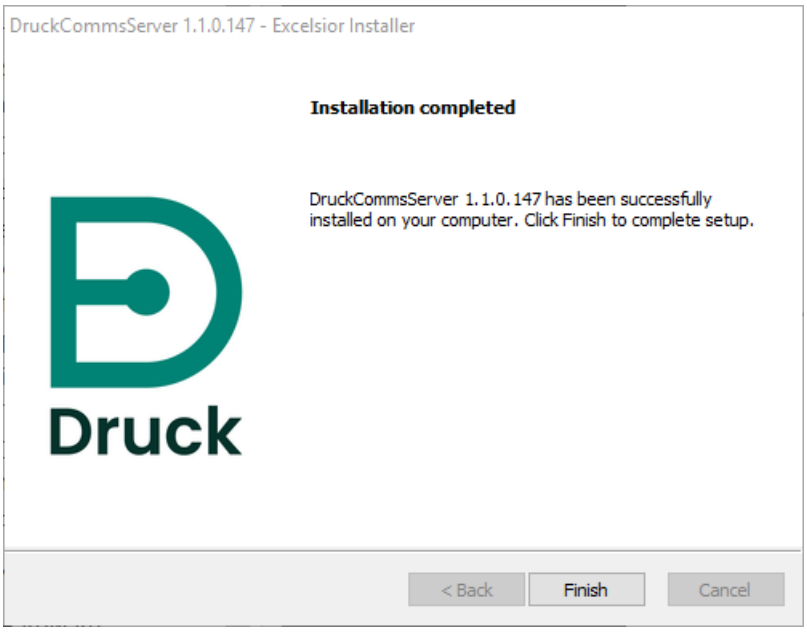
9. L'écran du dossier de programme (Program Folder) vous permet de choisir l'endroit où le programme d'installation ajoute l'icône de programme au dossier de programmes.



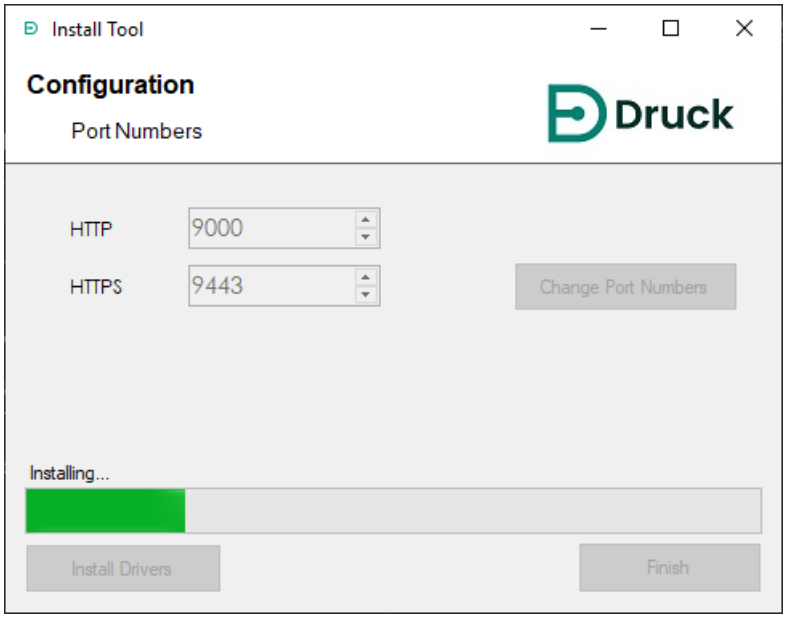
10. L'écran de démarrage de l'installation (Start installation) s'affiche ensuite ; sélectionnez **Next** (Suivant) pour démarrer l'installation.



11. Une fois que l'installation est terminée, cliquez sur **Finish** (Terminer).

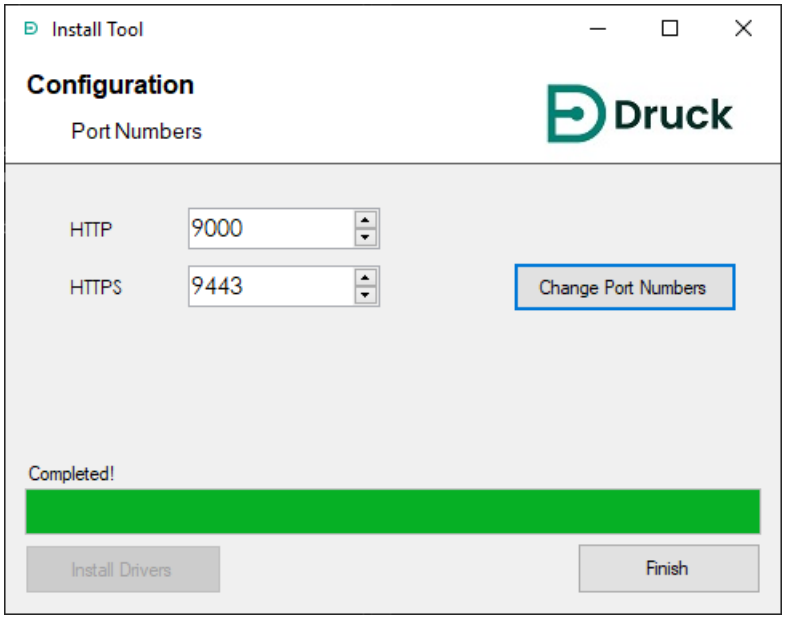


12. L'outil d'installation (Install tool) de CommsServer s'affiche ensuite pour installer les pilotes supplémentaires qui sont nécessaires.



13. Si vous n'êtes pas certain qu'un numéro de port de substitution est utilisé par 4Sight2, veuillez contacter l'utilisateur administratif.

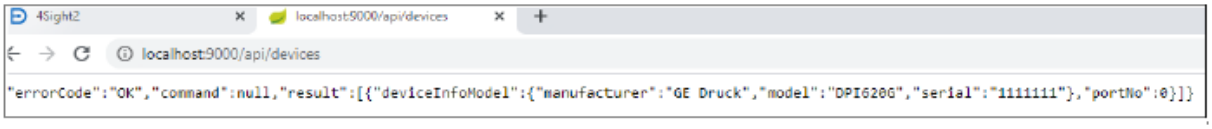
Remarque : L'outil d'installation peut être exécuté séparément après l'installation afin de reconfigurer ces numéros de port.



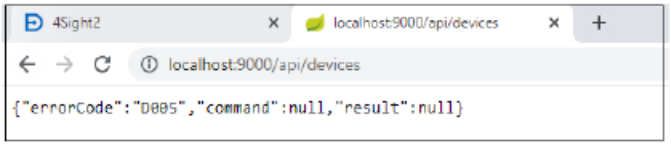
14. Testez l'installation du communicateur d'appareil de test en tapant l'adresse URL ci-après dans votre navigateur Internet :

    http:/localhost:[numéro de port http utilisé plus haut, 9000 par défaut]/api/devices

Le navigateur Internet doit afficher la liste de tous les appareils que vous avez connectés :



En l'absence d'appareils connectés, le message suivant s'affiche :



Remarque : Les pilotes nécessaires aux étalonneurs de température ne seront pas configurés automatiquement. Voir section 4.3 Configuration de pilote pour l'étalonneur de température

15. Si l'installation du pilote d'appareil a réussi, procédez comme indiqué à la section suivante pour configure manuellement les pilotes nécessaires.

4.1 Configuration manuelle des pilotes

Les paramètres de politique de sécurité informatique peuvent empêcher les pilotes Druck de se configurer automatiquement lors de l'installation. Cette volonté être apparent si 4Sight2 est incapable de communiquer avec les différents équipements. Pour plus d'informations,

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

ou

Pour résoudre ce problème, configurez manuellement les pilotes Druck. Veuillez consulter votre représentant informatique local si vous avez des doutes sur la façon de procéder et avez besoin d'assistance.

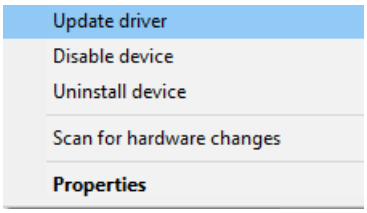
4.1.1 Conditions préalables

Pour installer les pilotes, vous devez avoir l'application 4Sight2 installée ou accessible sur ou depuis la machine. Avant de tenter d'installer les pilotes, vérifiez que vous pouvez accéder à l'application 4Sight2 depuis l'ordinateur.

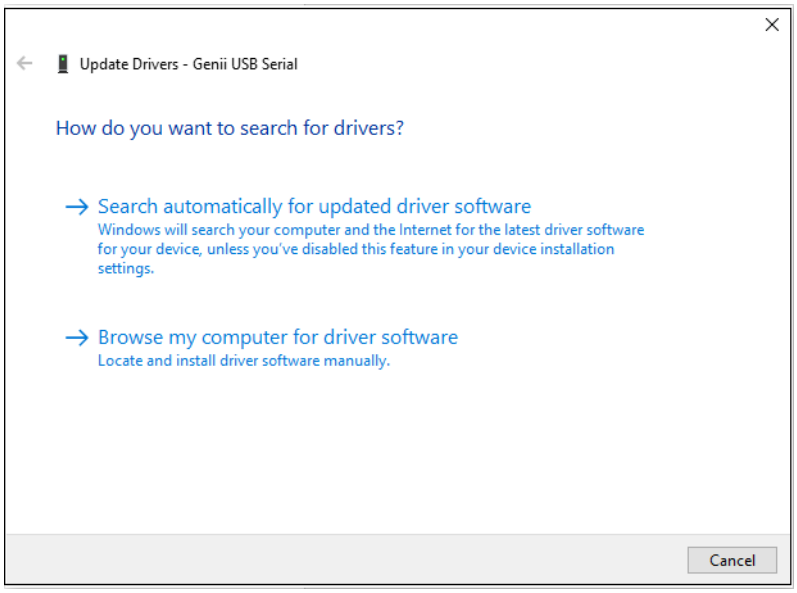
Pour installer manuellement le pilote, procédez comme suit :

1. Sur le bureau, recherchez le Gestionnaire de périphériques et exécutez-le.

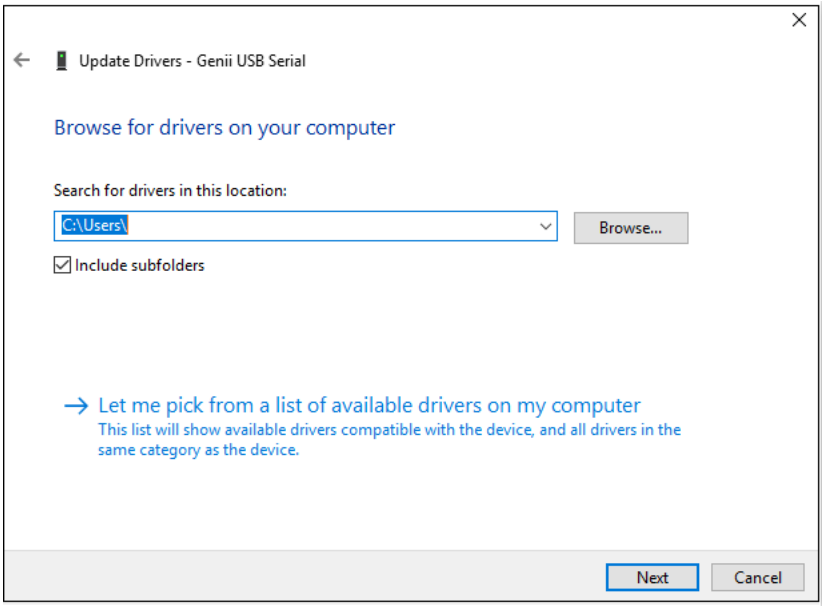
2. Faites défiler la liste des périphériques USB pour trouver ceux qui ne sont pas configurés (Périphérique inconnu ou Autres périphériques). Faites un clic droit et sélectionnez **Mettre à jour le pilote...**.



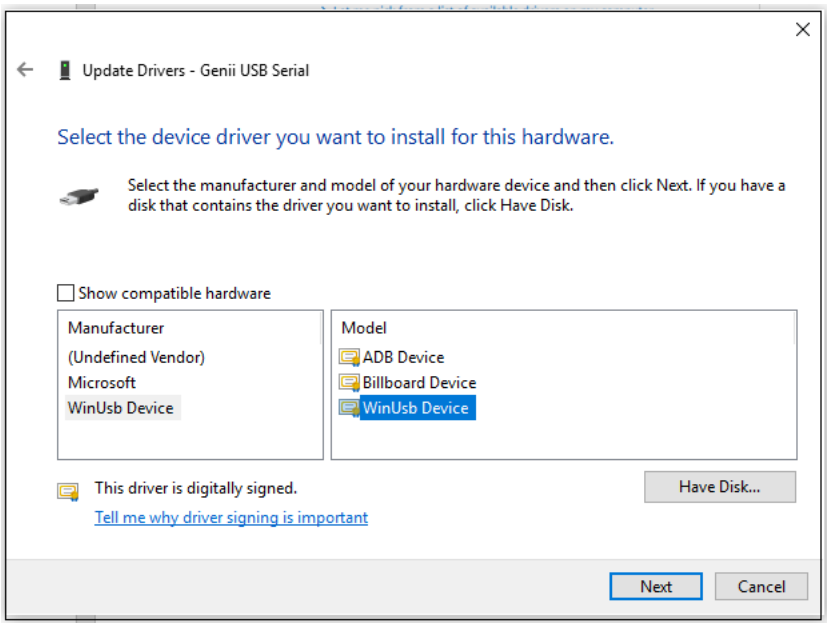
3. Sélectionnez **Rechercher un pilote sur mon ordinateur**.



4. Sélectionnez **Choisir parmi une liste de pilotes sur mon ordinateur**.

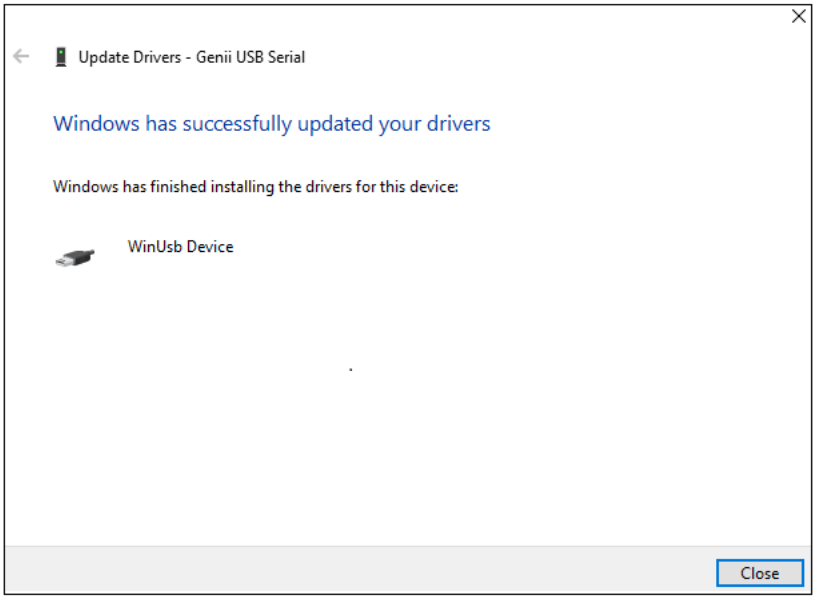


5. Décochez **Afficher les matériels compatibles** et sélectionnez **WinUsb Device** comme Fabricant et **WinUsb Device** comme Modèle.



6. L'avertissement suivant s'affiche. Cliquez sur **Oui**.

7. Le message indiquant que Windows a correctement mis à jour les pilotes s'affiche.

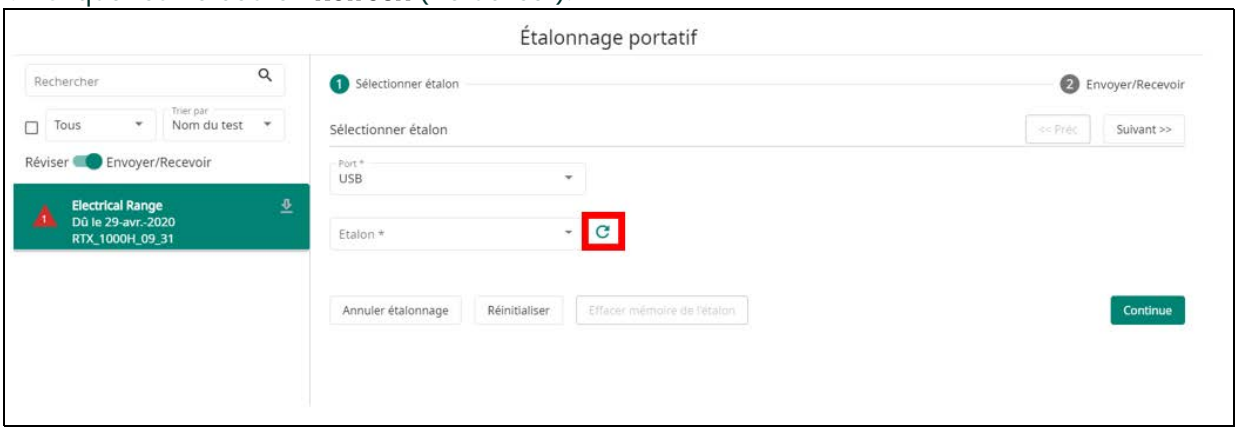


Renouvelez les étapes ci-dessus pour chaque catégorie d'appareil que vous connectez pour la première fois.

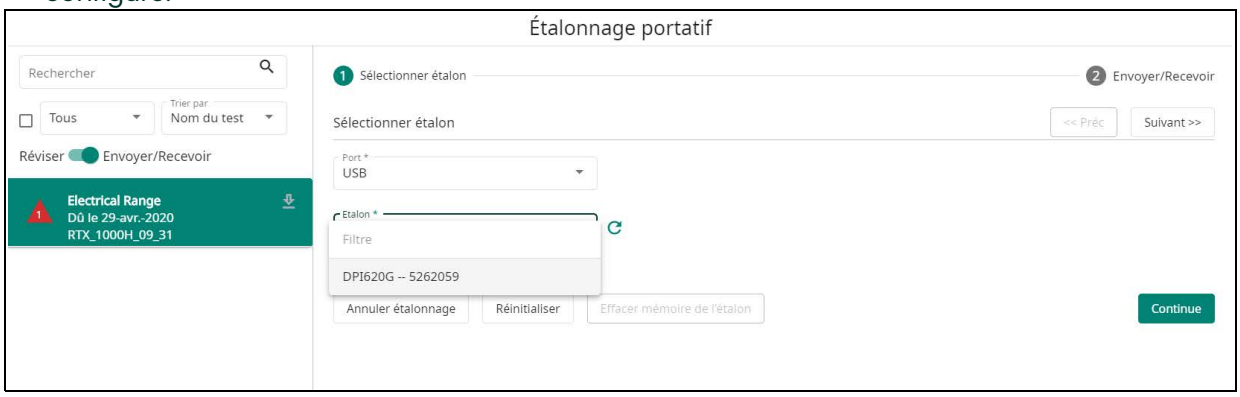
Par exemple, si vous connectez un PACE et un Genii pour la première fois, il se peut que vous deviez réaliser la démarche ci-dessus séparément pour le PACE et le Genii. Par la suite, tous les appareils PACE et Genii doivent fonctionner sans avoir à effectuer ce paramétrage préalable. Mais, si vous connectez ultérieurement une autre catégorie d'appareil comme un DPI611/612, il vous faudra renouveler l'opération pour cette catégorie d'appareil.

4.2 Test du communicateur d'appareil de test

1. Accédez à 4Sight2 en tant que Technicien.
2. Allez dans **Assets >> Worklist** (Actifs >> Liste de travail)
3. Sélectionnez une ou plusieurs gammes et attribuez-les au flux d'étalonnage Portable (Portatif) ou Automated (Automatisé).
4. Cliquez sur le bouton **Refresh** (Actualiser).



5. Cliquez sur la liste déroulante **Test Equipment** (Appareils de test). Si vous voyez l'appareil connecté dans la liste, c'est que le communicateur d'appareil de test est correctement configuré.



4.3 Configuration du pilote pour l'étalonneur de température

Pour permettre à l'étalonneur de température de communiquer avec 4Sight2, il faut installer un pilote FTDI.

1. Téléchargez le pilote FTDI à partir du lien suivant : https://www.ftdichip.com/Drivers/VCP.htm.

2. Extrayez le fichier téléchargé du fichier zip et enregistrez le fichier dans un emplacement connu sur votre machine.
3. Allez dans le Gestionnaire de périphériques Windows sur votre machine.
4. Sélectionnez Ports (COM & LPT) dans la liste des périphériques, pour voir l'étalonneur de température.
5. Faites un clic droit sur l'étalonneur de température et sélectionnez Mettre à jour le pilote.
6. Sélectionnez Rechercher un pilote sur mon ordinateur.
7. Sélectionnez Parcourir, à côté du champ intitulé Rechercher les pilotes à cet emplacement.
8. Sélectionnez le dossier extrait contenu le pilote téléchargé.
9. Sélectionnez Suivant puis fermez.
10. Le pilote est désormais installé.
11. Pour tester les communications avec un étalonneur de température dans 4Sight2, allez jusqu'à l'étalonnage automatisé et vérifiez que vous pouvez choisir l'étalonnage de température comme contrôleur d'entrée (Input Controller). Si ce n'est pas le cas, ré-exécutez l'étape 14 à partir de la section 4.

Guide de déploiement

5. Guide de déploiement

5.1 Architecture de déploiement

L'architecture type comprend une application Internet 4Sight2 et un serveur UAA (User Authentication and Authorization : authentification et autorisation d'utilisateur) fonctionnant sur le serveur Web Tomcat avec la base de données PostgreSQL exploitée sur la même machine.

L'application client sur navigateur Web se connecte au serveur 4Sight2, qui à son tour stocke et récupère des informations dans et depuis la base de données PostgreSQL.

5.2 Déploiement physique

Nous supposons que l'utilisateur qui installe 4Sight2 a déjà mis en place des mesures de cybersécurité qui respectent les politiques de sécurité de l'entreprise, notamment les mesures suivantes :

- Le serveur est placé dans un endroit sûr, à l'accès physiquement limité.
- Le contrôle de l'accès au serveur est protégé par des droits d'accès limités.
- Le réseau du serveur est protégé par un pare-feu afin d'en limiter l'accès aux applications parfaitement connues et uniquement sur des ports connus.
- Les applications fonctionnent dans leur propre contexte et ont accès à la base de données et aux fichiers systèmes qui se trouvent dans leur propre dossier seulement.

5.3 Réseau

Les clients sont connectés par l'intermédiaire de navigateurs Web, soit par des connexions Ethernet soit via un réseau sans fil. Le réseau sans fil peut présenter une certaine latence en fonction de la bande passante sans fil et du nombre d'appareils connectés.

Il est conseillé de désactiver ou de supprimer tous les modules complémentaires et extensions du navigateur installés sur le navigateur.

Le serveur Web 4Sight2 ne doit pas être exposé à Internet ; tout accès nécessaire doit être fourni via Intranet ou VPN.

5.4 Séquence de déploiement

PostgreSQL, Tomcat et Java Runtime doivent être préalablement installés pour que l'application 4Sight2 fonctionne. PostgreSQL est installé séparément tandis que les autres logiciels sont regroupés dans l'application. Si PostgreSQL est déjà installé sur la machine utilisateur, il suffit du mot de passe de super-utilisateur pour effectuer sa connexion et sa configuration.

L'installation exige des droits d'administrateur Windows sur la machine. Avant l'installation, l'utilisateur doit posséder le mot de passe de super-utilisateur PostgreSQL, le nom d'utilisateur et le mot de passe d'administrateur de l'application ainsi que le nom d'utilisateur et le mot de passe de la base de données.

Le mot de passe de super-utilisateur PostGreSQL est requis pour créer la base de données et d'autres structures à l'intérieur du serveur PostGreSQL. L'administrateur de l'application est le premier utilisateur de l'application. Il est responsable de la création d'autres utilisateurs et de l'attribution de différents rôles à ceux-ci. L'utilisateur de la base de données a accès à la base de données 4Sight2 et UAA. Ces identifiants sont utilisés pour accéder à la base de données.

L'application est publiée sur le port machine. Le port par défaut est 8083. L'utilisateur peut modifier le port au moment de l'installation ou plus tard. Le contexte applicatif par défaut dans Tomcat est 4Sight2.

Pour durcir le système d'exploitation, respectez la procédure de durcissement du système d'exploitation conformément aux directives Microsoft ou CIS. La procédure d'installation invite l'utilisateur à installer PostgreSQL avant d'installer le serveur 4Sight2.

Le communicateur d'appareil de test est installé sur les machines clients au moment où l'appareil de test est raccordé via des ports USB. Si le communicateur d'appareil de test n'est pas encore installé sur la machine, l'utilisateur est invité à le télécharger depuis le serveur 4Sight2 et à l'installer sur la machine. Le communicateur d'appareil de test est à l'écoute sur le port 9000 et ne peut communiquer que sur une couche sécurisée.

5.5 Tâches après déploiement

5.5.1 Ajout d'utilisateurs et de groupes

L'administrateur est chargé de créer dans l'application différents utilisateurs tels que le superviseur, le chef technicien, le technicien et l'auditeur. Il peut les affecter à différents groupes internes par défaut. S'il faut assurer davantage de contrôle ou une granularité de l'accès plus fine, l'administrateur peut créer des groupes personnalisés et leur attribuer des accès spécifiques.

5.5.2 Mots de passe par défaut

Nous utilisons le mot de passe par défaut pour l'utilisateur Tomcat, codé en dur dans le fichier “C:\Program Files\Druck\4Sight2\<<latest folder number>>\apache-tomcat\conf\tomcat-user.xml”.

Il est conseillé de modifier le mot de passe par défaut et de toujours utiliser un mot de passe qui respecte pleinement les meilleures pratiques concernant les mots de passe.

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

Les meilleures pratiques ont été mises en oeuvre pour veiller à ce que cette application soit sécurisée. Pour renforcer la sécurité, veuillez effectuer les tâches suivantes :

Par défaut, le service et les systèmes ont uniquement des droits d'accès aux fichiers et dossiers de configuration. Au début, l'administrateur n'a donc qu'un accès en lecture/écriture au dossier C:\Program Files\Druck\4Sight2\<<latest folder number>>\apache-tomcat\conf, si bien qu'avant de tenter d'exécuter les tâches ci-dessous, il faut ouvrir l'invite de commande avec les identifiants d'administrateur.

5.5.3 Communications sécurisées

Cette section explique comment configurer 4sight2 en mode sécurité (également appelé mode SSL) à l'aide d'un certificat auto-signé. Avant de poursuivre, veuillez lire les hypothèses effectuées ainsi que les modalités présentées dans l'application 4Sight2. Un certificat auto-signé constitue l'un des moyens d'activer le mode SSL dans 4Sight2. Il est également possible d'acquérir un certificat CA tiers auprès de fournisseurs tels que Symantec, Digicert et autres.

Remarque : La simple activation du mode SSL ne suffit pas à rendre votre application sécurisée. Il s'agit de l'une des pratiques les plus courantes visant à construire une application Web sécurisée.

5.5.3.1 Hypothèses et avertissements

Pour que les consignes ci-dessous soient valides, les hypothèses suivantes sont faites :

Le logiciel OpenSSL for Windows est nécessaire pour la génération des certificats auto-signés. 4Sight2 suppose que votre entreprise ainsi que les réglementations nationales et supranationales vous autorisent à utiliser le logiciel OpenSSL.

- Keytool est un utilitaire de gestion de clés et de certificats fourni par Java pour générer divers composants intervenant dans une configuration https. 4Sight2 suppose que votre entreprise ainsi que les réglementations nationales et supranationales vous autorisent à utiliser l'utilitaire Keytool.
- Il se peut que vous deviez disposer de droits d'administrateur pour exécuter les configurations ci-dessous. Pour plus d'informations sur l'obtention des droits d'administrateur, contactez votre service informatique.
- Les étapes ci-dessous exigent des connaissances élémentaires sur les processus informatiques à tel point qu'il est préférable qu'elles soient exécutées par un informaticien ou sous sa supervision.
- Le contenu présenté ici tel que les noms d'hôte, les mots de passe, les adresses URL et les chemins d'accès aux dossiers est uniquement donné à titre de référence. Veillez à modifier les commandes en conséquence avant leur exécution.
- Les sections ci-après présentent deux scénarios. Le premier est celui d'un serveur et d'un client sur la même machine et le second celui d'un serveur et d'un client sur des machines différentes (par exemple, un scénario à plusieurs clients).

5.5.3.2 Étapes de la configuration de l'application 4Sight2 dans Https

1. Arrêtez 4Sight2 à partir des services Windows.
2. Ouvrez l'invite de commande en **mode Admin**.
3. Allez dans le dossier ci-dessous du répertoire d'installation de 4Sight2 en exécutant la commande ci-après :

   cd "C:\Program Files\Druck\4Sight2\<<latest folder number>>\apache-tomcat\conf"
4. Vérifiez si Keytool est présent en exécutant la commande suivante dans l'invite de commande : **Keytool** -?

   Si ce n'est pas le cas, définissez le chemin d'accès à l'environnement sur JRE bin dans le dossier d'installation de 4Sight2 comme indiqué ci-dessous. Corrigez le chemin en fonction du dossier d'installation.

   C:\Program Files\Druck\4Sight2\<<latest folder number>>\jre\bin
   Set "Path=%Path%;C:\Program Files\Druck\4Sight2\<<latest folder number>>\jre\bin"
5. Pour créer un nouveau certificat, passez directement au point 6. Par contre, si un certificat existe déjà, procédez comme suit :

   a. Vérifiez si le fichier de certificat 4Sight.jks existe dans la base de stockage de clés Java

   keytool -list -alias <<nomhôte>> -storepass <<MotdepasseClé>> -keystore 4Sight.jks

   b. Si un certificat est déjà installé, supprimez-le.

   keytool -delete -noprompt -alias <<nomhôte>> -storepass <<MotdepasseClé>> -keystore 4Sight.jks

c. Vérifiez si 4SightV2PublicKey.cer existe et si c'est le cas, supprimez-le.
del "../../app/Certificate/4SightV2PublicKey.cer"

d. Vérifiez si le certificat existe déjà dans cacert de Java.
keytool -list -alias <<nomhôte>> -storepass changeit -keystore "../../jre/lib/security/cacerts"

e. Supprimez le certificat s'il existe dans la base de stockage Java.
keytool -delete -noprompt -alias <<nomhôte>> -storepass changeit -keystore "../../jre/lib/security/cacerts" -file "../../app/Certificate/4SightV2PublicKey.cer"

6. Créez le nouveau certificat en procédant comme suit :

   keytool -genkey -trustcacerts -keyalg "RSA" -keysize 2048 -validity 1095 -keypass <<MotdepasseClé>> -alias <<nomhôte>> -keystore 4Sight.jks -storepass <<MotdepasseStockage>> -dname "CN=%COMPUTERNAME%, OU=<<unité commerciale>>, O=<<entreprise>>, L=<<emplacement>>, S=<<état>>, C=<<initiales pays>>" -ext eku:critical=sa

7. Exportez le certificat vers le fichier 4SightV2PublicKey.cer (ne modifiez pas le nom ni le chemin d'accès).

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

   Une fois la commande exécutée avec succès, le message suivant : "Certificate stored in file C:\Program Files\Druck\4Sight2\<<latest folder number>>\app\Certificate\4SightV2PublicKey.cer" (Certificat stocké dans fichier C:\Program Files\Druck\4Sight2\<<latest folder number>>\app\Certificate\4SightV2PublicKey.cer) s'affiche pour indiquer l'emplacement de stockage du certificat.

8. Importez le certificat dans le fichier CAcert Java.

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

Après la bonne exécution de la commande, le message "Certificate was added to keystore" (Certificat ajouté à la base de stockage des clés) s'affiche.

9. Effectuez la saisie du certificat dans le fichier de configuration Tomcat.

   a. Ouvrez le fichier server.xml à partir de l'emplacement ci-dessous.
   C:\Program Files\Druck\4Sight2\<<latest folder number>>\apache-tomcat\conf\server.xml"

   b. Effectuez la saisie suivante dans server.xml.
   <Connector port="8443" protocol="org.apache.coyote.http11.Http11NioProtocol" maxThreads="150" SSLEnabled="true" sslProtocol="TLSv1.2" keystoreFile="conf/4Sight.jks"
   keystorePass="<<MotdepasseClé>>" keyAlias="tomcat" scheme="https" secure="true" clientAuth="false" />

   c. Commentez la section suivante pour désactiver les connexions http.
   <connectionTimeout="20000" maxSwallowSize="104857600" port="8083" protocol="HTTP/1.1" redirectPort="8443" relaxedPathChars=""[\]^`{|}+" relaxedQueryChars="&quot;[\]^`{|}+"/>

Remarque : L'application ne fonctionnera pas si vous ne commentez pas cette partie.

10. La configuration Https de l'application 4Sight2 est terminée à ce stade.
11. Pour tester les configurations définies ci-dessus, redémarrez le service 4Sight2 dans le service Windows.
12. Ouvrez Google Chrome, supprimez la mémoire cache du navigateur et redémarrez ce dernier.
13. Dans le navigateur, saisissez l'adresse URL suivante : https://<<nom-hôte>>:8443/4sight2

- La première fois, le chargement de l'adresse URL peut prendre un certain temps.
- L'écran affiche "Your connection is not private" (Votre connexion n'est pas privée).
- Cliquez sur le bouton **Advanced** (Avancé) >> lien **Proceed to XX** (Passer à XX).
- Si vous ne voyez pas l'écran 4sight2, cliquez sur le bouton **Reload** (Recharger).
- Vous serez redirigé vers la page 4sight2.
- La barre d'adresse indiquera l'erreur "Not Secure" (Non sécurisé), qui disparaîtra lorsque le certificat sera enregistré dans mmc.

5.5.3.3 Étapes de configuration de DruckCommsServer dans Https dans le cas d'une installation sur la machine serveur

Remplacez les valeurs dans << >> par des données appropriées avant d'exécuter la commande.

1. Arrêtez DruckCommsServer à partir des services Windows.
2. Ouvrez l'invite de commande en **mode Admin**.
3. Vérifiez si Keytool est présent en exécutant la commande suivante dans l'invite de commande : **Keytool -?**

   Si ce n'est pas le cas, définissez le chemin d'accès à l'environnement sur JRE bin dans le dossier d'installation de 4Sight2 comme indiqué ci-dessous.
   Corrigez le chemin en fonction du dossier d'installation.
   C:\Program Files\Druck\4Sight2\<<latest folder number>>\jre\bin
   Set "Path=%Path%;C:\Program Files\Druck\4Sight2\<<latest folder number>>\jre\bin"
4. Allez dans le dossier ci-dessous du répertoire d'installation de DruckCommServer en exécutant la commande ci-après :

   cd " C:\Program Files\Druck\DruckCommsServer\<< Version du service de communication>>"
5. S'il existe déjà un certificat, procédez comme suit :

   a. Vérifiez si le certificat existe déjà dans cacert de Java.
   keytool -list -alias tomcat -storepass changeit -keystore cacerts

   b. Supprimez le certificat s'il existe dans la base de stockage Java.
   keytool -delete -noprompt -alias tomcat -storepass changeit -keystore cacerts

   c. Supprimez les certificats de CommsServer préconfigurés par défaut
   del 4Sight.jks
   del 4SightV2DeviceMngr.pfx
6. Créez le nouveau certificat en procédant comme suit :

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

<<MotdepasseStockage>> dname "CN=localhost, OU=<<unité commerciale>>, O=<<entreprise>>, L=<<emplacement>>, S=<<état>>, C=<<initiales pays>>" -ext eku:critical=sa

7. Exportez le certificat vers le fichier DruckCommServer.cer.

   keytool -export -alias tomcat -keystore CommServer.jks -storepass <<MotdepasseStockage>> -storetype JKS -file DruckCommServer.cer
   Une fois la commande exécutée avec succès, le message suivant :
   "Certificate stored in file DruckCommServer.cer " (Certificat stocké dans fichier DruckCommServer.cer) s'affiche.

8. Importez le certificat du serveur de communication dans le fichier CAcert Java.

   keytool -import -noprompt -trustcacerts -alias tomcat -storepass changeit -keystore cacerts -file DruckCommServer.cer
   Après la bonne exécution de la commande, le message "Certificate was added to keystore" (Certificat ajouté à la base de stockage des clés) s'affiche.

9. Importez le certificat 4Sight dans le fichier CAcert Java.

   keytool -import -noprompt -trustcacerts -alias <<nomhôte serveur>> -storepass changeit -keystore cacerts -file "C:\Program Files\Druck\4Sight2\<<latest folder number>>\app\Certificate\4SightV2PublicKey.cer"
   Après la bonne exécution de la commande, le message "Certificate was added to keystore" (Certificat ajouté à la base de stockage des clés) s'affiche.

10. Éditez le mot de passe de la base de stockage des clés pour application.properties dans DruckCommsServer.

    Ouvrez le fichier :
    C:\Program Files\Druck\DruckCommsServer\<<Version du service de communication>>\application.properties et modifiez la ligne suivante :
    keystore = CommServer.jks
    key-store.password= << MotdepasseStockage >>
    Remarque : **<< MotdepasseStockage >>** renvoie au **MotdepasseStockage** utilisé à l'étape 6.

11. Redémarrez les services 4Sight2 et DruckCommsServer.

5.5.3.4 Étapes de configuration de DruckCommsServer dans Https dans le cas d'une installation sur une machine client

1. L'utilitaire Keytool est livré avec Java si bien que vous pouvez installer Java sur votre machine ou vérifier directement la disponibilité de Java Keytool sans installer Java.
2. Arrêtez DruckCommsServer à partir des services Windows.
3. Ouvrez l'invite de commande en **mode Admin**.
4. Vérifiez si Keytool est présent en exécutant la commande suivante dans l'invite de commande :
   Keytool -?

   Si ce n'est pas le cas, définissez le chemin d'accès à l'environnement sur JRE bin dans le cas où vous avez installé Java sur la machine ; vous pouvez définir le chemin d'accès sur Keytool comme indiqué ci-dessous.
   Corrigez le chemin en fonction du dossier d'installation.
   C:\Program Files\Java\<< version Java >>\bin
   Set Path=%Path%; "C:\Program Files\Java\<< version Java >>\bin"

5. Obtenez le fichier **4SightV2PublicKey.cer** depuis la machine serveur sur laquelle l'application 4Sight est installée. Ce fichier est situé sur le serveur comme indiqué ci-dessous :

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

6. Copiez ce fichier **4SightV2PublicKey.cer** dans le chemin d'accès suivant :

   C:\Program Files\Druck\DruckCommsServer\<< Version du service de communication>>

7. Exécutez maintenant les étapes 4 à 8 à la section 5.5.3.3.
8. Importez le certificat 4Sight dans le fichier CAcert Java.

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

   Après la bonne exécution de la commande, le message "Certificate was added to keystore" (Certificat ajouté à la base de stockage des clés) s'affiche.

9. Exécutez maintenant les étapes 10 à 11 à la section 5.5.3.3.

5.5.3.5 Étapes de génération du certificat auto-signé pour 4Sight2

1. Téléchargez et installez Open SSL for Windows.
2. Arrêtez les services 4Sight2 à partir des services Windows.
3. Créez un nouveau dossier appelé **4Sight2Certificate** à l'intérieur du lecteur C.

   Vous pouvez choisir n'importe quel emplacement ou dossier à condition que vous ayez un droit administratif d'accès à ce dossier.

4. Créez un nouveau fichier à l'intérieur du dossier ci-dessus dans le bloc-notes et enregistrez le fichier sous **openssl-ca.cnf**.

   Copiez le contenu ci-dessous dans le fichier et enregistrez le fichier.

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

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

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

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

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

x509_extensions = ca_extensions # The extensions to add to the cert

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

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

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

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

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

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

commonName        = [Company Name]
commonName_default = Test CA

emailAddress      = Email Address
emailAddress_default = test@example.com

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

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

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

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

Remarque : Mettez à jour le **[Company Name]** ci-dessus et enregistrez le fichier. Il s'agit du nom de l'émetteur du certificat qui apparaîtra dans la console de gestion.

5. Créez un nouveau fichier à l'intérieur du dossier ci-dessus dans le bloc-notes et enregistrez le fichier sous **openssl-server.cnf**.

Copiez le contenu ci-dessous dans le fichier et enregistrez le fichier.

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

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

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

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

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

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

commonName          = [Hostname of server]
commonName_default  = Test Server

emailAddress         = Email Address
emailAddress_default = test@example.com

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

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

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

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

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

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

Remarque : Mettez à jour le nom d'hôte et l'adresse IPv4 ci-dessus et enregistrez le fichier.

6. Ouvrez l'invite de commande à l'aide des droits d'administrateur.
7. Allez jusqu'au dossier 4Sight2Certificate en exécutant ce qui suit :
   cd "<<chemin complet à 4Sight2Certificate >>"
8. Définissez la variable de chemin d'accès au dossier OpenSSL bin en exécutant la commande ci-dessous.
   Set path=%path%;"<<dossier bin de openssl>>"
   Exemple de chemin d'accès par défaut :
   Set Path=%Path%;"C:\Program Files\OpenSSL-Win64\bin"
9. Définissez la variable de chemin d'accès au dossier JRE bin en exécutant la commande ci-dessous. Remarque : le chemin ci-dessous peut différer.
   Set path=%path%;"C:\Program Files\Druck\4Sight2\<<latest folder number>>\jre\bin"
10. Exécutez la commande ci-dessous pour générer les fichiers cacert.pem et cakey.pem.
    openssl req -x509 -config openssl-ca.cnf -newkey rsa:4096 -days <<Number of days>> -sha256 -nodes -out cacert.pem -outform PEM
    Saisissez les données de certificat correctes lorsque vous y êtes invité, par exemple pays, état, etc.
11. Exécutez les commandes ci-dessous pour générer les fichiers servercert.csr et serverkey.pem
    openssl req -config openssl-server.cnf -newkey rsa:2048 -days <<Number of days>> -sha256 -nodes -out servercert.csr -outform PEM
    Saisissez les données de certificat correctes lorsque vous y êtes invité, par exemple pays, état, etc.
12. Créez un nouveau fichier dans le bloc-notes et nommez-le index.txt. Enregistrez le fichier dans le dossier 4Sight2Certificate.
13. Créez un nouveau fichier dans le bloc-notes et nommez-le serial.txt. Enregistrez le fichier dans le dossier 4Sight2Certificate.
    Ouvrez le fichier et saisissez **01**. Enregistrez et fermez le fichier.
14. Exécutez la commande ci-dessous pour générer les nouveaux certificats dans les fichiers servercert.pem et serverkey.pem.
    openssl ca -config openssl-ca.cnf -policy signing_policy -extensions signing_req -out servercert.pem -infiles servercert.csr
    Saisissez Y (Oui) pour valider les modifications. La base de données sera mise à jour après l'exécution correcte.

15. Regroupez les fichiers de clés existants au format PFX en exécutant la commande ci-dessous.

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

    Vous serez invité à saisir le mot de passe deux fois.

16. Convertissez la base de stockage PFX en une base de stockage de clés Java, triée par emplacement JRE bin mentionné plus haut, à savoir le chemin tomcat/config.

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

    Remarque : Gardez le même mot de passe pour les deux bases de stockage. Vérifiez que vous mentionnez bien le fichier 4Sight.jks présent dans le dossier de configuration de tomcat, comme indiqué plus haut.

    Vous serez invité à saisir le mot de passe de la base de stockage de clés de destination et celui de la base de stockage source. Après la bonne exécution de la commande, vous verrez le message "Import command completed: 1 entries successfully imported" (Commande d'importation exécutée : 1 entrée correctement importée).

17. Exportez le certificat de la base de stockage de clés Java vers le fichier situé à l'emplacement suivant :

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

    Remarque : Vérifiez que vous mentionnez bien le fichier 4Sight.jks présent dans le dossier de configuration de tomcat, comme indiqué plus haut.

    Après l'exécution réussie, vous verrez le message indiquant que le certificat est stocké dans le fichier.

18. Importez le fichier de certificat dans le dossier cacerts à l'intérieur du répertoire d'installation de 4sight2.

    Remarque : le chemin d'accès varie en fonction du répertoire d'installation et de la version de 4sight2.

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

    Remarque : si, pour une raison quelconque, l'alias que vous tentez de créer existe déjà, exécutez la commande ci-dessous pour le supprimer dans un premier temps, puis ré-exécutez les étapes ci-dessus pour créer un nouvel alias :

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

    Une fois la commande correctement exécutée, vous verrez le message "Certificate was added to keystore" (Certificat ajouté à la base de stockage de clés).

19. Apportez la modification suivante dans le fichier server.xml (dans C:\Program Files\Druck\4Sight2\<<latest folder number>>\apache-tomcat\conf).

a. Effectuez la saisie suivante dans server.xml.

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

b. Commentez la section suivante pour désactiver les connexions http.

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

20. La configuration https pour 4Sight2 est terminée. Démarrez maintenant le service 4sight2 à partir des services Windows.

5.5.3.6 Étapes de configuration de certificat auto-signé pour DruckCommsServer en cas d'installation sur une machine serveur

Nous supposons ici que vous avez correctement converti l'application 4sight2 dans HTTPs en exécutant les étapes décrites à la section 5.5.3.5 et que vous disposez déjà des fichiers ci-dessous dans le dossier **4Sight2Certificate** :

- openssl-server.cnf
- openssl-ca.cnf
- cacert.pem
- cakey.pem
- index.txt
- serial.txt
- 4SightV2PublicKey.cer (ce fichier peut être situé dans le dossier C:\Program Files\Druck\4Sight2\<<latest folder number>>\app\Certificate)

1. Créez un nouveau dossier nommé **CommserverCertificate**, copiez les fichiers ci-dessus et apportez les modifications ci-après :

- openssl-server.cnf

  Sous la section **req**, donnez à **default_keyfile** la valeur "**DruckCommServerCertKey.pem**".

  - Sous **server_distinguished_name**, donnez à **commonName** la valeur "**localhost**".
  - Sous **alternate_names**, donnez à **DNS.1** la valeur "**localhost**".
  - Sous **alternate_names**, donnez à **IP.1** la valeur "**127.0.0.1**"
  - Enregistrez le fichier.

- openssl-ca.cnf. (Ne changez rien à l'intérieur)
- cacert.pem. (Ne changez rien à l'intérieur)
- index.txt (supprimez tout le contenu à l'intérieur, càd. faites-en un fichier vide)
- serial.txt (supprimez tout le contenu à l'intérieur et gardez seulement une entrée 01 à l'intérieur)

2. Arrêtez le service DruckCommsServer à partir des services Windows.
3. Ouvrez l'invite de commande à l'aide des droits d'administrateur.
4. Allez jusqu'au dossier **CommserverCertificate** en exécutant ce qui suit :

   cd "<<chemin complet à CommserverCertificate >>"
5. Définissez la variable de chemin d'accès au dossier OpenSSL bin en exécutant la commande ci-dessous.

   Set path=%path%;"<<dossier bin de openssl>>"
   Exemple de chemin d'accès par défaut :
   Set Path=%Path%;"C:\Program Files\OpenSSL-Win64\bin"
6. Définissez la variable de chemin d'accès au dossier JRE bin en exécutant la commande ci-dessous. Remarque : le chemin ci-dessous peut différer.

   Set path=%path%;"C:\Program Files\Druck\4Sight2\<<latest folder number>>\jre\bin"
7. Une fois cette étape effectuée, créez une requête de certificat Comm Server par la commande suivante :

   openssl req -config openssl-server.cnf -newkey rsa:2048 -sha256 -nodes -out DruckCommServer.csr -outform PEM
   Une fois cette commande exécutée, vous avez une requête dans **DruckCommServer.csr** et une clé privée dans **DruckCommServerCertKey.pem**
8. Puis, procédez comme suit pour signer la requête csr avec votre autorité de certification (ca) :

   openssl ca -config openssl-ca.cnf -policy signing_policy -extensions signing_req -out DruckCommServerCert.pem -infiles DruckCommServer.csr
9. Après quoi, créez un fichier PFX avec l'alias **tomcat** pour le serveur de communication, via la commande suivante :

   openssl pkcs12 -export -in DruckCommServerCert.pem -inkey DruckCommServerCertKey.pem -certfile cacert.pem -name "tomcat" -out DruckCommServer.pfx
10. Convertissez la base de stockage PFX en une base de stockage de clés Java à l'aide de Keytool.

    Remarque : Gardez le même mot de passe pour les deux bases de stockage de clés.
    keytool -importkeystore -srckeystore DruckCommServer.pfx -srcstoretype PKCS12 -destkeystore CommServer.jks -deststoretype jks
11. Importez maintenant le certificat dans cacert.

    a. Supprimez l'alias tomcat existant livré avec l'installation par défaut
    keytool -delete -noprompt -trustcacerts -alias tomcat -storepass changeit -keystore "C:\Program Files\Druck\DruckCommsServer\<< Version du service de communication >>\cacerts"

    b. Après avoir supprimé l'alias tomcat existant, importez le certificat dans cacerts comme suit :
    keytool -import -noprompt -trustcacerts -alias tomcat -storepass changeit -keystore "C:\Program Files\Druck\DruckCommsServer\<< Version du service de communication >>\cacerts" -file DruckCommServerCert.pem
12. Il nous faut maintenant importer la clé publique 4sight dans le fichier cacert de CommServer pour l'authenfication des communications. Pour cela, exécutez la commande suivante :

    keytool -import -noprompt -trustcacerts -alias <<4sight server hostname>> -storepass changeit -keystore "C:\Program Files\Druck\DruckCommsServer\<< Version du service de

communication >>\cacerts" -file "C:\Program Files\Druck\4Sight2\<<latest folder number>>\app\Certificate\4SightV2PublicKey.cer"

13. Après avoir terminé toutes les étapes ci-dessus, les fichiers **DruckCommServer.pfx** et **CommServer.jks** seront dans le dossier **CommserverCertificate** actuel.

    Copiez ces fichiers et collez-les dans le répertoire **"C:\Program Files\Druck\DruckCommsServer\<< Version du service de communication >>\"**. Puis éditez **application.properties** à partir du même emplacement. Modifiez la valeur de propriété comme suit :

    a. Keystore = CommServer.jks

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

    c. key-store.type=JKS

5.5.3.6.1 Installation du certificat dans Windows pour 4sight et DruckCommsServer

1. Ouvrez Exécuter et saisissez "mmc" puis appuyez sur Entrée.
2. Allez à Fichier et sélectionnez Ajouter/Supprimer un composant logiciel enfichable.
3. Dans le menu gauche, sélectionnez Certificats. Appuyez sur Ajouter et sélectionnez Un compteur d'ordinateur >> Suivant >> Terminer. Cliquez ensuite sur OK.
4. Développez la section Certificats (ordinateur local). Développez Autorités de certification racine.

   Cliquez avec le bouton droit sur le dossier Certificats >> Toutes les tâches >> Importer.

   Sélectionnez le fichier cacert.pem >> Suivant >> Terminer.

   Ainsi, notre autorité de certification personnalisée est installée correctement sous l'autorité de confiance.

Après avoir exécuté toutes ces étapes, lancez le service DruckCommsServer.

5.5.3.7 Étapes de configuration de certificat auto-signé pour DruckCommsServer en cas d'installation sur une machine client

Pour convertir DruckCommsServer en HTTPs, vous devez disposer de Java Keytool et de l'utilitaire OpenSSL.

1. L'utilitaire Keytool est livré avec Java si bien que vous pouvez installer Java sur votre machine ou vérifier directement la disponibilité de Java Keytool sans installer Java.
2. Téléchargez et installez OpenSSL for Windows.
3. Définissez la variable de chemin d'accès au dossier OpenSSL bin en exécutant la commande ci-dessous.

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

   Exemple de chemin d'accès par défaut :

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

4. Définissez la variable de chemin d'accès au dossier JRE bin en exécutant la commande ci-dessous.

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

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

5. Arrêtez le service DruckCommsServer à partir des services Windows.
6. Créez un nouveau dossier appelé **CommserverCertificate** à l'intérieur du lecteur C ou de tout autre lecteur souhaité.
7. Obtenez le fichier de certificat public de 4sight2 **4SightV2PublicKey.cer** à partir de la machine serveur, située dans le répertoire C:\Program Files\Druck\4Sight2\<<latest folder number>>\app\Certificate et copiez ce fichier dans le dossier **CommserverCertificate**.

8. Créez maintenant les fichiers **openssl-server.cnf** et **openssl-ca.cnf** en exécutant les étapes 4 et 5 de la section 5.5.3.5 et les fichiers index.txt et serial.txt en suivant les étapes 12 et 13 et copiez ces fichiers dans le dossier **CommserverCertificate**.
9. Ces fichiers sont donc désormais dans le dossier CommServerCertificate.
    a. openssl-server.cnf
    b. openssl-ca.cnf
    c. index.txt
    d. serial.txt
    e. 4SightV2PublicKey.cer
10. Ouvrez l'invite de commande à l'aide des droits d'administrateur.
    Allez jusqu'au dossier CommserverCertificate en exécutant ce qui suit :
    cd "<<chemin complet à CommserverCertificate >>"
11. Exécutez la commande ci-dessous pour générer les fichiers cacert.pem et cakey.pem.
    openssl req -x509 -config openssl-ca.cnf -newkey rsa:4096 -sha256 -nodes -out cacert.pem -outform PEM
    Saisissez les données de certificat correctes lorsque vous y êtes invité, par exemple pays, état, etc.
12. Modifiez ensuite le contenu des fichiers dans le dossier **CommserverCertificate** en exécutant l'étape 1 de la section 5.5.3.6.
13. Exécutez maintenant les étapes 7 à 11 de la section 5.5.3.6.
14. Il nous faut maintenant importer la clé publique 4sight dans le fichier cacert de CommServer pour l'authenfication des communications. Pour cela, exécutez la commande suivante :
    keytool -import -noprompt -trustcacerts -alias <<4sight server hostname>> -storepass changeit -keystore "C:\Program Files\Druck\DruckCommsServer\<< Version du service de communication >>\cacerts" -file 4SightV2PublicKey.cer
15. Après avoir terminé toutes les étapes ci-dessus, les fichiers **DruckCommServer.pfx** et **CommServer.jks** seront dans le dossier **CommserverCertificate** actuel.
    Copiez ces fichiers et collez-les dans le répertoire **"C:\Program Files\Druck\DruckCommsServer\<< Version du service de communication >>\"**. Puis éditez **application.properties** à partir du même emplacement. Modifiez la valeur de propriété comme suit :
    a. Keystore = CommServer.jks
    b. key-store.password = <<MotdepasseStockageClés>>
    c. key-store.type=JKS

5.5.3.7.1 Installation du certificat dans Windows pour DruckCommsServer

1. Ouvrez Exécuter et saisissez "mmc" puis appuyez sur Entrée.
2. Allez à Fichier et sélectionnez Ajouter/Supprimer un composant logiciel enfichable.
3. Dans le menu gauche, sélectionnez Certificats. Appuyez sur Ajouter et sélectionnez Un compteur d'ordinateur >> Suivant >> Terminer. Cliquez ensuite sur OK.
4. Développez la section Certificats (ordinateur local). Développez Autorités de certification racine.
    Cliquez avec le bouton droit sur le dossier Certificats >> Toutes les tâches >> Importer.
    Sélectionnez le fichier cacert.pem >> Suivant >> Terminer.
    Ainsi, notre autorité de certification personnalisée est installée correctement sous l'autorité de confiance.

Après avoir exécuté toutes ces étapes, lancez le service DruckCommsServer.

Si vous souhaitez simplement vérifier que DruckCommsServer est correctement converti en https, dans l'onglet Google Chrome, ouvrez le lien suivant : **https://localhost:9443/api/devicemanager/**

version (veuillez indiquer votre numéro de port de serveur de communication si vous avez un port autre que le port par défaut, 9443)

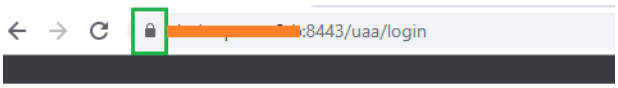
5.5.3.8 Validation du certificat dans 4Sight2

1. Redémarrez le PC du serveur.
2. Redémarrez les services 4Sight2 et DruckCommsServer à partir des services Windows.
3. Ouvrez Google Chrome, supprimez la mémoire cache du navigateur et redémarrez ce dernier. Assurez-vous qu'aucune autre instance de Google Chrome n'est active.
4. Saisissez l'adresse URL ci-dessous dans la barre d'adresse puis appuyez sur Entrée.

   Https://<<nom hôte serveur>>:8443/4sight2.

   Remarque : vous devez utiliser le nom d'hôte dans l'adresse URL ci-dessus.
5. L'écran d'accueil avec l'adresse URL correcte doit s'afficher.

   Remarque : l'erreur rouge a disparu de la barre d'adresse. Si le lien n'est toujours pas sécurisé, redémarrez votre ordinateur et allez à l'étape 3.



FAQ sur l'installation de 4Sight2

6. FAQ sur l'installation de 4Sight2

6.1 Configuration et installation

Question 1 : Mon organisation compte plusieurs sites dans différentes régions du monde. Quelle est la meilleure méthode pour configurer 4Sight2 ?

Réponse : Cela dépend de votre méthode de gestion et d'exploitation de ces sites. Si tous les sites sont gérés et exploités à partir d'un concentrateur informatique central, vous pouvez installer une seule licence 4Sight2 de manière centralisée. Tous les sites peuvent accéder à 4Sight2 via le réseau ou le LAN. Par ailleurs, si votre organisation compte des entités distinctes exploitées et gérées de manière indépendante, vous pouvez acheter plusieurs licences 4Sight2.

Question 2 : Si j'achète plusieurs licences 4Sight2, pourront-elles communiquer entre elles ?

Réponse : Non. Chaque licence 4Sight2 constitue un logiciel isolé distinct avec une installation d'application et une base de données propres. Des installations distinctes ne communiquent pas entre elles. Contactez l'équipe 4Sight2 pour plus d'informations ou pour discuter d'exigences spéciales.

Question 3 : Comment puis-je télécharger 4Sight2 ?

Réponse : Vous pouvez télécharger facilement 4Sight2 à partir du site Web de la société. Vous trouverez ci-dessous le lien.

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

OU

Vous pouvez contacter les bureaux de vente et demander un bon de commande. Vous recevrez alors la version de démonstration sur une clé USB.

Question 4 : Puis-je installer 4Sight2 sur un système d'exploitation non Windows ?

Réponse : Non. 4Sight2 est uniquement pris en charge sur la plate-forme Windows.

Question 5 : J'ai téléchargé et installé 4Sight2. Comment puis-je accéder à 4Sight2 ?

Réponse : 4Sight2 est un logiciel basé sur le Web. Aucune icône n'est donc ajoutée sur votre bureau ou ordinateur lorsque vous installez 4Sight2. Pour accéder à 4Sight2 :

- Ouvrez Google Chrome, collez l'URL ci-dessous dans la barre d'adresse, puis appuyez sur Entrée.
- Si 4Sight2 est installé sur le même ordinateur, utilisez http://localhost:<numéro_port_application> / 4sight2. Si 4Sight2 est installé sur un autre ordinateur du réseau, utilisez

  http://<Computer name OR IP address>:<numéro_port_application>/4sight2
- Créez un signet dans Google Chrome pour référence ultérieure.

Question 6 : Le programme d'installation de 4Sight2 ne parvient pas à localiser les fichiers de base de données Postgres

Veuillez vous assurer que le programme d'installation a été extrait en un emplacement local et que le fichier exécutable est exécuté à partir du dossier Disk 1. Vérifiez que l'emplacement local sur lequel le programme d'installation a été extrait ne possède pas un nom d'accès trop long, ce qui pourrait aussi conduire au fait que le programme d'installation ne trouve pas les fichiers prérequis.

Question 7 : Que se passe-t-il si le processus de mise à niveau est annulé à n'importe quel stade de la mise à niveau ?

Réponse : Si l'administrateur annule, à n'importe quel stade, le processus de mise à niveau, la version 1.4 est rétablie et doit être fonctionnelle. L'administrateur doit redémarrer le processus de mise à niveau pour l'exécuter correctement.

Question 8 : Lors de l'installation de l'application 4Sight2, si l'utilisateur reçoit le message suivant : Please enter valid port number. To know valid port numbers please refer installation manual" (Veuillez saisir un numéro de port valide. Pour connaître les numéros de ports valides, veuillez vous reporter au guide d'installation).

Réponse : Vous trouverez ci-dessous la plage de ports non valides. Choisissez un port valide pour continuer l'installation.

- Les ports 0 à 1024 sont réservés pour la connexion TCP.
- Liste des ports non sécurisés : 2049, 3659, 4045, 6000, 6665-6669, 65535.

Question 9 : 4Sight2 avec HTTPS ne fonctionne pas dans le système.

Réponse : Suivez la syntaxe du nom de domaine de l'ordinateur sur lequel l'application 4sight2 sera installée.

<domaine> ::= <sous-domaine>

<sous-domaine> ::= <libellé> | <sous-domaine> "." <libellé>

<libellé> ::= <lettre> [[<ldh-str>] <let-dig>]

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

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

<let-dig> ::= <lettre> | <chiffre>

<lettre> ::= un des 52 caractères alphabétiques de A à Z en

majuscule et de a à z en minuscule

<chiffre> ::= un des dix chiffres de 0 à 9

Remarque : Les lettres en majuscules et minuscules sont autorisées dans les noms de domaines. Deux noms à l'orthographe identique mais de casse différente sont considérés comme identiques.

6.2 FAQ sur le communicateur d'appareil de test

Question 1 : J'ai achevé toutes les étapes décrites dans le guide d'installation et je ne vois toujours pas mon appareil dans la liste.

Réponse : Si vous ne voyez toujours pas l'appareil de test dans la liste après avoir exécuté ces étapes, réinstallez les pilotes 4Sight2. Pour cela, allez dans **Panneau de configuration >> Programmes et fonctionnalités** et désinstallez DruckCommsServer de la liste. Installez de nouveau le communicateur d'appareil de test.

Question 2 :. J'obtiens l'erreur '**No Devices Found**' (Aucun appareil trouvé).

Réponse : Pour résoudre le problème,

- Vérifiez que vous avez physiquement bien connecté l'appareil à l'aide du câble USB. Pour le vérifier, allez dans le Gestionnaire de périphériques pour localiser votre appareil dans la liste. Vous devriez le trouver dans la section Universal Serial Bus. Si vous le voyez dans la section

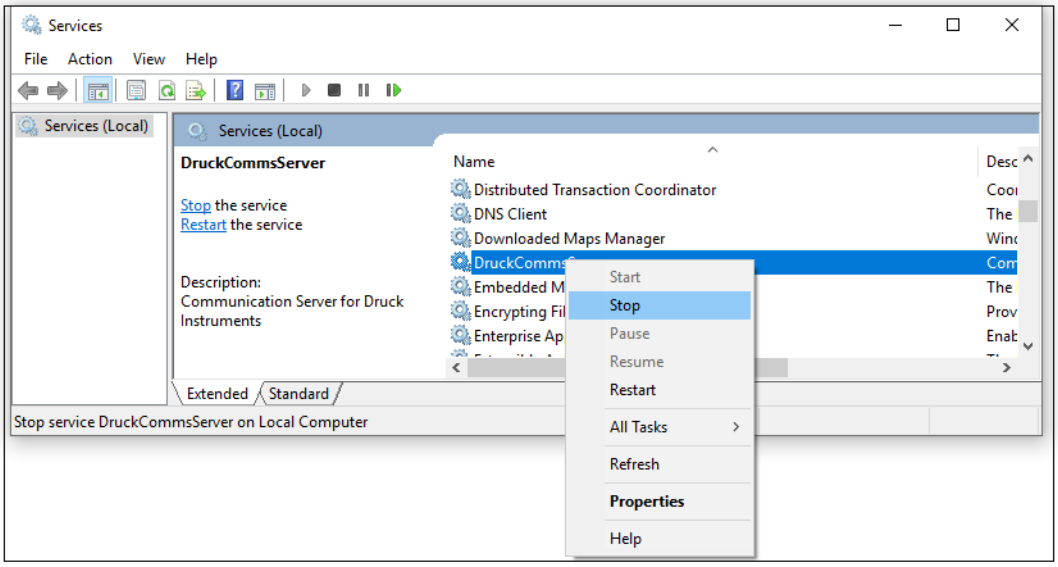
Autres dispositifs, vous devez effectuer le paramétrage ci-dessus pour que votre appareil devienne un appareil USB.

- Vérifiez que votre appareil est en communication ou en mode de communication. Voir l'étape 1 ci-dessus.
- Vérifiez que le chemin d'accès au pilote pointe vers C:\Windows\INF... Voir l'étape 2 ci-dessus.

Question 3 : J'obtiens l'erreur '**Internal Server Error**' (Erreur de serveur interne) lorsque je clique sur le bouton d'actualisation ou sur l'appareil de test dans la liste.

Réponse : Pour résoudre le problème,

- Allez dans les services Windows (autrement appelés les Services),
- Faites un clic droit sur le service **DruckCommsServer** dans la liste et cliquez sur **Redémarrer**.



- Allez dans 4Sight2 >> Cliquez sur le bouton **Actualiser**. Vous devriez voir l'appareil dans la liste.

Question 4 : J'obtiens l'erreur '**Communications Error**' (Erreur de communication).

Réponse : Il arrive que le logiciel ne puisse pas communiquer avec l'appareil pour des raisons diverses : mauvais contact USB, dispositif ayant raccroché, dispositif occupé à exécuter d'autres tâches, serveur occupé à exécuter d'autres tâches, et ainsi de suite. Cliquez de nouveau sur le bouton d'actualisation ; le problème doit disparaître (essayez 2-3 fois).

Mais, si l'erreur persiste, tentez la procédure ci-après :

- Relancez votre appareil (Genii / PACE) en vérifiant que cette opération est sûre, autrement dit que l'appareil n'est pas en train d'exécuter une opération critique. Renouvelez la demande. Vérifiez également que l'appareil est physiquement connecté.

Si la procédure ci-dessus n'aboutit pas, passez aux instructions à l'étape 3 ci-dessus et redémarrez le service **DruckCommsServer**.

Dépannage de l'installation

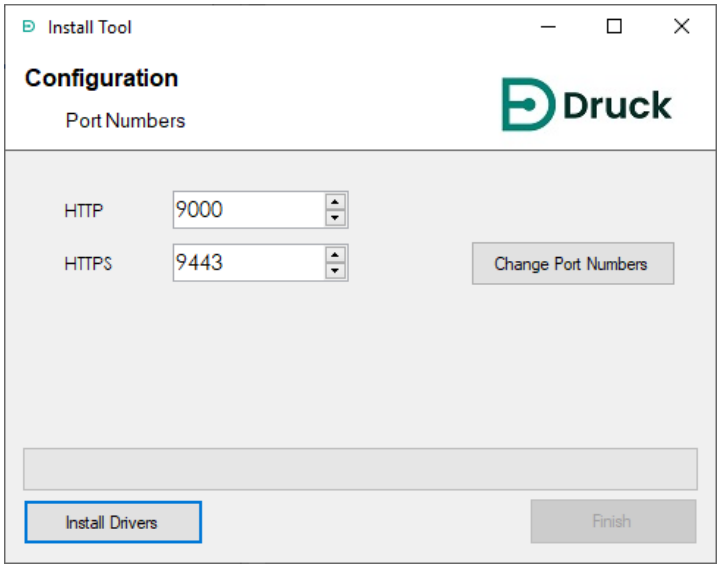
7. Dépannage de l'installation

7.1 Problèmes de communication de l'appareil de test

Lorsque vous utilisez 4Sight2 pour communiquer avec l'appareil de test, vous ne trouvez aucun appareil de test en retour alors que vous avez vérifié que le communicateur d'appareil de test renvoie bien une chaîne Json lorsqu'il est directement appelé. Il peut s'agir de l'un des deux problèmes suivants :

- Les numéros de port ont été mal configurés - veuillez contacter votre utilisateur administratif pour connaître les ports utilisés par 4Sight2 pour entrer en contact avec le communicateur d'appareil de test.

  Une fois que connaissez les ports à utiliser, allez à C:\Program Files\Druck\DruckCommsServer\[Version] et exécutez CommsServerInstallTool.exe



Modifiez les numéros de port puis cliquez sur le bouton **Change Port Numbers** (Modifier numéros de port). Attendez que le service redémarre. Les numéros de port ont désormais changé. Sélectionnez le bouton **Finish** (Terminer).

- Le communicateur d'appareil de test n'est pas configuré pour Https alors que 4Sight2 l'est.

  Contactez votre administrateur pour installer un certificat autosigné pour le communicateur d'appareil de test.

7.2 Sauvegarde de la base de données Postgres

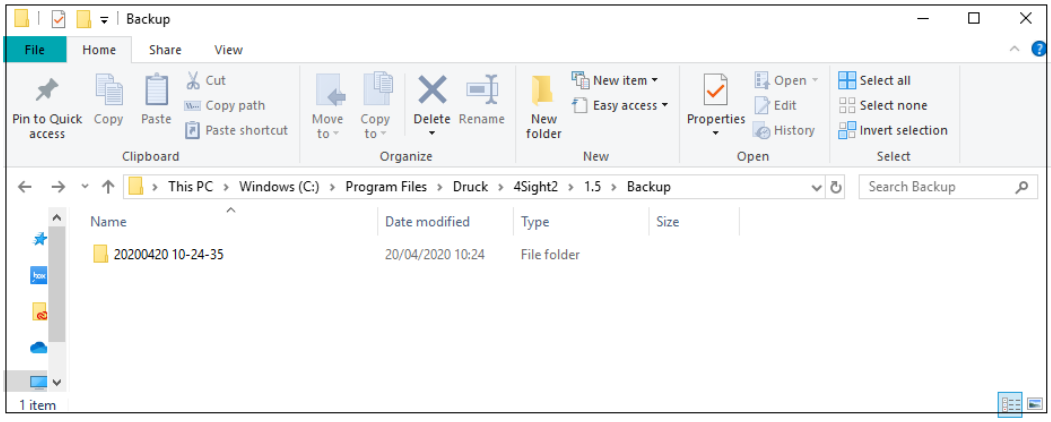
Reportez-vous au guide d'utilisation de 4Sight2 - 123M3138, pour obtenir des informations sur la sauvegarde de base de données Postgres.

7.3 Restauration de la base de données Postgres

On suppose que vous avez déjà effectué une sauvegarde de base de données à l'aide de l'application 4Sight.

L'application 4Sight (version 1.4 et supérieure) propose une interface pour effectuer une sauvegarde (lancée/planifiée par l'utilisateur). Cette opération crée des fichiers dans le répertoire

de sauvegarde situé dans le répertoire d'installation de 4Sight sur le serveur. Chaque sauvegarde crée un nouveau dossier dans le dossier de sauvegarde au format AAAAMMDDHHSS (année, mois, date, heure et seconde) en fonction de la date et heure de fin d'exécution de la sauvegarde.



Il est recommandé de sauvegarder le contenu du dossier de sauvegarde sur un support distinct.

Chaque dossier contient 5 fichiers.

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

Les fichiers *.bck sont accompagnés d'un suffixe indiquant la version de l'application 4Sight. Veuillez vous assurer que vous restaurez une base de données correspondant à la version exacte de votre application. Les versions supérieures/inférieures de bases de données ne sont pas prises en charge par l'application. Notez que la version inclut un trait de soulignement (_) et non un point (.), par exemple, 1_4 et non 1.4. Lorsque vous utilisez les commandes ci-dessous dans les étapes de restauration, veillez à bien remplacer <VERSION_APPLICATION> par la version de 4Sight installée.

Le fichier metadata.properties contient le nom de la sauvegarde tel qu'il est saisi au lancement de la sauvegarde.

Vérification SHA 256

Une sauvegarde comprend 3 fichiers, un pour chaque base de données, portant l'extension .bck. Le fichier metadata.properties contient le SHA 256 de chacun des fichiers de sauvegarde.

1. Ouvrez une invite de commande en tant qu'administrateur et accédez au dossier contenant les fichiers de sauvegarde sélectionnés.
2. Utilisez les commandes ci-dessous pour calculer le SHA 256 de chaque fichier.

   certutil -hashfile 4Sight**<VERSION_APPLICATION>**.bck SHA256

   certutil -hashfile 4Sightaudit**<VERSION_APPLICATION>**.bck SHA256

certutil -hashfile uaa**<VERSION_APPLICATION>**.bck SHA256

3. Avant de passer aux étapes de restauration, vérifiez que le SHA 256 de chaque fichier correspond au SHA 256 indiqué dans le fichier de métadonnées. Un fichier de sauvegarde peut être restauré si la somme de contrôle de l'invite de commande et la somme de contrôle du fichier de métadonnées sont strictement identiques. Ne passez aux étapes de restauration que si elles sont identiques.

7.4 Étapes de restauration :

1. Connectez-vous au serveur 4Sight en tant qu'administrateur.
2. Recherchez le port sur lequel la base de données Postgres est exécutée. Vous le retrouverez dans la propriété spring.datasource.url, dans le fichier <RÉPERTOIRE D'INSTALLATION DE 4Sight>\apache-tomcat\webapps\application.properties. Utilisez un Bloc-notes, exécuté en tant qu'administrateur, pour ouvrir ce fichier. Il s'agit du nombre indiqué juste avant 4Sight**<VERSION_APPLICATION>.**
3. Connectez-vous à l'utilitaire de commande psql à partir d'une invite de commande exécutée en tant qu'administrateur, en utilisant l'utilisateur Postgres.

   C:\Program Files\PostgreSQL\11\bin\psql" --port=<DB_PORT> postgres postgres
4. Vous retrouverez l'utilisateur de base de données utilisé par l'application dans la propriété spring.datasource.username, dans le fichier <RÉPERTOIRE D'INSTALLATION DE 4Sight>\apache-tomcat\webapps\application.properties. Utilisez un Bloc-notes, exécuté en tant qu'administrateur, pour ouvrir ce fichier.
5. Si applicable, supprimez les bases de données *_temp, puis créez les bases de données *_temp vides en exécutant les commandes ci-dessous dans l'invite psql.

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

   Remplacez le propriétaire de base de données des 3 bases de données ci-dessus par cet utilisateur. Notez que le nom d'utilisateur est sensible à la casse.

   ALTER DATABASE "4Sight**<VERSION_APPLICATION>**_temp" OWNER TO "**<UTILISATEUR_BD>**";
   ALTER DATABASE "4Sightaudit**<VERSION_APPLICATION>**_temp" OWNER TO "**<UTILISATEUR_BD>**";
   ALTER DATABASE "uaa**<VERSION_APPLICATION>**_temp" OWNER TO "**<UTILISATEUR_BD>**";
6. Vérifiez les fichiers metadata.properties des sauvegardes et choisissez la sauvegarde que vous devez restaurer.

7. Ouvrez une autre invite de commande en tant qu'administrateur et accédez au dossier contenant les fichiers de sauvegarde sélectionnés ci-dessus.

   Restaurez la base de données à partir des fichiers *.bck en bases de données *_temp à l'aide des commandes ci-dessous. Si un mot de passe vous est demandé, saisissez le mot de passe de super-utilisateur Postgres.

   "C:\Program Files\PostgreSQL\11\bin\pg_restore" --port=**<PORT_BD>** --no-owner --username=postgres --dbname=4Sight**<VERSION_APPLICATION>**_temp -n public --role=**<UTILISATEUR_BD>** 4Sight**<VERSION_APPLICATION>**.bck

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

   "C:\Program Files\PostgreSQL\11\bin\pg_restore" --port=**<PORT_BD>** --no-owner --username=postgres --dbname=uaa**<VERSION_APPLICATION>**_temp -n public --role=**<UTILISATEUR_BD>** uaa**<VERSION_APPLICATION>**.bck

8. Si applicable, supprimez les bases de données *_old en exécutant les commandes ci-dessous dans l'invite psql.

   DROP DATABASE IF EXISTS "4Sight**<VERSION_APPLICATION>**_old";
   DROP DATABASE IF EXISTS "4Sightaudit**<VERSION_APPLICATION>**_old";
   DROP DATABASE IF EXISTS "uaa**<VERSION_APPLICATION>**_old";

9. Arrêtez le service 4Sight et les applications pgadmin ouvertes.

10. Renommez les bases de données 4Sight en *_old en exécutant les commandes ci-dessous dans l'invite psql.

    ALTER DATABASE "4Sight**<VERSION_APPLICATION>**" RENAME TO "4Sight**<VERSION_APPLICATION>**_old";
    ALTER DATABASE "4Sightaudit**<VERSION_APPLICATION>**" RENAME TO "4Sightaudit**<VERSION_APPLICATION>**_old";
    ALTER DATABASE "uaa**<VERSION_APPLICATION>**" RENAME TO "uaa**<VERSION_APPLICATION>**_old";

11. Renommez les bases de données *_temp en bases de données 4Sight en exécutant les commandes ci-dessous dans l'invite psql.

    ALTER DATABASE "4Sight**<VERSION_APPLICATION>_temp**" RENAME TO "4Sight**<VERSION_APPLICATION>**";
    ALTER DATABASE "4Sightaudit**<VERSION_APPLICATION>_temp**" RENAME TO "4Sightaudit**<VERSION_APPLICATION>**";
    ALTER DATABASE "uaa**<VERSION_APPLICATION>_temp**" RENAME TO "uaa**<VERSION_APPLICATION>**";

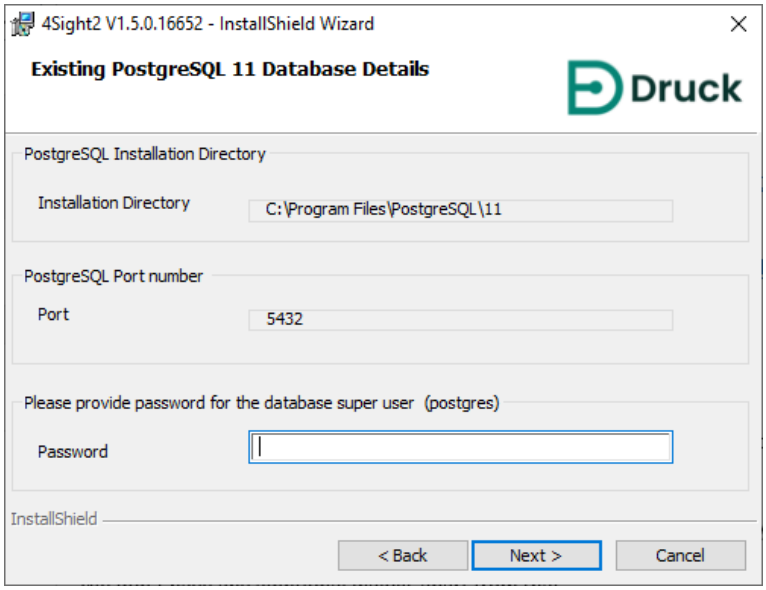
12. Démarrez le service 4Sight et essayez de vous connecter en tant qu'administrateur. Notez que le mot de passe de l'administrateur utilisé au moment de la sauvegarde doit être utilisé ici pour se connecter.

7.5 Comment rétablir le fonctionnement à partir d'une panne de machine 4Sight2 ?

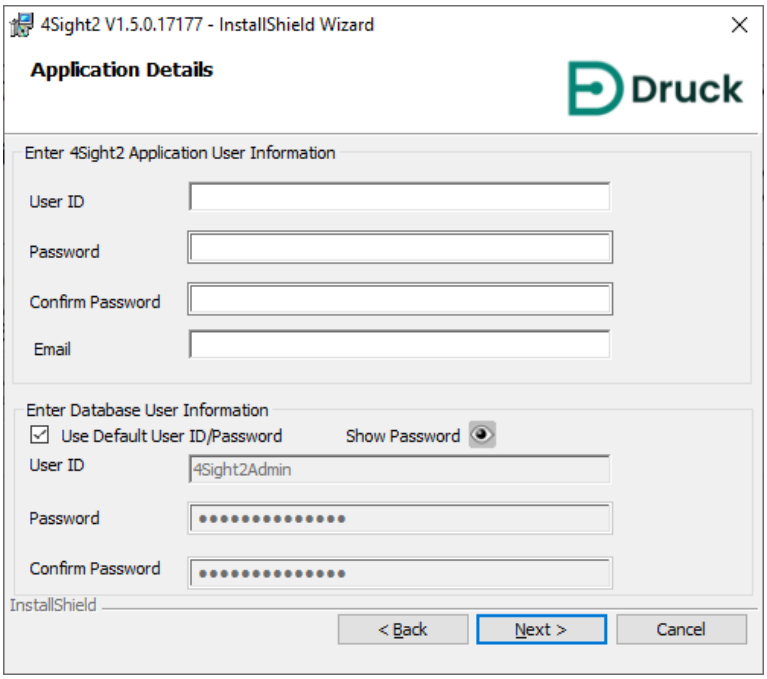
Hypothèses : L'utilisateur a effectué une sauvegarde de la base de données 4Sight2 avant la panne.

L'utilisateur connaît déjà le nom d'utilisateur et le mot de passe pour l'application et la base de données.

1. Configurez la machine avec le système d'exploitation et les pilotes appropriés.
2. Installez 4Sight2 sur la machine.
3. Pendant l'installation de l'application, donnez les mêmes nom d'utilisateur et mot de passe que ceux fournis au préalable pour l'application et la base de données Postgres.

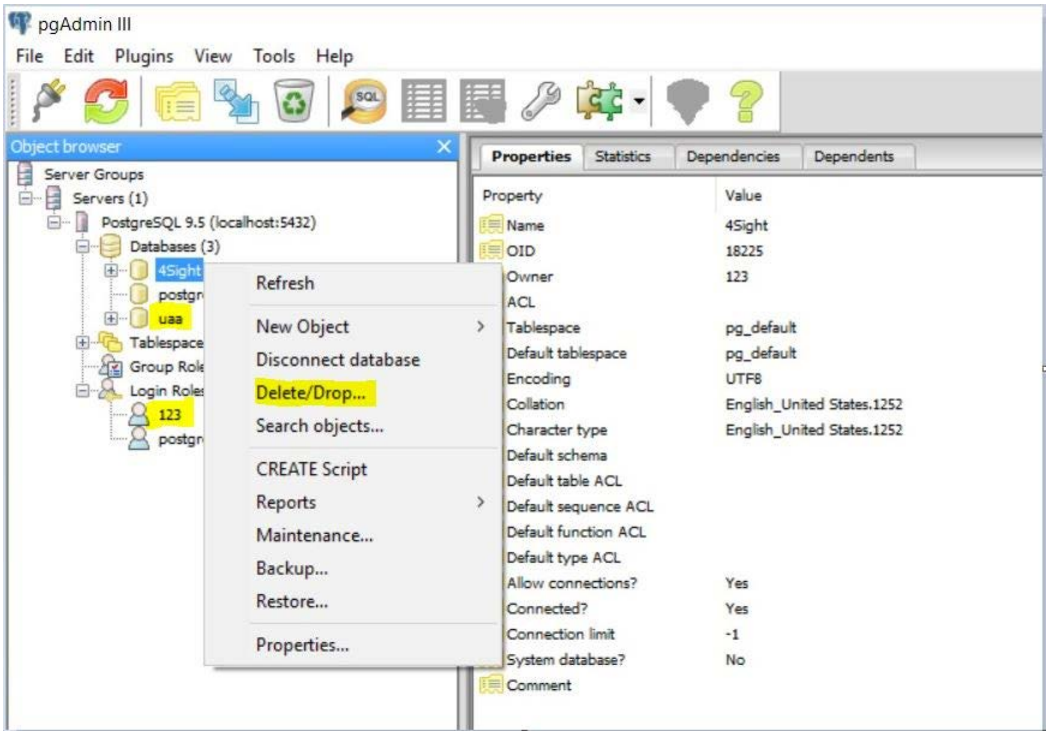


Mot de passe identique à celui de l'installation précédente



Renseignez tous les champs comme lors de l'installation précédente

4. Après avoir mené à bien l'installation de l'application, supprimez la base de données par défaut créée pendant l'installation de l'application à partir de pgAdmin (faites un clic droit sur la base de données et sélectionnez Delete/Drop). Si la suppression de la base de données donne lieu à une erreur, redémarrez le service Postgres et renouvelez la tentative après avoir procédé à l'actualisation.



5. Après avoir mené à bien la suppression de la base de données et de l'utilisateur. Suivez ces étapes pour restaurer la base de données comme expliqué plus haut, à partir de l'invite de commande.
6. Maintenant que vous avez restauré avec succès la base de données, ouvrez l'application à partir du navigateur et examinez celle-ci.

7.6 Scénario d'échec de l'installation :

Le tableau ci-dessous présente les divers scénarios d'échec pendant l'installation et leurs solutions.

Message d'erreur	Scénario	Solution/mesure à prendre
"Insufficient disk space available to install 4Sight2 application. Please ensure a minimum of 4096 MB is available. Free Space : available MB.	Échec dû à un problème de taille de disque dur (si l'espace nécessaire n'est pas disponible au démarrage de la mise à niveau).	L'administrateur doit libérer de l'espace dans le lecteur correspondant, puis réessayer d'appliquer le processus de mise à niveau.
"Deployment fail while Migrating database"	Échec dû à un problème de taille de disque dur (si l'espace suffisant n'est pas disponible après le démarrage de la mise à niveau).	L'administrateur doit libérer de l'espace dans le lecteur correspondant, puis réessayer d'appliquer le processus de mise à niveau.
"Installation failed while migrating Database. Please reinstall 4sight2"	Échec dû à l'intégrité des données lors de la copie de la base de données.	L'administrateur doit contacter le service client si cela se produit. Raison de l'intégrité des données consignée dans les journaux à l'emplacement [C:\Users\[Username]\App Data\Local\Temp\logs]
"Installation failed while migrating Database. Please reinstall 4sight2"	Échec dû à l'intégrité des données lors de l'étape de mise à jour du schéma.	L'administrateur doit contacter le service client si cela se produit. Raison de l'intégrité des données consignée dans les journaux à l'emplacement 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"	Cet échec se produit si le programme d'installation est incapable d'obtenir l'état du service.	L'administrateur doit vérifier que le service 4Sight2 est fonctionnel et en cours d'exécution.

Message d'erreur	Scénario	Solution/mesure à prendre
"Failed to start the 4Sight2 service. Please ensure the 4Sight2 service is present and running"	Échec si l'application est corrompue, certains fichiers sont supprimés ou le port est utilisé par une autre application, ou l'utilisateur a arrêté le service, etc.	Si l'administrateur parvient à obtenir l'état du service et s'il n'est pas en cours d'exécution pour quelque raison que ce soit (par exemple, application corrompue, certains fichiers sont supprimés, le port est utilisé par une autre application ou l'utilisateur a arrêté le service, etc.), le système tente alors de démarrer le service. Si le service ne peut pas démarrer, l'administrateur doit alors contacter le service après-vente pour résoudre le problème.
"Upgrade of 4Sight2 application is supported from version 1.3 onwards. For earlier version upgrade support please contact Customer Care."	La mise à niveau ne sera pas effectuée si une version antérieure à la version 1.3 est installée.	Une mise à niveau est possible uniquement à partir de la version 1.3 vers une version supérieure.
Installer has detected another minor version of PostgreSQL 11. Installer will not continue. Refer to 4Sight2 Installation manual for more details	4Sight2 ne peut poursuivre l'installation de 4Sight2 car une version (variante) de PostgreSQL identique existe sur la machine cible.	Options possibles 1. L'utilisateur peut choisir une autre machine. 2. L'utilisateur sauvegarde l'application existante qui utilise la version 11.3 de Postgres, la désinstalle et la déploie sur une autre machine. Désinstallez Postgres et redémarrez l'installation 4Sight2.
Installation failed while upgrading database. Please reinstall 4Sight2. Refer to 4Sight2 Installation manual for more details	Une erreur interne a pu survenir pendant la mise à niveau. L'utilisateur peut tenter une ré-installation.	Si le problème persiste, l'utilisateur peut consulter le journal d'installation pour en savoir plus.

7.7 Causes d'erreur fréquente

Vous trouverez ci-dessous une liste des problèmes fréquemment observés lors des communications 4sight2 avec les instruments Druck via USB.

- Perte ou instabilité de la connexion physique
- Câbles / ports usés
- Mauvaise qualité des adaptateurs USB
- Adaptateurs USB / ports en surcharge
- Appareils maintenus longtemps en service, ce qui les fait passer en mode veille
- Appareils ne sont pas en mode de communication
- Logiciel de pilote non installé ou non mis à niveau. Les versions de l'application 4Sight2 et des pilotes doivent être identiques pour établir les communications avec le matériel.
- Le firmware des appareils est très ancien.

7.8 Désinstallation de 4Sight2

Si vous devez installer une nouvelle copie de 4Sight2, une nouvelle version de 4Sight2 ou si vous devez désinstaller 4Sight2 en raison de problèmes d'installation, procédez comme suit.

La désinstallation du composant de base de données PostgreSQL supprime la base de données 4Sight2, ce qui conduit à la perte de données. La procédure ci-après n'inclut pas la création d'une sauvegarde automatique, si bien que vous devez effectuer une sauvegarde manuelle avant de suivre cette procédure et enregistrer cette sauvegarde dans un emplacement autre que le dossier d'installation de 4Sight2. Reportez-vous à la section Sauvegarde et restauration de la base de données Postgres, de ce guide.

Si vous choisissez de désinstaller uniquement l'application 4Sight2 et de conserver la base de données, consultez la partie de ce guide consacrée à l'installation de 4Sight2. Pour la ré-installation, vous aurez besoin des identifiants de super-utilisateur de la base de données. Ne vous lancez pas dans une désinstallation de la base de données si vous ne connaissez pas ces identifiants.

Si vous souhaitez mettre à niveau votre version de 4Sight2, sans désinstaller la base de données, **NE SUIVEZ PAS** ces instructions.

1. Allez dans le Panneau de configuration >> Programmes et fonctionnalités.
2. Faites un clic droit sur 4Sight2 et sélectionnez Désinstaller.
3. Suivez les instructions affichées par l'assistant de désinstallation.
4. Faites un clic droit sur PostgreSQL 11 et sélectionnez Désinstaller.
5. Suivez les instructions affichées par l'assistant de désinstallation.
6. La désinstallation de PostgreSQL ne supprime pas le dossier de données. Vous devez effectuer cette suppression manuellement. Supprimez le dossier de données qui se trouve à l'emplacement suivant : C:\Program Files\PostgreSQL\11\
   a. Si vous souhaitez supprimer l'intégralité du dossier PostgreSQL, vérifiez que les fichiers de sauvegarde et les scripts sont retirés du dossier bin avant de poursuivre.
   b. Par défaut, les sauvegardes de base de données 4Sight2 sont créées et enregistrées à l'emplacement suivant : C:\Program Files\PostgreSQL\11\bin
7. Il est conseillé de redémarrer l'ordinateur si possible.
8. 4Sight2 est désormais correctement désinstallé.

7.9 Dépannage des communications sécurisées

1. La commande 'nom de commande' n'est pas reconnue en tant que commande interne ou externe. Par exemple, 'Keytool' n'est pas reconnu en tant que commande interne ou externe.

- Si vous obtenez une telle erreur, cela signifie que dans le dossier actuel, l'invite de commande ne trouve pas la référence à la commande spécifiée.

  Pour résoudre cette erreur, utilisez la commande ci-dessous afin de pointer vers le dossier approprié.

  Set Path=%Path%;"<<chemin complet de l'emplacement où se trouve la commande>>"

  Par exemple, dans l'erreur ci-dessus liée à la commande Keytool', vous devez saisir le chemin ci-dessous,

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

2. Adresse IP erronée

- Si vous obtenez un message d'erreur avec ce texte, cela signifie que l'adresse IP ou le nom d'hôte dans l'un ou l'autre des fichiers openssl-ca.cnf ou openssl-server.cnf est incorrect. Remarque : il vous faudra peut-être rectifier cela en plusieurs endroits dans ces fichiers puis ré-exécuter la procédure.

3. Fichier ou répertoire introuvable...

- Si vous obtenez un message d'erreur avec ce texte, cela signifie que la commande que vous avez exécutée renvoie probablement à un nom de fichier incorrect. Vérifiez dans la commande s'il n'y a pas d'erreurs de nom de fichier et vérifiez aussi que le fichier ainsi nommé est présent dans le dossier, puis ré-exécutez les commandes. Il se peut que vous deviez corriger le nom de fichier dans la commande ou suivre la procédure pour générer les fichiers manquants.
- Cette erreur peut se produire pour les fichiers index.txt et serial.txt car, dans certains cas, l'extension de fichier est ajoutée deux fois au nom, donnant par exemple index.txt.txt.

  Éditez simplement le fichier et enregistrez-le sans l'extension .txt. Assurez-vous que le fichier a une seule extension .txt.

Meilleures pratiques

8. Meilleures pratiques

Durcissement du serveur

L'environnement serveur doit être durci conformément aux directives Microsoft ou CIS.

8.1 Tomcat

- Installez Tomcat dans un dossier sécurisé accessible exclusivement par l'administrateur ou LocalService, tel que *C:\Program Files(x86)*
- Installez Tomcat en tant que service exécuté sur le compte LocalService.
- Supprimez tous les éléments de WebApp, supprimez les applications par défaut non souhaitées.
- Remplacez la page d'erreur par défaut, telle que 404, 403, 500 etc.
- Exécutez HTTPS, activez SSL.
- L'application de gestion doit être exécutée sur SSL.
- Fichier journal individuel d'utilisateur pour chaque application Web.
- Supprimez la bannière du serveur.
- Activez la connexion d'accès.
- Modifiez le port et la commande d'arrêt.

8.2 PostgreSQL

- Tous les comptes à fort privilège tels que pgdba, postgres, depesz doivent être autorisés en connexion locale seulement.
- Vérifiez que la séquence dans le fichier pg-hba.conf est correcte de sorte que l'accès est accordé aux bons utilisateurs
- Configurez pg-hba.conf de sorte que le serveur ne puisse être connecté qu'à partir de la machine locale et non pas via le réseau.

8.3 Meilleures pratiques de pare-feu

Voici quelques-unes des meilleures pratiques qu'il est recommandé de mettre en place avec 4Sight2 concernant les pare-feu :

8.3.1 Politique

1. La configuration de pare-feu doit s'accorder avec la politique de sécurité de l'entreprise.
2. Faites toujours appel au principe de moindre privilège. Refusez tout par défaut. Autorisez le trafic spécifique (utilisation de source, destination et port).
3. Mettez d'abord en place des règles spécifiques et utilisez des règles de suppression explicites.
4. Consignez toutes les actions, notamment les échecs de consignation dans le journal d'audit.

8.3.2 Ressources

1. Surveillez l'utilisation de la mémoire.
2. Surveillez l'utilisation de l'unité centrale.
3. Surveillez l'utilisation de la bande passante.
4. Limitez le nombre d'applications exécutées sur la machine de pare-feu.

8.3.3 Installation et maintenance

1. Limitez l'accès physique à la machine de pare-feu.
2. Utilisez un identifiant utilisateur unique pour l'administration.
3. Suivez des règles strictes concernant les comptes sur la machine.
4. Apportez régulièrement des correctifs aux systèmes d'exploitation, logiciels applicatifs, firmware etc.
5. Archivez régulièrement la base de règles, la configuration et les journaux. Documentez toutes les règles et les modifications apportées selon une procédure de contrôle de source.
6. Effectuez des tests réguliers.
7. Supprimez toute règle inusitée lorsque le service est arrêté.
8. Procédez à l'audit et à l'examen des règles à intervalles réguliers.
9. Surveillez les avis de sécurité à intervalles réguliers.

8.3.4 Sécurité additionnelle

1. Utilisez des inspections dynamiques ("statefull").
2. Utilisez des proxies.
3. Recourez à une inspection et un filtrage de niveau applicatif.

8.3.5 Protection interne

1. Ayez une politique d'utilisation viable.
2. Pare-feu personnel pour chaque utilisateur.
3. Prévention d'intrusion basée sur l'hôte.
4. Surveillance du réseau.
5. Filtrage basé sur le contenu.
6. Contrôle de l'accès sur chaque ordinateur et application.

Bureaux

Siège social

Leicester, Royaume-Uni
Téléphone : +44 (0) 116 2317233
Courriel :
gb.sensing.sales@bakerhughes.com

Allemagne

Francfort
Téléphone : +49 (0) 69-22222-973
Courriel : sensing.de.cc@bakerhughes.com

Australie

Springfield Central
Téléphone : 1300 171 502
Courriel : custcare.au@ge.com

Chine

Beijing
Téléphone : +86 180 1929 3751
Courriel : fan.kai@bakerhughes.com

Chine

Guangzhou
Téléphone : +86 173 1081 7703
Courriel : dehou.zhang@bakerhughes.com

Chine

Shanghai
Téléphone +86 135 6492 6586
Courriel : hensen.zhang@bakerhughes.com

Émirats Arabes Unis

Abou Dabi
Téléphone : +971 528007351
Courriel :
suhel.aboobacker@bakerhughes.com

États-Unis

Boston
Téléphone : 1-800-833-9438
Courriel : custcareboston@bhge.com

France

Toulouse
Téléphone : +33 562 888 250
Courriel : sensing.FR.cc@bakerhughes.com

Inde

Bangalore
Téléphone : +91 9986024426
Courriel :
aneesh.madhav@bakerhughes.com

Italie

Milan
Téléphone : +39 02 36 04 28 42
Courriel : csd.italia@bakerhughes.com

Japon

Tokyo
Téléphone : +81 3 6890 4538
Courriel : gesitj@bakerhughes.com

Pays-Bas

Hoevelaken
Téléphone : +31 334678950
Courriel :
nl.sensing.sales@bakerhughes.com

Russie

Moscou
Téléphone : +7 915 3161487
Courriel :
aleksey.khamov@bakerhughes.com

Centres de service et d'assistance

Assistance technique

Monde
Courriel :
mstechsupport@bakerhughes.com

Brésil

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

Chine

Changzhou
Téléphone : +86 400 818 1099
Courriel :
service.mcchina@bakerhughes.com

Émirats Arabes Unis

Abou Dabi
Téléphone : +971 2 4079381
Courriel : gulfservices@bakerhughes.com

États-Unis

Billerica
Téléphone : +1 (281) 542-3650
Courriel : namservice@bakerhughes.com

France

Toulouse
Téléphone : +33 562 888 250
Courriel : sensing.FR.cc@bakerhughes.com

Inde

Pune
Téléphone : +91 213 5620426
Courriel :
mcsindia.inhouseservice@bakerhughes.com

Japon

Tokyo
Téléphone : +81 3 3531 8711
Courriel :
service.druck.jp@bakerhughes.com

Royaume-Uni

Leicester
Téléphone : +44 (0) 116 2317107
Courriel :
sensing.grobycc@bakerhughes.com

123M3140 Révision F | Français

Baker Hughes