Druck

4Sight2

Kalibriermanagementsoftware

Installationshandbuch 123M3140 Revision F

Inhaltsverzeichnis

1. Einleitung

Die Kalibriersoftware 4Sight2 ist ein webbasiertes Kalibriermanagementtool, das die Wartung und Kontrolle von Kalibrierumgebungen mit höchsten messtechnischen Standards unterstützt. Die Software kann für folgende Aufgaben verwendet werden:

- Verwaltung der Kalibrierung sämtlicher Messgeräte für einen bestimmten Unternehmensstandort
- Einrichtung eines Zeitplans für die Kalibrieraufgaben für Techniker
- Hoch- und Herunterladen von Daten auf bzw. von portablen Druck Kalibratoren (DPI620 Genii, DPI611 und DPI612), die über einen USB-Anschluss kommunizieren
- Verwaltung der Kalibrieraufzeichnungen für Geräte, die nicht von einem portablen Kalibrator unterstützt werden (manuelle Datenerfassung)
- Prüfung der Aufzeichnungen zur Kalibrierhistorie. Alle Kalibrierzertifikate können auch permanent aufgezeichnet werden. Beispiel: Für Qualitätskontrollverfahren nach ISO 9000
- Regelung für die automatisierte Kalibrierung mit Druckreglern (PACE 1000, 5000 & 6000), portablen Kalibratoren (DPI620 Genii, DPI611 und DPI612) und Temperaturkalibratoren (DryTC 165, DryTC 650, LiquidTC 165 und LiquidTC 255) von Druck

1.1 Zielgruppe

1.1.1 Administratoren

Ein Administrator ist für die Installation und Konfiguration der 4Sight2-Software verantwortlich. Nach der Erstinstallation von 4Sight2 ist ein einzelnes Administratorkonto verfügbar. Über dieses Konto können neue Benutzer erstellt und Gruppen/Berechtigungssets zugewiesen werden. Benutzer mit administrativen Rechten haben Lese- und Schreibzugriff auf alle Funktionen von 4Sight2.

1.1.2 Supervisor

Ein Supervisor ist für die Verwaltung von Geräten und der Kalibrierung verantwortlich. Er kann Geräte innerhalb des 4Sight2-Unternehmens erstellen und aktualisieren, einschließlich Werke, Standorte, Tags und Geräte. Supervisor sind für die Verknüpfung von Dokumenten mit Geräten zuständig, z. B. Werksprozesse und Gerätedatenblätter. Supervisor können die Prüfverfahren erstellen, die bei der Kalibrierung angewendet werden, Verfahren planen und den Zustand von Geräten übewachen. Supervisor sind berechtigt, Kalibrierungen zu genehmigen.

1.1.3 Techniker

Techniker sind für die Durchführung von Kalibrierungen verantwortlich. Kalibrierungen können portabel, manuell oder automatisiert sein, und der Techniker führt den jeweiligen Kalibrierungstyp an einem Gerät aus. Nachdem eine Kalibrierung durchgeführt wurde, können Techniker die Ergebnisse überprüfen und Kalibrierungen abschließen, die von einem Supervisor freigegeben wurden.

1.1.4 Prüfer

Ein Prüfer ist für die Überprüfung von Berichten zuständig. In manchen Werken ist die Auditierung gesetzlich vorgeschrieben.

2. Systemvoraussetzungen

Im Folgenden sind die mindestens erforderlichen Systemvoraussetzungen für die Installation von 4Sight2 auf Server- und Client-Computern aufgeführt:

2.1 Anwendungsserver

Betriebssystem	Windows 10, Windows Server 2012 R2, Windows Server 2016, Windows Server 2019
Updates	Sämtliche Windows-Updates sind installiert
Prozessor	Quad Core
RAM	8 GB oder mehr (32 GB empfohlen)
Festplattenspeicher	1 TB
Netzwerkgeschwindigkeit	10 MBit/s

2.2 Client-Arbeitsstation

Betriebssystem	Windows 10, Windows Server 2012 R2, Windows Server 2016, Windows Server 2019
Browser	Google Chrome V80+, Microsoft Edge V80, Firefox V74
Adobe Reader	Adobe Acrobat Reader DC Version 2015.017.20050 +
RAM	8 GB oder mehr
Prozessor	Dual Core
Festplattenspeicher	600 GB
Netzwerkgeschwindigkeit	10 MBit/s

2.3 Lokale Installation

Betriebssystem	Windows 10, Windows Server 2012 R2, Windows Server 2016, Windows Server 2019
Updates	Sämtliche Windows-Updates sind installiert
Adobe Reader	Adobe Acrobat Reader DC Version 2015.017.20050 +
Prozessor	Dual Core
RAM	16 GB oder mehr (32 GB empfohlen)
Festplattenspeicher	500 GB oder mehr Speicherplatz auf der Festplatte
Browser	Google Chrome V80+, Microsoft Edge V80, Firefox V74

2.4 Von 4Sight2 unterstützte Firmware

Die neuesten Informationen zu unterstützter Firmware finden Sie unter dem folgenden Link:

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

oder

Stecken Sie für PACE den USB B für die 4Sight2-Kommunikation wie in der Abbildung unten gezeigt ein:

Installation von 4Sight2

3. Installation von 4Sight2

Um 4Sight2 zu installieren, kopieren Sie zuerst die ZIP-Datei „4Sight2 Setup“ auf Ihren Desktop und extrahieren Sie die Dateien. Wählen Sie in den Setup-Dateien die ausführbare 4Sight2-Datei aus.

Hinweis: Die folgende Antivirensoftware wird verwendet, um 4Sight2- und CommServer-Installationen zu scannen:

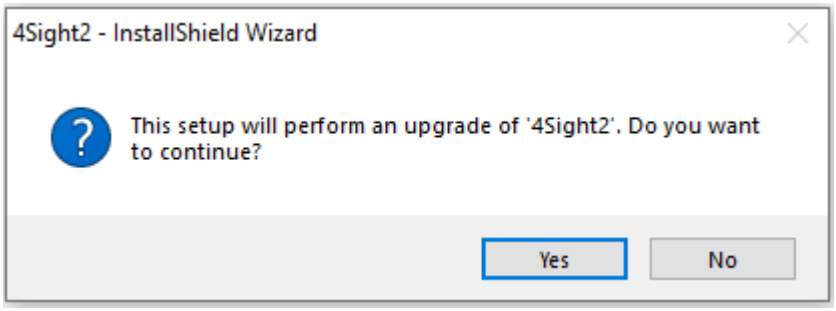
- McAfee VirusScan Enterprise + AntiSpyware Enterprise, Versionsnummer: 8.8.0
- Symantec Endpoint Protection, Versionsnummer: 14.3.558

Sobald Sie die Setup-Datei ausführen, wird der InstallShield-Assistent gestartet. Der InstallShield-Assistent führt die Installation von 4Sight2 in zwei Phasen aus:

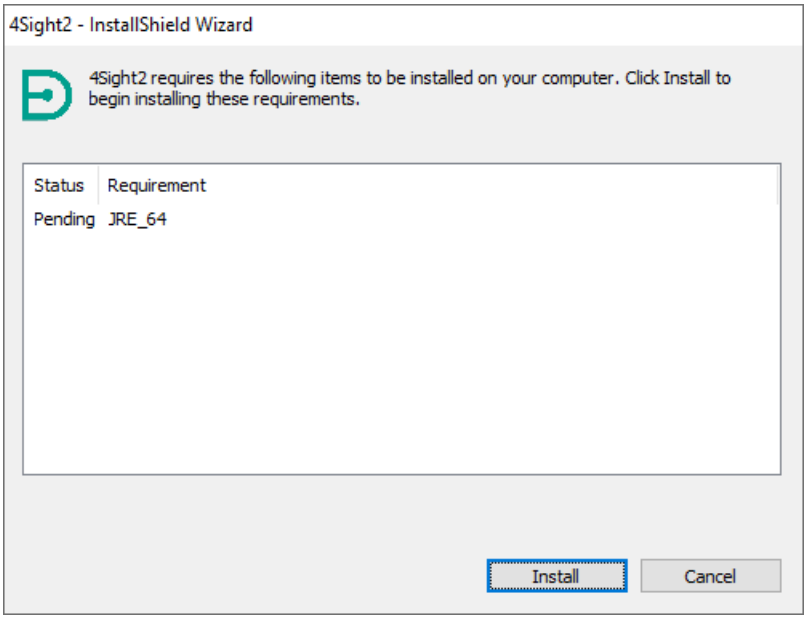
1. Installation der Datenbank
2. Installation der Web-Anwendung

Folgen Sie den Anweisungen des InstallShield-Assistenten oder führen Sie den Installationsvorgang wie in den beiden folgenden Abschnitten beschrieben aus.

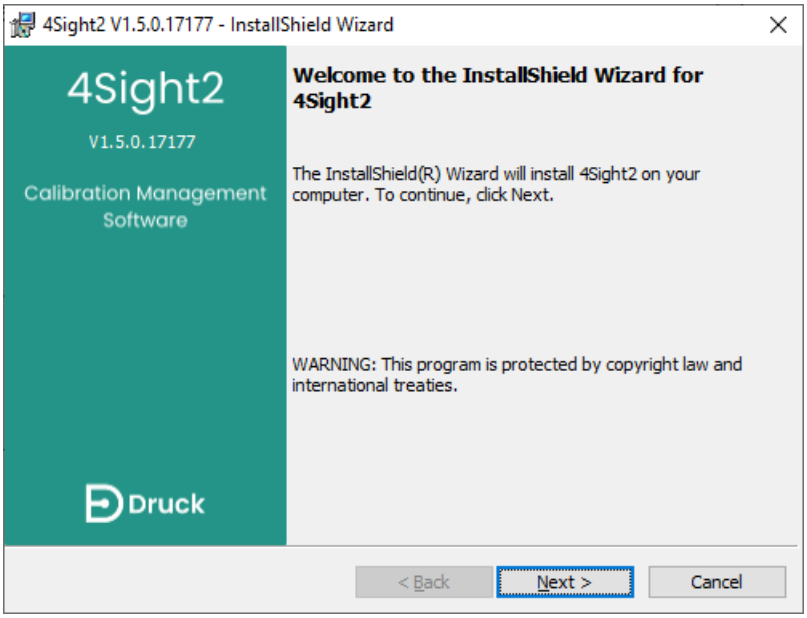
1. Wenn 4Sight2 bereits auf dem Computer installiert ist, werden Sie vom Installationsassistenten dazu aufgefordert, ein Upgrade auf eine aktuelle Version durchzuführen. Klicken Sie auf **Ja**, um das neueste Upgrade durchzuführen.



2. Wenn 4Sight2 zum ersten Mal auf dem Computer installiert wird, zeigt der Installationsassistent den folgenden Bildschirm an. Wählen Sie **Installieren**, und die angezeigten Elemente werden installiert.



3. Nachdem ggf. die Installation der Softwarevoraussetzungen abgeschlossen ist, wird der Begrüßungsbildschirm des InstallShield-Assistenten angezeigt. Klicken Sie auf **Weiter**, um fortzufahren.



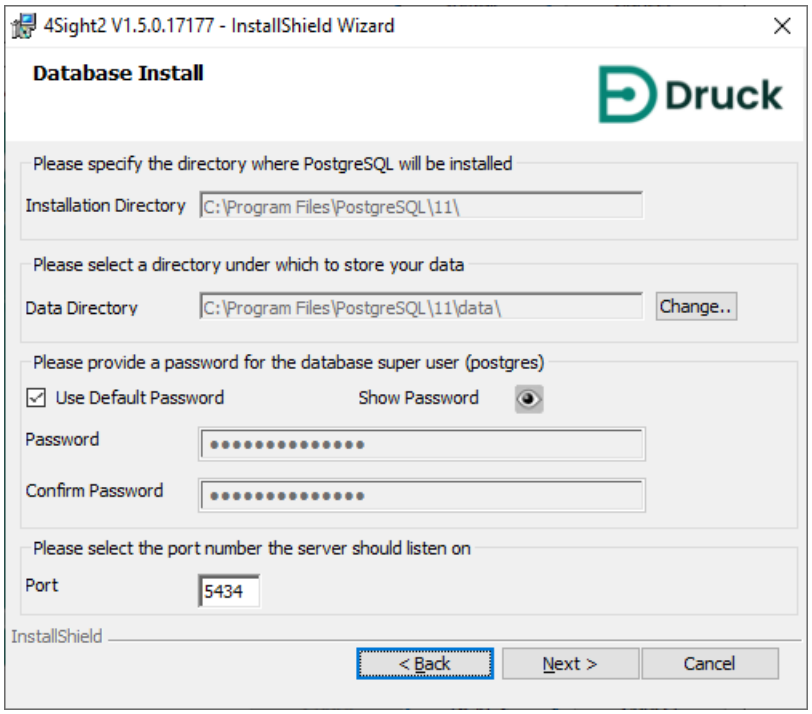
3.1 Installation der Datenbank

Die 4Sight2-Anwendung verwendet eine PostgreSQL-Datenbank. Im Folgenden finden Sie eine Anleitung zur Installation der PostgreSQL-Datenbank sowie die Schritte, die erforderlich sind, falls bereits eine PostgreSQL-Datenbank installiert ist.

3.2 Installation von PostgreSQL

Führen Sie diese Schritte aus, sofern auf dem Computer noch keine PostgreSQL-Datenbank installiert ist.

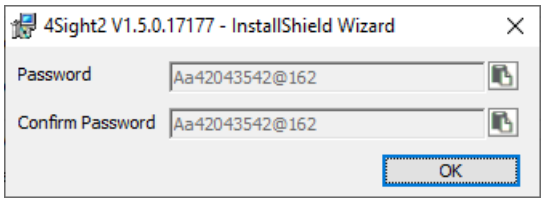
1. Sofern auf dem Computer keine Instanz der PostgreSQL-Datenbank installiert ist, zeigt der Installationsassistent den folgenden Bildschirm an.



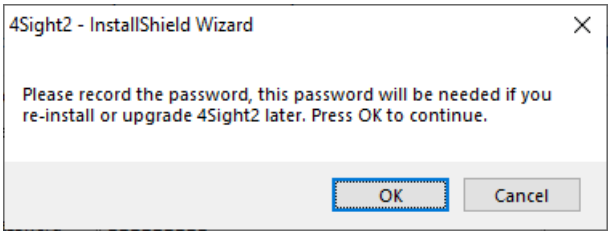
Installationsverzeichnis: Wählen Sie das Verzeichnis aus, in dem die PostgreSQL-Anwendung installiert werden soll.
Datenverzeichnis: Wählen Sie das Verzeichnis aus, in dem die PostgreSQL-Datenbank gespeichert werden soll.
Kennwort/Kennwort bestätigen: Geben Sie das Kennwort für den Superuser der PostgreSQL-Datenbank ein. Diese Eingabe wird nur angefordert, wenn die PostgreSQL-Datenbank erstmalig installiert wird.
Hinweis: Dieses Kennwort wird nach der Installation für den Zugriff auf die Datenbankinhalte benötigt.
Port: Dies ist die Adresse des Ports, an dem die PostgreSQL-Datenbank Anforderungen erhält.

Hinweis: Wenn die Portnummer bereits belegt ist, wenden Sie sich an das IT-Team. Sie können die Portnummer auch ändern. Notieren Sie sich die geänderte Portnummer, um sie zur Hand zu haben, wenn Sie die Anwendung später starten.

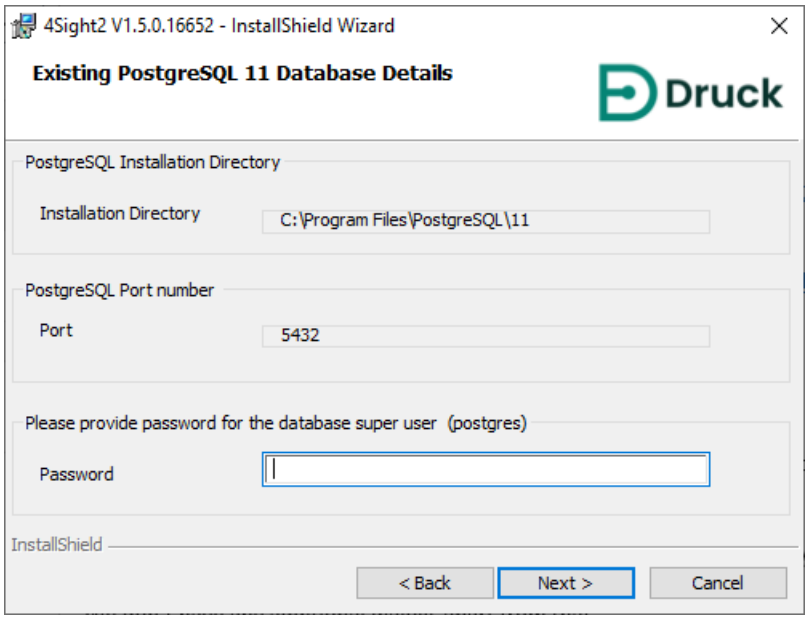
Wichtig: Der Benutzer muss sich das Kennwort für die Datenbank notieren. Der Verlust des Kennworts kann dazu führen, dass der Zugriff auf die Datenbank verweigert wird oder Daten verloren gehen. Deaktivieren Sie das Kontrollkästchen „Benutzer-Standardkennwort“, um das Superuser-Kennwort für die Datenbank zu aktualisieren. Wenn Sie das Standardkennwort behalten oder das eingegebene neue Kennwort anzeigen möchten, wählen Sie das Symbol (Kennwort einblenden) aus. Um das Kennwort in die Zwischenablage zu kopieren, klicken Sie auf das Symbol (In Zwischenablage kopieren).



Sie werden dann vom Installationsprogramm erneut aufgefordert, sich das Kennwort zu notieren. Klicken Sie auf **OK**, nachdem Sie sich das Kennwort notiert haben.

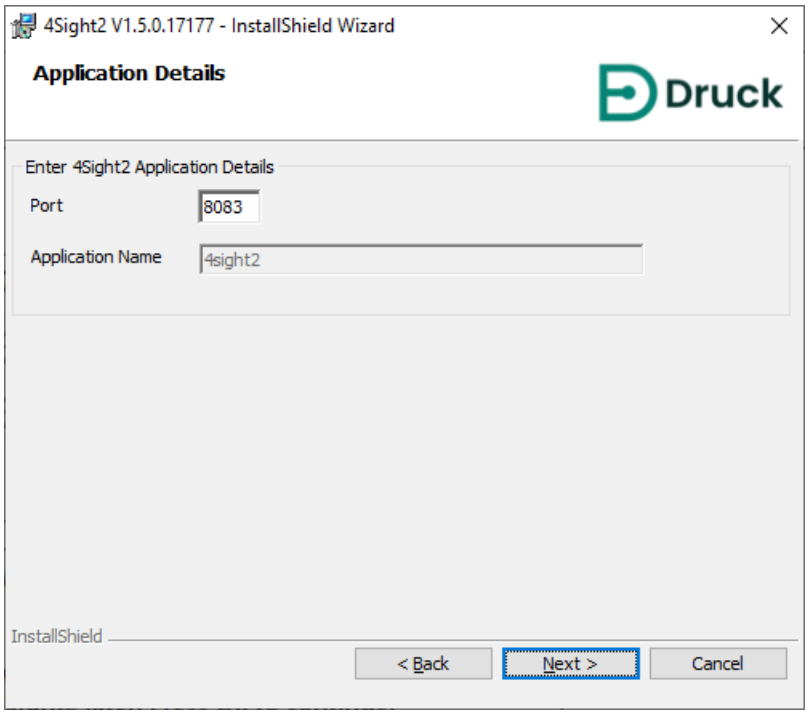


2. Dieser Schritt wird nur angezeigt, wenn die PostgreSQL-Datenbank bereits installiert ist.



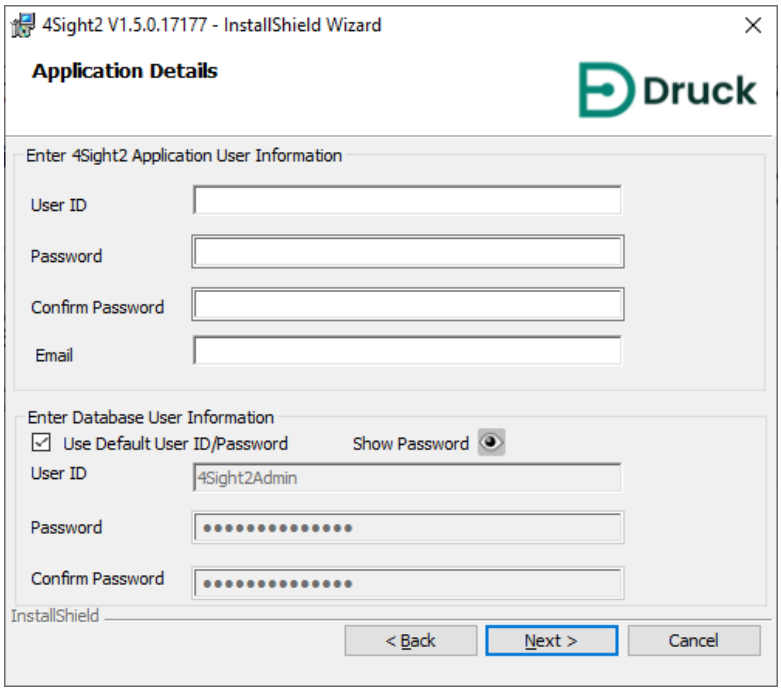
Installationsverzeichnis: Hier wird der Pfad angezeigt, unter dem PostgreSQL bereits installiert ist. Diese Information ist schreibgeschützt.
Kennwort: Geben Sie hier das Superuser-Kennwort für die PostgreSQL-Datenbank zur Bestätigung noch einmal ein.
Port: Dies ist die Nummer des Ports, über den die PostgreSQL-Datenbank Anforderungen ausführt.

3. Geben Sie in das Fenster „Anwendungsdetails“ die folgenden Daten ein.



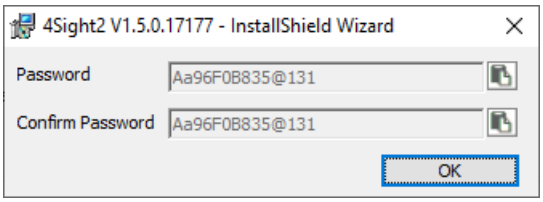
Port: Geben Sie den Port des Tomcat-Webservers ein, den die 4Sight2-Webanwendung verwendet, um auf HTTP-Anfragen zu antworten.
Anwendungsname: Geben Sie den Pfad für den Anwendungskontext ein, den Sie verwenden, um in Ihrem Browser eine Verbindung zur 4Sight2-Anwendung herzustellen. Standardmäßig ist dies 4sight2.
Hinweis: Wenn die Portnummer bereits belegt ist, wenden Sie sich an das IT-Team. Sie können die Portnummer auch ändern. Notieren Sie sich die geänderte Portnummer, um sie zur Hand zu haben, wenn Sie die Anwendung später starten.

4. Klicken Sie auf **Weiter**, und der Bildschirm „Informationen zum Anwendungsbenutzer“ wird angezeigt.

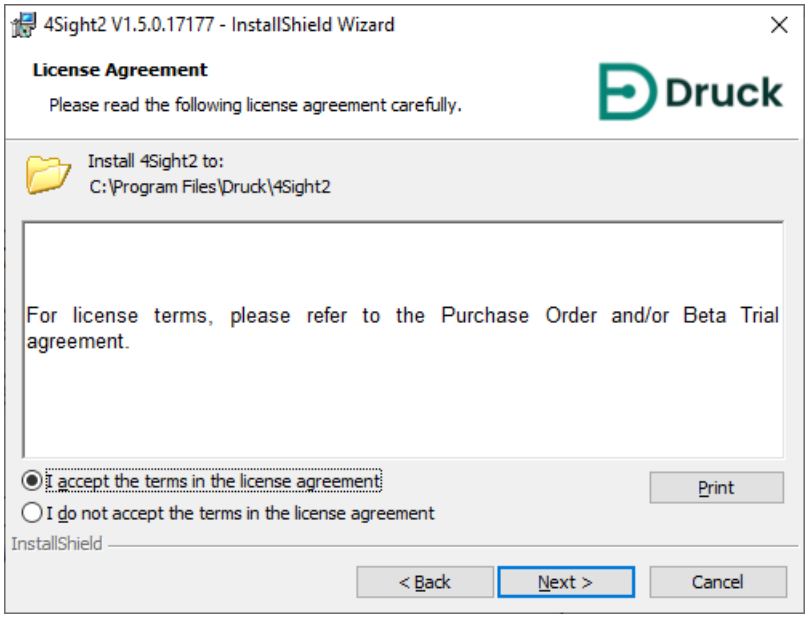


Informationen zum Anwendungsbenutzer: Geben Sie in diesem Abschnitt den Namen und das Kennwort des Superusers für den Zugriff auf die 4Sight2-Anwendung ein.
Hinweis: Dieses Kennwort wird bei der Installation für den Zugriff auf die 4Sight2-Anwendung benötigt.
Informationen zum Datenbankbenutzer: Geben Sie in diesem Abschnitt den Namen und das Kennwort des Datenbankbenutzers ein, den die 4Sight2-Anwendung für die Kommunikation mit der PostgreSQL-Datenbank verwendet.

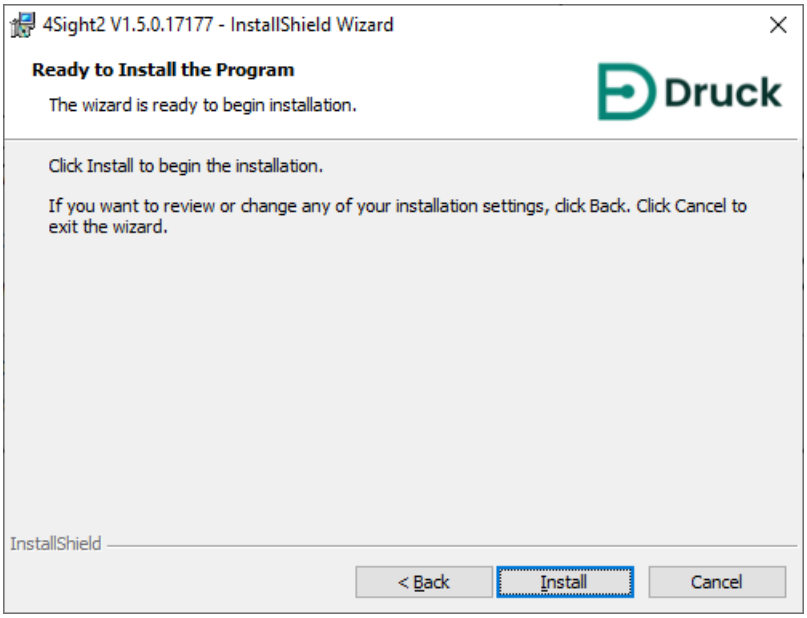
Wichtig: Der Benutzer muss sich das Kennwort für die Datenbank notieren. Der Verlust des Kennworts kann dazu führen, dass der Zugriff auf die Datenbank verweigert wird oder Daten verloren gehen. Deaktivieren Sie das Kontrollkästchen „Benutzer-Standardkennwort“, um das Superuser-Kennwort für die Datenbank zu aktualisieren. Wenn Sie das Standardkennwort behalten oder das eingegebene neue Kennwort anzeigen möchten, wählen Sie das Symbol (Kennwort einblenden) aus. Um das Kennwort in die Zwischenablage zu kopieren, klicken Sie auf das Symbol (In Zwischenablage kopieren).



5. Nachdem Sie die Lizenzbedingungen gelesen haben, aktivieren Sie die Optionsschaltfläche „Ich stimme den Lizenzbedingungen zu“ und klicken Sie dann auf **Weiter**.

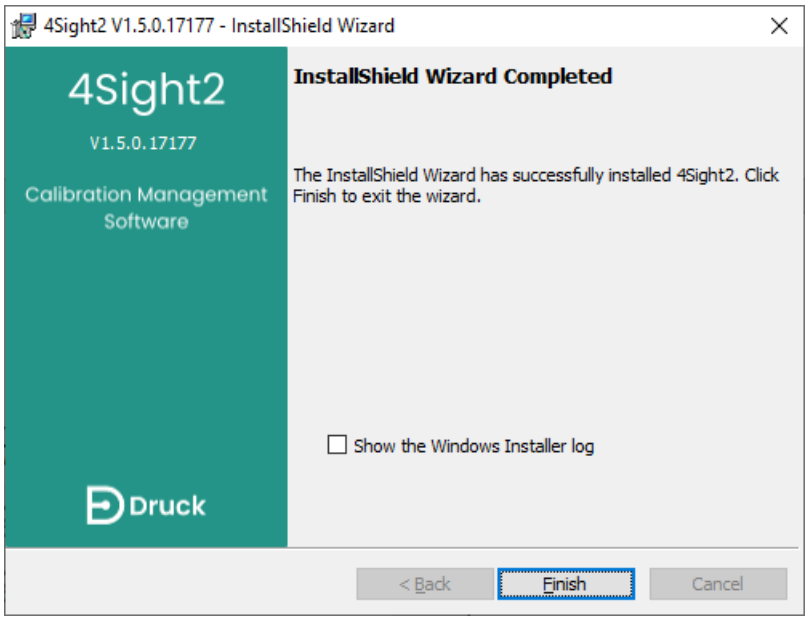


6. Klicken Sie auf **Installieren** und starten Sie die Installation. Alle zur 4Sight2-Anwendung gehörenden Softwarepakete und die Datenbank werden installiert.



Die 4Sight2-Anwendung wurde erfolgreich eingerichtet.

7. Klicken Sie auf die Schaltfläche **Fertig stellen**, um das Fenster zu schließen. Folgen Sie der Anleitung im nächsten Abschnitt, um sich bei der 4Sight2-Anwendung anzumelden.



Um sich lokal auf dem Server bei 4Sight2 anzumelden, wechseln Sie zu

http://Computername oder IPAdresse:PortNr/Anwendungsname

- **Computername** – Der Name des PCs, auf dem die 4Sight2-Anwendung installiert wurde. Sie finden ihn, wenn Sie mit der rechten Maustaste auf „Dieser PC“ klicken und „Eigenschaften“ auswählen.
- **IPAdresse** – Die IP-Adresse des PCs, auf dem die 4Sight2-Anwendung installiert wurde. Sie finden diese Adresse, indem Sie in einer Windows-Eingabeaufforderung „ipconfig“ eingeben.
- **PortNr** – Die Nummer des Ports, den Sie bei der Installation als Tomcat-Port angegeben haben.
- **Anwendungsname** – Der Name, den Sie bei der Installation als Anwendungsnamen eingegeben haben.

Installation des 4Sight2-Prüfmittelkommunikators

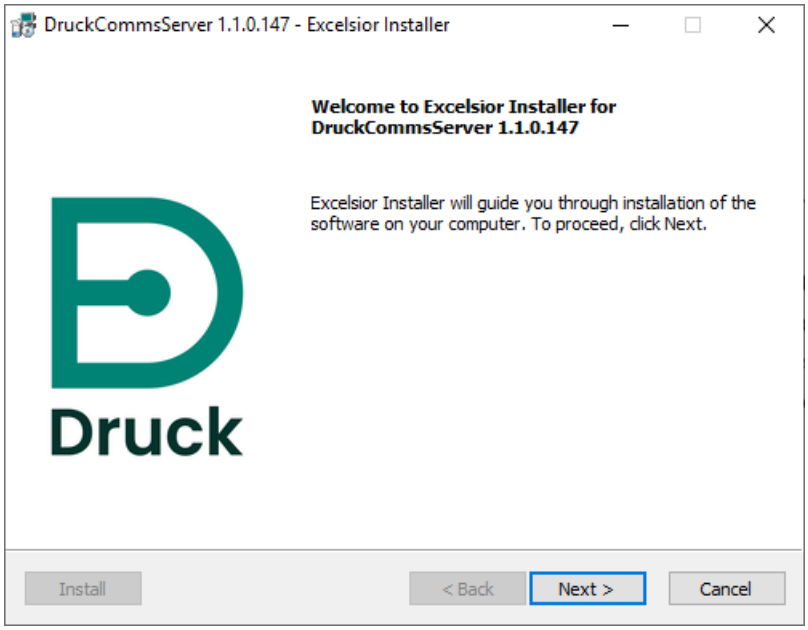
4. Installation des 4Sight2-Prüfmittelkommunikators

1. Der Prüfmittelkommunikator ermöglicht es Ihren Druck Instrumenten, mit der 4Sight2-Anwendung zu kommunizieren. Der Prüfmittelkommunikator kann entweder aus dem Setup-Ordner von 4Sight2 installiert oder bei der ersten Gerätekommunikation mit 4Sight2 heruntergeladen werden. Wenn der Prüfmittelkommunikator in der Setup-Datei nicht verfügbar ist, gehen Sie folgendermaßen vor: Melden Sie sich als Benutzer mit administrativen Rechten bei 4Sight2 an. Nachdem die Anwendung ausgeführt wird und ein Bereich erstellt wurde, gehen Sie zu „Kalibrierung > Portabel“ (Hinweise zur Navigation und Erstellung von Bereichen finden Sie in der 4Sight2-Bedienungsanleitung). Klicken Sie auf die Schaltfläche „Aktualisieren“ neben der Dropdownliste „Prüfmittel“. Wenn der Prüfmittelkommunikator nicht ausgeführt wird, erscheint folgende Meldung:

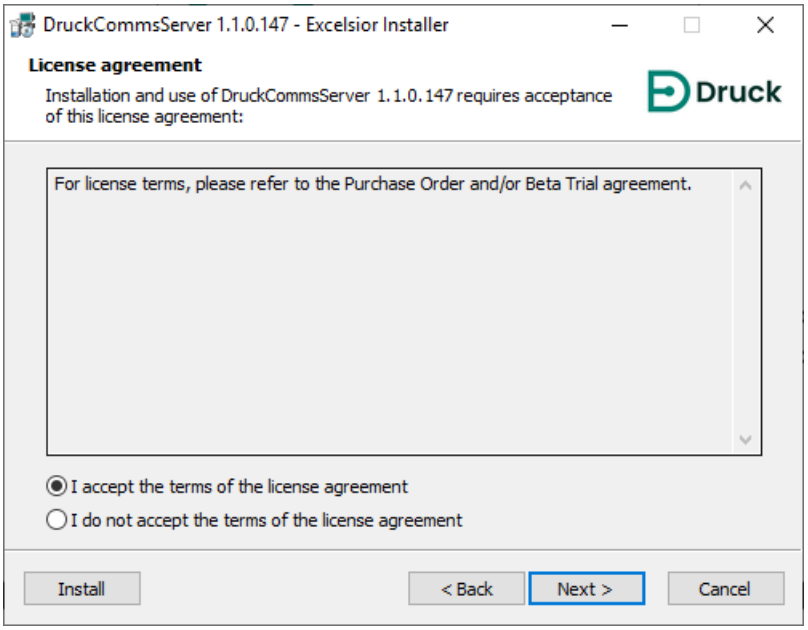
Kommunikation mit Prüfmittel nicht möglich

Laden Sie sich das Prüfmittelkommunikator-Paket herunter. Entpacken Sie das Paket nach dem Herunterladen und führen Sie die Datei „setup.exe“ aus, um die Software zu installieren. Hinweise zur Installation und zur Fehlerbehebung finden Sie im Installationshandbuch. Bitte wenden Sie sich wegen Unterstützung an Ihren Administrator.

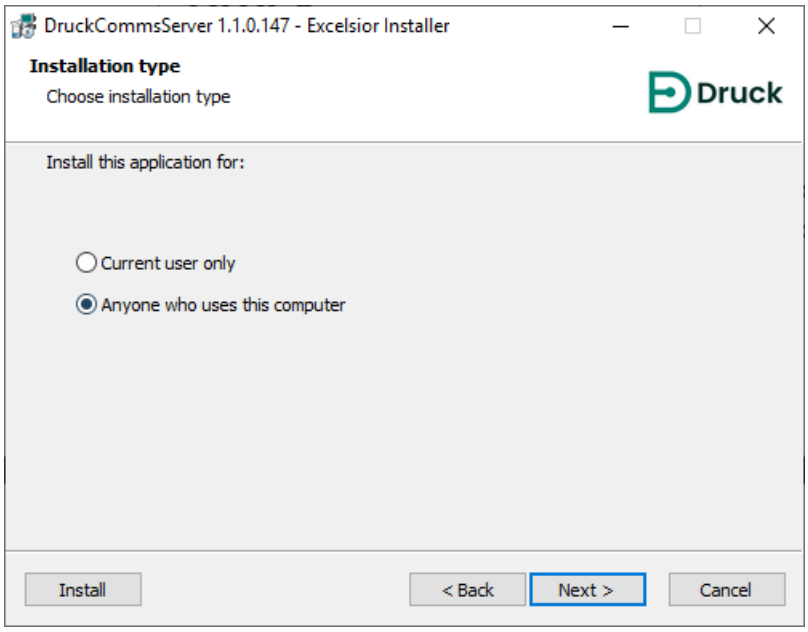
2. Klicken Sie auf **Herunterladen**, um die Setup-Datei für den Prüfmittelkommunikator herunterzuladen.
3. Die Setup-Dateien für den Prüfmittelkommunikator werden in der ZIP-Datei „CommsServerInstall“ heruntergeladen. Nachdem die ZIP-Datei heruntergeladen wurde, können Sie dieselben Schritte vor und nach der Installation von 4Sight2 ausführen.
4. Extrahieren Sie die Dateien aus der ZIP-Datei „CommsServerInstall“ und doppelklicken Sie auf die Datei „setup.exe“, um das Installationsprogramm auszuführen.
5. Das Installationsprogramm „DruckCommsServer“ wird angezeigt. Befolgen Sie die Anweisungen im Installationsprogramm oder in diesem Handbuch.



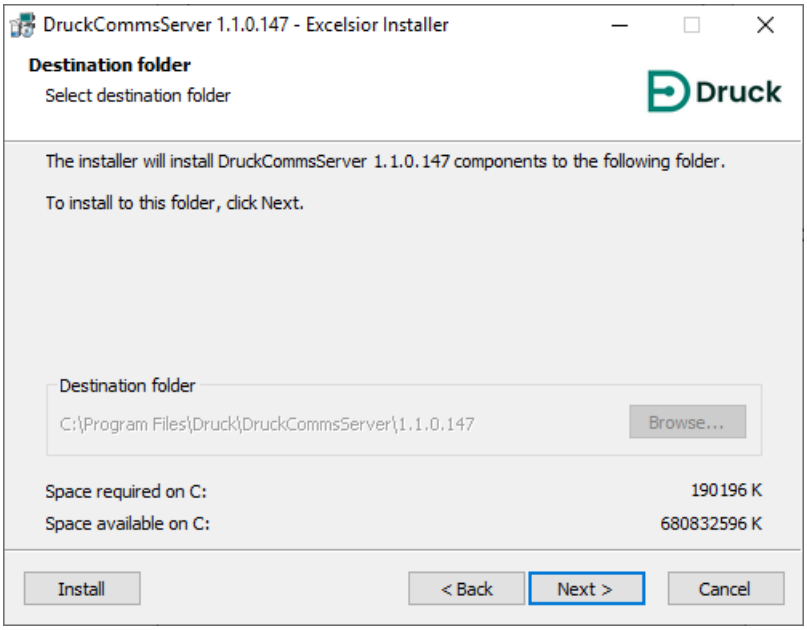
6. Wählen Sie **Weiter**, um den Bildschirm „Lizenzvereinbarung“ anzuzeigen, und lesen Sie die Lizenzbedingungen. Wenn Sie damit einverstanden sind, markieren Sie das Kontrollkästchen **Ich stimme den Lizenzbedingungen zu** und klicken Sie dann auf **Weiter**, um fortzufahren.



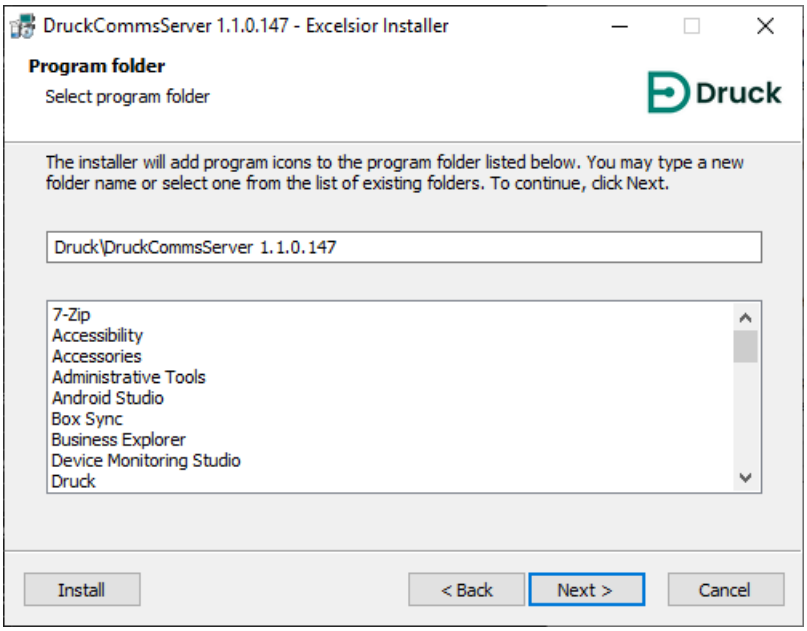
7. Wählen Sie auf dem Bildschirm „Installationsart“, ob Sie den CommsServer für alle Benutzer dieses PCs oder nur für den aktuellen Benutzer installieren möchten.



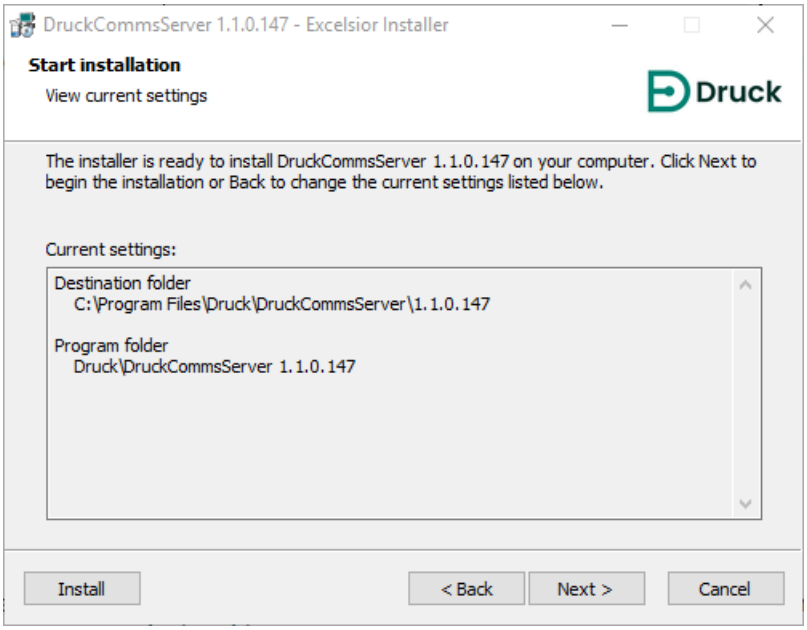
8. Der Bildschirm „Zielordner“ zeigt den Ordner an, in dem der DruckCommsServer installiert wird. Dies ist standardmäßig „C:\Programme\Druck\DruckCommsServer\[Anwendungsversion]“.



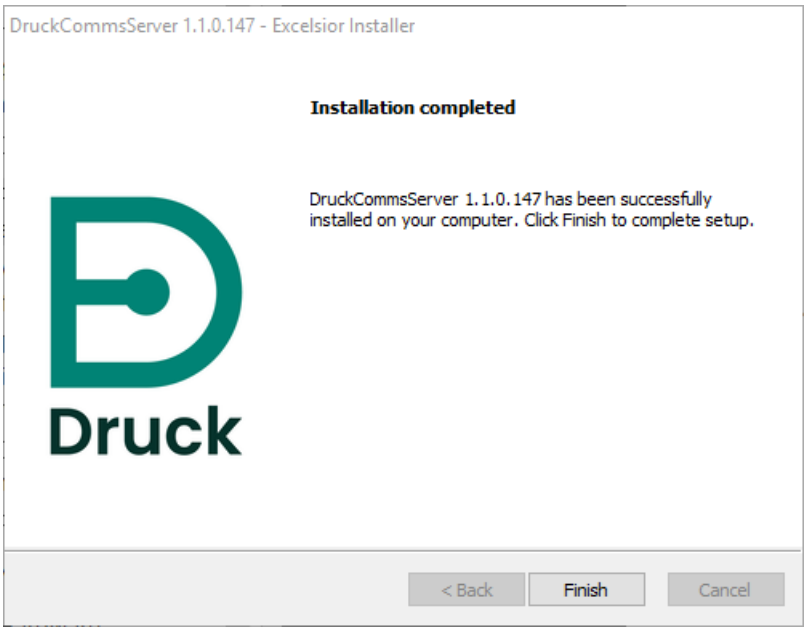
9. Auf dem Bildschirm „Programmordner“ können Sie wählen, wo das Installationsprogramm das Programmsymbol zum Programmordner hinzufügt.



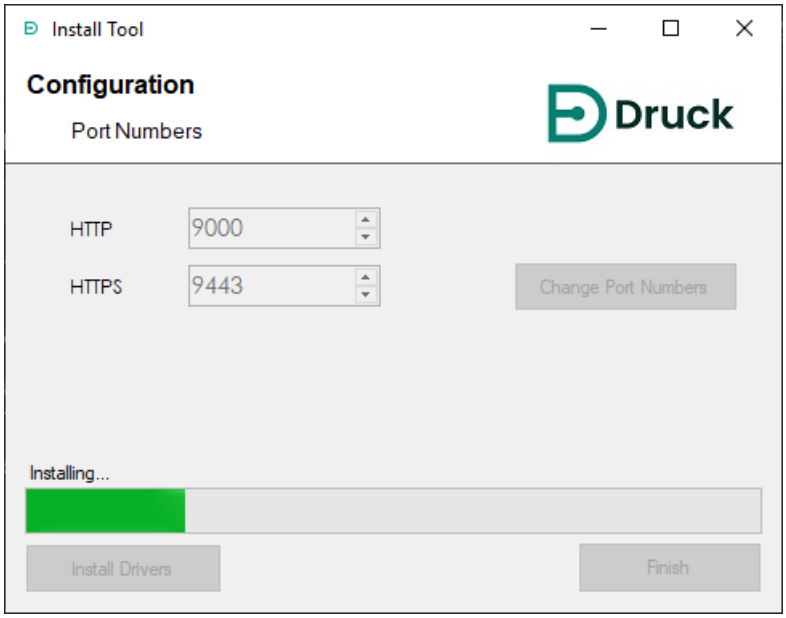
10. Danach wird der Bildschirm „Installation starten“ angezeigt. Klicken Sie auf **Weiter**, um die Installation zu starten.



11. Wenn die Installation abgeschlossen ist, klicken Sie auf **Fertig stellen**.

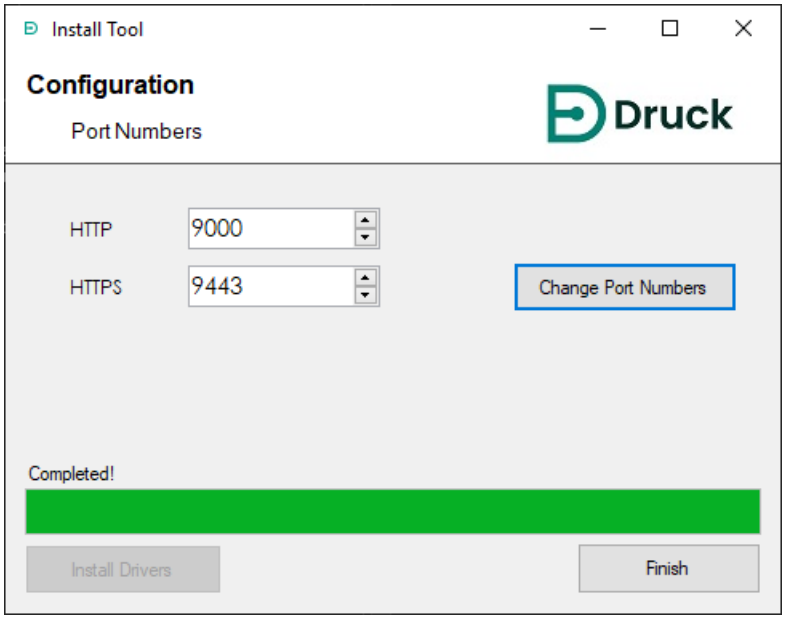


12. Als Nächstes wird das CommsServer-Installationstool angezeigt, um die weiteren erforderlichen Treiber zu installieren.



13. Wenn Sie sich nicht sicher sind, ob 4Sight2 alternative Portnummern verwendet, wenden Sie sich bitte an Ihren Benutzer mit administrativen Rechten.

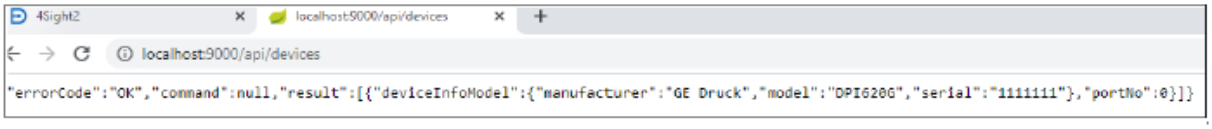
Hinweis: Das Installationstool kann nach der Installation separat ausgeführt werden, um diese Portnummern neu zu konfigurieren.



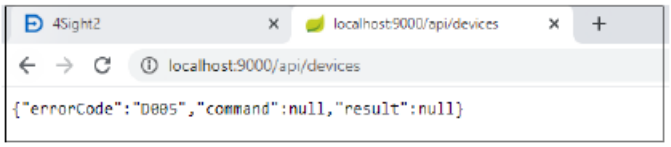
14. Testen Sie die Installation des Prüfmittelkommunikators, indem Sie die folgende URL in Ihren Webbrowser eingeben:

    http:/localhost:[oben verwendete HTTP-Portnummer, Standardeinstellung: 9000]/api/devices

Im Webbrowser sollte eine Liste mit allen Geräten angezeigt werden, die Sie verbunden haben:



Wenn keine Geräte verbunden sind, sehen Sie Folgendes:



Hinweis: Die für Temperaturkalibratoren benötigten Treiber werden nicht automatisch konfiguriert. Siehe Abschnitt 4.3, “Treiberkonfiguration für Temperaturkalibratoren“.

15. Wenn die Installation der Gerätetreiber fehlschlägt, führen Sie die Schritte im nächsten Abschnitt aus, um die benötigten Treiber manuell zu konfigurieren.

4.1 Manuelle Treiberkonfiguration

IT-Sicherheitsrichtlinieneinstellungen können verhindern, dass Druck-Treiber bei der Installation automatisch konfiguriert werden. Dieser Wille sichtbar sein, wenn 4Sight2 nicht mit den verschiedenen Geräten kommunizieren kann.

Für die neuesten Informationen https://www.bakerhughes.com/druck/test-and-calibration-instrumentation/calibrationmanagement-software-4sight2

oder

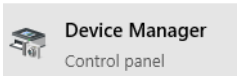
Um dieses Problem zu lösen, können die Druck-Treiber manuell konfiguriert werden. Wenden Sie sich an Ihren IT-Ansprechpartner vor Ort, wenn Sie unsicher sind oder Hilfe benötigen.

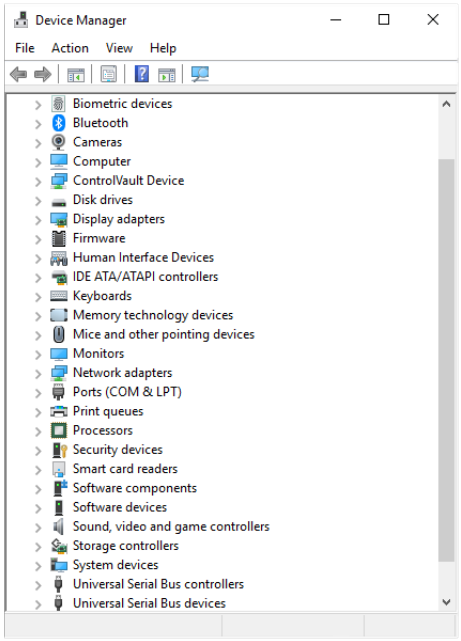
4.1.1 Voraussetzungen

Um die Treiber zu installieren, muss die 4Sight2-Anwendung auf Ihrem Computer installiert oder von diesem aus zugänglich sein. Stellen Sie sicher, dass Sie sich von dem Computer aus bei der 4Sight2-Anwendung anmelden können, bevor Sie versuchen, die Treiber zu installieren.

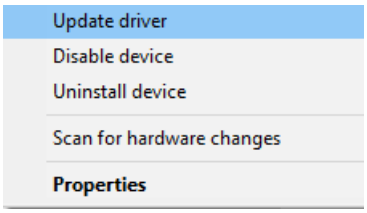
Um den Treiber manuell zu installieren, führen Sie die folgenden Schritte aus.

1. Suchen Sie auf dem Desktop nach dem Geräte-Manager und führen Sie ihn aus.

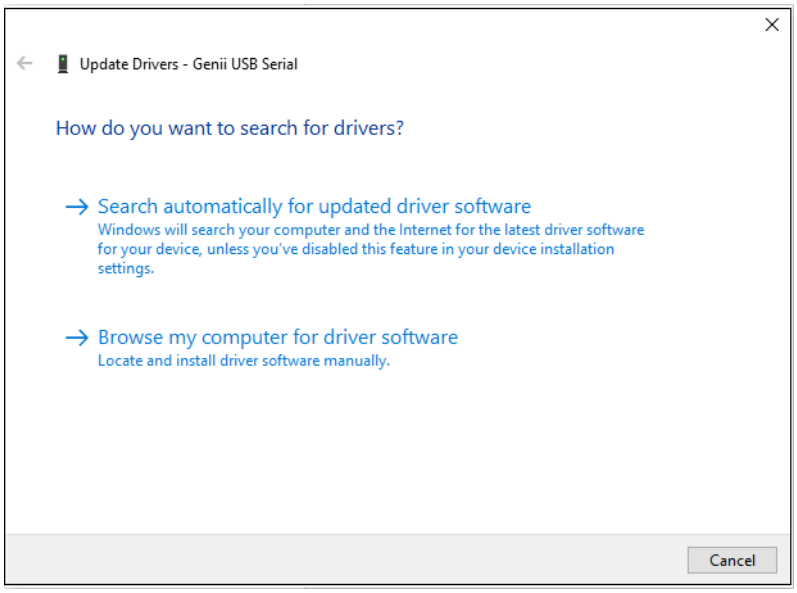




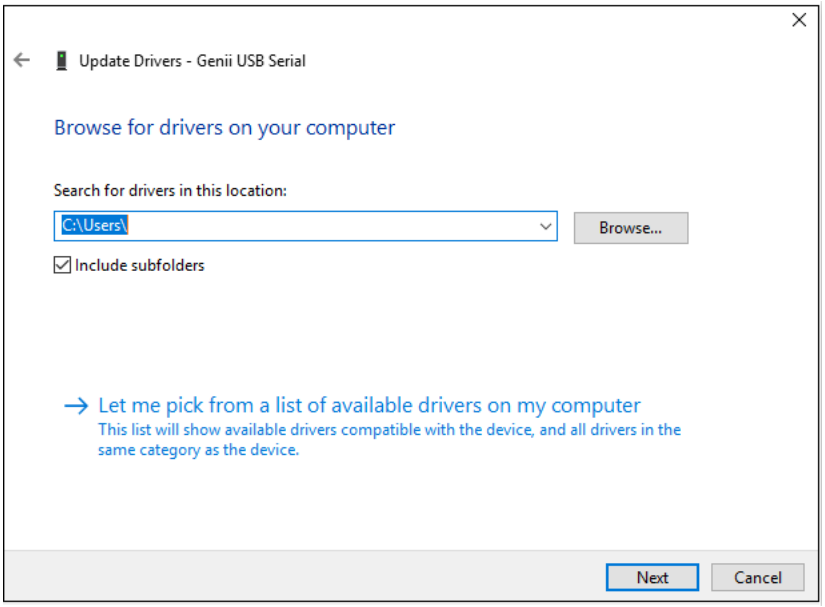
2. Blättern Sie durch die Liste der USB-Geräte, um das nicht konfigurierte Gerät zu finden (“Unbekanntes Gerät“ oder „Andere Geräte“). Klicken Sie mit der rechten Maustaste und wählen Sie **Treiber aktualisieren**.



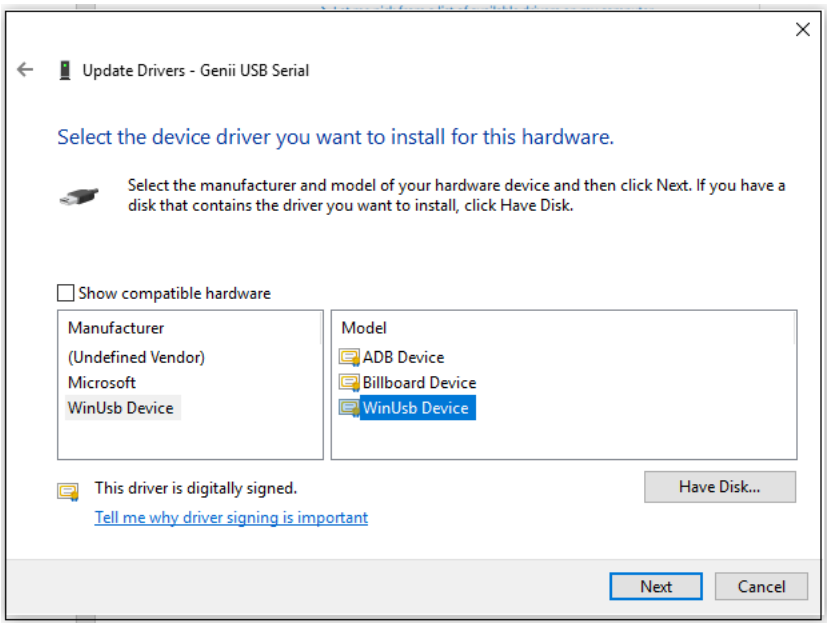
3. Wählen Sie **Auf dem Computer nach Treibersoftware suchen**.



4. Wählen Sie **Aus einer Liste verfügbarer Treiber auf meinem Computer auswählen**.

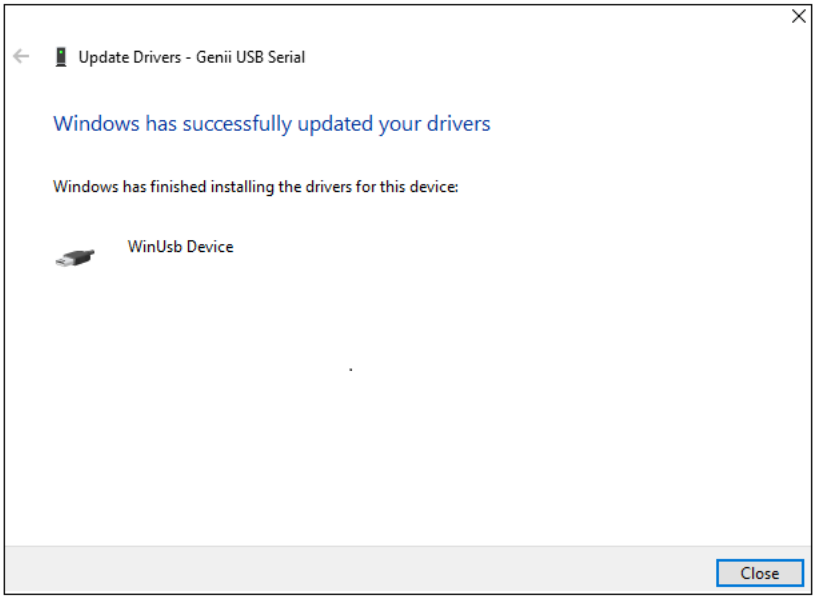


5. Deaktivieren Sie das Kontrollkästchen **Kompatible Hardware anzeigen** und markieren Sie **WinUsb-Gerät** für “Hersteller“ und **WinUsb-Gerät** für “Modell“.



6. Die folgende Warnmeldung wird angezeigt: Klicken Sie auf **Ja**.

7. Die Meldung “Ihre Treiber wurden von Windows erfolgreich aktualisiert.“ wird angezeigt.



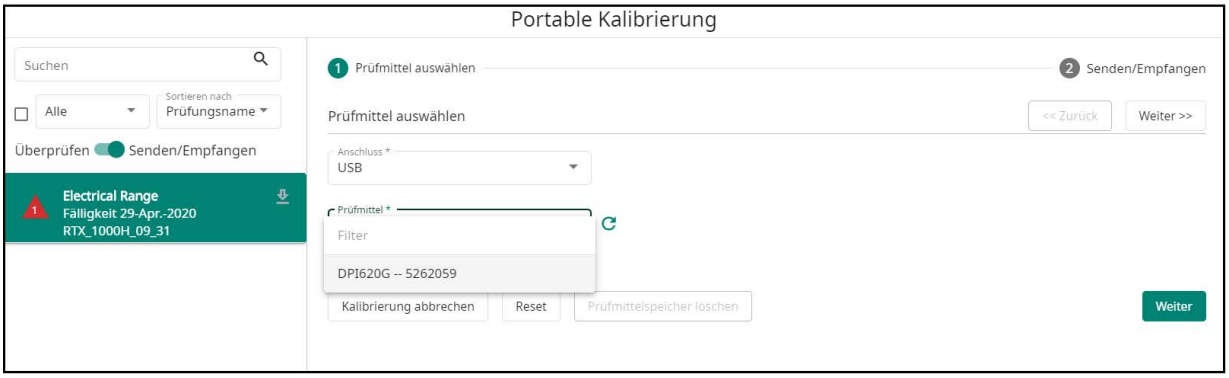
Wiederholen Sie die obenstehenden Schritte für jede Gerätekategorie, wenn Sie das Gerät zum ersten Mal verbinden.

Wenn Sie z. B. einen PACE und einen Genii zum ersten Mal verbinden, müssen Sie die obenstehenden Schritte möglicherweise für den PACE und den Genii separat wiederholen. Alle weiteren PACE- und Genii-Geräte sollten sich verbinden lassen, ohne diese Einstellungen vornehmen zu müssen. Wenn Sie jedoch zu einem späteren Zeitpunkt eine andere Gerätekategorie verbinden, wie z. B. einen DPI 611/612, müssen Sie die Schritte für diese Gerätekategorie erneut ausführen.

4.2 Prüfmittelkommunikator testen

1. Melden Sie sich bei 4Sight2 als Techniker an.
2. Gehen Sie zu **Geräte >> Arbeitsliste**.
3. Wählen Sie einen oder mehrere Bereiche aus und weisen Sie diesen den Kalibrierungs-Workflow “Portabel“ oder “Automatisiert“ zu.
4. Klicken Sie auf die Schaltfläche **Aktualisieren**.

5. Klicken Sie auf die Dropdownliste **Prüfmittel**. Wenn das verbundene Gerät in der Liste angezeigt wird, ist der Prüfmittelkommunikator ordnungsgemäß konfiguriert.



4.3 Treiberkonfiguration für Temperaturkalibratoren

Damit ein Temperaturkalibrator mit 4Sight2 kommunizieren kann, muss ein FTDI-Treiber installiert werden.

1. Laden Sie sich den FTDI-Treiber über folgenden Link herunter: https://www.ftdichip.com/Drivers/VCP.htm.
2. Extrahieren Sie die heruntergeladene Datei und speichern Sie sie an einem bekannten Speicherort auf Ihrem Computer.
3. Wechseln Sie auf Ihrem Computer zum Windows-Geräte-Manager.
4. Wählen Sie “Ports (COM & LPT)“ in der Geräteliste aus, um den Temperaturkalibrator anzuzeigen.
5. Rechtsklicken Sie auf den Temperaturkalibrator und wählen Sie “Treiber aktualisieren“.
6. Wählen Sie “Auf dem Computer nach Treibersoftware suchen“.
7. Wählen Sie “Durchsuchen“ neben dem Suchfeld mit der Bezeichnung “An diesem Ort nach Treibern suchen“.
8. Wählen Sie den extrahierten Ordner mit dem heruntergeladenen Treiber aus.
9. Klicken Sie auf “Weiter“ und dann auf “Schließen“.
10. Der Treiber wird jetzt installiert.
11. Um die Kommunikation mit einem Temperaturkalibrator in 4Sight2 zu testen, navigieren Sie zu „Automatisierte Kalibrierung“ und prüfen Sie, ob der Temperaturkalibrator als Eingangsregler ausgewählt werden kann. Alternativ können Sie Schritt 14 aus Abschnitt 4 wiederholen.

Bereitstellungsanleitung

5. Bereitstellungsanleitung

5.1 Bereitstellungsarchitektur

Zur Architektur gehören in der Regel die 4Sight2-Webanwendung und ein UAA-Server (User Authentication and Authorization), der innerhalb des Tomcat-Webservers auf demselben Computer wie die PostgreSQL-Datenbank ausgeführt wird.

Die Browser-Client-Webanwendung stellt eine Verbindung zum 4Sight2-Server her, der die Informationen in der PostgreSQL-Datenbank speichert bzw. daraus abruft.

5.2 Physische Bereitstellung

Wir gehen davon aus, dass Benutzer, die 4Sight2 installieren, bereits Maßnahmen zur Cybersicherheit ergriffen haben, die den Sicherheitsrichtlinien entsprechen, wie:

- Der Server befindet sich an einem sicheren Standort, der nur eingeschränkt zugänglich ist.
- Der Zugriff auf den Server ist durch eingeschränkte Rechte geschützt.
- Das Servernetzwerk ist durch eine Firewall geschützt, die nur eingeschränkten Zugriff auf bekannte Anwendungen erlaubt, der ausschließlich über bekannte Ports erfolgt.
- Die Anwendungen werden in ihrem eigenen Kontext ausgeführt und haben ausschließlich auf die in ihrem eigenen Ordner vorhandenen Datenbank- und Dateisysteme Zugriff.

5.3 Netzwerk

Die Clients werden in einem Webbrowser ausgeführt und sind über Ethernetverbindungen oder ein WLAN verbunden. Abhängig von der Bandbreite und der Anzahl der verbundenen Geräte können in einem WLAN Verzögerungen auftreten.

Es empfiehlt sich, im Browser installierte Plugins und Erweiterungen zu entfernen.

Der 4Sight2-Webserver sollte nicht mit dem Internet verbunden werden. Wenn ein dezentraler Zugriff erforderlich ist, sollte dieser über ein Intranet oder VPN erfolgen.

5.4 Bereitstellungssequenz

Für die Anwendung sind PostgreSQL, Tomcat und Java Runtime Voraussetzung. PostgreSQL wird als separates Paket installiert, die übrigen Komponenten befinden sich im Paket der Anwendung. Wenn PostgreSQL bereits auf dem Computer des Benutzers installiert ist, wird für die Verbindung und die Konfiguration nur ein Superuser-Kennwort benötigt.

Für die Installation sind Windows-Administratorrechte für den Computer erforderlich. Vor der Installation benötigt der Benutzer ein Superuser-Kennwort für PostgreSQL, den Benutzernamen und das Kennwort des Administrators der Anwendung sowie den Benutzernamen und das Kennwort für die Datenbank.

Das Superuser-Kennwort für PostgreSQL wird benötigt, um die Datenbank und andere Strukturen im PostgreSQL-Server zu erstellen. Der Administrator der Anwendung ist der erste Benutzer der Anwendung. Er ist dafür zuständig, weitere Benutzer zu erstellen und ihnen verschiedene Rollen zuzuweisen. Der Datenbankbenutzer hat Zugriff auf 4Sight2 und die UAA-Datenbank. Die Anmeldedaten dieses Benutzernamens werden für den Zugriff auf die Datenbank verwendet.

Die Anwendung wird an einem Computerport veröffentlicht. Standardmäßig ist dies Port 8083. Der Benutzer kann diesen Port jedoch bei der Installation oder zu einem späteren Zeitpunkt ändern. Der standardmäßige Anwendungskontext in Tomcat ist 4Sight2.

Beachten Sie die Richtlinien von Microsoft oder des CIS zum Härten des Betriebssystems. Das Installationsverfahren fordert Sie auf, vor dem 4Sight2-Server PostgreSQL zu installieren.

Der Prüfmittelkommunikator wird auf den Client-Computern installiert, wenn die Prüfmittel über USB-Anschlüsse verbunden werden. Falls auf einem Computer noch kein Prüfmittelkommunikator installiert ist, wird der Benutzer aufgefordert, den Prüfmittelkommunikator vom 4Sight2-Server herunterzuladen und auf dem Computer zu installieren. Der Prüfmittelkommunikator hört den Port 9000 ab und kommuniziert ausschließlich über eine sichere Verbindung.

5.5 Nach der Bereitstellung

5.5.1 Benutzer und Gruppen hinzufügen

Der Administrator muss in der Anwendung verschiedene Benutzer erstellen, wie Supervisor, Meister, Techniker und Prüfer. Der Administrator kann diese Benutzer verschiedenen vordefinierten Standardgruppen zuweisen. Falls mehr Kontrolle oder eine genauere Zugriffssteuerung erforderlich ist, kann der Administrator benutzerdefinierte Gruppen erstellen und ihnen bestimmte Berechtigungen zuweisen.

5.5.2 Standardkennwörter

Für den Tomcat-Benutzer wird das in der Datei „C:\Programme\Druck\4Sight2\<<latest folder number>>\apache-tomcat\conf\tomcat-user.xml“ hartcodierte Standardkennwort verwendet.

Es empfiehlt sich, das Standardkennwort zu ändern und stets ein den Best Practices entsprechendes starkes Kennwort zu benutzen.

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

Best Practices wurden implementiert, damit die Sicherheit dieser Anwendung gewährleistet ist. Indem Sie die folgenden Aufgaben durchführen, erhöhen Sie die Sicherheit noch weiter:

Die Konfigurationsdateien und -ordner sind dadurch geschützt, dass nur Dienste und Systeme zugreifen können, die standardmäßig über Zugriffsrechte verfügen. Nur der Admin-Benutzer verfügt für den Ordner “C:\Programme\Druck\4Sight2\<<latest folder number>>\apache-tomcat\conf“ über Lese-/Schreibrechte. Daher müssen Sie, bevor Sie die folgenden Aufgaben durchführen, die Eingabeaufforderung mit Administratorrechten öffnen.

5.5.3 Sichere Kommunikation

Dieser Abschnitt bietet Anweisungen, um 4Sight2 mithilfe eines selbstsignierten Zertifikats für einen sicheren Modus zu konfigurieren (auch als SSL-Modus bezeichnet). Bitte lesen Sie die Voraussetzungen und die allgemeinen Geschäftsbedingungen in der 4Sight2-Anwendung, bevor Sie fortfahren. Ein selbstsigniertes Zertifikat ist eine Möglichkeit, um SSL in 4Sight2 zu aktivieren. Alternativ kann ein Drittanbieter-CA-Zertifikat von verschiedenen Anbietern wie Symantec, Digicert usw. bezogen werden.

Hinweis: Durch die Aktivierung von SSL alleine wird Ihre Anwendung nicht unbedingt sicherer. SSL ist jedoch eines der gängigsten Verfahren, um eine sichere Webanwendung zu gewährleisten.

5.5.3.1 Voraussetzungen und Warnhinweise

Für die folgenden Arbeitsanweisungen gelten folgende Voraussetzungen:

Zur Erzeugung von selbstsignierten Zertifikaten wird die Software OpenSSL für Windows benötigt. 4Sight2 setzt voraus, dass Ihre Organisation sowie regionale und nationale Gesetze und Vorschriften es Ihnen gestatten, die OpenSSL-Software zu verwenden.

- Keytool ist ein von Java bereitgestelltes Dienstprogramm für die Code- und Zertifikatverwaltung und wird verwendet, um verschiedene Komponenten zu generieren, die für die HTTPS-Konfiguration benötigt werden. 4Sight2 setzt voraus, dass Ihre Organisation sowie regionale und nationale Gesetze und Vorschriften es Ihnen gestatten, das Dienstprogramm Keytool zu verwenden.
- Sie benötigen Administratorberechtigungen, um die folgenden Konfigurationen vorzunehmen. Wie Sie Administratorberechtigungen erhalten, erfahren Sie bei Ihrer IT-Abteilung.
- Die folgenden Schritte erfordern ein grundlegendes Verständnis von Computerprozessen. Es wird daher empfohlen, diese Schritte mit Anleitung durch die lokale IT-Abteilung auszuführen.
- Die in diesem Dokument verwendeten Inhalte wie Hostnamen, Kennwörter, URLs und Ordnerpfade dienen nur zu Referenzzwecken. Stellen Sie sicher, dass Sie die Befehle vor der Ausführung entsprechend anpassen.
- Die folgenden Abschnitte beschreiben zwei Szenarien. Bei einem befinden sich der Server und der Client auf demselben Computer, bei dem anderen auf unterschiedlichen Computern (d. h. ein Szenario mit mehreren Clients).

5.5.3.2 Schritte zum Konfigurieren der 4Sight2-Anwendung in HTTPS

1. Stoppen Sie 4Sight2 über die Windows-Dienste.
2. Öffnen Sie die Eingabeaufforderung im **Administratormodus**.
3. Navigieren Sie im 4Sight2-Installationsverzeichnis zu dem folgenden Ordner, indem Sie den folgenden Befehl ausführen:

   cd "C:\Programme\Druck\4Sight2\<<latest folder number>>\apache-tomcat\conf"
4. Prüfen Sie, ob Keytool vorhanden ist, indem Sie an der Eingabeaufforderung den folgenden Befehl eingeben: **Keytool** -?

Wenn nicht, richten Sie einen Umgebungspfad zum JRE-Bin-Ordner im 4Sight2-Installationsordner wie unten gezeigt ein. Aktualisieren Sie den richtigen Pfad basierend auf dem Installationsordner.

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

5. Um ein neues Zertifikat zu erstellen, fahren Sie mit Schritt 6 fort. Wenn bereits ein Zertifikat vorhanden ist, gehen Sie folgendermaßen vor:

    a. Prüfen Sie, ob die Zertifikatdatei „4Sight.jks“ im Java-Keystore vorhanden ist.
    keytool -list -alias <<hostname>> -storepass <<KeyPassword>> -keystore 4Sight.jks

    b. Wenn das Zertifikat bereits installiert ist, entfernen Sie es:
    keytool -delete -noprompt -alias <<hostname>> -storepass <<KeyPassword>> -keystore 4Sight.jks

    c. Prüfen Sie, ob die Datei „4SightV2PublicKey.cer“ vorhanden ist, und löschen Sie sie gegebenenfalls.
    del "../../app/Certificate/4SightV2PublicKey.cer"

    d. Prüfen Sie, ob das Zertifikat bereits im Cacerts-Speicher von Java vorhanden ist.
    keytool -list -alias <<hostname>> -storepass changeit -keystore "../../jre/lib/security/cacerts"

    e. Löschen Sie das Zertifikat, wenn es im Java-Speicher vorhanden ist.
    keytool -delete -noprompt -alias <<hostname>> -storepass changeit -keystore "../../jre/lib/security/cacerts" -file "../../app/Certificate/4SightV2PublicKey.cer"

6. Erstellen Sie ein neues Zertifikat, indem Sie folgenden Befehl ausführen:

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

7. Exportieren Sie das Zertifikat in die Datei „4SightV2PublicKey.cer“ (ändern Sie weder den Dateinamen noch den Pfad).

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

    Nachdem der Befehl erfolgreich ausgeführt wurde, wird die Meldung: „Zertifikat wurde in Datei C:\Programme\Druck\4Sight2\<<latest folder number>>\app\Certificate\4SightV2PublicKey.cer gespeichert“ angezeigt.

8. Importieren Sie das Zertifikat in die Java-Cacerts-Datei.

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

Nach erfolgreicher Ausführung des Befehls wird die Meldung „Zertifikat wurde zu Keystore hinzugefügt“ angezeigt.

9. Tragen Sie das Zertifikat in die Tomcat-Konfigurationsdatei ein.

    a. Öffnen Sie die Datei „server.xml“ am folgenden Speicherort.
    "C:\Programme\Druck\4Sight2\<<latest folder number>>\apache-tomcat\conf\server.xml"

    b. Fügen Sie den folgenden Eintrag zur Datei „server.xml“ hinzu.

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

c. Kommentieren Sie den folgenden Abschnitt aus, um HTTP-Verbindungen zu deaktivieren.
<connectionTimeout="20000" maxSwallowSize="104857600" port="8083" protocol="HTTP/1.1" redirectPort="8443" relaxedPathChars=""[\]^`{|}+" relaxedQueryChars="&quot;[\]^`{|}+"/>

Hinweis: Wenn Sie diesen Teil nicht auskommentieren, funktioniert die Anwendung nicht.

10. An diesem Punkt ist die HTTPS-Konfiguration der 4Sight2-Anwendung abgeschlossen.
11. Um die zuvor vorgenommenen Konfigurationen zu testen, starten Sie den 4Sight2-Dienst in den Windows-Diensten neu.
12. Öffnen Sie Google Chrome, leeren Sie den Browsercache und starten Sie den Browser neu.
13. Geben Sie die folgende URL in den Browser ein: https://<<host-name>>:8443/4sight2

- Es kann etwas länger dauern, wenn die URL erstmals geladen wird.
- Ein Bildschirm mit der Meldung „Ihre Verbindung ist nicht privat“ wird angezeigt.
- Klicken Sie auf die Schaltfläche **Erweitert** >> **Weiter zu XX**.
- Wenn der 4Sight2-Bildschirm nicht angezeigt wird, klicken Sie auf die Schaltfläche **Neu laden**.
- Sie werden zur 4Sight2-Seite weitergeleitet.
- In der Adresszeile wird der Fehler „Nicht sicher“ angezeigt und verschwindet eventuell, nachdem das Zertifikat in der MMC registriert wurde.

5.5.3.3 Schritte zum Konfigurieren von DruckCommsServer in HTTPS bei Installation auf einem Servercomputer

Ersetzen Sie Werte in << >> durch geeignete Daten, bevor Sie den Befehl ausführen.

1. Stoppen Sie DruckCommsServer über die Windows-Dienste.
2. Öffnen Sie die Eingabeaufforderung im **Administratormodus**.
3. Prüfen Sie, ob Keytool vorhanden ist, indem Sie an der Eingabeaufforderung den folgenden Befehl eingeben: **Keytool -?**

   Wenn nicht, richten Sie einen Umgebungspfad zum JRE-Bin-Ordner im 4Sight2-Installationsordner wie unten gezeigt ein.
   Aktualisieren Sie den richtigen Pfad basierend auf dem Installationsordner.
   C:\Programme\Druck\4Sight2\<<latest folder number>>\jre\bin
   Set "Path=%Path%;C:\Programme\Druck\4Sight2\<<latest folder number>>\jre\bin"
4. Navigieren Sie im DruckCommsServer-Installationsverzeichnis zu dem folgenden Ordner, indem Sie den folgenden Befehl ausführen:

   cd "C:\Programme\Druck\DruckCommsServer\<< Communication Service version >>"
5. Prüfen Sie, ob bereits ein Zertifikat vorhanden ist. Falls ja, gehen Sie folgendermaßen vor:

   a. Prüfen Sie, ob das Zertifikat bereits im Cacerts-Speicher von Java vorhanden ist.
   keytool -list -alias tomcat -storepass changeit -keystore cacerts

   b. Löschen Sie das Zertifikat, wenn es im Java-Speicher vorhanden ist.

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

c. Löschen Sie die standardmäßig vorkonfigurierten Zertifikate aus CommsServer.
del 4Sight.jks
del 4SightV2DeviceMngr.pfx

6. Erstellen Sie ein neues Zertifikat, indem Sie folgenden Befehl ausführen:

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

7. Exportieren Sie das Zertifikat in die Datei „DruckCommServer.cer“.

   keytool -export -alias tomcat -keystore CommServer.jks -storepass <<StorePassword>> -storetype JKS -file DruckCommServer.cer
   Nachdem der Befehl erfolgreich ausgeführt wurde, wird die Meldung:
   “Zertifikat wurde in Datei DruckCommServer.cer gespeichert“ angezeigt.

8. Importieren Sie das CommServer-Zertifikat in die Java-Cacerts-Datei.

   keytool -import -noprompt -trustcacerts -alias tomcat -storepass changeit -keystore cacerts -file DruckCommServer.cer
   Nach erfolgreicher Ausführung des Befehls wird die Meldung „Zertifikat wurde zu Keystore hinzugefügt“ angezeigt.

9. Importieren Sie das 4Sight-Zertifikat in die Java-Cacerts-Datei.

   keytool -import -noprompt -trustcacerts -alias <<server hostname>> -storepass changeit -keystore cacerts -file "C:\Programme\Druck\4Sight2\<<latest folder number>>\app\Certificate\4SightV2PublicKey.cer"
   Nach erfolgreicher Ausführung des Befehls wird die Meldung „Zertifikat wurde zu Keystore hinzugefügt“ angezeigt.

10. Bearbeiten Sie das Keystore-Kennwort für „application.properties“ in DruckCommsServer.

    Öffnen Sie die Datei:
    “C:\Programme\Druck\DruckCommsServer\<<Communication Service Version>>\application.properties“ und ändern Sie die folgende Zeile:
    keystore = CommServer.jks
    key-store.password= << StorePassword >>
    Hinweis: **<< StorePassword >>** bezieht sich auf das in Schritt 6 verwendete **StorePassword**.

11. Starten Sie die Dienste 4Sight2 und DruckCommsServer neu.

5.5.3.4 Schritte zum Konfigurieren von DruckCommsServer in HTTPS bei Installation auf einem Clientcomputer

1. Das Dienstprogramm Keytool ist in Java enthalten, sodass Sie entweder Java auf Ihrem Computer installieren können oder die Verfügbarkeit von Java Keytool direkt ohne Installation von Java prüfen können.
2. Stoppen Sie DruckCommsServer über die Windows-Dienste.
3. Öffnen Sie die Eingabeaufforderung im **Administratormodus**.
4. Prüfen Sie, ob Keytool vorhanden ist, indem Sie an der Eingabeaufforderung den folgenden Befehl eingeben: **Keytool -?**

   Wenn nicht, richten Sie einen Umgebungspfad zum JRE-Bin-Ordner ein, wenn Sie Java auf dem Computer installiert haben, oder richten Sie einen Pfad zu Keytool wie unten gezeigt ein.

   Aktualisieren Sie den richtigen Pfad basierend auf dem Installationsordner.

   C:\Programme\Java\<< Java version >>\bin
   Set Path=%Path%; "C:\Programme\Java\<< Java version >>\bin"
5. Rufen Sie die Datei **4SightV2PublicKey.cer** von dem Servercomputer ab, auf dem die 4Sight-Anwendung installiert ist. Diese Datei befindet sich auf dem Server an folgendem Speicherort:

   C:\Programme\Druck\4Sight2\<<latest folder number>>\app\Certificate\4SightV2PublicKey.cer
6. Kopieren Sie die Datei **4SightV2PublicKey.cer** an folgenden Speicherort:

   C:\Programme\Druck\DruckCommsServer\<< Communication Service version >>
7. Befolgen Sie jetzt die Schritte 4 bis 8 in Abschnitt 5.5.3.3.
8. Importieren Sie das 4Sight-Zertifikat in die Java-Cacerts-Datei.

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

   Nach erfolgreicher Ausführung des Befehls wird die Meldung „Zertifikat wurde zu Keystore hinzugefügt“ angezeigt.
9. Befolgen Sie jetzt die Schritte 10 bis 11 in Abschnitt 5.5.3.3.

5.5.3.5 Schritte zum Erzeugen eines selbstsignierten Zertifikats für 4Sight2

1. Laden Sie OpenSSL für Windows herunter und installieren Sie das Programm.
2. Stoppen Sie die 4Sight2-Dienste über die Windows-Dienste.
3. Erstellen Sie einen Ordner mit der Bezeichnung **4Sight2Certificate** auf Laufwerk C.

   Sie können einen beliebigen Speicherort oder Ordnernamen wählen, sofern Sie administrativen Zugriff auf diesen Ordner haben.
4. Erstellen Sie im obenstehenden Ordner eine neue Datei in Notepad und speichern Sie die Datei unter **openssl-ca.cnf**.

   Kopieren Sie die folgenden Inhalte in die Datei und speichern Sie diese.

```
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
```

Hinweis: Aktualisieren Sie den obenstehenden **[Company Name]** und speichern Sie die Datei. Dies ist der Name des Zertifikatsausstellers, der in der Verwaltungskonsole angezeigt wird.

5. Erstellen Sie im obenstehenden Ordner eine neue Datei in Notepad und speichern Sie die Datei unter **openssl-server.cnf**.

   Kopieren Sie die folgenden Inhalte in die Datei und speichern Sie diese.

```
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
```

Hinweis: Aktualisieren Sie den obenstehenden Hostnamen und die obenstehende IPv4-Adresse und speichern Sie die Datei.

6. Öffnen Sie die Eingabeaufforderung mit Administratorberechtigungen.
7. Navigieren Sie zum Ordner “4Sight2Certificate“, indem Sie den folgenden Befehl ausführen:

   cd "<<full path to 4Sight2Certificate >>"
8. Legen Sie die Pfadvariable für den OpenSSL-Bin-Ordner fest, indem Sie den folgenden Befehl ausführen.

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

   Beispiel-Standardpfad:

   Set Path=%Path%;"C:\Programme\OpenSSL-Win64\bin"
9. Legen Sie die Pfadvariable für den JRE-Bin-Ordner fest, indem Sie den folgenden Befehl ausführen. Hinweis: Der folgende Pfad kann abweichen.

   Set path=%path%;"C:\Programme\Druck\4Sight2\<<latest folder number>>\jre\bin"
10. Führen Sie den folgenden Befehl aus, um die Dateien „cacert.pem“ und „cakey.pem“ zu erzeugen.

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

    Geben Sie die richtigen Zertifikatdaten ein, wenn Sie dazu aufgefordert werden, z. B. Land, Bundesstaat usw.
11. Führen Sie die folgenden Befehle aus, um die Dateien „servercert.csr“ und „serverkey.pem“ zu erzeugen.

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

    Geben Sie die richtigen Zertifikatdaten ein, wenn Sie dazu aufgefordert werden, z. B. Land, Bundesstaat usw.
12. Erstellen Sie in Notepad eine neue Datei mit dem Namen „index.txt“. Speichern Sie die Datei im Ordner “4Sight2Certificate“.
13. Erstellen Sie in Notepad eine neue Datei mit dem Namen „serial.txt“. Speichern Sie die Datei im Ordner “4Sight2Certificate“.

    Öffnen Sie die Datei und geben Sie **01** ein. Speichern und schließen Sie die Datei.
14. Führen Sie den folgenden Befehl aus, um neue Zertifikate in den Dateien „servercert.csr“ und “serverkey.pem“ zu erzeugen.

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

    Geben Sie “J“ ein, um die Änderungen zu bestätigen. Nach erfolgreicher Ausführung des Befehls wird die Datenbank aktualisiert.

15. Packen Sie vorhandene Dateien im PFX-Format, indem Sie den folgenden Befehl ausführen.

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

    Sie werden aufgefordert, das Kennwort zweimal einzugeben.

16. Konvertieren Sie den PFX-Speicher in einen Java-Keystore unter dem oben genannten JRE-Bin-Speicherort, z. B. tomcat/config path.

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

    Hinweis: Das Kennwort für beide Speicher muss dasselbe sein. Stellen Sie sicher, dass Sie auf die Datei "4Sight.jks" im Konfigurationsordner von Tomcat verweisen (siehe oben).
    Sie werden aufgefordert, das Kennwort für den Ziel-Keystore und den Quell-Keystore einzugeben. Nach erfolgreicher Ausführung des Befehls wird die Meldung "Importbefehl abgeschlossen: 1 Einträge erfolgreich importiert" angezeigt.

17. Exportieren Sie das Zertifikat aus dem Java-Keystore in die Datei unter:

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

    Hinweis: Stellen Sie sicher, dass Sie auf die Datei "4Sight.jks" im Konfigurationsordner von Tomcat verweisen (siehe oben).
    Nach erfolgreicher Ausführung wird die Meldung "Zertifikat wurde in Datei gespeichert" angezeigt.

18. Importieren Sie die Zertifikatdatei in den Ordner "cacerts" im 4Sight2-Installationsverzeichnis.

    Hinweis: Der Pfad kann abhängig vom Installationsverzeichnis und der 4Sight2-Version abweichen.

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

    Hinweis: Der Alias, den Sie zu erstellen versuchen, ist bereits vorhanden. Führen Sie zuerst den folgenden Befehl aus, um ihn zu löschen, und dann den vorstehenden Befehl, um einen neuen Alias zu erstellen:

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

    Nach erfolgreicher Ausführung dieses Befehls wird die Meldung „Zertifikat wurde zu Keystore hinzugefügt" angezeigt.

19. Nehmen Sie an der Datei "server.xml" (vorhanden unter "C:\Programme\Druck\4Sight2\<<latest folder number>>\apache-tomcat\conf") folgende Änderung vor:

a. Fügen Sie den folgenden Eintrag zur Datei “server.xml“ hinzu.

<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. Kommentieren Sie den folgenden Abschnitt aus, um HTTP-Verbindungen zu deaktivieren.

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

20. Damit ist die HTTPS-Konfiguration für 4Sight2 abgeschlossen. Starten Sie jetzt den 4Sight2-Dienst über die Windows-Dienste.

5.5.3.6 Schritte zum Konfigurieren des selbstsignierten Zertifikats für DruckCommsServer bei Installation auf einem Servercomputer

Hier haben wir vorausgesetzt, dass Sie die 4Sight2-Anwendung mit den Schritten in Abschnitt 5.5.3.5 erfolgreich in HTTPS konvertiert haben und sich die folgenden Dateien bereits in Ihrem Ordner **4Sight2Certificate** befinden:

- openssl-server.cnf
- openssl-ca.cnf
- cacert.pem
- cakey.pem
- index.txt
- serial.txt
- 4SightV2PublicKey.cer (Diese Datei kann sich unter C:\Programme\Druck\4Sight2\<<latest folder number>>\app\Ordner „Zertifikate“ befinden.)

1. Erstellen Sie einen neuen Ordner **CommserverCertificate** und kopieren Sie die obenstehenden Dateien. Nehmen Sie dabei folgende Änderungen vor:

- openssl-server.cnf

  Ändern Sie im Abschnitt **req** den Wert **default_keyfile** zu “**DruckCommServerCertKey.pem**“.

  - Ändern Sie unter **server_distinguished_name** den Wert **commonName** zu „**localhost**“.
  - Ändern Sie unter **alternate_names** den Wert **DNS.1** zu “**localhost**“.
  - Ändern Sie unter **alternate_names** den Wert **IP.1** zu “**127.0.0.1**“.
  - Speichern Sie die Datei.
- openssl-ca.cnf (Nehmen Sie in dieser Datei keine Änderungen vor.)
- cacert.pem (Nehmen Sie in dieser Datei keine Änderungen vor.)
- index.txt (Löschen Sie den gesamten Inhalt der Datei, sodass sie leer ist.)
- serial.txt (Löschen Sie den gesamten Inhalt der Datei und tragen Sie lediglich 01 ein.)

2. Stoppen Sie den DruckCommsServer-Dienst über die Windows-Dienste.
3. Öffnen Sie die Eingabeaufforderung mit Administratorberechtigungen.
4. Navigieren Sie zum Ordner **CommserverCertificate**, indem Sie den folgenden Befehl ausführen:

   cd "<<full path to CommserverCertificate >>"
5. Legen Sie die Pfadvariable für den OpenSSL-Bin-Ordner fest, indem Sie den folgenden Befehl ausführen.

   Set path=%path%;"<<bin folder of openssl>>"
   Beispiel-Standardpfad:
   Set Path=%Path%;"C:\Programme\OpenSSL-Win64\bin"
6. Legen Sie die Pfadvariable für den JRE-Bin-Ordner fest, indem Sie den folgenden Befehl ausführen. Hinweis: Der folgende Pfad kann abweichen.

   Set path=%path%;"C:\Programme\Druck\4Sight2\<<latest folder number>>\jre\bin"
7. Erstellen Sie danach mit dem folgenden Befehl eine Anforderung für das CommServer-Zertifikat:

   openssl req -config openssl-server.cnf -newkey rsa:2048 -sha256 -nodes -out DruckCommServer.csr -outform PEM
   Nachdem dieser Befehl ausgeführt wurde, haben Sie eine Anforderung in **DruckCommServer.csr** und einen privaten Schlüssel in **DruckCommServerCertKey.pem**.
8. Führen Sie dann folgenden Befehl aus, um die CSR-Anforderung mit Ihrem CA zu signieren:

   openssl ca -config openssl-ca.cnf -policy signing_policy -extensions signing_req -out DruckCommServerCert.pem -infiles DruckCommServer.csr
9. Erstellen Sie danach mit folgendem Befehl eine PFX-Datei mit dem Alias **tomcat** für CommServer:

   openssl pkcs12 -export -in DruckCommServerCert.pem -inkey DruckCommServerCertKey.pem -certfile cacert.pem -name "tomcat" -out DruckCommServer.pfx
10. Konvertieren Sie den PFX-Speicher mithilfe von Keytool in einen Java-Keystore.

    Hinweis: Das Kennwort für beide Schlüsselspeicher muss dasselbe sein.
    keytool -importkeystore -srckeystore DruckCommServer.pfx -srcstoretype PKCS12 -destkeystore CommServer.jks -deststoretype jks
11. Importieren Sie jetzt das Zertifikat in den „Cacerts“-Speicher.

    a. Löschen Sie jetzt das vorhandene Tomcat-Alias, das standardmäßig installiert ist.
    keytool -delete -noprompt -trustcacerts -alias tomcat -storepass changeit -keystore "C:\Programme\Druck\DruckCommsServer\<< Communication Service version >>\cacerts"

    b. Nachdem Sie das vorhandene Tomcat-Alias gelöscht haben, importieren Sie mit folgendem Befehl das Zertifikat in den „Cacerts“-Speicher:
    keytool -import -noprompt -trustcacerts -alias tomcat -storepass changeit -keystore "C:\Programme\Druck\DruckCommsServer\<< Communication Service version >>\cacerts" -file DruckCommServerCert.pem
12. Jetzt müssen wir mit dem folgenden Befehl den öffentlichen 4Sight-Schlüssel für die Authentifizierung der Kommunikation in den CommServer-„Cacerts“-Speicher importieren:

    keytool -import -noprompt -trustcacerts -alias <<4sight server hostname>> -storepass changeit -keystore "C:\Programme\Druck\DruckCommsServer\<< Communication

Service version >>\cacerts" -file "C:\Programme\Druck\4Sight2\<<latest folder number>>\app\Certificate\4SightV2PublicKey.cer"

13. Nachdem alle obenstehenden Schritte abgeschlossen sind, befinden sich die Dateien **DruckCommServer.pfx** und **CommServer.jks** im aktuellen Ordner **CommserverCertificate**.

    Kopieren Sie diese Dateien und fügen Sie sie in das Verzeichnis "C:\Programme\Druck\DruckCommsServer\<< Communication Service version >>" ein.

    Bearbeiten Sie die **application.properties** am selben Speicherort, indem Sie den Wert der Eigenschaft wie folgt ändern:

    a. Keystore = CommServer.jks

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

    c. key-store.type=JKS

5.5.3.6.1 Installieren des Zertifikats für 4Sight und DruckCommsServer in Windows

1. Öffnen Sie die Eingabeaufforderung, geben Sie "mmc" ein und drücken Sie die Eingabetaste.
2. Gehen Sie auf Datei" und wählen Sie "Snap-In hinzufügen/entfernen".
3. Wählen Sie im Menü auf der linken Seite den Eintrag "Zertifikate". Wählen Sie "Hinzufügen" und dann "Computerkonto >> Weiter >> Fertig stellen". Klicken Sie auf dann auf „OK".
4. Erweitern Sie den Bereich „Zertifikate (Lokaler Computer)". Erweitern Sie den Bereich "Vertrauenswürdige Zertifizierungsstellen".

   Klicken Sie darin auf den Ordner "Zertifikate" >> "Alle Aufgaben" >> "Importieren".

   Wählen Sie die Datei "cacert.pem" >> "Weiter" >> "Fertig stellen".

   Damit wird unsere kundenspezifische Zertifizierungsstelle erfolgreich als vertrauenswürdige Zertifizierungsstelle installiert.

Nachdem Sie diese Schritte ausgeführt haben, starten Sie den DruckCommsServer-Dienst.

5.5.3.7 Schritte zum Konfigurieren des selbstsignierten Zertifikats für DruckCommsServer bei Installation auf einem Clientcomputer

Um DruckCommsServer in HTTPS zu konvertieren, benötigen Sie das Java-Dienstprogramm Keytool und OpenSSL.

1. Das Dienstprogramm Keytool ist in Java enthalten, sodass Sie entweder Java auf Ihrem Computer installieren können oder die Verfügbarkeit von Java Keytool direkt ohne Installation von Java prüfen können.
2. Laden Sie sich OpenSSL für Windows herunter und installieren Sie die Software.
3. Legen Sie die Pfadvariable für den OpenSSL-Bin-Ordner fest, indem Sie den folgenden Befehl ausführen.

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

   Beispiel-Standardpfad:

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

4. Legen Sie die Pfadvariable für den JRE-Bin-Ordner fest, indem Sie den folgenden Befehl ausführen.

   C:\Programme\Java\<< Java version >>\bin

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

5. Stoppen Sie den DruckCommsServer-Dienst über die Windows-Dienste.
6. Erstellen Sie einen neuen Ordner mit der Bezeichnung **CommserverCertificate** auf Laufwerk C oder einem beliebigen anderen Laufwerk.

7. Rufen Sie die öffentliche 4Sight2-Zertifikatdatei **4SightV2PublicKey.cer** vom Servercomputer unter C:\Programme\Druck\4Sight2\<<latest folder number>>\app\Verzeichnis „Zertifikate“ ab und kopieren Sie sie in den Ordner **CommserverCertificate**.
8. Erstellen Sie jetzt die Dateien **openssl-server.cnf** und **openssl-ca.cnf**, indem Sie Schritt 4 und 5 in Abschnitt 5.5.3.5 ausführen. Erstellen Sie dann die Dateien „index.txt“ und „serial.txt“, indem Sie die Schritte 12 und 13 ausführen, im Ordner **CommserverCertificate**.
9. Jetzt befinden sich fünf Dateien im Ordner „CommServerCertificate“.
    a. openssl-server.cnf
    b. openssl-ca.cnf
    c. index.txt
    d. serial.txt
    e. 4SightV2PublicKey.cer
10. Öffnen Sie die Eingabeaufforderung mit Administratorberechtigungen.

    Navigieren Sie zum Ordner „CommserverCertificate“, indem Sie den folgenden Befehl ausführen:
    cd "<<full path to CommserverCertificate >>"
11. Führen Sie den folgenden Befehl aus, um die Dateien „cacert.pem“ und „cakey.pem“ zu erzeugen.

    openssl req -x509 -config openssl-ca.cnf -newkey rsa:4096 -sha256 -nodes -out cacert.pem -outform PEM
    Geben Sie die richtigen Zertifikatdaten ein, wenn Sie dazu aufgefordert werden, z. B. Land, Bundesstaat usw.
12. Ändern Sie jetzt den Inhalt der Dateien im Ordner **CommserverCertificate**, indem Sie Schritt 1 in Abschnitt 5.5.3.6 ausführen.
13. Führen Sie jetzt die Schritte 7 bis 11 in Abschnitt 5.5.3.6 aus.
14. Jetzt müssen wir mit dem folgenden Befehl den öffentlichen 4Sight-Schlüssel für die Authentifizierung der Kommunikation in den CommServer-„Cacerts“-Speicher importieren:

    keytool -import -noprompt -trustcacerts -alias <<4sight server hostname>> -storepass changeit -keystore "C:\Programme\Druck\DruckCommsServer\<< Communication Service version >>\cacerts" -file 4SightV2PublicKey.cer
15. Nachdem alle obenstehenden Schritte abgeschlossen sind, befinden sich die Dateien **DruckCommServer.pfx** und **CommServer.jks** im aktuellen Ordner **CommserverCertificate**.

    Kopieren Sie diese Dateien und fügen Sie sie in das Verzeichnis “**C:\Programme\Druck\DruckCommsServer\<< Communication Service version >>**“ ein.
    Bearbeiten Sie die **application.properties** am selben Speicherort, indem Sie den Wert der Eigenschaft wie folgt ändern:
    a. Keystore = CommServer.jks
    b. key-store.password = <<KeystorePassword>>
    c. key-store.type=JKS

5.5.3.7.1 Installieren des Zertifikats für 4Sight und DruckCommsServer in Windows

1. Öffnen Sie die Eingabeaufforderung, geben Sie “mmc“ ein und drücken Sie die Eingabetaste.
2. Gehen Sie auf „Datei“ und wählen Sie “Snap-In hinzufügen/entfernen“.
3. Wählen Sie im Menü auf der linken Seite den Eintrag “Zertifikate“. Wählen Sie “Hinzufügen“ und dann „Computerkonto“ >> “Weiter“ >> “Fertig stellen“. Klicken Sie auf dann auf „OK“.
4. Erweitern Sie den Bereich „Zertifikate (Lokaler Computer)“. Erweitern Sie den Bereich “Vertrauenswürdige Zertifizierungsstellen“.

   Klicken Sie darin auf den Ordner “Zertifikate" >> “Alle Aufgaben“ >> “Importieren“.

   Wählen Sie die Datei “cacert.pem“ >> “Weiter“ >> “Fertig stellen“.

   Damit wird unsere kundenspezifische Zertifizierungsstelle erfolgreich als vertrauenswürdige Zertifizierungsstelle installiert.

Nachdem Sie diese Schritte ausgeführt haben, starten Sie den DruckCommsServer-Dienst.

Wenn Sie lediglich prüfen wollen, ob DruckCommsServer erfolgreich in HTTPS konvertiert wurde, öffnen Sie in Google Chrome den folgenden Link: **https://localhost:9443/api/devicemanager/version** (Geben Sie Ihre CommServer-Portnummer ein, wenn Sie sie geändert haben, der Standardwert ist jedoch 9443.)

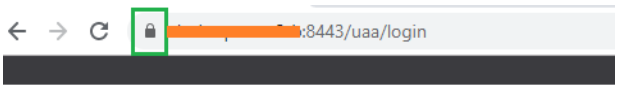
5.5.3.8 Validierung des Zertifikats in 4Sight2

1. Starten Sie den Server-PC neu.
2. Starten Sie die Dienste 4Sight2 und DruckCommsServer über die Windows-Dienste neu.
3. Öffnen Sie Google Chrome, leeren Sie den Browsercache und starten Sie Google Chrome neu. Stellen Sie sicher, dass keine anderen Instanzen von Google Chrome ausgeführt werden.
4. Fügen Sie die folgende URL in die Adressleiste ein und drücken Sie die Eingabetaste.

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

   Hinweis: Sie müssen den Hostnamen in der obenstehenden URL verwenden.
5. Daraufhin sollte der Anmeldungsbildschirm mit der richtigen HTTPS-URL angezeigt werden.

   Hinweis: Die rote Fehlermeldung in der Adressleiste ist nicht mehr vorhanden. Wenn die Verbindung weiterhin nicht sicher ist, starten Sie Ihren Computer neu und gehen Sie zu Schritt 3.



FAQs zur 4Sight2-Installation

6. FAQs zur 4Sight2-Installation

6.1 Einrichtung und Installation

Frage 1: Ich habe eine standortübergreifende Organisation, die sich über verschiedene Regionen der Welt hinweg global erstreckt. Wie kann ich 4Sight2 optimal einrichten?

Antwort: Das hängt davon ab, wie diese Standorte gepflegt und betrieben werden. Wenn alle Standorte über einen zentralen IT-Hub gepflegt und betrieben werden, können Sie eine einzige 4Sight2-Lizenz zentral installieren. Alle Standorte können so über das Netzwerk oder LAN auf 4Sight2 zugreifen. Bei Tochterfirmen, die separate Einheiten sind und selbstständig geführt und verwaltet werden, können Sie hingegen mehrere 4Sight2-Lizenzen erwerben.

Frage 2: Wenn ich mehrere 4Sight2-Lizenzen kaufe, kommunizieren diese miteinander?

Antwort: Nein. Bei jeder 4Sight2-Lizenz handelt es sich um eine isolierte separate Software mit eigener Anwendungsinstallation und Datenbank. Es gibt keine Kommunikation zwischen einzelnen Installationen. Kontaktieren Sie das 4Sight2-Team, um weitere Informationen zu erhalten oder spezielle Anforderungen zu besprechen.

Frage 3: Wie kann ich 4Sight2 herunterladen?

Antwort: Sie können 4Sight2 ganz einfach von der Website des Unternehmens herunterladen. Unten finden Sie den Link.

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

ODER

Sie können die Verkaufsbüros anrufen und eine Bestellung aufgeben. Sie sollten dann die Demoversion auf einem USB-Stick erhalten.

Frage 4: Kann ich 4Sight2 auf einem anderen Betriebssystem als Windows installieren?

Antwort: Nein. 4Sight2 wird nur für die Windows-Plattform unterstützt.

Frage 5: Ich habe 4Sight2 heruntergeladen und installiert. Wie kann ich auf 4Sight2 zugreifen?

Antwort: 4Sight2 ist eine webbasierte Software. Daher wird bei der Installation von 4Sight2 kein Symbol auf Ihrem Desktop oder Computer angelegt. Öffnen Sie für den Zugriff auf 4Sight2

- Google Chrome, fügen Sie die URL in die Adressleiste ein und drücken Sie die Eingabetaste,
- Wenn 4Sight2 auf demselben Computer installiert ist, verwenden Sie „http://localhost:<Anwendung_Portnummer> /4sight2“. Wenn 4Sight2 auf einem anderen Computer im selben Netzwerk installiert ist, verwenden Sie

  „http://<Computername ODER IP-Adresse>:<Anwendung_Portnummer>/4sight2“.
- Erstellen Sie ein Lesezeichen in Google Chrom zur späteren Verwendung.

Frage 6: Das 4Sight2-Installationsprogramm findet den Speicherort der Postgres-Datenbankdateien nicht.

Stellen Sie sicher, dass das Installationsprogramm an einem lokalen Speicherort extrahiert wurde und dass die ausführbare Datei in einem Ordner auf Datenträger 1 ausgeführt wird. Stellen Sie sicher, dass der lokale Speicherort, an dem das Installationsprogramm extrahiert wurde, keinen

langen Pfadnamen hat, da dies dazu führen kann, dass vom Installationsprogramm benötigte Dateien nicht gefunden werden.

Frage 7: Was passiert, wenn der Prozess zu irgendeinem Zeitpunkt während der Aktualisierung abgebrochen wird?

Antwort: Wenn der Administrator die Aktualisierung zu einem beliebigen Zeitpunkt abbricht, wird der Dienst auf die Version 1.4 zurückgesetzt und sollte funktionsfähig sein. Der Administrator muss die Aktualisierung erneut starten, um sie erfolgreich durchzuführen.

Frage 8: Bei der Installation der 4Sight2-Anwendung erhält der Benutzer möglicherweise diese Meldung: „Bitte geben Sie eine gültige Portnummer ein. Um die gültigen Portnummern zu erfahren, lesen Sie bitte das Installationshandbuch."

Antwort: Im Folgenden finden Sie den Bereich der ungültigen Ports. Wählen Sie einen gültigen Port, um mit der Installation fortzufahren.

- Die Ports 0 bis 1024 sind für die TCP-Verbindung reserviert.
- Liste der unsicheren Ports: 2049, 3659, 4045, 6000, 6665–6669, 65535

Frage 9: 4Sight2 mit HTTPS funktioniert im System nicht.

Antwort: Befolgen Sie die Syntax für den Domänennamen des Computers, auf dem die 4Sight2-Anwendung installiert werden soll.

<domain> ::= <subdomain>

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

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

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

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

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

<letter> ::= jeder der 52 Buchstaben A–Z in

Großschreibung und a–z in Kleinschreibung

<digit> ::= jede der zehn Ziffern 0–9

Hinweis: Bei Domänennamen sind Groß- und Kleinbuchstaben erlaubt. Zwei Namen mit gleicher Schreibweise, aber unterschiedlicher Groß- und Kleinschreibung werden als identisch behandelt.

6.2 FAQs zum Prüfmittelkommunikator

Frage 1: Ich habe alle Schritte im Installationshandbuch ausgeführt und kann mein Gerät in der Liste nicht sehen.

Antwort: Wenn Sie das Prüfmittel in der Liste nicht finden können, nachdem Sie diese Schritte ausgeführt haben, installieren Sie die 4Sight2-Treiber erneut. Gehen Sie zu **Systemsteuerung >> Programme und Funktionen** und deinstallieren Sie DruckCommsServer. Installieren Sie den Prüfmittelkommunikator erneut.

Frage 2: Ich erhalte die Fehlermeldung **Keine Geräte gefunden**.

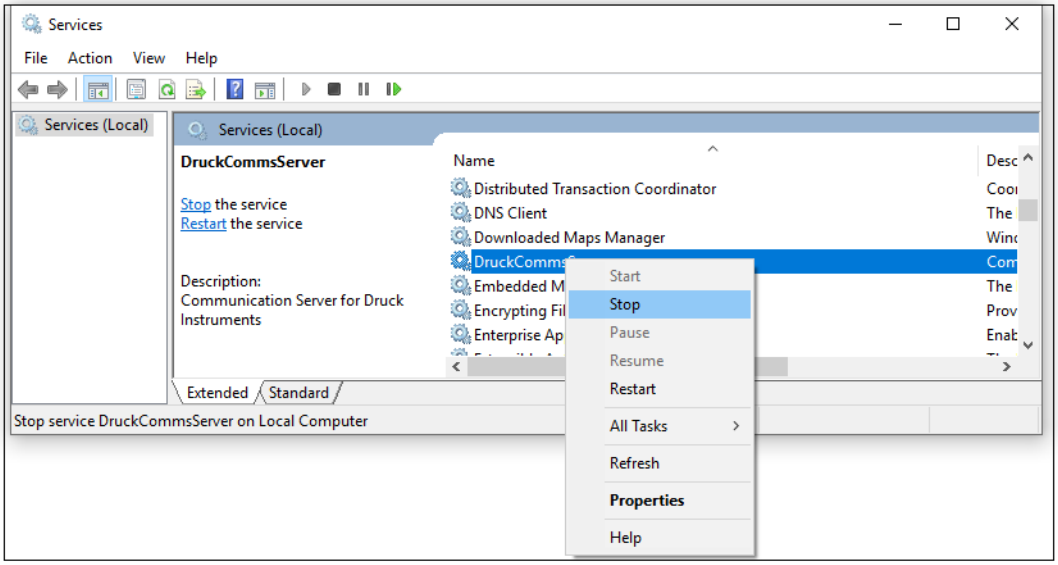
Antwort: Um das Problem zu beheben:

- Stellen Sie sicher, dass Sie das Gerät ordnungsgemäß über ein USB-Kabel physisch angeschlossen haben. Wechseln Sie dazu zum Geräte-Manager und suchen Sie Ihr Gerät in der Liste. Ihr Gerät sollte unter „Universal Serial Bus-Geräte“ angezeigt werden. Wenn Sie Ihr Gerät unter „Andere Geräte“ sehen, müssen Sie die obenstehenden Einstellungen vornehmen, um Ihr Gerät zu einem USB-Gerät zu machen.
- Stellen Sie sicher, dass sich Ihr Gerät im Kommunikations- oder Komm.-Modus befindet. Siehe Schritt 1 oben.
- Stellen Sie sicher, dass der Treiberpfad ordnungsgemäß auf „C:\Windows\INF…“ verweist (siehe Schritt 2 oben).

Frage 3: Ich erhalte die Fehlermeldung **Interner Serverfehler**, wenn ich auf „Aktualisieren“ klicke oder das Prüfmittel in der Liste auswähle.

Antwort: Um dieses Problem zu lösen, gehen Sie folgendermaßen vor:

- Gehen Sie zu den Windows-Diensten (auch als „Dienste“ bezeichnet).
- Rechtsklicken Sie in der Liste auf den Dienst **DruckCommsServer** und dann auf **Neu starten**.



- Gehen Sie zu 4Sight2 >> Klicken Sie auf die Schaltfläche **Aktualisieren**. Das Gerät sollte jetzt in der Liste angezeigt werden.

Frage 4: Ich erhalte die Fehlermeldung **Kommunikationsfehler**.

Antwort: Manchmal kann die Software mit dem Gerät nicht ordnungsgemäß kommunizieren. Dafür kann es mehrere Gründe geben, wie z. B. lose USB-Kontakte, ein aufgehängtes Gerät, ein mit anderen Aufgaben ausgelastetes Gerät, einen durch die Ausführung anderer Aufgaben ausgelasteten Server usw. Klicken Sie erneut auf die Schaltfläche „Aktualisieren“ und das Problem sollte behoben sein (versuchen Sie dies 2 bis 3 Mal).

Wenn der Fehler weiterhin angezeigt wird, versuchen Sie es mit den folgenden Schritten.

- Starten Sie Ihr Gerät (Genii/PACE) neu. Stellen Sie zuvor sicher, dass dies sicher möglich ist und das Gerät keinen kritischen Vorgang ausführt. Versuchen Sie es noch einmal. Stellen Sie auch sicher, dass das Gerät weiterhin physisch verbunden ist.

Wenn die obenstehenden Schritte nicht helfen, befolgen Sie die Anweisungen in Schritt 3 oben und starten Sie den Dienst **DruckCommsServer** neu.

Fehlerbehebung bei der Installation

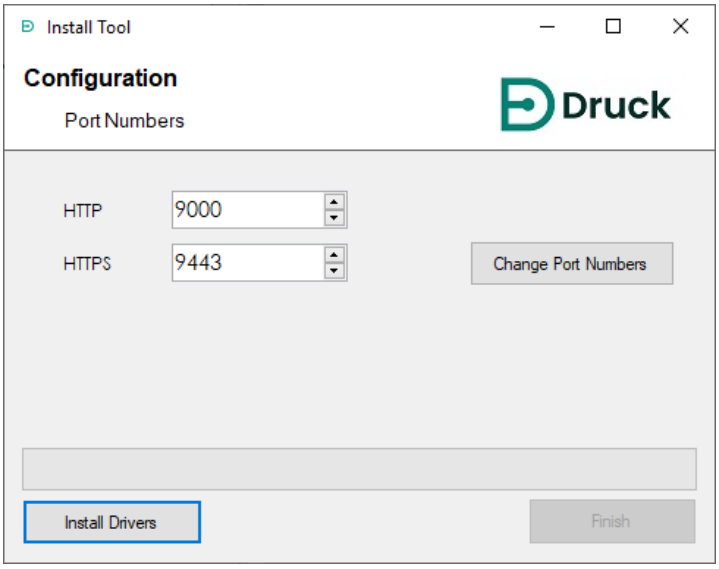
7. Fehlerbehebung bei der Installation

7.1 Kommunikationsprobleme mit Prüfmitteln

Wenn bei der Kommunikation mit Prüfmitteln über 4Sight2 keine Prüfmittel zurückgegeben werden, obwohl Sie erfolgreich geprüft haben, dass der Prüfmittelkommunikator bei einer direkten Abfrage des Kommunikators die Zeichenfolge „json“ zurückgibt, gibt es zwei mögliche Hauptursachen:

- Die Portnummern wurden falsch konfiguriert. Erkundigen Sie sich bitte bei Ihrem Benutzer mit administrativen Rechten, welche Ports 4Sight2 für die Kontaktaufnahme mit dem Prüfmittelkommunikator verwendet.

  Nachdem Sie in Erfahrung gebracht haben, welche Anschlüsse Sie verwenden sollten, navigieren Sie zu C:\Programme\Druck\DruckCommsServer\[Version] und führen Sie die Datei „CommsServerInstallTool.exe“ aus.



Bearbeiten Sie die Portnummern und klicken Sie auf die Schaltfläche **Portnummern ändern**. Warten Sie, bis der Dienst neu gestartet wird. Die Portnummern wurden jetzt geändert. Klicken Sie auf die Schaltfläche **Fertig stellen**.

- Der Prüfmittelkommunikator ist im Gegensatz zu 4Sight2 nicht für HTTPS konfiguriert.

  Wenden Sie sich an Ihren Administrator, um ein selbstsigniertes Zertifikat für den Prüfmittelkommunikator installieren zu lassen.

7.2 Postgres-Datenbanksicherung

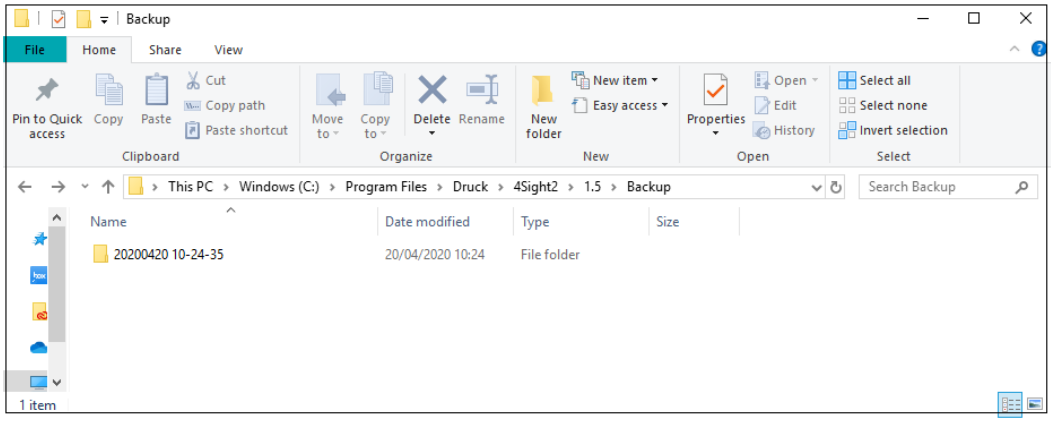
Nähere Informationen zur Postgres-Datenbanksicherung können Sie dem 4Sight2-Benutzerhandbuch – 123M3138 entnehmen.

7.3 Postgres-Datenbankwiederherstellung

Voraussetzung ist, dass Sie bereits eine Datenbanksicherung mithilfe der 4Sight-Anwendung durchgeführt haben.

Die 4Sight-Anwendung (ab Version 1.4) bietet eine Schnittstelle zum Initiieren einer Sicherung (benutzerinitiiert/geplant). Durch diesen Vorgang werden Dateien im Sicherungsordner des

4Sight-Installationsverzeichnis auf dem Server erstellt. Bei jeder initiierten Sicherung wird ein neuer Ordner innerhalb des Sicherungsordners mit dem Namen im Format YYYYMMDDHHSS (Jahr, Monat, Tag, Stunde und Sekunde) erstellt, abhängig von Datum und Uhrzeit, zu der die Sicherung erfolgreich abgeschlossen wurde.



Es wird empfohlen, den Inhalt des Sicherungsordners auf einem separaten Medium zu sichern.

Jeder Ordner enthält 5 Dateien.

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

Die *.bck-Dateien umfassen einen Suffix mit der 4Sight-Anwendungsversion. Bitte stellen Sie sicher, dass Sie eine Datenbank wiederherstellen, die genau der Version Ihrer Anwendung entspricht. Neuere oder ältere Versionen der Datenbank werden von der Anwendung nicht unterstützt. Beachten Sie, dass die Version einen Unterstrich (_) beinhaltet, keinen Punkt (.), z. B. 1_4 statt 1.4. Stellen Sie sicher, dass Sie <APPLICATION_VERSION> beim Verwenden der folgenden Befehle für die Wiederherstellungsschritte durch die korrekte installierte 4Sight-Version ersetzen.

Die metadata.properties-Datei enthält den Namen der Sicherung, wie er bei der Initiierung der Sicherung eingegeben wurde.

SHA 256-Prüfung

Bei einem Backup gibt es drei Dateien – eine für jede Datenbank mit der Erweiterung .bck. Die metadata.properties-Datei enthält den SHA 256 jeder Sicherungsdatei.

1. Öffnen Sie eine Eingabeaufforderung als Administrator und ändern Sie das Verzeichnis in den Ordner, der die ausgewählten Sicherungsdateien enthält.
2. Berechnen Sie anhand der folgenden Befehle den SHA256 der einzelnen Dateien.

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

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

3. Bevor Sie mit den Wiederherstellungsschritten fortfahren, überprüfen Sie, ob der SHA 256 der einzelnen Datei mit dem SHA 256 übereinstimmt, der in der Metadatendatei erwähnt wird. Die Sicherungsdatei ist für die Wiederherstellung gültig, wenn die Prüfsumme der Eingabeaufforderung und die der Metadatendatendatei genau übereinstimmen. Fahren Sie nur mit den Wiederherstellungsschritten fort, wenn dies der Fall ist.

7.4 Wiederherstellungsschritte

1. Melden Sie sich als Administrator beim 4Sight-Server an.
2. Suchen Sie den Port, auf dem die Postgres-Datenbank ausgeführt wird. Sie finden sie in der Eigenschaft „spring.datasource.url“ in der Datei „<4Sight INSTALLATION DIRECTORY>\apache-tomcat\webapps\application.properties“. Öffnen Sie diese Datei als Administrator mit Notepad. Es handelt sich um die Nummer direkt vor der 4Sight**<APPLICATION_VERSION>**.
3. Melden Sie sich über eine Eingabeaufforderung als Administrator beim psql command-Dienstprogramm an und verwenden Sie den Postgres-Benutzer.

   C:\Programme\PostgreSQL\11\bin\psql" --port=<DB_PORT> postgres postgres
4. Sie finden den Datenbankbenutzer, der von der Anwendung verwendet wird, in der Eigenschaft „spring.datasource.username“ in der Datei „<4Sight INSTALLATIONSVERZEICHNIS>\apache-tomcat\webapps\application.properties“. Öffnen Sie diese Datei als Administrator mit Notepad.
5. Löschen Sie *_temp-Datenbanken (falls vorhanden) und erstellen Sie dann mithilfe der folgenden Befehle leere *_temp-Datenbanken bei der psql-Aufforderung.

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

   Ändern Sie den Datenbankbesitzer der oben genannten 3 Datenbanken auf diesen Benutzer. Beachten Sie, dass beim Benutzernamen zwischen Groß- und Kleinschreibung unterschieden wird.

   ALTER DATABASE "4Sight**<APPLICATION_VERSION>**_temp" OWNER TO "**<DB_USER>**";
   ALTER DATABASE "4Sightaudit**<APPLICATION_VERSION>**_temp" OWNER TO "**<DB_USER>**";
   ALTER DATABASE "uaa**<APPLICATION_VERSION>**_temp" OWNER TO "**<DB_USER>**";
6. Überprüfen Sie die metadata.properties-Dateien der Sicherungen und legen Sie fest, welche Sicherung wiederhergestellt werden muss.

7. Öffnen Sie eine weitere Eingabeaufforderung als Administrator und ändern Sie das Verzeichnis in den Ordner, der die oben ausgewählten Sicherungsdateien enthält.

   Stellen Sie die Datenbanken der *.bck-Dateien anhand der folgenden Befehle auf *_temp-Datenbanken wieder her. Wenn Sie dazu aufgefordert werden, ein Kennwort einzugeben, verwenden Sie das Postgres-Superuser-Kennwort.
   "C:\Programme\PostgreSQL\11\bin\pg_restore" --port=**<DB_PORT>** --no-owner --username=postgres --dbname=4Sight**<APPLICATION_VERSION>**_temp -n public --role=**<DB_USER>** 4Sight**<APPLICATION_VERSION>**.bck

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

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

8. Löschen Sie die *_old-Datenbanken mithilfe der folgenden Befehle bei der psql-Aufforderung.

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

9. Beenden Sie den 4Sight-Dienst und pgAdmin-Anwendungen (falls geöffnet).

10. Benennen Sie die vorhandenen 4Sight-Datenbanken mithilfe der folgenden Befehle bei der psql-Aufforderung in *_old um.

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

11. Benennen Sie die *_temp-Datenbanken mithilfe der folgenden Befehle bei der psql-Aufforderung in 4Sight-Datenbanken um.

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

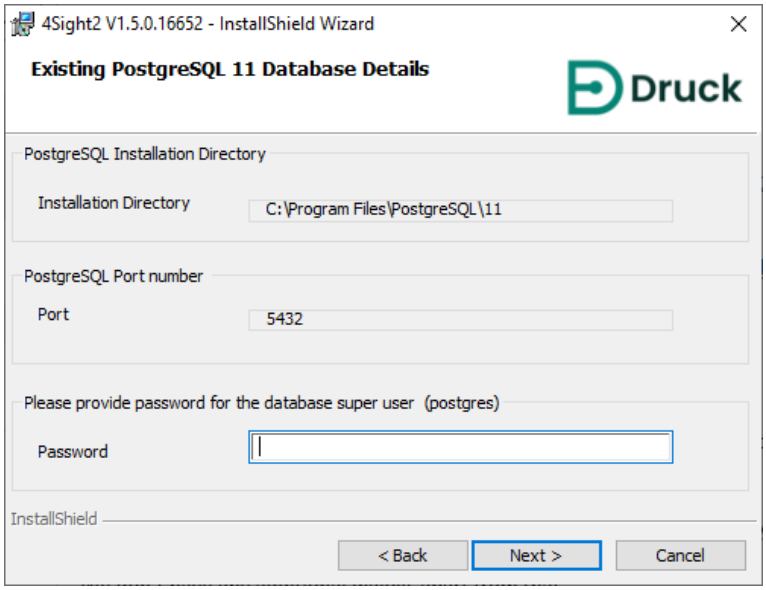
12. Starten Sie den 4Sight-Dienst und versuchen Sie, sich als Administrator anzumelden. Beachten Sie, dass für die Anmeldung jetzt das Kennwort des Administrators zum Zeitpunkt der Sicherungserstellung verwendet werden muss.

7.5 Wiederherstellung nach einem Crash des 4Sight2-Computers

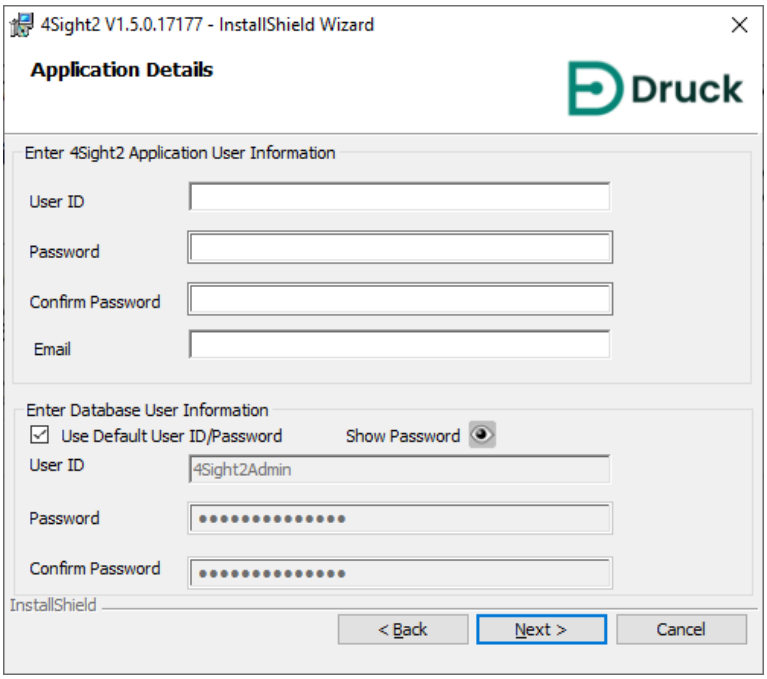
Voraussetzungen: Der Benutzer hat vor dem Computercrash eine Sicherung der 4Sight2-Datenbank erstellt.

Der Benutzer besitzt sowohl für die Anwendung als auch für die Datenbank den Benutzernamen und das Kennwort.

1. Installieren Sie das Betriebssystem und die Treiber auf dem Computer.
2. Installieren Sie 4Sight2 auf dem Computer.
3. Geben Sie bei der Installation der Anwendung dieselbe Kombination aus Benutzernamen und Kennwort ein, die Sie zuvor für die Anwendung und die Postgres-Datenbank verwendet haben.

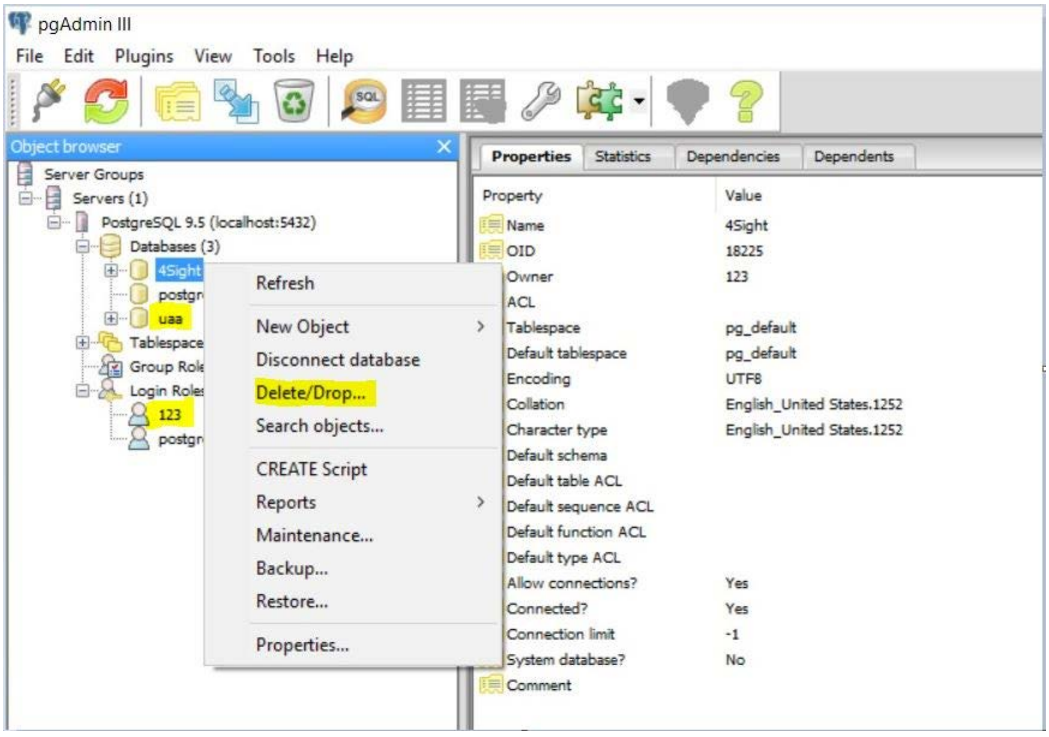


Verwenden Sie dasselbe Kennwort wie bei der vorherigen Installation.



Füllen Sie alle Felder so aus, wie Sie es bei der vorherigen Installation getan haben.

4. Nachdem die Anwendung erfolgreich installiert wurde, löschen Sie die bei der Anwendungsinstallation erstellte Standarddatenbank in pgAdmin (Rechtsklick auf die Datenbank und „Delete/Drop“). Wenn Sie beim Löschen der Datenbank eine Fehlermeldung erhalten, starten Sie den Postgres-Dienst neu und versuchen Sie es nach der Aktualisierung erneut.



5. Nachdem Sie die Datenbank und den Benutzer erfolgreich gelöscht haben, führen Sie die folgenden Schritte aus, um die Datenbank wie oben beschrieben in der Eingabeaufforderung wiederherzustellen.
6. Nachdem Sie die Datenbank erfolgreich wiederhergestellt haben, können Sie sie wie zuvor im Browser öffnen.

7.6 Szenario Installationsfehler

In der folgenden Tabelle sind die verschiedenen Fehlerszenarien während der Installation und die entsprechenden Lösungsansätze aufgeführt.

Fehlermeldung	Szenario	Erforderliche Lösung/Aktion
"Insufficient disk space available to install 4Sight2 application. Please ensure a minimum of 4096 MB is available. Free Space : available MB.	Fehler aufgrund von Problemen mit der Festplattengröße (wenn zu Beginn des Upgrades nicht genügend Speicherplatz vorhanden ist)	Der Administrator muss Speicherplatz auf dem jeweiligen Laufwerk freigeben und dann versuchen, den Aktualisierungsvorgang erneut durchzuführen.
"Deployment fail while Migrating database"	Fehler aufgrund von Problemen mit der Festplattengröße (wenn nach erfolgreichem Start des Upgrades nicht genügend Speicherplatz vorhanden ist)	Der Administrator muss Speicherplatz auf dem jeweiligen Laufwerk freigeben und dann versuchen, den Aktualisierungsvorgang erneut durchzuführen.
"Installation failed while migrating Database. Please reinstall 4sight2"	Fehler aufgrund von Datenintegrität in der Kopierdatenbank.	Der Administrator muss sich in diesem Fall an den Customer Help Desk wenden. Datenintegritätsgrund, der in Protokollen am Standort erfasst wird. [C:\Benutzer\[Benutzername]\ App Data\Local\Temp\logs]
"Installation failed while migrating Database. Please reinstall 4sight2"	Fehler aufgrund von Datenintegrität bei Schemaaktualisierungsphase.	Der Administrator muss sich in diesem Fall an den Customer Help Desk wenden. Datenintegritätsgrund, der in Protokollen am Standort erfasst wird. C:\Programme\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"	Diese Fehler tritt auf, wenn das Installationsprogramm nicht in der Lage ist, den Status des Dienstes abzurufen.	Der Administrator muss sicherstellen, dass der 4Sight2-Dienst ordnungsgemäß ausgeführt wird.

Fehlermeldung	Szenario	Erforderliche Lösung/Aktion
"Failed to start the 4Sight2 service. Please ensure the 4Sight2 service is present and running"	Fehler, wenn die Anwendung beschädigt ist, einige Dateien gelöscht wurden, der Port von einer anderen Anwendung verwendet wird oder der Benutzer den Dienst gestoppt hat usw.	Wenn der Administrator den Dienststatus abrufen kann und dieser aus irgendeinem Grund nicht ausgeführt wird (z. B. Anwendung beschädigt, einige Dateien wurden gelöscht, der Port wird von einer anderen Anwendung verwendet oder der Benutzer hat den Dienst gestoppt usw.), versucht das System, den Dienst zu starten. Wenn der Dienst nicht starten kann, muss der Administrator den Kundendienst kontaktieren, um das Problem zu beheben.
"Upgrade of 4Sight2 application is supported from version 1.3 onwards. For earlier version upgrade support please contact Customer Care."	Aktualisierung wird nicht durchgeführt, wenn eine ältere Version als 1.3 installiert ist.	Eine Aktualisierung ist nur von 1.3 auf eine höhere Version möglich.
Installer has detected another minor version of PostgreSQL 11. Installer will not continue. Refer to 4Sight2 Installation manual for more details	4Sight2 kann die Installation von 4Sight2 nicht fortsetzen, da dieselbe PostgreSQL-Version (Variante) auf dem Zielcomputer installiert ist.	Mögliche Abhilfen 1. Sie können einen anderen Computer wählen 2. Sichern Sie die bestehende Anwendung, die Postgres Version 11.3 verwendet, deinstallieren Sie diese Anwendung und installieren Sie sie auf einem anderen Gerät. Deinstallieren Sie Postgres und starten Sie die 4Sight2-Installation neu.
Installation failed while upgrading database. Please reinstall 4Sight2. Refer to 4Sight2 Installation manual for more details	Während des Upgrades ist möglicherweise ein interner Fehler aufgetreten. Der Benutzer kann versuchen, die Installation erneut durchzuführen.	Wenn sich das Problem nicht beheben lässt, kann der Benutzer die Installationsprotokolle übermitteln.

7.7 Allgemeine Fehlerursachen

Nachstehend sind einige gängige Probleme beschrieben, die bei der Kommunikation von 4Sight2 mit Druck Geräten über eine USB-Verbindung auftreten können.

- Die physische Verbindung ist lose oder instabil.
- Abgenutzte Kabel/Anschlüsse
- USB-Adapter schlechter Qualität
- Überlastetete USB-Adapter/Anschlüsse
- Die Geräte waren zu lange eingeschaltet, sodass sie sich in den Energiesparmodus oder Schlafmodus geschaltet haben.
- Die Geräte befinden sich nicht im Kommunikationsmodus.
- Die Treibersoftware wurde nicht installiert oder nicht aktualisiert. Um die Kommunikation mit der Hardware herzustellen, benötigen Sie die 4Sight2-Anwendung und die Treiber derselben Version.
- Auf den Geräten sind sehr alte Firmwareversionen installiert.

7.8 4Sight2 deinstallieren

Befolgen Sie diese Anweisungen, wenn Sie eine neue Kopie oder eine neue Version von 4Sight2 installieren möchten oder 4Sight2 wegen Problemen bei der Installation deinstallieren müssen.

Durch die Deinstallation der PostgreSQL-Datenbankkomponente wird die 4Sight2-Datenbank gelöscht, was zu Datenverlust führt. Durch die folgenden Schritte wird nicht automatisch eine Sicherung erstellt. Stellen Sie also sicher, dass Sie eine manuelle Sicherung erstellt und an einem anderen Speicherort im 4Sight2-Installationsordner gespeichert haben, bevor Sie fortfahren. Beachten Sie die Hinweise im Abschnitt „Sichern und Wiederherstellen der PostgreSQL-Datenbank“ in diesem Handbuch.

Wenn Sie nur die 4Sight2-Anwendung deinstallieren möchten und die Datenbank behalten wollen, lesen Sie im Abschnitt zur Installation von 4Sight2 in diesem Handbuch nach. Nach der erneuten Installation benötigen Sie die Anmeldedaten vom Datenbank-Superuser. Führen Sie keine Deinstallation durch, wenn Sie nicht über diese Daten verfügen.

Wenn Sie Ihre 4Sight2-Version aktualisieren möchten, ohne die Datenbank zu deinstallieren, befolgen Sie diese Anweisungen **NICHT**.

1. Gehen Sie zu „Systemsteuerung >> Programme und Funktionen“.
2. Rechtsklicken Sie auf „4Sight2“ und wählen Sie „Deinstallieren“.
3. Befolgen Sie die Anweisungen im Deinstallationsassistenten.
4. Rechtsklicken Sie auf „PostgreSQL 11“ und wählen Sie „Deinstallieren“.
5. Befolgen Sie die Anweisungen im Deinstallationsassistenten.
6. Durch die Deinstallation von PostgreSQL wird der Datenordner nicht gelöscht. Sie müssen dies manuell tun. Löschen Sie den Datenordner, den Sie unter C:\Programme\PostgreSQL\11\ finden.
   a. Wenn Sie den gesamten PostgreSQL-Ordner löschen möchten, stellen Sie sicher, dass jegliche Sicherungsdateien und Skripte aus dem Ordner „Papierkorb“ entfernt wurden, bevor Sie fortfahren.
   b. Standardmäßig werden 4Sight2-Datenbanksicherungen an folgendem Speicherort erstellt und gespeichert: C:\Program Files\PostgreSQL\11\bin
7. Es wird empfohlen, den Computer neu zu starten (falls möglich).
8. 4Sight2 wurde jetzt erfolgreich deinstalliert.

7.9 Fehlerbehebung für die sichere Kommunikation

1. Der Befehl „Befehlsname“ wird nicht als interner oder externer Befehl erkannt. Beispiel: „keytool“ wird nicht als interner oder externer Befehl erkannt.

- Wenn Sie eine solche Fehlermeldung erhalten, kann die Eingabeaufforderung in dem Ordner, in dem Sie sich gerade befinden, keinen Verweis auf den angegebenen Befehl finden.

  Um diesen Fehler zu beheben, verwenden Sie den folgenden Befehl, um auf den richtigen Ordner zu verweisen.

  Set Path=%Path%;“<<vollständiger Pfad des Speicherorts für den Befehl>>"

  Wenn Sie beispielsweise die obenstehende Fehlermeldung für den Befehl „keytool“ erhalten, geben Sie den Pfad wie folgt ein:

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

2. Ungültige IP-Adresse

- Wenn Sie eine Fehlermeldung mit diesem Text erhalten, bedeutet dies, dass die IP-Adresse oder der Hostname in der Datei „openssl-ca.cnf“ oder „openssl-server.cnf“ fehlerhaft ist. Hinweis: Sie müssen diese Angaben möglicherweise an mehreren Stellen in diesen Dateien korrigieren und die Schritte erneut ausführen.

3. Keine entsprechende Datei/kein entsprechendes Verzeichnis…

- Wenn Sie eine solche Fehlermeldung erhalten, verweist der von Ihnen ausgeführte Befehl wahrscheinlich auf einen fehlerhaften Dateinamen. Prüfen Sie den Befehl auf Fehler in Dateinamen und vergewissern Sie sich, dass die Datei mit dem entsprechenden Namen in dem Ordner vorhanden ist. Führen Sie dann den Befehl noch einmal aus. Sie müssen möglicherweise den Dateinamen im Befehl korrigieren oder die Schritte zur Erzeugung der fehlenden Datei(en) ausführen.
- Dieser Fehler kann für die Datei „index.txt“ und „serial.txt“ auftreten, da in bestimmten Fällen die Dateinamenerweiterung dem Namen zweimal hinzugefügt wird, z. B. „intex.txt.txt“.

  Bearbeiten Sie in diesem Fall einfach die Datei und speichern Sie sie ohne die Erweiterung „.txt“. Stellen Sie sicher, dass die Datei nur eine „.txt“-Erweiterung aufweist.

Best Practices

8. Best Practices

Härten des Servers

Serverumgebung entsprechend den Richtlinien von Microsoft oder des CIS härten.

8.1 Tomcat

- Tomcat in einem sicheren Ordner installieren, auf den nur der Administrator oder LocalService Zugriff haben, wie *„C:\Programme (x86)“*.
- Tomcat als Dienst installieren, der im LocalService-Konto ausgeführt wird.
- Alles an unerwünschten standardmäßigen Anwendungen aus der Webanwendung entfernen.
- Standard-Fehlerseiten wie 404, 403, 500 usw. ersetzen.
- HTTPS erzwingen, SSL aktivieren.
- Managementanwendung mit SSL ausführen.
- Für jede Webanwendung eine eigene Protokolldatei verwenden.
- Server-Banner entfernen.
- Zugriffsprotokollierung aktivieren.
- Port und Befehl für das Abschalten ändern.

8.2 PostgreSQL

- Für alle Konten mit erhöhten Rechten, wie pgdba, postgres, depesz, darf ausschließlich eine lokale Anmeldung zulässig sein.
- Die Reihenfolge in der Konfigurationsdatei „pg-hba.conf“ muss stimmen, damit die richtigen Benutzer den richtigen Zugriff erhalten.
- „Pg-hba.conf“ muss so konfiguriert sein, dass eine Verbindung zum Server nur vom lokalen Computer aus und nicht über das Netzwerk hergestellt werden kann.

8.3 Best Practices für die Firewall

Hier finden Sie einige bewährte Maßnahmen für die Firewall, die Sie mit 4Sight2 anwenden sollten:

8.3.1 Richtlinie

1. Die Firewallkonfiguration muss der Sicherheitsrichtlinie des Unternehmens entsprechen.
2. Stets das Prinzip der geringsten Rechte anwenden. Standardmäßig alles ablehnen. Spezifischen Datenverkehr zulassen (unter Verwendung von Ursprung, Ziel und Port).
3. Spezifische Regeln am Anfang platzieren und explizite Regeln für das Trennen nutzen.
4. Alle Aktionen für den Audit Trail protokollieren, insbesondere fehlgeschlagene Versuche.

8.3.2 Ressourcen

1. Speicherverwendung überwachen
2. CPU-Verwendung überwachen.
3. Bandbreitenverwendung überwachen.
4. Anzahl der Anwendungen begrenzen, die auf dem Firewall-Computer ausgeführt werden.

8.3.3 Installation und Wartung

1. Physischen Zugriff auf den Firewall-Computer einschränken.
2. Eindeutige Benutzer-ID für die Verwaltung verwenden.
3. Strikte Kontorichtlinie auf dem Computer einhalten.
4. Regelmäßiges Patchen von Betriebssystemen, Anwendungssoftware, Firmware usw.
5. Regelsätze, Konfiguration und Protokolle regelmäßig archivieren. Alle Regeln und durchgeführten Änderungen in einer Versionsverwaltung dokumentieren.
6. Regelmäßige Tests durchführen.
7. Nicht verwendete Regeln entfernen, wenn ein Dienst stillgelegt wird.
8. Regeln regelmäßig auditieren und überprüfen.
9. Sicherheitsmeldungen regelmäßig überwachen.

8.3.4 Zusätzliche Sicherheitsmaßnahmen

1. Zustandsbezogene Prüfungen durchführen.
2. Proxys verwenden.
3. Prüfung und Filterung auf Anwendungsebene verwenden.

8.3.5 Interner Schutz

1. Richtlinien für die akzeptable Nutzung festlegen (AUP, Acceptable Usage Policy).
2. Persönliche Firewall für alle Benutzer
3. Hostbasierte Verhinderung von Eindringversuchen
4. Netzwerküberwachung
5. Inhaltsfilterung
6. Zugriffskontrolle auf allen Computern und für alle Anwendungen

Geschäftsstellen

Hauptsitz
Leicester, Großbritannien
Telefon: +44 (0) 116 2317233
E-Mail: gb.sensing.sales@bakerhughes.com

Australien
Springfield (Zentrale)
Telefon: 1300 171 502
E-Mail: custcare.au@ge.com

China
Guangzhou
Telefon: +86 173 1081 7703
E-Mail: dehou.zhang@bakerhughes.com

China
Peking
Telefon: +86 180 1929 3751
E-Mail: fan.kai@bakerhughes.com

China
Schanghai
Telefon: +86 135 6492 6586
E-Mail: hensen.zhang@bakerhughes.com

Deutschland
Frankfurt
Telefon: +49 (0) 69-22222-973
E-Mail: sensing.de.cc@bakerhughes.com

Frankreich
Toulouse
Telefon: +33 562 888 250
E-Mail: sensing.FR.cc@bakerhughes.com

Indien
Bangalore
Telefon: +91 9986024426
E-Mail: aneesh.madhav@bakerhughes.com

Italien
Mailand
Telefon: +39 02 36 04 28 42
E-Mail: csd.italia@bakerhughes.com

Japan
Tokio
Telefon: +81 3 6890 4538
E-Mail: gesitj@bakerhughes.com

Niederlande
Hoevelaken
Telefon: +31 334678950
E-Mail: nl.sensing.sales@bakerhughes.com

Russland
Moskau
Telefon: +7 915 3161487
E-Mail: aleksey.khamov@bakerhughes.com

USA
Boston
Telefon: 1-800-833-9438
E-Mail: custcareboston@bhge.com

VAE
Abu Dhabi
Telefon: +971 528007351
E-Mail:
suhel.aboobacker@bakerhughes.com

Service- und Supportstandorte

Technischer Support
Global
E-Mail: mstechsupport@bakerhughes.com

Brasilien
Campinas
Telefon: +55 11 3958 0098, +55 19 2104 6983
E-Mail: mcs.services@bakerhughes.com

China
Changzhou
Telefon: +86 400 818 1099
E-Mail: service.mcchina@bakerhughes.com

Frankreich
Toulouse
Telefon: +33 562 888 250
E-Mail: sensing.FR.cc@bakerhughes.com

Großbritannien
Leicester
Telefon: +44 (0) 116 2317107
E-Mail: sensing.grobycc@bakerhughes.com

Indien
Pune
Telefon: +91 213 5620426
E-Mail:
mcsindia.inhouseservice@bakerhughes.com

Japan
Tokio
Telefon: +81 3 3531 8711
E-Mail: service.druck.jp@bakerhughes.com

USA
Billerica
Telefon: +1 (281) 542-3650
E-Mail: namservice@bakerhughes.com

VAE
Abu Dhabi
Telefon: +971 2 4079381
E-Mail: gulfservices@bakerhughes.com

123M3140 Revision F | Deutsch

Baker Hughes