



4Sight2

校正管理ソフトウェア

インストールマニュアル 123M3140 改訂 F

目次

1. はじめに	1
1.1 対象読者	1
1.1.1 管理者	1
1.1.2 スーパーバイザー	1
1.1.3 技術者	1
1.1.4 監査者	1
2. システム要件	2
2.1 アプリケーションサーバー	2
2.2 クライアントワークステーション	2
2.3 ローカルインストール	2
2.4 4Sight2 をサポートしているファームウェア	3
3. 4Sight2 のインストール	5
3.1 データベースのインストール	7
3.2 PostgreSQL のインストール	7
4. 4Sight2 試験機器コミュニケーターのインストール	14
4.1 手動でのドライバ構成	19
4.1.1 前提条件	19
4.2 試験機器コミュニケーターのテスト	23
4.3 温度校正器ドライバ構成	24
5. 展開ガイド	26
5.1 展開アーキテクチャ	26
5.2 物理的展開	26
5.3 ネットワーク	26
5.4 展開シーケンス	26
5.5 展開後のタスク	27
5.5.1 ユーザーおよびグループの追加	27
5.5.2 デフォルトパスワード	27
5.5.3 セキュアな通信	27
6. 4Sight2 のインストールに関する FAQ	44
6.1 設定とインストール	44
6.2 試験機器コミュニケーターに関するFAQ	45
7. インストール時のトラブルシューティング	48
7.1 試験機器の通信時の問題	48
7.2 Postgres データベースバックアップ	48
7.3 Postgres データベース復元	48
7.4 復元の手順:	50
7.5 4Sight2 マシンクラッシュからの回復方法	51
7.6 インストール時の障害のシナリオ:	53
7.7 エラーの一般的な原因	55
7.8 4Sight2 のアンインストール	56
7.9 セキュア通信に関するトラブルシューティング	56

8. ベストプラクティス.....	59
8.1 Tomcat	59
8.2 PostgreSQL.....	59
8.3 ファイアウォールのベストプラクティス.....	59
8.3.1 ポリシー	59
8.3.2 リソース	59
8.3.3 インストールと保守	60
8.3.4 さらなるセキュリティ強化	60
8.3.5 内部的な保護.....	60

1. はじめに

4Sight2 校正ソフトウェアは、測定技術分野の最高水準に合わせたお客様の校正環境の維持と管理に役立つ Web ベースの校正管理ツールです。ソフトウェアは次のタスクに使用できます。

- 指定の事業所のすべての測定装置の校正を管理
- 技術者用に構成スケジュールを設定
- USB 通信機能を備えた Druck のポータブル校正器 (DPI620 Genii、DPI611、および DPI612) との間でデータをアップロードおよびダウンロード
- ポータブル校正器でサポートされていない装置の校正記録を管理 (データの手動入力)
- 校正履歴記録を点検。各校正証明書のプリント記録も作成できます。例: ISO 9000 品質管理手順。
- Druck 圧力コントローラ (PACE 1000、5000、6000)、ポータブル校正器 (DPI620 Genii、DPI611、DPI612)、温度校正器 (DryTC165、DryTC 650、LiquidTC165、LiquidTC255) を使用した自動校正を制御

1.1 対象読者

1.1.1 管理者

管理者は 4Sight2 ソフトウェアのインストールおよび構成の責任を負います。4Sight2 の初期インストールの後に、単一の管理用アカウントが利用可能になります。このアカウントから新しいユーザーを作成し、グループ/権限のセットを割り当てます。管理者ユーザーは 4Sight2 の全機能の読み出しおよび書き込みができます。

1.1.2 スーパーバイザー

スーパーバイザーはアセットと校正管理の責任を負います。スーパーバイザーはプラント、ロケーション、タグ、装置を含む 4Sight2 Enterprise 内でアセットを作成し更新することができます。またプラントの工程、装置のデータシート等のドキュメントをアセットへリンクさせることに責任を負います。スーパーバイザーは校正中に使用する試験手順を作成し、また手順のスケジュールリングや装置の正常性の監視ができます。スーパーバイザーは校正を承認するために必要な許可を得ています。

1.1.3 技術者

技術者は校正の実行の責任を負います。校正はポータブル、手動、自動のどれかでを行い、装置に合った適切な校正を行うことが技術者の役割です。校正を行ったら、技術者がその結果を確認し、校正を完了してスーパーバイザーの承認を得ます。

1.1.4 監査者

監査者は報告の検査の責任を負います。一部のプラントでは、規制要件として監査の実行が必須である場合があります。

2. システム要件

4Sight2 アプリケーションをクライアントマシンおよびサーバーマシンにインストールするための最小システム要件を以下に示します。

2.1 アプリケーションサーバー

オペレーティングシステム	Windows 10、Windows Server 2012 R2、Windows Server 2016、Windows Server 2019
アップデート	Windows のすべての更新がインストールされている
プロセッサ	Quad Core
RAM	8GB 以上 (32GB 推奨)
ディスク容量	1TB
ネットワーク速度	10Mbps

2.2 クライアントワークステーション

オペレーティングシステム	Windows 10、Windows Server 2012 R2、Windows Server 2016、Windows Server 2019
ブラウザ	Google Chrome V80+、Microsoft Edge V80、Firefox V74
Adobe Reader	Adobe Acrobat Reader DC Version 2015.017.20050 +
RAM	8GB 以上
プロセッサ	Dual Core
ディスク容量	600GB
ネットワーク速度	10Mbps

2.3 ローカルインストール

オペレーティングシステム	Windows 10、Windows Server 2012 R2、Windows Server 2016、Windows Server 2019
アップデート	Windows のすべての更新がインストールされている
Adobe Reader	Adobe Acrobat Reader DC Version 2015.017.20050 +
プロセッサ	Dual Core
RAM	16GB 以上 (32GB 推奨)
ディスク容量	500GB 以上のディスク容量
ブラウザ	Google Chrome V80+、Microsoft Edge V80、Firefox V74

2.4 4Sight2 をサポートしているファームウェア

サポートされているファームウェアの最新情報については、次のリンクを参照してください。

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

また



PACE の場合、下の図に示すように 4Sight2 通信用の USB B を挿入します。



4Sight2 のインストール

3. 4Sight2 のインストール

4Sight2 をインストールするには、最初に 4Sight2 Setup zip をデスクトップにコピーして、zip からファイルを抽出します。設定ファイルから 4Sight2 実行ファイルを選択します。

注記: 4Sight2 や Comm Server がウイルスに感染していないか検査するため、次のソフトウェアを使っています。

- McAfee VirusScan Enterprise + AntiSpyware Enterprise (バージョン番号: 8.8.0)
- Symantec Endpoint Protection (バージョン番号: 14.3.558)

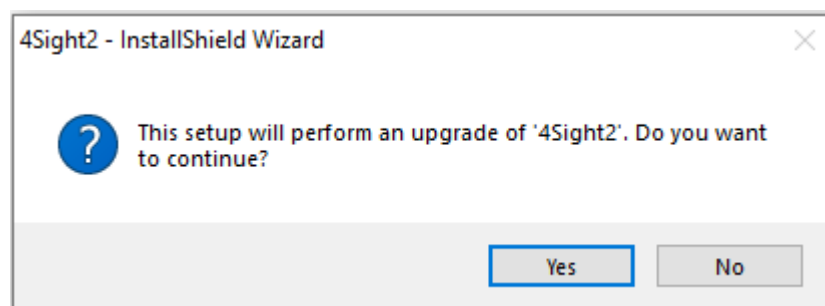


セットアップ実行形式ファイルを実行するとInstallShield ウィザードが開始されます。InstallShield ウィザードでは、以下の 2 段階で 4Sight2 のインストールを実行します。

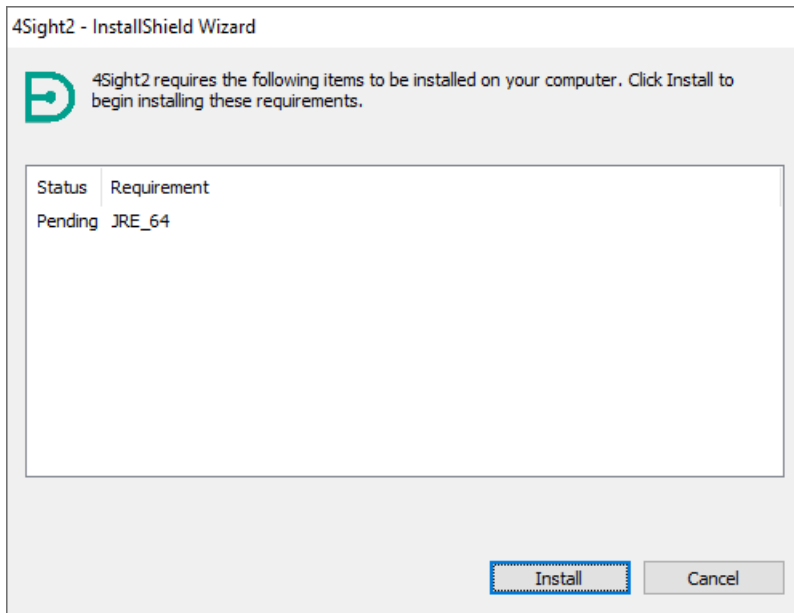
1. データベースのインストール
2. Web アプリケーションのインストール

InstallShield ウィザードからの指示に従うか、以降の 2 セクションを参照して、インストールのプロセスを段階的に実行します。

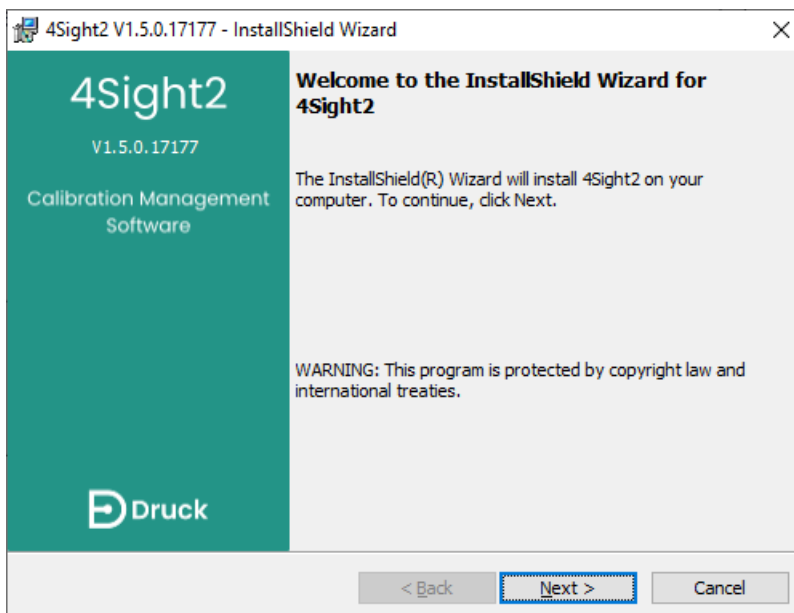
1. 4Sight2 がすでにマシンにインストールされている場合は、インストールウィザードによって最新バージョンへのアップグレードを行うように促されます。最新アップグレードを実行する場合は **[はい]** をクリックしてください。



2. このマシンに 4Sight2 を初めてインストールする場合は、インストールウィザードによって次の画面が表示されます。**[インストール]** を選ぶと、リスト表示されている項目がインストールされます。



3. 前もって必要な項目をインストールすると、[InstallShield ウィザードへようこそ] 画面が表示されます。[次へ] をクリックして続行します。



3.1 データベースのインストール

4Sight2 アプリケーションは PostgreSQL データベースを使用します。PostgreSQL データベースのインストール方法と PostgreSQL データベースがすでにインストールされている場合の操作について、以下に手順を示します。

3.2 PostgreSQL のインストール

マシンに PostgreSQL データベースがインストールされていない場合、この手順に従ってください。

1. インストールされた PostgreSQL データベースのインスタンスがマシンに存在しない場合は、インストールウィザードによって次の画面が表示されます。

The screenshot shows the 'Database Install' wizard window. It contains the following fields and options:

- Installation Directory:** C:\Program Files\PostgreSQL\11\
- Data Directory:** C:\Program Files\PostgreSQL\11\data\ (with a 'Change..' button)
- Password for postgres:** Includes a checked 'Use Default Password' box, a 'Show Password' eye icon, and two password input fields (one for Password, one for Confirm Password).
- Port:** 5434
- Buttons:** '< Back', 'Next >', and 'Cancel'.

[インストールディレクトリ]: PostgreSQL アプリケーションをインストールできるディレクトリを選択します。

[データディレクトリ]: PostgreSQL データベースを保存できるディレクトリを選択します。

[パスワード]/[パスワードの確認]: PostgreSQL データベースのスーパーユーザーのパスワードを入力します。この入力は、PostgreSQL データベースを初めてインストールする場合のみ求められます。

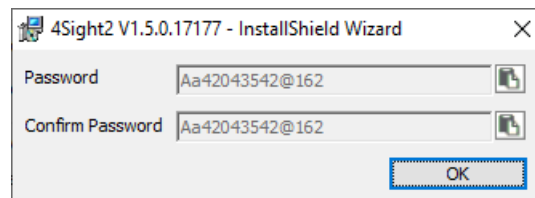
注記: このパスワードは、インストール後にデータベースの内容にアクセスするときが必要となります。

[ポート]: これは、アプリケーションリクエストに対応するための PostgreSQL データベースのポートアドレスです。

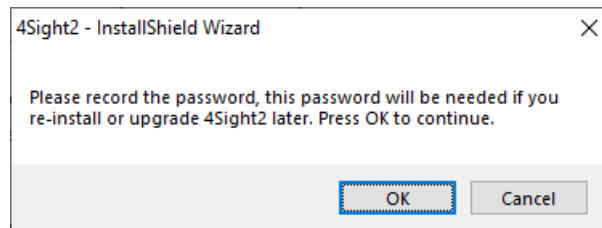
注記: ポート番号がすでに使用されている場合は、IT チームに連絡してください。ユーザーはポート番号を変更することもできます。ポート番号は、後でアプリケーションを起動するときに必要となるため書き留めておいてください。



重要: ユーザーはデータベースのパスワードをメモしておく必要があります。パスワード情報を無くすと、アクセス拒否やデータ消失を起こす恐れがあります。[デフォルトパスワードの使用]
 チェックボックスのチェックを外し、データベースのスーパーユーザーパスワードを更新します。デフォルトのパスワードを使い続けたい場合や、入力した新しいパスワードを表示したい場合は、
 (パスワード表示)アイコンを選択します。パスワードをクリップボードにコピーするには、
 (クリップボードにコピー)アイコンを使用します。



するとインストーラーに、パスワードを再度記録するように促されます。パスワードの記録ができれば、[OK]を選択します。



- このステップは、PostgreSQL データベースがすでにインストールされている場合のみユーザーに表示されます。

【インストールディレクトリ】: これは、PostgreSQL がすでにインストールされているパスを指定するためのものです。読み取り専用情報です。

【パスワード】: これは、PostgreSQL データベースのスーパーユーザーパスワードを確認するためのものです。

【ポート】: これは、db リクエストを実行するために PostgreSQL データベースが使用しているポート番号を指定するためのものです。

3. [アプリケーションの詳細] ウィンドウで、次の詳細情報を入力します。

[ポート]: 4Sight2 Web アプリケーションが HTTP リクエストに回答するために使用する Tomcat Web サーバーポートを入力します。

[アプリケーション名]: ブラウザで 4Sight2 アプリケーションに接続するために使用するアプリケーションコンテキストパスを入力します。デフォルトでは 4sight2 です。

注記: ポート番号がすでに使用されている場合は、IT チームに連絡してください。ユーザーはポート番号を変更することもできます。ポート番号は、後でアプリケーションを起動するときに必要となるため書き留めておいてください。

4. **[次へ]** を選択すると **[アプリケーションのユーザー情報]** 画面が表示されます。

[アプリケーションのユーザー情報]: このセクションでは、4Sight2 アプリケーションにアクセスするためのスーパーユーザー名とパスワードを入力します。

注記: このパスワードは、インストール時に 4Sight2 アプリケーションにアクセスするために必要になります。

[データベースのユーザー情報]: このセクションでは、4Sight2 アプリケーションが PostgreSQL データベースと通信するために使用するデータベースユーザー名とパスワードを入力します。

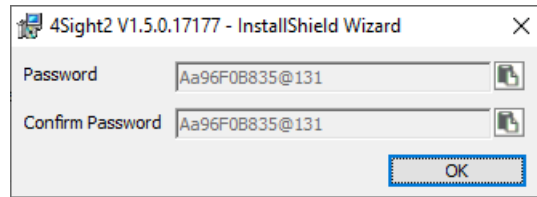


重要: ユーザーはデータベースのパスワードをメモしておく必要があります。パスワード情報を無くすと、アクセス拒否やデータ消失を起こす恐れがあります。[デフォルトパスワードの使用]

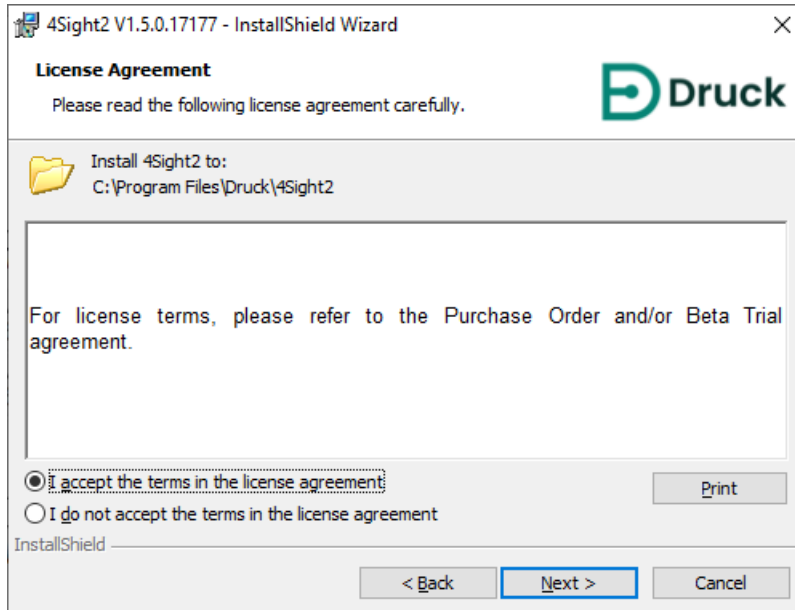
チェックボックスのチェックを外し、データベースのスーパーユーザーパスワードを更新します。デフォルトのパスワードを使い続けたい場合や、入力した新しいパスワードを表示したい場合は、

(パスワード表示) アイコンを選択します。パスワードをクリップボードにコピーするには、

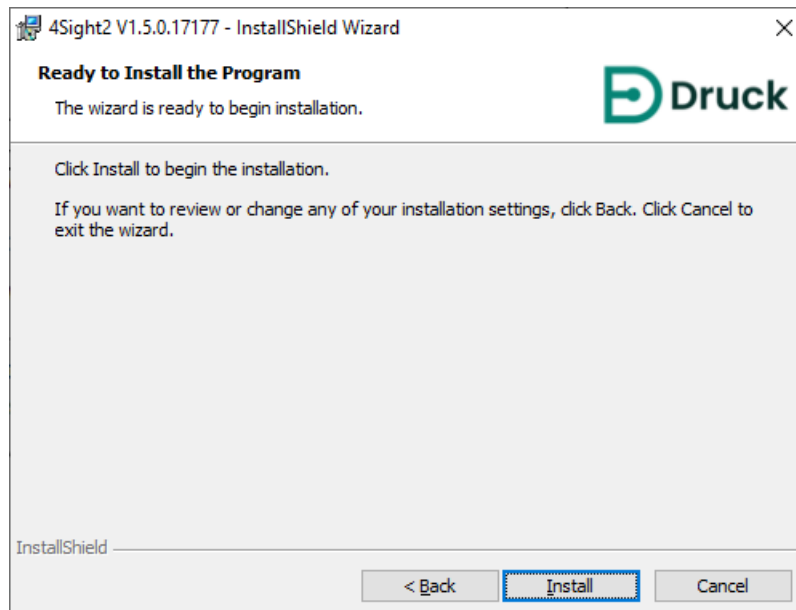
(クリップボードにコピー) アイコンを使用します。



5. ライセンスの契約条件を読んだ後、[ライセンスの契約条件に同意します。] ラジオボタンを選択し、[次へ] をクリックします。

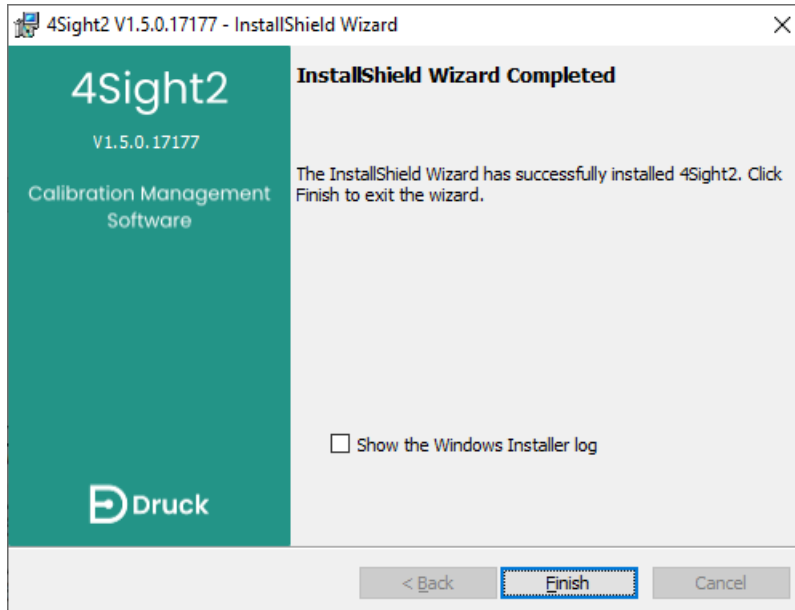


6. [インストール] をクリックするとインストールが開始されます。4Sight2 アプリケーションおよびデータベースに関連したすべてのソフトウェアパッケージがインストールされます。



以上で 4Sight2 アプリケーションのセットアップが完了です。

7. [完了] ボタンを押してウインドウを閉じ、次のセクションの指示に従って 4Sight2 アプリケーションにログインします。



サーバー上で 4Sight2 にローカルにログインするには、次の URL に移動します。

`http://ComputerName または IPAddress:PortNo/ApplicationName`

- **ComputerName** - 4Sight2 アプリケーションがインストールされた PC の名前です。この名前は、この PC を右クリックしてプロパティを選択すれば確認できます。
- **IPAddress** - 4Sight2 アプリケーションがインストールされた PC の IP アドレスです。このアドレスは、Windows コマンドウィンドウで「ipconfig」を実行することで確認できます。
- **PortNo** - アプリケーションのインストール時に [Tomcat ポート番号] フィールドに入力した番号です。
- **ApplicationName** - アプリケーションのインストール時に [アプリケーション名] フィールドに入力した名前です。

4Sight2 試験機器コミュニケーターのインストール

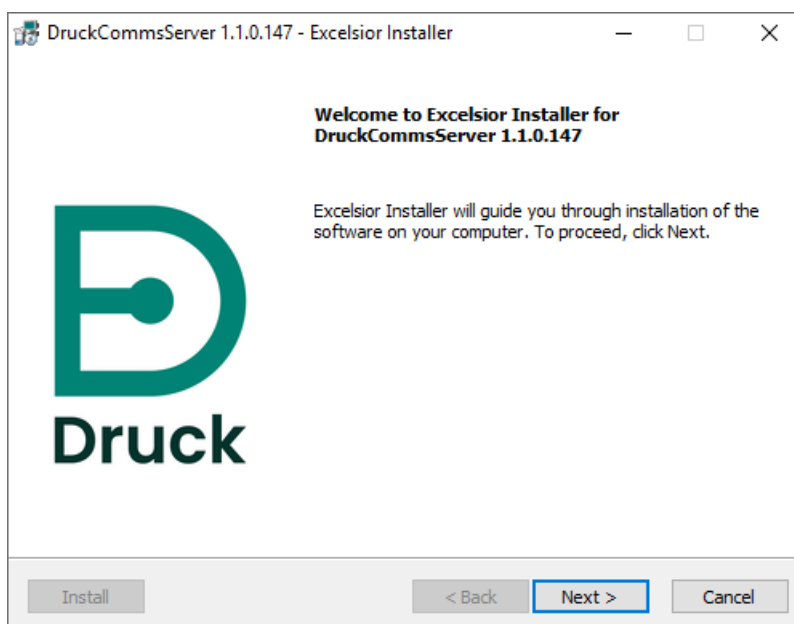
4. 4Sight2 試験機器コミュニケーターのインストール

1. 試験機器コミュニケーターは Druck の計器と 4Sight2 アプリケーションの通信手段を提供します。試験機器コミュニケーターは 4Sight2 設定フォルダからインストールするか、または 4Sight2 初期デバイス通信を介してダウンロードします。試験機器コミュニケーターが設定ファイルで利用できない場合に、一度 4Sight2 アプリケーションを起動して範囲を策定したら、管理者ユーザーとして 4Sight2 メニューを使って [校正] > [ポータブル] に移動して 4Sight2 ユーザーマニュアルを参照し、ナビゲーションと範囲の策定の参考にしてください。試験機器のドロップダウンメニューの隣にある [更新] ボタンを選択します。試験機器コミュニケーターが作動していない場合、次のメッセージが表示されます。

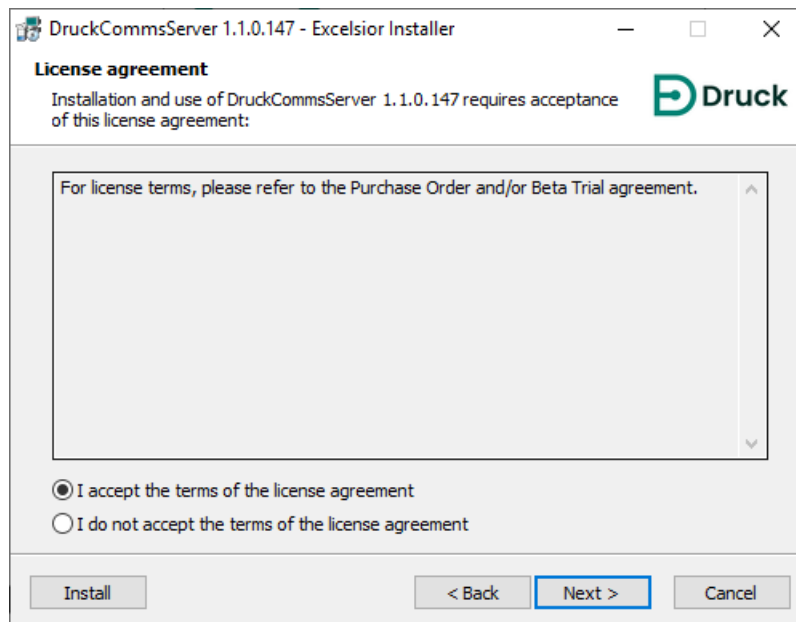
試験機器と通信できません

試験機器コミュニケーターのパッケージをダウンロードしてください。ダウンロード完了後、圧縮ファイルを解凍し、setup.exe ファイルを実行してインストールします。インストール手順またはトラブルシューティングについては「インストールマニュアル」を参照してください。サポートが必要な場合は管理者にお問い合わせください。

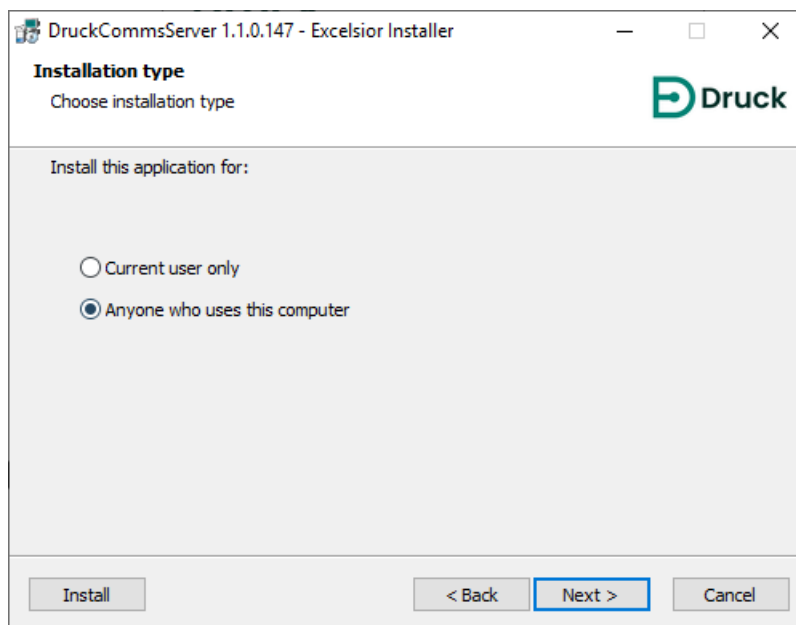
2. [ダウンロード] を選択して試験機器コミュニケーターの設定ファイルを取得します。
3. 試験機器コミュニケーターの設定ファイルは、CommsServerInstall Zip ファイルとして表示されます。CommsServerInstall Zip をダウンロードしたら、4Sight2 のインストールの前後で同じ手順を行います。
4. CommsServerInstall Zip を解凍してファイルを抽出し、setup.exe ファイルをダブルクリックしてインストーラを起動します。
5. DruckCommsServer インストーラが表示されます。インストーラの指示またはこのガイドに従います。



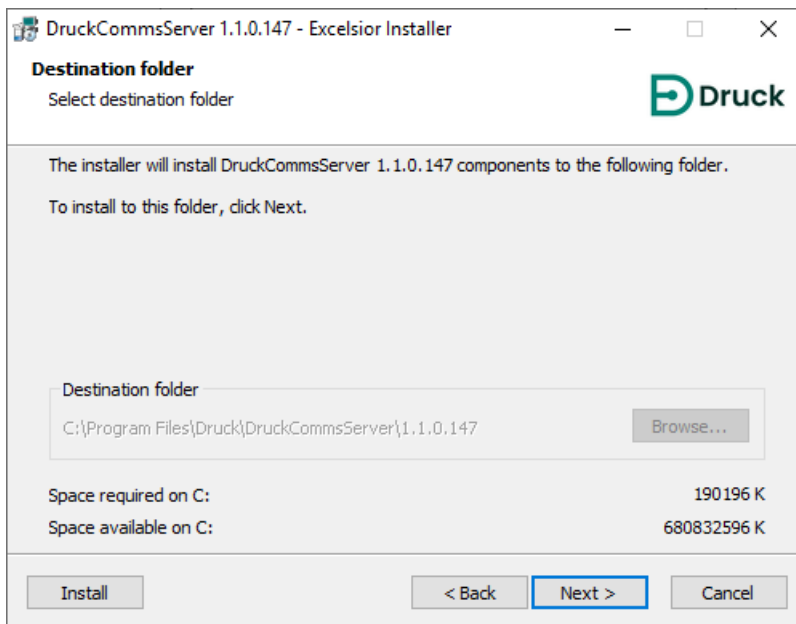
6. [次へ] を選択してライセンス契約画面を表示し、条項を読んで、[ライセンス契約の条件に同意します] を選択し、[次へ] をクリックします。



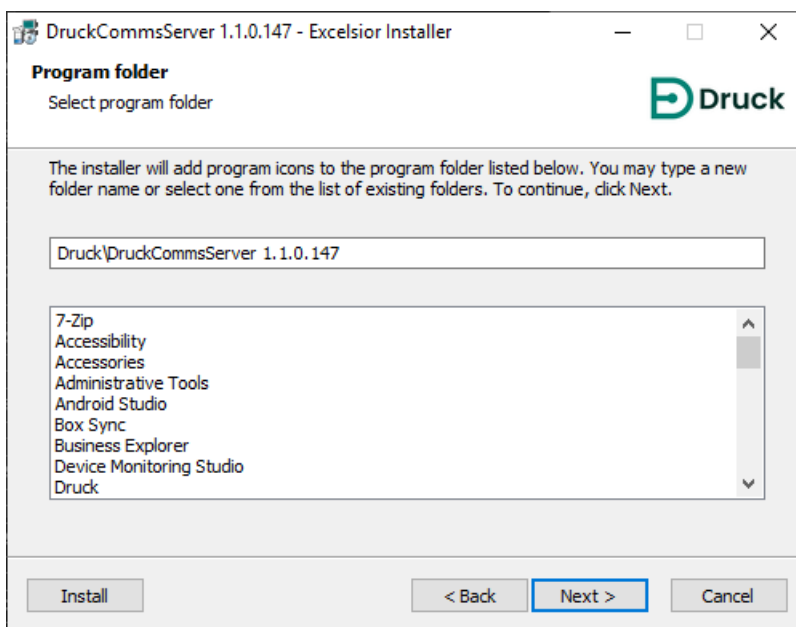
7. インストールタイプ画面で、この PC の全ユーザー用に CommsServer をインストールするのか、または現在のユーザー用のみにするのかを選択します。



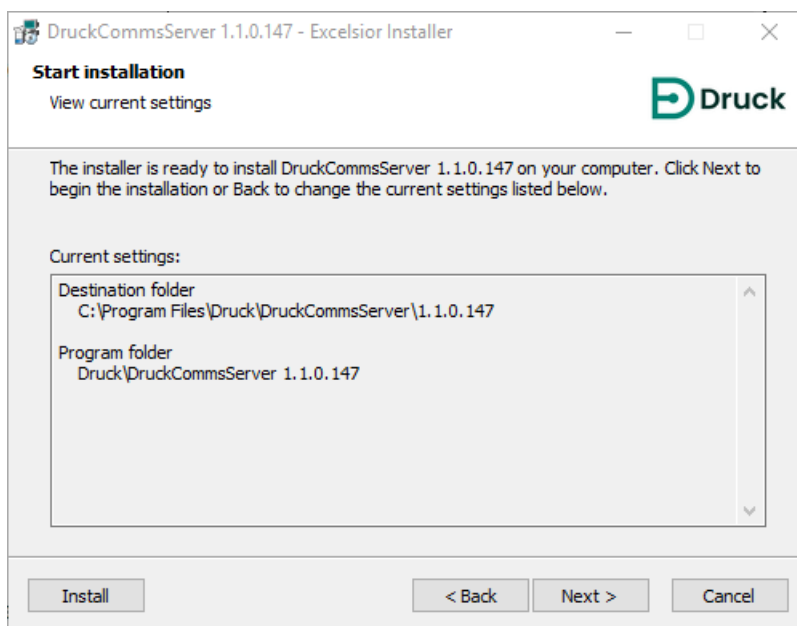
8. インストール先のフォルダ画面に、DruckCommsServer をインストールするフォルダが表示されます。デフォルトではインストール先のフォルダは、C:\Program Files\Druck\DruckCommsServer\[application_version] です。



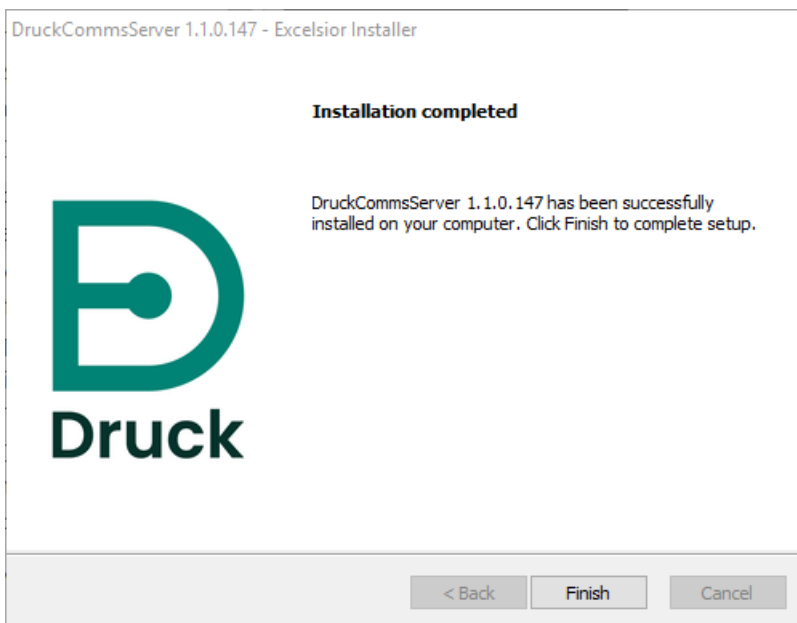
9. プログラムフォルダ画面で、インストーラがプログラムフォルダにプログラムアイコンを追加する場所を選択できます。



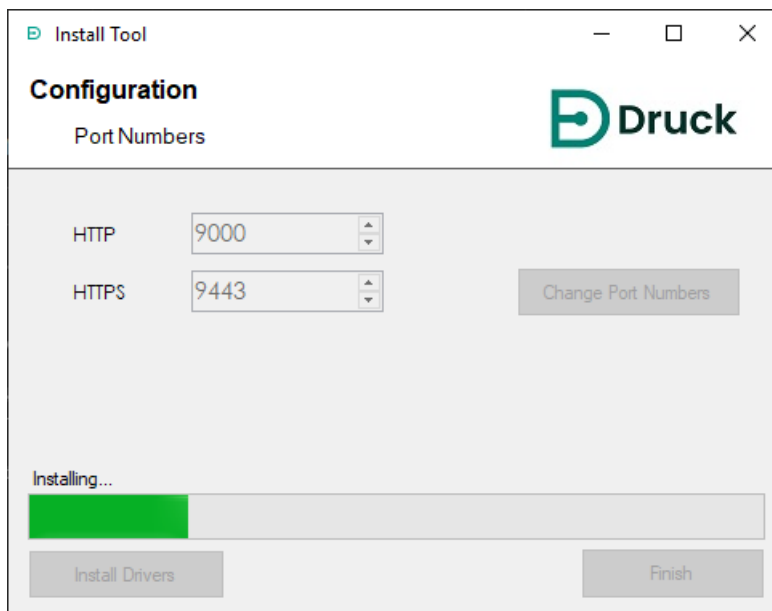
10. 次にインストール開始画面が表示されるので、[次へ] を選択してインストールを開始します。



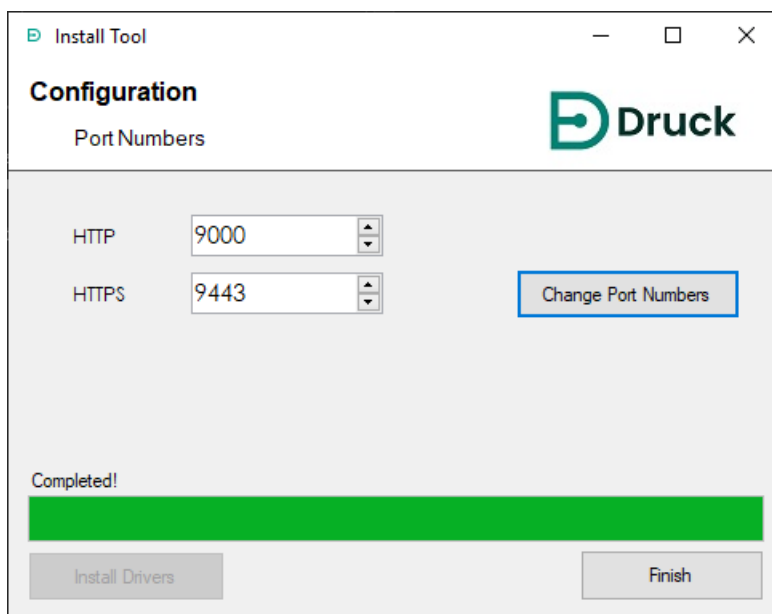
11. インストールが完了したら、[終了] を押します。



12. 次に CommsServer インストールツールアプリケーションが表示され、必要な追加のドライバがインストールされます。

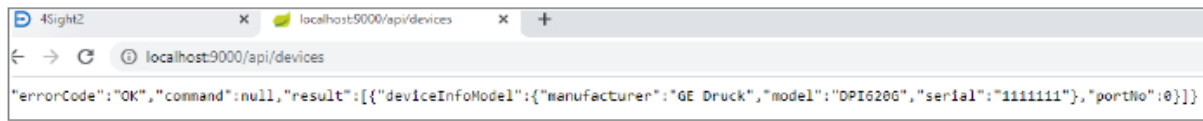


13. 代替のポート番号を 4Sight2 が使用しているか不確かな場合は、管理者ユーザーにお問い合わせください。
注記: インストールツールをインストール後に別に起動して、ポート番号を構成することができます。



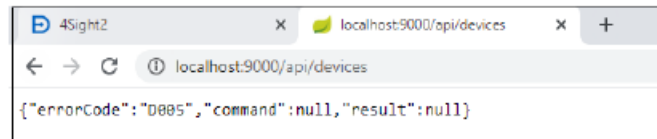
14. 試験機器コミュニケータのインストールのテストは、次の URL をウェブブラウザに入力して行います。
`Http://localhost:[上記の既定が使用される http ポート番号 9000]/api/devices`

ウェブブラウザには接続している全デバイスが一覧表示されるはずですが、



```
4Sight2 localhost:9000/api/devices  
localhost:9000/api/devices  
{"errorCode":"OK","command":null,"result":[{"deviceInfoModel":{"manufacturer":"GE Druck","model":"DPI620G","serial":"11111111"},"portNo":0}]}
```

デバイスを接続していない場合は、次の表示がされます。



```
4Sight2 localhost:9000/api/devices  
localhost:9000/api/devices  
{"errorCode":"D005","command":null,"result":null}
```

注記: 温度校正器に必要なドライバは、自動的に構成されません。セクション 4.3 の温度校正器ドライバの構成を参照してください。

15. デバイスドライバのインストールに失敗した場合、次のセクションの手順に従って手作業にて必要なドライバを構成してください。

4.1 手動でのドライバ構成

IT セキュリティ ポリシーの設定により、Druck ドライバがインストール時に自動構成されない場合があります。この意志 4Sight2 がさまざまな機器と通信できない場合は明らかです。

最新情報については <https://www.bakerhughes.com/druck/test-and-calibration-instrumentation/calibration-management-software-4sight2>

また



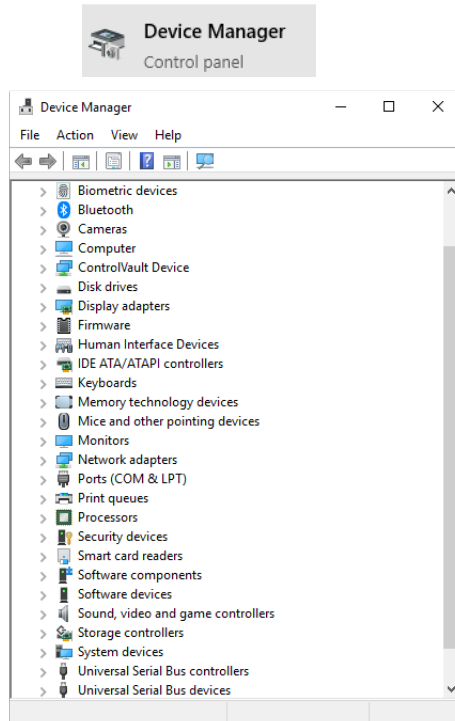
この問題を解決するには、Druck ドライバを手動で構成する必要があります。この問題に不明点がある場合、またはさらに支援が必要な場合は、最寄りの IT 担当者にご相談ください。

4.1.1 前提条件

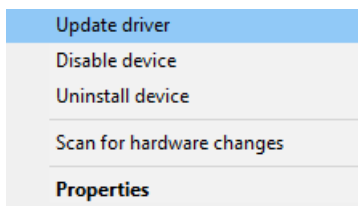
ドライバをインストールするには、4Sight2 アプリケーションを既にインストールしているか、マシンをすぐに利用できる状態である必要があります。ドライバをインストールする前に、お使いのコンピューターから 4Sight2 アプリケーションにログインできることを確認してください。

手動でドライバをインストールする場合は次の手順を実行してください。

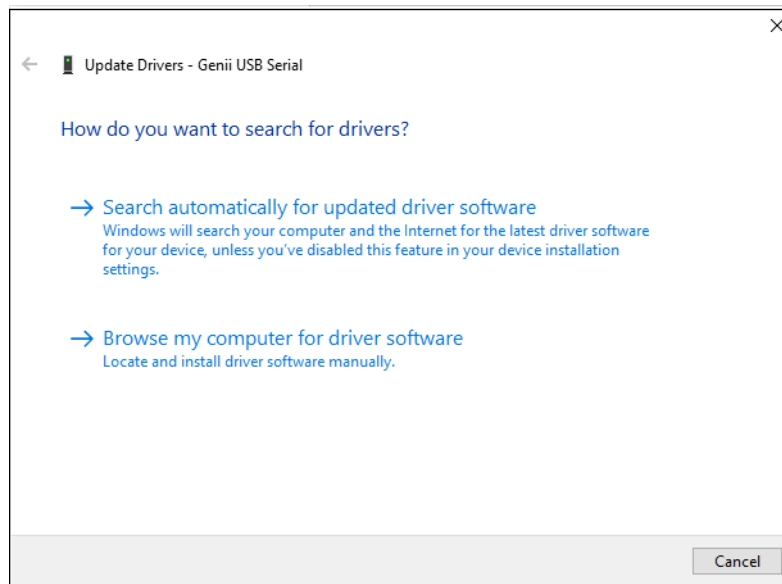
1. デスクトップでデバイスマネージャを検索し、実行します。



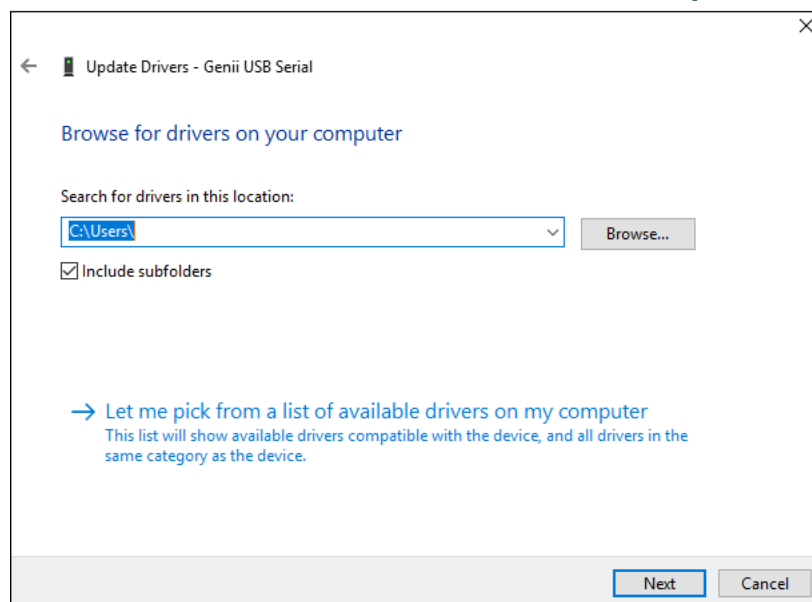
2. USB デバイスの一覧をスクロールして、未設定の装置、すなわち [不明なデバイス] または [その他のデバイス] を探します。右クリックして [ドライバの更新] を選択します。



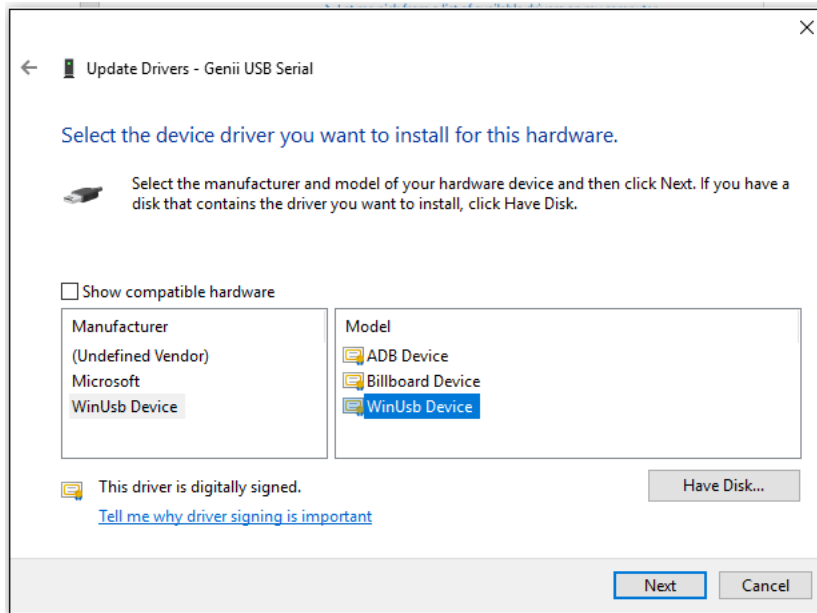
3. [コンピューターを参照してドライバー ソフトウェアを検索] を選択します。



4. PC 上で [コンピューター上の利用可能なドライバーの一覧から選択します] を選択します。



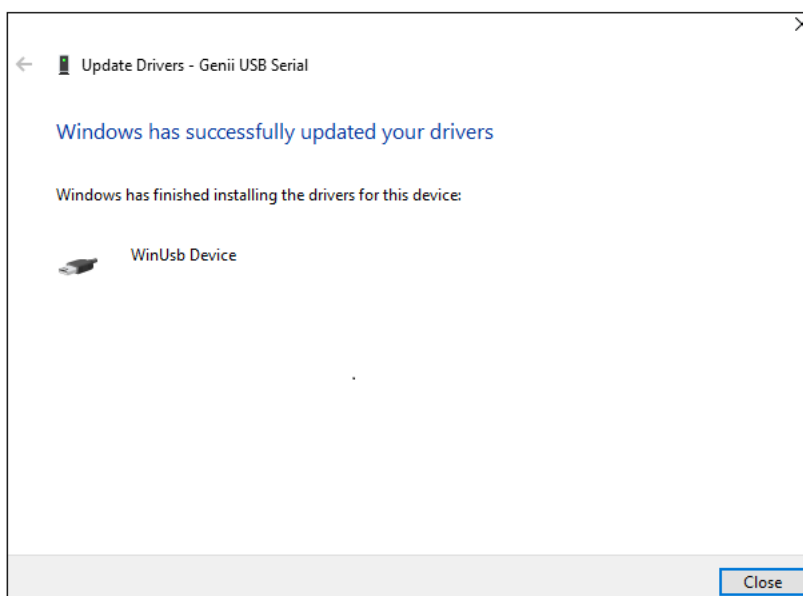
5. [互換性のあるハードウェアを表示] のチェックを外し、メーカー向けの [WinUsb デバイス] およびモデル向けの [WinUsb デバイス] を選択します。



6. 次の警告が表示されます。[はい] をクリックします。



7. 「ドライバーが正常に更新されました」というメッセージが表示されます。



デバイスを初めて接続する場合は、上記の手順をデバイスのカテゴリごとに繰り返します。

例えば最初に PACE と Genii に接続する場合、PACE と Genii それぞれに最初に上記の手順を繰り返す必要があります。それ以降は、PACE と Genii のインスタンスはすべて、この設定を行うことなく動作します。しかし、DPI611/612 などの別のカテゴリのデバイスを後で接続する場合は、対象のカテゴリのデバイスに対してこの手順を繰り返す必要があります。

4.2 試験機器コミュニケーターのテスト

1. 技術者として 4Sight2 にログインします。
2. **[アセット]** >> **[作業リスト]** に移動します。
3. 1つ以上の範囲を選択してポータブル校正または自動校正ワークフローに割り当てます。
4. **[更新]** ボタンをクリックします。

5. **[試験機器]** ドロップダウンをクリックします。一覧に接続されたデバイスが表示されていれば、試験機器コミュニケーターは正しく構成されています。

4.3 温度校正器ドライバ構成

温度校正器と 4Sight2 を通信させるには、FTDI ドライバをインストールする必要があります。

1. このリンクから FTDI ドライバをダウンロードします。 <https://www.ftdichip.com/Drivers/VCP.htm>
2. ダウンロードした zip ファイルを解凍し、ファイルを PC の適切な場所に保存します。
3. PC の Windows デバイスマネージャを開きます。
4. デバイスの一覧からポート (COM と LPT) を選択肢、温度校正器を表示します。
5. 温度校正器を右クリックし、ドライバのアップデートを選択します。
6. [コンピュータでドライバソフトウェアを検索] を選択します。
7. [次の場所でドライバーを検索します] という名前の検索ボックスの隣の [参照] を選択します。
8. ダウンロードしたドライバを格納している解凍したフォルダを選択します。
9. [次へ] を選択して閉じます。
10. これでドライバがインストールされました。
11. 4Sight2 で温度校正器との通信をテストするには、自動校正に移動して温度校正器を入力コントローラとして選択できるかをチェックします。あるいはセクション 4 の手順 14 を再実行します。

展開ガイド

5. 展開ガイド

5.1 展開アーキテクチャ

代表的なアーキテクチャは、4Sight2 Web アプリケーション、Tomcat Web サーバー内で稼働する UAA (User Authentication and Authorization: ユーザー認証と認可) サーバー、および同じマシン上で稼働する PostgreSQL データベースで構成されます。

ブラウザクライアント Web アプリケーションは 4Sight2 サーバーに接続し、このサーバーが PostgreSQL データベースからの情報を保存および取得します。

5.2 物理的展開

4Sight2 をインストールするユーザーが、以下のようにユーザーセキュリティポリシーに適合するサイバーセキュリティ対策を実施していることを前提にします。

- サーバーは、物理的な制限に基づくアクセス制御が行われる安全な場所に設置されている。
- サーバーアクセス制御は、制限付きの認可アクセスによって保護されている。
- サーバーネットワークは、ファイアウォールによって保護されており、既知のポート上のみで周知のアプリケーションへの限定的なアクセスが許可される。
- アプリケーションは、その固有のコンテキストで実行され、それぞれの固有フォルダ内のデータベースおよびファイルシステムのみへのアクセス権が与えられる。

5.3 ネットワーク

クライアントは、Ethernet 接続またはワイヤレスネットワーク経由で、Web ブラウザを使用して接続されます。ワイヤレスネットワーク上では、無線帯域幅と接続された装置数によっては、遅延が生じる可能性があります。

ブラウザのプラグインおよびブラウザにインストールされた拡張をすべて無効化または削除することが推奨されます。

4Sight2 ウェブサーバーをインターネットにさらす (公開する) べきではありません。イントラネットまたは VPN を介してアクセスしてください。

5.4 展開シーケンス

PostgreSQL、Tomcat、Java Runtime は、4Sight2 アプリケーションの前提条件です。PostgreSQL は独立したパッケージとしてインストールされ、その他は本アプリケーションと一緒にインストールされます。そのため、PostgreSQL がすでにユーザーマシンにインストールされている場合は、PostgreSQL に接続して構成するためのスーパーユーザーパスワードのみが必要になります。

インストールには、そのマシン上の Windows 管理者権限が必要です。インストールの前に、ユーザーは PostgreSQL スーパーユーザーパスワードを取得しておく必要があります。アプリケーション管理者のユーザー名とパスワード、およびデータベースユーザー名とパスワードです。

PostgreSQL スーパーユーザーパスワードは、PostgreSQL サーバー内のデータベースおよびその他の構造の作成に必須です。アプリケーション管理者はアプリケーションの最初のユーザーです。アプリケーション管理者は他のユーザーの作成と、それらのユーザーへ異なる役割を割り当てる責任を負います。データベースユーザーには 4Sight2 および UAA データベースへのアクセス権が付与されます。ユーザー名の認証情報はデータベースのアクセスに使用されます。

このアプリケーションはマシンポート上で公開されます。デフォルトポートは 8083 です。ユーザーはインストール時またはそれ以降にこのポートを変更できます。Tomcat でのデフォルトのアプリケーションコンテキストは 4Sight2 です。



オペレーティングシステムをハードニングするには、Microsoft または CIS ガイドラインによる OS のハードニング手順に従ってください。このインストール手順では、4Sight2 サーバーをインストールする前に PostgreSQL をインストールするように促されます。

試験機器コミュニケーターは、試験機器が USB ポート経由で接続された時に、クライアントのマシンにインストールされます。まだ試験機器コミュニケーターがマシン上にインストールされていない場合、ユーザーは試験機器コミュニケーターを 4Sight2 サーバーからダウンロードしてマシンにインストールするように求められます。試験機器コミュニケーターはポート 9000 をリスニングします。またセキュアレイヤ上でのみ通信できます。

5.5 展開後のタスク

5.5.1 ユーザーおよびグループの追加

管理者は、アプリケーションにおける各種ユーザー（スーパーバイザー、シニア技術者、技術者、監査者など）の作成を担います。管理者は組み込み済みの各種デフォルトグループにこれらのユーザーを割り当てられます。アクセスの制御強化またはさらに詳細なアクセス制御が必要な場合、管理者はカスタムグループを作成し、特定のアクセス権をそれらのグループに割り当てることができます。

5.5.2 デフォルトパスワード

“C:\Program Files\Druck\4Sight2\<<latest folder number>>\apache-tomcat\conf\tomcat-user.xml” ファイルではハードコードされた Tomcat ユーザー用のデフォルトパスワードを使用しています。

デフォルトパスワードを変更し、パスワードのベストプラクティスに準拠したパスワードを常に使用することが推奨されます。

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

このアプリケーションのセキュリティを確保するためのベストプラクティスがすでに実践されています。さらなるセキュリティを達成するには、以下のタスクを実行してください。

構成ファイルおよびフォルダは、デフォルトでアクセス権を持つサービスおよびシステムのみで保護されています。したがって、以下のタスクの実行を試みる前は C:\Program Files\Druck\4Sight2\<<latest folder number>>\apache-tomcat\conf フォルダの読み取り/書き込みアクセス権を持つのは管理者ユーザーのみです。そのため、管理者ユーザーの認証情報でコマンドプロンプトを開く必要があります。

5.5.3 セキュアな通信

この節では、自己署名証明書を用い、セキュアモード (SSL モード) で 4sight2 の設定をする手順を解説します。あらかじめ、4Sight2 アプリケーションに規定されている前提条件と契約条件をお読みください。自己署名証明書は 4Sight2 で SSL を有効化する手段のひとつです。別の方法として、サードパーティの CA 証明書を購入することも可能です。Symantec、Digicert など、さまざまなベンダから購入できます。

注記: SSL を有効にしさえすればアプリケーションがセキュアになるわけではありません。安全なウェブアプリケーションの構築にはさまざまな作業が必要であり、SSL はそのひとつに過ぎないのです。

5.5.3.1 前提条件と警告

以下の指示に従って操作するには、次の前提条件を満たしている必要があります。



OpenSSL (Windows 版) ソフトウェアが、自己署名証明書を生成するために必要です。社内規約、法令、規制などにより、OpenSSL の使用が認められていることが前提となります。

- keytool はキーと証明書の管理ユーティリティであり、Java に付属しています。https の設定に必要な、さまざまなコンポーネントを生成するために使用します。社内規約、法令、規制などに従い、keytool ユーティリティの使用が認められていることが前提となります。
- 以下の設定を進めるには管理者権限が必要です。管理者権限の付与に関しては、IT 部門にお問い合わせください。
- 手順に沿って作業を進めるには、コンピュータの処理に関する基本的な知識が必要です。IT 技術者に委ねるか、または IT 技術者の指導のもとで実施するようお勧めします。
- この資料で使っているホスト名、パスワード、URL、フォルダパスなどは、例として示しているものです。実際の環境に合わせ、コマンドを修正した上で実行してください。
- 以下、2 つのシナリオについて説明します。サーバーとクライアントが同じマシン上で稼働するシナリオと、異なるマシン上で稼働する (複数のクライアントがある) シナリオです。

5.5.3.2 4Sight2 アプリケーションが https で動作するよう設定する手順

1. Windows Services から 4Sight2 を停止してください。
2. コマンドプロンプトを**管理者モード**で開きます。
3. 4Sight2 のインストール先ディレクトリ以下、次に示すフォルダに移動します。次のコマンドを実行してください。

```
cd "C:\Program Files\Druck\4Sight2\<<latest folder number>>\apache-tomcat\conf"
```

4. keytool があることを確認します。コマンドプロンプトで、次のコマンドを実行してください。**Keytool -?** 見つからない場合は、4Sight2 のインストール先ディレクトリ以下、JRE の bin を指すよう、環境変数 Path を設定します。次のように実行してください。ただし具体的なパスは、インストール先に合わせて修正する必要があります。

```
C:\Program Files\Druck\4Sight2\<<latest folder number>>\jre\bin
```

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

5. 証明書を新規に生成する場合は手順 6 に進みます。既に証明書がある場合は、次のように実行してください。

a. 証明書ファイル 4Sight.jks が java キーストアにあることを確認します。

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

b. 証明書がインストール済みであれば削除します。

```
keytool -delete -noprompt -alias <<hostname>> -storepass <<KeyPassword>> -keystore 4Sight.jks
```

c. 4SightV2PublicKey.cer の有無を確認し、あれば削除します。

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

d. 証明書がすでに java の cacert に存在するかどうかを確認します。

```
keytool -list -alias <<hostname>> -storepass changeit -keystore "../jre/lib/security/cacerts"
```

e. 証明書が java ストアにあれば削除します。

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

6. 証明書を新規に生成します。次のように実行してください。

```
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. 証明書を 4SightV2PublicKey.cer にエクスポートします (ファイル名やパスを変更しないでください)。

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

正常に実行されると、「Certificate stored in file

C:\Program Files\Druck\4Sight2\<<latest folder

number>>\app\Certificate\4SightV2PublicKey.cer」というメッセージが表示されます。

8. 証明書を java CACert ファイルにインポートします。

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

正常に実行されると「Certificate was added to keystore」というメッセージが表示されます。

9. Tomcat 構成ファイルに証明書のエントリを作成します。

a. 次の場所にある、server.xml というファイルを開いてください。

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

b. server.xml に以下のエントリを作成します。

```
<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. 以下のセクションをコメントアウトして http 接続を無効化します。

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

注記: この部分をコメントアウトしないとアプリケーションは動作しません。

10. 以上で 4Sight2 アプリケーションが https で動作するよう設定する作業が終わりました。

11. 正しく設定できたかテストしたい場合は、Windows Services から 4Sight2 を再起動してください。

12. google chrome を起動し、キャッシュをクリアした後、起動し直します。

13. 次の URL にアクセスしてください: https://<<host-name>>:8443/4sight2

- 初回は読み込みに多少時間がかかるかもしれません。
- 「Your connection is not private」と表示された画面が現れます。
- [詳細設定] ボタンを押し、「>>XXに進む」というリンクをクリックしてください。
- 4sight2 の画面が表示されない場合は [再読み込み] ボタンを押してみてください。

- 4sight2 のページにリダイレクトされます。
- アドレスバーに、エラーを表す「Not Secure」という文字列が現れます。MMC で証明書を登録すれば、この表示はなくなります。



5.5.3.3 DruckCommsServer が https で動作するよう設定する手順 (サーバー機にインストールした場合)

コマンドを実行する前に、<< >> の値を適切なデータに置き換えます。

1. Windows Services から DruckCommsServer を停止してください。
2. コマンドプロンプトを**管理者モード**で開きます。
3. keytool があることを確認します。コマンドプロンプトで、次のコマンドを実行してください。**Keytool -?**
見つからない場合は、4Sight2 のインストール先ディレクトリ以下、JRE の bin を指すよう、環境変数 Path を設定します。次のように実行してください。
ただし具体的なパスは、インストール先に合わせて修正する必要があります。
C:\Program Files\Druck\4Sight2\<<latest folder number>>\jre\bin
Set "Path=%Path%;C:\Program Files\Druck\4Sight2\<<latest folder number>>\jre\bin"
4. DruckCommServer のインストール先ディレクトリ以下、次に示すフォルダに移動します。次のコマンドを実行してください。
cd "C:\Program Files\Druck\DruckCommsServer\<< Communication Service version >>"
5. 証明書が既にある場合は削除します。次の手順で操作してください。
 - a. 証明書がすでに java の cacert に存在するかどうかを確認します。
keytool -list -alias tomcat -storepass changeit -keystore cacerts
 - b. 証明書が java ストアにあれば削除します。
keytool -delete -noprompt -alias tomcat -storepass changeit -keystore cacerts
 - c. 設定済みの証明書 (CommsServer に付属していたもの) を削除します。
del 4Sight.jks
del 4SightV2DeviceMngr.pfx
6. 証明書を新規に生成します。次のように実行してください。
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. 証明書をファイル DruckCommServer.cer にエクスポートします。
keytool -export -alias tomcat -keystore CommServer.jks -storepass <<StorePassword>> -storetype JKS -file DruckCommServer.cer
正常に実行されると、
「Certificate stored in file DruckCommServer.cer」というメッセージが表示されます。
8. CommServer の証明書を java CACert ファイルにインポートします。
keytool -import -noprompt -trustcacerts -alias tomcat -storepass changeit -keystore cacerts -file DruckCommServer.cer

正常に実行されると「Certificate was added to keystore」というメッセージが表示されます。

9. 4Sight の証明書を java CACert ファイルにインポートします。

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

正常に実行されると「Certificate was added to keystore」というメッセージが表示されます。

10. DruckCommsServer 以下にある application.properties の、key-store.password を編集します。

ファイル

C:\Program Files\Druck\DruckCommsServer\<<Communication Service Version>>\application.properties を開き、次の行を書き換えます。

```
keystore = CommServer.jks
```

```
key-store.password= << StorePassword >>
```

注記: << StorePassword >> は、手順 6 で指定した、StorePassword に当たる文字列になります。

11. 4Sight2 および DruckCommsServer サービスを再起動します。

5.5.3.4 DruckCommsServer が https で動作するよう設定する手順 (クライアント機にインストールした場合)

1. keytool ユーティリティは Java に付属しています。Java をインストールしても、インストールせずに直接、java keytool があるかどうか確かめても構いません。
2. Windows Services から DruckCommsServer を停止してください。
3. コマンドプロンプトを**管理者モード**で開きます。
4. keytool があることを確認します。コマンドプロンプトで、次のコマンドを実行してください。**Keytool -?** 見つからない場合は、環境変数 Path を適切に設定します。JRE の bin を指すように設定する (java をインストールした場合) か、または次のように、keytool を指すように設定してください。ただし具体的なパスは、インストール先に合わせて修正する必要があります。

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

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

5. **4SightV2PublicKey.cer** ファイルを、4Sight アプリケーションのインストール先サーバー機から取得してください。次の場所にあるはずですが。

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

6. この **4SightV2PublicKey.cer** を次の場所にコピーしてください。

```
C:\Program Files\Druck\DruckCommsServer\<< Communication Service version >>
```

7. 5.5.3.3 節の手順 4 ~ 8 を実行してください。

8. 4Sight の証明書を java CACert ファイルにインポートします。

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

正常に実行されると「Certificate was added to keystore」というメッセージが表示されます。

9. 5.5.3.3 節の手順 10 ~ 11 を実行してください。

5.5.3.5 4Sight2 で使用する自己署名証明書を生成する手順

1. OpenSSL (Windows 版) をダウンロード、インストールしておきます。
2. Windows Services から 4Sight2 サービスを停止してください。
3. **4Sight2Certificate** というフォルダを C ドライブ内に作成します。
管理者としてアクセスできれば、どのような場所でもフォルダ名でも構いません。
4. 上記のフォルダ内に「メモ帳」で新規ファイルを作成し、**openssl-ca.cnf** という名前で保存します。
ファイルには以下に示す内容を、この資料からコピーすることにより入力してください。

```
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 certificate
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
```

注記: 上記の会社名を更新し、ファイルを保存します。これは、証明書の発行者名です。

管理コンソールに表示されます。

- 上記のフォルダ内に「メモ帳」で新規ファイルを作成し、**openssl-server.cnf** という名前で保存します。ファイルには以下に示す内容を、この資料からコピーすることにより入力してください。

```
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
```

注記: [Hostname of server] および [IP Address of server] の部分には、実際のホスト名と IPv4 アドレスを入れてください。

6. コマンドプロンプトを管理者権限で開きます。

7. 4Sight2Certificate フォルダに移動します。次のように実行してください。

```
cd "<<full path to 4Sight2Certificate >>"
```

8. OpenSSL の bin フォルダを環境変数 Path に設定します。次のように実行してください。

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

具体的なパス (デフォルト値) を指定して実行する例:

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

9. JRE の bin フォルダを環境変数 Path に設定します。次のように実行してください。注記: 以下に示すパスの例は、実際とは違っているかもしれません。

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

10. 次のコマンドで、cacert.pem および cakey.pem というファイルを生成します。

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

証明書のデータ (国、州など) を入力するよう求められるので、正しく入力してください。

11. 次のコマンドで、servercert.csr および serverkey.pem というファイルを生成します。

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

証明書のデータ (国、州など) を入力するよう求められるので、正しく入力してください。

12. 「メモ帳」で新規ファイルを作成し、index.txt という名前で、4Sight2Certificate フォルダ以下に保存してください。

13. 「メモ帳」で新規ファイルを作成し、serial.txt という名前で、4Sight2Certificate フォルダ以下に保存してください。

ファイルを開いて「01」と入力し、保存して閉じます。

14. ファイル servercert.pem および serverkey.pem に証明書を生成します。次のコマンドを実行してください。

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

変更を承認するため「Y」と入力すると、生成処理が始まります。正常に終了するとデータベースが更新されます。

15. 既存のキーファイルを PFX 形式にパッケージ化します。次のコマンドを実行してください。

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

パスワードを 2 回入力するよう求められます。

16. PFX ストアを、先ほど指定した JRE bin の場所に応じて分類した、Java キーストアに変換します (例: tomcat の設定フォルダパス)。

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

注記: どちらのストアにも同じパスワードを使ってください。上記のように、tomcat の設定フォルダ内にある、4Sight.jks というファイルを指定する必要があります。

変換先および変換元キーストアのパスワードを入力するよう求められます。正常に終了すると、「Import command completed: 1 entries successfully imported」というメッセージが表示されます。

17. 証明書を、java キーストアから次のファイルにエクスポートします。

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

注記: 上記のように、tomcat の設定フォルダ内にある、4Sight.jks というファイルを指定する必要があります。

正常に終了すると、「Certificate stored in file」というメッセージが表示されます。

18. 証明書ファイルを、4sight2 のインストール先ディレクトリ以下、cacerts フォルダ内にインポートします。

注記: 具体的なパスは、インストール先ディレクトリや 4sight2 のバージョンに応じて変わります。

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

注記: 何らかの理由で、作成しようとするエイリアスが既に存在する場合は、次のコマンドで削除した後、上記のコマンドで改めて作成してください。

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

正常に終了すると、「Certificate was added to keystore」というメッセージが表示されます。

19. server.xml ファイル (C:\Program Files\Druck\4Sight2\<<latest folder number>>\apache-tomcat\conf 以下) を次のように変更します。

a. server.xml に以下のエントリを作成します。

```
<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. 以下のセクションをコメントアウトして http 接続を無効化します。

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

20. これで 4Sight2 が https で動作するよう設定する作業が終わりました。Windows Services から 4Sight2 サービスを起動してください。

5.5.3.6 DruckCommsServer で用いる自己署名証明書の設定手順 (サーバー機にインストールした場合)

ここでは、4sight2 アプリケーションが https で動作するよう変換済みで (5.5.3.5 節を参照)、次のファイルが **4Sight2Certificate** フォルダ内にあるものと想定します。

- openssl-server.cnf
 - openssl-ca.cnf
 - cacert.pem
 - cakey.pem
 - index.txt
 - serial.txt
 - 4SightV2PublicKey.cer (C:\Program Files\Druck\4Sight2\<<latest folder number>>\app\Certificate フォルダ以下にある可能性もあり)
1. **CommserverCertificate** という名前で新しいフォルダを作成し、上記のファイルをコピーして次のように編集します。

req セクションで **default_keyfile** の値を「**DruckCommServerCertKey.pem**」に変更します。

- **server_distinguished_name** で **commonName** の値を「**localhost**」に変更します。
 - **alternate_names** で **DNS.1** の値を「**localhost**」に変更します。
 - **alternate_names** で **IP.1** の値を「**127.0.0.1**」に変更します。
 - ファイルを保存します。
- openssl-ca.cnf。(内容は一切変更しないでください)
 - cacert.pem。(内容は一切変更しないでください)
 - index.txt (内容をすべて削除し、空のファイルにします)
 - serial.txt (内容をすべて削除し、エントリが 01 のみになるようにします)
2. Windows Services から DruckCommsServer サービスを停止します。
 3. コマンドプロンプトを管理者権限で開きます。
 4. **CommserverCertificate** フォルダに移動します。次のように実行してください。
cd "<<full path to CommserverCertificate >>"
 5. OpenSSL の bin フォルダを環境変数 Path に設定します。次のように実行してください。

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

具体的なパス (デフォルト値) を指定して実行する例:

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

6. JRE の bin フォルダを環境変数 Path に設定します。次のように実行してください。注記: 以下に示すパスの例は、実際とは違っているかもしれません。

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

7. この操作の完了後、以下のコマンドを使用して、Comm Server 証明書リクエストを作成します。

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

このコマンドを実行すると、リクエストが **DruckCommServer.csr** に作成され、秘密キーが **DruckCommServerCertKey.pem** に作成されます。

8. 次のようにして、csr リクエストに自分の ca で署名します。

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

9. この後、以下のコマンドで Comm Server 用のエイリアス **tomcat** で PFX ファイルを作成します。

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

10. keytool を使って、PFX ストアを Java キーストアに変換します。

注記: 両方のキーストアに対して同じパスワードを維持してください。

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

11. 証明書を cacert にインポートします。

a. インストールの時点で付属していた tomcat エイリアスを削除してください。

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

b. その後、証明書を cacerts にインポートします。次のように実行してください。

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

12. 4sight 公開キーを Comm Server の cacert にインポートして、通信の認証に使えるようにします。次のコマンドを実行してください。

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

13. 以上の処理が終わると、**DruckCommServer.pfx** および **CommServer.jks** というファイルが、**CommserverCertificate** フォルダ以下にできます。

このファイルを **"C:\Program Files\Druck\DruckCommsServer\<< Communication Service version >>\"** ディレクトリ以下にコピーしてください。同じ場所にある **application.properties** を編集し、プロパティ値を次のように変更します。

a. Keystore = CommServer.jks

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

c. key-store.type=JKS

5.5.3.6.1 証明書を Windows にインストール (4sight および DruckCommsServer で使用)

1. 「Run」画面を開いて「mmc」と入力し、Enter キーを押します。
2. [ファイル] メニューから [スナップインの追加/削除] を実行します。
3. 左側のメニューから証明書を選択します。[追加] を押し、[コンピュータアカウント]、[次へ]、[終了] の順に選択した後、[OK] をクリックします。
4. 「証明書 (ローカルコンピュータ)」セクションを展開します。次に「信頼されるルート認証局」を展開します。
[証明書フォルダ] を右クリックし、[すべてのタスク]、[インポート] の順に選択します。
「cacert.pem」を選択し、[次へ]、[終了] の順に押します。
カスタム CA 証明書が、「trusted authority」以下にインストールされます。

以上がすべて終了したら、DruckCommsServer サービスを起動します。

5.5.3.7 DruckCommsServer で使用する自己署名証明書の設定手順 (クライアント機にインストールした場合)

DruckCommsServer が https で動作するように変換するには、java keytool と OpenSSL ユーティリティが必要です。

1. keytool ユーティリティは Java に付属しています。Java をインストールしても、インストールせずに直接、java keytool があるかどうか確かめても構いません。
2. OpenSSL (Windows 版) をダウンロード、インストールしておきます。
3. OpenSSL の bin フォルダを環境変数 Path に設定します。次のように実行してください。
Set path=%path%;"<<bin folder of openssl>>"
具体的なパス (デフォルト値) を指定して実行する例:
Set Path=%Path%; "C:\Program Files\OpenSSL-Win64\bin"
4. JRE の bin フォルダを環境変数 Path に設定します。次のように実行してください。
C:\Program Files\Java\<< Java version >>\bin
Set Path=%Path%; "C:\Program Files\Java\<< Java version >>\bin"
5. Windows Services から DruckCommsServer サービスを停止します。
6. **CommserverCertificate** というフォルダを、C ドライブ内 (それ以外の適当なドライブでも可) に作成します。
7. 4sight2 公開証明書ファイル **4SightV2PublicKey.cer** をサーバー機の C:\Program Files\Druck\4Sight2\<<latest folder number>>\app\Certificate ディレクトリ以下から取得し、**CommserverCertificate** フォルダ以下にコピーしてください。
8. **openssl-server.cnf** および **openssl-ca.cnf** というファイルを作成します (5.5.3.5 節の手順 4 ~ 5)。次に、index.txt および serial.txt というファイルを、**CommserverCertificate** フォルダ以下に作成してください (手順 12 ~ 13)。
9. この時点で、CommServerCertificate フォルダ以下には次の 5 つのファイルがあるはずで
 - a. openssl-server.cnf
 - b. openssl-ca.cnf
 - c. index.txt

- d. serial.txt
- e. 4SightV2PublicKey.cer

10. コマンドプロンプトを管理者権限で開きます。
CommserverCertificate フォルダに移動します。次のように実行してください。
cd "<<full path to CommserverCertificate >>"
11. 次のコマンドで、cacert.pem および cakey.pem というファイルを生成します。
openssl req -x509 -config openssl-ca.cnf -newkey rsa:4096 -sha256 -nodes -out cacert.pem -outform PEM
証明書のデータ (国、州など) を入力するよう求められるので、正しく入力してください。
12. **CommserverCertificate** フォルダ内のファイルの内容を変更します。5.5.3.6 節の手順 1 を実行してください。
13. 次に、5.5.3.6 節の手順 7 ~ 11 を実行します。
14. 4sight 公開キーを Comm Server の cacert にインポートして、通信の認証に使えるようにします。次のコマンドを実行してください。
keytool -import -noprompt -trustcacerts -alias <<4sight server hostname>> -storepass changeit -keystore "C:\Program Files\Druck\DruckCommsServer\<< Communication Service version >>\cacerts" -file 4SightV2PublicKey.cer
15. 以上の処理が終わると、**DruckCommServer.pfx** および **CommServer.jks** というファイルが **CommserverCertificate** フォルダ以下にできます。
このファイルを "**C:\Program Files\Druck\DruckCommsServer\<< Communication Service version >>**" ディレクトリ以下にコピーしてください。同じ場所にある **application.properties** を編集し、プロパティ値を次のように変更します。
 - a. **Keystore = CommServer.jks**
 - b. **key-store.password = <<KeystorePassword>>**
 - c. **key-store.type=JKS**

5.5.3.7.1 証明書を Windows にインストール (DruckCommsServer で使用)

1. 「Run」画面を開いて「mmc」と入力し、Enter キーを押します。
2. [ファイル] メニューから [スナップインの追加/削除] を実行します。
3. 左側のメニューから証明書を選択します。[追加] を押し、[コンピュータアカウント]、[次へ]、[終了] の順に選択した後、[OK] をクリックします。
4. 「証明書 (ローカルコンピュータ)」セクションを展開します。次に「信頼されるルート認証局」を展開します。
[証明書フォルダ] を右クリックし、[すべてのタスク]、[インポート] の順に選択します。
「cacert.pem」を選択し、[次へ]、[終了] の順に押します。
カスタム CA 証明書が、「trusted authority」以下にインストールされます。

以上がすべて終了したら、DruckCommsServer サービスを起動します。

DruckCommsServer が https で動作するように変換できたか確認したいだけであれば、google chrome タブで、次のリンク先を開いてみてください。**<https://localhost:9443/api/devicemanager/version>** (Comm Server のポート番号をデフォルトの 9443 以外に変更していた場合は、正しい番号に置き換えます)

5.5.3.8 4Sight2 の証明書の検証

1. サーバー PC を再起動します。

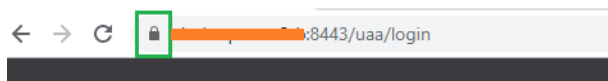
2. Windows Services から、4Sight2 および DruckCommsServer サービスを再起動してください。
3. google chrome を起動し、キャッシュをクリアした後、起動し直します。ほかに google chrome のインスタンスが動作していないか確認します。
4. アドレスバーに次の URL を入力し、Enter キーを押します。

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

注記: この URL にはホスト名を使う必要があります。

5. ログイン画面が開き、正しい HTTPS URL が表示されるはずですが。

注記: アドレスバーの赤いエラー表示が消えます。この表示が消えない (リンクがセキュアでないままである) 場合は、コンピュータを再起動し、手順 3 に戻ってください。



4Sight2 のインストールに関する FAQ

6. 4Sight2 のインストールに関する FAQ

6.1 設定とインストール

質問 1: 世界中のさまざまな地域にまたがるマルチサイト組織があります。4Sight2 を設定する最良の方法を教えてください。

回答: これらのサイトをどのように管理運営するかによります。すべてのサイトが中央の IT ハブから管理運営される場合は、単一の 4Sight2 ライセンスを中央にインストールする方法があります。すべてのサイトがネットワークまたは LAN 経由で 4Sight2 にアクセスできます。一方、自己運営および管理されている独立事業体としての子ビジネスがある場合は、複数の 4Sight2 ライセンスを購入することができます。

質問 2: 複数の 4Sight2 ライセンスを購入した場合、それらの間でやり取りはありますか？

回答: いいえ。4Sight2 の各ライセンスは分離された個別のソフトウェアであり、それぞれが固有のアプリケーションインストールとデータベースを備えています。個別のインストール間でのやり取りはありません。詳細および特別な要件のご相談については、4Sight2 チームにお問い合わせください。

質問 3: 4Sight2 のダウンロード方法を教えてください。

回答: 4Sight2 は 当社の Web サイトから簡単にダウンロードできます。以下のリンクを使用してください。

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

または

営業所に電話して発注することもできます。後日、USB メモリでデモバージョンが届けられます。

質問 4: Windows 以外のオペレーティングシステムに 4Sight2 をインストールできますか？

回答: いいえ。4Sight2 は Windows プラットフォームのみでサポートされます。

質問 5: 4Sight2 のダウンロードおよびインストールが完了しました。どうすれば 4Sight2 にアクセスできますか？

回答: 4Sight2 は Web ベースのソフトウェアです。そのため、4Sight2 のインストール時にデスクトップやコンピュータにアイコンは生成されません。4Sight2 にアクセスするには、

- Google Chrome を開き、以下の URL をアドレスバーに貼り付けて Enter キーを押してください。
- 4Sight2 が同じコンピュータにインストールされている場合は、
`http://localhost:<application_port_number>/4sight2` を使用してください。4Sight2 が同じネットワーク内の別のコンピュータにインストールされている場合は、
`http://<コンピュータ名または IP アドレス>:<application_port_number>/4sight2` を使用してください。
- 今後の参照用に、Google Chrome でブックマークを作成します。

質問 6: 4Sight2 インストーラが Postgres データベースファイルを見つけることができません

回答: インストーラがローカルの場所に解凍され、実行可能ファイルが Disk 1 フォルダから実行されていることを確認します。インストーラが解凍されたローカルの場所に長いパス名がないことを確認します。長いパス名があると、インストーラの前提条件ファイルが見つからない場合もあります。

質問 7: アップグレード中の任意の段階でアップグレードプロセスを中止した場合の動作はどうなりますか？

回答: いずれかの段階で、管理者がアップグレードプロセスを中止すると、アプリケーションは 1.4 バージョンにロールバックして起動し、動作します。アップグレードを正しく実行するには、管理者がアップグレードプロセスを再度開始する必要があります。

質問 8: 4Sight2 アプリケーションのインストール中に「有効なポート番号を入力してください。有効なポート番号を把握するにはインストールマニュアルを参照してください」というメッセージを受け取った場合

回答: 以下に、有効なポートの範囲を示します。インストールを続行するには有効なポートを選択してください。

- ポート 0 ~ 1024 は TCP 接続用に予約済み
- 安全でない一連のポートは 2049、3659、4045、6000、6665 ~ 6669、65535

質問 9: Https を指定しても 4Sight2 がシステムで動作しません

回答: 4Sight2 アプリケーションをインストールするコンピュータのドメイン名の構文に従ってください。

<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> ::= 大文字の A から Z および小文字の a から z までの 52 個の

アルファベット文字のいずれか 1 つ

<digit> ::= 0 から 9 までの数字のいずれか 1 つ

注記: ドメイン名には大文字と小文字を使用できます。同じスペルで大文字と小文字が異なる 2 つの名前は同じものとして扱われます。

6.2 試験機器コミュニケーターに関するFAQ

質問 1: インストールマニュアルのすべての手順を実行しましたが、それでもデバイスが一覧に表示されません。

回答: この手順を行っても一覧に試験機器が表示されない場合、4Sight2 ドライバーを再インストールしてください。再インストールするには **[コントロールパネル] >> [プログラムと機能]** に移動し、一覧から DruckCommsServer ソフトウェアをアンインストールします。試験機器コミュニケーターを再度インストールします。

質問 2: **[デバイスが見つかりません]** というエラーメッセージが表示されました。

回答: この問題を解決するには、

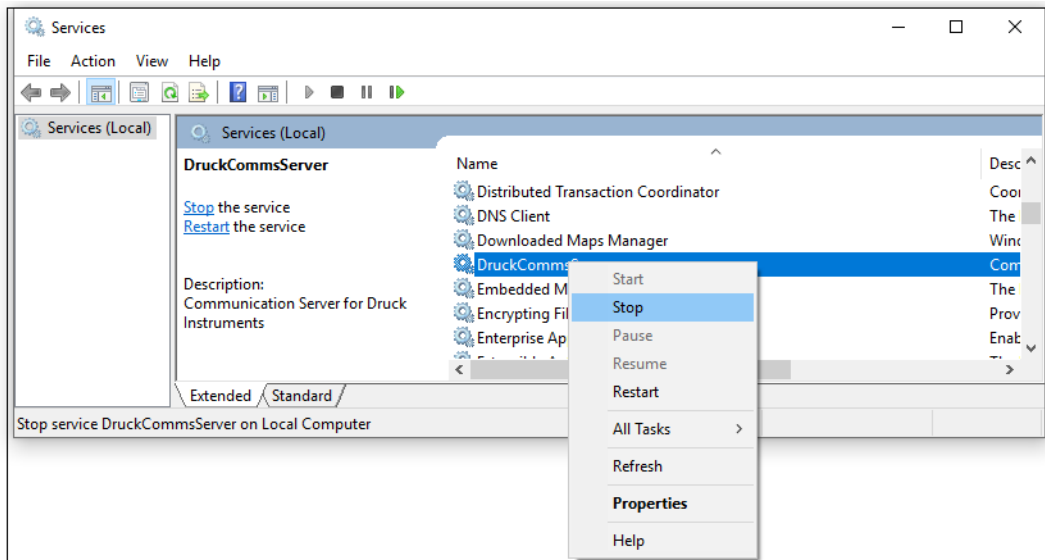
- デバイスが USB ケーブルを使用して、物理的に正しく接続されていることを確認してください。この確認を行うには、デバイスマネージャに移動して一覧でデバイスを探します。その際、デバイスが **[ユニバーサルシリアルバス]** のデバイスセクションにあることが理想的です。デバイスが **[その他のデバイス]** にある場合は、上記の設定手順を行いデバイスを USB デバイスにする必要があります。
- デバイスが通信中か通信モードであることを確認します。上記の手順 1 を参照してください。

- ドライバのパスが正しく C:\Windows\INF... になっていることを確認します。上記の手順 2 を参照してください。

質問 3: [更新] をクリックしたとき、または一覧で試験機器をクリックしたら「内部サーバー エラー」というエラーが表示されました。

回答: この問題を解決するには、

- Windows サービス(あるいはサービス)に移動し、
- 一覧の [DruckCommsServer サービス] を右クリックして [再起動] をクリックします。



- 4Sight2 に移動し、[更新] ボタンをクリックします。一覧にデバイスが表示されます。

質問 4: [通信エラー] が表示されました。

回答: USB が正しく接続されていない、デバイスがハングアップしている、別のタスクによりデバイスやサーバーがビジー状態である、などの理由でソフトウェアがデバイスと適切に通信できない場合があります。再び [更新] ボタンをクリック (2,3 回試してください) すれば問題は解決します。

それでもこのエラーが解消されない場合は、次の手順を試してください。

- デバイスが重要な動作中でなく、安全な状態でデバイス (Genii / PACE) を再起動してください。もう一度試してください。また、デバイスが物理的に正しく接続されていることを再確認します。

上記の手順でも解決できない場合、手順 3 に従い [DruckCommsServer サービス] を再起動してください。

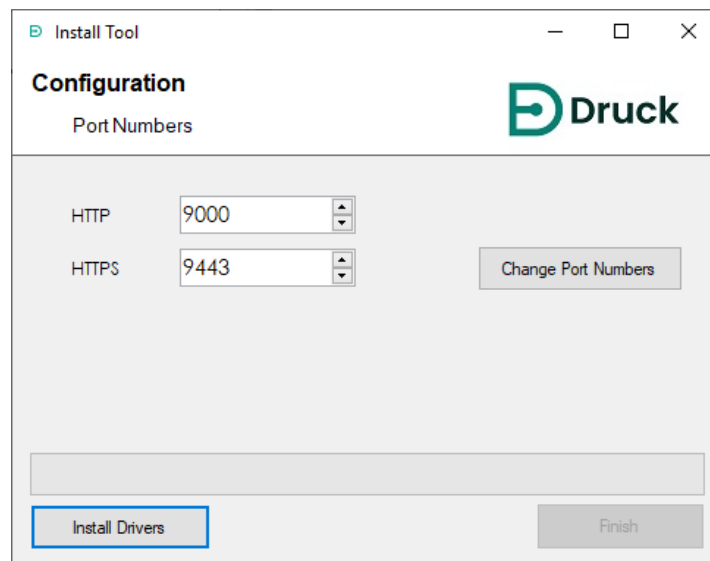
インストール時のトラブルシューティング

7. インストール時のトラブルシューティング

7.1 試験機器の通信時の問題

4Sight2 を使って試験機器と通信する場合、試験機器コミュニケータを直接呼び出した場合にコミュニケータが json string を応答することを確認していたにもかかわらず、試験機器から応答が返ってこない場合があります。これは主に2つの原因のどれかによる可能性があります。

- ポート番号の構成が不適切な場合 - 4Sight2 がどのポートを使って試験機器コミュニケータと通信しているのか、管理者に問い合わせてください。
どのポートを使用しているかを把握したら、C:\Program Files\Druck\DruckCommsServer\[Version] に移動して CommsServerInstallTool.exe を実行します。



ポート番号を編集して [ポート番号の変更] ボタンをクリックします。サービスの再開を待ちます。これでポート番号が変更されました。[終了] ボタンを選択します。

- 試験機器コミュニケータは Https ではなく、4Sight2 に設定しています。
試験機器コミュニケータ用に自己署名証明書をインストールするよう、管理者に問い合わせてください。

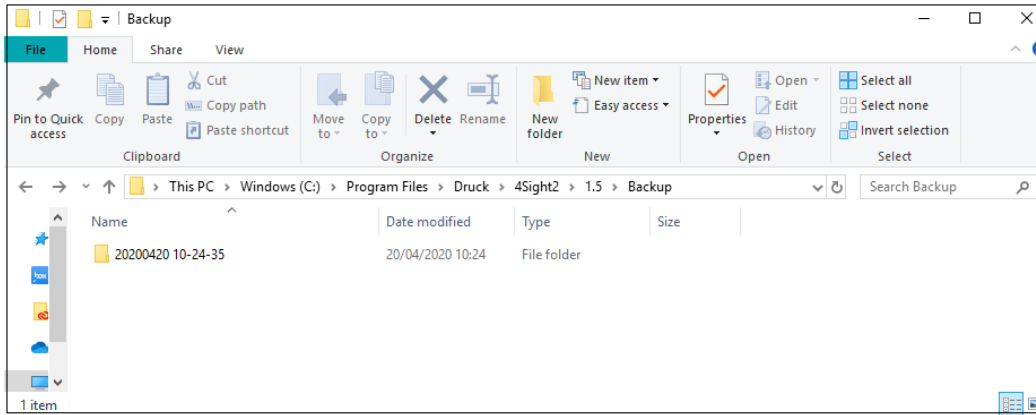
7.2 Postgres データベースバックアップ

データベースバックアップについては、4Sight2 ユーザーマニュアル - 123M3138 を参照してください。

7.3 Postgres データベース復元

すでに 4Sight アプリケーションを使用してデータベースのバックアップを行っていることが前提です。

4Sight アプリケーション (バージョン 1.4 以上) は、バックアップを開始 (ユーザーが開始 / スケジュール設定) するためのインターフェースを提供します。この操作により、サーバーの 4Sight インストールディレクトリ内のバックアップフォルダにファイルが作成されます。バックアップを開始するごとに、バックアップが正常に完了した日時に応じて、YYYYMMDDHHSS (年、月、日、時、秒) の形式の名前で、バックアップフォルダ内に新規フォルダを作成します。



バックアップフォルダ内の内容を個別のメディアにバックアップすることが推奨されます。

各フォルダには 5 つのファイルがあります。

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

*.bck ファイルには、4Sight アプリケーションのバージョンを示すサフィックスが付けられます。復元するデータベースは、使用しているアプリケーションのバージョンに完全に一致していることを確認してください。データベースの上位 / 下位バージョンはアプリケーションでサポートされません。バージョンは、ピリオド (.) ではなくアンダースコア (_) で表記される点に注意してください (たとえば、1.4 ではなく 1_4)。復元の手順で下記のコマンドを使用するときは、必ず <APPLICATION_VERSION> をインストールされている 4Sight の正しいバージョンに置き換えてください。

metadata.properties ファイルには、バックアップ開始時に入力されたバックアップの名前が含まれています。

```

metadata.properties - Notepad
File Edit Format View Help
##
#Tue Oct 23 15:26:44 IST 2018
Name=Backup taken before adding Sao Paulo Plant
4Sight1_4.bck=daeabd2f83224b0611648ee78415ddefd784eab580afa1e6613c927de6561c7f
uaa1_4.bck=79cc5efd42dbeda88685ec59b07c9800eb93bf4c0cab9932cb7d639a4340a1ce
4Sightaudit1_4.bck=92cfcd6e8ce97a49f4f9470e197f9170e80cfe8de059b53b86faf86c5633fc3
    
```

SHA 256 チェック

バックアップでは各データベース用に1つずつ、計 3 つのファイルがあり、それぞれ .bck の拡張子が付いています。metadata.properties ファイルには、各バックアップファイルの SHA 256 が含まれています。

1. 管理者としてコマンドプロンプトを開き、選択したバックアップファイルが含まれるフォルダにディレクトリを変更します。
2. 次のコマンドを使用して各ファイルの SHA256 を計算します。

```

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

3. 復元の手順を続行する前に、各ファイルの SHA 256 がメタデータファイルに記載されている SHA 256 と一致していることを確認します。コマンドプロンプトによるチェックサムとメタデータファイルによるチェックサムが完全に一致する場合に、バックアップファイルが復元用に有効となります。それらが同一である場合のみ、復元の手順を続行してください。

7.4 復元の手順:

1. 4Sight サーバーに管理者としてログインします。
2. Postgres データベースが稼働しているポートを探します。〈4Sight INSTALLATION DIRECTORY〉\apache-tomcat\webapps\application.properties ファイル内の spring.datasource.url プロパティで見つけることができます。メモ帳を管理者として実行してこのファイルを開きます。4Sight〈APPLICATION_VERSION〉の直前の番号が相当します。
3. 管理者として実行しているコマンドプロンプトから postgres ユーザーを使用して psql コマンドユーティリティにログインします。
C:\Program Files\PostgreSQL\11\bin\psql" --port=〈DB_PORT〉 postgres postgres
4. アプリケーションが使用しているデータベースユーザーは、〈4Sight INSTALLATION DIRECTORY〉\apache-tomcat\webapps\application.properties ファイル内の spring.datasource.username プロパティで見つけることができます。メモ帳を管理者として実行してこのファイルを開きます。
5. *_temp データベースが存在する場合はそれらを削除し、psql プロンプトで以下のコマンドを実行することによって空の *_temp データベースを作成します。

```
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";
```

上記 3 つのデータベースのデータベース所有者をこのユーザーに変更します。ユーザー名は大文字と小文字が区別されます。

```
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. metadata.properties ファイルをチェックし、復元が必要なバックアップがどれなのかを判別します。
7. 別のコマンドプロンプトを管理者として開き、選択した上記のバックアップファイルが含まれるフォルダにディレクトリを変更します。

以下のコマンドを使用してデータベースを *.bck ファイルから *_temp データベースに復元します。パスワードを入力するように促されたら、postgres のスーパーユーザーのパスワードを入力します。

```
"C:\Program Files\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:\Program Files\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:\Program Files\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. *_old databases が存在する場合は、psql プロンプトで以下のコマンドを使用して削除します。


```
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. 4Sight サービスおよび pgadmin アプリケーションが開いている場合は、停止します。
10. psql プロンプトで以下のコマンドを実行して、既存の 4Sight データベースの名前を *_old に変更します。


```
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. psql プロンプトで以下のコマンドを実行して、*_temp データベースの名前を 4Sight データベースに変更します。


```
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. 4Sight サービスを開始し、管理者としてログインを試みます。今回のログインには、バックアップ作成時の管理者パスワードを使用する必要があります。

7.5 4Sight2 マシンクラッシュからの回復方法

前提条件: クラッシュ発生前にユーザーが 4Sight2 データベースのバックアップを作成していること。

アプリケーションとデータベースの両方のユーザー名とパスワードを既にユーザーが把握していること。

1. サポートする OS およびドライバを使用してマシンをセットアップします。
2. 4Sight2 をマシンにインストールします。

- アプリケーションをインストールする場合は、アプリケーションと Postgres データベースで以前使用したものと同一ユーザー名とパスワードを使用してください。

4Sight2 V1.5.0.16652 - InstallShield Wizard

Existing PostgreSQL 11 Database Details

PostgreSQL Installation Directory

Installation Directory: C:\Program Files\PostgreSQL\11

PostgreSQL Port number

Port: 5432

Please provide password for the database super user (postgres)

Password: []

InstallShield

< Back Next > Cancel

以前のインストール時と同じパスワード

4Sight2 V1.5.0.17177 - InstallShield Wizard

Application Details

Enter 4Sight2 Application User Information

User ID: []

Password: []

Confirm Password: []

Email: []

Enter Database User Information

Use Default User ID/Password Show Password

User ID: 4Sight2Admin

Password: []

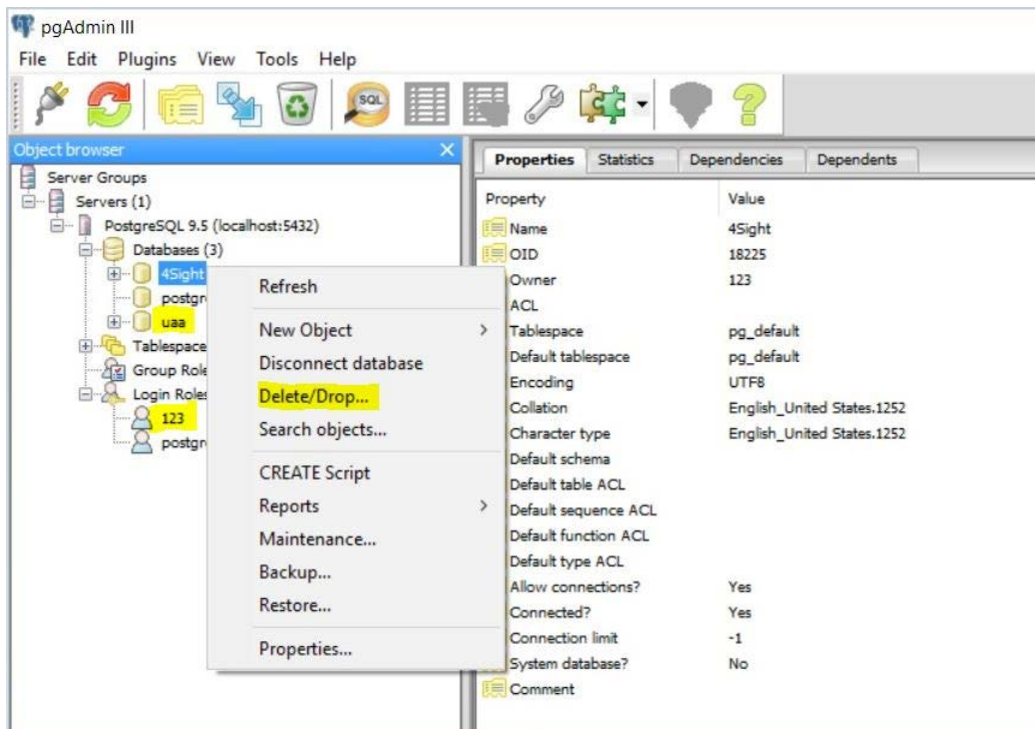
Confirm Password: []

InstallShield

< Back Next > Cancel

以前のインストール時と同じ情報をすべてのフィールドに入力

- アプリケーションのインストールが完了したら、アプリケーションのインストール中に作成したデフォルトのデータベースを pgAdmin からドロップ(データベース上で右クリックして [削除 / ドロップ])を選択します。データベースのドロップ操作中にエラーが発生した場合、Postgres サービスを再起動してリフレッシュしてからもう一度試してください。



- データベースおよびユーザーの削除を正常に終了した後、上記の手順に従ってコマンドプロンプトからデータベースを復元します。
- これで正常にデータベースが復元されました。ブラウザでアプリケーションを開き、復元されていることを確認してください。

7.6 インストール時の障害のシナリオ:

以下の表で、インストール時のさまざまな障害のシナリオとその修復処置について説明します。

エラーメッセージ	シナリオ	修復とその処置
"Insufficient disk space available to install 4Sight2 application. Please ensure a minimum of 4096 MB is available. Free Space : available MB."	ハードディスクサイズの問題による障害 (アップグレードの開始時に必要な容量がない場合)	管理者はそれぞれのドライブで容量を解放して、アップグレードプロセスを再度試みる必要があります。
"Deployment fail while Migrating database"	ハードディスクサイズの問題による障害 (アップグレードを正常に開始した後に十分な容量がない場合)	管理者はそれぞれのドライブで容量を解放して、アップグレードプロセスを再度試みる必要があります。

エラーメッセージ	シナリオ	修復とその処置
"Installation failed while migrating Database. Please reinstall 4sight2"	データベースコピー時のデータ整合性による障害	この問題が発生する場合、管理者はカスタマーヘルプデスクに連絡する必要があります。データ整合性の理由は次の場所にあるログに取り込まれています。 [C:\Users\[Username]\App Data\Local\Temp\logs]
"Installation failed while migrating Database. Please reinstall 4sight2"	スキーマ更新段階でのデータ整合性による障害	この問題が発生する場合、管理者はカスタマーヘルプデスクに連絡する必要があります。データ整合性の理由は次の場所にあるログに取り込まれています。 [C:\Program Files\Druck\4Sight2\<<latest folder number>>\logs]
"Failed to locate existing 4Sight2 service. Please ensure existing 4Sight2 version is installed on this machine and the service is running"	この障害はインストーラがサービスの状態を取得できなかった場合に発生します。	管理者は、4Sight2 サービスが起動しており、稼働中であることを確認する必要があります。
"Failed to start the 4Sight2 service. Please ensure the 4Sight2 service is present and running"	障害が発生するのは、アプリケーションが破損している場合、一部のファイルが削除されている場合、ポートが別のアプリケーションによって使用されている場合、ユーザーがサービスを停止している場合などです。	管理者がサービス状態の取得に成功し、何らかの理由（たとえば、アプリケーションが破損している、一部のファイルが削除されている、ポートが別のアプリケーションによって使用されている、ユーザーがサービスを停止しているなど）によって稼働していない場合には、システムがサービスの開始を試みます。サービスを開始できない場合、管理者はカスタマーサポートに連絡して問題を解決する必要があります。
"Upgrade of 4Sight2 application is supported from version 1.3 onwards. For earlier version upgrade support please contact Customer Care."	1.3 より前のバージョンがインストールされている場合、アップグレードは実行されません。	1.3 以降のバージョンからのアップグレードのみ可能です。
Installer has detected another minor version of PostgreSQL 11. Installer will not continue. Refer to 4Sight2 Installation manual for more details	ターゲットマシン上に同じ PostgreSQL バージョン（バリエーション）が存在するために 4Sight2 は 4Sight2 のインストールを続行できません。	実行可能なオプション 1.ユーザーが別のマシンを選択する。 2.ユーザーが Postgres バージョン 11.3 を使用する既存アプリケーションのバックアップを作成し、そのアプリケーションをアンインストールした後、別のマシンに展開する。Postgres をアンインストールし、4Sight2 インストールを再開する。

エラーメッセージ	シナリオ	修復とその処置
Installation failed while upgrading database. Please reinstall 4Sight2. Refer to 4Sight2 Installation manual for more details	アップグレード中に何らかの内部エラーが発生した可能性があります。ユーザーは再インストールを試行できます。	問題が解決されない場合、ユーザーは理解しやすいようにインストールログを共有できます。

7.7 エラーの一般的な原因

以下に示すのは、USB を介した Druck 機器との 4sight2 の通信に関連して一般に生じる問題です。

- 物理的な接続が緩いまたはあまい
- ケーブル / ポートの摩耗
- USB アダプタの劣化
- USB アダプタ / ポートへの過負荷
- デバイスが長期間にわたり動作したため、休止またはスリープモードになっている
- デバイスが通信モードでない
- ドライバのソフトウェアが未インストールまたは未アップグレード。ハードウェアとの通信を確立するには、4Sight2 アプリケーションとドライバのバージョンが同じである必要があります。
- デバイスには非常に古いファームウェアバージョンが存在します。

7.8 4Sight2 のアンインストール

4Sight2 の新しいコピー、すなわち新バージョンの 4Sight2 をインストールする必要がある場合、またはインストール中に問題が起こって 4Sight2 をアンインストールする必要がある場合、この指示に従ってください。



PostgreSQL データベースコンポーネントをアンインストールすると、4Sight2 データベースが削除され、データを損失します。次の手順ではバックアップを自動的に作成しないので、この手順を進める前に手作業でバックアップを作成し、4Sight2 インストールフォルダとは別の場所にバックアップを保存します。Postgres データベースバックアップと、本マニュアルの復元セクションを参照してください。

4Sight2 アプリケーションだけをアンインストールしてデータベースを残す選択をする場合には、本マニュアルの 4Sight2 インストール部分を参照してください。再インストールにはデータベースのスーパーユーザーとしての認証情報が必要です。認証情報についての知識がない場合には、アンインストールを行わないでください。

データベースをアンインストールせずに 4Sight2 のバージョンを更新したい場合は、この指示には**従わないで**ください。

1. [コントロールパネル] >> [プログラムと機能] に移動します。
2. 4Sight2 を右クリックし、[アンインストール] を選択します。
3. アンインストールウィザードの指示に従います。
4. PostgreSQL 11 を右クリックし、[アンインストール] を選択します。
5. アンインストールウィザードの指示に従います。
6. PostgreSQL をアンインストールしてもデータフォルダは削除されません。削除は手作業で行う必要があります。削除するデータフォルダは C:\Program Files\PostgreSQL\11\ にあります。
 - a. PostgreSQL フォルダ全体を削除したい場合は、作業を進める前にバックアップファイルやスクリプトを bin フォルダから移動するようにしてください。
 - b. デフォルト設定では、4Sight2 データベースのバックアップは次の場所に作成、保存されています。
C:\Program Files\PostgreSQL\11\bin
7. 可能であれば、コンピュータの再起動を推奨します。
8. 4Sight2 はこれで正常にアンインストールされました。

7.9 セキュア通信に関するトラブルシューティング

1. あるコマンドが、内部コマンドとしても外部コマンドとしても認識されない。例えば「keytool」と入力しても、コマンドとして認識されない。
- このようなエラーが起こる場合、現在のフォルダから、指定されたコマンドに対応する実行ファイルを参照できない状態です。

適切なフォルダを参照できるよう、環境変数を設定してください。

Set Path=%Path%;<< コマンドの実行ファイルがある場所の完全パス >>

例えば keytool が認識されない場合、次のように Path を設定します。

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

2. Bad IP address
 - このような文言のエラーメッセージが現れる場合、openssl-ca.cnf または openssl-server.cnf に記述された IP アドレスまたはホスト名が不適切です。注記: ファイル内の複数箇所を修正し、同じ手順を繰り返す必要があるかも知れません。

3. No such file or directory ...

- このような文言のエラーメッセージが現れる場合、コマンドが参照しようとしたファイルの名前が正しくありません。コマンドに指定したファイル名を確認し、さらに、当該ファイルが所定のフォルダ以下にあることを確認した上で、改めてコマンドを実行してください。コマンドのファイル名を修正するだけで済む場合と、欠けているファイルを生成し直さなければならない場合があります。
- index.txt および serial.txt については、拡張子が二重に付加され、例えば「intex.txt.txt」というファイルを参照しようとするために起こることもあります。
このファイル名を記述しているファイルを編集し、拡張子「.txt」を省いてみてください。ファイル名には拡張子「.txt」が1回だけ現れるようにしなければなりません。

ベストプラクティス

8. ベストプラクティス

サーバーのハードニング

サーバー環境は Microsoft または CIS のガイドラインによってハードニングすることが推奨されます。

8.1 Tomcat

- Tomcat のインストール先は、管理者または LocalService のみにアクセス権がある安全なフォルダとします。C:\Program Files(x86) など。
- Tomcat は LocalService アカウントで実行するサービスとしてインストールします。
- WebApp からすべてのアプリケーションを削除します。不要なデフォルトアプリケーションも削除します。
- 404、403、500 など、デフォルトエラーページを置き換えます。
- HTTPS を適用し、SSL を有効化します。
- 管理アプリケーションは SSL 上で実行します。
- Web アプリケーションごとのユーザー個別のログファイル。
- サーバーバナーを削除します。
- アクセスロギングを有効化します。
- シャットダウンポートおよびシャットダウンコマンドを変更します。

8.2 PostgreSQL

- pgdba、postgres、depesz のような高特権のアカウントはすべて、ローカルログインのみを許可します。
- 正しいユーザーが正しいアクセス権を取得できるように、pg-hba.conf ファイルでシーケンスが正しいことを確認します。
- ネットワーク経由ではなく、ローカルマシンからのみサーバーに接続できるように pg-hba.conf ファイルを構成します。

8.3 ファイアウォールのベストプラクティス

ここでは、4Sight2 を使用する場合に推奨されるファイアウォールのベストプラクティスを示します。

8.3.1 ポリシー

1. ファイアウォールの構成は組織セキュリティポリシーとの整合性がなければなりません。
2. 常に最小限の特権ポリシーを使用します。デフォルト設定をすべて否定します。特定のトラフィックを許可します (送信元、送信先、ポートの使用)。
3. 明確なルールを最初に設定し、明示的な削除ルールを使用します。
4. すべてのアクション (特に失敗した試み) を監査証跡用にログに記録します。

8.3.2 リソース

1. メモリ使用状況を監視する
2. CPU 使用状況を監視する
3. 帯域幅使用状況を監視する
4. ファイアウォールマシン上で稼働するアプリケーションの数を制限する

8.3.3 インストールと保守

1. ファイアウォールマシンへの物理的アクセスを制限する
2. 管理者には固有のユーザー ID を使用する
3. マシン上の厳格なアカウントポリシーに従う
4. オペレーティングシステム、アプリケーションソフトウェア、ファームウェアなどのパッチ処理を定期的に行う
5. ルールベース、構成、およびログを定期的アーカイブするルールおよびソース制御中に実施した変更のすべてを文書化する
6. 定期的なテストを実行する
7. サービス廃止時には使用されないルールを除去する
8. 定期的なルール監査およびレビューを実施する
9. 定期的なセキュリティアドバイザリー報告

8.3.4 さらなるセキュリティ強化

1. ステートフルインスペクションを使用する
2. プロキシを使用する
3. アプリケーションレベルのインスペクションとフィルタリングを使用する

8.3.5 内部的な保護

1. 利用規約を設定する
2. ユーザーごとのパーソナルファイアウォール
3. ホストベースの侵入防止
4. ネットワーク監視
5. コンテンツフィルタリング
6. 各コンピュータおよびアプリケーションでのアクセス制御

オフィス所在地

本社

レスター、英国

電話番号 : +44 (0) 116 2317233

Eメール :

gb.sensing.sales@bakerhughes.com

UAE

アブダビ

電話番号 : +971 528007351

Eメール : suhel.aboobacker@bakerhughes.com

イタリア

ミラノ

電話番号 : +39 02 36 04 28 42

Eメール : csd.italia@bakerhughes.com

インド

パンガロール

電話番号 : +91 9986024426

Eメール : aneesh.madhav@bakerhughes.com

オーストラリア

スプリングフィールドセントラル

電話番号 : 1300 171 502

Eメール : custcare.au@ge.com

オランダ

フーヴェラーケン

電話番号 : +31 334678950

Eメール :

nl.sensing.sales@bakerhughes.com

ドイツ

フランクフルト

電話番号 : +49 (0) 69-22222-973

Eメール : sensing.de.cc@bakerhughes.com

フランス

トゥールーズ

電話番号 : +33 562 888 250

Eメール : sensing.FR.cc@bakerhughes.com

ロシア

モスクワ

電話番号 : +7 915 3161487

Eメール : aleksey.khamov@bakerhughes.com

米国

ボストン

電話番号 : 1-800-833-9438

Eメール : custcareboston@bhge.com

日本

東京

電話番号 : +81 3 6890 4538

Eメール : gesitj@bakerhughes.com

中国

北京

電話番号 : +86 180 1929 3751

Eメール : fan.kai@bakerhughes.com

中国

広州

電話番号 : +86 173 1081 7703

Eメール : dehoul.zhang@bakerhughes.com

中国

上海

電話番号 +86 135 6492 6586

Eメール : hensenzhang@bakerhughes.com

サービスおよびサポート拠点

技術サポート

グローバル

Eメール : mstechsupport@bakerhughes.com

UAE

アブダビ

電話番号 : +971 2 4079381

Eメール : gulfservices@bakerhughes.com

インド

ブネー

電話番号 : +91 213 5620426

Eメール :

mcsindia.inhouseservice@bakerhughes.com

ブラジル

カンピーナス

電話番号 : +55 11 3958 0098、+55 19 2104 6983

Eメール : mcs.services@bakerhughes.com

フランス

トゥールーズ

電話番号 : +33 562 888 250

Eメール : sensing.FR.cc@bakerhughes.com

米国

ビレリカ

電話番号 : +1 (281) 542-3650

Eメール : namservice@bakerhughes.com

日本

東京

電話番号 : +81 3 3531 8711

Eメール :

service.druck.jp@bakerhughes.com

英国

レスター

電話番号 : +44 (0) 116 2317107

Eメール :

sensing.grobycc@bakerhughes.com

中国

常州

電話番号 : +86 400 818 1099

Eメール : service.mcchina@bakerhughes.com

Copyright 2020 Druck, Baker Hughes 社の事業。本書にはベーカー・ヒューズ・カンパニー、および各国の関連会社の1つ以上の登録商標が含まれています。サードパーティのすべての製品名および社名は、それぞれの所有者の商標です。

123M3140 改訂 F | 日本語

Baker Hughes 