Druck

4Sight2

교정 관리 소프트웨어

설치 설명서 123M3140 개정 F

Druck.com

목차

1. 소개

4Sight2 교정 소프트웨어는 교정 환경을 최고 수준의 경량학적 표준에 맞게 유지하고 제어하는 데 도움을 주는 웹 기반 교정 관리 툴입니다. 이 소프트웨어를 사용할 수 있는 작업은 다음과 같습니다.

- 지정된 사업장의 모든 측정 장치에 대한 교정 관리
- 기술자의 교정 작업 일정 설정
- USB 통신 기능이 있는 Druck 휴대용 교정기(DPI620 Genii, DPI611 및 DPI612)에서 데이터 업로드 및 다운로드
- 휴대용 교정기(수동 데이터 입력)에서 지원되지 않는 장치에 대한 교정 기록 관리
- 교정 기록 검사. 각 교정 인증서의 영구 기록을 작성할 수도 있습니다. 예: ISO 9000 품질 제어 절차.
- Druck 압력 컨트롤러(PACE 1000, 5000, 6000), 휴대용 교정기(DPI620 Genii, DPI611, DPI612) 및 온도 교정기(DryTC165, DryTC 650, LiquidTC165, LiquidTC255)를 사용한 자동 교정 제어

1.1 대상 독자

1.1.1 관리자

관리자는 4Sight2 소프트웨어의 설치 및 구성을 담당합니다. 4Sight2를 처음 설치하면 단일 관리자 계정을 사용할 수 있게 됩니다. 이 계정에서 새 사용자를 생성하고 그룹/권한 세트를 할당할 수 있습니다. 관리자 사용자는 4Sight2의 모든 기능에 대한 읽기 및 쓰기 액세스 권한을 보유합니다.

1.1.2 감독자

감독자는 자산 및 교정 관리를 담당합니다. 감독자는 4Sight2 Enterprise 내에서 플랜트, 위치, 태그 및 장치를 포함한 자산을 생성 및 업데이트할 수 있습니다. 감독자는 플랜트 프로세스 및 장치 데이터시트와 같은 문서를 자산에 연결할 책임이 있습니다. 감독자는 교정 시 사용할 테스트 절차를 생성하고, 절차를 예약하고, 장치의 상태를 모니터링할 수 있습니다. 감독자는 교정을 승인하는 데 필요한 권한을 보유하고 있습니다.

1.1.3 기술자

기술자는 교정을 수행할 책임이 있습니다. 교정에는 휴대용, 수동 또는 자동 교정이 있으며 기술자의 역할은 장치에서 관련 교정 유형을 수행하는 것입니다. 교정이 수행된 후 기술자는 결과를 검토하고 교정을 완료하게 되며 이후 감독자가 교정을 승인할 수 있습니다.

1.1.4 감사자

감사자는 보고서를 검사할 책임이 있습니다. 일부 플랜트에서는 규정상 반드시 감사를 실시해야 합니다.

2. 시스템 요구 사항

서버 및 클라이언트 시스템에 4Sight2 애플리케이션을 설치하는 데 필요한 최소 시스템 요구 사항은 아래와 같습니다.

2.1 애플리케이션 서버

운영 체제	Windows 10, Windows Server 2012 R2, Windows Server 2016, Windows Server 2019
업데이트	모든 Windows 업데이트가 완전히 설치된 상태
프로세서	쿼드 코어
RAM	8GB 이상(32GB 권장)
디스크 공간	1TB
네트워크 속도	10Mbps

2.2 클라이언트 워크스테이션

운영 체제	Windows 10, Windows Server 2012 R2, Windows Server 2016, Windows Server 2019
브라우저	Google Chrome V80+, Microsoft Edge V80, Firefox V74
Adobe Reader	Adobe Acrobat Reader DC 버전 2015.017.20050 +
RAM	8GB 이상
프로세서	듀얼 코어
디스크 공간	600GB
네트워크 속도	10Mbps

2.3 로컬 설치

운영 체제	Windows 10, Windows Server 2012 R2, Windows Server 2016, Windows Server 2019
업데이트	모든 Windows 업데이트가 완전히 설치된 상태
Adobe Reader	Adobe Acrobat Reader DC 버전 2015.017.20050 +
프로세서	듀얼 코어
RAM	16GB 이상(32GB 권장)
디스크 공간	500GB 이상의 디스크 공간
브라우저	Google Chrome V80+, Microsoft Edge V80, Firefox V74

2.4 4Sight2 지원 펌웨어

지원되는 펌웨어에 대한 최신 정보는 아래 링크를 참조하십시오.

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

또는

PACE의 경우 아래 이미지와 같이 4Sight2 통신용 USB B를 삽입합니다.

4Sight2 설치

3. 4Sight2 설치

4Sight2를 설치하려면 먼저 4Sight2 Setup zip을 바탕화면에 복사하고 zip에서 파일을 추출합니다. 설정 파일에서 4Sight2 실행 파일을 선택합니다.

참고: 다음의 바이러스 백신 소프트웨어는 4Sight2 및 통신 서버 설치를 검사하는 데 사용됩니다.

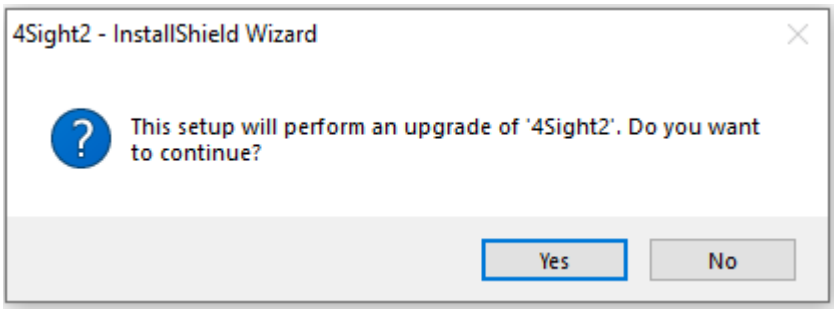
- McAfee VirusScan Enterprise + AntiSpyware Enterprise 버전 번호: 8.8.0
- Symantec Endpoint Protection 버전 번호: 14.3.558

설치 실행 파일을 실행하면 InstallShield 마법사가 시작됩니다. InstallShield 마법사에는 4Sight2 설치의 두 단계가 포함되어 있습니다.

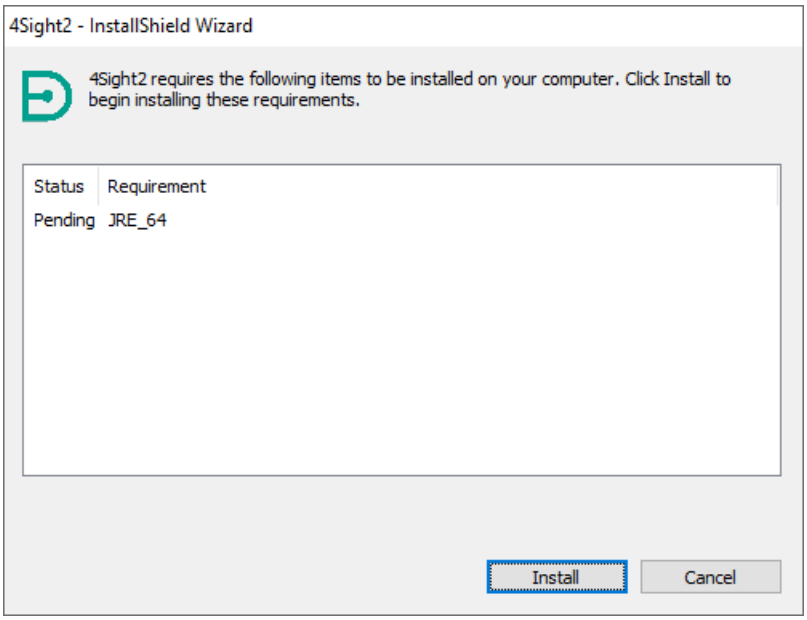
1. 데이터베이스 설치
2. 웹 애플리케이션 설치

InstallShield 마법사의 안내를 따르거나 다음 두 섹션을 참조하여 설치 프로세스를 진행하십시오.

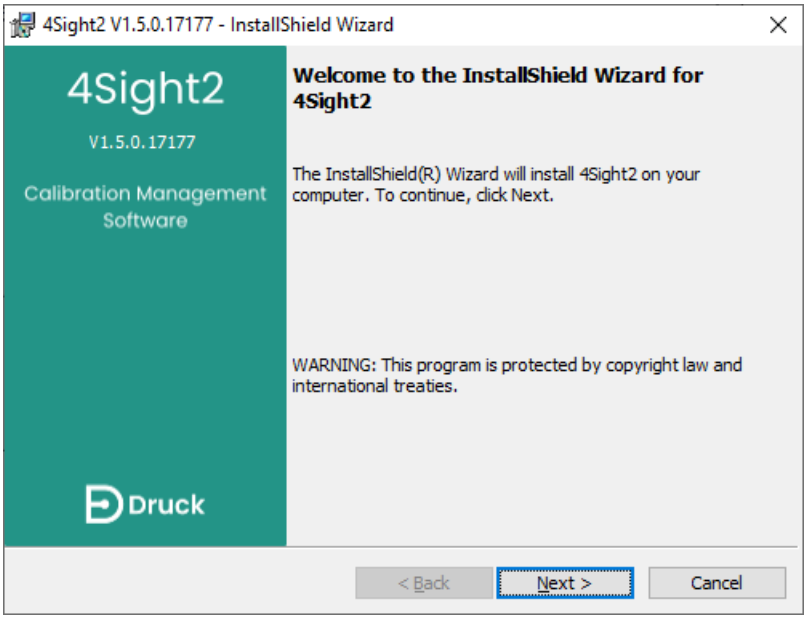
1. 시스템에 이미 4Sight2가 설치되어 있으면 설치 마법사에서는 최신 버전으로 업그레이드하라는 메시지를 표시합니다. **예**를 클릭하여 최신 업그레이드를 수행합니다.



2. 시스템에 4Sight2를 처음 설치하는 경우에는 아래와 같은 화면이 나타납니다. **설치**를 선택하면 표시된 항목이 설치됩니다.



3. 필수 항목 설치가 완료되면 InstallShield 마법사 시작 화면이 표시됩니다. **다음**을 클릭하여 계속합니다.



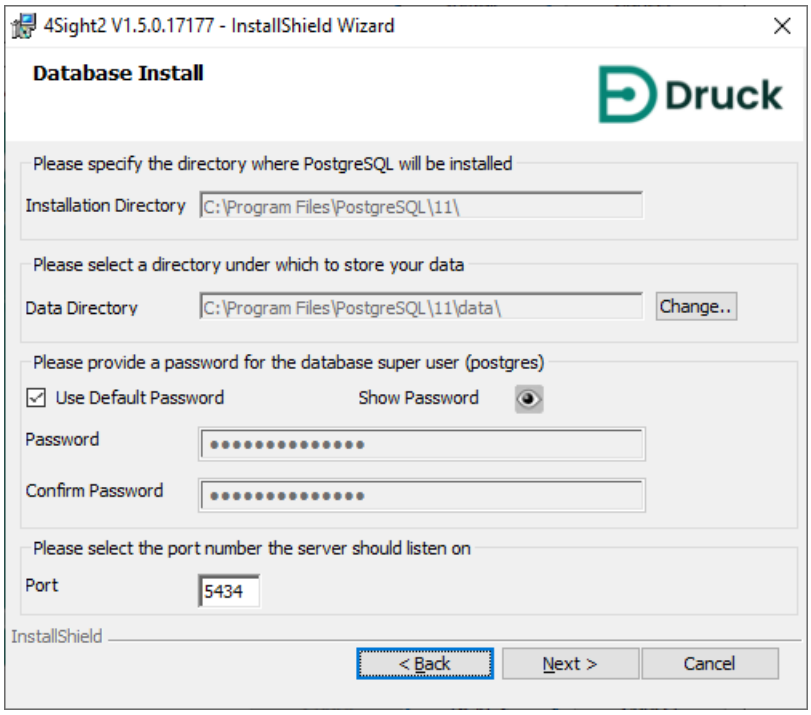
3.1 데이터베이스 설치

4Sight2 애플리케이션은 PostgreSQL 데이터베이스를 사용합니다. PostgreSQL 데이터베이스를 설치하는 방법과 PostgreSQL 데이터베이스가 이미 설치된 경우에 할 일에 대한 지침은 아래에 나와 있습니다.

3.2 PostgreSQL 설치

시스템에 PostgreSQL 데이터베이스를 설치하지 않은 경우 이 절차를 따르십시오.

1. 시스템에 설치된 PostgreSQL 데이터베이스의 인스턴스가 없는 경우 아래와 같은 화면이 나타납니다.



설치 디렉터리: PostgreSQL 애플리케이션을 설치할 수 있는 디렉터리를 선택합니다.

데이터 디렉터리: PostgreSQL 데이터베이스를 저장할 수 있는 디렉터리를 선택합니다.

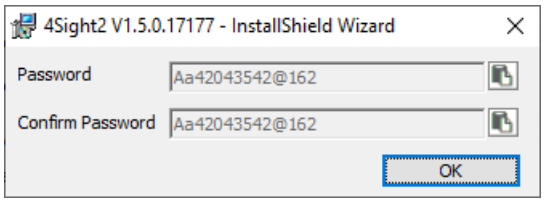
암호/암호 재입력: PostgreSQL 데이터베이스 슈퍼 사용자의 암호를 입력합니다. 이 과정은 PostgreSQL 데이터베이스를 처음 설치하는 경우에만 요구됩니다.

참고: 이 암호는 설치 후에 데이터베이스 콘텐츠에 액세스할 때 필요합니다.

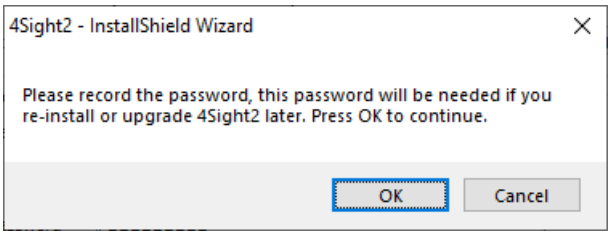
포트: 애플리케이션 요청에 적합한 PostgreSQL 데이터베이스의 포트 주소입니다.

참고: 포트 번호가 이미 나와 있는 경우 IT 팀에 문의하여 주십시오. 사용자도 포트 번호를 변경할 수 있습니다. 나중에 애플리케이션을 시작하려면 이 포트 번호를 기록해 두어야 합니다.

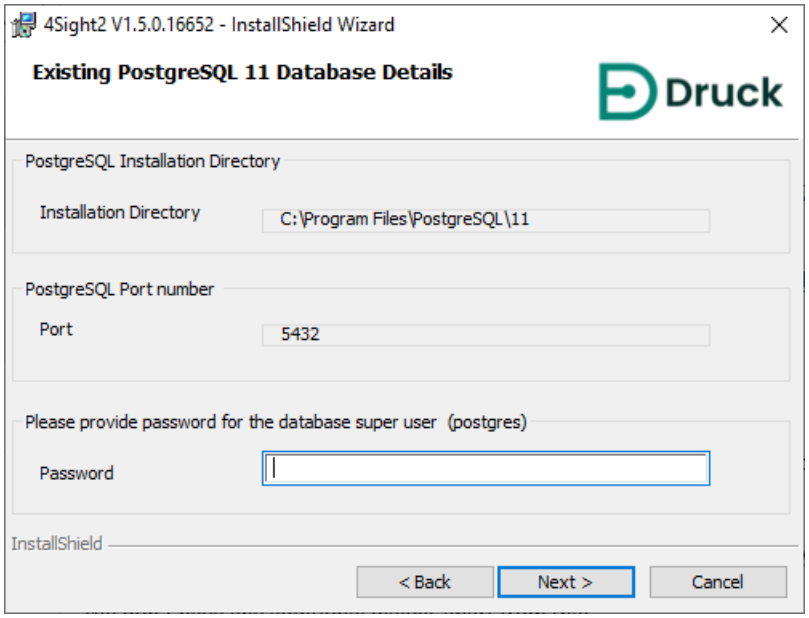
중요: 사용자는 데이터베이스 암호를 적어 두어야 합니다. 암호 정보를 잃어버리면 액세스가 거부되거나 데이터가 손실될 수 있습니다. 데이터베이스 슈퍼 사용자 암호를 업데이트하려면 사용자 기본 암호 확인란을 선택 해제하십시오. 기본 암호를 유지하거나 입력한 새 암호를 보려면 (암호 표시) 아이콘을 선택하십시오. 암호를 클립보드에 복사하려면 (클립보드에 복사) 아이콘을 사용하십시오.



그러면 설치 프로그램에서 암호를 다시 기록하라는 메시지를 표시합니다. 암호를 기록한 후 **확인**을 선택합니다.

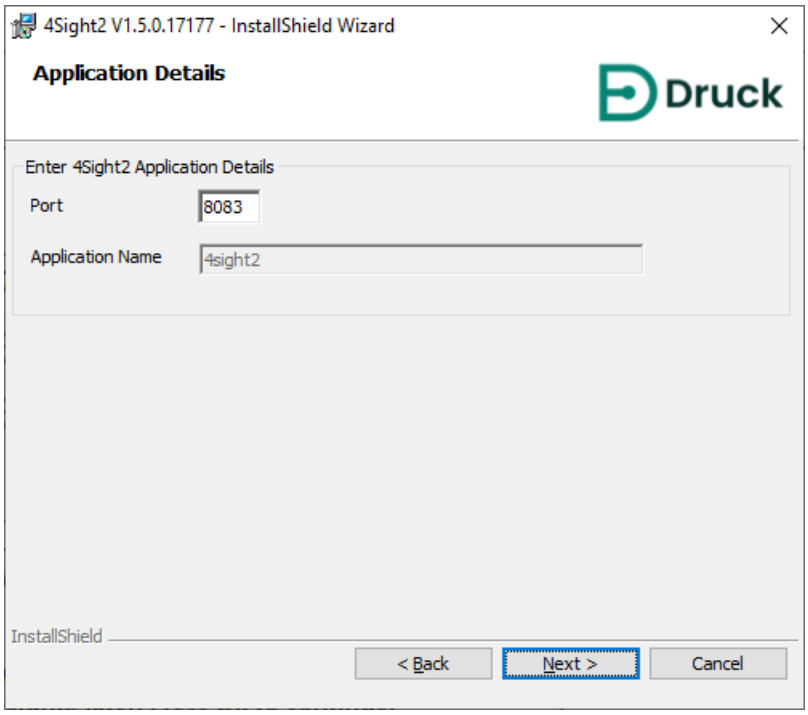


2. 이 단계는 PostgreSQL 데이터베이스가 이미 설치된 경우에만 사용자에게 표시됩니다.



설치 디렉터리: PostgreSQL이 이미 설치된 경로를 명시하는 섹션으로, 읽기 전용 정보입니다.
암호: PostgreSQL 데이터베이스 슈퍼 사용자 암호를 확인하기 위한 것입니다.
포트: PostgreSQL 데이터베이스에서 db. 요청을 실행하기 위해 사용하는 포트 번호를 명시하는 섹션입니다.

3. 애플리케이션 세부 정보 창에서 아래 세부 정보를 입력합니다.

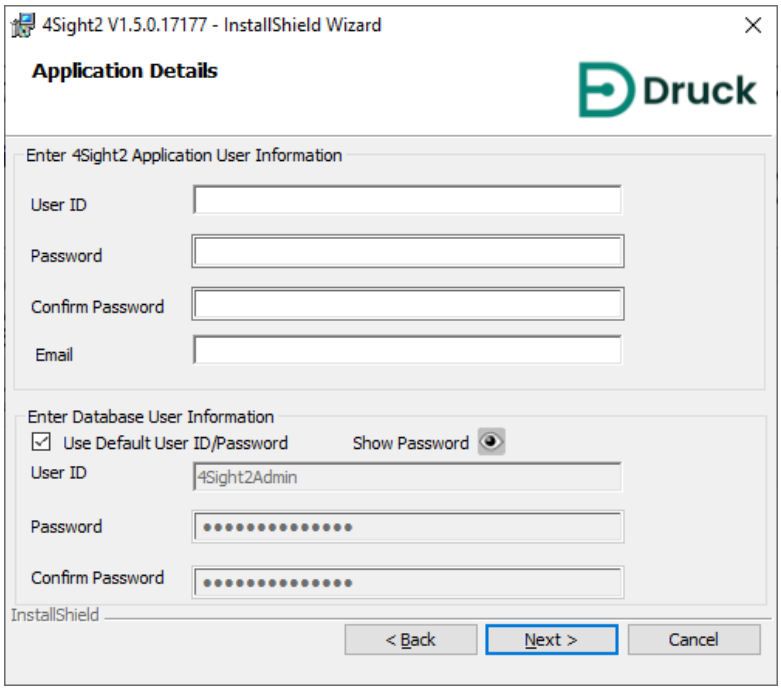


포트: 4Sight2 웹 애플리케이션에서 HTTP 요청에 응답하기 위해 사용되는 Tomcat 웹 서버 포트를 입력합니다.

애플리케이션 이름: 브라우저에서 4Sight2 애플리케이션을 연결하는 데 사용할 애플리케이션 컨텍스트 경로를 입력합니다. 기본적으로 애플리케이션 이름은 4sight2입니다.

참고: 포트 번호가 이미 나와 있는 경우 IT 팀에 문의하여 주십시오. 사용자도 포트 번호를 변경할 수 있습니다. 나중에 애플리케이션을 시작하려면 이 포트 번호를 기록해 두어야 합니다.

4. **다음**을 선택하면 애플리케이션 사용자 정보 화면이 표시됩니다.

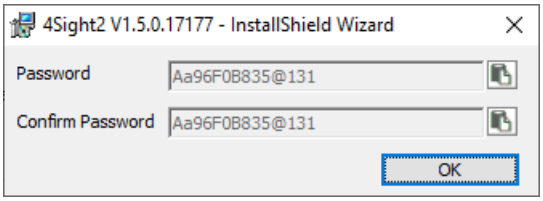


애플리케이션 사용자 정보: 4Sight2 애플리케이션에 액세스하는 데 필요한 슈퍼 사용자 이름과 암호를 입력하는 섹션입니다.

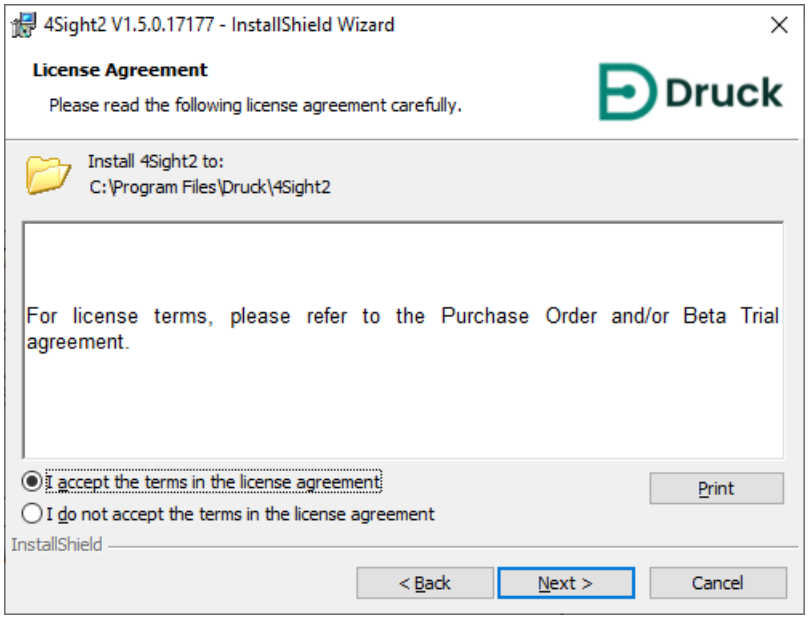
참고: 이 암호는 설치 시 4Sight2 애플리케이션에 액세스할 때 필요합니다.

데이터베이스 사용자 정보: 4Sight2 애플리케이션에서 PostgreSQL 데이터베이스와 통신할 수 있도록 데이터베이스 사용자 이름과 암호를 입력하는 섹션입니다.

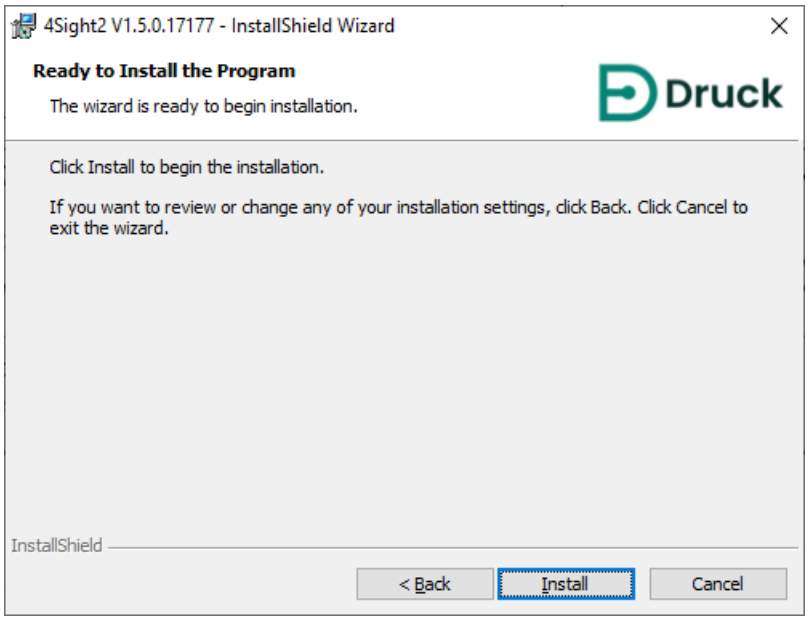
중요: 사용자는 데이터베이스 암호를 적어 두어야 합니다. 암호 정보를 잃어버리면 액세스가 거부되거나 데이터가 손실될 수 있습니다. 데이터베이스 슈퍼 사용자 암호를 업데이트하려면 사용자 기본 암호 확인란을 선택 취소하십시오. 기본 암호를 유지하거나 입력한 새 암호를 보려면 (암호 표시) 아이콘을 선택하십시오. 암호를 클립보드에 복사하려면 (클립보드에 복사) 아이콘을 사용하십시오.



5. 라이선스 약관을 읽은 다음,"라이선스 약관에 동의함"라디오 버튼을 선택하고 **다음**을 클릭합니다.

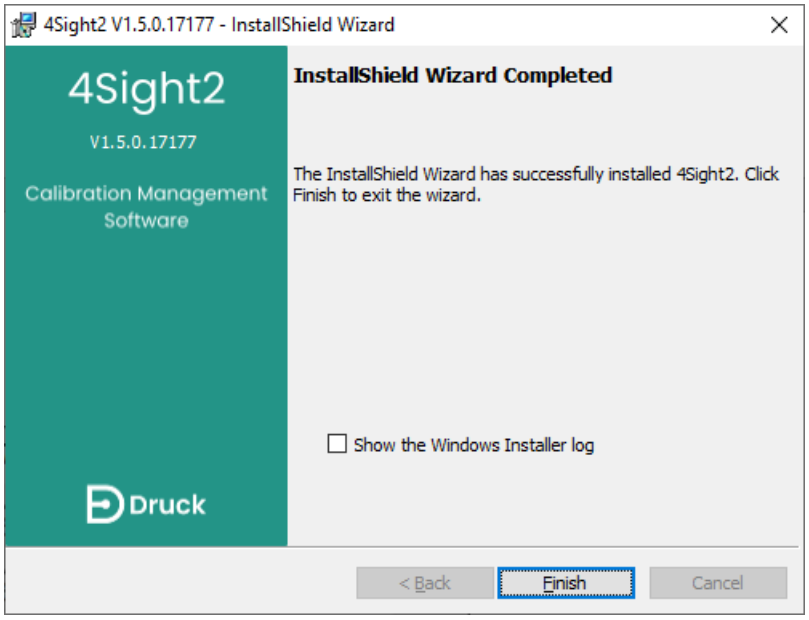


6. **설치**를 클릭하여 설치를 시작합니다. 4Sight2 애플리케이션 및 데이터베이스와 관련된 모든 소프트웨어 패키지가 설치됩니다.



축하합니다. 이제 4Sight2 애플리케이션이 설치되었습니다.

7. **완료** 버튼을 클릭하여 창을 닫고 다음 섹션의 지시에 따라 4Sight2 애플리케이션에 로그인하십시오.



서버에서 로컬로 4Sight2에 로그인하려면 다음으로 이동합니다.

http://컴퓨터이름 또는 IP주소:포트번호/애플리케이션이름

- **컴퓨터이름 –** 4Sight2 애플리케이션이 설치된 PC의 이름입니다. 이 PC의 이름은 이 PC를 마우스 오른쪽 버튼으로 클릭하고 속성을 선택하여 찾을 수 있습니다.
- **IP주소** - 4Sight2 애플리케이션이 설치된 PC의 IP 주소입니다. 이 IP 주소는 Windows 명령 창에서 'ipconfig'를 실행하여 찾을 수 있습니다.
- **포트번호 –** 애플리케이션 설치 중에 Tomcat 포트 번호 필드에 입력한 번호입니다.
- **애플리케이션이름 –** 애플리케이션 설치 중에 애플리케이션 이름 필드에 입력한 이름입니다.

4Sight2 테스트 장비 통신기 설치

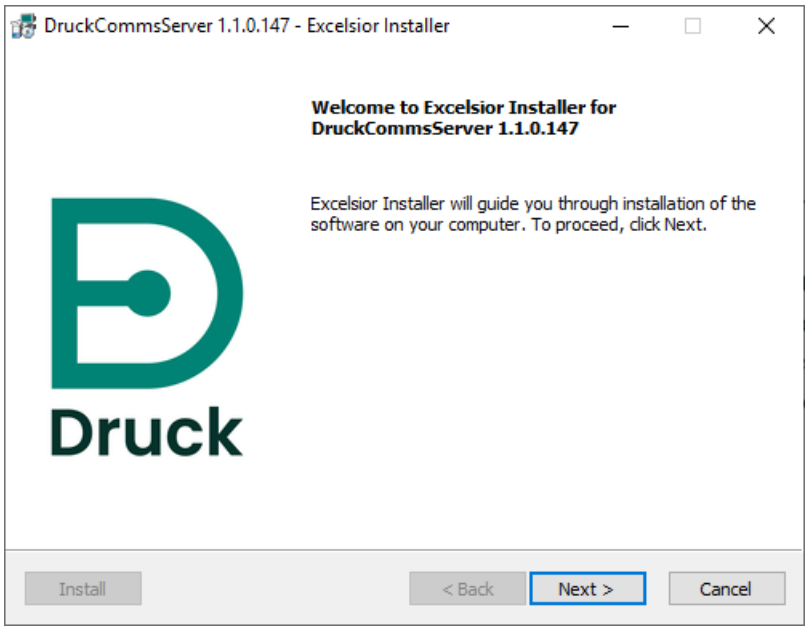
4. 4Sight2 테스트 장비 통신기 설치

1. 테스트 장비 통신기는 Druck 기기가 4Sight2 애플리케이션과 통신할 수 있는 수단을 제공합니다. 테스트 장비 통신기는 4Sight2 설정 폴더에서 설치하거나 4Sight2 초기 장치 통신을 통해 다운로드할 수 있습니다. 설정 파일에서 테스트 장비 통신기를 사용할 수 없는 경우 4Sight2 애플리케이션이 실행 중이고 범위가 생성되었으면 관리자 사용자는 4Sight2 메뉴를 사용해 교정 > 휴대용으로 이동합니다. 범위 및 생성 도움말은 4Sight2 사용 설명서를 참조하십시오. 테스트 장비 드롭다운 옆의 새로 고침 버튼을 선택합니다. 테스트 장비 통신기가 실행되고 있지 않은 경우 다음 메시지가 표시됩니다.

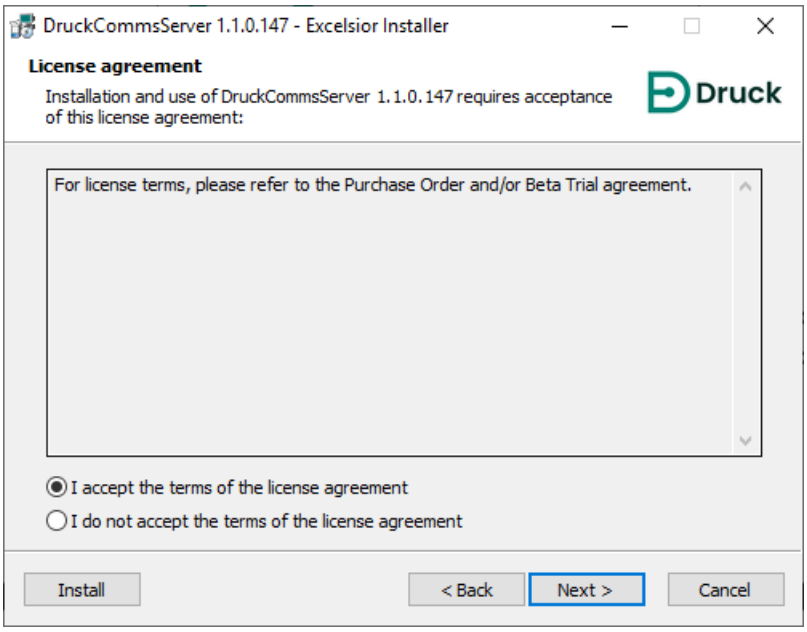
   테스트 장비와 통신할 수 없습니다.

   테스트 장비 통신기 패키지를 다운로드합니다. 다운로드 이후 압축을 풀고 setup.exe를 실행하여 설치하십시오. 설치 지침 또는 문제 해결은 설치 설명서를 참조하십시오. 도움이 필요한 경우 관리자에게 문의하십시오.

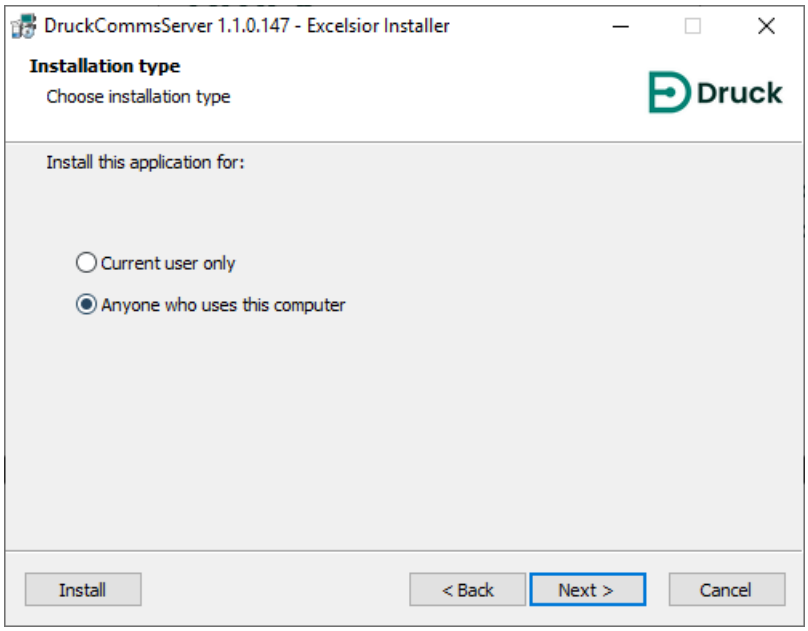
2. **다운로드**를 선택하여 테스트 장비 통신기 설정 파일을 가져옵니다.
3. 테스트 장비 통신기 설정 파일이 CommsServerInstall Zip 파일로 나타납니다. Comms Server Zip을 다운로드한 후에는 4Sight2 설치 전 및 후에 동일한 단계를 따를 수 있습니다.
4. Comms Server Zip 파일에서 파일을 추출하고 setup.exe 파일을 더블 클릭해 설치 프로그램을 실행합니다.
5. DruckCommsServer 설치 프로그램이 표시됩니다. 설치 프로그램의 지침을 따르거나 이 가이드를 따릅니다.



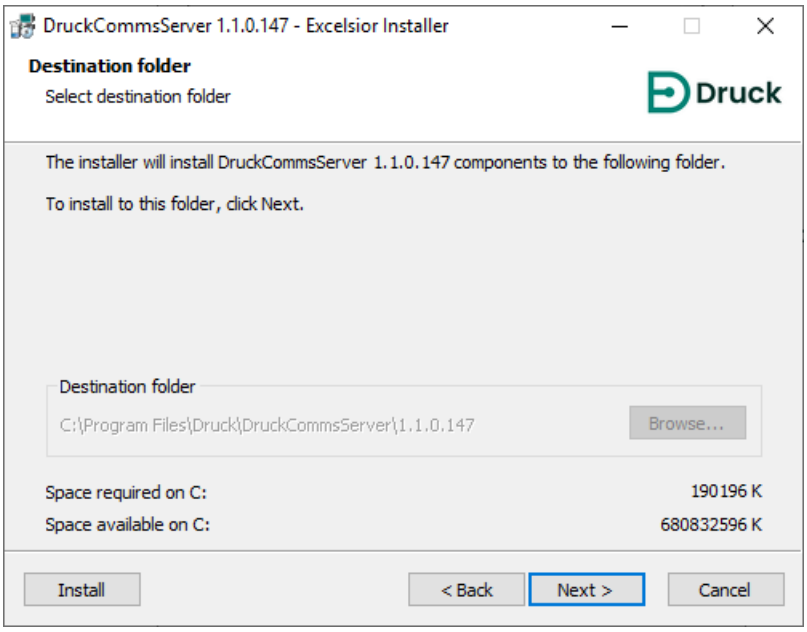
6. **다음**을 선택하여 라이선스 동의 화면을 표시하고 약관을 빠짐없이 읽은 다음 **라이선스 계약의 약관에 동의합니다**를 선택하고 **다음**을 선택해 계속 진행합니다.



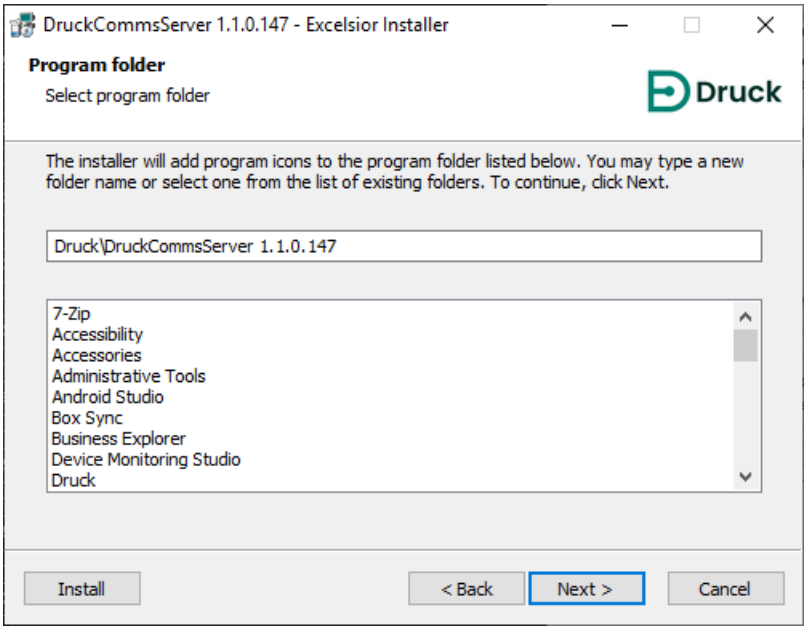
7. 설치 유형 화면에서 CommsServer를 이 PC의 모든 사용자에 대해 설치할지 아니면 현재 사용자에 대해서만 설치할지를 선택합니다.



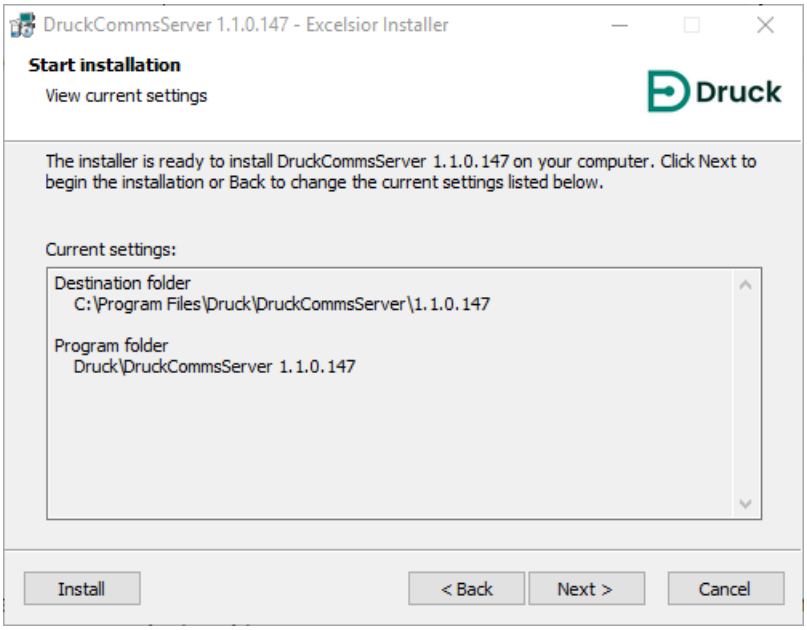
8. 대상 폴더 화면에 DruckCommsServer가 설치될 폴더가 표시됩니다. 기본적으로 이 폴더의 경로는 C:\Program Files\Druck\DruckCommsServer\[application_version]입니다.



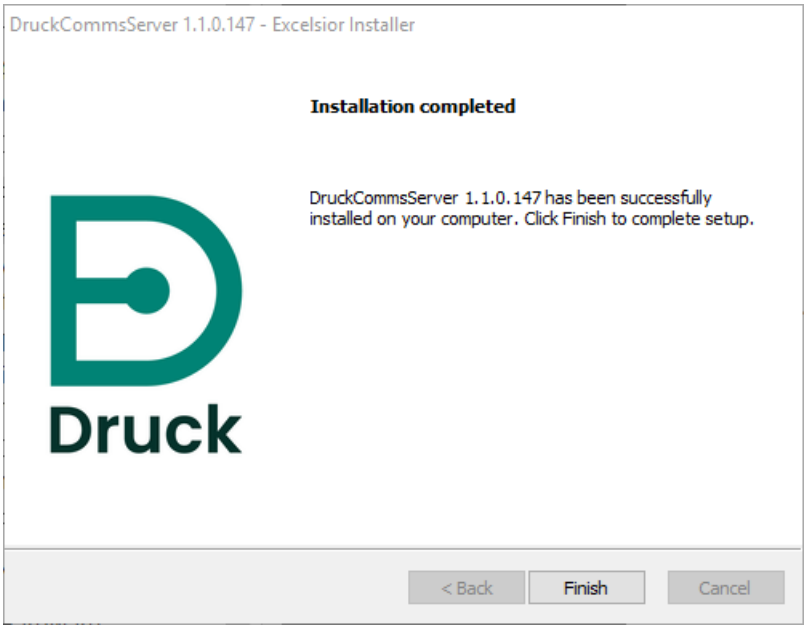
9. 프로그램 폴더 화면에서 설치 프로그램이 프로그램 아이콘을 추가할 프로그램 폴더의 위치를 선택할 수 있습니다.



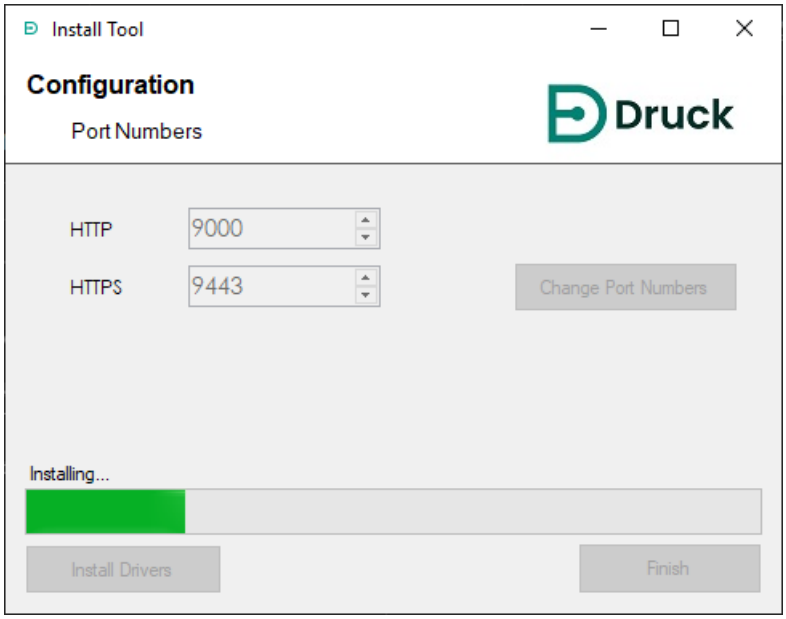
10. 설치 시작 화면이 표시되면 **다음**을 선택하여 설치를 시작합니다.



11. 설치가 완료되면 **완료**를 선택합니다.

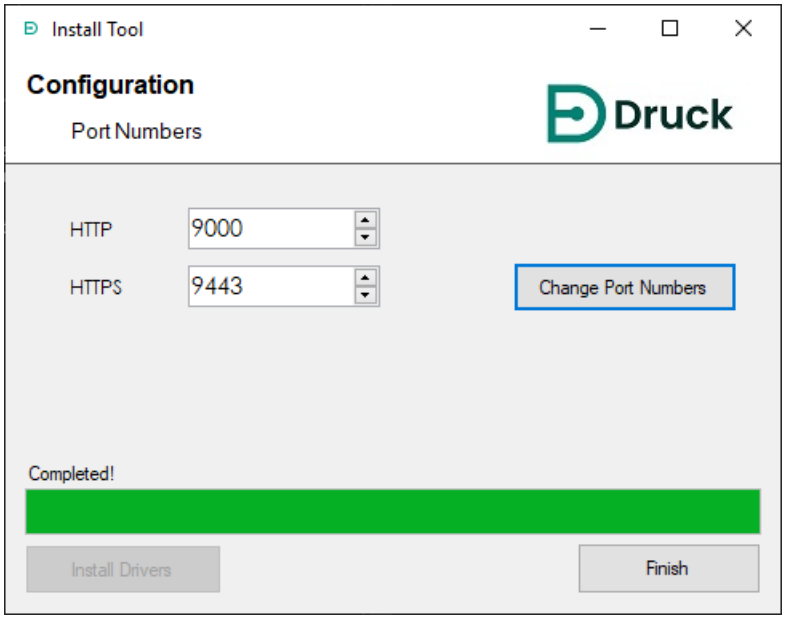


12. 그러면 필요한 추가 드라이버를 설치할 수 있도록 CommsServer 설치 도구 애플리케이션이 표시됩니다.



13. 4Sight2에서 대체 포트 이름을 사용하고 있는지 확실치 않을 경우 관리자 사용자에게 문의하십시오.

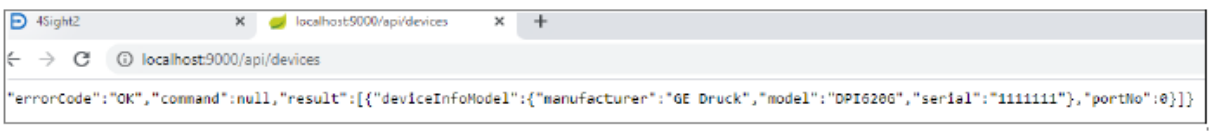
참고: 설치 후에 설치 도구를 별도로 실행하여 이러한 포트 번호를 재구성할 수 있습니다.



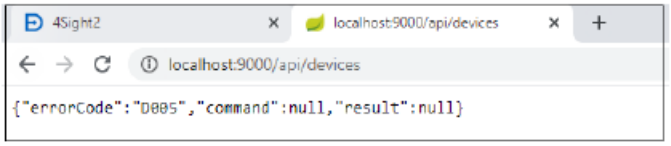
14. 다음 URL을 웹 브라우저에 입력하여 테스트 장비 통신기 설치를 테스트합니다.

    http:/localhost:[http port number used above default 9000]/api/devices

연결한 장치의 목록이 웹 브라우저에 표시되어야 합니다.



장치가 연결되지 않은 경우 다음과 같은 내용이 표시되어야 합니다.



참고: 온도 교정기에 필요한 드라이버는 자동으로 구성되지 않습니다. 섹션 4.3 온도 교정기 드라이버 구성을 참조하십시오.

15. 장치 드라이버 설치가 실패한 경우 다음 섹션의 단계를 사용하여 필요한 드라이버를 수동으로 구성합니다.

4.1 수동 드라이버 구성

IT 보안 정책 설정으로 인해 Druck 드라이버가 설치 시 자동 구성되지 않을 수 있습니다. 이것은 4Sight2가 다양한 장비와 통신할 수 없는 경우 명백합니다.

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

또는

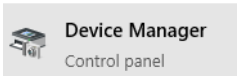
Druck 드라이버를 수동으로 구성하면 이 문제가 해결됩니다. 이에 대해 확실하지 않거나 추가적인 도움이 필요한 경우 로컬 IT 담당자에게 문의하십시오.

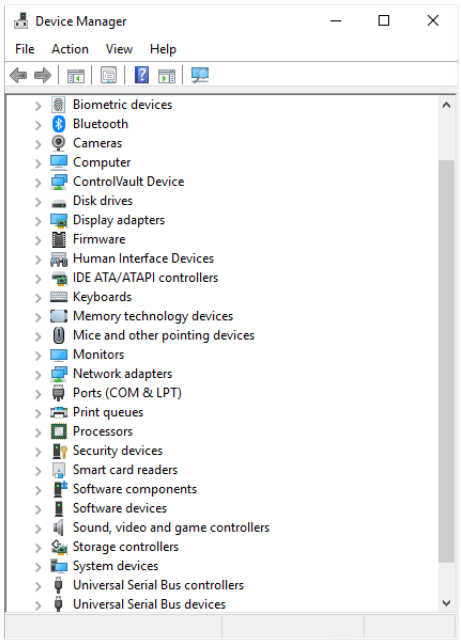
4.1.1 전제 조건

드라이버를 설치하려면 4Sight2 애플리케이션이 설치되어 있거나 시스템에서 4Sight2 애플리케이션에 액세스할 수 있어야 합니다. 드라이버를 설치하기 전에 컴퓨터에서 4Sight2 애플리케이션에 로그인할 수 있는지 확인하십시오.

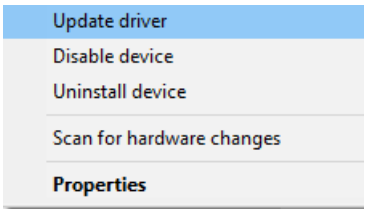
드라이버를 수동으로 설치하려면 다음 단계를 수행하십시오.

1. 바탕화면에서 장치 관리자를 검색해서 실행합니다.

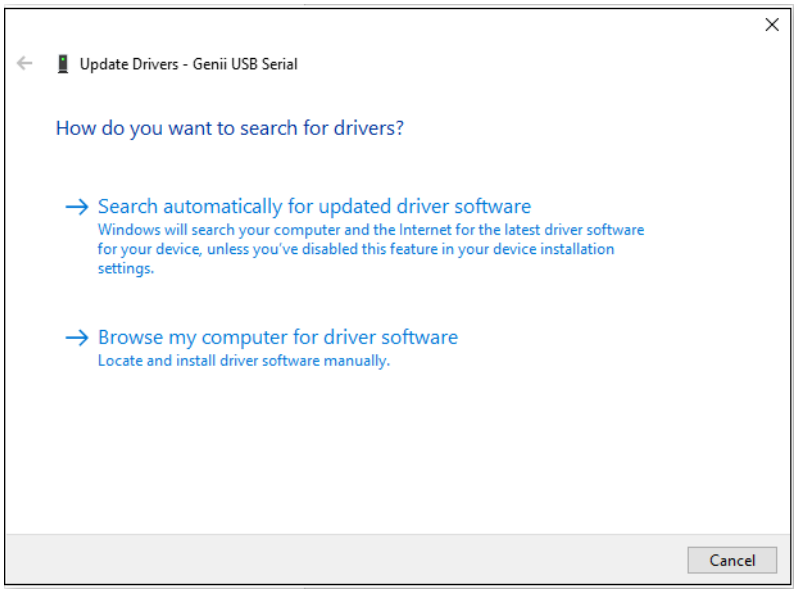




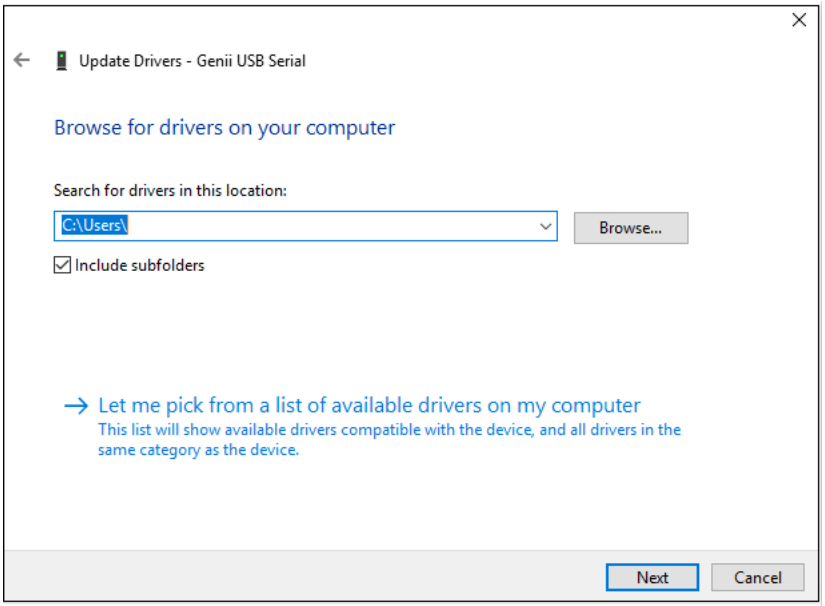
2. USB 장치 목록에서 스크롤하여 구성되지 않은 장치(알 수 없는 장치 또는 기타 장치)를 찾습니다. 마우스 오른쪽 버튼을 클릭하고 **드라이버 업데이트**를 선택합니다.



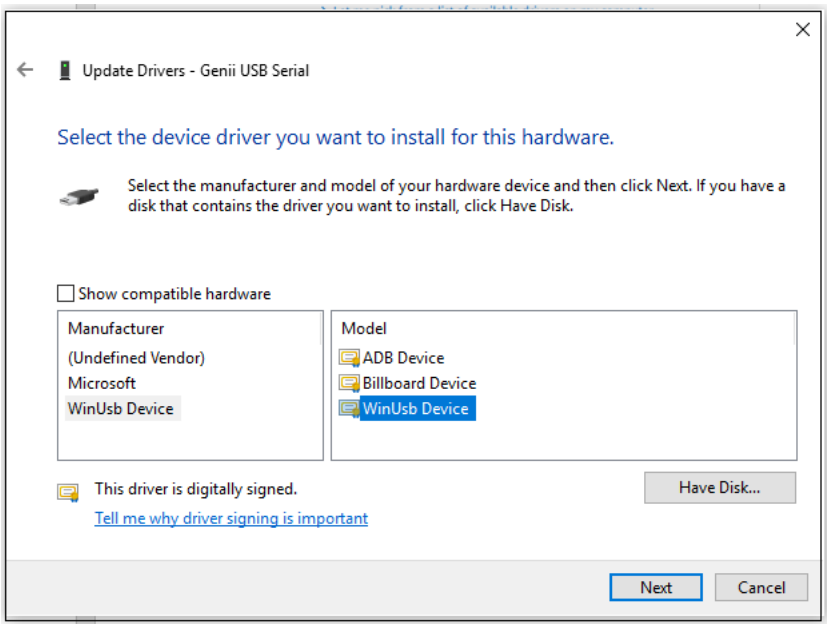
3. **내 컴퓨터에서 드라이버 소프트웨어 찾아보기**를 선택합니다.



4. 컴퓨터에서 **사용 가능한 드라이버 목록에서 직접 선택**을 선택합니다.

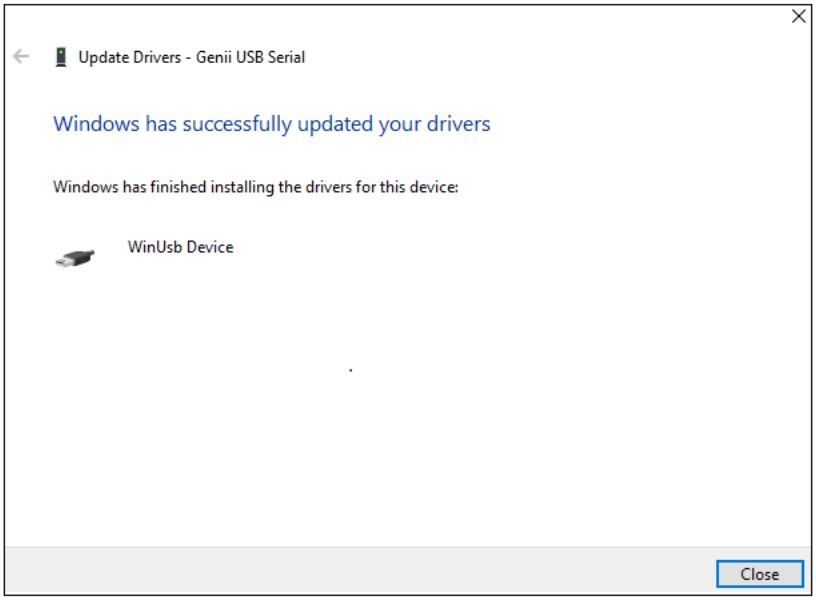


5. **호환 가능한 하드웨어 표시**를 선택 해제하고 제조업체에 대해 **WinUsb 장치**를 선택하고 모델에 대해 **WinUsb 장치**를 선택합니다.



6. 다음 경고가 표시됩니다. **예**를 클릭합니다.

7. "Windows에서 드라이버를 성공적으로 업데이트했습니다"가 표시됩니다.



장치를 처음 연결하는 경우 각 장치 범주에 대해 위의 단계를 반복합니다.

예를 들어, PACE와 Genii를 처음 연결하는 경우 처음에 PACE와 Genii에 대해 각각 따로 위의 단계를 반복해야 할 수 있습니다. PACE와 Genii의 모든 추가 인스턴스는 이런 설정을 수행하지 않아도 잘 작동합니다. 그러나 나중에 DPI611/612와 같은 다른 범주의 장치를 연결할 경우에는 이 장치 범주에 대해 다시 단계를 반복해야 합니다.

4.2 테스트 장비 통신기 테스트

1. 4Sight2에 기술자로 로그인합니다.
2. **자산 >> 작업 목록**으로 이동합니다.
3. 하나 이상의 범위를 선택하여 이러한 범위를 휴대용 또는 자동 교정 워크플로에 할당합니다.
4. **새로 고침** 버튼을 클릭합니다.

5. **테스트 장비** 드롭다운을 클릭합니다. 목록에 연결된 장치가 표시되면 테스트 장비 통신기가 올바르게 구성된 것입니다.

4.3 온도 교정기 드라이버 구성

온도 교정기가 4Sight2와 통신할 수 있게 하려면 FTDI 드라이버를 설치해야 합니다.

1. 이 링크를 사용해 FTDI 드라이버를 다운로드합니다. https://www.ftdichip.com/Drivers/VCP.htm.
2. Zip에서 다운로드한 파일을 추출하고 시스템의 알고 있는 위치에 저장합니다.
3. 시스템에서 Windows 장치 관리자로 이동합니다.
4. 장치 목록에서 포트(COM & LPT)를 선택해 온도 교정기를 봅니다.
5. 온도 교정기를 마우스 오른쪽 버튼으로 클릭하고 드라이버 업데이트를 선택합니다.
6. 내 컴퓨터에서 드라이버 소프트웨어 찾아보기를 선택합니다.
7. 이 위치에서 드라이버 검색이라는 검색 상자 옆의 찾아보기를 선택합니다.
8. 폴더에서 추출한 드라이버 다운로드를 포함하는 폴더를 선택합니다.
9. 다음을 선택한 다음 닫기를 선택합니다.
10. 이제 드라이버가 설치됩니다.
11. 4Sight2에서 온도 교정기와의 통신을 테스트하려면 자동 교정으로 이동하여 온도 교정기를 입력 컨트롤러로 선택할 수 있는지 확인합니다. 또는 섹션 4의 14단계를 다시 실행합니다.

배포 가이드

5. 배포 가이드

5.1 배포 아키텍처

일반적인 아키텍처에는 Tomcat Web Server 내에서 실행되는 4Sight2 웹 애플리케이션 및 UAA(User Authentication and Authorization) 서버와 동일한 시스템에서 실행되는 PostgreSQL 데이터베이스가 포함됩니다.

Browser Client Web 애플리케이션은 4Sight2 서버에 연결되며, 연결된 후에는 PostgreSQL 데이터베이스에서 정보를 저장하고 검색합니다.

5.2 물리적 배포

당사는 4Sight2를 설치하는 사용자가 이미 사이버 보안 조치를 취했으며 다음을 포함한 사용자 보안 정책을 준수한다고 가정합니다.

- 서버는 관리 규정에 따라 물리적인 접근이 제한된 안전한 위치에 있습니다.
- 서버 액세스 제어는 제한된 승인 액세스로 보호됩니다.
- 서버 네트워크는 방화벽으로 보호되어 알려진 포트의 잘 알려진 애플리케이션에 대해서만 제한적인 액세스가 허용됩니다.
- 애플리케이션은 자체 컨텍스트에서 실행되며 자체 폴더의 데이터베이스와 파일 시스템에만 액세스할 수 있습니다.

5.3 네트워크

클라이언트는 이더넷 연결을 통해 또는 무선 네트워크를 통해 웹 브라우저를 사용하여 연결됩니다. 무선 대역폭과 연결된 장치 수에 따라 무선 네트워크에 잠재적인 지연 시간이 있을 수 있습니다.

브라우저에 설치된 모든 브라우저 플러그인과 확장 프로그램을 비활성화하거나 제거하는 것이 좋습니다.

4Sight2 웹 서버가 인터넷에 노출되어서는 안 되며, 필요한 액세스 권한은 Intranet 또는 VPN을 통해 제공해야 합니다.

5.4 배포 순서

4Sight2 애플리케이션을 사용하려면 PostgreSQL, Tomcat 및 Java Runtime을 먼저 설치해야 합니다. PostgreSQL은 별도의 패키지로 설치되지만 다른 것들은 애플리케이션과 함께 패키지로 제공됩니다. 따라서 PostgreSQL이 이미 사용자 시스템에 설치된 경우 슈퍼 사용자 암호만 있으면 이 프로그램에 연결하고 구성할 수 있습니다.

설치하려면 시스템에 Windows 관리자 권한이 필요합니다. 설치 전에 사용자에게 PostgreSQL 슈퍼 사용자 암호는 물론, 애플리케이션 관리자 사용자 이름 및 암호와 데이터베이스 사용자 이름 및 암호가 있어야 합니다.

PostgreSQL 슈퍼 사용자 암호는 PostgreSQL 서버 내에서 데이터베이스와 기타 구조를 만드는 데 필요합니다. 애플리케이션 관리자는 애플리케이션의 첫 사용자이며, 다른 사용자를 만들고 여러 가지 역할을 할당할 책임이 있습니다. 데이터베이스 사용자는 4Sight2 및 UAA 데이터베이스에 액세스할 수 있습니다. 이러한 사용자 이름 자격 증명은 데이터베이스에 액세스하는 데 사용됩니다.

애플리케이션은 시스템 포트에 게시됩니다. 기본 포트는 8083이고, 사용자는 설치할 때나 나중에 포트를 변경할 수 있습니다. Tomcat의 기본 애플리케이션 컨텍스트는 4Sight2입니다.

Microsoft 또는 CIS 지침에 따라 운영 체제 강화 절차를 수행하여 OS를 강화합니다. 설치 절차에서는 4Sight2 서버를 설치하기 전에 PostgreSQL을 설치하는 과정을 사용자에게 안내합니다.

USB 포트를 통해 테스트 장비를 연결할 경우 테스트 장비 통신기가 클라이언트 시스템에 설치됩니다. 테스트 장비 통신기가 아직 시스템에 설치되지 않은 경우 4Sight2 서버에서 테스트 장비 통신기를 다운로드하여 시스템에 설치하라는 메시지가 사용자에게 표시됩니다. 테스트 장비 통신기는 포트 9000을 수신하고 보안 레이어에서만 통신할 수 있습니다.

5.5 배포 후 작업

5.5.1 사용자 및 그룹 추가

관리자는 애플리케이션에서 감독자, 선임 기술자, 기술자, 감사자 같은 다양한 사용자를 생성할 책임이 있습니다. 관리자는 이들을 기본 제공되는 다양한 기본 그룹에 할당할 수 있습니다. 더 세분화된 액세스 권한이 필요한 경우 관리자가 사용자 지정 그룹을 만들어 해당 그룹에 특정 액세스 권한을 할당할 수 있습니다.

5.5.2 기본 암호

4Sight2에서는 tomcat 사용자에 대해 “C:\Program Files\Druck\4Sight2\<<latest folder number>>\apache-tomcat\conf\tomcat-user.xml” 파일에 있는 하드코딩된 기본 암호를 사용하고 있습니다.

기본 암호를 변경하고 항상 암호 모범 사례를 준수하는 암호를 사용할 것을 권장합니다.

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

애플리케이션의 안전을 보장하기 위해 모범 사례를 따랐습니다. 추가적인 보안을 위해서는 다음 작업을 수행하십시오.

구성 파일 및 폴더는 기본적으로 액세스 권한이 있는 서비스 및 시스템으로만 보호됩니다. 관리자 사용자만 C:\Program Files\Druck\4Sight2\<<latest folder number>>\apache-tomcat\conf 폴더에 대한 읽기/쓰기 액세스 권한을 갖고 있으므로 아래 작업을 수행하기 전에 관리자 사용자 자격 증명으로 명령 프롬프트를 엽니다.

5.5.3 보안 통신

이 섹션에는 자체 서명 인증서를 사용하는 보안 모드(즉, SSL 모드)에서의 4Sight2 구성 지침이 나와 있습니다. 계속하기 전에 4Sight2 애플리케이션에 정의된 가정과 조건을 읽어 보시기 바랍니다. 자체 서명 인증서는 4Sight2에서 SSL을 활성화하는 한 가지 방법입니다. 또는 Symantec, Digicert 등과 같은 여러 벤더에서 제삼자 CA 인증서를 구입할 수 있습니다.

참고: SSL을 활성화한다고 해서 애플리케이션의 보안이 보장되는 것은 아닙니다. 이는 안전한 웹 애플리케이션을 구축하기 위한 가장 일반적인 관행 중 하나입니다.

5.5.3.1 가정 및 경고

아래의 지침이 작용하도록 다음과 같이 가정합니다.

자체 서명 인증서를 생성하는 데 Windows용 OpenSSL 소프트웨어가 필요합니다. 4Sight2는 귀하의 조직, 국가/지역법 및 규제 지침에서 OpenSSL 소프트웨어를 사용하도록 허용하는 것으로 가정합니다.

- Keytool은 Java에서 제공하는 키 및 인증서 관리 유틸리티로, https 구성에 관련된 다양한 구성요소를 생성하는 데 사용됩니다. 4Sight2는 귀하의 조직, 국가/지역법 및 규제 지침에서 Keytool 유틸리티를 사용하도록 허용하는 것으로 가정합니다.
- 아래의 구성을 실행하려면 관리자 권한이 필요합니다. 관리자 권한을 얻는 방법에 대한 자세한 내용은 현지 IT 부서에 문의하십시오.
- 아래의 단계를 수행하려면 컴퓨터 프로세스에 대한 기본적인 이해가 필요하므로, 현지 IT 부서의 지침에 따라 이러한 단계를 수행하는 것이 좋습니다.
- 호스트 이름, 암호, URL 및 폴더 경로 등 본 문서에 나와 있는 콘텐츠는 참조용으로만 사용됩니다. 실행하기 전에 명령을 적절히 수정해야 합니다.
- 다음 섹션에서는 두 가지 시나리오를 다룹니다. 첫째는 서버와 클라이언트가 동일한 시스템에 있는 경우이고, 둘째는 서버와 클라이언트가 서로 다른 시스템에 있는 경우(즉, 클라이언트가 여러 개인 시나리오)입니다.

5.5.3.2 Https에서 4Sight2 애플리케이션을 구성하는 단계

1. Windows 서비스에서 4Sight2를 중지합니다.
2. **관리자 모드**에서 명령 프롬프트를 엽니다.
3. 다음 명령을 실행하여 4Sight2 설치 디렉터리 내의 아래 폴더로 이동합니다.
   cd "C:\Program Files\Druck\4Sight2\<<latest folder number>>\apache-tomcat\conf"
4. 명령 프롬프트에서 다음 명령을 실행하여 keytool이 있는지 확인합니다. **Keytool** -?
   없는 경우 아래와 같이 4Sight2 설치 폴더 내 JRE bin으로 환경 경로를 설정합니다. 설치 폴더를 기준으로 올바른 경로를 업데이트합니다.
   C:\Program Files\Druck\4Sight2\<<latest folder number>>\jre\bin
   Set "Path=%Path%;C:\Program Files\Druck\4Sight2\<<latest folder number>>\jre\bin"
5. 새 인증서를 만들 경우 6번 항목으로 건너뛰고, 그렇지 않고 인증서가 이미 있는 경우 다음을 수행합니다.
   a. Java 키 저장소에 4Sight.jks 인증서 파일이 있는지 확인합니다.
   keytool -list -alias <<호스트 이름>> -storepass <<키 암호>> -keystore 4Sight.jks
   b. 인증서가 이미 설치되어 있으면 제거합니다.
   keytool -delete -noprompt -alias <<호스트 이름>> -storepass <<키 암호>> -keystore 4Sight.jks
   c. 4SightV2PublicKey.cer 파일이 있는지 확인하고 삭제합니다.
   del "../../app/Certificate/4SightV2PublicKey.cer"
   d. 인증서가 Java의 cacert에 이미 있는지 확인합니다.
   keytool -list -alias <<호스트 이름>> -storepass changeit -keystore "../../jre/lib/security/cacerts"
   e. Java 저장소에 있으면 인증서를 삭제합니다.
   keytool -delete -noprompt -alias <<호스트 이름>> -storepass changeit -keystore "../../jre/lib/security/cacerts" -file "../../app/Certificate/4SightV2PublicKey.cer"

6. 다음을 실행하여 새 인증서를 만듭니다.

   keytool -genkey -trustcacerts -keyalg "RSA" -keysize 2048 -validity 1095 -keypass <<키 암호>> -alias <<호스트 이름>> -keystore 4Sight.jks -storepass <<저장소 암호>> -dname "CN=%COMPUTERNAME%, Ou=<<조직 구성 단위>>, O=<<조직>>, L=<<위치>>, S=<<시/도>>, C=<<국가 이니셜>>" -ext eku:critical=sa

7. 4SightV2PublicKey.cer 파일로 인증서를 내보냅니다(이름 또는 경로 변경 금지).

   keytool -export -alias <<호스트 이름>> -keystore 4Sight.jks -storepass <<저장소 암호>> -storetype JKS -file "C:\Program Files\Druck\4Sight2\<<latest folder number>>\app\Certificate\4SightV2PublicKey.cer"
   명령이 성공적으로 실행되면 다음과 같은 메시지가 표시됩니다. "파일에 저장된 인증서 C:\Program Files\Druck\4Sight2\<<latest folder number>>\app\Certificate\4SightV2PublicKey.cer"가 표시됩니다.

8. 인증서를 Java CACert 파일로 가져옵니다.

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

명령이 성공적으로 실행되면 "인증서가 키 저장소에 추가되었습니다."라는 메시지가 표시됩니다.

9. 인증서를 Tomcat 구성 파일에 입력합니다.

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

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

   c. http 연결을 비활성화하려면 다음 섹션을 주석 처리합니다.
   <connectionTimeout="20000" maxSwallowSize="104857600" port="8083" protocol="HTTP/1.1" redirectPort="8443" relaxedPathChars=""[\]^`{|}+" relaxedQueryChars="&quot;[\]^`{|}+"/>

참고: 이 부분을 주석 처리하지 않으면 애플리케이션이 작동하지 않습니다.

10. 이 시점에서 4Sight2 애플리케이션 Https 구성이 완료됩니다.
11. 위에서 완료한 구성을 테스트하려면 Windows 서비스에서 4Sight2 서비스를 다시 시작합니다.
12. Google Chrome을 열고 브라우저 캐시를 지운 뒤 브라우저를 다시 시작합니다.
13. 브라우저에 다음 URL, 즉 https://<<host-name>>:8443/4sight2를 입력합니다.

- URL을 처음 로드하는 데 시간이 오래 걸릴 수 있습니다.
- "연결이 비공개가 아닙니다."라는 메시지가 화면에 표시됩니다.
- **고급** 버튼 >> **XX로 이동** 링크를 클릭합니다.
- 4Sight2 화면이 표시되지 않으면 **다시 로드** 버튼을 클릭합니다.
- 4Sight2 페이지로 리디렉션됩니다.

- mmc에 인증서를 등록하면 결국 사라지게 될 "안전하지 않음" 오류가 주소 표시줄에 나타납니다.

5.5.3.3 서버 시스템에 설치된 경우 Https에서 DruckCommsServer를 구성하는 단계

명령을 실행하기 전에 << >>의 값을 적절한 데이터로 바꿉니다.

1. Windows 서비스에서 DruckCommsServer를 중지합니다.
2. **관리자 모드**에서 명령 프롬프트를 엽니다.
3. 명령 프롬프트에서 다음 명령을 실행하여 keytool이 있는지 확인합니다. **Keytool -?**

   없는 경우 아래와 같이 4Sight2 설치 폴더 내 JRE bin으로 환경 경로를 설정합니다.
   설치 폴더를 기준으로 올바른 경로를 업데이트합니다.
   C:\Program Files\Druck\4Sight2\<<latest folder number>>\jre\bin
   Set "Path=%Path%;C:\Program Files\Druck\4Sight2\<<latest folder number>>\jre\bin"
4. 다음 명령을 실행하여 DruckCommServer 설치 디렉터리 내의 아래 폴더로 이동합니다.

   cd "C:\Program Files\Druck\DruckCommsServer\<< 통신 서비스 버전 >>"
5. 인증서가 이미 있는지 확인하려면 다음을 수행합니다.

   a. 인증서가 Java의 cacert에 이미 있는지 확인합니다.
   keytool -list -alias tomcat -storepass changeit -keystore cacerts

   b. Java 저장소에 있으면 인증서를 삭제합니다.
   keytool -delete -noprompt -alias tomcat -storepass changeit -keystore cacerts

   c. 기본값과 함께 제공되는 CommsServer에서 사전 구성된 인증서를 삭제합니다.
   del 4Sight.jks
   del 4SightV2DeviceMngr.pfx
6. 다음을 실행하여 새 인증서를 만듭니다.

   keytool -genkey -trustcacerts -keyalg "RSA" -keysize 2048 -validity 1095 -keypass <<키 암호>> -alias tomcat -keystore CommServer.jks -storepass <<저장소 암호>> dname "CN=localhost, Ou=<<조직 구성 단위>>, O=<<조직>>, L=<<위치>>, S=<<시/도>>, C=<<국가 이니셜>>" -ext eku:critical=sa
7. DruckCommServer.cer 파일로 인증서를 내보냅니다.

   keytool -export -alias tomcat -keystore CommServer.jks -storepass <<저장소 암호>> -storetype JKS -file DruckCommServer.cer
   명령이 성공적으로 실행되면 다음과 같은 메시지가 표시됩니다.
   "DruckCommServer.cer 파일에 저장된 인증서"가 표시됩니다.
8. 통신 서버 인증서를 Java CACert 파일로 가져옵니다.

   keytool -import -noprompt -trustcacerts -alias tomcat -storepass changeit -keystore cacerts -file DruckCommServer.cer
   명령이 성공적으로 실행되면 "인증서가 키 저장소에 추가되었습니다."라는 메시지가 표시됩니다.

9. 4Sight 인증서를 Java CACert 파일로 가져옵니다.

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

   명령이 성공적으로 실행되면 "인증서가 키 저장소에 추가되었습니다."라는 메시지가 표시됩니다.

10. DruckCommsServer의 application.properties에 대한 키 저장소 암호를 편집합니다.

    다음 파일, 즉

    C:\Program Files\Druck\DruckCommsServer\<<통신 서비스 버전>>\application.properties를 열고 다음 줄을 변경합니다.

    keystore = CommServer.jks

    key-store.password= << 저장소 암호 >>

    참고: **<< 저장소 암호 >>**는 6단계에서 사용된 **저장소 암호**를 가리킵니다.

11. 4Sight2 및 DruckCommsServer 서비스를 다시 시작합니다.

5.5.3.4 클라이언트 시스템에 설치된 경우 HTTPs에서 DruckCommsServer를 구성하는 단계

1. Keytool 유틸리티는 Java와 함께 패키지로 제공되므로, Java를 설치하지 않고도 시스템에 Java를 설치하거나 Java keytool의 가용성을 직접 확인할 수 있습니다.
2. Windows 서비스에서 DruckCommsServer를 중지합니다.
3. **관리자 모드**에서 명령 프롬프트를 엽니다.
4. 명령 프롬프트에서 다음 명령을 실행하여 keytool이 있는지 확인합니다. **Keytool -?**

   없는 경우 Java가 시스템에 설치되어 있으면 JRE bin으로 환경 경로를 설정하거나, 아래와 같이 keytool 경로를 설정할 수 있습니다.

   설치 폴더를 기준으로 올바른 경로를 업데이트합니다.

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

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

5. 4Sight 애플리케이션이 설치된 Server 시스템에서 **4SightV2PublicKey.cer** 파일을 가져옵니다. 이 파일은 아래와 같은 서버에 있습니다.

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

6. 이 **4SightV2PublicKey.cer** 파일을 다음 경로에 복사합니다.

   C:\Program Files\Druck\DruckCommsServer\<< 통신 서비스 버전 >>

7. 이제 섹션 5.5.3.3의 4~8단계를 따릅니다.
8. 4Sight 인증서를 Java CACert 파일로 가져옵니다.

   keytool -import -noprompt -trustcacerts -alias <<서버 호스트 이름>> -storepass changeit -keystore cacerts -file 4SightV2PublicKey.cer

   명령이 성공적으로 실행되면 "인증서가 키 저장소에 추가되었습니다."라는 메시지가 표시됩니다.

9. 이제 섹션 5.5.3.3의 10~11단계를 따릅니다.

5.5.3.5 4Sight2용 자체 서명 인증서를 생성하는 단계

1. Windows용 Open SSL을 다운로드하여 설치합니다.
2. Windows 서비스에서 4Sight2 서비스를 중지합니다.
3. C 드라이브 안에 **4Sight2Certificate**라는 새 폴더를 만듭니다.
   해당 폴더에 대한 관리자 액세스 권한이 있는 경우 위치 또는 폴더 이름을 선택할 수 있습니다.
4. 메모장에서 위 폴더 안에 새 파일을 만들고 해당 파일을 **openssl-ca.cnf**로 저장합니다.
   아래의 콘텐츠를 파일에 복사하고 해당 파일을 저장합니다.

```
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
```

참고: 위의 회사 이름을 업데이트하고 파일을 저장합니다. "인증서 발급자 이름은 관리 콘솔에 나타납니다".

5. 메모장에서 위 폴더 안에 새 파일을 만들고 해당 파일을 **openssl-server.cnf**로 저장합니다.

   아래의 콘텐츠를 파일에 복사하고 해당 파일을 저장합니다.

```
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
```

참고: 위의 호스트 이름 및 IPv4 주소를 업데이트하고 파일을 저장합니다.

6. 관리자 권한으로 명령 프롬프트를 엽니다.
7. 아래를 실행하여 4Sight2Certificate 폴더로 이동합니다.

   cd "<<4Sight2Certificate의 전체 경로>>"
8. 아래의 명령을 실행하여 OpenSSL bin 폴더 경로 변수를 설정합니다.

   Set path=%path%;"<<openssl의 bin 폴더>>"
   기본 경로의 예:
   Set Path=%Path%;"C:\Program Files\OpenSSL-Win64\bin"
9. 아래의 명령을 실행하여 JRE bin 폴더 경로 변수를 설정합니다. 참고: 아래의 경로는 다를 수 있습니다.

   Set path=%path%;"C:\Program Files\Druck\4Sight2\<<latest folder number>>\jre\bin"
10. 아래의 명령을 실행하여 cacert.pem 및 cakey.pem 파일을 생성합니다.

    openssl req -x509 -config openssl-ca.cnf -newkey rsa:4096 -days <<Number of days>> -sha256 -nodes -out cacert.pem -outform PEM
    메시지가 나타나면 올바른 인증서 데이터를 입력합니다(예: 국가, 시/도 등).
11. 아래의 명령을 실행하여 servercert.csr 및 serverkey.pem 파일을 생성합니다.

    openssl req -config openssl-server.cnf -newkey rsa:2048 -days <<Number of days>> -sha256 -nodes -out servercert.csr -outform PEM
    메시지가 나타나면 올바른 인증서 데이터를 입력합니다(예: 국가, 시/도 등).
12. 메모장에서 새 파일을 만들고 index.txt로 이름을 지정합니다. 4Sight2Certificate 폴더에 파일을 저장합니다.
13. 메모장에서 새 파일을 만들고 serial.txt로 이름을 지정합니다. 4Sight2Certificate 폴더에 파일을 저장합니다.
    파일을 열고 **01**을 입력한 후 저장하고 파일을 닫습니다.
14. 아래의 명령을 실행하여 servercert.pem 및 serverkey.pem 파일에 새 인증서를 생성합니다.

    openssl ca -config openssl-ca.cnf -policy signing_policy -extensions signing_req -out servercert.pem -infiles servercert.csr
    Y를 입력하여 변경 사항을 커밋합니다. 성공적으로 실행되면 업데이트된 데이터베이스가 표시됩니다.
15. 아래의 명령을 실행하여 기존 키 파일을 PFX 형식으로 패키지를 만듭니다.

    openssl pkcs12 -export -in servercert.pem -inkey serverkey.pem -certfile cacert.pem -name "<<호스트 이름>>" -out <<호스트 이름>>.p12
    암호를 두 번 입력하라는 메시지가 나타납니다.
16. 위에서 언급한 JRE bin 위치(예: tomcat/config 경로)별로 정렬된 Java 키 저장소로 PFX 저장소를 변환합니다.

    keytool -importkeystore -srckeystore <<호스트 이름>>.p12 -srcstoretype PKCS12 -destkeystore "C:\Program Files\Druck\4Sight2\<<latest folder number>>\apache-

tomcat\conf\4Sight.jks"
-deststoretype jks
참고: 두 저장소의 암호를 동일하게 유지하십시오. 위와 같이 tomcat의 구성 폴더에 있는 4Sight.jks를 가리키는지 확인합니다.
대상 키 저장소 암호와 소스 키 저장소 암호를 입력하라는 메시지가 표시됩니다. 명령이 성공적으로 실행되면 "가져오기 명령이 완료되었습니다. 한 항목을 성공적으로 가져왔습니다"라는 메시지가 나타납니다.

17. Java 키 저장소에서 다음 위치에 있는 파일로 인증서를 내보냅니다.
C:\Program Files\Druck\4Sight2\<<latest folder number>>\app\Certificate\4SightV2PublicKey.cer
keytool -export -alias <<호스트 이름>> -keystore "C:\Program Files\Druck\4Sight2\<<latest folder number>>\apache-tomcat\conf\4Sight.jks" -storePass "<<암호>>" -storetype JKS -file "C:\Program Files\Druck\4Sight2\<<latest folder number>>\app\Certificate\4SightV2PublicKey.cer"
참고: 위와 같이 tomcat의 구성 폴더에 있는 4Sight.jks를 가리키는지 확인합니다.
성공적으로 실행되면 파일 메시지에 인증서가 저장됩니다.

18. 4Sight2 설치 디렉터리 내에 있는 cacerts 폴더로 인증서 파일을 가져옵니다.
참고: 경로는 설치 디렉터리 및 4Sight2 버전에 따라 다를 수 있습니다.
keytool -import -noprompt -trustcacerts -alias <<호스트 이름>> -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"
참고: 알 수 없는 이유로 만들려고 하는 별칭이 이미 존재합니다. 아래의 명령을 실행하여 먼저 이 별칭을 삭제한 다음 위의 명령을 실행하여 새 별칭을 만드십시오.
keytool -delete -noprompt -trustcacerts -alias <<호스트 이름>> -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"
이 명령이 성공적으로 실행되면 "인증서가 키 저장소에 추가되었습니다."라는 메시지를 받게 됩니다.

19. server.xml 파일(위치 - C:\Program Files\Druck\4Sight2\<<latest folder number>>\apache-tomcat\conf)을 다음과 같이 변경합니다.

    a. server.xml에서 다음을 입력합니다.

```
<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. http 연결을 비활성화하려면 다음 섹션을 주석 처리합니다.
<connectionTimeout="20000" maxSwallowSize="104857600" port="8083" protocol="HTTP/1.1" redirectPort="8443" relaxedPathChars=""[\]^`{|}+" relaxedQueryChars="&quot;[\]^`{|}+"/>

20. 이렇게 하면 4Sight2에 대한 https 구성이 완료됩니다. 그럼 이제 Windows 서비스에서 4Sight2 서비스가 시작됩니다.

5.5.3.6 서버 시스템에 설치된 경우 DruckCommsServer용 자체 서명 인증서를 구성하는 단계

여기에서는 섹션 5.5.3.5의 단계를 실행하여 4Sight2 애플리케이션을 HTTPs로 성공적으로 변환했으며, **4Sight2Certificate** 폴더에 아래의 파일이 이미 있는 것으로 가정했습니다.

- openssl-server.cnf
- openssl-ca.cnf
- cacert.pem
- cakey.pem
- index.txt
- serial.txt
- 4SightV2PublicKey.cer(이 파일은 C:\Program Files\Druck\4Sight2\<<latest folder number>>\app\Certificate 폴더에 있을 수 있음)

1. 새 폴더를 **CommserverCertificate**로 만들고 위의 파일을 복사한 후 아래와 같이 변경합니다.

- openssl-server.cnf

  req 섹션에서 **default_keyfile** 값을 "**DruckCommServerCertKey.pem**"으로 변경합니다.

  - **server_distinguished_name**에서 **commonName** 값을 "**localhost**"로 변경합니다.
  - **alternate_names**에서 **DNS.1** 값을 "**localhost**"로 변경합니다.
  - **alternate_names**에서 **IP.1** 값을 "**127.0.0.1**"로 변경합니다.
  - 파일을 저장합니다.

- openssl-ca.cnf (내부에서 아무것도 변경 금지)
- cacert.pem (내부에서 아무것도 변경 금지)
- index.txt(내부의 모든 콘텐츠를 삭제하여 빈 파일로 만드십시오.)
- serial.txt(내부의 모든 콘텐츠를 삭제하고 내부에 01 항목만 만드십시오.)

2. Windows 서비스에서 DruckCommsServer 서비스를 중지합니다.
3. 관리자 권한으로 명령 프롬프트를 엽니다.
4. 아래를 실행하여 **CommserverCertificate** 폴더로 이동합니다.

   cd "<<CommserverCertificate의 전체 경로>>"

5. 아래의 명령을 실행하여 OpenSSL bin 폴더 경로 변수를 설정합니다.

   Set path=%path%;"<<openssl의 bin 폴더>>"
   기본 경로의 예:
   Set Path=%Path%;"C:\Program Files\OpenSSL-Win64\bin"

6. 아래의 명령을 실행하여 JRE bin 폴더 경로 변수를 설정합니다. 참고: 아래의 경로는 다를 수 있습니다.

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

7. 이를 완료한 후에는 다음 명령으로 통신 서버 인증서 요청을 만듭니다.

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

   이 명령을 실행하면 **DruckCommServer.csr**에 요청이, **DruckCommServerCertKey.pem**에 비공개 키가 생깁니다.

8. 이제 다음을 수행하여 ca로 csr 요청에 서명합니다.

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

9. 그 후 다음 명령으로 통신 서버용 **tomcat** 별칭으로 PFX 파일을 만듭니다.

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

10. keytool을 사용하여 PFX 저장소를 Java 키 저장소로 변환

    참고: 두 키 저장소의 암호를 동일하게 유지하십시오.

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

11. 이제 인증서를 cacert로 가져옵니다.

    a. 이때 기본적으로 설치하면 제공되는 기존 tomcat 별칭을 삭제합니다.

    keytool -delete -noprompt -trustcacerts -alias tomcat -storepass changeit -keystore "C:\Program Files\Druck\DruckCommsServer\<< 통신 서비스 버전 >>\cacerts"

    b. 기존 tomcat 별칭을 삭제한 후 다음을 통해 인증서를 cacerts로 가져옵니다.

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

12. 이제 통신 인증을 위해 4sight 공용 키를 통신 서버 cacert로 가져와야 합니다. 이렇게 하려면 아래의 명령을 실행합니다.

    keytool -import -noprompt -trustcacerts -alias <<4sight 서버 호스트 이름>> -storepass changeit -keystore "C:\Program Files\Druck\DruckCommsServer\<< 통신 서비스 버전 >>\cacerts" -file "C:\Program Files\Druck\4Sight2\<<latest folder number>>\app\Certificate\4SightV2PublicKey.cer"

13. 위 과정을 모두 완료하면 현재 **CommserverCertificate** 폴더에 **DruckCommServer.pfx** 및 **CommServer.jks**가 생깁니다.

    이러한 파일을 복사한 후 **"C:\Program Files\Druck\DruckCommsServer\<< 통신 서비스 버전 >>\"** 디렉터리에 붙여 넣습니다. 동일한 위치에서 **application.properties**를 편집하고 속성 값을 아래와 같이 변경합니다.

    a. Keystore = CommServer.jks

    b. key-store.password = <<키 저장소 암호>>

    c. key-store.type=JKS

5.5.3.6.1 Windows에서 4sight 및 DruckCommsServer용 인증서 설치

1. 실행을 열고 "mmc"를 입력한 후 Enter 키를 누릅니다.
2. 파일로 이동하여 스냅 인 추가/제거를 선택합니다.

3. 왼쪽 사이드 메뉴에서 인증서를 선택합니다. 추가를 누른 후 컴퓨터 계정 >> 다음 >> 완료를 선택합니다. 그런 다음 확인을 클릭합니다.
4. 인증서(로컬 컴퓨터) 섹션을 확장합니다. 신뢰할 수 있는 루트 인증 기관을 확장합니다.
   그곳에서 인증서 폴더 >> 모든 작업 >> 가져오기를 마우스 오른쪽 버튼으로 클릭합니다.
   cacert.pem >> 다음 >> 완료를 선택합니다.
   이렇게 하면 사용자 지정 CA 기관이 신뢰할 수 있는 기관 아래에 성공적으로 설치됩니다.

이러한 모든 단계를 수행하면 DruckCommsServer 서비스가 시작됩니다.

5.5.3.7 클라이언트 시스템에 설치된 경우 DruckCommsServer용 자체 서명 인증서를 구성하는 단계

DruckCommsServer를 HTTPs로 변환하려면 Java keytool과 OpenSSL 유틸리티가 있어야 합니다.

1. Keytool 유틸리티는 Java와 함께 패키지로 제공되므로, Java를 설치하지 않고도 시스템에 Java를 설치하거나 Java keytool의 가용성을 직접 확인할 수 있습니다.
2. Windows용 OpenSSL을 다운로드하여 설치합니다.
3. 아래의 명령을 실행하여 OpenSSL bin 폴더 경로 변수를 설정합니다.
   Set path=%path%;"<<openssl의 bin 폴더>>"
   기본 경로의 예:
   Set Path=%Path%;"C:\Program Files\OpenSSL-Win64\bin"
4. 아래의 명령을 실행하여 JRE bin 폴더 경로 변수를 설정합니다.
   C:\Program Files\Java\<< Java 버전 >>\bin
   Set Path=%Path%; "C:\Program Files\Java\<< Java 버전 >>\bin"
5. Windows 서비스에서 DruckCommsServer 서비스를 중지합니다.
6. C 드라이브 또는 원하는 다른 드라이브 내에 **CommserverCertificate**라는 새 폴더를 만듭니다.
7. 서버 시스템에서 **4SightV2PublicKey.cer** 4Sight2 공용 인증서 파일(위치 - 경로 C:\Program Files\Druck\4Sight2\<<latest folder number>>\app\Certificate 디렉터리)을 가져와 **CommserverCertificate** 폴더에 복사합니다.
8. 이제 섹션 5.5.3.5에서 4, 5단계를 수행하여 **openssl-server.cnf** 및 **openssl-ca.cnf**를 만들고 12, 13단계에 따라 **CommserverCertificate** 폴더에 index.txt 및 serial.txt를 만듭니다.
9. 이제 CommServerCertificate 폴더에 파일이 다섯 개 생깁니다.
   a. openssl-server.cnf
   b. openssl-ca.cnf
   c. index.txt
   d. serial.txt
   e. 4SightV2PublicKey.cer
10. 관리자 권한으로 명령 프롬프트를 엽니다.
    아래를 실행하여 CommserverCertificate 폴더로 이동합니다.
    cd "<<CommserverCertificate의 전체 경로>>"
11. 아래의 명령을 실행하여 cacert.pem 및 cakey.pem 파일을 생성합니다.
    openssl req -x509 -config openssl-ca.cnf -newkey rsa:4096 -sha256 -nodes -out cacert.pem -outform PEM
    메시지가 표시되면 올바른 인증서 데이터를 입력합니다(예: 국가, 시/도 등).

12. 이제 섹션 5.5.3.6에서 1단계를 실행하여 **CommserverCertificate** 폴더에서 파일의 콘텐츠를 변경합니다.
13. 이제 섹션 5.5.3.6에서 7~11단계를 실행합니다.
14. 이제 통신 인증을 위해 4sight 공용 키를 통신 서버 cacert로 가져와야 합니다. 이렇게 하려면 아래의 명령을 실행합니다.

    keytool -import -noprompt -trustcacerts -alias <<4sight 서버 호스트 이름>> -storepass changeit -keystore "C:\Program Files\Druck\DruckCommsServer\<< 통신 서비스 버전 >>\cacerts" -file 4SightV2PublicKey.cer

15. 위 과정을 모두 완료하면 현재 **CommserverCertificate** 폴더에 **DruckCommServer.pfx** 및 **CommServer.jks**가 생깁니다.

    이러한 파일을 복사한 후 **"C:\Program Files\Druck\DruckCommsServer\<< 통신 서비스 버전 >>\"** 디렉터리에 붙여 넣습니다. 동일한 위치에서 **application.properties**를 편집하고 속성 값을 아래와 같이 변경합니다.

    a. Keystore = CommServer.jks

    b. key-store.password = <<키 저장소 암호>>

    c. key-store.type=JKS

5.5.3.7.1 Windows에서 DruckCommsServer용 인증서 설치

1. 실행을 열고 "mmc"를 입력한 후 Enter 키를 누릅니다.
2. 파일로 이동하여 스냅 인 추가/제거를 선택합니다.
3. 왼쪽 사이드 메뉴에서 인증서를 선택합니다. 추가를 누른 후 컴퓨터 계정 >> 다음 >> 완료를 선택합니다. 그런 다음 확인을 클릭합니다.
4. 인증서(로컬 컴퓨터) 섹션을 확장합니다. 신뢰할 수 있는 루트 인증 기관을 확장합니다.

   그곳에서 인증서 폴더 >> 모든 작업 >> 가져오기를 마우스 오른쪽 버튼으로 클릭합니다.

   cacert.pem >> 다음 >> 완료를 선택합니다.

   이렇게 하면 사용자 지정 CA 기관이 신뢰할 수 있는 기관 아래에 성공적으로 설치됩니다.

이러한 모든 단계를 수행하면 DruckCommsServer 서비스가 시작됩니다.

DruckCommsServer가 https로 성공적으로 변환되었는지 여부를 확인하려면 Google Chrome 탭에서 다음 링크를 열면 됩니다. **https://localhost:9443/api/devicemanager/version**(변경한 경우 통신 서버 포트 번호를 입력하십시오. 기본값은 9443입니다.)

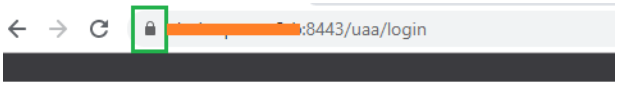
5.5.3.8 4Sight2에서 인증서 검증

1. 서버 PC를 다시 시작합니다.
2. 열린 Windows 서비스에서 4Sight2 및 DruckCommsServer 서비스를 다시 시작합니다.
3. Google Chrome을 열고 브라우저 캐시를 지운 뒤 Google Chrome을 다시 시작합니다. Google Chrome의 다른 인스턴스가 실행되고 있지 않은지 확인합니다.
4. 주소 표시줄에 아래의 URL을 입력하고 Enter 키를 누릅니다.

   Https://<<서버 호스트 이름>>:8443/4sight2.

   참고: 위 URL에는 호스트 이름을 사용해야 합니다.
5. 올바른 HTTPS URL을 사용하는 로그인 화면이 표시되어야 합니다.

   참고: 빨간색 오류가 주소 표시줄에서 사라졌습니다. 링크가 여전히 안전하지 않은 경우 컴퓨터를 다시 시작하고 3단계로 이동합니다.



4Sight2 설치 FAQ

6. 4Sight2 설치 FAQ

6.1 설정 및 설치

질문 1: 전 세계 다양한 지역에 걸쳐 여러 사업장을 보유하고 있습니다. 4Sight2를 설정하는 가장 좋은 방법은 무엇입니까?

답변: 현장을 어떻게 유지관리하고 운영하느냐에 따라 다릅니다. 모든 현장을 중앙 IT 허브에서 유지관리하고 운영하는 경우 중앙에 하나의 4Sight2 라이선스를 설치할 수 있습니다. 각 현장에서는 네트워크나 LAN을 통해 4Sight2에 액세스할 수 있습니다. 반대로, 자체적으로 운영 및 관리되는 별도의 독립체로 기능하는 지사가 있는 경우에는 4Sight2 라이선스를 여러 개 구입할 수 있습니다.

질문 2: 4Sight2 라이선스를 여러 개 구입할 경우, 해당 라이선스 간에 통신이 이루어집니까?

답변: 아니요. 각 4Sight2 라이선스는 고유한 애플리케이션 설치 및 데이터베이스를 사용하며 구분된 개별 소프트웨어입니다. 개별 설치 사이에 통신은 없습니다. 더 명확히 알고 싶거나 특별한 요구 사항에 대해 논의하려면 4Sight2 팀에 문의하십시오.

질문 3: 4Sight2는 어떻게 다운로드할 수 있습니까?

답변: 회사 웹사이트에서 4Sight2를 쉽게 다운로드할 수 있습니다. 아래에 링크가 있습니다.

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

또는

영업 사무소에 전화하여 구매 주문을 해 주십시오. 그러면 USB 스틱에 들어 있는 데모 버전을 받게 됩니다.

질문 4: Windows 이외의 운영 체제에 4Sight2를 설치할 수 있습니까?

답변: 아니요. 4Sight2는 Windows 플랫폼에서만 지원됩니다.

질문 5: 4Sight2를 다운로드하고 설치했습니다. 어떻게 4Sight2에 액세스합니까?

답변: 4Sight2는 웹 기반 소프트웨어입니다. 그러므로 4Sight2를 설치할 때 바탕 화면이나 컴퓨터에 아이콘이 생성되지 않습니다. 4Sight2에 액세스하려면 다음을 수행하십시오.

- Google Chrome을 열고 주소 표시줄에 아래의 URL을 붙여넣은 다음, Enter를 누릅니다.
- 4Sight2가 동일한 컴퓨터에 설치된 경우 http://localhost:<애플리케이션_포트_번호> /4sight2를 사용하고, 4Sight2가 같은 네트워크의 다른 컴퓨터에 설치된 경우

  Http://<컴퓨터 이름 또는 IP 주소>:<애플리케이션_포트_번호>/4sight2를 사용합니다.
- 나중에 참조할 수 있도록 Google Chrome에서 북마크를 생성합니다.

질문 6: 4Sight2 설치 프로그램이 Postgres 데이터베이스 파일을 찾지 못합니다.

설치 프로그램은 로컬 위치에 압축을 풀고 실행 파일을 Disk 1 폴더에서 실행해야 합니다. 설치 프로그램의 압축을 푼 로컬 위치의 경로명이 너무 길지 않아야 합니다. 너무 길면 설치 프로그램 필수 구성 요소 파일도 못 찾을 수 있습니다.

질문 7: 업그레이드 중에 어떤 단계에서 업그레이드 프로세스가 취소되면 어떻게 됩니까?

답변: 어떤 단계에서든 관리자가 업그레이드 프로세스를 취소하면 1.4 버전으로 롤백되고 로드 후 계속 작동되어야 합니다. 관리자는 다시 업그레이드 프로세스를 시작하여 성공적으로 업그레이드를 수행해야 합니다.

질문 8: 4Sight2 애플리케이션을 설치하는 동안 사용자에게 "유효한 포트 번호를 입력하십시오. 유효한 포트 번호를 알려면 설치 설명서를 참조하십시오."라는 메시지가 표시될 경우

답변: 잘못된 포트의 범위는 다음과 같으므로, 유효한 포트를 선택하여 설치를 계속하십시오.

- 포트 0~1024는 TCP 연결용입니다.
- 안전하지 않은 포트 목록은 ~2049, 3659, 4045, 6000, 6665~6669, 65535입니다.

질문 9: https를 사용하는 4Sight2가 시스템에서 작동하지 않을 경우

답변: 4sight2 애플리케이션을 설치할 컴퓨터의 도메인 이름에 대한 구문을 따르십시오.

<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> ::= 대문자로 된 A부터 Z까지와

소문자로 된 a부터 z까지의 알파벳 문자 52개 중 하나

<digit> ::= 0부터 9까지의 숫자 10개 중 하나

참고: 도메인 이름에는 대문자와 소문자가 허용됩니다. 맞춤법은 같지만 대/소문자는 다른 두 가지 이름은 동일한 것으로 처리됩니다.

6.2 테스트 장비 통신기 FAQ

질문 1: 설치 설명서의 단계를 모두 수행했는데도 목록에 장치가 표시되지 않습니다.

답변: 이러한 단계를 수행한 후에도 목록에서 테스트 장비를 찾을 수 없으면 4Sight2 드라이버를 다시 설치하십시오. 그렇게 하려면 **제어판 >> 프로그램 및 기능**으로 이동하여 목록에서 DruckCommsServer를 제거하고 테스트 장비 통신기를 다시 설치합니다.

질문 2:. '**장치를 찾을 수 없습니다**'라는 오류가 나타납니다.

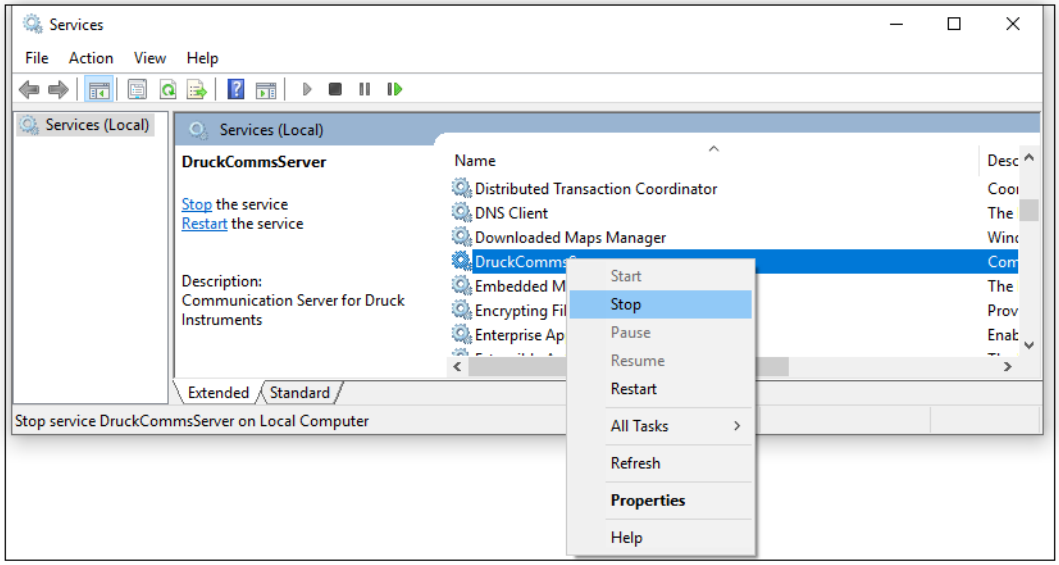
답변: 이 문제의 해결 방법은 다음과 같습니다.

- USB 케이블을 사용하여 장치가 물리적으로 올바르게 연결되었는지 확인합니다. 이를 확인하려면 장치 관리자로 이동하여 목록에서 해당 장치를 찾습니다. 문제가 없다면 장치는 범용 직렬 버스 장치 섹션에 있어야 합니다. 장치가 기타 장치에 있다면 위 설정을 수행하여 장치를 USB 장치로 만들어야 합니다.
- 장치가 통신 중이거나 통신 모드인지 확인합니다. 위에서 설명한 1단계를 참조하십시오.
- 드라이버 경로가 C:\Windows\INF...를 제대로 가리키는지 확인합니다. 위에서 설명한 2단계를 참조하십시오.

질문 3: 새로고침을 클릭하거나 목록에서 테스트 장비를 클릭하면 '**Internal Server Error(내부 서버 오류)**'가 나타납니다.

답변: 이 문제의 해결 방법은 다음과 같습니다.

- Windows 서비스(서비스라고도 함)로 이동합니다.
- 목록에서 **DruckCommsServer** 서비스를 마우스 오른쪽 버튼으로 클릭하고 **다시 시작**을 클릭합니다.



- 4Sight2로 이동하고 **새로 고침** 버튼을 클릭합니다. 목록에 장치가 표시될 것입니다.

질문 4: '**통신 오류**'라는 오류가 나타납니다.

답변: 가끔 소프트웨어가 USB 접촉이 느슨하거나, 장치 연결이 끊어졌거나, 장치가 다른 작업을 수행하는 중이거나, 서버가 다른 작업을 실행하는 등의 다양한 이유로 장치와 제대로 통신할 수 없는 경우가 있습니다. Refresh(새로고침) 버튼을 다시 클릭하면 문제가 사라질 것입니다(2~3회 시도하십시오).

그러나 이 오류가 지속적으로 나타나면 아래 단계를 수행해 보십시오.

- 장치(Genii/PACE)를 다시 부팅해도 되는지, 중요한 작업이 진행 중인 것은 아닌지 확인한 후 장치를 재부팅합니다. 다시 시도하십시오. 장치가 아직 물리적으로 연결되어 있는지도 확인합니다.

위 방법으로도 해결되지 않는 경우 위에서 설명한 3단계의 지침을 따르고 **DruckCommsServer** 서비스를 다시 시작합니다.

설치 문제 해결

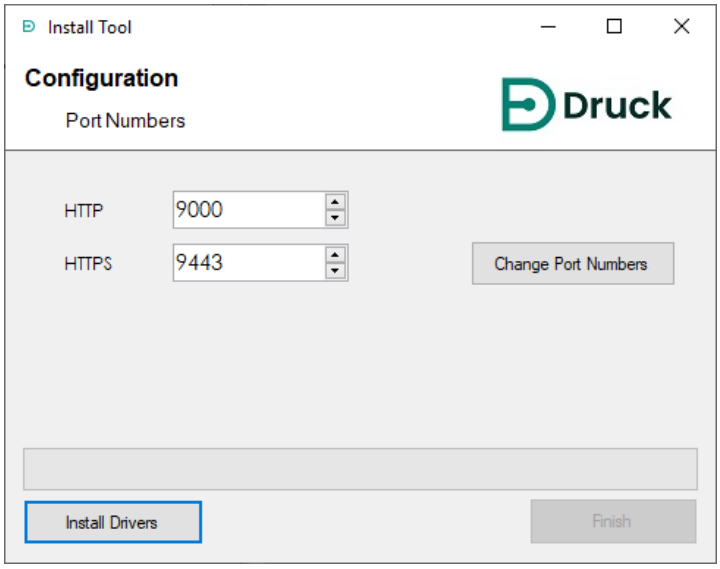
7. 설치 문제 해결

7.1 테스트 장비 통신기 문제

통신기를 직접 호출했을 때 테스트 장비 통신기가 json 문자열을 반환하는 것을 확인했더라도 4Sight2를 사용하여 테스트 장비와 통신할 경우 반환되는 테스트 장비를 찾을 수 없는 경우가 있을 수 있습니다. 이 문제는 다음 두 가지 주요 원인 중 하나 때문에 발생할 수 있습니다.

- 포트 번호가 잘못 구성되었습니다 - 관리자 사용자에게 연락해 4Sigth2가 테스트 장비 통신기와 통신하는 데 사용하고 있는 포트를 확인하십시오.

  사용해야 하는 포트를 파악했으면 C:\Program Files\Druck\DruckCommsServer\[Version] and run the CommsServerInstallTool.exe로 이동합니다.



포트 번호를 편집한 다음 **포트 번호 변경** 버튼을 클릭합니다. 서비스가 다시 시작될 때까지 기다립니다. 이제 포트 번호가 변경되었습니다. **완료** 버튼을 선택합니다.

- 테스트 장비 통신기가 Https에 대해 구성되지 않았지만 4Sight2는 구성되었습니다.

  관리자에게 연락해 테스트 장비 통신기의 자체 서명 인증서를 설치하십시오.

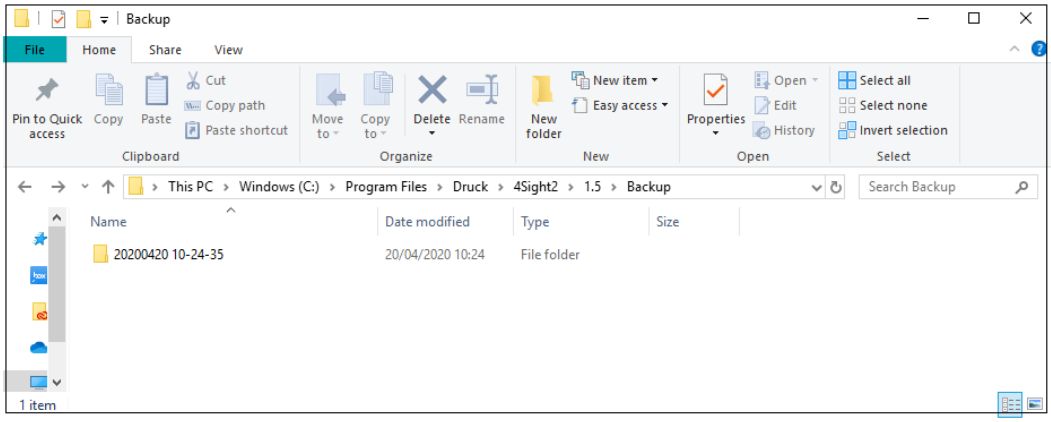
7.2 Postgres 데이터베이스 백업

Postgres 데이터베이스 백업에 대한 정보는 4Sight2 사용 설명서 - 123M3138을 참조하십시오.

7.3 Postgres 데이터베이스 복원

이미 4Sight 애플리케이션을 사용하여 데이터베이스 백업을 수행했다고 가정합니다.

4Sight 애플리케이션(버전 1.4 이상)에서는 백업을 시작(사용자 시작/예약)할 수 있는 인터페이스를 제공합니다. 이 작업은 서버의 4Sight 설치 디렉터리 내에 있는 백업 폴더에 파일을 생성합니다. 백업을 시작할 때마다 백업이 성공적으로 완료된 날짜와 시간에 따라 백업 폴더 내에 YYYYMMDDHHSS(연도, 월, 일, 시간 및 초) 형식의 새 폴더가 생성됩니다.



백업 폴더의 콘텐츠는 별개의 미디어에 백업하는 것을 권장합니다.

각 폴더에는 5개의 파일이 있습니다.

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

*.bck 파일에는 4Sight 애플리케이션 버전이 포함된 접미사가 있습니다. 정확한 애플리케이션의 버전과 일치하는 데이터베이스를 복원해야 합니다. 더 높거나 낮은 버전의 데이터베이스는 애플리케이션에서 지원되지 않습니다. 버전에 밑줄(_)은 포함되지만 마침표(.)는 포함되지 않는다는 점에 유의하십시오(예: 1_4는 되지만 1.4는 안 됨). 복원 단계에서 아래 명령을 사용할 경우 <애플리케이션_버전>을 설치된 4Sight의 정확한 버전으로 바꾸어야 합니다.

metadata.properties 파일에는 백업 시작 중에 입력한 백업의 이름이 포함되어 있습니다.

SHA 256 체크

백업에는 확장명이 .bck인 파일이 각 데이터베이스에 하나씩 3개가 있습니다. metadata.properties 파일에는 각 백업 파일의 SHA 256이 포함되어 있습니다.

1. 관리자로 명령 프롬프트를 열고, 디렉터리를 선택된 백업 파일이 포함된 폴더로 변경합니다.
2. 아래 명령을 사용하여 각 파일의 SHA256를 계산합니다.

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

3. 복원 단계를 계속하기 전에 각 파일의 SHA 256이 메타데이터 파일에 언급된 SHA 256과 일치하는지 확인합니다. 명령 프롬프트의 체크섬과 메타데이터 파일의 체크섬이 정확히 같다면 백업 파일은 복원에 대해 유효한 것입니다. 체크섬이 서로 같은 경우에만 복원 단계를 계속합니다.

7.4 복원 단계:

1. 4Sight 서버에 관리자로 로그인합니다.
2. Postgres 데이터베이스가 실행 중인 포트를 찾습니다. 이 포트는 <4Sight 설치 디렉터리>\apache-tomcat\webapps\application.properties 파일 내의 spring.datasource.url 속성에서 찾을 수 있습니다. 관리자로 실행 중인 메모장을 사용하여 이 파일을 엽니다. 4Sight**<애플리케이션_버전>** 바로 앞에 있는 숫자입니다.
3. postgres 사용자를 사용하여 관리자로 실행 중인 명령 프롬프트에서 psql 명령 유틸리티에 로그인합니다.

   C:\Program Files\PostgreSQL\11\bin\psql" --port=<DB_포트> postgres postgres
4. 애플리케이션에서 사용되는 데이터베이스 사용자는 <4Sight 설치 디렉터리>\apache-tomcat\webapps\application.properties 파일 내의 spring.datasource.username 속성에서 찾을 수 있습니다. 관리자로 실행 중인 메모장을 사용하여 이 파일을 엽니다.
5. *_temp 데이터베이스가 있으면 삭제한 다음 psql 프롬프트에서 아래 명령을 실행하여 빈 *_temp 데이터베이스를 생성합니다.

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

   위 세 데이터베이스의 데이터베이스 소유자를 이 사용자로 변경합니다. 사용자 이름은 대/소문자를 구분합니다.

   ALTER DATABASE "4Sight**<애플리케이션_버전>**_temp" OWNER TO "**<DB_사용자>**";
   ALTER DATABASE "4Sightaudit**<애플리케이션_버전>**_temp" OWNER TO "**<DB_사용자>**";
   ALTER DATABASE "uaa**<애플리케이션_버전>**_temp" OWNER TO "**<DB_사용자>**";
6. 백업의 metadata.properties 파일을 확인하고 복원해야 할 백업을 결정합니다.
7. 관리자로 다른 명령 프롬프트를 열고, 디렉터리를 위에서 선택한 백업 파일이 포함된 폴더로 변경합니다.

   아래 명령을 사용하여 *.bck 파일의 데이터베이스를 *_temp 데이터베이스로 복원합니다. 암호를 묻는 메시지가 표시되면 postgres 슈퍼 사용자의 암호를 입력합니다.

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

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

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

8. *_old 데이터베이스가 있으면 psql 프롬프트에서 아래 명령을 실행하여 삭제합니다.

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

9. 4Sight 서비스 및 pgadmin 애플리케이션이 열려 있으면 중지합니다.
10. psql 프롬프트에서 아래 명령을 실행하여 기존 4Sight 데이터베이스 이름을 *_old로 변경합니다.

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

11. 프롬프트에서 아래 명령을 실행하여 *_temp 데이터베이스 이름을 4Sight 데이터베이스로 변경합니다.

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

12. 4Sight 서비스를 시작하고 관리자로 로그인합니다. 이제 백업 당시의 관리자 암호를 사용하여 로그인해야 합니다.

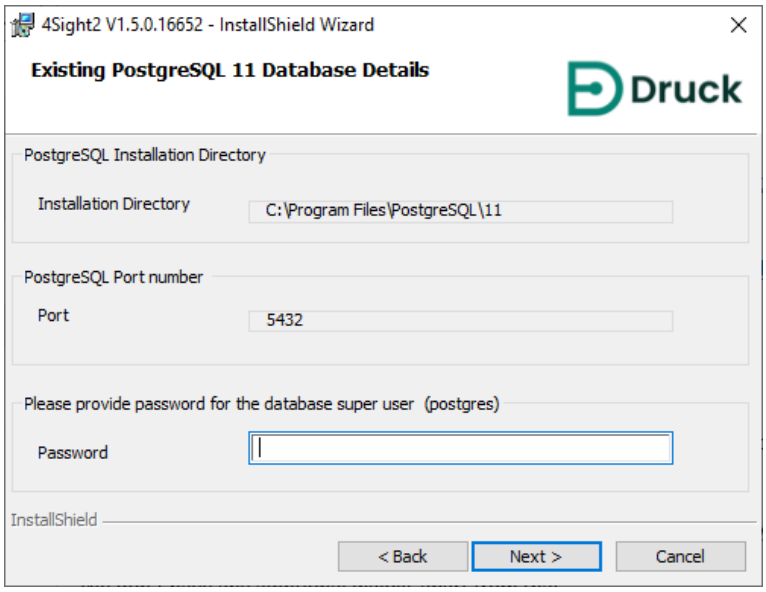
7.5 4Sight2 시스템 충돌 시 복구하는 방법은?

가정: 충돌 전에 사용자가 4Sight2 데이터베이스를 백업했습니다.

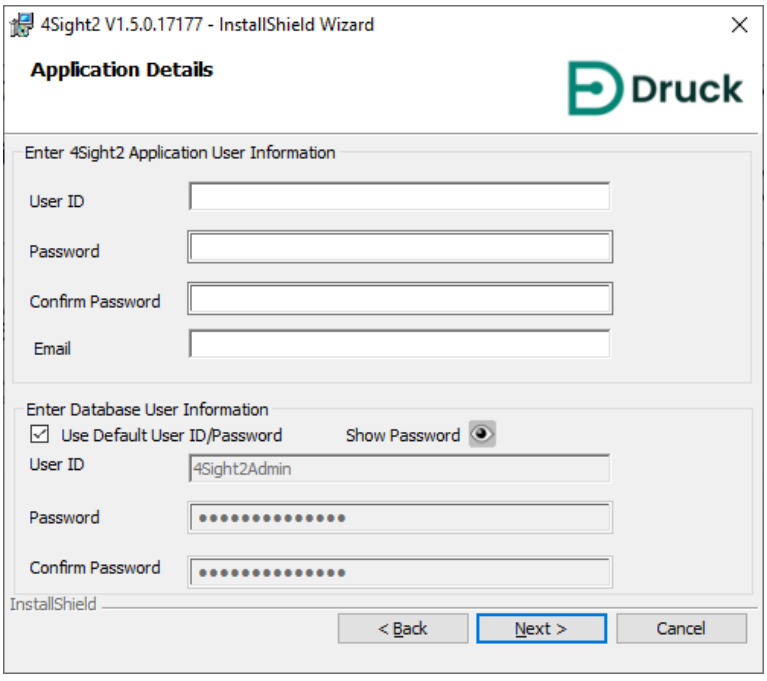
사용자는 애플리케이션과 데이터베이스의 사용자 이름과 암호를 모두 알고 있습니다.

1. OS와 드라이버 지원 기능으로 시스템을 설정합니다.
2. 시스템에서 4Sight2를 설치합니다.

3. 애플리케이션을 설치할 때 이전에 애플리케이션과 Postgres 데이터베이스에 입력한 것과 동일한 사용자 이름과 암호를 제공합니다.

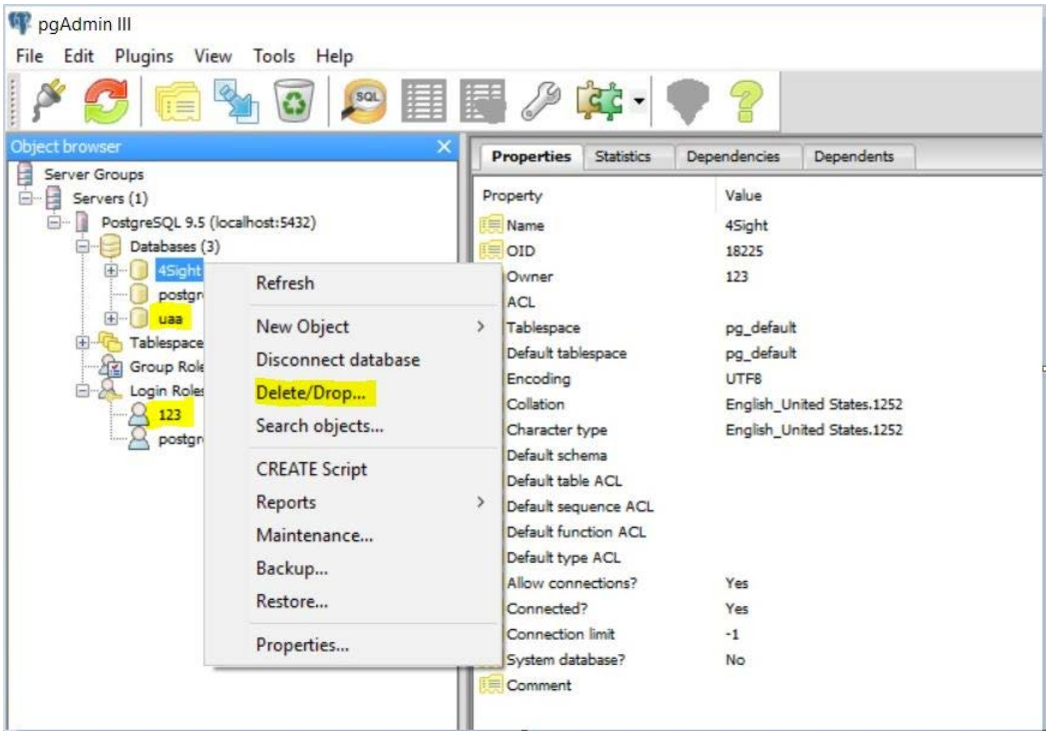


이전 설치와 동일한 암호



이전 설치처럼 모든 필드 작성

4. 애플리케이션을 성공적으로 설치한 후에는 pgAdmin에서 애플리케이션을 설치하는 동안 생성된 기본 데이터베이스를 삭제합니다(데이터베이스를 마우스 오른쪽 버튼으로 클릭하고 Delete/Drop(삭제/제거) 선택). 데이터베이스를 제거하는 동안 오류가 발생하면 새로 고친 후 똑같이 다시 시작해 보십시오.



5. 데이터베이스와 사용자를 성공적으로 제거한 후에는 이러한 단계를 따라 명령 프롬프트에서 위에 언급한 대로 데이터베이스를 복원합니다.
6. 이제 데이터베이스를 성공적으로 복원했으므로 브라우저에서 애플리케이션을 열고 동일한 내용을 검토합니다.

7.6 설치 오류 시나리오:

아래 표에는 설치 중에 발생할 만한 다양한 오류 시나리오와 이를 해결하기 위한 조치가 나와 있습니다.

오류 메시지	시나리오	해결 방법/수행할 조치
"Insufficient disk space available to install 4Sight2 application. Please ensure a minimum of 4096 MB is available. Free Space : available MB."	하드 디스크 크기 문제로 인한 오류(업그레이드를 시작하려는 데 필수 공간이 없는 경우)	관리자가 각 드라이브에서 여유 공간을 확보한 다음 다시 업그레이드 프로세스를 시작해야 합니다.
"Deployment fail while Migrating database"	하드 디스크 크기 문제로 인한 오류(업그레이드를 성공적으로 시작한 후에 충분한 공간이 없는 경우)	관리자가 각 드라이브에서 여유 공간을 확보한 다음 다시 업그레이드 프로세스를 시작해야 합니다.

오류 메시지	시나리오	해결 방법/수행할 조치
"Installation failed while migrating Database. Please reinstall 4sight2"	데이터베이스 복사 시 데이터 무결성으로 인한 오류	이 문제가 발생하면 관리자는 고객 지원 센터에 문의해야 합니다. 데이터 무결성 이유는 [C:\Users\[Username]\App Data\Local\Temp\logs]위치의로그에 캡처됩니다.
"Installation failed while migrating Database. Please reinstall 4sight2"	스키마 업데이트 단계에서 데이터 무결성으로 인한 오류	이 문제가 발생하면 관리자는 고객 지원 센터에 문의해야 합니다. 데이터 무결성 이유는 C:\Program Files\Druck\4Sight2\<<latest folder number>>\logs 위치의 로그에 캡처됩니다.
"Failed to locate existing 4Sight2 service. Please ensure existing 4Sight2 version is installed on this machine and the service is running"	설치 프로그램이 서비스의 상태를 파악할 수 없는 경우 발생하는 오류	관리자는 4Sight2 서비스가 로드되어 실행 중인지 확인해야 합니다.
"Failed to start the 4Sight2 service. Please ensure the 4Sight2 service is present and running"	애플리케이션이 손상되거나, 일부 파일이 삭제되거나, 다른 애플리케이션에서 포트를 사용하고 있거나, 사용자가 서비스를 중지하는 등의 경우 발생하는 오류	관리자가 서비스 상태를 파악하는 데 성공하고 어떠한 이유로든(예: 애플리케이션이 손상되거나, 일부 파일이 삭제되거나, 다른 애플리케이션이 포트를 사용하거나, 사용자가 서비스를 중지하는 등) 서비스가 실행되지 않은 경우 시스템은 서비스를 시작하려고 시도합니다. 서비스를 시작할 수 없으면 관리자가 고객 지원 센터에 문의하여 문제를 해결해야 합니다.
"Upgrade of 4Sight2 application is supported from version 1.3 onwards. For earlier version upgrade support please contact Customer Care."	1.3보다 오래된 버전을 설치하면 업그레이드되지 않음	업그레이드는 1.3 이상의 버전에서만 가능합니다.
Installer has detected another minor version of PostgreSQL 11. Installer will not continue. Refer to 4Sight2 Installation manual for more details	동일한 PostgreSQL 버전(변형)이 대상 시스템에 있는 경우 4Sight2가 4Sight2 설치를 계속할 수 없음	가능한 옵션 1. 사용자가 다른 시스템을 선택할 수 있습니다. 2. 사용자가 Postgres 버전 11.3을 사용하는 기존 애플리케이션을 백업하고, 이 애플리케이션을 다른 시스템에서 제거 및 배포합니다. Postgres를 제거하고 4Sight2 설치를 다시 시작합니다.
Installation failed while upgrading database. Please reinstall 4Sight2. Refer to 4Sight2 Installation manual for more details	업그레이드 중에 몇 가지 내부 오류가 발생했을 수 있으며, 사용자는 재설치를 시도할 수 있음	문제가 지속될 경우 사용자는 문제가 더욱 잘 파악될 수 있도록 설치 로그를 공유할 수 있습니다.

7.7 일반적인 오류의 원인

USB를 통한 Druck 장비와 4sight2 간 통신과 관련하여 일반적으로 관찰되는 문제는 다음과 같습니다.

- 물리적 연결이 느슨하거나 불안정합니다.
- 케이블/포트가 닳았습니다.
- USB 어댑터가 저품질입니다.
- USB 어댑터/포트가 오버로드되었습니다.
- 장치가 장시간 계속 실행되어 최대 절전 모드나 수면 모드 상태입니다.
- 장치가 통신 모드가 아닙니다.
- 드라이버 소프트웨어가 설치되거나 업그레이드되지 않았습니다. 하드웨어와의 통신을 설정하려면 동일한 버전의 4Sight2 애플리케이션 및 드라이버가 필요합니다.
- 장치에 매우 오래된 펌웨어 버전이 있습니다.

7.8 4Sight2 제거

4Sight2의 새로운 사본, 새 버전의 4Sight2를 설치해야 하거나 설치 도중 발생한 문제로 인해 4Sight2를 제거해야 할 경우 이러한 지침을 따르십시오.

PostgreSQL 데이터베이스 구성요소를 제거하면 4Sight2 데이터베이스가 삭제되어 데이터가 손실됩니다. 다음 단계를 수행할 경우 백업이 자동으로 생성되지 않으므로 진행하기 전에 수동 백업을 생성하고 이 백업을 4Sight2 설치 폴더의 대체 위치에 저장했는지 확인하십시오. 이 설명서의 Postgres 데이터베이스 백업 및 복원 섹션을 참조하십시오.

4Sight2 애플리케이션만 제거하고 데이터베이스는 유지하려는 경우 이 설명서의 4Sight2 설치 부분을 참조하십시오. 재설치 시 데이터베이스 슈퍼 사용자에 대한 자격 증명이 필요합니다. 이러한 자격 증명을 모를 경우 제거를 시도하지 마십시오.

데이터베이스를 제거하지 않고 4Sight2 버전을 업그레이드하려면 이러한 지침을 따르지 **마십시오**.

1. 제어판 >> 프로그램 및 기능으로 이동합니다.
2. 4Sight2를 마우스 오른쪽 버튼으로 클릭하고 제거를 선택합니다.
3. 제거 마법사의 지침을 따릅니다.
4. PostgreSQL 11을 마우스 오른쪽 버튼으로 클릭하고 제거를 선택합니다.
5. 제거 마법사의 지침을 따릅니다.
6. PostgreSQL을 제거해도 데이터 폴더는 삭제되지 않습니다. 데이터 폴더는 수동으로 삭제해야 합니다. C:\Program Files\PostgreSQL\11\에서 데이터 폴더를 찾아 삭제합니다.
   a. 전체 PostgreSQL 폴더를 삭제하려면 계속하기 전에 백업 파일, 스크립트가 Bin 폴더에서 이동되었는지 확인합니다.
   b. 기본적으로 4Sight2 데이터베이스 백업이 생성되어 다음 위치에 저장됩니다. C:\Program Files\PostgreSQL\11\bin
7. 가능하면 컴퓨터를 다시 시작하는 것이 좋습니다.
8. 이제 4Sight2가 성공적으로 제거되었습니다.

7.9 보안 통신 문제 해결

1. '명령 이름' 명령은 내외부 명령으로 인식되지 않습니다. 예를 들어 'keytool'은 내외부 명령으로 인식되지 않습니다.

- 이와 같은 오류가 발생했다면 현재 폴더에서 명령 프롬프트가 지정된 명령에 대한 참조를 찾을 수 없음을 의미합니다.

  이 오류를 해결하려면 아래의 명령을 사용하여 올바른 폴더를 가리키도록 합니다.

  Set Path=%Path%;"<<명령이 있는 위치의 전체 경로>>"

  예를 들어 keytool과 관련된 위의 오류에서는 경로를 아래로 설정해야 합니다.

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

2. 잘못된 IP 주소

- 이 텍스트가 포함된 오류 메시지가 표시된다면 openssl-ca.cnf 또는 openssl-server.cnf 파일 중 하나에 있는 IP 주소 또는 호스트 이름이 올바르지 않음을 의미합니다. 참고: 이러한 파일의 여러 위치에서 이를 수정하고 해당 단계를 다시 실행해야 할 수도 있습니다.

3. 해당 파일 또는 디렉터리가 없는 경우...

- 이 텍스트가 포함된 오류 메시지가 표시된다면 실행한 명령이 올바르지 않은 파일 이름을 참조할 수 있음을 의미합니다. 명령에 파일 이름 오류가 있는지, 해당 이름을 사용하는 파일이 폴더에 있는지 확인하고 명령을 다시 실행합니다. 명령에서 파일 이름을 수정하거나, 누락된 파일을 생성하기 위한 단계를 수행해야 할 수도 있습니다.
- 이 오류는 특정한 경우 파일 확장명이 이름에 두 번 추가(예: intex.txt.txt)되어, index.txt 및 serial.txt 파일에서 발생할 수 있습니다.

  파일을 편집하고 .txt 확장명 없이 저장하기만 하면 됩니다. 파일에 .txt 확장명이 한 번 포함되어 있는지 확인합니다.

모범 사례

8. 모범 사례

서버 강화

Microsoft 또는 CIS 지침에 따라 서버 환경을 강화해야 합니다.

8.1 Tomcat

- 관리자 또는 LocalService만 액세스할 수 있는 보안 폴더(예: *C:\Program Files(x86)*)에 Tomcat을 설치합니다.
- Tomcat을 LocalService 계정으로 실행하는 서비스로 설치합니다.
- WebApp에서 모든 것을 제거하고, 불필요한 기본 애플리케이션을 제거합니다.
- 기본 오류 페이지(예: 404, 403, 500 등)를 교체합니다.
- HTTPS를 적용하고 SSL을 활성화합니다.
- 관리 애플리케이션은 SSL에서 실행해야 합니다.
- 각 웹 애플리케이션에 대해 개별 로그 파일을 사용합니다.
- 서버 배너를 제거합니다.
- 액세스 로깅을 사용합니다.
- 종료 포트 및 명령을 변경합니다.

8.2 PostgreSQL

- pgdba, postgres, depesz 등 높은 권한의 계정은 로컬 로그인에만 허용해야 합니다.
- 올바른 사용자가 적절한 액세스 권한을 받을 수 있도록 pg-hba.conf 파일에서 시퀀스가 올바른지 확인합니다.
- 네트워크가 아니라 로컬 시스템에서만 서버를 연결할 수 있도록 pg-hba.conf를 구성합니다.

8.3 방화벽 모범 사례

4Sight2 사용 시 권장되는 방화벽 모범 사례는 다음과 같습니다.

8.3.1 정책

1. 방화벽 구성은 조직 보안 정책과 일치해야 합니다.
2. 항상 최소 권한 정책을 사용합니다. 모두 거부하는 것을 기본값으로 하고, 특정 트래픽(소스, 대상 및 포트 사용)을 허용합니다.
3. 먼저 구체적인 규칙을 설정하고 명시적인 삭제 규칙을 사용합니다.
4. 감사 추적을 위해 모든 작업, 특히 실패한 시도를 로그로 남깁니다.

8.3.2 리소스

1. 메모리 사용을 모니터링합니다.
2. CPU 사용을 모니터링합니다.
3. 대역폭 사용을 모니터링합니다.
4. 방화벽 시스템에서 실행되는 애플리케이션의 수를 제한합니다.

8.3.3 설치 및 유지 보수

1. 방화벽 시스템에 대한 물리적 액세스를 제한합니다.
2. 관리 시 고유한 사용자 ID를 사용합니다.
3. 시스템의 엄격한 계정 정책을 준수합니다.
4. 운영 체제, 애플리케이션 소프트웨어, 펌웨어 등을 정기적으로 패치합니다.
5. 규칙 기반, 구성 및 로그를 정기적으로 보관합니다. 소스 제어에서 작성한 모든 규칙과 변경 사항을 기록합니다.
6. 정기적으로 테스트를 수행합니다.
7. 서비스가 해체되면 사용되지 않은 규칙을 제거합니다.
8. 정기적으로 규칙을 감사하고 검토합니다.
9. 정기적으로 보안 권고를 모니터링합니다.

8.3.4 추가 보안

1. 상태 기반 검사 방식을 사용합니다.
2. 프록시를 사용합니다.
3. 애플리케이션 수준의 검사 및 필터링을 사용합니다.

8.3.5 내부 보호

1. 수용 가능한 사용 정책 마련
2. 사용자별 개인 방화벽
3. 호스트 기반 침입 방지
4. 네트워크 모니터링
5. 콘텐츠 필터링
6. 각 컴퓨터 및 애플리케이션에 대한 액세스 제어

지사 위치

본사
영국 레스터
전화: +44 (0) 116 2317233
이메일: gb.sensing.sales@bakerhughes.com

네덜란드
호벨라켄
전화: +31 334678950
이메일: nl.sensing.sales@bakerhughes.com

독일
프랑크프루트
전화: +49 (0) 69-22222-973
이메일: sensing.de.cc@bakerhughes.com

러시아
모스크바
전화: +7 915 3161487
이메일: aleksey.khamov@bakerhughes.com

미국
보스턴
전화: 1-800-833-9438
이메일: custcareboston@bhge.com

아랍에미리트
아부다비
전화: +971 528007351
이메일suhel.aboobacker@bakerhughes.com

이탈리아
밀란
전화: +39 02 36 04 28 42
이메일: csd.italia@bakerhughes.com

인도
방갈로르
전화: +91 9986024426
이메일: aneesh.madhav@bakerhughes.com

일본
도쿄
전화: +81 3 6890 4538
이메일: gesitj@bakerhughes.com

중국
광저우
전화: +86 173 1081 7703
이메일: dehou.zhang@bakerhughes.com

중국
베이징
전화: +86 180 1929 3751
이메일: fan.kai@bakerhughes.com

중국
상하이
전화: +86 135 6492 6586
이메일: hensen.zhang@bakerhughes.com

프랑스
툴루즈
전화: +33 562 888 250
이메일: sensing.FR.cc@bakerhughes.com

호주
스프링필드 센트럴
전화: 1300 171 502
이메일: custcare.au@ge.com

서비스 및 지원

기술 지원
전 세계
이메일: mstechsupport@bakerhughes.com

미국
빌레리카
전화: +1 (281) 542-3650
이메일: namservice@bakerhughes.com

브라질
캄피나스
전화: +55 11 3958 0098, +55 19 2104 6983
이메일: mcs.services@bakerhughes.com

아랍에미리트
아부다비
전화: +971 2 4079381
이메일: gulfservices@bakerhughes.com

영국
레스터
전화: +44 (0) 116 2317107
이메일: sensing.grobycc@bakerhughes.com

인도
푸네
전화: +91 213 5620426
이메일:
mcsindia.inhouseservice@bakerhughes.com

일본
도쿄
전화: +81 3 3531 8711
이메일: service.druck.jp@bakerhughes.com

중국
창저우
전화: +86 400 818 1099
이메일: service.mcchina@bakerhughes.com

프랑스
툴루즈
전화: +33 562 888 250
이메일: sensing.FR.cc@bakerhughes.com

123M3140 개정 F | 한국어

Baker Hughes