Druck

4Sight2

校准管理软件

安装手册 123M3140 修订版 F

目录

1. 简介 1
   1.1 目标受众 1
      1.1.1 管理员 1
      1.1.2 监督员 1
      1.1.3 技术人员 1
      1.1.4 审核人 1
2. 系统要求 2
   2.1 应用程序服务器 2
   2.2 客户端工作站 2
   2.3 本地安装 2
   2.4 4Sight2 支持的固件 3
3. 4Sight2 安装 5
   3.1 数据库安装 7
   3.2 安装 PostgreSQL 7
4. 安装 4Sight2 测试设备通信器 13
   4.1 手动驱动程序配置 18
      4.1.1 前提条件 19
   4.2 对测试设备通信器进行测试 22
   4.3 温度校准仪驱动程序配置 23
5. 部署指南 25
   5.1 部署架构 25
   5.2 物理部署 25
   5.3 网络 25
   5.4 部署顺序 25
   5.5 部署后的任务 26
      5.5.1 添加用户和组 26
      5.5.2 默认密码 26
      5.5.3 安全通信 26
6. 4Sight2 安装常见问题 41
   6.1 设置和安装 41
   6.2 测试设备通信器常见问题 42
7. 安装故障排查 45
   7.1 测试设备通信器问题 45
   7.2 Postgres 数据库备份 45
   7.3 Postgres 数据库还原 45
   7.4 还原步骤： 47
   7.5 如何从 4Sight2 计算机崩溃中恢复？ 48
   7.6 安装出错情况： 50
   7.7 一般错误原因 51
   7.8 卸载 4Sight2 52
   7.9 安全通信故障排除 52

8. 最佳做法 54
8.1 Tomcat 54
8.2 PostgreSQL 54
8.3 防火墙最佳做法 54
8.3.1 政策 54
8.3.2 资源 54
8.3.3 安装和维护 54
8.3.4 其他安全事项 55
8.3.5 内部保护 55

1. 简介

4Sight2 校准软件是一种基于 Web 的校准管理工具，可帮助维护和控制校准环境以保持最高计量标准。可使用该软件完成以下任务：

- 管理指定公司位置的所有测量设备的校准
- 为技术人员设置校准工作计划
- 在具有 USB 通信功能的 Druck （DPI620 Genii、 DPI611 和 DPI612）便携式校准仪上下载和上传数据
- 管理便携式校准仪不支持的设备的校准记录 （手动输入数据）
- 检查校准历史记录。还可为每个校准证书创建永久记录。例如：对于 ISO 9000 质量控制过程
- 使用 Druck 压力控制器 （PACE 1000、 5000 和 6000）、便携式校准仪 （DPI620 Genii、 DPI611 和 DPI612）以及温度校准仪 （DryTC165、 DryTC 650、 LiquidTC165 和 LiquidTC255）控制自动校准

1.1 目标受众

1.1.1 管理员

管理员负责安装和配置 4Sight2 软件。 4Sight2 初始安装之后，将提供一个管理帐户。通过此帐户可以创建新用户，分配组/权限集。管理用户对于所有 4Sight2 功能均具有读写权限。

1.1.2 监督员

监督员负责资产和校准管理。他们能够在 4Sight2 Enterprise 中创建和更新资产，包括设施、位置、标签和设备。他们负责将文档链接到资产，如设施过程和设备数据表。监督员可以创建校准期间要使用的测试程序，还可以安排程序，监控设备的运行状况。监督员具有批准校准所需的权限。

1.1.3 技术人员

技术人员负责执行校准。校准可以是便携式、手动或自动校准，技术人员负责在设备上执行相关校准类型。校准执行后，技术人员可以复查结果，完成校准，以便由监督员进行批准。

1.1.4 审核人

审核人负责检查报告。作为一项法规要求，可能必须在某些设施中执行审核。

2. 系统要求

在服务器和客户端计算机上安装 4Sight2 应用程序的最低系统要求如下所示：

2.1 应用程序服务器

操作系统	Windows10、WindowsServer2012R2、WindowsServer2016、WindowsServer 2019
更新	安装全部 Windows 更新
处理器	四核
RAM	8GB 或更大（推荐 32GB）
磁盘空间	1TB
网速	10Mbps

2.2 客户端工作站

操作系统	Windows10、WindowsServer2012R2、WindowsServer2016、Windows Server 2019
浏览器	Google Chrome V80+，Microsoft Edge V80，Firefox V74
Adobe Reader	Adobe Acrobat Reader DC，版本 2015.017.20050 +
RAM	8GB 或更大
处理器	双核
磁盘空间	600GB
网速	10Mbps

2.3 本地安装

操作系统	Windows10、WindowsServer2012R2、WindowsServer2016、Windows Server 2019
更新	安装全部 Windows 更新
Adobe Reader	Adobe Acrobat Reader DC，版本 2015.017.20050 +
处理器	双核
RAM	16GB 或更大（推荐 32GB）
磁盘空间	500GB 或更大磁盘空间
浏览器	Google Chrome V80+，Microsoft Edge V80，Firefox V74

2.4 4Sight2 支持的固件

有关支持的固件的最新信息，请参阅以下链接：
https://www.bakerhughes.com/druck/test-and-calibration-instrumentation/calibration-management-software-4sight2

或者

对于 PACE，插入用于 4Sight2 通信的 USB B，如下图所示：

4Sight2 安装

3. 4Sight2 安装

要安装 4Sight2，首先将 4Sight2 安装 zip 文件复制到计算机，然后从 zip 文件解压缩文件。在安装文件中，选择 4Sight2 可执行文件。

注：以下杀毒软件用于扫描安装的 4Sight2 和通信服务器。

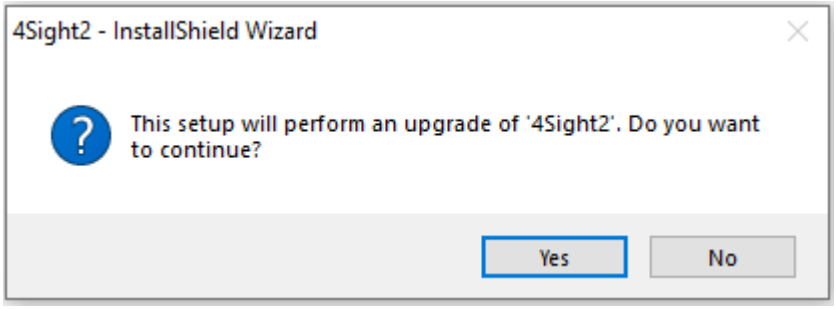
- McAfee VirusScan Enterprise + AntiSpyware Enterprise 版本号：8.8.0
- Symantec Endpoint Protection 版本号：14.3.558

运行安装程序的可执行文件后，即会启动 InstallShield 向导。 InstallShield 向导包含 4Sight2 的两个安装阶段：

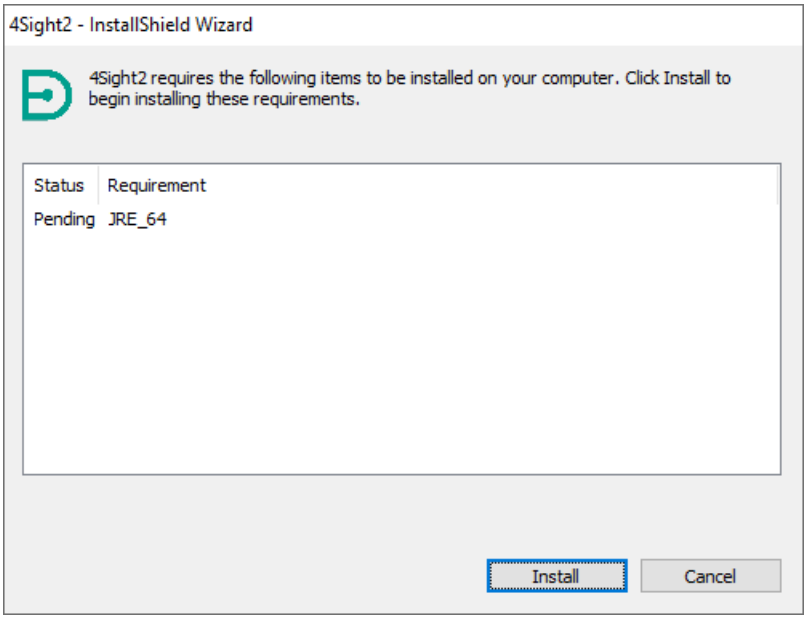
1. 数据库安装
2. Web 应用程序安装

遵循 InstallShield 向导的操作说明或按照以下两节的内容完成整个安装过程。

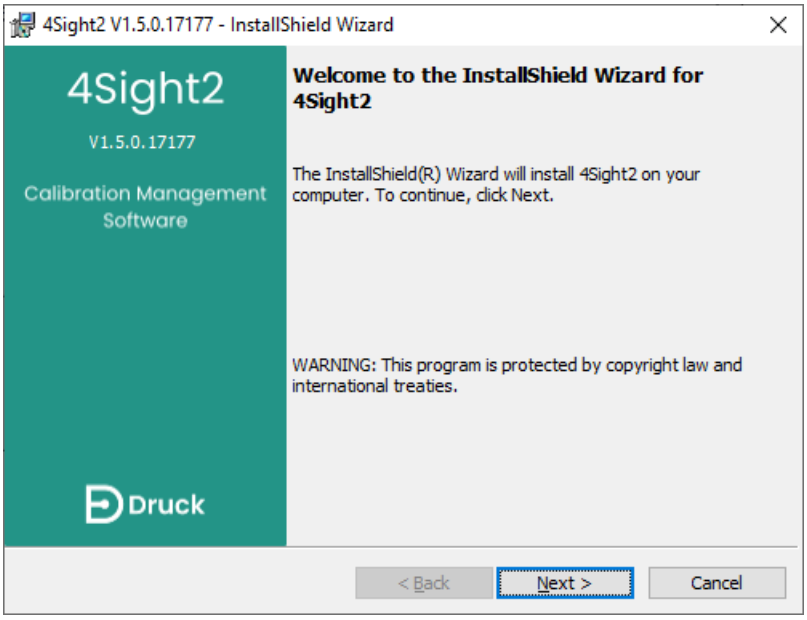
1. 如果已在计算机上安装了 4Sight2，则安装向导将会提示升级到最新版本。单击 **Yes （是）**执行最新升级。



2. 如果是首次在计算机上安装 4Sight2，则安装向导将显示出以下屏幕。选择 **Install （安装）**，然后列出的显示项目将开始安装。



3. 任何前提项的安装完成后，将显示 InstallShield 向导欢迎屏幕。单击 **Next**（下一步）继续。



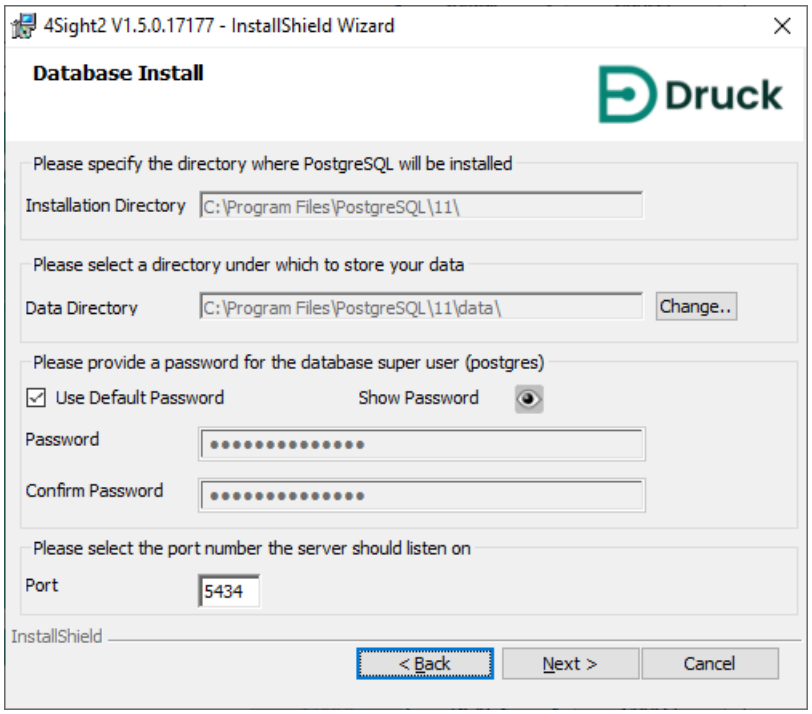
3.1 数据库安装

4Sight2 应用程序使用 PostgreSQL 数据库。以下提供了有关如何安装 PostgreSQL 数据库以及在已安装 PostgreSQL 数据库时该如何做的说明。

3.2 安装 PostgreSQL

如果计算机上未安装 PostgreSQL 数据库，则按此过程操作。

1. 如果计算机上未安装任何 PostgreSQL 数据库实例，则安装向导将显示出以下屏幕。



Installation Directory （安装目录）：选择用于安装 PostgreSQL 应用程序的目录。

Data Directory （数据目录）：选择用于存储 PostgreSQL 数据库的目录。

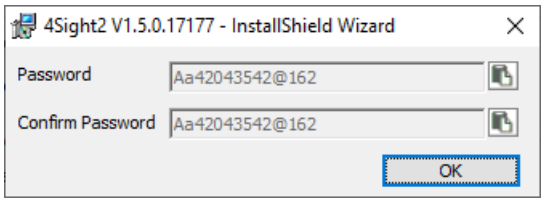
Password （密码）/Confirm Password （确认密码）：输入 PostgreSQL 数据库超级用户的密码。仅当首次安装 PostgreSQL 数据库时才会出现此提示。

注：安装后访问数据库内容时，需要使用此密码。

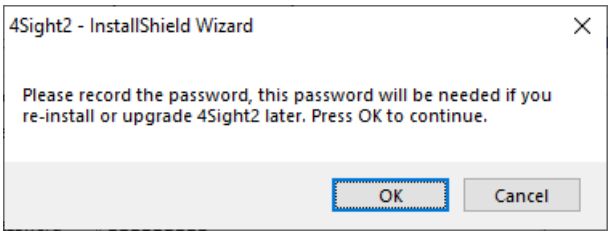
Port （端口）：这是 PostgreSQL 数据库用来满足应用程序请求的端口地址。

注：如果端口号已被占用，则联系 IT 团队。用户还可更改端口号，必须记下该端口号以在随后启动应用程序。

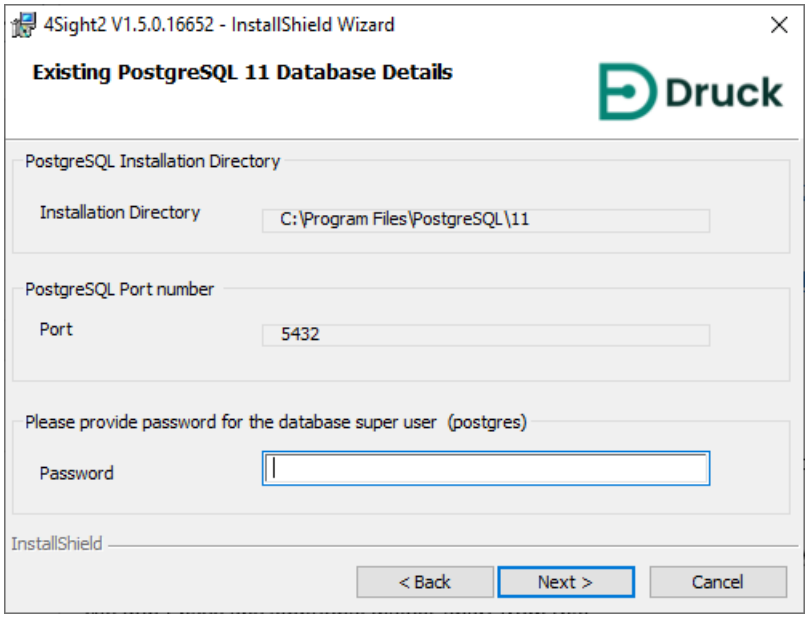
重要事项：用户必须记下数据库密码。丢失密码信息可能导致访问被拒绝或数据丢失。取消选中 UserDefaultPassword（用户默认密码）复选框，更新数据库超级用户密码。如果希望保持默认密码或查看输入的新密码，则选择 （显示密码）图标。要将密码复制到剪贴板，使用 （复制到剪贴板）图标。



然后，安装程序将提示您再次记录该密码。记录密码后，选择 **OK （确定）**。

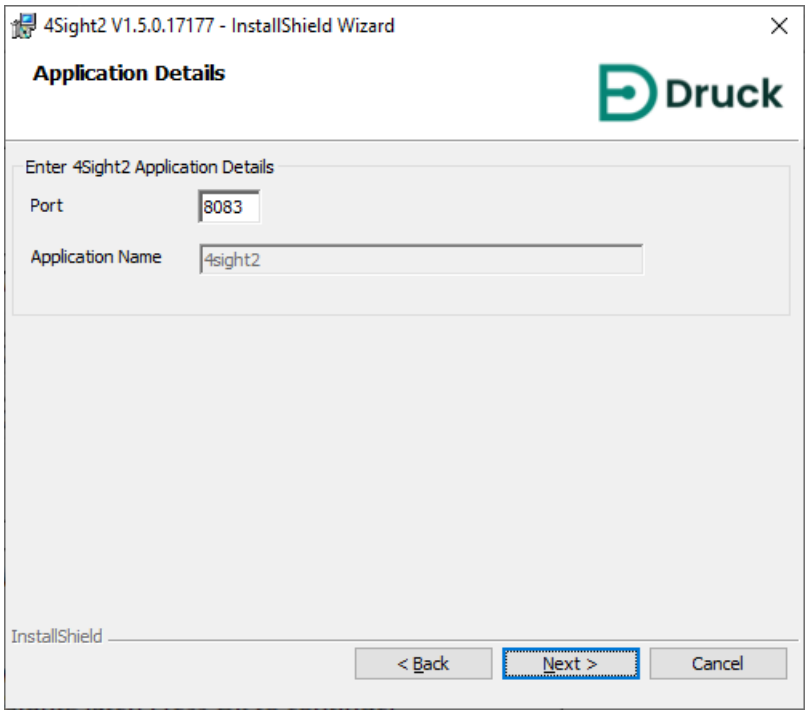


2. 仅当已安装 PostgreSQL 数据库后，用户才能看到此步骤。



Installation Directory （安装目录）：用于指定已安装 PostgreSQL 的路径。它是只读信息。
Password （密码）：用于确认 PostgreSQL 数据库超级用户密码。
Port （端口）：用于指定 PostgreSQL 数据库执行数据库请求时使用的端口号。

3. 在 Application Details （应用程序详细信息）窗口中，输入以下详细信息：

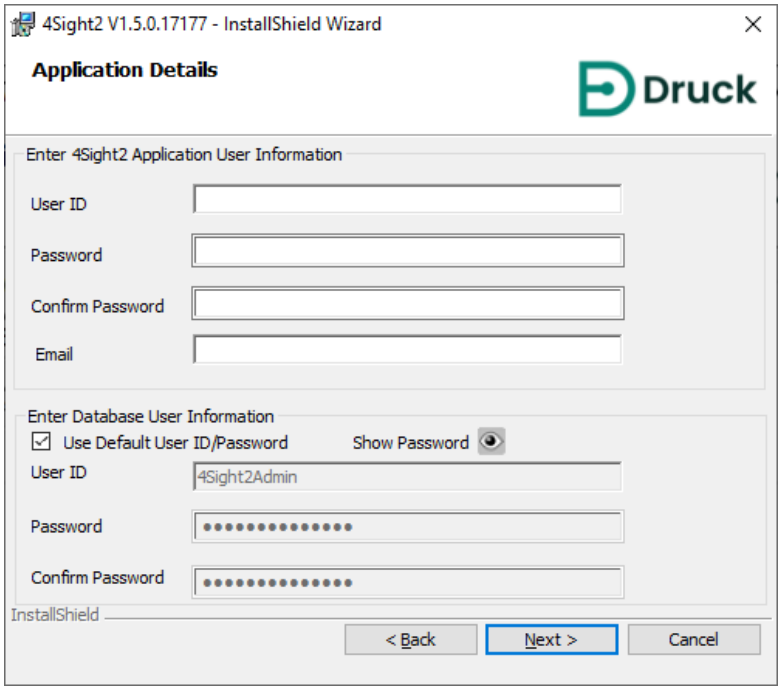


Port （端口）：输入 4Sight2 Web 应用程序用于响应 HTTP 请求的 Tomcat Web 服务器端口。

Application Name （应用程序名称）：输入您将在浏览器中用于连接到 4Sight2 应用程序的应用环境路径。默认情况下为 4sight2。

注：如果端口号已被占用，则联系 IT 团队。用户还可更改端口号，必须记下该端口号以在随后启动应用程序。

4. 选择 **Next （下一步）**，此时将显示 Application User Information （应用程序用户信息）屏幕。

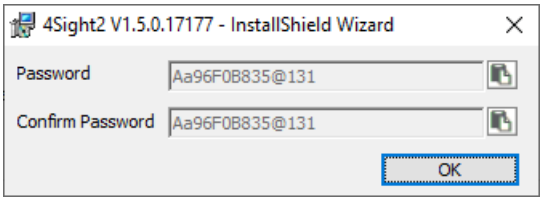


应用程序用户信息：此部分用于输入访问 4Sight2 应用程序时需使用的超级用户名和密码。

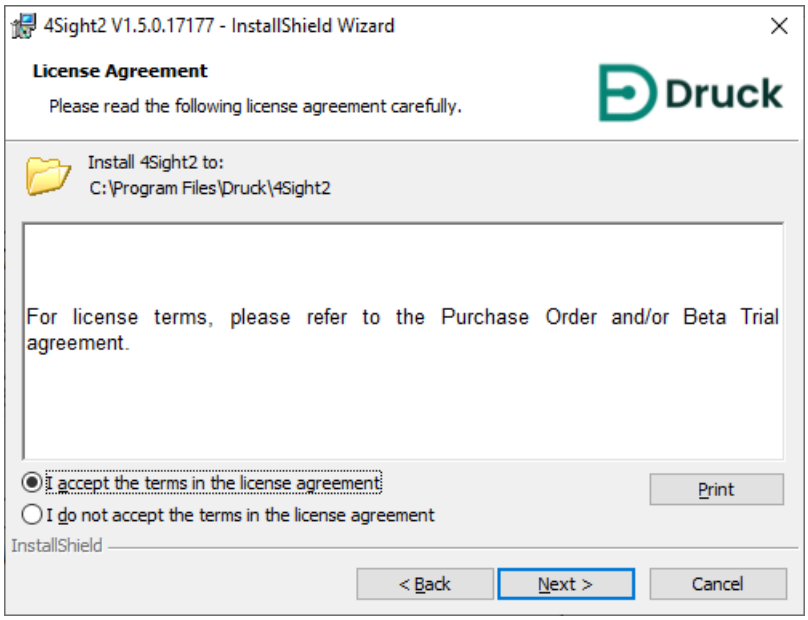
注：安装后访问 4Sight2 应用程序时，将需要此密码。

数据库用户信息：此部分用于输入数据库用户名和密码， 4Sight2 应用程序使用该用户名和密码与 PostgreSQL 数据库通信。

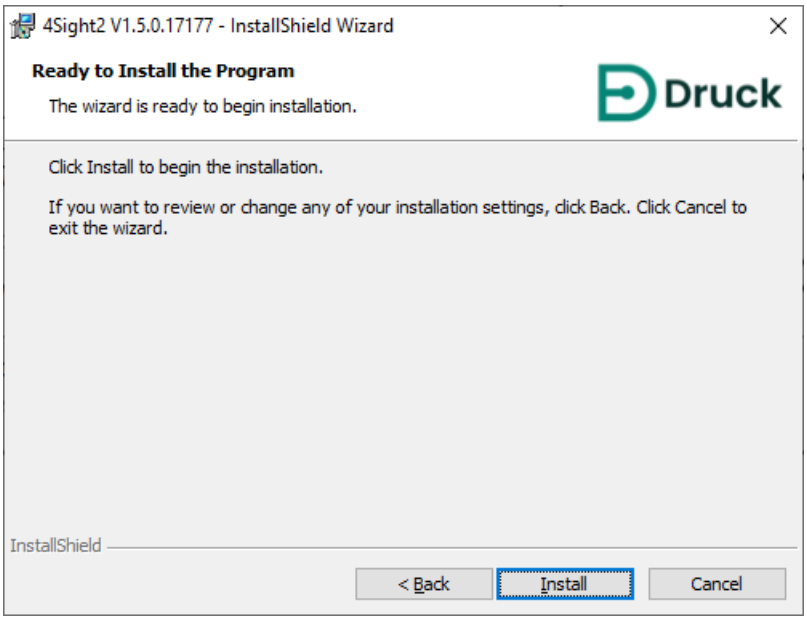
重要事项：用户必须记下数据库密码。丢失密码信息可能导致访问被拒绝或数据丢失。取消选中 UserDefaultPassword（用户默认密码）复选框，更新数据库超级用户密码。如果希望保持默认密码或查看输入的新密码，则选择 （显示密码）图标。要将密码复制到剪贴板，使用 （复制到剪贴板）图标。



5. 阅读许可条款和条件后，选中"I accept the terms in the license agreement"（我接受许可协议中的条款）单选按钮然后单击 **Next**（下一步）。

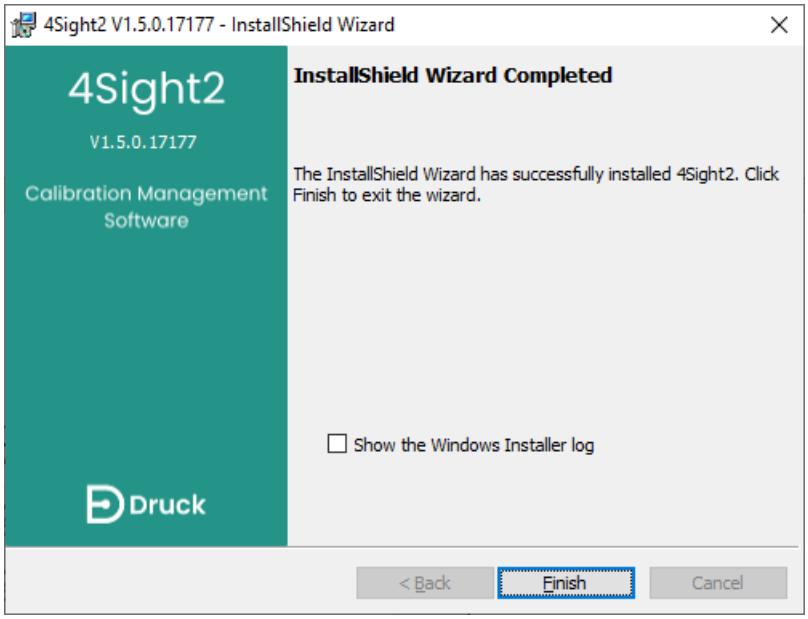


6. 单击 **Install （安装）**可开始安装。将安装与 4Sight2 应用程序和数据库相关的所有软件包。



恭喜！ 4Sight2 应用程序现已成功安装。

7. 单击 **Finish （完成）**按钮关闭窗口，按照下一部分中的操作说明登录 4Sight2 应用程序。



要在服务器本地登录到 4Sight2，则转至 http://计算机名或 IP 地址:端口号/应用程序名称

- **计算机名 –** 已安装 4Sight2 应用程序的计算机的名称。这可通过右键单击本计算机然后选择 Properties （属性）来找到。
- **IP 地址** – 已安装 4Sight2 应用程序的计算机的 IP 地址。这可通过在 Windows 命令窗口中运行“ipconfig”来确定。
- **端口号 –** 应用程序安装过程中在 Tomcat 的 Port Number （端口号）中输入的编号。
- **应用程序名称 –** 应用程序安装过程中在 Application Name （应用程序名称）字段中输入的名称。

安装 4Sight2 测试设备通信器

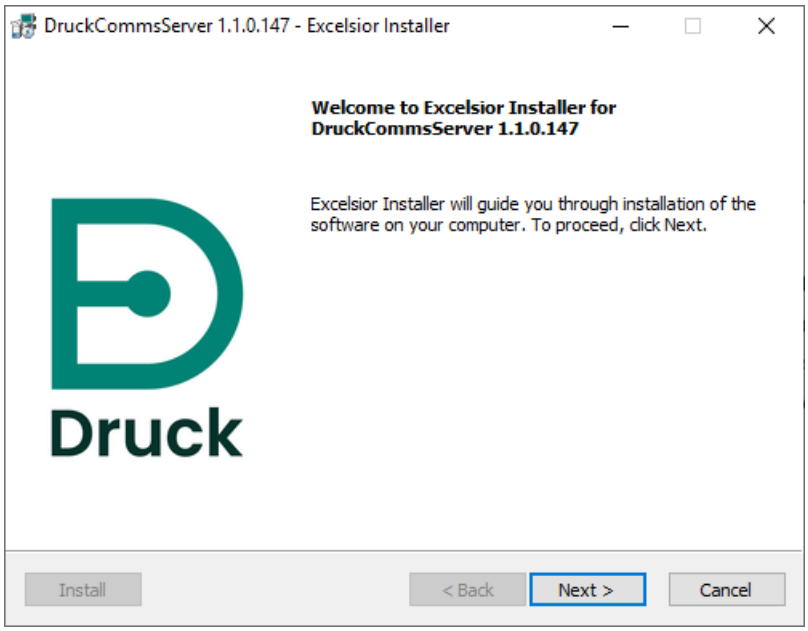
4. 安装 4Sight2 测试设备通信器

1. 测试设备通信器为 Druck 设备提供与 4Sight2 应用程序进行通信的方式。测试设备通信器可以从 4Sight2 安装文件夹进行安装，也可以通过 4Sight2 初始设备通信进行下载。如果安装文件中没有测试设备通信器，则在 4Sight2 应用程序运行且创建范围之后，立即以管理用户身份，使用 4Sight2 菜单导航至 Calibration（校准）> Portable （便携式），参见 4Sight2 用户手册获取导航和范围创建帮助。选择测试设备下拉列表旁边的刷新按钮。如果测试设备通信器未在运行，则会看到以下消息：

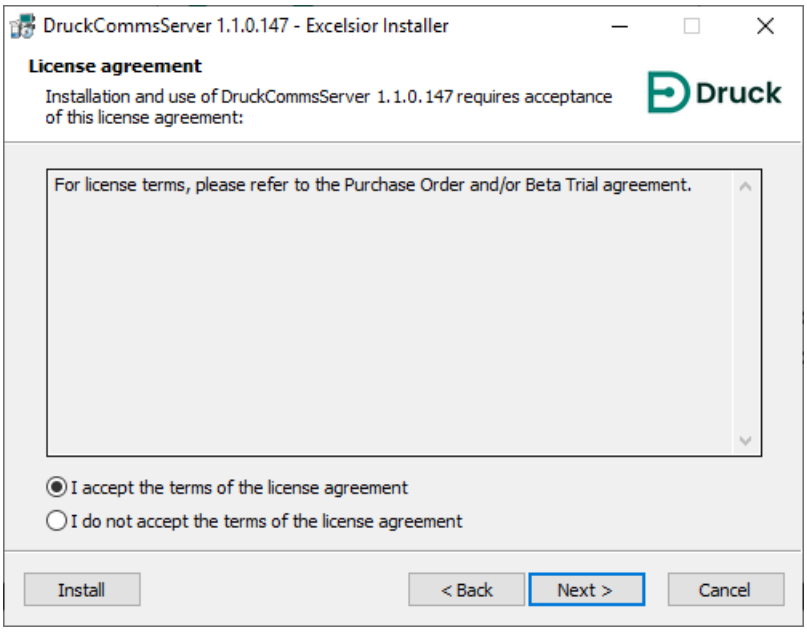
   无法与测试设备进行通信。

   下载测试设备通信器程序包。下载之后，解压缩并运行 setup.exe 进行安装。有关安装说明或故障排查，请参考安装手册。请联系管理员获取帮助。

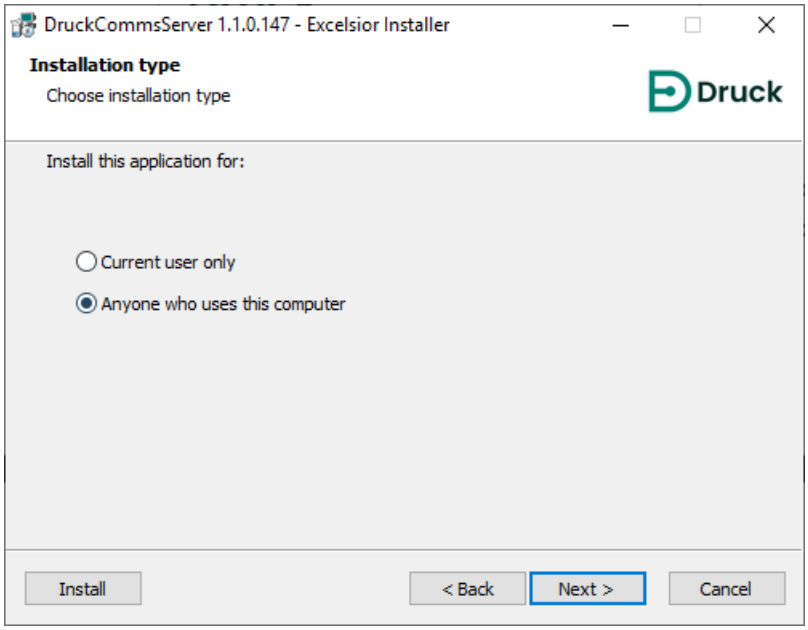
2. 选择 **Download**（下载）可获取测试设备通信器安装文件。
3. 测试设备通信器安装文件是一个 CommsServerInstall Zip 文件。 Comms Server Zip 文件下载后，可以在 4Sight2 安装前和安装后遵循相同的步骤。
4. 从 Comms Server Zip 文件提取文件，双击 setup.exe 文件运行安装程序。
5. 此时显示 DruckCommsServer 安装程序。遵循安装程序中的说明，或遵循本指南中的说明。



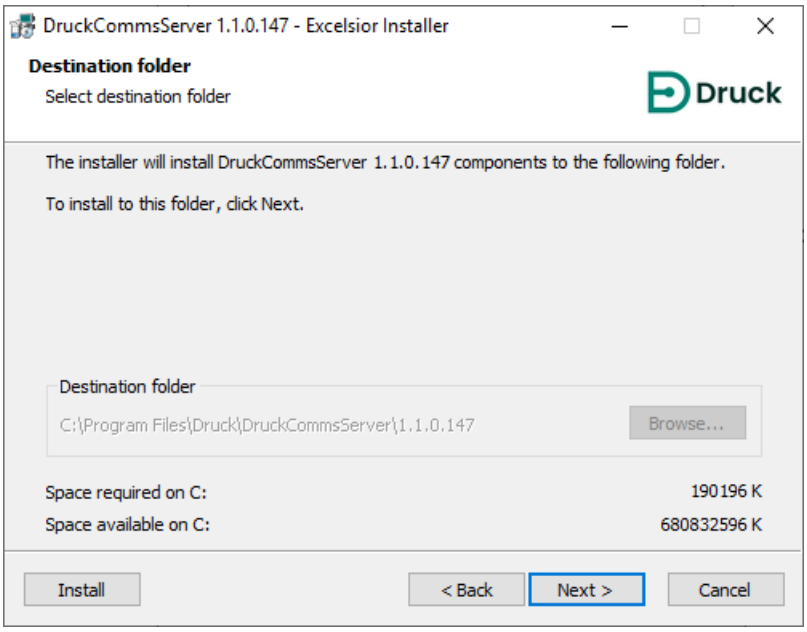
6. 选择 **Next**（下一步）显示许可协议屏幕，然后选择 **I accept the terms of the license agreement**（我接受许可协议中的条款），然后单击 **Next**（下一步）继续。



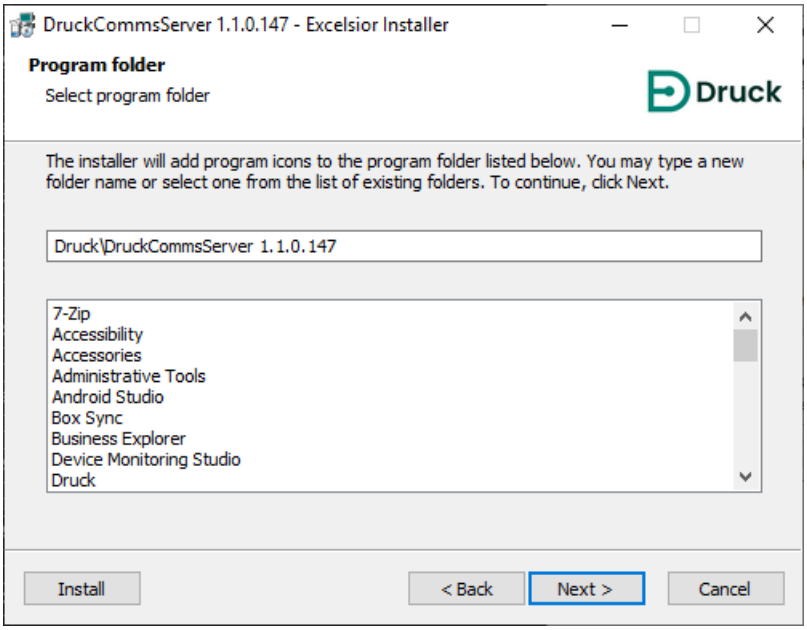
7. 在安装类型屏幕中，选择对本 PC 的所有用户安装 CommsServer 还是仅对当前用户进行安装。



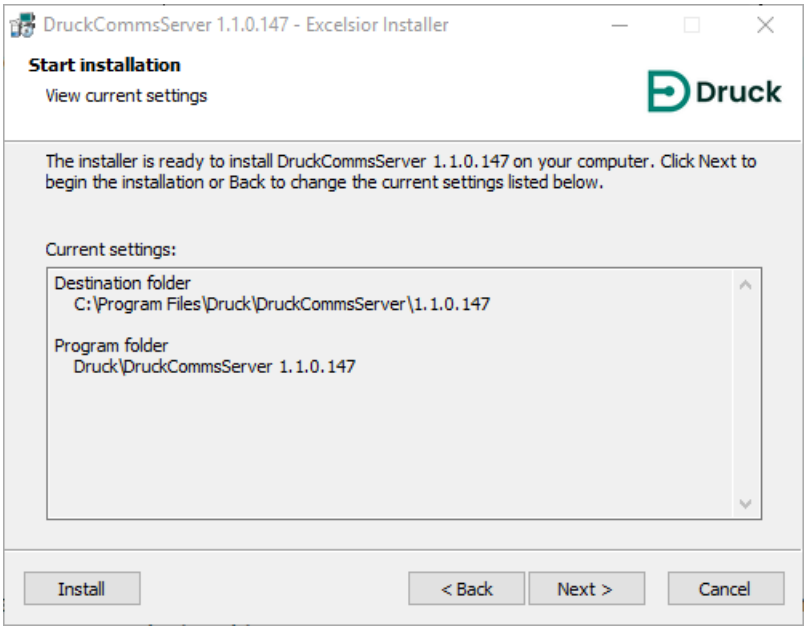
8. 目标文件夹屏幕显示安装 DruckCommsServer 的文件夹。默认情况下为 C:\Program Files\Druck\DruckCommsServer\[应用程序版本]。



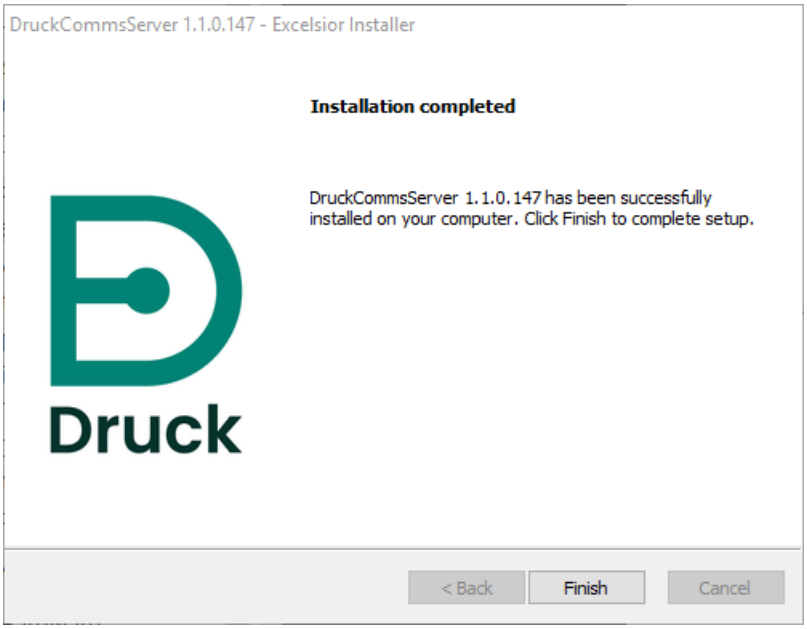
9. 程序文件夹屏幕可用于选择安装程序将程序图标安装到程序文件夹中的位置。



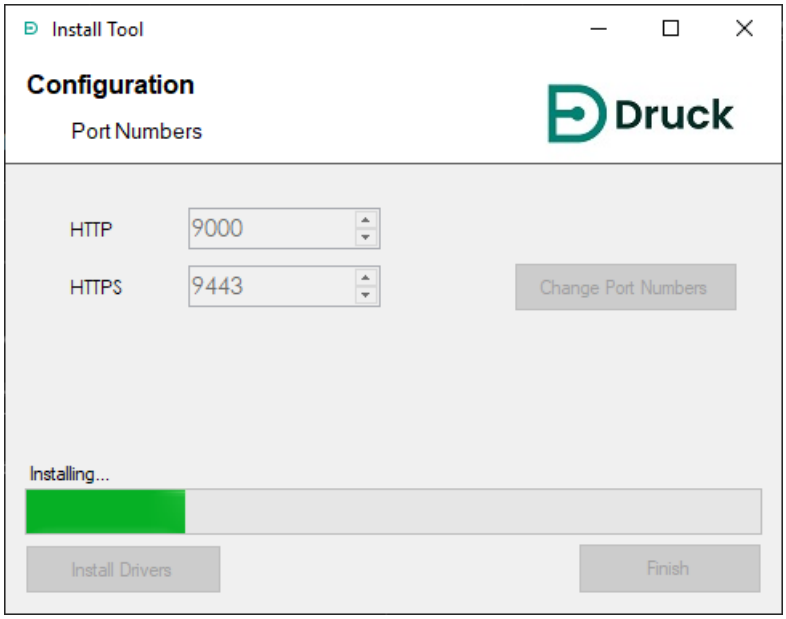
10. 然后显示开始安装屏幕，选择 **Next**（下一步）开始安装。



11. 安装完成后，选择 **Finish**（完成）。

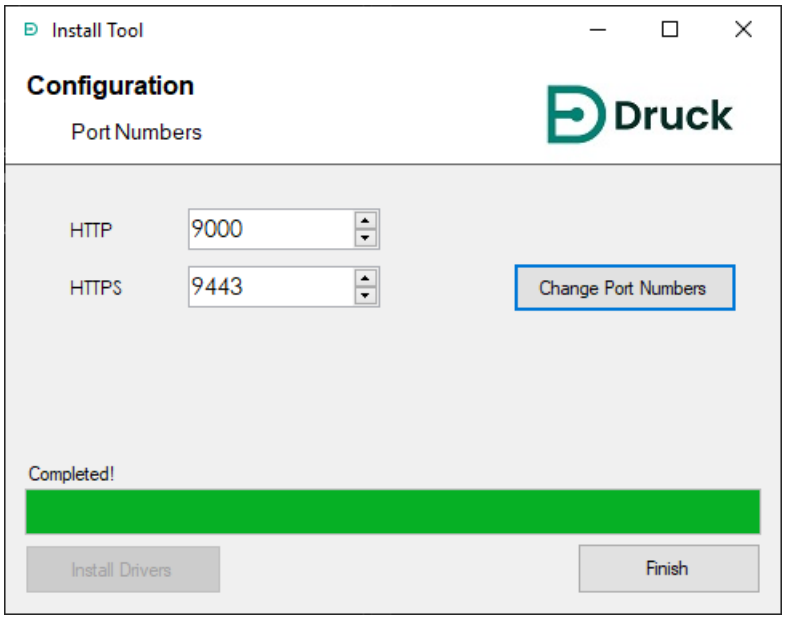


12. 接下来将显示 CommsServer 安装工具应用程序，安装所需的其他驱动程序。



13. 如果不确定 4Sight2 是否使用其他端口号，请联系管理员用户。

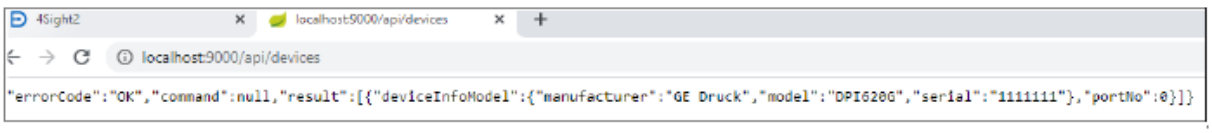
注：可以在安装之后单独运行安装工具，重新配置这些端口号。



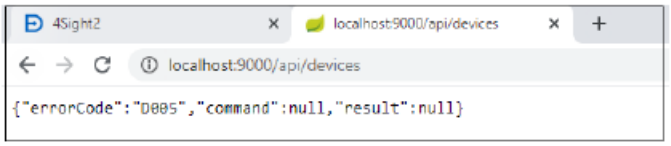
14. 在 Web 浏览器中键入以下 URL，对测试设备通信器进行测试：

    Http:/localhost:[上面使用的 http 端口号，默认为 9000]/api/devices

Web 浏览器应显示已连接的所有设备的列表：



如果未连接任何设备，则会看到以下内容：



注：温度校准仪所需的驱动程序不自动配置。参见第 4.3 节“温度校准仪驱动程序配置”

15. 如果设备驱动程序安装不成功，使用下一节中的步骤，手动配置必需驱动程序。

4.1 手动驱动程序配置

IT 安全政策设置可能会阻止 Druck 驱动程序自动配置安装。如果 4Sight2 无法与以下设备通信，很明显属于这种情况：

获取最新信息 https://www.bakerhughes.com/druck/test-and-calibration-instrumentation/calibration-management-software-4sight2

或者

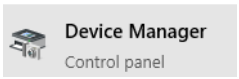
为解决此问题，可手动配置 Druck 驱动程序。如果对此不确定或需要更多帮助，请向当地的 IT 代表咨询。

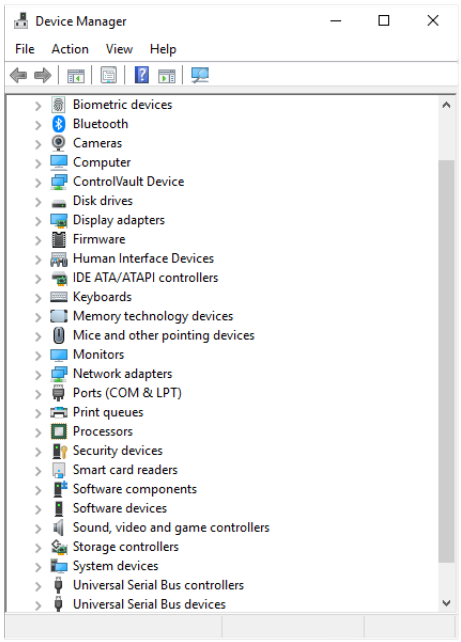
4.1.1 前提条件

要安装驱动程序，需要在计算机上安装 4Sight2 应用程序或可从计算机访问它。尝试安装驱动程序之前，确保从计算机登录到 4Sight2 应用程序。

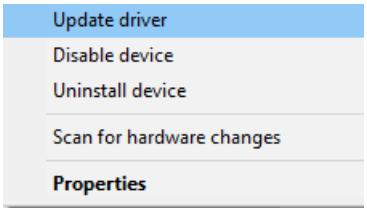
要手动安装驱动程序，请执行以下步骤：

1. 在桌面上，搜索设备管理器，然后运行。

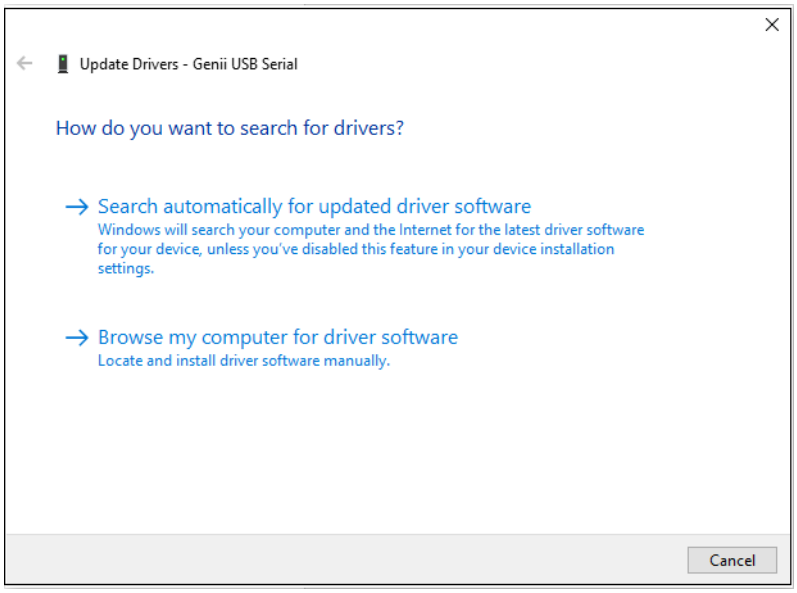




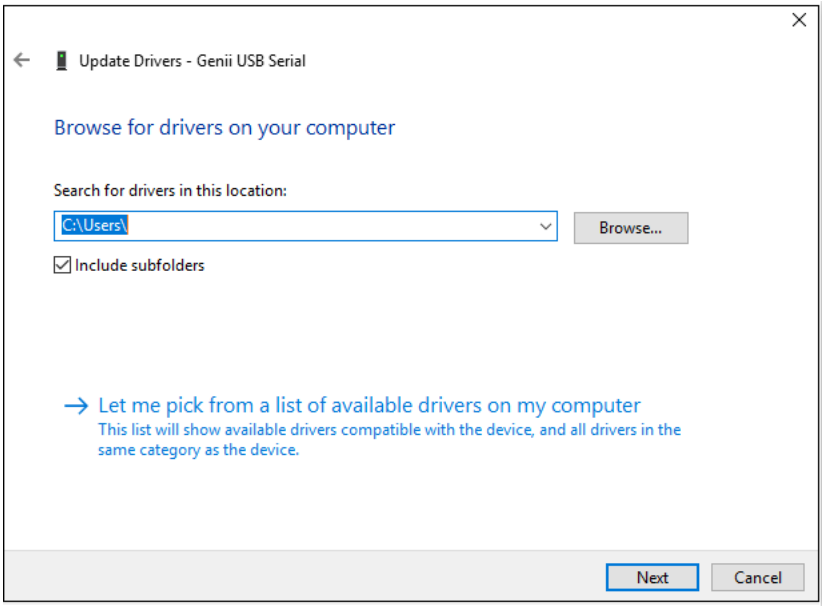
2. 在 USB 设备列表中滚动查找未配置的设备 （“未知设备”或“其他设备”）。右键单击并选择**更新驱动程序**。



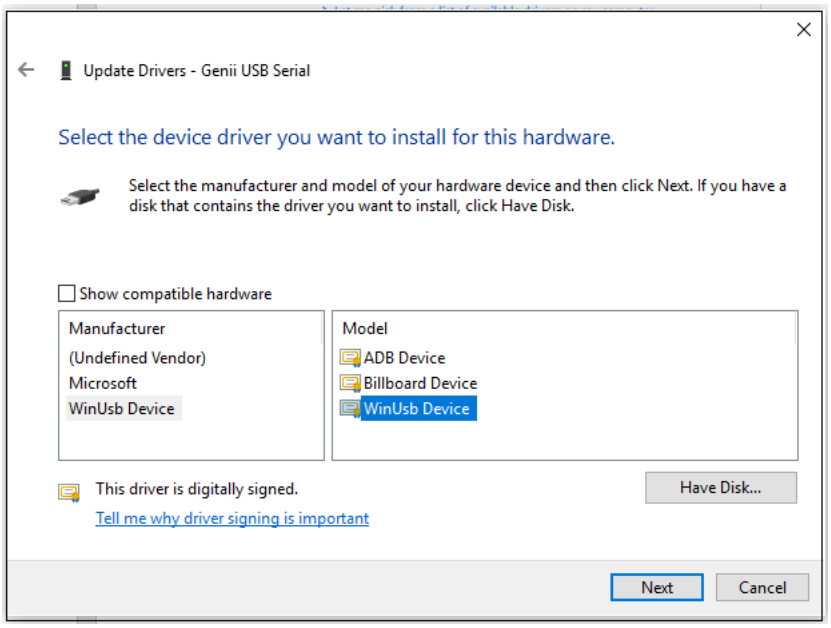
3. 选择**浏览电脑查找驱动程序软件**选项。



4. 选择**从我的电脑的可用驱动程序列表中选择**。

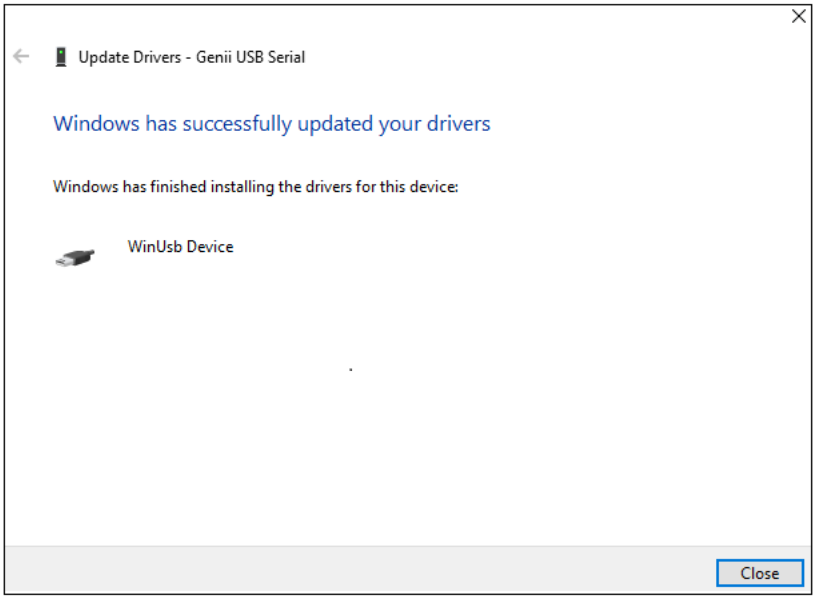


5. 取消选中**显示兼容硬件**，然后对于制造商选择 **WinUsb Device**，型号选择 **WinUsb Device** 。



6. 此时显示以下警告。单击**是**。

7. 此时将显示“Windows 已成功更新您的驱动程序”。



首次连接设备时，对每类设备重复上述步骤。

例如，如果首次连接 PACE 和 Genii，则必须针对 PACE 和 Genii 分别重复上述步骤。 PACE 和 Genii 的后续所有实例都将正常运行而无需执行这些设置。然而，如果之后连接不同类别的设备，如 DPI611/612，则需要对于此类设备再次重复上述步骤。

4.2 对测试设备通信器进行测试

1. 以“技术人员”身份登录到 4Sight2。
2. 转到 **Assets （资产） >> Worklist （工作列表）**。
3. 选择一个或多个范围并将它们分配给便携式或自动校准工作流程。
4. 单击 **Refresh （刷新）**按钮。

5. 单击 **Test Equipment （测试设备）**下拉列表。如果在列表中看到所连接的设备，则说明已正确配置测试设备通信器。

4.3 温度校准仪驱动程序配置

为了使温度校准仪能够与 4Sight2 进行通信，须安装 FTDI 驱动程序。

1. 使用此链接下载 FTDI 驱动程序：https://www.ftdichip.com/Drivers/VCP.htm。
2. 从 zip 文件提取下载的文件，将文件保存到计算机上一个已知位置。
3. 导航至计算机上的 Windows 设备管理器。
4. 从设备列表中选择“端口 （COM 和 LPT） ”，查看温度校准仪。
5. 右键单击该温度校准仪，然后选择更新驱动程序。
6. 选择“浏览电脑查找驱动程序软件”。
7. 在此位置的“搜索驱动程序”搜索框旁边，选择“浏览”。
8. 选择包含驱动程序下载的解压缩文件夹。
9. 选择“下一步”然后关闭。
10. 现在将安装驱动程序。
11. 要在 4Sight2 中测试与温度校准仪的通信，导航至自动校准，然后检查是否可以将温度校准仪选择为 Input Controller （输入控制器）。另外也可以再次运行第 4 节中的步骤 14。

部署指南

5. 部署指南

5.1 部署架构

典型架构包括在 Tomcat Web 服务器内运行的 4Sight2 Web 应用程序和 UAA （用户身份验证和授权）服务器，且在同一计算机上运行 PostgreSQL 数据库。

浏览器客户端 Web 应用程序将连接到 4Sight2 服务器，该服务器使用 PostgreSQL 数据库存储和检索信息。

5.2 物理部署

假设安装 4Sight2 的用户已采取网络安全措施，遵守用户安全政策，包括以下方面：

- 服务器放置在安全位置，且物理访问控制受限。
- 服务器访问控制由有限的授权访问保护。
- 服务器网络由防火墙提供保护，仅允许通过已知端口对众所周知的应用程序进行有限访问。
- 应用程序在自己的环境中运行，只能访问它们自己的文件夹内的数据库和文件系统。

5.3 网络

客户端使用 Web 浏览器通过以太网接口或无线网络连接。无线网络可能存在延迟，具体取决于无线带宽和连接的设备数量。

建议禁用或删除浏览器上安装的任何插件和扩展件。

4Sight2 Web 服务器不得连接到 Internet, 需要进行的任何访问都必须通过内部网或 VPN 来进行。

5.4 部署顺序

PostgreSQL、Tomcat 和 Java Runtime 是运行 4Sight2 应用程序的前提。PostgreSQL 以单独的软件包形式进行安装，而其他软件与该应用程序打包在一起。因此，如果已在用户计算机上安装了 PostgreSQL，则只需要超级用户密码即可连接和配置它。

安装需要拥有相应计算机的 Windows 管理员权限。安装之前，用户必须具有 PostgreSQL 超级用户密码。此外，还必须具有应用程序管理员用户名和密码以及数据库用户名和密码。

在 PostgreSQL 服务器内创建数据库和其他结构时，需要使用 PostgreSQL 超级用户密码。应用程序管理员是该应用程序的首位用户。管理员用户负责创建其他用户并为他们分配不同角色。数据库用户有权访问 4Sight2 和 UAA 数据库。这些用户名凭据用于访问数据库。

该应用程序发布在计算机端口上。默认端口为 8083，用户可在安装时或在以后更改该端口。 Tomcat 中的默认应用环境为 4Sight2。

遵循 Microsoft 或 CIS 规范执行操作系统加固过程对操作系统进行加固。安装过程在安装 4Sight2 服务器之前将指示先安装 PostgreSQL。

测试设备通过 USB 端口连接时，测试设备通信器将安装在客户端计算机上。如果尚未在该计算机上安装测试设备通信器，则将出现消息，提示用户从 4Sight2 服务器下载测试设备通信器然后在该计算机上安装它。测试设备通信器侦听端口 9000，只能在安全层通信。

5.5 部署后的任务

5.5.1 添加用户和组

管理员负责在应用程序中创建不同用户，比如监督员、高级技术人员、技术人员和审核人。管理员可将它们分配给不同的内置默认组。如果需要更多控制或粒度更细的访问控制，则管理员可自定义组然后将特定访问权限分配给它们。

5.5.2 默认密码

对于文件"C:\Program Files\Druck\4Sight2\<<latest folder number>>\apache-tomcat\conf\tomcat-user.xml"中的 Tomcat 用户，我们使用硬编码的默认密码。

建议更改默认密码且始终使用遵循密码设置最佳做法的密码。

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

已实施最佳做法以确保应用程序安全。为了进一步提高安全性，请执行以下任务：

配置文件和文件夹通过仅具有默认访问权限的服务和系统来保护。因此，尝试执行以下任务前，管理员用户对 C:\Program Files\Druck\4Sight2\<<latest folder number>>\apache-tomcat\conf 文件夹仅具有读/写访问权限，因此，使用管理员用户凭据打开命令提示符。

5.5.3 安全通信

本节提供使用自签名的证书在安全模式 （也称为 SSL 模式）下配置 4sight2 的操作说明。继续之前，请阅读 4Sight2 应用程序中定义的假设以及条款和条件。自签名的证书是在 4Sight2 中启用 SSL 的一种方法。或者，也可从诸如 Symantec、 Digicert 等许多供应商处购买第三方 CA 证书。

注：启用 SSL 并不能确保应用程序安全。这是构建安全的 Web 应用程序的最常见做法之一。

5.5.3.1 假设和警告

下列操作说明在以下假设下有效：

需要使用OpenSSLforWindows软件来生成自签名的证书。4Sight2假设您的组织、地区、国家的法律和法规允许使用 OpenSSL 软件。

- Keytool 是由 Java 提供的密钥和证书管理实用工具，用于生成 https 配置中涉及的各种组件。 4Sight2 假设您的组织、地区、国家的法律和法规允许使用 Keytool 实用工具。
- 您需要具有管理员权限才能执行以下配置。有关获取管理员权限的更多信息，请联系当地的 IT 部门。
- 以下步骤需要具备有关计算机进程的基本知识，因此，理想情况下，建议由当地 IT 人员或在他们的指导下执行这些步骤。
- 本文档中包括的诸如主机名、密码、 URL 和文件夹路径等内容仅供参考。确保在执行前相应修改命令。
- 以下章节介绍了两种方案。一种是服务器和客户端位于同一计算机上，另一种是服务器和客户端位于不同计算机上 （即，多客户端方案）。

5.5.3.2 在 Https 中配置 4Sight2 应用程序的步骤

1. 在 Windows 服务中停止 4Sight2
2. 在**管理员模式**下打开命令提示符
3. 通过执行以下命令导航到 4Sight2 安装目录中的以下文件夹：
   cd "C:\Program Files\Druck\4Sight2\<<latest folder number>>\apache-tomcat\conf"
4. 在命令提示符下运行以下命令以检查是否存在 Keytool：**Keytool** -?
   如果不存在，则将环境变量设置为 4Sight2 安装文件夹内的 JRE bin，如下所示。根据安装文件夹更新正确路径。
   C:\Program Files\Druck\4Sight2\<<latest folder number>>\jre\bin
   Set "Path=%Path%;C:\Program Files\Druck\4Sight2\<<latest folder number>>\jre\bin"
5. 要创建新证书，请跳至第 6 步，否则，如果已存在证书，则执行以下操作：
   a. 检查 Java 密钥库中是否存在证书文件 4Sight.jks：
   keytool -list -alias <<主机名>> -storepass <<密钥密码>> -keystore 4Sight.jks
   b. 如果已安装证书，则删除它：
   keytool -delete -noprompt -alias <<主机名>> -storepass <<密钥密码>> -keystore 4Sight.jks
   c. 检查文件 4SightV2PublicKey.cer 是否存在，如果存在，则删除它：
   del "../../app/Certificate/4SightV2PublicKey.cer"
   d. 检查证书是否已位于 Java 的 CACert 中：
   keytool -list -alias <<主机名>> -storepass changeit -keystore "../../jre/lib/security/cacerts"
   e. 如果 java 库中存在证书，则删除它：
   keytool -delete -noprompt -alias <<主机名>> -storepass changeit -keystore "../../jre/lib/security/cacerts" -file "../../app/Certificate/4SightV2PublicKey.cer"
6. 执行以下操作创建新证书：
   keytool -genkey -trustcacerts -keyalg "RSA" -keysize 2048 -validity 1095 -keypass <<密钥密码>> -alias <<主机名>> -keystore 4Sight.jks -storepass <<库密码>> -dname "CN=%COMPUTERNAME%, OU=<<组织单位>>, O=<<组织>>, L=<<位置>>, S=<<州>>, C=<<国家首字母缩写>>" -ext eku:critical=sa
7. 将证书导出到文件 4SightV2PublicKey.cer （请勿更改名称或路径）：
   keytool -export -alias <<主机名>> -keystore 4Sight.jks -storepass <<库密码>> -storetype JKS -file "C:\Program Files\Druck\4Sight2\<<latest folder number>>\app\Certificate\4SightV2PublicKey.cer"
   成功执行命令后，将显示出一条消息，指明："Certificate stored in file C:\Program Files\Druck\4Sight2\<<latest folder number>>\app\Certificate\4SightV2PublicKey.cer"（证书存储在文件 C:\Program Files\Druck\4Sight2\<<latest folder number>>\app\Certificate\4SightV2PublicKey.cer 中）。
8. 将证书导入到 Java CACert 文件中。

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

成功执行命令后，将显示出一条消息，指明 "Certificate was added to keystore"（证书已被添加到密钥库中）。

9. 在 Tomcat 配置文件中添加证书条目。

   a. 打开以下位置中的 server.xml 文件：
   C:\Program Files\Druck\4Sight2\<<latest folder number>>\apache-tomcat\conf\server.xml"

   b. 在 server.xml 中添加以下条目。
   <Connector port="8443" protocol="org.apache.coyote.http11.Http11NioProtocol" maxThreads="150" SSLEnabled="true" sslProtocol="TLSv1.2" keystoreFile="conf/4Sight.jks"
   keystorePass="<<密钥密码>>" keyAlias="tomcat" scheme="https" secure="true" clientAuth="false" />

   c. 注释掉以下部分以禁用 http 连接。
   <connectionTimeout="20000" maxSwallowSize="104857600" port="8083" protocol="HTTP/1.1" redirectPort="8443" relaxedPathChars=""[\]^`{|}+" relaxedQueryChars="&quot;[\]^`{|}+"/>

注：如果未注释掉此部分，则应用程序将无法工作。

10. 至此， 4Sight2 应用程序 Https 配置完成。
11. 要对上面完成的配置进行测试，在 Windows 服务中重启 4Sight2 服务。
12. 打开 Google Chrome，清除浏览器缓存，然后重启该浏览器。
13. 在浏览器中输入以下 URL：https://<<host-name>>:8443/4sight2

- 首次加载该 URL 时，可能需要更长时间。
- 将显示出一个屏幕，指明 "Your connection is not private" （您的连接不是私密连接）。
- 单击 **Advanced** （高级）按钮 >> **Proceed to XX** （继续 XX）链接。
- 如果未看到 4sight2 屏幕，则单击 **Reload** （重新加载）按钮。
- 您将被重定向至 4sight2 页。
- 地址栏中将出现 "Not Secure" （不安全）错误，在 mmc 中注册证书后，该错误将消失。

5.5.3.3 在 Https 中配置安装在服务器计算机上的 DruckCommsServer 的步骤

在执行命令之前将 << >> 中的值替换为合适的数据。

1. 在 Windows 服务中停止 DruckCommsServer。
2. 在**管理员模式**下打开命令提示符。
3. 在命令提示符下运行以下命令以检查是否存在 Keytool：**Keytool -?**

   如果不存在，则将环境变量设置为 4Sight2 安装文件夹内的 JRE bin，如下所示。
   根据安装文件夹更新正确路径。
   C:\Program Files\Druck\4Sight2\<<latest folder number>>\jre\bin
   Set "Path=%Path%;C:\Program Files\Druck\4Sight2\<<latest folder number>>\jre\bin"
4. 执行以下命令导航到 DruckCommServer 安装目录中的以下文件夹：

   cd " C:\Program Files\Druck\DruckCommsServer\<< 通信服务版本 >>"
5. 检测是否存在证书，如果是，则执行以下操作。

a. 检查证书是否已位于 Java 的 CACert 中：
keytool -list -alias tomcat -storepass changeit -keystore cacerts

b. 如果 java 库中存在证书，则删除它：
keytool -delete -noprompt -alias tomcat -storepass changeit -keystore cacerts

c. 从默认的 CommsServer 中删除预先配置的证书：
del 4Sight.jks
del 4SightV2DeviceMngr.pfx

6. 执行以下操作创建新证书：

   keytool -genkey -trustcacerts -keyalg "RSA" -keysize 2048 -validity 1095 -keypass <<密钥密码>> -alias tomcat -keystore CommServer.jks -storepass <<库密码>> dname "CN=localhost, OU=<<组织单位>>, O=<<组织>>, L=<<位置>>, S=<<州>>, C=<<国家首字母缩写>>" -ext eku:critical=sa

7. 将证书导出至文件 DruckCommServer.cer：

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

   成功执行命令后，将显示出一条消息，指明：
   "Certificate stored in file DruckCommServer.cer "（证书存储在文件 DruckCommServer.cer 中）。

8. 将通信服务器证书导入到 Java CACert 文件中。

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

   成功执行命令后，将显示出一条消息，指明 "Certificate was added to keystore"（证书已被添加到密钥库中）。

9. 将 4Sight 证书导入到 Java CACert 文件中。

   keytool -import -noprompt -trustcacerts -alias <<服务器主机名>> -storepass changeit -keystore cacerts -file "C:\Program Files\Druck\4Sight2\<<latest folder number>>\app\Certificate\4SightV2PublicKey.cer"

   成功执行命令后，将显示出一条消息，指明 "Certificate was added to keystore"（证书已被添加到密钥库中）。

10. 编辑 DruckCommsServer 中应用程序属性的密钥库密码。

    打开此文件：
    C:\Program Files\Druck\DruckCommsServer\<<通信服务版本>>\application.properties 并更改以下行：
    keystore = CommServer.jks
    key-store.password= << 库密码 >>
    注：**<< 库密码 >>** 是第 6 步中使用的**库密码**。

11. 重启 4Sight2 和 DruckCommsServer 服务。

5.5.3.4 在 Https 中配置安装在客户端计算机上的 DruckCommsServer 的步骤

1. Keytool 实用工具与 Java 打包在一起，因此，可在计算机上安装 Java，或者无需安装 Java 而直接检查能否使用 Java Keytool。
2. 在 Windows 服务中停止 DruckCommsServer。

3. 在**管理员模式**下打开命令提示符。
4. 在命令提示符下运行以下命令以检查是否存在 Keytool：**Keytool -?**

   如果不存在，则在计算机上安装了 Java 时将环境路径设置为 JRE bin，或者将路径设置为 Keytool，如下所示。

   根据安装文件夹更新正确路径。

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

   Set Path=%Path%; "C:\Program Files\Java\<< Java 版本 >>\bin"
5. 从安装有 4Sight 应用程序的服务器计算机上获取 **4SightV2PublicKey.cer** 文件。此文件位于服务器上，如下所示。

   C:\Program Files\Druck\4Sight2\<<latest folder number>>\app\Certificate\4SightV2PublicKey.cer
6. 将此 **4SightV2PublicKey.cer** 复制到以下路径中：

   C:\Program Files\Druck\DruckCommsServer\<< 通信服务版本 >>
7. 现在，按照第 5.5.3.3 节中的第 4 步至第 8 步操作。
8. 将 4Sight 证书导入到 Java CACert 文件中。

   keytool -import -noprompt -trustcacerts -alias <<服务器主机名>> -storepass changeit -keystore cacerts -file 4SightV2PublicKey.cer

   成功执行命令后，将显示出一条消息，指明 "Certificate was added to keystore"（证书已被添加到密钥库中）。
9. 现在，按照第 5.5.3.3 节中的第 10 步至第 11 步操作。

5.5.3.5 为 4Sight2 生成自签名的证书的步骤

1. 下载并安装 OpenSSL for Windows。
2. 在 Windows 服务中停止 4Sight2 服务。
3. 在 C 盘中创建一个名为 **4Sight2Certificate** 的新文件夹。

   可以选择您拥有管理员权限的任何位置或文件夹名称。
4. 使用记事本在上述文件夹内创建一个新文件，并将该文件保存为 **openssl-ca.cnf**。

   将以下内容复制到该文件中然后保存该文件。

```
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
```

注：更新上面的公司名称并保存文件。这是证书颁发者的名称，它将 出现在管理控制台中。

5. 使用记事本在上述文件夹内创建一个新文件，并将该文件保存为 **openssl-ca.cnf**。

   将以下内容复制到该文件中然后保存该文件。

```
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：更新上述主机名和 IPv4 地址并保存该文件。

6. 使用管理员权限打开命令提示符。
7. 执行以下命令导航到 4Sight2Certificate 文件夹：
   cd "<<full path to 4Sight2Certificate >>"
8. 执行以下命令设置 OpenSSL bin 文件夹路径变量。
   Set path=%path%;"<<openssl 的 bin 文件夹>>"
   默认路径示例：
   Set Path=%Path%;"C:\Program Files\OpenSSL-Win64\bin"
9. 执行以下命令设置 JRE bin 文件夹路径变量。注：下面的路径可能与此不同。
   Set path=%path%;"C:\Program Files\Druck\4Sight2\<<latest folder number>>\jre\bin"
10. 执行以下命令以生成 cacert.pem 和 cakey.pem 文件：
    openssl req -x509 -config openssl-ca.cnf -newkey rsa:4096 -days <<Number of days>> -sha256 -nodes -out cacert.pem -outform PEM
    当提示输入国家、州等信息时，输入正确的证书数据。
11. 执行以下命令以生成 servercert.csr 和 serverkey.pem 文件：
    openssl req -config openssl-server.cnf -newkey rsa:2048 -days <<Number of days>> -sha256 -nodes -out servercert.csr -outform PEM
    当提示输入国家、州等信息时，输入正确的证书日期。
12. 在记事本中创建一个新文件并将其命名为 index.txt。将该文件保存到 4Sight2Certificate 文件夹中。
13. 在记事本中创建一个新文件并将其命名为 serial.txt。将该文件保存到 4Sight2Certificate 文件夹中。
    打开该文件，输入 **01**，保存并关闭该文件。
14. 执行以下命令在文件 servercert.pem 和 serverkey.pem 中生成新证书。
    openssl ca -config openssl-ca.cnf -policy signing_policy -extensions signing_req -out servercert.pem -infiles servercert.csr
    输入 Y 以提交更改。成功执行操作后，将看到数据库被更新。
15. 执行以下命令将现有密钥文件打包为 PFX 格式。
    openssl pkcs12 -export -in servercert.pem -inkey serverkey.pem -certfile cacert.pem -name "<<主机名>>" -out <<主机名>>.p12
    将出现提示，要求输入两次密码。
16. 将 PFX 库转换为按以上提到的 JRE bin 位置分类的 Java 密钥库，即 tomcat/config 路径。
    keytool -importkeystore -srckeystore <<主机名>>.p12 -srcstoretype PKCS12 -destkeystore "C:\Program Files\Druck\4Sight2\<<latest folder number>>\apache-tomcat\conf\4Sight.jks" -deststoretype jks

注：保持两个密钥库的密码相同。确保指向位于 tomcat 的 config 文件夹中的 4Sight.jks，如上所示。
将出现提示，要求输入目标密钥库密码和源密钥库密码。成功执行命令后，将会看到消息 "Import command completed: 1 entries successfully imported"（已完成导入命令：成功导入 1 项）。

17. 将证书从 Java 密钥库导出至以下位置中的文件：

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

注：确保指向位于 tomcat 的 config 文件夹中的 4Sight.jks，如上所示。
成功执行命令后，将得到"证书已存储到文件中"的消息。

18. 将证书文件导入到 4sight2 安装目录中的 cacerts 文件夹中。

注：路径可能有所不同，具体取决于安装目录和 4sight2 版本。

keytool -import -noprompt -trustcacerts -alias <<主机名>> -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：由于一些原因，您尝试创建的别名已存在，运行以下命令先删除它，然后执行上述命令创建一个新别名：

keytool -delete -noprompt -trustcacerts -alias <<主机名>> -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"

成功执行此命令后，将会收到 "Certificate was added to keystore"（证书已被添加到密钥库）消息。

19. 在 server.xml 文件（位于 C:\Program Files\Druck\4Sight2\<<latest folder number>>\apache-tomcat\conf 文件夹中）中进行以下更改：

a. 在 server.xml 中添加以下条目。

```
<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. 注释掉以下部分以禁用 http 连接。

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

20. 这将完成 4Sight2 的 https 配置。因此，现在从 Windows 服务中启动 4sight2 服务。

5.5.3.6 为安装在服务器计算机上的 DruckCommsServer 配置自签名的证书的步骤

此处，我们假定您已执行第 5.5.3.5 节中的步骤成功将 4sight2 应用程序转换为 HTTPs，并且 **4Sight2Certificate** 文件夹中已包含以下文件：

- openssl-server.cnf
- openssl-ca.cnf
- cacert.pem
- cakey.pem
- index.txt
- serial.txt
- 4SightV2PublicKey.cer （可将此文件移至 C:\Program Files\Druck\4Sight2\<<latest folder number>>\app\Certificate 文件夹中）

1. 创建一个名为 **CommserverCertificate** 的新文件夹，复制上述这些文件并进行如下更改：

- openssl-server.cnf

  在 **req** 部分下，将 **default_keyfile** 值更改为 "**DruckCommServerCertKey.pem**"。

  - 在 **server_distinguished_name** 下，将 **commonName** 值更改为 "**localhost**"。
  - 在 **alternate_names** 下，将 **DNS.1** 值更改为 "**localhost**"。
  - 在 **alternate_names** 下，将 **IP.1** 值更改为 "**127.0.0.1**"。
  - 保存该文件。

- openssl-ca.cnf （请勿更改其中任何内容）。
- cacert.pem （请勿更改其中任何内容）。
- index.txt （删除其中所有内容，形成一个空文件）
- serial.txt （删除其中除 01 条目以外的所有内容）。

2. 在 Windows 服务中停止 DruckCommsServer 服务。
3. 使用管理员权限打开命令提示符。
4. 执行以下命令导航到 **CommserverCertificate** 文件夹：

   cd "<<CommserverCertificate 的完整路径>>"

5. 执行以下命令设置 OpenSSL bin 文件夹路径变量。

   Set path=%path%;"<<openssl 的 bin 文件夹>>"

   默认路径示例：
   Set Path=%Path%;"C:\Program Files\OpenSSL-Win64\bin"

6. 执行以下命令设置 JRE bin 文件夹路径变量。注：下面的路径可能与此不同。

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

7. 完成此操作后，使用以下命令来创建一个通信服务器证书请求：

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

   执行此命令后，将在 **DruckCommServer.csr** 中有一个请求，并在 **DruckCommServerCertKey.pem** 中有一个私钥。

8. 然后，执行以下命令使用您的 CA 对 csr 请求进行签名：

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

9. 接下来，通过以下命令使用别名 **tomcat** 为通信服务器创建一个 PFX 文件：

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

10. 使用 Keytool 将 PFX 库转换为 Java 密钥库

    注：保持两种密钥库的密码相同。

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

11. 现在，将证书导入到 cacert 中。

    a. 现在，删除安装时默认的现有 tomcat 别名：

    keytool -delete -noprompt -trustcacerts -alias tomcat -storepass changeit -keystore "C:\Program Files\Druck\DruckCommsServer\<< 通信服务版本 >>\cacerts"

    b. 删除现有别名 tomcat 后，使用以下命令将证书导入到 cacerts 中：

    keytool -import -noprompt -trustcacerts -alias tomcat -storepass changeit -keystore "C:\Program Files\Druck\DruckCommsServer\<< 通信服务版本 >>\cacerts" -file DruckCommServerCert.pem

12. 现在，我们需要将 4sight 公钥导入到通信服务器 cacert 中进行通信身份验证，为此，执行以下命令：

    keytool -import -noprompt -trustcacerts -alias <<4sight 服务器主机名>> -storepass changeit -keystore "C:\Program Files\Druck\DruckCommsServer\<< 通信服务版本 >>\cacerts" -file "C:\Program Files\Druck\4Sight2\<<latest folder number>>\app\Certificate\4SightV2PublicKey.cer"

13. 完成上述所有操作后，当前 **CommserverCertificate** 文件夹中将包括 **DruckCommServer.pfx** 和 **CommServer.jks**。

    复制这些文件并将它们粘贴到 "C:\Program Files\Druck\DruckCommsServer\<< 通信服务版本 >>\" 目录中。然后，从同一位置编辑 **application.properties**，按以下所示更改属性值：

    a. Keystore = CommServer.jks

    b. key-store.password = <<密钥库密码>>

    c. key-store.type=JKS

5.5.3.6.1 在 Windows 中安装 4sight 和 DruckCommsServer 的证书

1. 打开“运行”对话框并运行 "mmc" 然后按 Enter。
2. 转到“文件”并选择“添加/删除管理单元”。
3. 从左侧菜单中，选择“证书”。点按“添加”然后选择“计算机帐户 >> 下一步 >> 完成”。然后单击“确定”。
4. 展开证书 （本地计算机）部分。展开“受信任的根证书颁发机构”。

   在其中，右键单击“‘证书’文件夹 >> 全部任务 >> 导入”。

   选择“cacert.pem >> 下一步 >> 完成”。

   因此，我们的自定义证书颁发机构将成功安装在受信任的颁发机构下。

完成执行所有这些步骤后，启动 DruckCommsServer 服务。

5.5.3.7 为安装在客户端计算机上的 DruckCommsServer 配置自签名的证书的步骤

要将 DruckCommsServer 转换为 HTTPs，需要使用 Java Keytool 和 OpenSSL 实用工具。

1. Keytool 实用工具与 Java 打包在一起，因此，可在计算机上安装 Java，或者无需安装 Java 而直接检查能否使用 Java Keytool。
2. 下载并安装 OpenSSL for Windows。
3. 执行以下命令设置 OpenSSL bin 文件夹路径变量。

   Set path=%path%;"<<openssl 的 bin 文件夹>>"

   默认路径示例：
   Set Path=%Path%;"C:\Program Files\OpenSSL-Win64\bin"
4. 执行以下命令设置 JRE bin 文件夹路径变量。

   C:\Program Files\Java\<< Java 版本 >>\bin
   Set Path=%Path%; "C:\Program Files\Java\<< Java 版本 >>\bin"
5. 在 Windows 服务中停止 DruckCommsServer 服务。
6. 在驱动器 C 或您要使用的任何其他驱动器中创建一个名为 **CommserverCertificate** 的新文件夹。
7. 在服务器计算机上的 C:\Program Files\Druck\4Sight2\<<latest folder number>>\app\Certificate 文件夹上获取 4sight2 公共证书文件 **4SightV2PublicKey.cer**，然后将该文件复制到 **CommserverCertificate** 文件夹中。
8. 现在，按照第 5.5.3.5 节中的第 4 步和第 5 步，在 **CommserverCertificate** 文件夹中创建 **openssl-server.cnf** 和 **openssl-ca.cnf**，然后按照第 12 步和第 13 步在该文件夹中创建 index.txt 和 serial.txt。
9. 现在， CommServerCertificate 文件夹中将具有五个文件：

   a. openssl-server.cnf
   b. openssl-ca.cnf
   c. index.txt
   d. serial.txt
   e. 4SightV2PublicKey.cer
10. 使用管理员权限打开命令提示符。

    执行以下命令导航到 CommserverCertificate 文件夹：
    cd "<<CommserverCertificate 的完整路径>>"
11. 执行以下命令以生成 cacert.pem 和 cakey.pem 文件：

    openssl req -x509 -config openssl-ca.cnf -newkey rsa:4096 -sha256 -nodes -out cacert.pem -outform PEM

    当提示输入国家、州等信息时，输入正确的证书数据。
12. 现在，执行第 5.5.3.6 节中的第 1 步更改 **CommserverCertificate** 文件夹中的文件的内容。
13. 现在，执行第 5.5.3.6 节中的第 7 步至第 11 步。
14. 现在，我们需要将 4sight 公钥导入到通信服务器 cacert 中进行通信身份验证，为此，执行以下命令：

    keytool -import -noprompt -trustcacerts -alias <<4sight 服务器主机名>> -storepass changeit -keystore "C:\Program Files\Druck\DruckCommsServer\<< Communication Service version >>\cacerts" -file 4SightV2PublicKey.cer
15. 完成上述所有操作后，当前 **CommserverCertificate** 文件夹中将包括 **DruckCommServer.pfx** 和 **CommServer.jks**。

复制这些文件并将它们粘贴到 **"C:\Program Files\Druck\DruckCommsServer\<< 通信服务版本 >>\"** 目录中。然后，从同一位置编辑 **application.properties**，按以下所示更改属性值：

a. Keystore = CommServer.jks

b. key-store.password = <<密钥库密码>>

c. key-store.type=JKS

5.5.3.7.1 在 Windows 中安装 DruckCommsServer 的证书

1. 打开“运行”对话框并运行 "mmc" 然后按 Enter。
2. 转到“文件”并选择“添加/删除管理单元”。
3. 从左侧菜单中，选择“证书”。点按“添加”然后选择“计算机帐户 >> 下一步 >> 完成”。然后单击“确定”。
4. 展开证书 （本地计算机）部分。展开“受信任的根证书颁发机构”。

   在其中，右键单击“‘证书’文件夹 >> 全部任务 >> 导入”。

   选择“cacert.pem >> 下一步 >> 完成”。

   因此，我们的自定义证书颁发机构将成功安装在受信任的颁发机构下。

完成执行所有这些步骤后，启动 DruckCommsServer 服务。

如果只是希望检查是否已将 DruckCommsServer 成功转换为 https，则在 Google Chrome 标签中打开以下链接：**https://localhost:9443/api/devicemanager/version**（如果已更改，提供您的通信服务器端口号，但默认值为 9443）

5.5.3.8 在 4Sight2 中验证证书

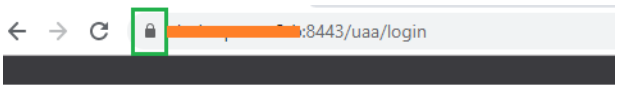
1. 重启服务器 PC。
2. 在 Windows 服务中，选择“打开”重启 4Sight2 和 DruckCommsServer 服务。
3. 打开 Google Chrome，清除浏览器缓存并重启 Google Chrome。确保没有其他 Google Chrome 实例在运行。
4. 在地址栏中输入以下 URL，然后按 Enter。

   Https://<<服务器主机名>>:8443/4sight2

   注：需要使用上述 URL 中的主机名。

5. 使用正确的 HTTPS URL，应能看到登录屏幕。

   注：红色错误从地址栏消失。如果链接仍不安全，则重启计算机，然后转至第 3 步。



4Sight2 安装常见问题

6. 4Sight2 安装常见问题

6.1 设置和安装

问题 1：我所属公司在全球不同地区设有多个站点。设置 4Sight2 的最佳方法是什么？

回答：这取决于如何维护和运营这些站点。如果所有站点都通过中央 IT 中心进行维护和运营，则可在中央安装单个 4Sight2 许可证。所有站点都通过网络或局域网访问 4Sight2。另一方面，如果拥有作为单独实体的自营和自管理的子公司，则可购买多个 4Sight2 许可证。

问题 2：如果我购买了多个 4Sight2 许可证，它们之间是否进行通信？

回答：否。每个 4Sight2 许可证都是孤立的单独软件，需要自行安装应用程序并具有自己的数据库。各个单独安装之间无任何通信。请联系 4Sight2 团队以获取更多解释或讨论任何特殊要求。

问题 3：如何下载 4Sight2？

回答：可从公司网站轻松下载 4Sight2。以下是链接。

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

或

致电销售办事处并发出采购订单。然后，应会收到通过 U 盘提供的演示版本。

问题 4：能否在非 Windows 操作系统上安装 4Sight2？

回答：不能。只有 Windows 平台支持 4Sight2。

问题 5：我已下载并安装 4Sight2，我该如何访问 4Sight2？

回答：4Sight2 是基于 Web 的软件。因此，安装 4Sight2 时不会在桌面或计算机上生成图标。要访问 4Sight2：

- 打开 Google Chrome，在地址栏中粘贴以下 URL，然后按 Enter。
- 如果在同一计算机上安装了 4Sight2，则使用 http://localhost:<应用程序端口号> /4sight2；如果 4Sight2 安装在同一网络的不同计算机上，则使用

  Http://<计算机名称或 IP 地址>:<应用程序端口号>/4sight2
- 在 Google Chrome 上创建书签以供未来参考。

问题 6：4Sight2 安装程序找不到 Postgres 数据库文件

请确保安装程序已被解压缩到本地位置，且可执行文件正在从磁盘 Disk 1 文件夹运行。确保安装程序已被解压缩到的本地位置不具有长路径名，否则还会导致在查找安装程序必需文件时出错。

问题 7：如果在升级过程中的任何阶段取消升级会发生什么？

回答：如果管理员在任何阶段取消升级过程，则将回滚到 1.4 版，且应能启动和运行。管理员需要再次启动升级过程来成功执行升级。

问题 8：安装 4Sight2 应用程序时，如果用户看到此消息“Please enter valid port number.To know valid port numbers please refer installation manual”（请输入有效的端口号。要了解有效端口号，请参考安装手册）

回答：以下是无效端口号范围，请选择有效端口继续安装

- 端口 0 至 1024 保留用于 TCP 连接
- 不安全端口的列表 - 2049、 3659、 4045、 6000、 6665-6669、 65535

问题 9：使用 https 的 4Sight2 无法在系统中工作

回答：遵循将要安装 4sight2 应用程序的计算机的域名语法

<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> ::= 52 个字母字符中的任何一个：大写的 A 到 Z 和

小写的 a 到 z

<digit> ::= 0 到 9 十个数字中的任何一个

注：域名中允许使用大小写字母。拼写相同但大小写不同的两个名称被视作相同。

6.2 测试设备通信器常见问题

问题 1：我已完成安装手册中的所有步骤，但仍无法在列表中看到我的设备。

回答：如果在执行这些步骤后仍无法在列表中找到测试设备，则重新安装 4Sight2 驱动程序。为此，转到 **控制面板 >> 程序和功能**，从列表中卸载 DruckCommsServer。重新安装测试设备通信器。

问题 2：出现一条错误消息“**找不到任何设备**”

回答：要解决此问题：

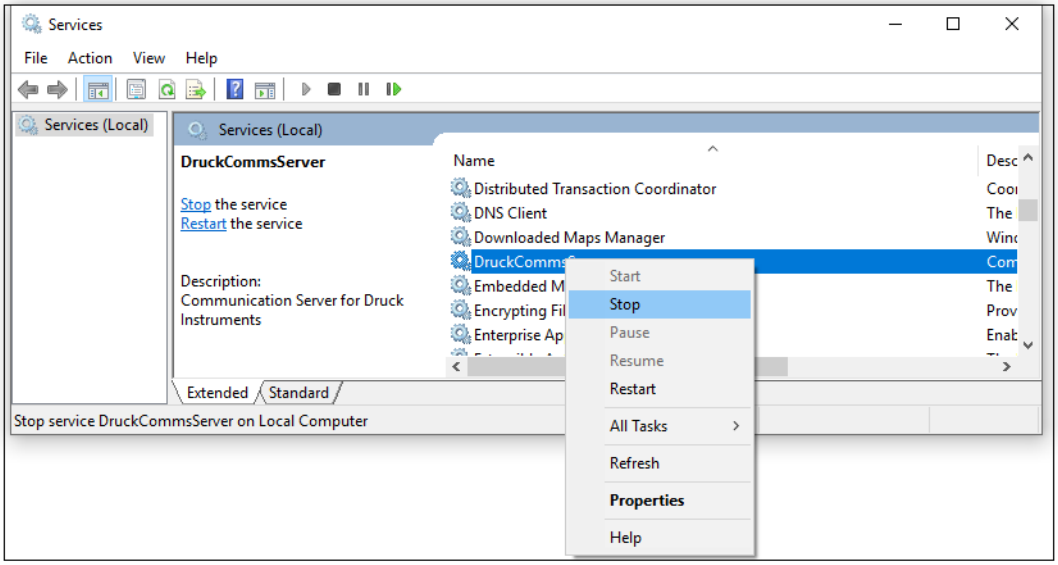
- 确保使用 USB 电缆正确连接设备。为检查这一点，转到设备管理器并在列表中找到相应设备。理想情况下，应能在**通用串行总线设备**部分下找到相应设备。如果在“其他设备”下看到相应设备，则需要执行上述设置以将该设备配置为 USB 设备。
- 确保设备处于通讯模式。请参阅上述第 1 步。
- 确保驱动程序路径正确指向 C:\Windows\INF…。请参阅上述第 2 步。

问题 3：单击“刷新”或列表中的测试设备时，出现一条错误消息‘**Internal Server Error**’（**内部服务器错误**）。

回答：要解决此问题：

- 转到 Windows Services （Windows 服务）（亦称为“服务”）。

- 右键单击列表中的 **DruckCommsServer** 服务然后单击**重新启动**。



- 转到 4Sight2 >> 单击**刷新**按钮。现在应能在列表中看到相应设备。

问题 4：出现一条错误消息**"通信错误"**。

回答：有时，软件因多种原因而无法与设备正常通信，比如 USB 触点松脱、设备断开、设备正忙着执行其他任务、服务器正忙着执行其他任务等。再次单击 Refresh （刷新）按钮，该问题应已解决 （尝试此操作 2-3 次）

但是，如果仍然持续出现此错误，则尝试以下步骤：

- 重启设备 (Genii / PACE)，确保可以安全重启，且设备未在执行关键操作。重试。此外，还请确保设备仍然处于连接状态。

如果上述步骤无效，则按照上述第 3 步中的说明操作，重启 **DruckCommsServer 服务**。

安装故障排查

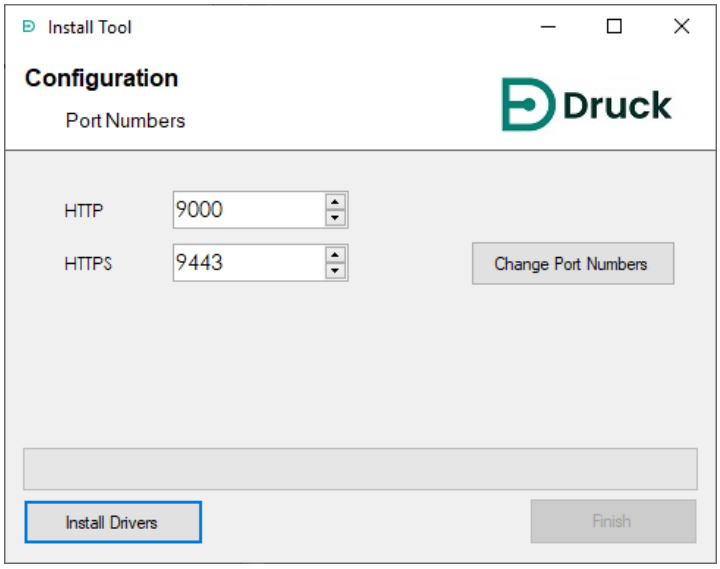
7. 安装故障排查

7.1 测试设备通信器问题

使用 4Sight2 与测试设备进行通信，不返回任何测试设备，但与测试设备通信器直接联系时，通信器会返回 json 字符串。这可能是由于两个主要问题之一导致的：

- 端口号配置不正确 - 请联系管理员用户，了解 4Sigth2 使用哪些端口与测试设备通信器联系。

  知道应使用哪些端口后，导航至 C:\Program Files\Druck\DruckCommsServer\[版本]，然后运行 CommsServerInstallTool.exe



编辑端口号，然后单击 **Change Port Numbers （更改端口号）**按钮。等待服务重启。现在端口号已更改。选择 **Finish （完成）**按钮。

- 测试设备通信器未配置为 Https，而 4Sight2 进行了此配置。

  联系管理员安装测试设备通信器的自签名证书。

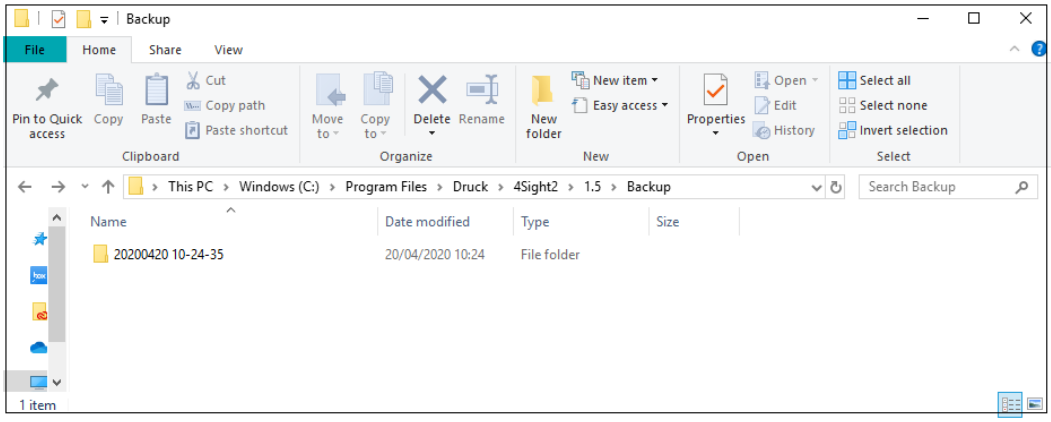
7.2 Postgres 数据库备份

请参考 4Sight2 用户手册 - 123M3138，了解有关 Postgres 数据库备份的信息。

7.3 Postgres 数据库还原

假设已使用 4Sight 应用程序执行了数据库备份。

4Sight 应用程序 （版本 1.4 和更高版本）提供了用于启动备份 （用户启动 / 计划）的界面。此操作将在服务器上的 4Sight 安装目录中的备份文件夹下创建文件。每次启动备份后，都将在备份文件夹中创建一个新的文件夹，该文件夹的名称格式为 YYYYMMDDHHSS （年、月、日、小时和秒），具体取决于成功完成备份后的日期和时间。



建议在单独媒体上对备份文件夹的内容进行备份。

每个文件夹包含 5 个文件。

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

*.bck 文件的后缀包含 4Sight 应用程序版本。请确保还原与所用的应用程序的准确版本相匹配的数据库。该应用程序不支持更高/更低版本的数据库。注意，版本名称中包含一个下划线 (_) 而不是句点 (.)，比如，是 1_4 而不是 1.4。在还原步骤中使用以下命令时，请确保使用已安装的 4Sight 的正确版本替换 <应用程序版本>。

metadata.properties 文件包含启动备份过程中输入的备份名称。

SHA 256 校验

一个备份包含 3 个文件 - 每个数据库一个，扩展名为 .bck。 metadata.properties 文件包含每个备份文件的 SHA 256。

1. 以管理员身份打开命令提示符，将目录切换到包含所选备份文件的文件夹。
2. 使用以下命令计算每个文件的 SHA256。

   certutil -hashfile 4Sight**<应用程序版本>**.bck SHA256

   certutil -hashfile 4Sightaudit**<应用程序版本>**.bck SHA256

   certutil -hashfile uaa**<应用程序版本>**.bck SHA256

3. 继续执行还原步骤前，检查每个文件的 SHA 256 是否与元数据文件中提到的 SHA 256 一致。如果命令提示符中的校验和与元数据文件中的校验和完全相同，则说明备份文件有效，可以用于还原。仅当它们相同时，才能继续执行还原步骤。

7.4 还原步骤：

1. 以管理员身份登录到 4Sight 服务器。
2. 找到 Postgres 数据库正在其上运行的端口。可在 <4Sight 安装目录>\apache-tomcat\webapps\application.properties 文件内的属性 spring.datasource.url 中找到该端口。以管理员身份使用记事本打开此文件。端口号即位于以下内容之前的数字：4Sight**<应用程序版本>**
3. 以管理员身份从命令提示符使用 postgres 用户名登录到 psql 命令行实用程序：
   C:\Program Files\PostgreSQL\11\bin\psql" --port=<DB_PORT> postgres postgres
4. 该应用程序使用的数据库用户可在 <4Sight 安装目录>\apache-tomcat\webapps\application.properties 文件内的属性 spring.datasource.username 中找到。以管理员身份使用记事本打开此文件。
5. 删除 *_temp 数据库 （如果存在），然后在 psql 提示符后运行以下命令来创建空白 *_temp 数据库：

   DROP DATABASE IF EXISTS "4Sight**<应用程序版本>**_temp";
   CREATE DATABASE "4Sight**<应用程序版本>**_temp" WITH TEMPLATE template0 OWNER "**<数据库用户>**"
   LC_COLLATE = "C" LC_CTYPE = "C" TABLESPACE = "4Sight_**<应用程序版本>**_4Sight";
   DROP DATABASE IF EXISTS "4Sightaudit**<应用程序版本>**_temp";
   CREATE DATABASE "4Sightaudit**<应用程序版本>**_temp" WITH TEMPLATE template0 OWNER "**<数据库用户>**" LC_COLLATE = "C" LC_CTYPE = "C" TABLESPACE = "4Sight_**<应用程序版本>**_4Sightaudit";
   DROP DATABASE IF EXISTS "uaa**<应用程序版本>**_temp";
   CREATE DATABASE "uaa**<应用程序版本>**_temp" WITH TEMPLATE template0 OWNER "**<数据库用户>**"
   LC_COLLATE = "C" LC_CTYPE = "C" TABLESPACE = "4Sight_**<应用程序版本>**_uaa";

   将上述 3 个数据库的所有者更改为此用户。注意用户名区分大小写。

   ALTER DATABASE "4Sight**<应用程序版本>**_temp" OWNER TO "**<数据库用户>**";
   ALTER DATABASE "4Sightaudit**<应用程序版本>**_temp" OWNER TO "**<数据库用户>**";
   ALTER DATABASE "uaa**<应用程序版本>**_temp" OWNER TO "**<数据库用户>**";
6. 检查各个备份的 metadata.properties 文件，决定需要还原哪个备份。
7. 以管理员身份打开另一个命令提示符，将目录切换到包含上述选定备份文件的文件夹。
   使用以下命令将数据库从 *.bck 文件还原到 *_temp 数据库。如果出现提示，要求输入密码，则输入 postgres 超级用户的密码。
   "C:\Program Files\PostgreSQL\11\bin\pg_restore" --port=**<数据库端口>** --no-owner --username=postgres --dbname=4Sight**<应用程序版本>**_temp -n public --role=**<数据库用户>** 4Sight**<应用程序版本>**.bck

   "C:\Program Files\PostgreSQL\11\bin\pg_restore" --port=**<数据库端口>** --no-owner --username=postgres --dbname=4Sightaudit**<应用程序版本>**_temp -n public --role=**<数据库用户>** 4Sightaudit**<应用程序版本>**.bck

"C:\Program Files\PostgreSQL\11\bin\pg_restore" --port=**<数据库端口>** --no-owner --username=postgres --dbname=uaa**<应用程序版本>**_temp -n public --role=**<数据库用户>** uaa**<应用程序版本>**.bck

8. 在 psql 提示符下运行以下命令删除 *_old 数据库 （如果存在）。

   DROP DATABASE IF EXISTS "4Sight**<应用程序版本>**_old";
   DROP DATABASE IF EXISTS "4Sightaudit**<应用程序版本>**_old";
   DROP DATABASE IF EXISTS "uaa**<应用程序版本>**_old";

9. 如果有任何 4Sight 服务和 pgadmin 应用程序打开，则停止它们。
10. 在 psql 提示符下运行以下命令将现有 4Sight 数据库重命名为 *_old。

    ALTER DATABASE "4Sight**<应用程序版本>**" RENAME TO "4Sight**<应用程序版本>**_old";
    ALTER DATABASE "4Sightaudit**<应用程序版本>**" RENAME TO "4Sightaudit**<应用程序版本>**_old";
    ALTER DATABASE "uaa**<应用程序版本>**" RENAME TO "uaa**<应用程序版本>**_old";

11. 在 psql 提示符下运行以下命令将 *_temp 数据库重命名为 4Sight 数据库。

    ALTER DATABASE "4Sight**<应用程序版本>**_temp" RENAME TO "4Sight**<应用程序版本>**";
    ALTER DATABASE "4Sightaudit**<应用程序版本>**_temp" RENAME TO "4Sightaudit**<应用程序版本>**";
    ALTER DATABASE "uaa**<应用程序版本>**_temp" RENAME TO "uaa**<应用程序版本>**";

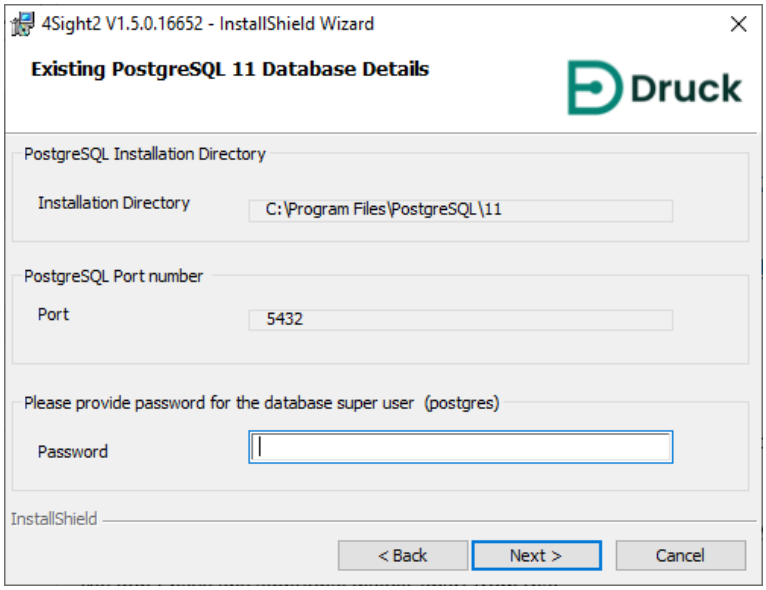
12. 启动 4Sight 服务并尝试以管理员身份登录。注意，此时必须使用进行备份时所用的管理员密码来登录。

7.5 如何从 4Sight2 计算机崩溃中恢复？

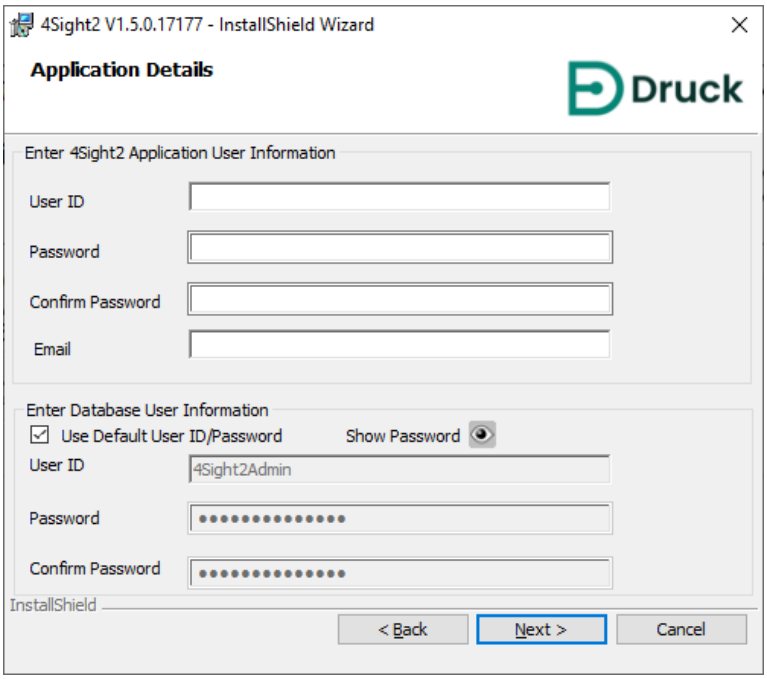
假设：用户已在崩溃前对 4Sight2 数据库进行了备份。

用户已知道应用程序和数据库的用户名和密码。

1. 使用支持的操作系统和驱动程序设置计算机。
2. 在计算机上安装 4Sight2。
3. 安装应用程序时，提供以前为应用程序和Postgres 数据库提供的同一用户名和密码。

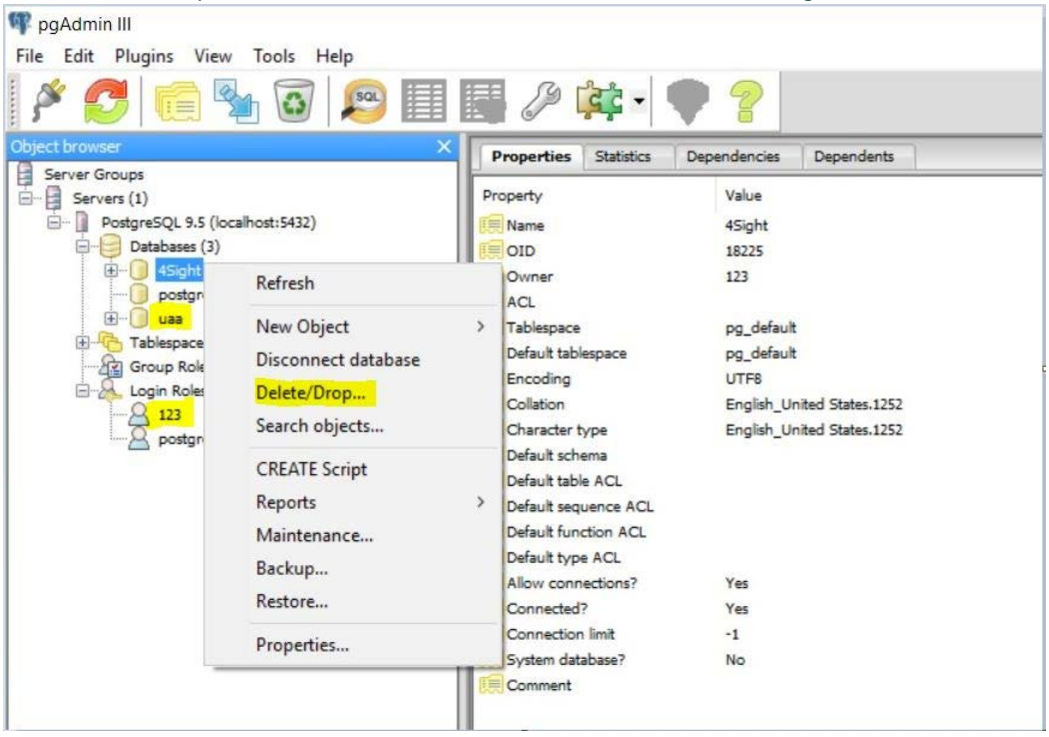


使用以前安装时所用的同一密码。



像以前安装一样完成填写所有字段。

4. 成功安装应用程序后，从 pgAdmin 删除安装应用程序时创建的默认数据库 （右键单击数据库然后选择 Delete （删除） /Drop （删除））。如果在删除数据库时出错，则重启 Postgres 服务并在刷新后重试。



5. 成功删除数据库和用户后，从命令提示符按照上述步骤还原数据库。
6. 现在，您已成功还原数据库，从浏览器打开应用程序并进行查看。

7.6 安装出错情况：

下表说明了安装过程中的各种错误情况及其纠正措施。

错误消息	情况	采取的补救/措施
"Insufficient disk space available to install 4Sight2 application. Please ensure a minimum of 4096 MB is available. Free Space : available MB."	因硬盘空间问题而出错（如果开始升级时达不到所需空间）	管理员需要释放相应驱动器上的空间，然后重试升级过程。
"Deployment fail while Migrating database"	因硬盘空间问题而出错（如果成功启动升级后没有足够空间）	管理员需要释放相应驱动器上的空间，然后重试升级过程。
"Installation failed while migrating Database. Please reinstall 4sight2"	因复制数据库时丧失数据完整性而出错	如果出现此问题，管理员需要联系客户帮助中心。丧失数据完整性的原因记录在以下位置的日志中：[C:\Users\[用户名]\App Data\Local\Temp\logs]
"Installation failed while migrating Database. Please reinstall 4sight2"	因模式更新阶段丧失数据完整性而出错	如果出现此问题，管理员需要联系客户帮助中心。丧失数据完整性的原因记录在以下位置的日志中：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"	如果安装程序无法获得服务状态，则将出现此错误。	管理员需要确保 4Sight2 服务已启动且正在运行
"Failed to start the 4Sight2 service. Please ensure the 4Sight2 service is present and running"	如果应用程序损坏、一些文件被删除或端口正在由其他应用程序使用或用户已停止服务等，则将出错。	如果管理员成功获取服务状态，且服务因任何原因而未在运行（比如，应用程序损坏、一些文件被删除或端口正在由其他应用程序使用或用户已停止服务等），则系统将尝试启动服务。如果无法启动服务，管理员需要联系客户支持人员来修正问题。
"Upgrade of 4Sight2 application is supported from version 1.3 onwards. For earlier version upgrade support please contact Customer Care."	如果安装的应用程序版本低于 1.3，则无法升级。	仅能从 1.3 或更高版本进行升级。
Installer has detected another minor version of PostgreSQL 11. Installer will not continue. Refer to 4Sight2 Installation manual for more details	4Sight2 无法继续安装，因为目标计算机上存在相同的 PostgreSQL 版本（变体）	可能选项 1.用户可选择另一计算机。 2.用户备份正在使用 11.3 版的 Postgres 的现有应用程序，卸载该应用程序然后在其他计算机上部署。卸载 Postgres 然后重新开始安装 4Sight2

错误消息	情况	采取的补救/措施
Installation failed while upgrading database. Please reinstall 4Sight2. Refer to 4Sight2 Installation manual for more details	升级过程中可能出现一些内部错误，用户可尝试重新安装	如果问题继续出现，用户可共享安装日志以了解更多信息

7.7 一般错误原因

以下为与 4sight2 通过 USB 与 Druck 设备通信相关联的常见问题。

- 物理连接松脱或摇晃。
- 电缆/端口磨损。
- USB 适配器质量不佳。
- USB 适配器/端口过载。
- 设备保持长时间运行，从而导致它们进入休眠模式。
- 设备未处于通信模式。
- 驱动程序软件未安装或未升级。需要使用同一版本的 4Sight2 应用程序和驱动程序来与硬件通信。
- 设备的固件版本非常旧。

7.8 卸载 4Sight2

如果在安装过程中需要安装 4Sight2 的新副本、 4Sight2 的新版本或需要卸载 4Sight2，则遵循这些说明。

卸载PostgreSQL数据库组件将删除4Sight2数据库，导致数据丢失。以下步骤不会自动创建备份，因此请确保首先创建手动备份，并将此备份放在 4Sight2 安装文件夹之外的其他位置，然后再继续。参考本手册的 Postgres 数据库备份和还原章节。

如果选择仅卸载 4Sight2 应用程序而保留数据库，请参考本手册的 4Sight2 安装部分。重新安装时需要数据库超级用户的凭据。如果不知道这些凭据，请勿尝试执行卸载。

如果希望升级您的 4Sight2 版本而不卸载数据库，请**不要**遵循这些说明。

1. 转至“控制面板”>> “程序和功能”。
2. 右键单击 4Sight2，然后选择“卸载”。
3. 遵循卸载向导中的说明。
4. 右键单击 PostgreSQL 11，然后选择“卸载”。
5. 遵循卸载向导中的说明。
6. 卸载 PostgreSQL 不会删除数据文件夹。您需要手动执行此操作。删除位于该位置的数据文件夹：C:\Program Files\PostgreSQL\11\
   a. 如果要删除整个 PostgreSQL 文件夹，确保将任何备份文件、脚本从垃圾箱文件夹移走，然后再继续。
   b. 默认情况下 4Sight2 数据库备份会在以下位置创建并保存：C:\Program Files\PostgreSQL\11\bin
7. 建议尽可能重启计算机。
8. 4Sight2 现已成功卸载。

7.9 安全通信故障排除

1. 命令“命令名称”未被识别为内部或外部命令。例如， 'keytool' 未被识别为内部或外部命令。

- 如果看到此类错误消息，则意味着命令提示符无法在当前文件夹内找到对指定命令的引用。

  要纠正此错误，使用以下命令指向正确的文件夹。

  Set Path=%Path%;"<<命令所在位置的完整路径>>"

  例如，与 keytool 相关的上述错误中，需要将路径设置为以下内容：

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

2. IP 地址错误

- 如果出现此错误消息，则意味着 openssl-ca.cnf 或 openssl-server.cnf 文件中的 IP 地址或主机名不正确。注：可能需要在这些文件中的多个位置纠正此错误并重新执行相关步骤。

3. 不存在此文件或目录...

- 如果出现此错误消息，则意味着已执行的命令引用的是错误的文件名。检查命令中有无任何文件名错误，同时检查文件夹中是否存在具有该名称的文件，然后重新运行相关命令。可能需要更正命令中的文件名或按照步骤生成缺失的文件。
- index.txt 和 serial.txt 文件可能会出现此错误，因为在某些情况下，名称后会附加两个文件扩展名，比如 intex.txt.txt。

  只需编辑该文件并将它保存为无 .txt 扩展名的格式。确保文件只有一个 .txt 扩展名。

最佳做法

8. 最佳做法

服务器加固

应按照 Microsoft 或 CIS 规范对服务器环境进行加固。

8.1 Tomcat

- 将 Tomcat 安装在只有管理员或“本地服务”才有权访问的安全文件夹中，比如 *C:\Program Files(x86)*。
- 将 Tomcat 安装为以“本地服务”帐户运行的服务。
- 从 WebApp 上删除所有内容，删除默认的不需要的应用程序。
- 替换默认错误页，如 404、 403、 500 等。
- 强制实施 HTTPS，启用 SSL。
- 管理应用程序应在 SSL 上运行。
- 对每个 Web 应用程序提供特定于用户的日志文件。
- 删除服务器版本号信息。
- 雇用访问记录功能。
- 更改关闭端口和命令。

8.2 PostgreSQL

- 只允许所有高权限帐户进行本地登录，如 pgdba、 postgres、 depesz。
- 确保 pg-hba.conf 文件中的顺序正确，以便正确的用户获得适合的访问权限。
- 配置 pg-hba.conf 以便只能从本地计算机而不是通过网络连接服务器。

8.3 防火墙最佳做法

以下是一些推荐用于 4Sight2 的防火墙最佳做法：

8.3.1 政策

1. 防火墙配置应与组织安全政策保持一致。
2. 始终使用最低权限政策。默认情况下全部拒绝。允许特定流量 （使用源、目标和端口）。
3. 先应用特定规则然后使用显式删除规则。
4. 记录所有操作，特别是失败的审计跟踪尝试。

8.3.2 资源

1. 监控内存利用率。
2. 监控 CPU 利用率。
3. 监控带宽利用率。
4. 限制防火墙所在计算机上运行的应用程序数。

8.3.3 安装和维护

1. 限制对防火墙所在计算机的物理访问权限。
2. 使用唯一用户 ID 进行管理。

3. 遵循计算机上严格的帐户政策。
4. 定期修补操作系统、应用程序软件、固件等。
5. 定期存档规则库、配置和日志。记录在源控制中定义的所有规则和所做的全部更改。
6. 定期执行测试。
7. 当服务退役时，删除不用的规则。
8. 定期对规则进行审计和审核。
9. 定期监控安全警告。

8.3.4 其他安全事项

1. 使用有状态检测。
2. 使用代理。
3. 使用应用程序级别检测和筛选。

8.3.5 内部保护

1. 制定可接受的使用政策。
2. 为每个用户提供个人防火墙。
3. 基于主机的入侵防御。
4. 网络监控。
5. 内容筛选。
6. 对每个计算机和应用程序进行访问控制。

办事处位置

总部

英国莱斯特
电话：+44 (0) 116 2317233
电子邮件：gb.sensing.sales@bakerhughes.com

阿联酋

阿布扎比
电话：+971 528007351
电子邮件：
suhel.aboobacker@bakerhughes.com

澳大利亚

斯普林菲尔德中心
电话：1300 171 502
电子邮件：custcare.au@ge.com

德国

法兰克福
电话：+49 (0) 69-22222-973
电子邮件：sensing.de.cc@bakerhughes.com

俄罗斯

莫斯科
电话：+7 915 3161487
电子邮件：aleksey.khamov@bakerhughes.com

法国

图卢兹
电话：+33 562 888 250
电子邮件：sensing.FR.cc@bakerhughes.com

荷兰

胡弗拉肯
电话：+31 334678950
电子邮件：nl.sensing.sales@bakerhughes.com

美国

波斯顿
电话：1-800-833-9438
电子邮件：custcareboston@bhge.com

日本

东京
电话：+81 3 6890 4538
电子邮件：gesitj@bakerhughes.com

意大利

米兰
电话：+39 02 36 04 28 42
电子邮件：csd.italia@bakerhughes.com

印度

班加罗尔
电话：+91 9986024426
电子邮件：aneesh.madhav@bakerhughes.com

中国

北京
电话：+86 180 1929 3751
电子邮件：fan.kai@bakerhughes.com

中国

广州
电话：+86 173 1081 7703
电子邮件：dehou.zhang@bakerhughes.com

中国

上海
电话：+86 135 6492 6586
电子邮件：hensen.zhang@bakerhughes.com

服务和支持位置

技术支持

全球
电子邮件：mstechsupport@bakerhughes.com

阿联酋

阿布扎比
电话：+971 2 4079381
电子邮件：gulfservices@bakerhughes.com

巴西

坎皮纳斯
电话：+55 11 3958 0098，+55 19 2104 6983
电子邮件：mcs.services@bakerhughes.com

法国

图卢兹
电话：+33 562 888 250
电子邮件：sensing.FR.cc@bakerhughes.com

美国

比尔里卡
电话：+1 (281) 542-3650
电子邮件：namservice@bakerhughes.com

日本

东京
电话：+81 3 3531 8711
电子邮件：service.druck.jp@bakerhughes.com

印度

浦那
电话：+91 213 5620426
电子邮件：
mcsindia.inhouseservice@bakerhughes.com

英国

莱斯特
电话：+44 (0) 116 2317107
电子邮件：
sensing.grobycc@bakerhughes.com

中国

常州
电话：+86 400 818 1099
电子邮件：service.mcchina@bakerhughes.com

123M3140 修订版 F | 中文

Baker Hughes