Druck

4Sight2

Kalibrasyon Yönetim Yazılımı

Kurulum Kılavuzu 123M3140 Revizyon F

Druck.com

1. Giriş

4Sight2 Kalibrasyon yazılımı, kalibrasyon ortamınızı en yüksek metroloji standartlarında tutmanıza ve kontrol etmenize yardımcı olan web tabanlı bir kalibrasyon yönetim aracıdır. Yazılımı şu görevler için kullanabilirsiniz:

- Belirli bir iş yeri için tüm ölçüm cihazlarının kalibrasyonunu yönetin
- Teknisyenler için bir kalibrasyon çalışması planı oluşturun
- USB haberleşme portuna sahip olan Druck taşınabilir kalibratörlerden (DPI620 Genii, DPI611 ve DPI612) gelen verileri bu yazılım programına indirin ve bu yazılım sistemindeki verileri bahsedilen portatif kalibratörlere yükleyin
- Taşınabilir bir kalibratör tarafından desteklenmeyen cihazlar için kalibrasyon kayıtlarınızı yönetin (Manuel Veri Girişi)
- Geçmiş kalibrasyon kayıtlarınızı gözden geçirin. Her kalibrasyon sertifikası için kalıcı kayıtlar oluşturabilirsiniz. Örneğin: ISO 9000 kalite kontrol prosedürleri için.
- Druck Basınç Kontrolörleri (PACE1000, PACE5000 ve PACE6000), Portatif Kalibratörleri (DPI620 Genii, DPI611 ve DPI612) ve Sıcaklık Kalibratörleri (DryTC165, DryTC650, LiquidTC165 ve LiquidTC255) kullanarak otomatik kalibrasyonlarınızı kontrol edin

1.1 Hedef Kitle

1.1.1 Yöneticiler

4Sight2 yazılımının kurulumundan ve yapılandırılmasından bir yönetici sorumludur. 4Sight2'nin ilk kurulumundan sonra tek bir yönetici hesabı açılacaktır. Bu hesaptan yeni Kullanıcılar oluşturulabilir ve Gruplar / İzin Setleri atanabilir. Yönetici kullanıcılar, 4Sight2'nin bütün özelliklerinin okuma ve yazma erişimine sahiptirler.

1.1.2 Süpervizör

Bir süpervizör, varlık ve kalibrasyon yönetiminden sorumludur. Süpervizör kullanıcıları, 4Sight2 İşletmesi içerisinde bulunan Tesisler, Konumlar, Etiketler ve Cihazlar kapsamındaki varlıkları oluşturma ve güncelleme görevlerine sahiptirler. Tesis prosedürleri ve cihazların teknik özellik dökümanları gibi evrakların ilgili varlıklarla eşleştirilmelerinden sorumludurlar. Süpervizör kullanıcıları kalibrasyon sırasında kullanılacak test prosedürlerini oluşturabilir, prosedürleri programlayabilir ve cihazların güncel durumlarını izleyebilirler. Süpervizör kullanıcıları kalibrasyonları onaylamak için gerekli izinlere sahiptir.

1.1.3 Teknisyenler

Kalibrasyonların yapılmasından teknisyenler sorumludur. Kalibrasyonlar Taşınabilir, Manuel veya Otomatik versiyonda olabilir ve bir cihazın ilgili kalibrasyon türünü gerçekleştirmek teknisyen kullanıcılarının rolüdür. Bir kalibrasyon işlemi gerçekleştirildikten sonra, teknisyenler tarafından kalibrasyon sonuçları gözden geçirebilir ve cihaz kalibrasyonları tamamlandıktan sonra ilgili süpervizör tarafından kalibrasyon işlemi onaylanabilir.

1.1.4 Denetçi

Raporların incelenmesinden denetçi sorumludur. Bazı senaryolarda bazı Tesislerde denetim yapmak zorunlu bir gereklilik olabilir.

2. Sistem Gereksinimleri

4Sight2 uygulamasını Sunucu ve İstemci makinelerinde kurulumunu gerçekleştirebilmek için minimum sistem gereksinimleri aşağıda listelenmiştir:

2.1 Uygulama Sunucusu

İşletim sistemi	Windows 10, Windows Server 2012 R2, Windows Server 2016, Windows Server 2019
Güncellemeler	Tüm Windows Güncellemeleri tamamen yüklendi
İşlemci	Dört çekirdekli
Veri deposu	8GB veya üstü (32GB Önerilen)
Disk alanı	1TB
Ağ Hızı	10Mbps

2.2 Müşteri İş istasyonu

İşletim sistemi	Windows 10, Windows Server 2012 R2, Windows Server 2016, Windows Server 2019
Tarayıcı	Google Chrome V80+, Microsoft Edge V80, Firefox V74
Adobe Okuyucu	Adobe Acrobat Reader DC Sürümü 2015.017.20050 +
Veri deposu	8GB veya üstü
İşlemci	Çift çekirdekli
Disk alanı	600GB
Ağ Hızı	10Mbps

2.3 Yerel Kurulum\

İşletim sistemi	Windows 10, Windows Server 2012 R2, Windows Server 2016, Windows Server 2019
Güncellemeler	Tüm Windows Güncellemeleri tamamen yüklendi
Adobe Okuyucu	Adobe Acrobat Reader DC Sürümü 2015.017.20050 +
İşlemci	Çift çekirdekli
Veri deposu	16GB veya üstü (32GB Önerilen)
Disk alanı	500GB veya daha fazla disk alanı
Tarayıcı	Google Chrome V80+, Microsoft Edge V80, Firefox V74

2.4 4Sight2 Desteklenen Aygıt Yazılımı

Desteklenen bellenim hakkında en son bilgiler için aşağıdaki bağlantıya bakın:
https://www.bakerhughes.com/druck/test-and-calibration-instrumentation/calibration-management-software-4sight2

Veya

PACE için, 4Sight2 İletişimi için USB B'yi aşağıdaki resimde gösterildiği gibi takın:

4Sight2 Kurulumu

3. 4Sight2 Kurulumu

4Sight2 Kalibrasyon yazılımını kurmak için öncelikle 4Sight2 Setup zip dosyasını masaüstünüze kopyalayın ve bütün dosyaları zip dosyasından çıkartın. Kurulum dosyası içerisinden 4Sight2 executable dosyasını seçin.

Not: 4Sight2 ve Comm Server kurulumlarını taramak için aşağıdaki antivirüs yazılım programı kullanılır,

- McAfee VirusScan Enterprise + AntiSpyware Enterprise Sürüm numarası: 8.8.0
- Symantec Endpoint Protection Sürüm numarası: 14.3.558

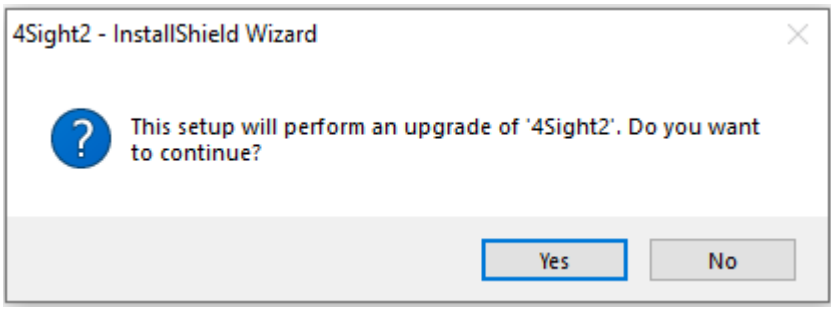
4Sight2 executable dosyasını çalıştırdıktan sonra, InstallShield wizard başlayacaktır. InstallShield wizard, 4Sight2 kurulumunun iki aşamasını içerir:

1. Application Installation

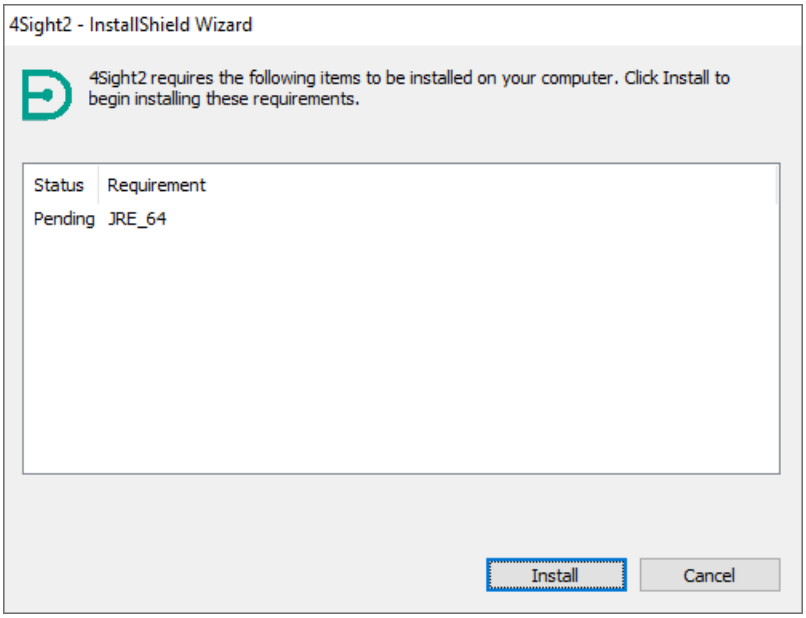
2. Web Application Installation

InstallShield talimatlarını takip ediniz veya kurulum sürecini yürütmek için aşağıdaki iki bölümü kullanınız.

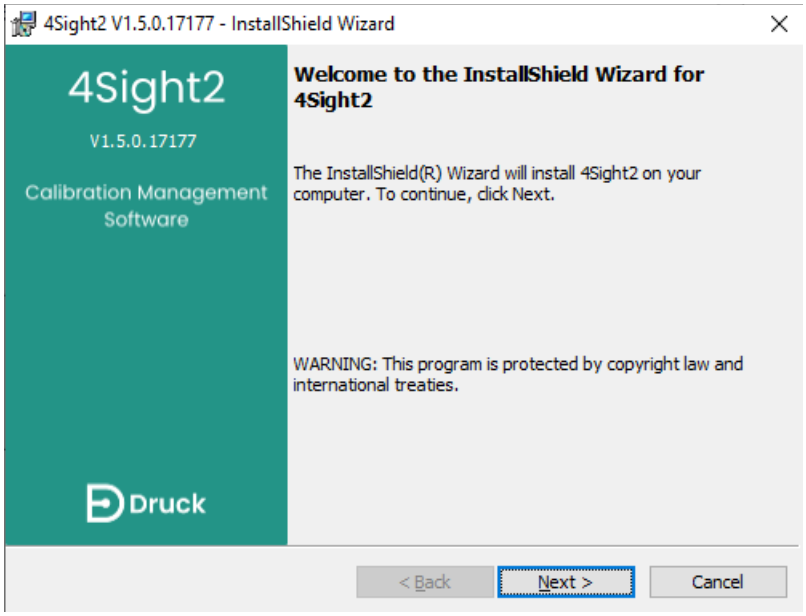
1. 4Sight2 makinede zaten kuruluysa, kurulum sihirbazı sizden en son sürüme yükseltme yapmanızı isteyecektir. 4Sight2 en son sürüm yükseltmesini gerçekleştirmek için **Yes** butonuna tıklayınız.



2. Eğer 4Sight2 makinede ilk defa yükleniyor ise, kurulum sihirbazı aşağıdaki ekran gibi görüntülenecektir. **Install** butonunu seçiniz sonrasında listelenen öğeler yüklenecektir.



3. Herhangi bir ön koşul öğesinin kurulumu tamamlandığında, InstallShield Wizard Welcome ekranı görüntülenecektir. **Next** butonuna tıklayarak devam ediniz.



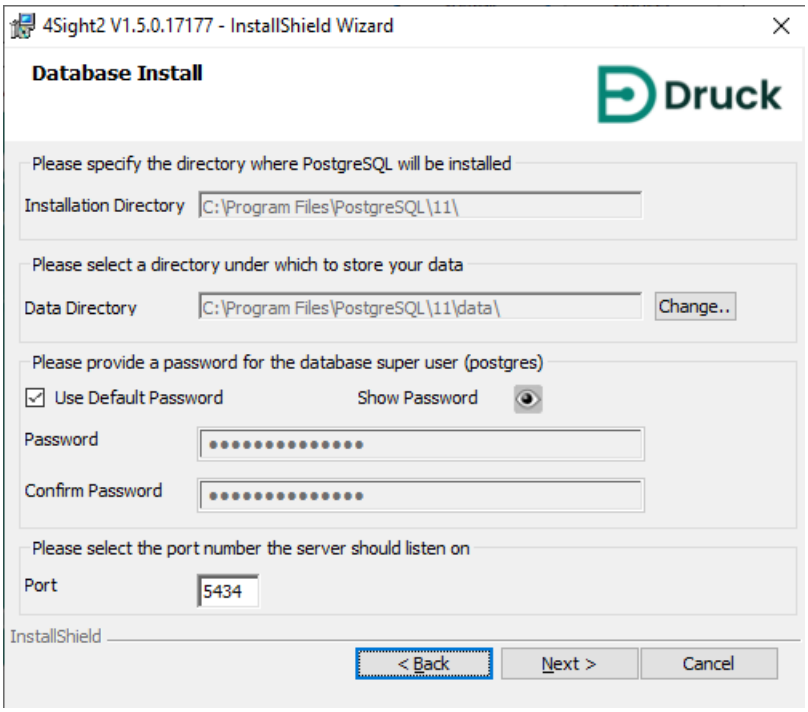
3.1 Veritabanı Kurulumu

4Sight2 uygulaması bir PostgreSQL veritabanı kullanmaktadır. Aşağıda PostgreSQL veritabanının nasıl kurulacağı ve bir PostgreSQL veritabanı zaten kurulu ise ne yapılması gerektiği ile ilgili talimatlar verilmiştir.

3.2 PostgreSQL Kurulumu

Makinede bir PostgreSQL veritabanı kurulu değilse bu prosedürü uygulayın.

1. Eğer makinede yüklü bir PostgreSQL veritabanı yok ise, kurulum sihirbazı ekranda aşağıdaki gibi görüntülenecektir.



Installation Directory: PostgreSQL uygulamasının kurulabileceği dizini seçiniz.

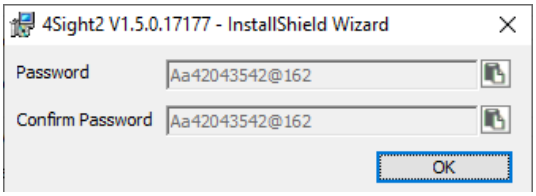
Data Directory: PostgreSQL veritabanının saklanabileceği dizini seçin.

Password/Confirm Password: PostgreSQL veritabanı super user şifresini giriniz. Bu, yalnızca PostgreSQL veritabanı ilk kez kurulduğunda istenir.

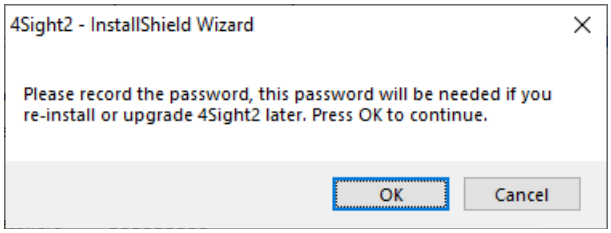
Not: Kurulumdan sonra veritabanı içeriğine erişmek için bu şifre gerekecektir.

Port: Bu, PostgreSQL veritabanının uygulama talebini karşılamak için kullanılan port adresidir.
Not: Port numarası zaten kullanılıyorsa, IT ekibiyle iletişime geçin. Kullanıcı ayrıca daha sonra uygulamayı başlatmak için gerekli olan port numarasını değiştirebilir.

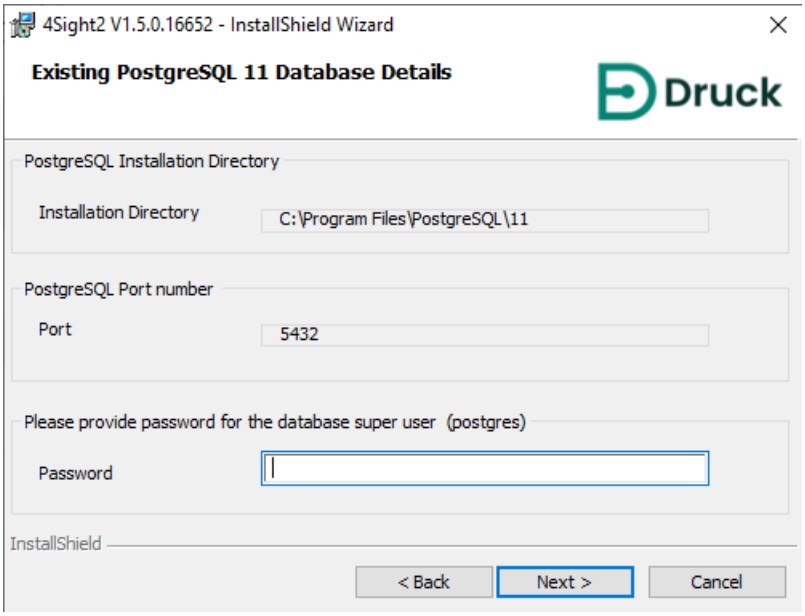
Önemli: Kullanıcı, veritabanı şifresini not etmelidir. Parola bilgilerinin kaybı, erişimin reddedilmesine veya veri kaybına neden olabilir. Veritabanı super user parolasını güncellemek için User Default Password onay kutusunun işaretini kaldırın. Varsayılan parolayı takip etmek ya da yeni girilen şifreyi görüntülemek için (Show Password) ikonunu seçiniz. Panoya şifreyi kopyalamak için (Copy to Clipboard) ikonunu kullanınız.



Akabinde, yükleyici tarafından parolayı tekrar kaydetmeniz istenecektir. **Ok** butonuna tıkladığınızda, şifreniz oluşturulacaktır.



2. Bu adım, PostgreSQL veritabanı zaten kurulu olması durumunda kullanıcıya gösterilecektir.

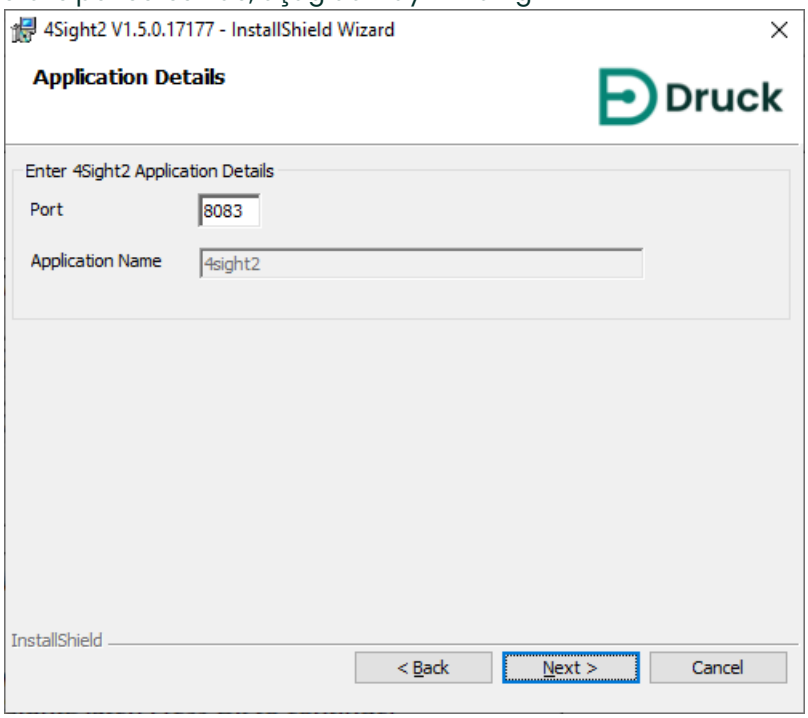


Installation Directory: Bu, PostgreSQL veritabanınız zaten kurulu olduğu adresi belirtmek içindir. Salt okunur bilgidir.

Password: Bu, PostgreSQL veritabanı super user şifresini onaylamak içindir.

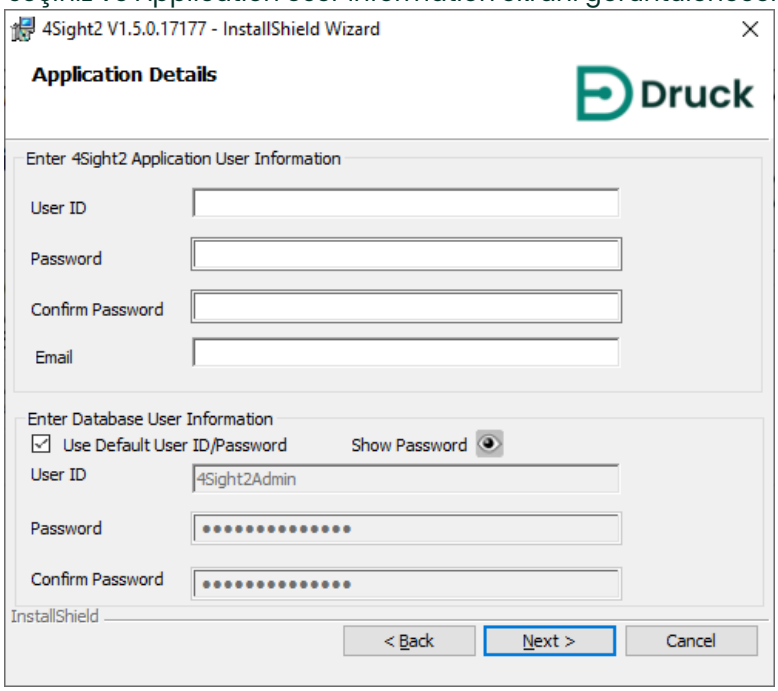
Port: Bu, PostgreSQL veritabanının kullandığı port numarasını belirtmek içindir.

3. Application Details penceresinde, aşağıdaki ayrıntıları giriniz



Port: HTTP isteğine yanıt vermek için 4Sight2 web uygulaması tarafından kullanılan Tomcat web sunucusu port numarasını giriniz.
Application Name: Tarayıcınızdaki 4Sight2 uygulamasına bağlanmak için kullanacağınız uygulama Bağlam yolunu giriniz. Varsayılan olarak bu 4sight2'dir.
Not: Port numarası zaten kullanılıyorsa, IT ekibiyle iletişime geçin. Kullanıcı ayrıca daha sonra uygulamayı başlatmak için gerekli olan port numarasını değiştirebilir.

4. **Next** butonunu seçiniz ve Application User Information ekranı görüntülenecektir.

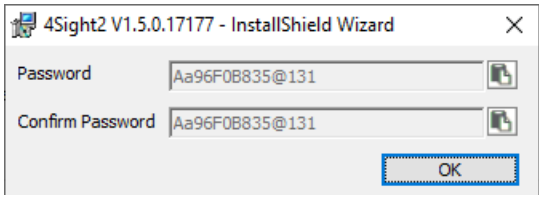


Application User Information: Bu bölüm, 4Sight2 uygulamasına erişim için super user adını ve şifresini girmek içindir.

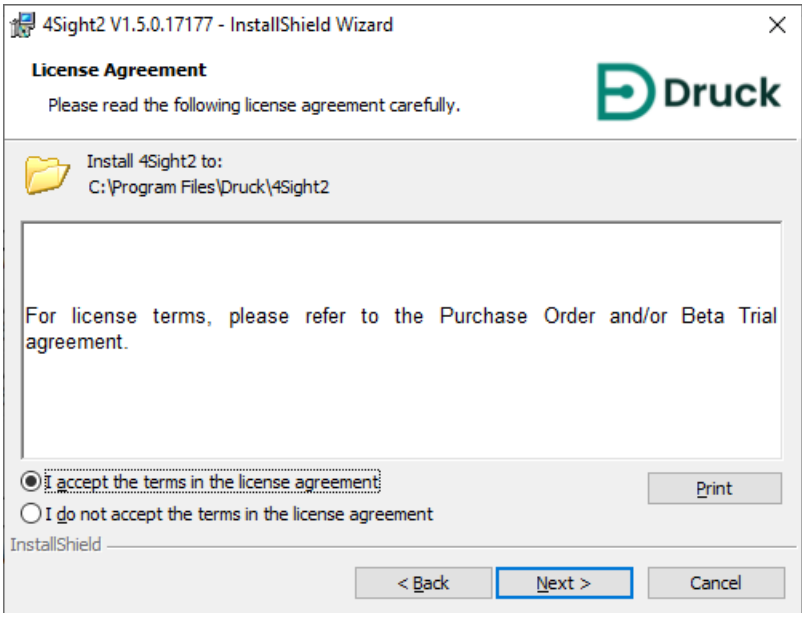
Not: Bu şifre, kurulumun ardından 4Sight2 uygulamasına erişmek için gerekli olacaktır.

Database User Information: Bu bölüm veritabanı kullanıcı adı ve şifresini içindir. Bu bilgiler, 4Sight2 uygulaması tarafından PostgreSQL veritabanı ile iletişim kurmak için kullanılacaktır.

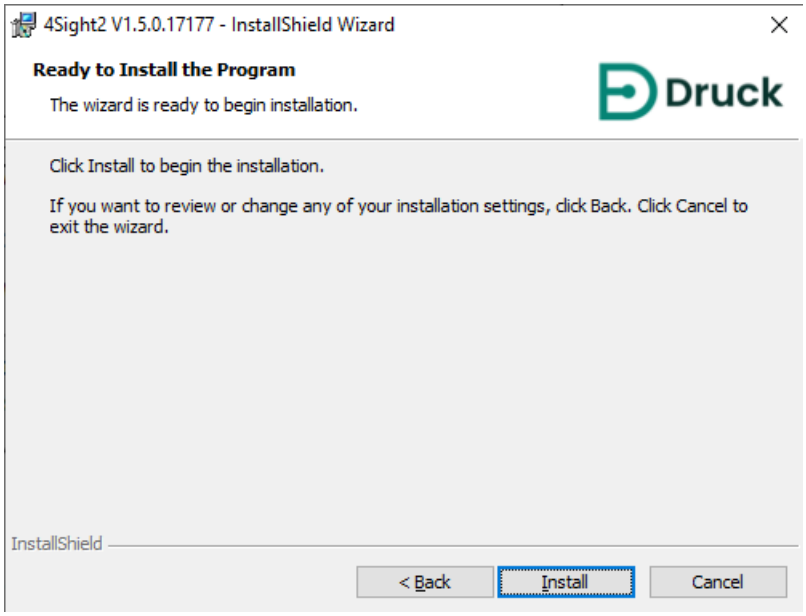
Önemli: Kullanıcı, veritabanı şifresini not etmelidir. Parola bilgilerinin kaybı, erişimin reddedilmesine veya veri kaybına neden olabilir. Veritabanı super user parolasını güncellemek için User Default Password onay kutusunun işaretini kaldırın. Varsayılan parolayı takip etmek ya da yeni girilen şifreyi görüntülemek için (Show Password) ikonunu seçiniz. Panoya şifreyi kopyalamak için (Copy to Clipboard) ikonunu kullanınız



5. Lisans şartları ve koşullarının okunmasının ardından, "I agree to the License terms and conditions." butonunu seçerek **Next** butonuna tıklayınız.

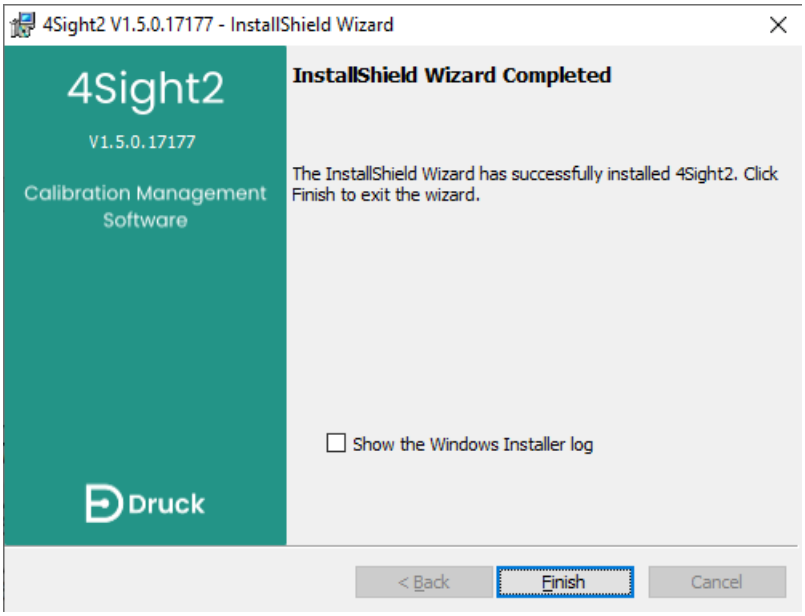


6. Kuruluma başlamak için **Install** butonuna tıklayınız. Akabinde 4Sight2 uygulaması ve veritabanı ile ilgili tüm yazılım paketleri kurulacaktır.



Tebrikler 4Sight2 uygulaması artık kuruldu.

7. Pencereyi kapatmak için **Finish** butonuna tıklayınız ve 4Sight2 uygulamasında oturum açmak için sonraki bölümdeki talimatları takip ediniz.



Yerel olarak sunucuda 4Sight2 uygulaması oturumunu açmak

için http://ComputerName veya IPAddress:PortNo/ApplicationName adresine gidiniz

- **ComputerName**- 4Sight2 uygulamasının yüklendiği bilgisayarın adıdır. Bu ad PC üzerinde sağ butona tıklayarak ekrana gelen pencerede özellikler bölümünden bulunabilir.
- **IPAddress**- 4Sight2 uygulamasının yüklendiği bilgisayarın IP adresidir. Bu IP adresi Windows komut penceresinde 'ipconfig' komutu çalıştırılarak bulunabilir.
- **PortNo**- Bu port numarası uygulama kurulumu sırasında Tomcat Port Number alanına girilennumaradır.
- **ApplicationName**- Bu ad uygulama kurulumu sırasında Uygulama Adı alanına girilen addır.

4Sight2 Test Ekipmanı İletişim Cihazı Kurulumu

4. 4Sight2 Test Ekipmanı İletişim Cihazı Kurulumu

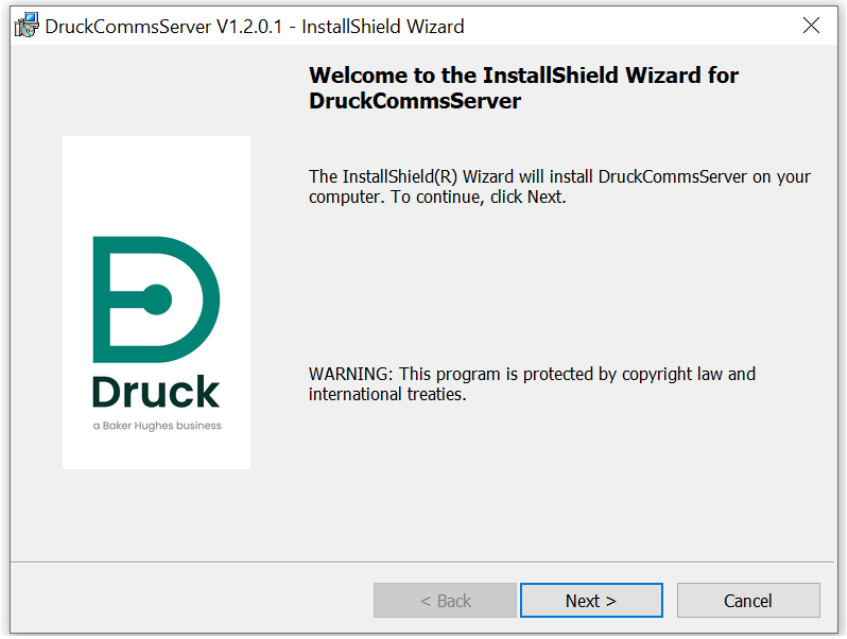
1. Test Ekipmanı İletişim Cihazı, Druck cihazlarınızın 4Sight2 uygulamasıyla iletişim kurması için bağlantı sağlamaktadır. Test Ekipmanı İletişim Cihazı, 4Sight2 kurulum klasörü üzerinden kurulabilir veya 4Sight2 ilk cihaz iletişimi yoluyla indirilebilir. Eğer, Test Ekipmanı İletişim Cihazı set-up dosyası içerisinde hazır değilse, 4Sight2 uygulaması çalıştırıldığı anda iletişim yolu oluşturulmaktadır, yönetici kullanıcı olarak 4Sight2 menüsünü kullanarak Calibration > Portable bölümlerini takip ediniz, yol haritası ve iletişim yolu oluşturabilmek için 4Sight2 Kullanım Kılavuzuna bakınız. Test Ekipmanı açılır menüsünün yanındaki **Yenile** butonuna tıklayınız.
   Eğer Test Ekipmanı İletişim cihazı çalışmıyorsa, aşağıdaki uyarı mesajını göreceksiniz: "Test Ekipmanı ile İletişim Kurulamıyor"

   "Test Ekipmanı ile İletişim Kurulamıyor"

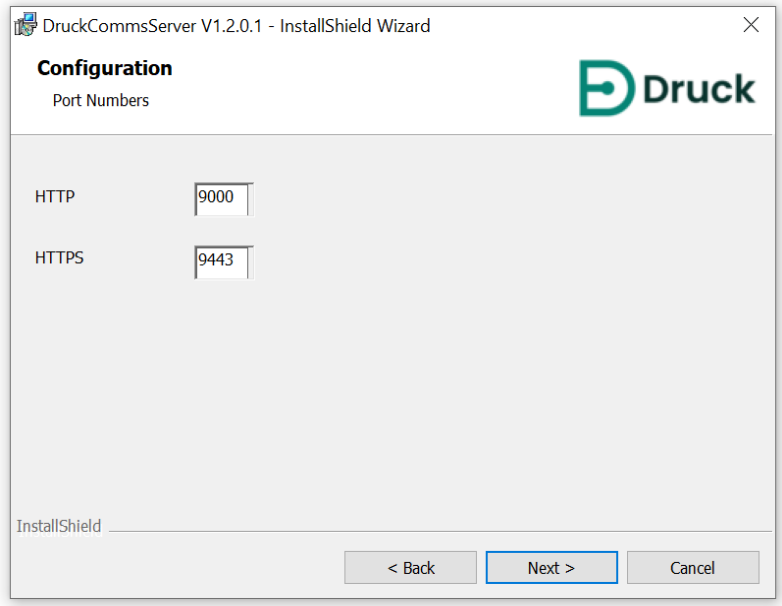
   Test Ekipmanı iletişimci paketini indirin. İndirdikten sonra, kurmak için setup.exe dosyasını açın ve çalıştırın. Kurulum talimatları veya sorun giderme için Kurulum Kılavuzuna bakın. Lütfen yardım için Yönetici ile iletişime geçin.

Not: Test ekipmanı iletişimcisi, DruckCommsServer olarak da bilinir.

2. Test Ekipmanı İletişim Cihazı kurulum dosyasını edinmek için **Download** butonunu seçiniz.
3. Test Ekipmanı İletişim Cihazı kurulum dosyaları, CommsServerInstall Zip dosyası olarak görünecektir. Bir kez Comms Server Zip dosyası indirdiği zaman, 4Sight2 kurulumu öncesi ve sonrası aynı adımlar takip edilebilir.
4. Dosyaları Comms Server Zip dosyası üzerinden ayıklayınız ve setup.exe dosyasına çift tıklayarak yükleyiciyi çalıştırınız.
5. DruckCommsServer yükleyicisi görüntülenecektir. Yükleyici içerisindeki talimatları ya da bu kılavuzu takip ediniz. Herhangi bir önkoşul aracı gerekiyorsa yükleyici dili seçmenizi ve yüklemenizi ister ve ardından aşağıdaki ekran görüntülenir.

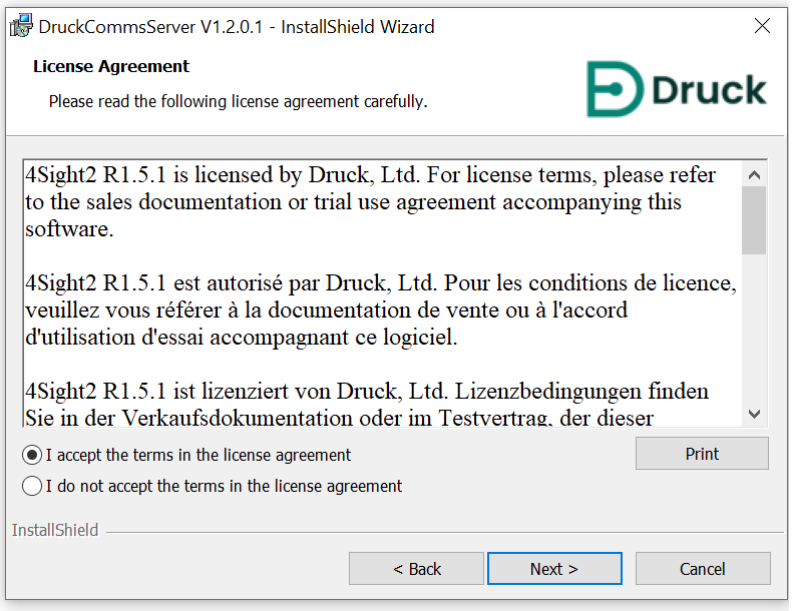


6. Configuration Ekranını görüntülemek için Next butonuna tıklayınız ve port numaralarını giriniz

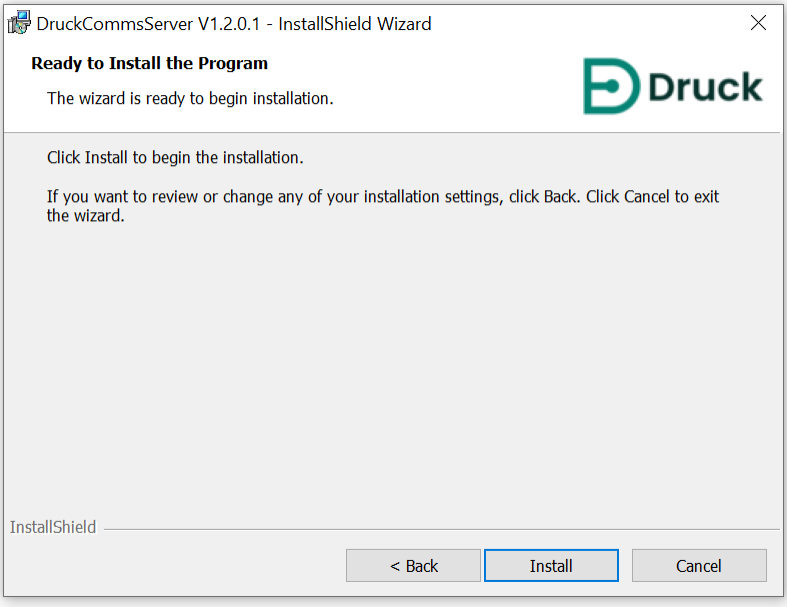


Not: 4Sight2 tarafından alternatif port numarasının kullanılıp kullanılmadığından emin değilseniz, lütfen yönetici kullanıcınıza başvurun.

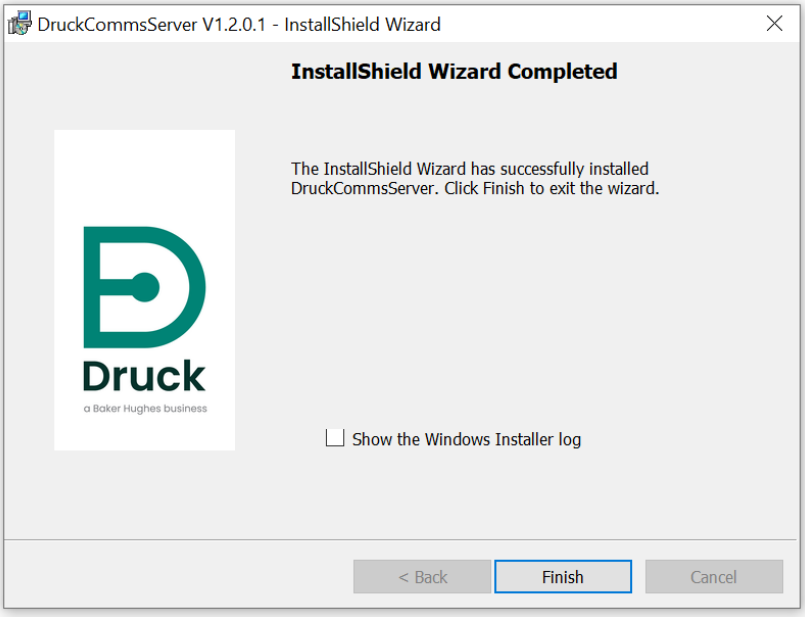
7. License Agreement Ekranını görüntülemek için **Next** butonuna tıklayınız. Lisans şartları ve koşullarının okunmasının ardından, "I agree to the License terms and conditions." butonunu seçerek **Next** butonuna tıklayınız.



8. Kurulumu başlatmak için **Install** butonuna tıklayınız.



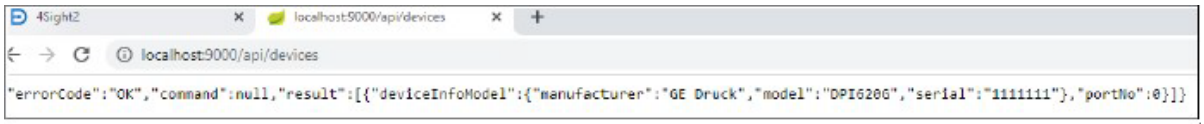
9. Kurulum tamamlandıktan sonra **Finish** butonuna tıklayınız.



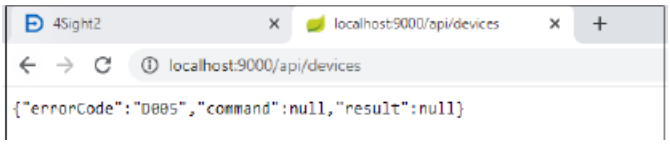
10. Test Ekipmanı iletişim cihazı kurulumunu aşağıdaki URL adresini web tarayıcısına yazarak test ediniz:

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

Web tarayıcısı bağladığınız herhangi bir aygıtın listesini görüntülemelidir::



Hiçbir cihaz bağlı değilse, aşağıdakileri görmelisiniz



Not: Sıcaklık kalibratörleri için gerekli sürücüler otomatik olarak yapılandırılmayacaktır. Bkz. Bölüm 4.3 Sıcaklık Kalibratörü Sürücü Yapılandırması

11. Eğer aygıt sürücüsü kurulumu başarısız olursa, gerekli sürücüleri manuel olarak yapılandırmak için bir sonraki bölümdeki adımları kullanın.

4.1 Manuel Sürücü Yapılandırması

IT güvenlik ilkesi ayarları, Druck sürücülerinin kurulum sırasında otomatik olarak yapılandırılmasını engelleyebilir. 4Sight2 aşağıdaki ekipmanlarla iletişim kuramazsa bu daha belirgin olacaktır:

En son bilgiler için, https://www.bakerhughes.com/druck/test-and-calibration-instrumentation/calibration-management-software-4sight2

veya

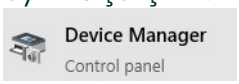
Bu sorunu çözmek için, Druck sürücüleri el ile yapılandırılabilir. Bundan emin değilseniz veya daha fazla yardıma ihtiyacınız varsa lütfen yerel IT temsilcinize danışınız.

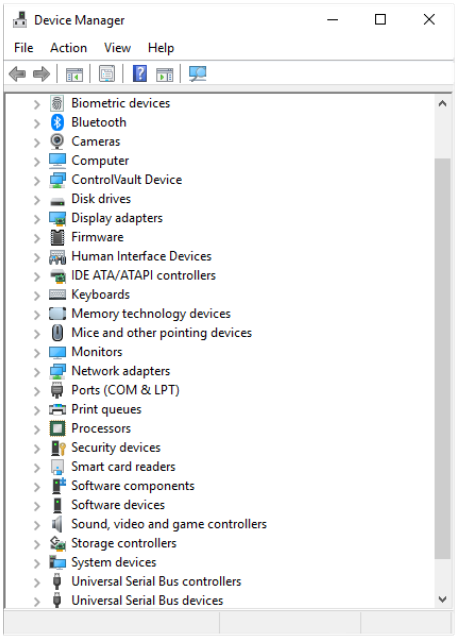
4.1.1 Önkoşullar

Sürücüleri yüklemek için, 4Sight2 uygulamasının yüklü olması veya makine üzerinden / makineye erişilebilir olması gerekir. Sürücüleri yüklemeyi denemeden önce bilgisayardan 4Sight2 uygulamasında oturum açabildiğinizden emin olun.

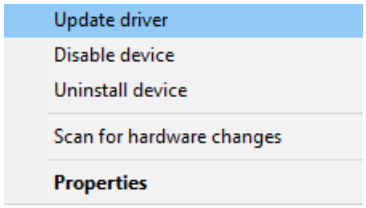
Sürücüyü manuel olarak kurmak için aşağıdaki adımları uygulayın,

1. Masaüstünde Aygıt Yöneticisini arayın ve çalıştırın.

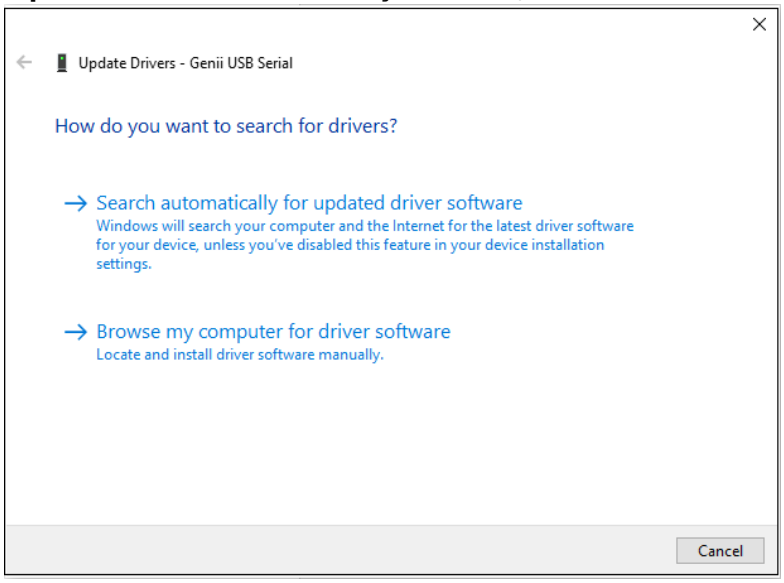




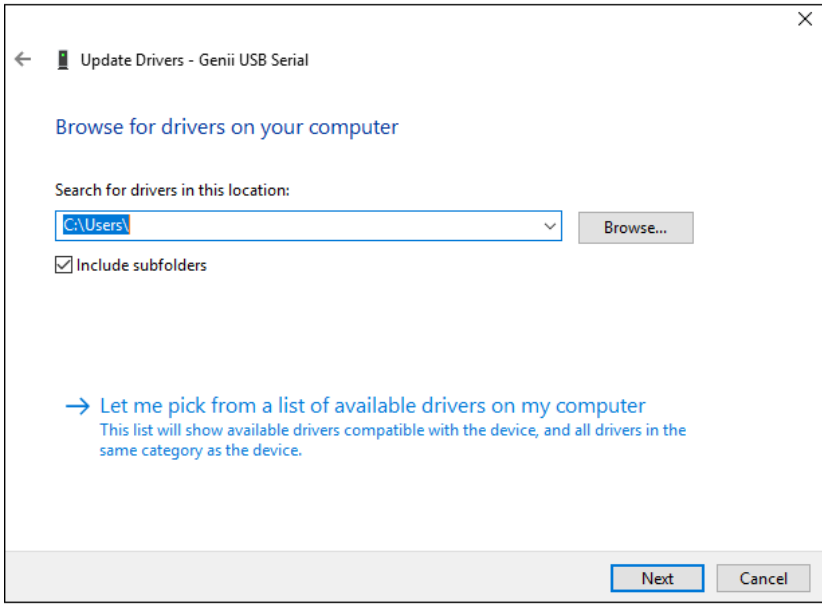
2. Yapılandırılmamış cihazları (Bilinmeyen Cihaz veya Diğer cihazlar) bulmak için USB cihazları listesinde ilerleyiniz. Sağ tıklayın ve **Update driver** ı seçiniz.



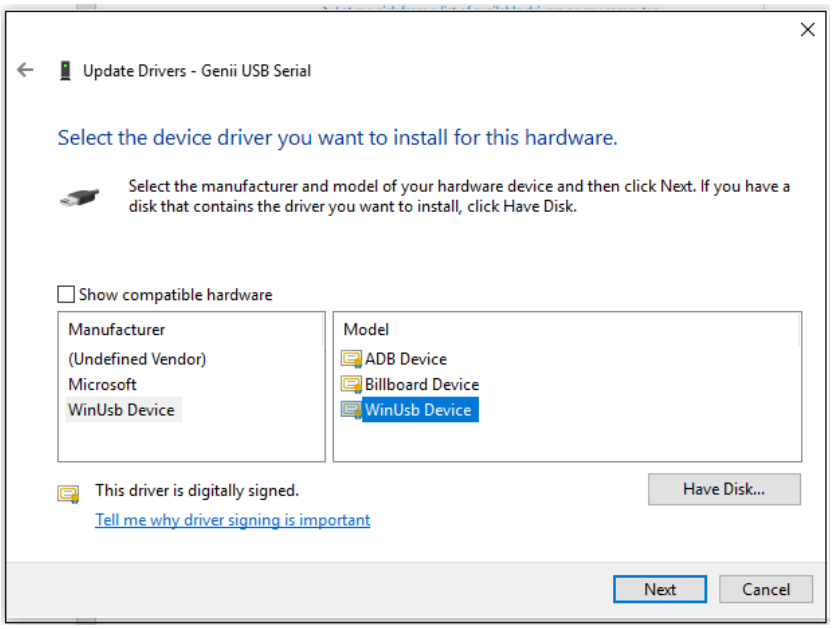
3. **Browse my computer for driver software** seçeneğini seçiniz.



4. Bilgisayarım üzerinden "**Let me pick from a list of available drivers''** seçeneğini seçiniz.

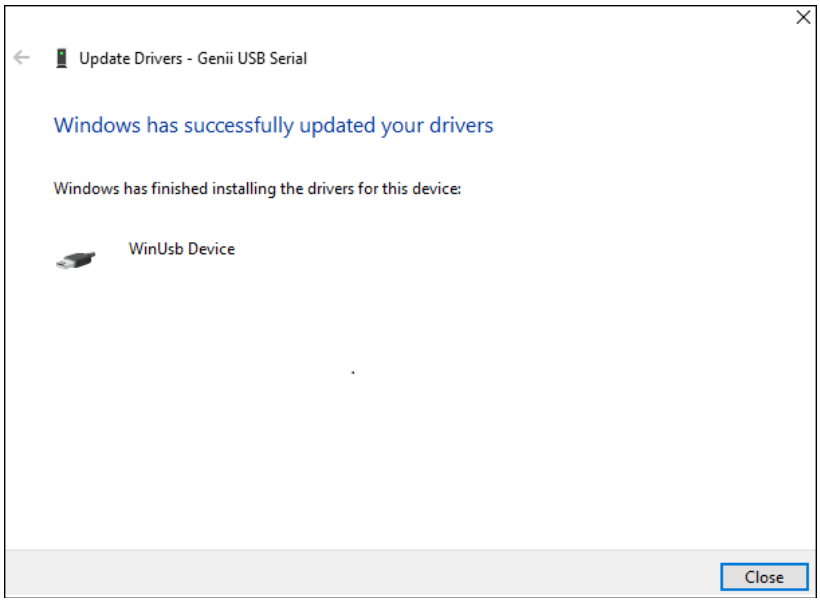


5. ''**Show compatible hardware**'' seçeneğinin işaretini kaldırın ve Manufacture için ''**WinUsb Aygıtı**'' ve Model için ''**WinUsb Device**'' öğesini seçiniz.



6. Aşağıdaki Uyarı görüntülenecektir. **Yes** butonuna tıklayınız.

7. Ekranda "Windows has successfully updated your drivers" uyarısı görüntülenecektir.

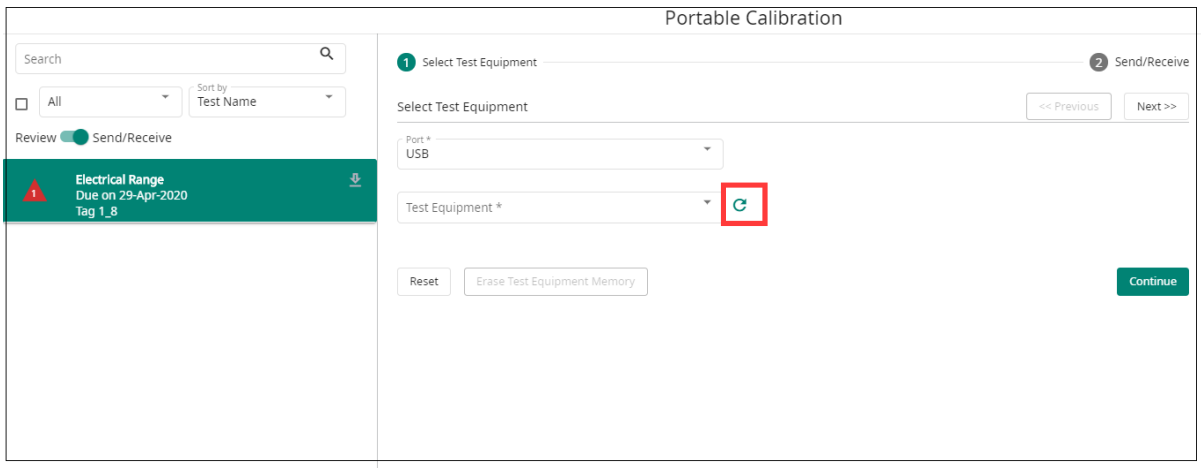


Cihazı ilk kez bağladığınızda her cihaz kategorisi için yukarıdaki adımları tekrarlayınız.

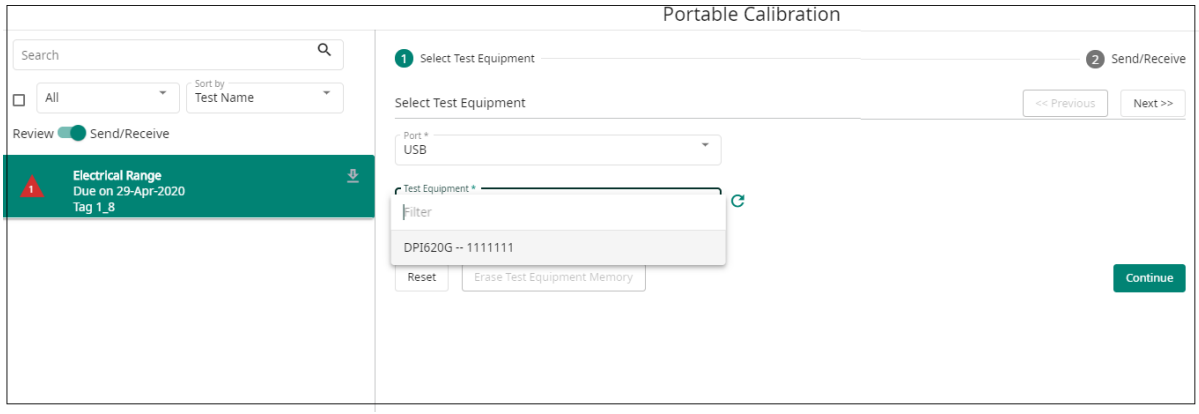
Örneğin, bir PACE ve Genii ekipmanını ilk kez bağlarsanız, PACE ve Genii için yukarıdaki adımları ilk seferde ayrı ayrı tekrarlamanız gerekebilir. Sonrasında, Tüm PACE ekipmanlarının ve Genii ekipmanlarının diğer tüm örnekleri, bu ayarları yapmaya gerek kalmadan çalışmalıdır. Ancak, daha sonra DPI611 / 612 gibi farklı bir cihaz kategorisi bağlarsanız, bu cihaz kategorisi için adımları tekrarlamanız gerekecektir.

4.2 Test Ekipmanı İletişim Cihazının Test Edilmesi

1. 4Sight2'de Teknisyen olarak oturum açınız.
2. **Varlıklar >> Çalışma** Listesi gidiniz.
3. Bir veya daha fazla aralık seçiniz ve bunları Taşınabilir veya Otomatik kalibrasyon iş akışına atayınız.
4. **Yenile** butonuna tıklayınız..



5. **Test Ekipmanı** açılır menüsüne tıklayınız. Bağlı cihazı listede görüyorsanız, Test Ekipmanı İletişim Cihazı doğru şekilde yapılandırılmıştır.



4.3 Sıcaklık Kalibratörü Sürücü Yapılandırması

Sıcaklık Kalibratörünün 4Sight2 ile iletişim kurmasına izin vermek için bir FTDI sürücüsü kurulmalıdır.

1. Bu bağlantıyı kullanarak FTDI sürücüsünü indirin: https://www.ftdichip.com/Drivers/VCP.htm.
2. İndirilen dosyaları zip klasöründen ayıklayınız ve dosyayı bilgisayarınızda bilinen bir konuma kaydediniz.
3. Bilgisayarınızda Windows Aygıt Yöneticisine gidiniz.
4. Sıcaklık kalibratörünü görüntülemek için cihaz listesinden Portlar (COM & LPT) öğesini seçiniz.
5. Sıcaklık kalibratörüne sağ tıklayın ve ‘‘update drivers’’ seçeneğini seçiniz.
6. Sürücü yazılımı için bilgisayarıma Gözat seçeneğini seçiniz.
7. Bu konumdaki sürücüleri ara başlıklı arama kutusunun yanındaki Gözat seçeneğini seçiniz.
8. Sürücü yüklemesini içeren çıkarılmış klasörü seçiniz.
9. İleri'yi seçin ve ardından kapatın.
10. Sürücü şimdi yüklenecektir.
11. 4Sight2'de bir sıcaklık kalibratörü ile iletişimi test etmek için, Otomatik kalibrasyona gidin ve sıcaklık kalibratörünün, Giriş Kontrolörü olarak seçilebileceğini kontrol edin. Alternatif olarak, 4. bölümden 14. Adımı tekrar çalıştırınız.

Dağıtım Kılavuzu

5. Dağıtım Kılavuzu

5.1 Dağıtım Mimarisi

Tipik mimari, aynı makinede çalışan PostgreSQL veritabanıyla Tomcat Web Sunucusu içinde çalışan 4Sight2 web uygulamasını ve UAA (Kullanıcı Kimlik Doğrulaması ve Yetkilendirme) sunucusunu içerir.

Tarayıcı İstemcisi Web Uygulaması 4Sight2 sunucusuna bağlanır ve bu sunucu da PostgreSQL veritabanından bilgileri depolar ve alır.

5.2 Fiziksel Dağıtım

4Sight2'yi kuran kullanıcının, aşağıdakiler de dahil olmak üzere kullanıcı güvenlik politikalarını karşılayan Siber Güvenlik Önlemlerine sahip olduğunu varsayıyoruz:

- Sunucu, fiziksel sınırlı erişim kontrolü olan güvenli bir konuma yerleştirilir.
- Sunucu erişim kontrolü, sınırlı yetkilendirme erişimiyle korunmaktadır.
- Sunucu ağı, yalnızca bilinen portlarda iyi bilinen uygulamalara sınırlı erişime izin vermek için güvenlik duvarıyla korunur.
- Uygulamalar kendi bağlamlarında çalışır ve yalnızca kendi klasörlerindeki veritabanı ve dosya sistemlerine erişime sahiptir.

5.3 Ağ

İstemciler, ethernet bağlantıları veya kablosuz ağ aracılığıyla Web Tarayıcılarını kullanılarak bağlanırlar. Kablosuz bant genişliğine ve bağlanan cihazların sayısına bağlı olarak kablosuz ağda potansiyel gecikme olabilir.

Tarayıcıda yüklü tüm tarayıcı eklentilerini ve uzantılarını devre dışı bırakmanız veya kaldırmanız önerilir.

4Sight2 web sunucusu internete açık olmamalı, ihtiyaç duyulan herhangi bir erişim Intranet veya VPN aracılığıyla sağlanmalıdır.

5.4 Dağıtım Sırası

PostgreSQL, Tomcat ve Java Runtime, 4Sight2 uygulamasının ön koşullarıdır. PostgreSQL ayrı bir paket olarak kurulurken, diğerleri uygulamayla birlikte paketlenir. Dolayısıyla, PostgreSQL zaten kullanıcı makinesinde kuruluysa, bağlanmak ve yapılandırmak için sadece super user şifresine ihtiyacımız vardır.

Kurulum, makinede Windows yönetici haklarını gerektirir. Kurulumdan önce, kullanıcının PostgreSQL super user şifresine sahip olması gerekir. Uygulama yöneticisi kullanıcı adı & şifresi ve Veritabanı kullanıcı adı & şifresi.

PostgreSQL super user şifresi, veritabanı ve PostgreSQL sunucusu içindeki diğer yapıları oluşturmak için gereklidir. Uygulama yöneticisi, uygulamanın ilk kullanıcısıdır. Diğer kullanıcıları oluşturmaktan ve onlara farklı roller atamaktan sorumludurlar. Veritabanı kullanıcısının 4Sight2 ve UAA veritabanına erişimi vardır. Bu kullanıcı adı kimlik bilgileri, veritabanına erişim için kullanılır.

Uygulama bir makine portunda yayınlanır. Varsayılan port numarası 8083'tür ve kullanıcı yükleme sırasında veya daha sonra port numarasını değiştirebilir. Tomcat'teki varsayılan uygulama içeriği 4Sight2'dir.

İşletim sistemini güçlendirmek için Microsoft veya CIS yönergelerine göre İşletim Sistemi sertleştirme prosedürünü izleyiniz. Kurulum prosedürü, kullanıcıya 4Sight2 sunucusunu kurmadan önce PostgreSQL kurması için rehberlik edecektir.

Test ekipmanı, USB portu üzerinden bağlandığında, Test Ekipmanı İletişim Cihazı istemci makinesine yüklenecektir. Eğer Test Ekipmanı İletişim Cihazı makinede hali hazırda kurulu değilse, kullanıcıdan 4Sight2 sunucusundan Test Ekipmanı İletişim Cihazı indirilmesi ve makineye kurulması istenir. Test Ekipmanı İletişim Cihazı, 9000 numaralı portu dinler ve yalnızca güvenli katman üzerinden iletişim kurabilir.

5.5 Dağıtım Sonrası Görevler

5.5.1 Kullanıcı ve Grup Ekleme

Yönetici, uygulamada Süpervizör, Kıdemli Teknisyen, Teknisyen ve Denetçi gibi farklı kullanıcılar oluşturmaktan sorumludur. Yönetici bunları farklı yerleşik varsayılan gruplara atayabilir. Daha fazla kontrol veya daha ayrıntılı erişim gerekiyorsa, yönetici özel gruplar oluşturabilir ve bunlara belirli erişimler atayabilir.

5.5.2 Varsayılan şifreler

Tomcat kullanıcısı için "C:\ProgramFiles\Druck\4Sight2\<<latest folder number>>\apache-tomcat\conf\tomcat-user.xml" dosyasında sabit kodlanmış varsayılan parolayı kullanıyoruz.

Varsayılan parolayı değiştirmeniz ve her zaman en iyi parola uygulamalarına uyan bir parola kullanmanız önerilir.

<role rolename = "tomcat" />

<kullanıcı kullanıcı adı = "tomcat" password = "P @ 55w0rd" roles = "tomcat" />

</tomcat-users>

Bu uygulamanın güvenli olmasını sağlamak için en iyi uygulamalar yapılmıştır. Ek güvenlik sağlamak için lütfen aşağıdaki görevleri gerçekleştirin:

Yapılandırma dosyaları ve klasörleri, yalnızca varsayılan olarak erişim haklarına sahip Hizmet ve Sistemler ile korunur. Bu nedenle, aşağıdaki görevleri gerçekleştirmeye çalışmadan önce, yönetici kullanıcı yalnızca C:\Program Files\Druck\4Sight2\<<latest folder number>>\apache-tomcat\conf klasörüne okuma/yazma erişimine sahiptir, bu nedenle komut istemini yönetici kullanıcı kimlik bilgileriyle açın.

5.5.3 Güvenli İletişim

Bu bölüm, 4sight2'yi kendinden imzalı bir sertifika kullanarak güvenli bir modda (SSL modu olarak da bilinir) yapılandırmak için talimatlar sağlar. Lütfen devam etmeden önce 4Sight2 uygulamasında tanımlanan varsayımları ve hüküm ve koşulları okuyun. Kendinden imzalı sertifika, 4Sight2'de SSL'yi etkinleştirmenin bir yoludur. Alternatif olarak, üçüncü taraf bir CA sertifikası, Symantec, Digicert ve benzeri birçok satıcıdan satın alınabilir.

Not: Yalnızca SSL'yi etkinleştirmek, uygulamanızı tam olarak güvenli hale getirmez. Bu, güvenli bir web uygulaması oluşturmaya yönelik en yaygın uygulamalardan biridir.

5.5.3.1 Varsayımlar ve Uyarılar

Aşağıdaki talimatların uygulanabilmesi için aşağıdaki varsayımlar yapılmıştır:

Kendinden İmzalı Sertifikalar oluşturmak için Windows için OpenSSL yazılımı gereklidir. 4Sight2, kuruluşlarınızın, bölgesel ve ulusal yasaların ve düzenleyici yönergelerin OpenSSL yazılımını kullanmanıza izin verdiğini varsayar.

- Keytool, Java tarafından sağlanan ve https yapılandırmasında yer alan çeşitli bileşenleri oluşturmak için kullanılan bir Anahtar ve Sertifika yönetimi yardımcı programıdır. 4Sight2, kuruluşlarınızın, bölgesel ve ulusal yasaların ve düzenleyici yönergelerin Keytool yardımcı programını kullanmanıza izin verdiğini varsayar.
- Aşağıdaki yapılandırmaları gerçekleştirmek için yönetici ayrıcalıklarına ihtiyacınız var. Yönetim haklarını alma konusunda daha fazla bilgi için yerel IT departmanınızla iletişime geçiniz.
- Aşağıdaki adımlar, bilgisayar süreci hakkında temel anlayış gerektirir, bu nedenle ideal olarak bu adımların yerel IT departmanı tarafından veya rehberliğinde gerçekleştirilmesi tavsiye edilir
- Bu belgede sunulan ana bilgisayar adları, parolalar, URL'ler ve klasör yolları gibi içerik yalnızca referans içindir. Yürütmeden önce komutları uygun şekilde değiştirdiğinizden emin olun.
- Aşağıdaki bölümler iki senaryoyu kapsamaktadır. Biri Sunucu & İstemci aynı makinede ve ikincisi Sunucu & İstemci farklı makinelerde (yani, Çoklu İstemci senaryosu).

5.5.3.2 yılında 4Sight2 Uygulamasını yapılandırma adımları Https

1. 4Sight2'yi Windows Hizmetlerinden durdurunuz
2. Komut istemini Admin Mode olarak açınız
3. Aşağıdaki komutu uygulayarak 4Sight2 kurulum dizininde aşağıdaki klasöre gidiniz,

   cd "C: \ Program Files \ Druck \ 4Sight2 \ <<latest folder number>> \ apache-tomcat \ conf"
4. Komut isteminde aşağıdaki komutu çalıştırarak tuş takımının mevcut olup olmadığını kontrol edin:

   Key- tool -?

   Değilse, aşağıda gösterildiği gibi 4Sight2 kurulum klasöründeki JRE bölmesine ortam yolunu ayarlayın. Kurulum klasörüne göre doğru yolu güncelleyin.

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

   Set "Path=%Path%;C:\Program Files\Druck\4Sight2\<<latest folder number>>\jre\bin"
5. Yeni bir sertifika oluşturmak için 6. Adıma geçiniz, aksi takdirde zaten bir sertifika mevcut ise sıradakileri takip ediniz:

   a. 4Sight.jks sertifika dosyasının java anahtar deposunda bulunup bulunmadığını kontrol edin

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

   b. Sertifika zaten yüklüyse kaldırın,
   keytool -delete -noprompt -alias <<hostname>> -storepass <<KeyPassword>> -anahtar deposu 4Sight.jks

   c. 4SightV2PublicKey.cer olup olmadığını kontrol edin ve silin,

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

   d. Java cacert dosyasında sertifika olup olmadığını kontrol edin.
   keytool -list -alias <<hostname>> -storepass changeit -keystore "../../jre/lib/security/cacerts"

   e. Java belleğinde sertifika varsa sertifikayı silin.

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

6. Aşağıdaki linki yürüterek yeni sertifika oluşturun:
   keytool -genkey -trustcacerts -keyalg "RSA" -keysize 2048 -geçerlilik 1095 -keypass <<KeyPassword>> -alias <<hostname>> -keystore 4Sight.jks -storepass <<StorePassword>> -dname "CN =% COMPUTERNAME%, OU = << Organization Unit >>, O = <<Organization>>, L = <<Location>>, S = <<State>>, C = << Country Initial >> "-ext eku: crit = sa
7. Sertifikayı 4SightV2PublicKey.cer (Do not change name or path) dosyasından dışarıya aktarınız.
   keytool -İhracat -Alias << hostname >> -keystore 4Sight.jks -storepass << StorePassword >> - C" -dosyadan StoreType JKS: \ Program Files \ Druck \ 4Sight2 \ <<latest folder number>> \ app \ Certificate \ 4SightV2PublicKey.cer "
   Komut başarıyla yürütüldüğünde, "Certificate stored in file C:\Program Files\Druck\4Sight2\<<latest folder number>>\app\Certificate\4SightV2PublicKey.cer" mesajı görüntülenir.
8. Sertifikayı java CACert dosyasına aktarın.
   keytool -import -noprompt -trustcacerts -alias <<ana bilgisayar adı>> -storepass changeit -keystore "../../jre/lib/security/cacerts" -file ../../app/Certificate/4SightV2PublicKey.cer
   Başarılı komutun ardından, "Certificate was added to keystore" mesajı görüntülenecektir.
9. Sertifikayı Tomcat yapılandırma dosyasına girin
   a. Server.xml dosyasını aşağıdaki konumdan açın.
   C: \ Program Files \ Druck \ 4Sight2 \ <<latest folder number>> \ apache-tomcat \ conf \ server.xml "
   b. Server.xml'de aşağıdaki girişi yapın.
   <Connector port = "8443" protocol = "org.apache.coyote.http11.Http11NioProtocol" maxThreads = "150" SSLEnabled = "true" sslProtocol = "TLSv1.2" keystoreFile = "conf / 4Sight.jks"
   keystorePass = "<<KeyPassword>>" keyAlias = "tomcat" şeması = "https" secure = "true" clientAuth = "false" />
   c. Http bağlantılarını devre dışı bırakmak için aşağıdaki bölümü yorumlayın.
   <connectionTimeout = "20000" maxSwallowSize = "104857600" port = "8083" protocol = "HTTP / 1.1" redirectPort = "8443" relaxedPathChars = "& quot; [\ ] ^` {|} + "relaxedQueryChars =" & quot; [ \ ] ^ `{|} +" />

   Not: Bu bölüme yorum yapmazsanız uygulama çalışmayacaktır.
10. Bu noktada 4Sight2 uygulamasının Https yapılandırması tamamlanmıştır.
11. Yukarıda yapılan yapılandırmaları test etmek için Windows Hizmetinde 4Sight2 Service yeniden başlatın.
12. Google chrome'u açın, tarayıcı önbelleğini temizleyin ve tarayıcıyı yeniden başlatınız.
13. Tarayıcıya şu URL'yi girin: https: // <<host-name>>: 8443 / 4sight2

- URL'yi ilk kez yüklemek daha uzun sürebilir.
- "Your connection is not private" yazan ekran görüntülenecektir
- **Advanced** butonuna tıklayın >> **Proceed to XX** bağlantısını başlatın.
- 4sight2 ekranını görmüyorsanız, **Reload** düğmesine tıklayın.
- 4sight2 sayfasına yönlendirileceksiniz.

- Adres çubuğunda bir "Not Secure" hatası olacak ve sonunda mmc'de sertifika kaydettikten sonra kaybolacaktır.

5.5.3.3 Sunucu Makineye Yüklüyse Https'de DruckCommsServer'ı yapılandırma adımları

Komutu çalıştırmadan önce << >> içindeki değerleri uygun verilerle değiştirin.

1. DruckCommsServer'ı Windows Hizmetleri üzerinden durdurun.
2. **Admin Mode** komut istemini açın.
3. Komut isteminde aşağıdaki komutu çalıştırarak anahtar aracının mevcut olup olmadığını kontrol edin: **Keytool-?**

   Değilse, aşağıda gösterildiği gibi 4Sight2 kurulum klasöründeki JRE bölmesine ortam yolunu ayarlayın. Kurulum klasörüne göre doğru yolu güncelleyin.

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

   "Path=%Path%;C:\Program Files\Druck\4Sight2\<<latest folder number>>\jre\bin" olarak ayarlayın.
4. Aşağıdaki komutu yürüterek DruckCommServer kurulum dizini içinde aşağıdaki klasöre gidin,

   cd " C:\Program Files\Druck\DruckCommsServer\<< Communication Service version >>"
5. Bir sertifikanın mevcut olup olmadığını kontrol edin, aşağıdakileri yapın:

   a. Java cacert dosyası içersinde sertifika olup olmadığını kontrol edin.

   keytool -list -alias tomcat -storepass changeit -keystore cacerts

   b. Java belleğinde varsa sertifikayı silin.

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

   c. Varsayılan olarak gelen CommsServer'dan önceden yapılandırılmış sertifikaları silin

   del 4Sight.jks

   del 4SightV2DeviceMngr.pfx
6. Aşağıdakini adresi yürüterek yeni sertifika oluşturun:

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

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

   Komut başarıyla yürütüldüğünde, "Certificate stored in file DruckCommServer.cer" mesajı görüntülenir.
8. Comm sunucu sertifikasını java CACert dosyasına aktarın.

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

   Başarılı komutun ardından, "Certificate was added to keystore" mesajı görüntülenecektir.
9. 4Sight sertifikasını java CACert dosyasına aktarın.

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

Başarılı komutun ardından, "Certificate was added to keystore" mesajı görüntülenecektir.

10. DruckCommsServer'da application.properties için anahtar deposu parolasını düzenleyin. Bu dosyayı açın:

    C: \ Program Files \ Druck \ DruckCommsServer \ << İletişim Hizmeti Version >> \ application.properties ve aşağıdaki satırı değiştirin:

    keystore = CommServer.jks

    key-store.password = << StorePassword >>

    Not: << **StorePassword** >> 6. adımda kullanılan **StorePassword** parolasına atıfta bulunur.

11. 4Sight2 ve DruckCommsServer Service hizmetlerini yeniden başlatın.

5.5.3.4 İstemci Makineye Yüklüyse DruckCommsServer'ı HTTP'lerde Yapılandırma Adımları

1. Keytool yardımcı programı Java ile paketlenmiştir, böylece makinenize Java yükleyebilir veya Java'yı yüklemeden doğrudan java keytool'un kullanılabilirliğini kontrol edebilirsiniz.
2. DruckCommsServer'ı Windows Hizmetlerinden durdurun.
3. **Admin Mode** komut istemini açın.
4. Komut isteminde aşağıdaki komutu çalıştırarak anahtar aracının mevcut olup olmadığını kontrol edin: **Keytool-?**

    Değilse, aşağıda gösterildiği gibi 4Sight2 kurulum klasöründeki JRE bölmesine ortam yolunu ayarlayın. Kurulum klasörüne göre doğru yolu güncelleyin.
    C: \ Program Files \ Java \ << Java sürümü >> \ bin "Path=%Path%;C:\Program Files\Druck\4Sight2\<<latest folder number>>\jre\bin" olarak ayarlayın.

5. 4SightV2PublicKey.cer dosyasını 4Sight uygulamasının kurulu olduğu Sunucu makinesinden alın. Bu dosya aşağıdaki gibi sunucuda bulunur,

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

6. Bu **4SightV2PublicKey.cer dosyasını** aşağıdaki konuma kopyalayın :

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

7. Şimdi bölüm 5.5.3.3'teki 4 ile 8 arasındaki adımları izleyin.
8. 4Sight sertifikasını java CACert dosyasına aktarın.

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

    Başarılı komutun ardından, "Certificate was added to keystore" mesajı görüntülenecektir.
9. Şimdi bölüm 5.5.3.3'teki 10'dan 11'e kadar olan adımları izleyin.

5.5.3.5 4Sight2 için kendinden imzalı sertifika oluşturma adımları

1. Windows için Open SSL'yi indirin ve yükleyin.
2. Windows Hizmetlerinden 4Sight2 Service hizmetlerini durdurun.
3. C sürücüsünün içinde **4Sight2Certificate** adlı yeni bir klasör oluşturun.
   Bu klasöre yönetici erişiminiz olması koşuluyla herhangi bir konumu veya klasör adını seçebilirsiniz.
4. Not defterinde yukarıdaki klasörün içinde yeni bir dosya oluşturun ve dosyayı **openssl-ca.cnf** olarak kaydedin.
   Aşağıdaki içeriği dosyaya kopyalayın ve dosyayı kaydedin.

```
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
```

Not: Yukarıdaki **[Company Name]** güncelleyin ve dosyayı kaydedin. Bu, sertifika verenlerin adıdır. yönetim konsolunda görün

5. Not defterinde yukarıdaki klasörün içinde yeni bir dosya oluşturun ve dosyayı **openssl-server.cnf** olarak kaydedin, aşağıdaki içeriği dosyaya kopyalayın ve dosyayı kaydedin.

```
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 localhostIP.2
= ::
```

Not: Yukarıdaki Ana Bilgisayar Adını ve IPv4 adresini güncelleyin ve dosyayı kaydedin.

6. Yönetici ayrıcalıklarına sahip komut istemini açın.
7. Aşağıdakini adresi yürüterek 4Sight2Certificate klasörüne gidin,
   cd "<<full path to 4Sight2Certificate >>"
8. Aşağıdaki komutu yürüterek OpenSSL bin klasör yolu değişkenini ayarlayın.
   path=%path%;"<<bin folder of openssl>>" olarak ayarlayın
   Örnek varsayılan path:
   Path=%Path%;"C:\Program Files\OpenSSL-Win64\bin" olarak ayarlayın
9. Aşağıdaki komutu yürüterek JRE bin klasörü path değişkenini ayarlayın. Not: aşağıdaki path farklı olabilir.
   path=%path%;"C:\Program Files\Druck\4Sight2\<<latest folder number>>\jre\bin" olarak ayarlayın
10. cacert.pem ve cakey.pem dosyalarını oluşturmak için aşağıdaki komutu çalıştırın
    openssl req -x509 -config openssl-ca.cnf -newkey rsa:4096 -days <<Number of days>> -sha256 -nodes -out cacert.pem -outform PEM
    Örneğin ülke, eyalet vb. İstendiğinde doğru sertifika verilerini girin.
11. servercert.csr ve serverkey.pem dosyalarını oluşturmak için aşağıdaki komutları yürütün
    openssl req -config openssl-server.cnf -newkey rsa:2048 -days <<Number of days>> -sha256 -nodes -out servercert.csr -outform PEM
    Örneğin ülke, eyalet vb. İçin sorulduğunda doğru sertifika tarihini girin.
12. Not defterinde yeni bir dosya oluşturun ve bunu index.txt olarak adlandırın. Dosyayı 4Sight2Certificate klasörüne kaydedin.
13. Not defterinde yeni bir dosya oluşturun ve bunu serial.txt olarak adlandırın. Dosyayı 4Sight2Certificate klasörüne kaydedin. Dosyayı açın ve 01 girin Dosyayı kaydedin ve kapatın.
14. servercert.pem ve server- key.pem dosyalarında yeni sertifikalar oluşturmak için aşağıdaki komutu yürütün.
    openssl ca -config openssl-ca.cnf -policy signing_policy -extensions signing_req -out servercert.pem -infiles servercert.csr
    Değişiklikleri uygulamak için Y komutunu girin. Başarıyla yürütüldükten sonra veritabanının güncellendiğini göreceksiniz.
15. Aşağıdaki komutu uygulayarak mevcut anahtar dosyalarını PFX formatında paketleyin.
    openssl pkcs12 -export -in servercert.pem -inkey serverkey.pem -certfile cacert.pem -name "<<hostname>>" -out <<hostname>> .p12
    iki kez şifre girmeniz istenecektir.
16. PFX belleğini, yukarıda belirtilen JRE bellek yerine, yani tomcat / config yoluna göre sıralanmış Java anahtar belleğine dönüştürün.

keytool -importkeystore -srckeystore <<hostname>> .p12 -srcstoretype PKCS12 -destkeystore "C: \ Program Files \ Druck \ 4Sight2 \ <<latest folder number>> \ apache-tomcat \ conf \ 4Sight.jks"
-deststoretype jks
Not: Parolayı her iki bellek için de aynı tutun. Tomcat'in yapılandırma klasöründe bulunan 4Sight.jks'yi yukarıda gösterildiği gibi gösterdiğinizden emin olun.
Hedef anahtar bellek parolasını ve kaynak anahtar bellek parolasını girmeniz istenecektir. Başarılı bir komut yürütmeden sonra "Import command completed: 1 entries successfully imported" mesajını göreceksiniz.

17. Sertifikayı java anahtar belleğinden aşağıdaki dosyaya aktarın:
C: \ Program Files \ Druck \ 4Sight2 \ <<latest folder number>> \ app \ Certificate \ 4SightV2PublicKey.cer keytool
-export -alias <<hostname>> -keystore "C: \ Program Files \ Druck \ 4Sight2 \ <<latest folder number>> \ apache-tomcat \ conf \ 4Sight.jks "-storePass "<<password>>" - storetype JKS -file" C: \ Program Files
\ Druck \ 4Sight2 \ <<latest folder number>> \ app \ Certificate \ 4SightV2PublicKey.cer "
Not: Tomcat'in yapılandırma klasöründe bulunan 4Sight.jks'yi yukarıda gösterildiği gibi gösterdiğinizden emin olun. Başarılı bir yürütmeden sonra dosya mesajında saklanan Sertifika alacaksınız,

18. Sertifika dosyasını 4sight2 kurulum dizini içindeki cacerts klasörüne alın.
Not: path, kurulum dizinine ve 4sight2 sürümüne bağlı olarak değişebilir
keytool -import -noprompt -trustcacerts -alias <<hostname>> -storepass changeit -keystore "C:\Program Files\Druck\4Sight2\<<latest folder number>>\jre\lib\security\cacerts" -file "C:\ProgramFiles\Druck\4Sight2\<<latest folder number>>\app\Certificate\4SightV2PublicKey.cer"
Not: Bazı nedenlerden dolayı oluşturmaya çalıştığınız takma ad zaten mevcut, önce onu silmek için aşağıdaki komutu çalıştırın ve ardından yeni bir takma ad oluşturmak için yukarıda çalıştırın:
keytool -delete -noprompt -trustcacerts -alias <<hostname>> -storepass changeit -keystore "C:\Program Files\Druck\4Sight2\<<latest folder number>>\jre\lib\security\cacerts" -file "C:\ProgramFiles\Druck\4Sight2\<<latest folder number>>\app\Certificate\4SightV2PublicKey.cer"
Bu komutun başarılı bir şekilde çalıştırılmasından sonra "Certificate was added to keystore" mesajını alacaksınız.

19. server.xml dosyasında aşağıdaki değişikliği yapın
(C: \ Program Files \ Druck \ 4Sight2 \ <<latest folder number>> \ apache-tomcat \ conf içinde bulunur).
    a. Server.xml'de aşağıdaki girişi yapın.

```
<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 bağlantılarını devre dışı bırakmak için aşağıdaki bölümü yorumlayın.
<connectionTimeout = "20000" maxSwallowSize = "104857600" port = "8083" protocol = "HTTP / 1.1" redirectPort = "8443" relaxedPathChars = "& quot; [\ ] ^` {|} + "relaxedQueryChars =" & quot; [ \ ] ^ `{|} +" />

20. Bu, 4Sight2 için https yapılandırmasını tamamlar. Şimdi 4sight2 hizmetini pencere hizmetlerinden başlatın.

5.5.3.6 Sunucu Makineye Yüklendiyse DruckCommsServer İçin Kendinden İmzalı Sertifikayı Yapılandırma Adımları

Burada, 5.5.3.5 bölümündeki adımları uygulayarak 4sight2 uygulamasını başarıyla HTTP'lere dönüştürdüğünüzü ve 4Sight2Certificate klasöründe aşağıdaki dosyalara sahip olduğunuzu varsaydık:

- openssl-server.cnf
- openssl-ca.cnf
- cacert.pem
- cakey.pem
- index.txt
- serial.txt
- 4SightV2PublicKey.cer (Bu dosya C: \ Program Files \ Druck \ 4Sight2 \ <<latest folder number>> \ app \Certificate klasöründe bulunabilir)

1. **CommserverCertificate** olarak yeni bir klasör oluşturun ve yukarıdaki dosyaları kopyalayıp aşağıdaki gibi değişiklikler yapın:

- openssl-server.cnf

  Req bölümü altında **default_keyfile** değerini "**DruckCommServerCertKey.pem**" olarak değiştirin

  - **server_distinguished_name** altında **commonName** değerini "**localhost**" olarakdeğiştirin
  - **alternate_names** altında, DNS.1 değerini "**localhost**" olarak değiştirin.
  - **alternate_names** altında, **IP.1** değerini " **127.0.0.1** " olarak değiştirin.
  - Dosyayı kaydedin.

- openssl-ca.cnf. (İçinde hiçbir şeyi değiştirmeyin)
- cacert.pem. (İçinde hiçbir şeyi değiştirmeyin)
- index.txt (İçindeki tüm içeriği silin, boş dosya yapın)
- serial.txt (içindeki tüm içeriği silin ve içeride sadece 02 girişi yapın)

2. DruckCommsServer hizmetini Windows Service hizmetlerinde durdurun.
3. Yönetici ayrıcalıklarına sahip komut istemini açın.
4. Aşağıdakini yürüterek **CommserverCertificate** klasörüne gidin,

   cd "<<full path to CommserverCertificate >>"
5. Aşağıdaki komutu yürüterek OpenSSL bin klasör path değişkenini ayarlayın.

   path=%path%;"<<bin folder of openssl>>" olarak ayarlayın

   Örnek varsayılan yol:

   Path=%Path%;"C:\Program Files\OpenSSL-Win64\bin" olarak ayarlayın
6. Aşağıdaki komutu yürüterek JRE bin klasörü path değişkenini ayarlayın.

   Not: aşağıdaki yol farklı olabilir,

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

7. Bunu bitirdikten sonra, **openssl req -config openssl-server.cnf -newkey rsa: 2048 -sha256 -nodes -out DruckCommServer.csr -outform PEM** komutunu izleyerek bir Comm Sunucusu sertifika isteği oluşturun.

   Bu komut çalıştırıldıktan sonra, **DruckCommServer.csr'de** bir isteğiniz

   ve **DruckCommServerCertKey.pem'de** özel bir anahtara sahip olacaksınız.

8. Ardından, csr isteğini ca'nızla imzalamak için aşağıdakileri gerçekleştirin:

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

9. Bundan sonra, aşağıdaki komutu kullanarak iletişim sunucusu için tomcat takma adıyla bir PFX dosyası oluşturun, **openssl pkcs12 -export -in DruckCommServerCert.pem -inkey DruckCommServerCertKey.pem -certfile cacert.pem -name "tomcat" -out DruckCommServer.pfx**

10. Anahtar aracını kullanarak PFX deposunu Java anahtar deposuna dönüştürün

    Not: Her iki anahtar deposu için parolayı aynı tutun.

    keytool -importkeystore -srckeystore DruckCommServer.pfx -srcstoretype PKCS12 -

    destkeystore CommServer.jks -deststoretype jks

11. Şimdi sertifikayı cacert'e aktarın .

    a. Şimdi, varsayılan **keytool** ile birlikte gelen mevcut tomcat diğer adını silin **-delete -noprompt -trustcacerts -alias tomcat -storepass changeit -keystore "C: \ Program Files \ Druck \ DruckCommsServer \ << Communication Service version >> \ cacerts "**

    b. Varolan tomcat takma adını sildikten sonra sertifikayı cacerts'a aktarın: **keytool -import -noprompt -trustcacerts -alias tomcat -storepass changeit -keystore "C: \ Program Files \ Druck \ DruckCommsServer \ << Communication Service version >> \ cacerts "-dosya DruckCommServerCert.pem**

12. Şimdi, aşağıdaki komutu yürütmek için 4sight genel anahtarını iletişim kimlik doğrulaması için iletişim sunucusu cacert'ine aktarmamız gerekiyor.

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

13. Yukarıdakilerin hepsini bitirdikten sonra, mevcut durumda CommserverCertificate klasörü içerisinde DruckCommServer.pfx ve CommServer.jks'ye sahip olacaksınız

    Bu dosyaları kopyalayın ve "C:\Program Files\Druck\DruckCommsServer\<< Communication Service version >> " dizinine **yapıştırın** ve **application.properties** dosyasını aynı konumda düzenleyin, özellik değerini aşağıdaki gibi değiştirin

    a. Keystore = CommServer.jks

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

    c. **key-store.type = JKS**

5.5.3.6.1 4sight ve DruckCommsServer için Windows'ta Sertifika Yükleme

1. Çalıştır'ı açın ve "mmc" yazın, Enter tuşuna basın.
2. Dosya'ya gidin ve Ek bileşen olarak Ekle / Kaldır'ı seçin.
3. Sol taraftaki menüden sertifikaları seçin. Ekle'ye basın ve ardından Computer account >> Next >> Finish seçin. Ardından Ok tuşuna tıklayın.
4. Sertifikalar (Local computer) bölümünü genişletin. Güvenilir Kök Sertifika Yetkililerini genişletin. Bunun içinde sağ tıklayın Certificates folder>>All tasks>>Import.

   cacert.pem >> next >> finish seçiniz.

   Bu nedenle, özel CA yetkilimiz güvenilir yetki altında başarıyla yüklenir.

   Tüm bu adımları gerçekleştirdikten sonra DruckCommsServer hizmetini başlatın.

5.5.3.7 İstemci Makineye Yüklendiyse DruckCommsServer İçin Kendinden İmzalı Sertifikayı Yapılandırma Adımları

DruckCommsServer'ı HTTP'lere dönüştürmek için java keytool ve OpenSSL yardımcı programına sahip olmanız gerekir.

1. Keytool yardımcı programı Java ile paketlenmiştir, böylece makinenize Java yükleyebilir veya Java'yı yüklemeden doğrudan java keytool'un kullanılabilirliğini kontrol edebilirsiniz.
2. Windows için OpenSSL'yi indirin ve kurun.
3. Aşağıdaki komutu yürüterek OpenSSL bin klasör path değişkenini ayarlayın.

   path=%path%;"<<bin folder of openssl>>" olarak ayarlayın

   Örnek varsayılan path:

   Path=%Path%;"C:\Program Files\OpenSSL-Win64\bin" olarak ayarlayın
4. Aşağıdaki komutu yürüterek JRE bin klasör path değişkenini ayarlayın.

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

   Path=%Path%; "C:\Program Files\Java\<< Java version >>\bin" olarak ayarlayın
5. DruckCommsServer hizmetini Windows Services hizmetlerinde durdurun.
6. C sürücüsünde veya istediğiniz başka bir sürücüde **CommserverCertificate** adlı yeni bir klasöroluşturun.
7. C: \ Program Files \ Druck \ 4Sight2 \ <<latest folder number>> \ app \ Certificate dizininde bulunan sunucumakinesinden 4sight2 genel sertifika dosyası **4SightV2PublicKey.cer**'ı alın ve bu dosyayı **CommserverCertificate** klasörüne kopyalayın.
8. Şimdi, bölümdeki 4. ve 5. adımları izleyerek **openssl-server**.cnf ve **openssl-ca.cnf** oluşturun 5.5.3.5 ve **CommserverCertifiCate** klasörüne adım 12 ve 13'ü izleyerek index.txt ve serial.txt oluşturun.
9. Şimdi CommServerCertificate klasöründe beş dosyanız olacak
   a. openssl-server.cnf
   b. openssl-ca.cnf
   c. index.txt
   d. serial.txt
   e. 4SightV2PublicKey.cer
10. Yönetici ayrıcalıklarına sahip komut istemini açın.

    Aşağıdakini çalıştırarak CommserverCertificate klasörüne gidin,

    cd "<<full path to CommserverCertificate >>"
11. cacert.pem ve cakey.pem dosyalarını oluşturmak için aşağıdaki komutu çalıştırın.

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

    Örneğin ülke, eyalet vb. İçin sorulduğunda doğru sertifika verilerini girin.
12. Şimdi, 5.5.3.6 bölümündeki 1. Adımı yürüterek **CommserverCertificate** klasöründeki dosyaların içeriğini değiştirin.
13. Şimdi 5.5.3.6'daki 7'den 11'e kadar olan adımları yürütün.
14. Şimdi, aşağıdaki komutu yürütmek için 4sight ortak anahtarını iletişim yetkilendirmesi için iletişim sunucusu cacert'e aktarmamız gerekiyor.

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

15. Yukarıdakilerin hepsini bitirdikten sonra, mevcut durumda CommserverCertificate klasöründe DruckCommServer.pfx ve CommServer.jks'ye sahip olacaksınız

    Bu dosyaları kopyalayın ve "**C:\Program Files\Druck\DruckCommsServer\<< Communication Service version >>**" dizinine yapıştırın ve **application.properties** dosyasını aynı konumdan düzenleyin, özellik değerini aşağıdaki gibi değiştirin

    a. Keystore = CommServer.jks

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

    c. key-store.type=JKS

5.5.3.7.1 Installing certificate in Windows for DruckCommsServer.

1. Çalıştır'ı açın ve "mmc" yazın, Enter tuşuna basın.
2. Dosya'ya gidin ve Ek bileşen olarak Ekle / Kaldır'ı seçin.
3. Sol taraftaki menüden sertifikaları seçin. Ekle'ye basın ve ardından Computer account >> Next >> Finish seçin. Ardından Ok tuşuna tıklayın.
4. Sertifikalar (Local computer) bölümünü genişletin. Güvenilir Kök Sertifika Yetkililerini genişletin. Bunun içinde sağ tıklayın Certificates folder>>All tasks>>Import.

   cacert.pem >> next >> finish seçiniz.

Bu nedenle, özel CA yetkilimiz güvenilir yetki altında başarıyla yüklenir.

Tüm bu adımları gerçekleştirdikten sonra DruckCommsServer hizmetini başlatın.

Sadece DruckCommsServer'ın başarılı bir şekilde https'ye dönüştürülüp dönüştürülmediğini kontrol etmek istiyorsanız, google chrome sekmesinde aşağıdaki bağlantıyı açmanız yeterlidir: **https: // localhost: 9443 / api / devicemanager / version** (Lütfen değiştirdiyseniz iletişim sunucusu port numaranızı girin ancak varsayılan olan 9443'tür)

5.5.3.8 4Sight2'de Sertifikayı Doğrulama

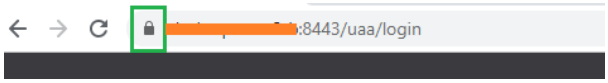
1. Sunucu PC'yi yeniden başlatın.
2. 4Sight2 ve DruckCommsServer hizmetlerini Windows Services Open'dan yeniden başlatın.
3. Google chrome'u açın, tarayıcı önbelleğini temizleyin ve Google chrome'u yeniden başlatın. Başka hiçbir Google chrome örneğinin çalışmadığından emin olun.
4. Adres çubuğuna aşağıdaki URL'yi girin, Enter tuşuna basın.

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

   Not: yukarıdaki URL'de ana bilgisayar adını kullanmanız gerekir

5. Doğru HTTPS URL'si ile giriş ekranını görüntülemelisiniz.

   Not: Kırmızı hata adres çubuğundan kayboldu. Bağlantı hala güvenli değilse, bilgisayarınızı yeniden başlatın ve 3. adıma gidin.



4Sight2 Kurulum SSS'leri

6. 4Sight2 Kurulum SSS'leri

6.1 Ayarlar ve Kurulum

Soru 1: Küresel olarak dünyanın farklı bölgelerine yayılan çok tesisli bir kuruluşum var. 4Sight2'yi kurmanın en iyi yolu nedir?

Cevap: Bu durum, tesisleri nasıl sürdürdüğünüze ve çalıştırdığınıza bağlıdır. Tüm tesislerin bakımı merkezi bir IT hub'ından yapılıyorsa, tek 4Sight2 lisansını merkezi olarak kurabilirsiniz. Tüm tesisler 4Sight2'ye ağ veya LAN üzerinden erişebilir. Öte yandan, kendi kendine çalışan ve yönetilen ayrı varlıkları olan alt işletmeleriniz varsa, birden çok 4Sight2 lisansı satın alabilirsiniz.

Soru 2: Birden fazla 4Sight2 lisansı satın alırsam, aralarında herhangi bir iletişim olacak mı?

Cevap: Hayır. Her 4Sight2 lisansı, kendi uygulama kurulumu ve veritabanı ile izole edilmiş ayrı bir yazılımdır. Ayrı kurulumlar arasında iletişim yoktur. Daha fazla netlik için veya özel gereksinimleri görüşmek için 4Sight2 lokal satış ekibiyle iletişime geçin.

Soru 3: 4Sight2'yi nasıl indirebilirim?

Cevap: 4Sight2'yi şirket web sitesinden kolayca indirebilirsiniz. Bağlantı aşağıdadır.

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

VEYA

Lokal Satış ofislerini arayabilir ve bir satın alma emri verebilirsiniz. Daha sonra demo sürümünü bir USB belleğe alabilirsiz.

Soru 4: 4Sight2'yi Windows olmayan bir işletim sistemine yükleyebilir miyim?

Cevap: Hayır. 4Sight2 yalnızca Windows platformu için desteklenir.

Soru 5: 4Sight2'yi indirip yüklediğim zaman, 4Sight2'ye nasıl erişirim?

Cevap: 4Sight2 web tabanlı bir yazılımdır. Bu nedenle, 4Sight2'yi kurduğunuzda masaüstünüzde veya bilgisayarınızda hiçbir simge oluşturulmaz. 4Sight2'ye erişmek için,

- Google Chrome'u açın, adres çubuğundaki URL'nin altına yapıştırın ve enter tuşuna basın, 4Sight2 aynı bilgisayara kuruluysa, http: // localhost: <application_port_number> / 4sight2If kullan, 4Sight2 aynı ağdaki farklı bir bilgisayara kuruluysa, şunu kullanın: http://<Computer name VEYA IP address>:<application_port_number>/4sight2
- İleride başvurmak için Google Chrome'da Yer İşareti oluşturun.

Soru 6: 4Sight2 yükleyici Postgres Veritabanı dosyalarını bulma problemi yaşıyor ise,

Lütfen yükleyicinin yerel bir konuma çıkarıldığından ve yürütülebilir dosyanın Disk 1 klasöründen çalıştırıldığından emin olun. Yükleyicinin çıkarıldığı yerel konumun uzun bir yol adı olmadığından emin olun çünkü bu, yükleyici önkoşul dosyalarının bulunamamasına da neden olabilir.

Soru 7: Yükseltme işlemi sırasında herhangi bir aşamada yükseltme işlemi iptal edilirse ne olur?

Cevap: Herhangi bir aşamada, yönetici yükseltme işlemini iptal ederse, 1.4 sürümüne geri döner ve çalışır durumda olmalıdır. Yükseltmeyi başarıyla gerçekleştirmek için yöneticinin yükseltme işlemini yeniden başlatması gerekir.

Soru 8: 4Sight2 uygulamasını yüklerken kullanıcı şu mesajı alırsa "Please enter valid port number. To know valid port numbers please refer installation manual"

Cevap: Aşağıda geçersiz port numaraları aralığı verilmiştir, kuruluma devam etmek için geçerli port numarasını seçin

- 0-1024 arasındaki port numaraları TCP bağlantısı için ayrılmıştır
- Güvenli olmayan port numaraları listesi - 2049, 3659, 4045, 6000, 6665-6669, 65535

Soru 9: Https ile 4Sight2 sistemde çalışmıyor

Cevap: 4sight2 uygulamasının kurulacağı bilgisayarın alan adı için sözdizimini takip edin

<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> ::= A'dan Z'ye kadar 52 alfabetik karakterden herhangi biri ve küçük harfle a'dan z'ye kadar

<digit> ::= 0 ile 9 arasındaki on basamaktan herhangi biri

Not: Alan adlarında büyük ve küçük harflere izin verilir. Aynı yazılıma sahip ancak büyük / küçük harfe farklı iki ad aynı kabul edilir.

6.2 Test Ekipmanı İletişim Cihazı SSS'leri

Soru 1: Kurulum kılavuzundaki tüm adımları tamamladım ve hala cihazımı listede göremiyorum.

Cevap: Bu adımları uyguladıktan sonra Test ekipmanını listede hala bulamıyorsanız, 4Sight2 sürücülerini yeniden yükleyin. Bunu yapmak için **Control Panel >> Programs and Features** gidin, listeden DruckCommsServer'ı kaldırın. Test Ekipmanı İletişim Cihazını tekrar kurun.

Soru 2: '**No Devices Found**' hatası alıyorum.

Cevap: Sorunu çözmek için,

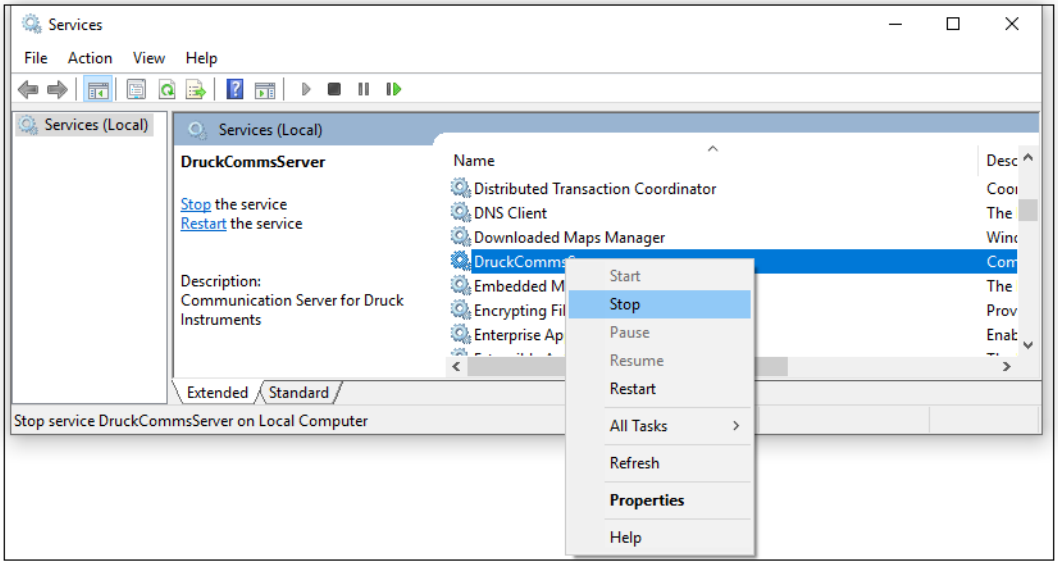
- USB kablosunu kullanarak cihazı fiziksel olarak doğru şekilde bağladığınızdan emin olun. Bunu kontrol etmek için, cihaz yöneticisine gidin ve listede cihazınızı bulun. Cihazınızı ideal olarak Universal Serial Bus cihazları bölümünde bulmalısınız. Cihazınızı Other devices altında görüyorsanız, cihazınızı bir USB cihazı yapmak için yukarıdaki ayarları yapmanız gerekir.
- Cihazınızın haberleşme veya iletişim modunda olduğundan emin olun. Yukarıdaki 1. adıma bakın.
- Sürücü yolunun (path) doğru şekilde C: \ Windows \ INF... konumuna yönlendirildiğinden emin olun. Yukarıdaki 2. adıma bakın.

Soru 3: Yenile tuşuna tıkladığımda veya listeden test ekipmanına tıkladığımda '**Internal Server Error**' hatası alıyorum.,

Cevap: Bu sorunu çözmek için,

- Windows Services (Services olarak da bilinir) bölümüne gidin,

- Listeden **DruckCommsServer** Hizmetine sağ tıklayın ve **Yeniden Başlat'a** tıklayın.



- 4Sight2'ye gidin>> **Yenile** düğmesine tıklayın. Cihazı listede görmelisiniz.

Soru 4: '**Communications Error**' hatası alıyorum.

Cevap: Bazen USB bağlantısının gevşek olması, cihazın kapanması, cihazın diğer görevleri yerine getirmesiyle meşgul olması, sunucunun diğer görevleri yürütmekle meşgul olması gibi çeşitli nedenlerden dolayı yazılım cihazla düzgün iletişim kuramaz. Yenile düğmesine tekrar tıklayın ve sorun ortadan kalkmalıdır (bunu 2-3 kez deneyin)

Ancak, bu hatayı yine de sürekli ve ısrarla alıyorsanız, aşağıdaki adımları deneyin,

- Cihazınızı (Genii / PACE) yeniden başlatın, bunun güvenli olduğundan ve cihazın kritik bir işlemin ortasında olmadığından emin olun. Tekrar deneyin. Ayrıca cihazın hala fiziksel olarak bağlı old-uğundan emin olun.

Yukarıdaki adım işe yaramazsa, yukarıdaki 3. adımdaki talimatları izleyin ve DruckCommsServer Hizmeti'ni yeniden başlatın..

Kurulum Sorunlarını Giderme

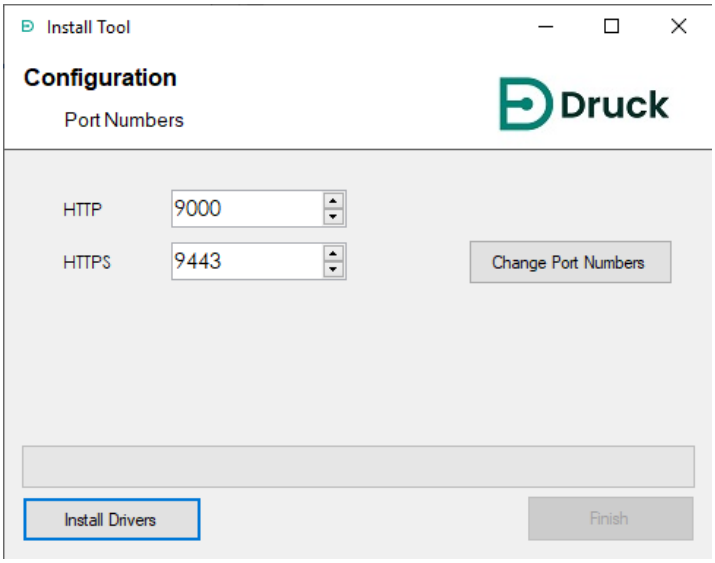
7. Kurulum Sorunlarını Giderme

7.1 Test Ekipmanı İletişim Cihazı Sorunları

Test ekipmanı ile iletişim kurmak için 4Sight2'yi kullandığınızda, herhangi bir test ekipmanının geri gönderilmediğini görebilirsiniz, ancak Test Ekipmanı iletişimcisinin, iletişimci ile doğrudan bir çağrı üzerine json dizisine geri döndüğünü kontrol etmiş olmanıza rağmen. Bu, iki ana sorundan birinden kaynaklanıyor olabilir:

Port numaraları yanlış yapılandırılmış - 4Sigth2'nin Test Ekipmanı İletişimcisi ile iletişim kurmak için hangi port numaralarının kullanıldığını öğrenmek için lütfen yönetici kullanıcınızla iletişime geçin.

Hangi port numaralarını kullanmanız gerektiğini öğrendikten sonra C: \ Program Files \ Druck \ DruckCommsServer \ [Version] 'a gidin ve CommsServerInstallTool.exe dosyasını çalıştırın.



Port numaralarını düzenleyin ve ardından **Change Port Numbers** düğmesine tıklayın. Hizmet yeniden başlarken bekleyin. Port numaraları artık değişmiştir. **Finish** düğmesini seçin.

- Test Ekipmanı İletişimcisi Https için yapılandırılmamıştır, ancak 4Sight2 yapılandırılmıştır. Test Ekipmanı İletişimcisi için kendinden imzalı bir sertifika yüklemek için yöneticinizle iletişime geçin.

7.2 Postgres Veritabanı Yedeklemesi

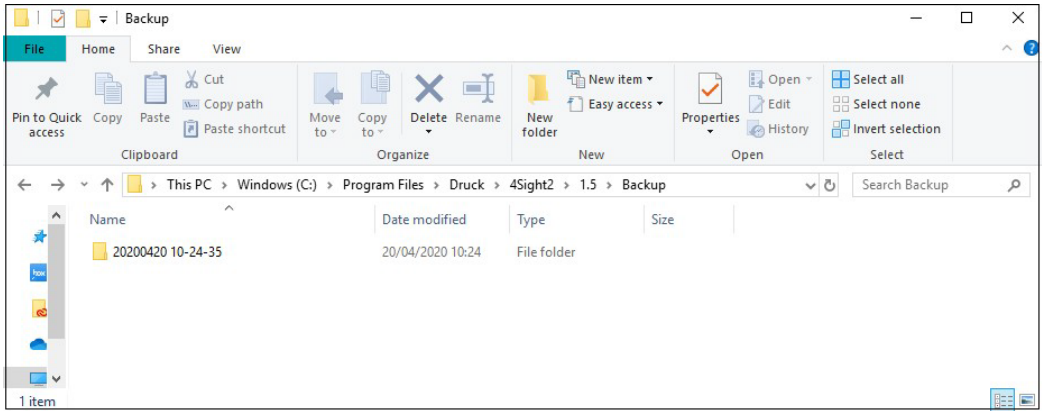
Postgres veritabanı yedeklemesi hakkında bilgi için 4Sight2 kullanım kılavuzu - 123M3138'e bakınız.

7.3 Postgres Veritabanı Geri Yükleme

4Sight Uygulamasını kullanarak zaten bir veritabanı yedeklemesi yaptığınızı varsayarsak.

4Sight uygulaması (Sürüm 1.4 ve üzeri), bir yedeklemeyi başlatmak için bir arayüz sağlar (kullanıcı tarafından başlatılır / programlanır). Bu işlem, sunucudaki 4Sight kurulum dizininin içindeki yedekleme klasöründe dosyalar oluşturur. Başlatılan her yedekleme, yedeklemenin başarıyla

tamamlandığı tarih ve saate bağlı olarak YYYYAAGGHSS (Yıl, Ay, Tarih, Saat ve Saniye) biçiminde adla yedekleme klasörü içinde yeni bir klasör oluşturur.



Yedekleme klasörünün içeriğini ayrı bir ortama yedeklemek tavsiye edilen bir uygulamadır. Her klasörde 5 dosya vardır.

1. 4Sight <APPLICATION_VERSION> .bck

2. 4Sightaudit <APPLICATION_VERSION> .bck

3. uaa <APPLICATION_VERSION> .bck

4. metadata.properties

5. status.json

*.bck dosyalarının 4Sight uygulama sürümüyle birlikte bir soneki vardır. Lütfen uygulamanızın tam sürümüyle eşleşen bir veritabanını geri yüklediğinizden emin olun. Veritabanının daha yüksek / daha düşük sürümü uygulama tarafından desteklenmemektedir. Sürümün nokta (.) Değil alt çizgi (_) içerdiğini unutmayın. 1_4 & 1.4 değil. Geri Yükleme Adımlarında aşağıdaki komutları kullanırken, lütfen <APPLCATION_VERSION> 'u kurulu olan 4Sight'ın doğru sürümüyle değiştirdiğinizden emin olun.

metadata.properties dosyası, yedeklemenin başlatılması sırasında girildiği şekliyle yedeklemenin adını içerir.

SHA 256 Kontrolü

Bir yedeklemede, her veritabanı için .bck uzantılı 3 dosya vardır. Metadata.properties dosyası, yedekleme dosyalarının her birinin SHA 256'sını içerir.

1. Yönetici olarak bir komut istemi açın ve dizini seçilen yedekleme dosyalarını içeren klasöre değiştirin.
2. Her dosyanın SHA256'sını hesaplamak için aşağıdaki komutları kullanın
   certutil -hashfile 4Sight**<APPLICATION_VERSION>**.bck SHA256 certutil -hashfile 4Sightaudit**<APPLICATION_VERSION>**.bck SHA256 certutil -hashfile uaa**<APPLICATION_VERSION>**.bck SHA256

3. Geri yükleme adımlarına geçmeden önce, her dosyanın SHA 256'nın meta veri dosyasında belirtilen SHA 256 ile eşleşip eşleşmediğini kontrol edin. Yedekleme dosyası, komut isteminden gelen sağlama toplamı ile meta veri dosyasındaki sağlama toplamı tamamen aynıysa geri yükleme için geçerlidir. Yalnızca aynıysa geri yükleme adımlarına devam edin.

7.4 Geri Yükleme Adımları:

1. 4Sight sunucusunda Yönetici olarak oturum açın.
2. Postgres Veritabanının çalıştığı port numarasını bulun. <4Sight INSTALLATION DIRECTORY> \ apache-tom- cat \ webapps \ application.properties dosyasında spring.datasource.url özelliğinde bulunabilir. Bu dosyayı açmak için Yönetici olarak çalışan bir Not Defteri kullanın. 4Sight <APPLICATION_VERSION> 'dan hemen önceki sayıdır
3. Postgres kullanıcısını kullanarak Yönetici olarak çalışan bir komut isteminden psql komut yardımcı programına giriş yapın

   "C: \ Program Files \ PostgreSQL \ 11 \ bin \ psql" --port = <DB_PORT> postgres postgres
4. Uygulama tarafından kullanılan veritabanı kullanıcısı, <4Sight INSTALLATION DIRECTORY> \ apache-tom-cat \ webapps \ application.properties dosyasında spring.data- source.username özelliğinde bulunabilir. Bu dosyayı açmak için Yönetici olarak çalışan bir Not Defteri kullanın.
5. Varsa * _temp veritabanlarını silin ve ardından psql komut isteminde aşağıdaki komutları çalıştırarak boş * _temp veritabanlarını oluşturun

   VERİTABANI VARSA "4Sight **<APPLICATION_VERSION>** _temp";
   VERİ TABANI OLUŞTUR "4Sight **<APPLICATION_VERSION>** _temp" ŞABLON şablon0 OWNER İLE " **<DB_USER>** " LC_COLLATE = "C" LC_CTYPE = "C" TABLESPACE = "4Sight_ **<APPLICATION_VERSION>** _4Sight";
   VERİTABANI VARSA "4Sightaudit **<APPLICATION_VERSION>** _temp";
   VERİTABANI OLUŞTUR "4Sightaudit **<APPLICATION_VERSION>** _temp" ŞABLON şablonu0 SAHİBİ " **<DB_USER>** " LC_COLLATE = "C" LC_CTYPE = "C" TABLESPACE = "4Sight_ **<APPLICATION_VERSION>** _4Sightaudit";
   VERİTABANI VARSA "uaa **<APPLICATION_VERSION>** _temp";
   VERİ TABANI OLUŞTUR "uaa **<APPLICATION_VERSION>** _temp" ŞABLON şablon0 OWNER İLE " **<DB_USER>** " LC_COLLATE = "C" LC_CTYPE = "C" TABLESPACE = "4Sight_ **<APPLICATION_VERSION>** _uaa";

   Yukarıdaki 3 veritabanının sahibini bu kullanıcı olarak değiştirin. Kullanıcı adının büyük / küçük harfe duyarlı olduğunu unutmayın.

   ALTER VERİTABANI "4Sight **<APPLICATION_VERSION>** _temp" SAHİBİ " **<DB_USER>** "; ALTER VERİTABANI "4Sightaudit **<APPLICATION_VERSION>** _temp" OWNER TO " **<DB_USER>** "; ALTER VERİTABANI "uaa **<APPLICATION_VERSION>** _temp" OWNER TO " **<DB_USER>** ";
6. Yedeklemelerin metadata.properties dosyalarını kontrol edin ve hangi yedeklemeyi geri yüklemeniz gerektiğine karar verin.
7. Yönetici olarak başka bir komut istemi açın ve dizini yukarıda seçilen yedekleme dosyalarını içeren klasöre değiştirin.

Aşağıdaki komutları kullanarak veritabanını * .bck dosyalarından * _temp veritabanlarına geri yükleyin. Bir şifre istenirse, postgres süper kullanıcısının şifresini girin.

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

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

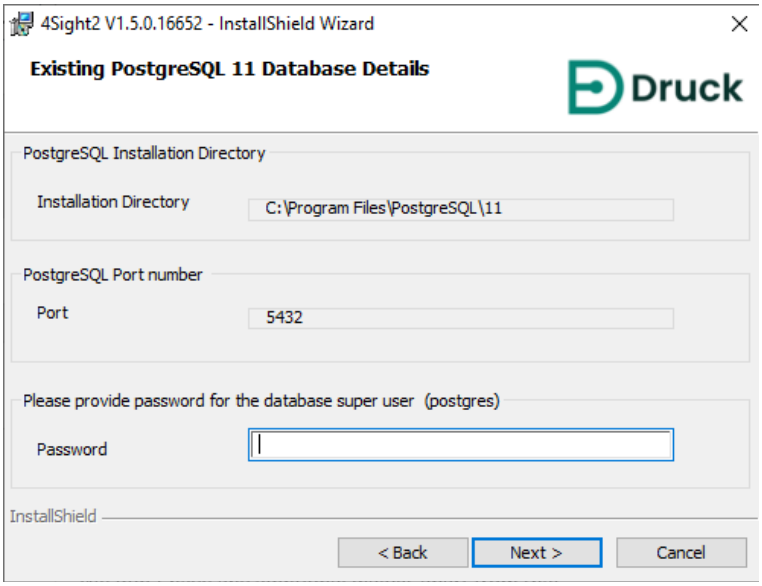
"C: \ Program Files \ PostgreSQL \ 11 \ bin \ pg_restore" --port = **<DB_PORT>** --no-owner -username = postgres --dbname = uaa **<APPLICATION_VERSION>** _temp -n public - role = **<DB_USER >** uaa **<APPLICATION_VERSION>** .bck

8. Varsa, * _old veritabanlarını psql isteminde aşağıdaki komutları çalıştırarak silin.
   VERİTABANI VARSA "4Sight <APPLICATION_VERSION> _old";
   VERİTABANI VARSA "4Sightaudit <APPLICATION_VERSION> _old";
   VERİ TABANI VARSA "uaa <APPLICATION_VERSION> _old";
9. Açıksa, 4Sight hizmetini ve pgadmin uygulamalarını durdurun.
10. psql komut isteminde aşağıdaki komutları çalıştırarak mevcut 4Sight veritabanlarını * _old olarak yeniden adlandırın.
    ALTER VERİTABANI "4Sight <APPLICATION_VERSION>" "4Sight <APPLICATION_VERSION> _old" İÇİN YENİDEN ADLANDIR;
    ALTER VERİTABANI "4Sightaudit <APPLICATION_VERSION>" ŞUNA YENİDEN ADLANDIR;
    "4Sightaudit <APPLICATION_VERSION> _old";
    ALTER VERİTABANI "uaa <APPLICATION_VERSION>" "uaa <APPLICATION_VERSION> _old" olarak YENİDEN ADLANDIR;
11. psql komut isteminde aşağıdaki komutları çalıştırarak * _temp veritabanlarını 4Sight veritabanları olarak yeniden adlandırın.
    ALTER VERİTABANI "4Sight **<APPLICATION_VERSION>** _temp"
    "4Sight **<APPLICATION_VERSION>** " İÇİN YENİDEN ADLANDIR;
    ALTER VERİTABANI "4Sightaudit **<APPLICATION_VERSION>** _temp"
    "4Sightaudit **<APPLICATION_VERSION>** " İÇİN YENİDEN ADLANDIR;
    ALTER VERİTABANI "uaa **<APPLICATION_VERSION>** _temp"
    "uaa **<APPLICATION_VERSION>** " OLARAK YENİDEN ADLANDIR;
12. 4Sight Hizmetini başlatın ve Yönetici olarak oturum açmayı deneyin. Yedeklemeyi alırken Yönetici parolasının şimdi oturum açmak için kullanılması gerektiğini unutmayın.

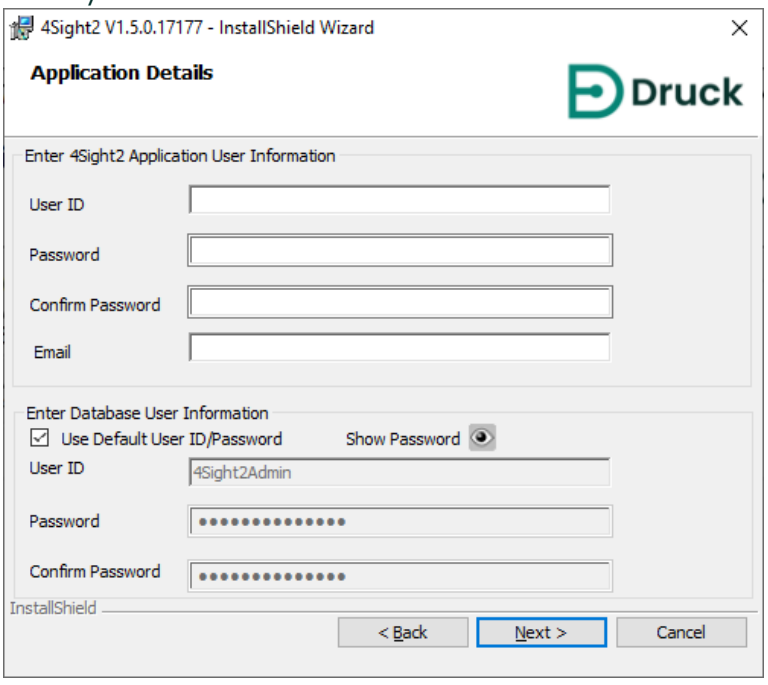
7.5 How to recover from a 4Sight2 Machine Crash?

Varsayımlar: Kullanıcı bilgisayar çökmeden önce 4Sight2 veritabanının yedeğini almıştır. Kullanıcı, hem uygulama hem de veritabanı için kullanıcı adını ve parolayı zaten biliyor.

1. Makineyi, desteklenen İşletim Sistemi ve Sürücüler ile kurun.
2. 4Sight2'yi makineye kurun.
3. Uygulamayı yüklerken, hem uygulama hem de Postgres veritabanı için daha önce verilen kullanıcı adı ve parolanın aynısını girin.



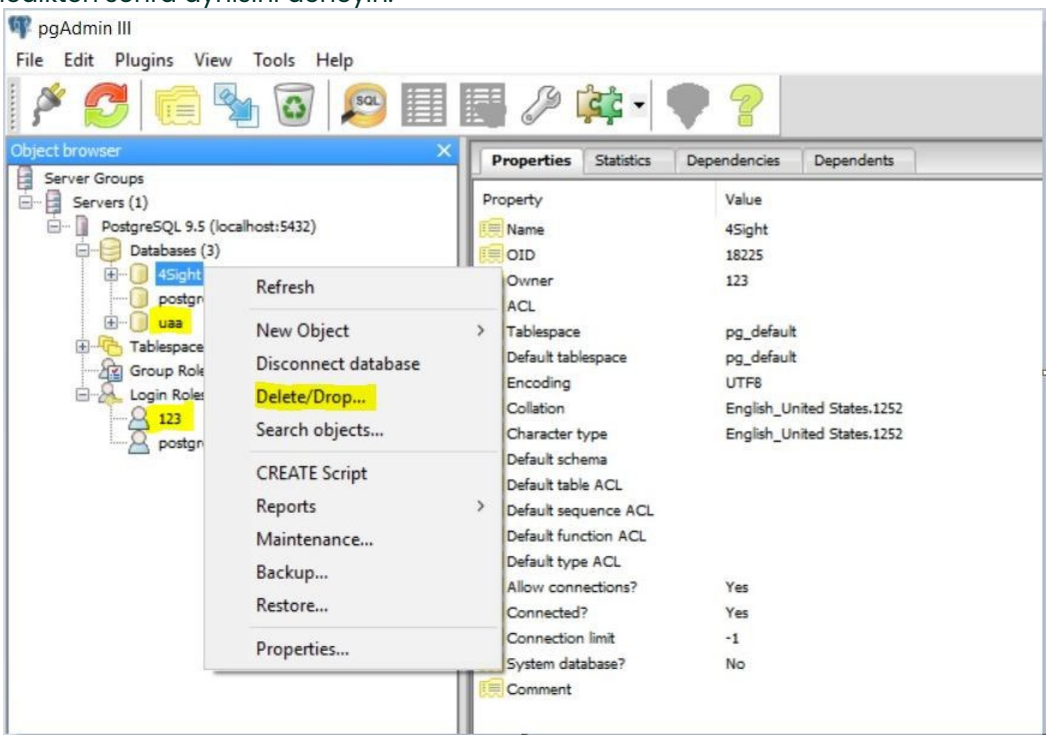
Parola önceki Kurulumla aynıdır



Önceki kurulumda olduğu gibi tüm alanları doldurun

4. Uygulamayı başarıyla yükledikten sonra, pgAdmin'den uygulamayı yüklerken oluşturulan varsayılan veritabanını bırakın (Veritabanına sağ tıklayın ve Sil / Bırak'ı seçin). Eğer alıyorsanız, ver-

itabanı bırakılırken hata oluşmuştur, ardından Postgres hizmetini yeniden başlatın ve yeniledikten sonra aynısını deneyin.



5. Veritabanını ve kullanıcıyı başarıyla bıraktıktan sonra. Veritabanını yukarıda belirtildiği gibi komut isteminden geri yüklemek için bu adımları izleyin.
6. Artık veritabanını başarıyla geri yüklediniz, uygulamayı tarayıcıdan açın ve aynısını inceleyin.

7.6 Kurulum hatası senaryosu:

Aşağıdaki tablo, kurulum sırasındaki çeşitli hata senaryolarını ve bunların çözüm eylemlerini açıklamaktadır.

Error Message	Scenario	Remedy/Action to take
"Insufficient disk space available to install 4Sight2 application. Please ensure a minimum of 4096 MB is available. Free Space : available MB.	Failure due to hard disk size issue (If there is no required space at the start of upgrade)	Admin need to free space in respective drive and then try Upgrade process again.
"Deployment fail while Migrating database"	Failure due to hard disk size issue (If there is not sufficient space after upgrade started successfully)	Admin need to free space in respective drive and then try Upgrade process again.

Error Message	Scenario	Remedy/Action to take
"Installation failed while migrating Database. Please reinstall 4sight2"	Failure due to data Integrity at copy data base	Admin need to contact Customer help desk if this occurs. Data integrity reason captured in logs at location.[C:\Users\[Username]\App Data\Local\Temp\logs]
"Installation failed while migrating Database. Please reinstall 4sight2"	Failure due to data Integrity at schema update stage	Admin need to contact Customer help desk if this occurs. Data integrity reason captured in logs at location.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"	This failure happens If installer unable to get the state of the service"	Admin needs to ensure that 4Sight2 service is up and running
"Failed to start the 4Sight2 service. Please ensure the 4Sight2 service is present and running"	Failure if application corrupted, some files are deleted or port is in use by other application or user has stopped the service etc.	If admin succeed to get the service state and if it is not running for any reason(e.g. application corrupted, some files are deleted or port is in use by other application or user has stopped the service etc.) then system try to start the service. If service is not able to start than admin need to contact customer support to fix the problem.
"Upgrade of 4Sight2 application is supported from version 1.3 onwards. For earlier version upgrade support please contact Customer Care."	Upgrade will not happen if older than 1.3 version is installed.	Upgrade is only possible from 1.3 to higher version.
Installer has detected another minor version of PostgreSQL 11. Installer will not continue. Refer to 4Sight2 Installation manual for more details	4Sight2 cannot continue the 4Sight2 installation as same PostgreSQL version (variant) exists on target machine	Possible options 1. User can choose another machine 2. User backup existing application which is using Postgres version 11.3, un-install and deploy that application on other machine. Un-install Postgres and re-start 4Sight2 Installation
Installation failed while upgrading database. Please reinstall 4Sight2. Refer to 4Sight2 Installation manual for more details	Some internal error might have happened during the upgrade, user can attempt re-install	If problem persists, User can share installation logs for more understanding

Hata mesajı	Senaryo	Çözüm / Yapılacak İşlem
"4Sight2 uygulamasını yüklemek için yetersiz disk alanı. Lütfen en az 4096 MB kullanılabilir olduğundan emin olun. Boş Alan: kullanılabilir MB.''	Sabit disk boyutu sorunu nedeniyle hata (Yükseltmenin başlangıcında gerekli alan yoksa)	Yöneticinin ilgili sürücüde alan boşaltması ve ardından Yükseltme işlemini tekrar denemesi gerekir.
"Veritabanı taşınırken dağıtım başarısız"	Başarısızlık nedeniyle e tmek zor diski boyutu sorunu (yükseltme başarıyla başladıktan sonra yeterli alan yoksa)	Yöneticinin ilgili sürücüde alan boşaltması ve ardından Yükseltme işlemini tekrar denemesi gerekir.
"Veritabanı taşınırken yükleme başarısız oldu. Lütfen 4sight2'yi yeniden yükleyin"	Kopyalama veri tabanındaki veri bütünlüğünden kaynaklanan arıza	Böyle bir durumda yöneticinin Müşteri yardım masasıyla iletişime geçmesi gerekir. Konumdaki günlüklerde yakalanan veri bütünlüğü nedeni. [C: \ Kullanıcılar \ [Kullanıcı Adı] \ Uygulama Verileri \ Yerel \ Temp \ günlükler]
"Veritabanı taşınırken yükleme başarısız oldu. Lütfen 4sight2'yi yeniden yükleyin"	Şema güncelleme aşamasında veri bütünlüğü nedeniyle hata	Böyle bir durumda yöneticinin Müşteri yardım masasıyla iletişime geçmesi gerekir. Konumdaki günlüklerde yakalanan veri bütünlüğü nedeni C: \ Program Files \ Druck \ 4Sight2 \ <<latest folder number>> \ logs
"Mevcut 4Sight2 hizmeti bulunamadı. Lütfen mevcut 4Sight2 sürümünün bu makineye yüklendiğinden ve hizmetin çalıştığından emin olun "	''Bu hata, Yükleyici hizmetin durumunu alamazsa gerçekleşir "	Yöneticinin 4Sight2 hizmetinin çalışır durumda olduğundan emin olması gerekir
" 4Sight2 hizmeti başlatılamadı. Lütfen 4Sight2 hizmetinin mevcut ve çalışır durumda olduğundan emin olun "	Uygulama bozulmuşsa, bazı dosyalar silinmişse veya bağlantı noktası başka bir uygulama tarafından kullanılıyorsa veya kullanıcı hizmeti durdurmuşsa vb.	Yönetici hizmet durumunu almayı başarırsa ve herhangi bir nedenle çalışmıyorsa (örneğin, uygulama bozulmuşsa, bazı dosyalar silinmiş veya bağlantı noktası başka bir uygulama tarafından kullanılıyor veya kullanıcı hizmeti durdurmuşsa vb.), Sistem başlatmaya çalışır. Hizmet başlatılamıyorsa, yöneticinin sorunu çözmek için müşteri desteğiyle iletişime geçmesi gerekir.

"4Sight2 uygulamasının yükseltilmesi sürüm 1.3'ten itibaren desteklenmektedir. Daha eski sürüm yükseltme desteği için lütfen Müşteri Hizmetleri ile iletişime geçin."	1.3 sürümünden daha eski bir sürüm kurulursa yükseltme yapılmaz.	Yükseltme yalnızca 1.3'ten daha yüksek sürüme mümkündür.
Yükleyici, PostgreSQL 11'in başka bir küçük sürümünü tespit etti. Yükleyici devam etmeyecek. Daha fazla ayrıntı için 4Sight2 Kurulum kılavuzuna bakın	4Sight2, aynı PostgreSQL sürümü (varyantı) hedef makinede mevcut olduğu için 4Sight2 kurulumuna devam edemez	Olası seçenekler 1. Kullanıcı başka bir makine seçebilir 2. Kullanıcı, Postgres 11.3 sürümünü kullanan mevcut uygulamayı yedekleyin, bu uygulamayı kaldırın ve başka bir makineye dağıtın. Postgres'i kaldırın ve 4Sight2 Kurulumunu yeniden başlatın
Veritabanı yükseltilirken kurulum başarısız oldu. Lütfen 4Sight2'yi yeniden yükleyin. Daha fazla ayrıntı için 4Sight2 Kurulum kılavuzuna bakın	Yükseltme sırasında bazı dahili hatalar olmuş olabilir, kullanıcı yeniden yüklemeyi deneyebilir	Sorun devam ederse, Kullanıcı daha fazla anlamak için kurulum günlüklerini paylaşabilir

7.7 Genel Hata Nedenleri

Aşağıda, USB aracılığıyla Druck ekipmanları ve 4sight2 arasındaki iletişimle ilişkili yaygın olarak görülen sorunlar bulunmaktadır.

- Fiziksel bağlantı gevşek veya titriyor
- Aşınmış kablolar / bağlantı noktaları
- Düşük kaliteli USB adaptörleri
- Aşırı yüklenmiş USB adaptörleri / bağlantı noktaları
- Cihazlar uzun süre çalışmaya devam etmeleri hazırda bekletme veya uyku moduna geçmelerine neden olur
- İletişim modunda olmayan cihazlar
- Sürücü yazılımı yüklenmemiş veya yükseltilmemiş. Donanımla iletişim kurmak için 4Sight2 uygulamasının aynı sürümüne ve sürücülere ihtiyacınız vardır.
- Cihazların çok eski ürün yazılımı sürümleri vardır.

7.8 4Sight2 Uygulamasını Kaldırma

4Sight2'nin yeni bir kopyasının, 4Sight2'nin yeni bir sürümünün yüklenmesine ihtiyacınız varsa veya yükleme sırasında meydana gelen sorunlar nedeniyle 4Sight2'yi kaldırmanız gerekiyorsa bu talimatları izleyin.

PostgreSQL veritabanı bileşeninin kaldırılması 4Sight2 veritabanını silerek veri kaybına neden olur. Aşağıdaki adımlar otomatik olarak bir yedekleme oluşturulmayacaktır, bu nedenle devam etmeden önce manuel bir yedekleme oluşturduğunuzdan ve bu yedeği 4Sight2 kurulum klasörüne alternatif bir konuma kaydettiğinizden emin olun. Bu kılavuzun Postgres Veritabanı yedekleme ve geri yükleme bölümüne bakın.

Yalnızca 4Sight2 uygulamasını kaldırmayı ve veritabanını saklamayı seçerseniz, lütfen bu kılavuzun 4Sight2 kurulum bölümüne bakın. Yeniden kurulum sırasında veritabanı super user için kimlik bilgilerine ihtiyacınız olacak. Bu kimlik bilgilerini bilmiyorsanız, kaldırma işlemini gerçekleştirmeye çalışmayın.

Veritabanını kaldırmadan 4Sight2 sürümünüzü yükseltmek isterseniz, lütfen bu talimatları TAKİP ETMEYİN.

1. Kontrol Paneli >> Programlar ve Özellikler gidin.
2. 4Sight2'ye sağ tıklayın ve Kaldır'ı seçin.
3. Kaldırma sihirbazındaki talimatları izleyin
4. PostgreSQL 11'e sağ tıklayın ve Kaldır'ı seçin.
5. Kaldırma sihirbazındaki talimatları izleyin.
6. PostgreSQL'in kaldırılması veri klasörünü silmez. Bunu elle yapmanız gerekiyor . C: \ Program Files \ PostgreSQL \ 11 \ adresinde bulunan veri klasörünü silin.
   a. PostgreSQL klasörünün tamamını silmek isterseniz, devam etmeden önce tüm yedekleme dosyalarının, komut dosyalarının bin klasöründen taşındığından emin olun.
   b. Varsayılan olarak 4Sight2 veritabanı yedekleri şu konumda oluşturulur ve kaydedilir: C: \ Program Files \ PostgreSQL \ 11 \ bin
7. Mümkünse bilgisayarı yeniden başlatmanız önerilir.
8. 4Sight2 artık başarıyla kaldırılmıştır.

7.9 Güvenli İletişim Sorunu Giderme

1. Komut 'command name' dahili veya harici bir komut olarak tanınmıyor. Örneğin, 'key- tool' dahili veya harici bir komut olarak tanınmaz,

- Bunun gibi bir hata alırsanız, yani içinde bulunduğunuz geçerli klasörde, komut istemi belirtilen komuta referans bulamaz.

Bu hatayı çözmek için, doğru klasöre işaret etmek için aşağıdaki komutu kullanın. **Path=%Path%;"<<full path of the location where the command is>>".** Örnek, anahtar araçla ilgili yukarıdaki hatada yolu aşağıya ayarlamanız gerekir, **"Path=%Path%;C: \ Program Files \ Druck \ 4Sight2 \ <<latest folder number>> \ jre \ bin"**

2. Kötü IP adresi

- Bu metinde bir hata mesajı alırsanız, bu, openssl-ca.cnf veya openssl-server.cnf dosyalarındaki IP Adresinin veya Ana Bilgisayar Adının yanlış olduğu anlamına gelir. Not: Bu dosyalarda birden çok yerde bunu düzeltmeniz ve adımları yeniden uygulamanız gerekebilir.

3. Böyle bir dosya veya dizin yok

- Bu metinle birlikte bir hata mesajı alırsanız, bu, muhtemelen çalıştırdığınız komutun doğru olmayan bir dosya adına başvurduğu anlamına gelir. Herhangi bir dosya adı hatası olup olmadığını kontrol edin ve klasörde o isimdeki dosyanın bulunup bulunmadığını da kontrol edin ve komutları yeniden çalıştırın. Eksik dosyaları oluşturmak için komuttaki dosya adını düzeltmeniz veya adımları izlemeniz gerekebilir.
- Bu hata, index.txt ve serial.txt dosyalarında ortaya çıkabilir, çünkü bazı durumlarda dosya uzantısı isme iki kez eklenir, örn. intex.txt.txt. Dosyayı düzenleyin ve .txt uzantısı olmadan kaydedin. Dosyanın bir .txt uzantısına sahip olduğundan emin olun.

En İyi Uygulamalar

8. En İyi Uygulamalar

Sunucu Sağlamlaştırma

Sunucu ortamı, Microsoft veya CIS yönergelerine göre sağlamlaştırılmalıdır.

8.1 Tomcat

- Tomcat'i yalnızca yönetici veya LocalService'in C: \ Program Dosyaları (x86) gibi erişime sahip olduğu güvenli klasöre yükleyin
- Tomcat'i LocalService hesabında çalışan bir hizmet olarak kurun.
- WebApp'tan her şeyi kaldırın, varsayılan istenmeyen uygulamaları kaldırın.
- 404, 403, 500 vb. Gibi Varsayılan hata sayfasını değiştirin
- HTTPS'yi zorunlu kılın, SSL'yi etkinleştirin.
- Yönetim uygulaması SSL üzerinde çalışmalıdır.
- Her web uygulaması için kullanıcıya özel günlük dosyası.
- Sunucu başlığını kaldırın.
- Erişim günlüğünü etkinleştirin.
- Kapatma portunu ve komutunu değiştirin.

8.2 PostgreSQL

- pgdba, postgres, depesz gibi tüm yüksek ayrıcalıklı hesaplara yalnızca yerel oturum açma izni verilmelidir.
- Doğru kullanıcıların doğru erişime sahip olması için pg-hba.conf dosyasındaki sıranın doğru olduğundan emin olun
- pg-hba.conf dosyasını, sunucunun ağ üzerinden değil, yalnızca yerel makineden bağlanabileceği şekilde yapılandırın.

8.3 En İyi Güvenlik Duvarı Uygulamaları

4Sight2 ile kullanılması önerilen en iyi güvenlik duvarı uygulamalarından bazıları şunlardır:

8.3.1 Politika

1. Güvenlik duvarı yapılandırması, Organization Security Policy ile tutarlı olmalıdır.
2. Her zaman Least privilege policy'i kullanın. Varsayılan olarak tümünü reddedin. Belirli trafiğe izin verin traffic (using source, desti- nation and port).
3. Önce belirli kuralları yerleştirin ve açık bırakma kuralları kullanın.
4. Tüm eylemleri, özellikle denetim izi için başarısızlık girişimlerini günlüğe kaydedin

8.3.2 Kaynaklar

1. Bellek kullanımını izleyin
2. CPU kullanımını izleyin
3. Bant genişliği kullanımını izleyin
4. Güvenlik Duvarı makinesinde çalışan uygulama sayısını sınırlayın

8.3.3 Kurulum ve Bakım

1. Güvenlik duvarı makinesine Fiziksel Erişimi sınırlayın
2. Yönetim için benzersiz kullanıcı kimliği kullanın
3. Makinedeki katı hesap politikasına uyun
4. İşletim sistemlerini, uygulama yazılımlarını, aygıt yazılımlarını vb. düzenli olarak yamalayın.
5. Kural tabanını, yapılandırmayı ve günlükleri düzenli olarak arşivleyin. Bir kaynak kontrolünde yapılan tüm kuralları ve değişiklikleri belgeleyin.
6. Düzenli testler yapın.
7. Hizmet devre dışı bırakıldığında kullanılmayan kuralı kaldırın.
8. Kuralları düzenli olarak denetleyin ve gözden geçirin.
9. Düzenli olarak izleme güvenlik önerileri

8.3.4 Ek Güvenlik

1. Durum denetimlerini kullanın.
2. Vekilleri Kullanın
3. Uygulama düzeyinde inceleme ve filtrelemeyi kullanın.

8.3.5 Dahili Koruma

1. Kabul edilebilir kullanım politikasına sahip olun
2. Her kullanıcı için kişisel güvenlik duvarı
3. Host tabanlı saldırı önleme
4. Ağ İzleme
5. İçerik Filtreleme
6. Her bilgisayarda ve uygulamada Erişim Kontrolü.

Ofis Lokasyonları

Merkez
Leicester, İngiltere
Phone: +44 (0) 116 2317233
Email: gb.sensing.sales@bakerhughes.com

Çin
Guangzhou
Phone: +86 173 1081 7703
Email: dehou.zhang@bakerhughes.com

Almanya
Frankfurt
Phone: +49 (0) 69-22222-973
Email: sensing.de.cc@bakerhughes.com

Avustralya
Springfield Central
Phone: +61 414191649

Çin
Shanghai
Phone +86 135 6492 6586
Email: hensen.zhang@bakerhughes.com

Hindistan
Bangalore
Phone: +91 9986024426
Email: aneesh.madhav@bakerhughes.com

Çin
Beijing
Phone: +86 180 1929 3751
Email: fan.kai@bakerhughes.com

Fransa
Toulouse
Phone: +33 562 888 250
Email: sensing.FR.cc@bakerhughes.com

İtalya
Milano
Phone: +39 02 36 04 28 42
Email: csd.italia@bakerhughes.com

Japonya
Tokyo
Phone: +81 3 6890 4538
Email: gesitj@bakerhughes.com

Hollanda
Hoevelaken
Phone: +31 334678950
Email: nl.sensing.sales@bakerhughes.com

Rusya
Moskova
Phone: +7 915 3161487
Email: aleksey.khamov@bakerhughes.com

BAE
Abu Dhabi
Phone: +971 528007351
Email:suhel.aboobacker@bakerhughes.com

ABD
Boston
Phone: 1–800-833-9438
Email: ccpressureusa@bakerhughes.com

Servis ve Teknik Destek Lokasyonları

Teknik Destek
Global
Email: drucktechsupport@bakerhughes.com

Brezilya
Campinas
Phone: +55 11 3958 0098, +55 19 2104 6983
Email: mcs.services@bakerhughes.com

Çin
Changzhou
Phone: +86 400 818 1099
Email: service.mcchina@bakerhughes.com

Fransa
Toulouse
Phone: +33 562 888 250
Email: sensing.FR.cc@bakerhughes.com

Hindistan
Pune
Phone: +91 213 5620426
Email: mcsindia.inhouseservice@bakerhughes.com

Japonya
Tokyo
Phone: +81 3 3531 8711
Email: service.druck.jp@bakerhughes.com

BAE
Abu Dhabi
Phone: +971 2 4079381
Email: gulfservices@bakerhughes.com

İngiltere
Leicester
Phone: +44 (0) 116 2317107
Email: sensing.grobycc@bakerhughes.com

ABD
Billerica
Phone: +1 (281) 542-3650
Email: namservice@bakerhughes.com

123M3140 Düzeltme F | Türkçe

Baker Hughes