



4Sight2

**Software di gestione della
calibrazione**

Manuale di installazione 123M3140 Revisione F

Sommario

1. Introduzione	1
1.1 Destinatari	1
1.1.1 Amministratori	1
1.1.2 Supervisore	1
1.1.3 Tecnici	1
1.1.4 Auditor	1
2. Requisiti di sistema	2
2.1 Application Server	2
2.2 Workstation client	2
2.3 Installazione locale	2
2.4 Firmware 4Sight2 supportato	3
3. Installazione di 4Sight2	5
3.1 Installazione del database	7
3.2 Installazione di PostgreSQL	7
4. Installazione del comunicatore dell'apparecchiatura di prova di 4Sight2	15
4.1 Configurazione manuale dei driver	20
4.1.1 Prerequisiti	20
4.2 Prova del comunicatore dell'apparecchiatura di prova	24
4.3 Configurazione del driver del calibratore di temperatura	25
5. Guida all'implementazione	27
5.1 Architettura di implementazione	27
5.2 Implementazione fisica	27
5.3 Rete	27
5.4 Sequenza di implementazione	27
5.5 Attività post-implementazione	28
5.5.1 Aggiunta di utenti e gruppi	28
5.5.2 Password predefinite	28
5.5.3 Comunicazioni protette	28
6. Domande frequenti sull'installazione di 4Sight2	44
6.1 Impostazione e installazione	44
6.2 Domande frequenti sul comunicatore dell'apparecchiatura di prova	45
7. Risoluzione dei problemi di installazione	48
7.1 Problemi di comunicazione dell'apparecchiatura di prova	48
7.2 Backup del database Postgres	48
7.3 Ripristino del database Postgres	48
7.4 Procedura per il ripristino	50
7.5 Procedura di ripristino in seguito a un arresto anomalo di un computer 4Sight2	51
7.6 Installazione non riuscita	53
7.7 Cause generali di errore	55
7.8 Disinstallazione di 4Sight2	56
7.9 Risoluzione dei problemi per le comunicazioni protette	56

8. Procedure consigliate.....	59
8.1 Tomcat	59
8.2 PostgreSQL.....	59
8.3 Procedure consigliate per i firewall	59
8.3.1 Policy.....	59
8.3.2 Risorse	59
8.3.3 Installazione e manutenzione.....	60
8.3.4 Sicurezza avanzata	60
8.3.5 Protezione interna	60

1. Introduzione

Il software di calibrazione 4Sight2 è uno strumento di gestione della calibrazione basato sul Web che aiuta a mantenere e controllare l'ambiente di calibrazione ai massimi standard di metrologia. Il software può essere utilizzato per:

- Gestire la calibrazione di tutti i dispositivi di misura per una sede aziendale specificata
- Impostare un programma dei lavori di calibrazione per i tecnici
- Caricare e scaricare dati in e da calibratori portatili Druck (DPI620 Genii, DPI611 e DPI612) che dispongono di funzione di comunicazione USB
- Gestire i record di calibrazione per i dispositivi che non sono supportati da un calibratore portatile (immissione manuale dei dati)
- Ispezionare i propri record della cronologia delle calibrazioni. È inoltre possibile creare un record permanente di ciascun certificato di calibrazione. Ad esempio: per procedure di controllo qualità ISO 9000.
- Controllare le calibrazioni automatiche utilizzando controllori di pressione Druck (PACE 1000, 5000 e 6000), calibratori portatili (DPI620 Genii, DPI611 e DPI612) e calibratori di temperatura (DryTC165, DryTC 650, LiquidTC165 e LiquidTC255)

1.1 Destinatari

1.1.1 Amministratori

Gli amministratori sono responsabili dell'installazione e della configurazione del software 4Sight2. Dopo l'installazione iniziale di 4Sight2 è disponibile un singolo account amministrativo. Da tale account è possibile creare nuovi utenti e assegnare gruppi e serie di autorizzazioni. Gli utenti amministrativi hanno accesso in lettura e scrittura a tutte le funzioni di 4Sight2.

1.1.2 Supervisore

Un supervisore è responsabile della gestione di asset e calibrazione. Può creare e aggiornare asset in 4Sight2 Enterprise, compresi impianti, ubicazioni, tag e dispositivi. È responsabile del collegamento di documenti ad asset, quali processi di impianto e schede tecniche dei dispositivi. I supervisori possono creare procedure di prova da utilizzare durante la calibrazione, nonché programmare procedure e monitorare lo stato dei dispositivi. I supervisori dispongono delle autorizzazioni necessarie per approvare le calibrazioni.

1.1.3 Tecnici

I tecnici sono responsabili dell'esecuzione delle calibrazioni. Le calibrazioni possono essere portatili, manuali o automatiche. Il tecnico deve effettuare il tipo di calibrazione adeguato per il dispositivo. Dopo avere effettuato la calibrazione, i tecnici possono esaminare i risultati e completare le calibrazioni, in modo che successivamente siano approvate da un supervisore.

1.1.4 Auditor

Un auditor è responsabile dell'ispezione dei rapporti. Per alcuni impianti la verifica rappresenta un requisito normativo obbligatorio.

2. Requisiti di sistema

I requisiti minimi del sistema per installare l'applicazione 4Sight2 su computer server e client sono i seguenti:

2.1 Application Server

Sistema operativo	Windows 10, Windows Server 2012 R2, Windows Server 2016, Windows Server 2019
Aggiornamenti	Tutti gli aggiornamenti Windows installati
Processore	Quad Core
RAM	8 GB o superiore (consigliati 32 GB)
Spazio su disco	1 TB
Velocità di rete	10 Mbps

2.2 Workstation client

Sistema operativo	Windows 10, Windows Server 2012 R2, Windows Server 2016, Windows Server 2019
Browser	Google Chrome V80+, Microsoft Edge V80, Firefox V74
Adobe Reader	Adobe Acrobat Reader DC Versione 2015.017.20050 o successiva
RAM	8 GB o maggiore
Processore	Dual Core
Spazio su disco	600 GB
Velocità di rete	10 Mbps

2.3 Installazione locale

Sistema operativo	Windows 10, Windows Server 2012 R2, Windows Server 2016, Windows Server 2019
Aggiornamenti	Tutti gli aggiornamenti Windows installati
Adobe Reader	Adobe Acrobat Reader DC Versione 2015.017.20050 o successiva
Processore	Dual Core
RAM	Min. 16 GB (consigliati 32 GB)
Spazio su disco	Min. 500 GB di spazio su disco
Browser	Google Chrome V80+, Microsoft Edge V80, Firefox V74

2.4 Firmware 4Sight2 supportato

Per le informazioni più recenti sul firmware supportato, fare riferimento al collegamento seguente:

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

o



Per PACE, inserire l'USB B per la comunicazione 4Sight2 come indicato nell'immagine sottostante:



Installazione di 4Sight2

3. Installazione di 4Sight2

Per installare 4Sight2, in primo luogo copiare il file zip di installazione di 4Sight2 nel desktop ed estrarre i file in esso contenuti. Dal file di installazione, selezionare il file eseguibile di 4Sight2.

Nota: per la scansione delle installazioni di 4Sight2 e Comm Server, vengono utilizzati i seguenti software antivirus:

- McAfee VirusScan Enterprise + AntiSpyware Enterprise numero di versione: 8.8.0
- Symantec Endpoint Protection numero di versione: 14.3.558

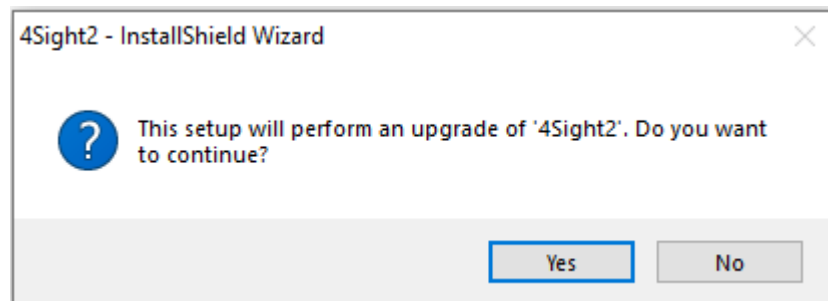


Una volta lanciato l'eseguibile di installazione, verrà avviata l'installazione guidata InstallShield. L'installazione guidata InstallShield contiene due passaggi della procedura di installazione di 4Sight2:

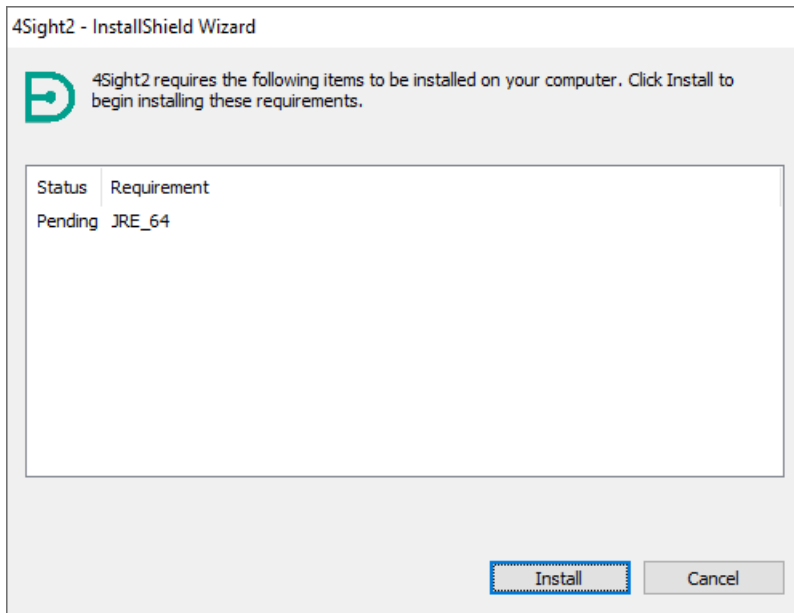
1. Installazione del database
2. Installazione dell'applicazione Web

Per procedere nell'installazione, attenersi alle istruzioni del programma di installazione guidata InstallShield o nelle due sezioni riportate di seguito.

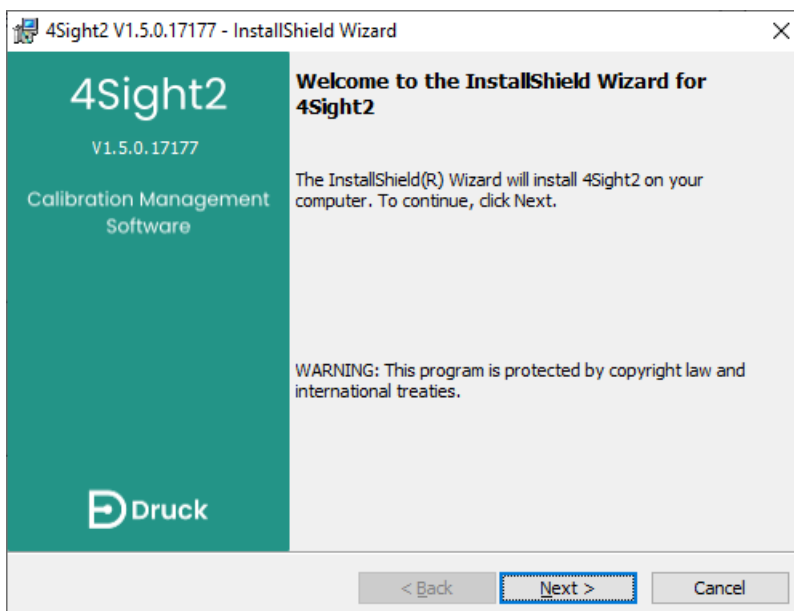
1. Se 4Sight2 è già installato nel computer, la procedura guidata di installazione richiede di effettuare un aggiornamento a una versione recente. Fare clic su **Si** per effettuare l'aggiornamento.



2. Se 4Sight2 viene installato per la prima volta sul computer, la procedura guidata visualizza la schermata riportata di seguito. Selezionando **Installa** vengono installati gli elementi visualizzati.



3. Al completamento dell'installazione dei prerequisiti, viene visualizzata la schermata iniziale della procedura guidata di installazione InstallShield. Fare clic su **Avanti** per proseguire.



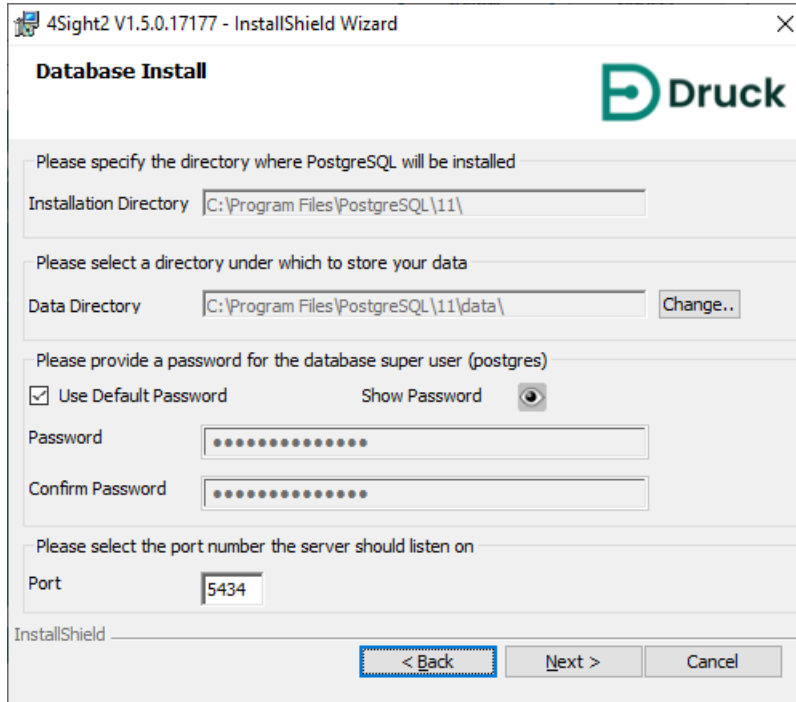
3.1 Installazione del database

L'applicazione 4Sight2 utilizza un database PostgreSQL. Di seguito vengono fornite le istruzioni relative alla procedura di installazione del database PostgreSQL e alla procedura da seguire nel caso in cui il database PostgreSQL fosse già installato.

3.2 Installazione di PostgreSQL

Se sul computer non è installato alcun database PostgreSQL, attenersi alla seguente procedura.

1. Se sul computer non sono installate istanze del database PostgreSQL, viene visualizzata la schermata riportata di seguito.



Directory di installazione: selezionare la directory in cui è possibile installare l'applicazione PostgreSQL.

Directory dati: selezionare la directory in cui è possibile salvare il database PostgreSQL.

Password/Conferma password: immettere la password dell'utente con privilegi avanzati del database PostgreSQL. Viene richiesta solo al momento della prima installazione del database PostgreSQL.

Nota: questa password sarà necessaria per accedere al contenuto del database al termine dell'installazione.

Porta: indirizzo della porta del database PostgreSQL per soddisfare la richiesta dell'applicazione.

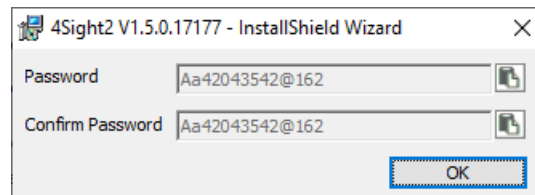
Nota: se il numero di porta è già occupato, rivolgersi all'assistenza IT. Gli utenti possono anche cambiare il numero di porta, che deve essere annotato per avviare l'applicazione in un secondo momento.



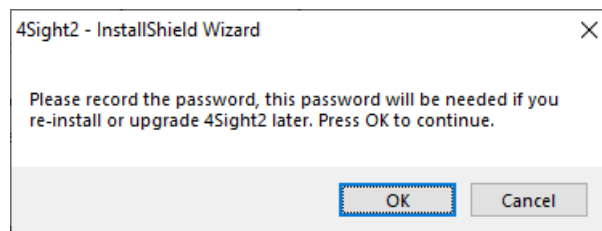
Importante: l'utente deve annotare la password del database. La perdita delle informazioni sulla password può causare un accesso negato o la perdita di dati. Deselezionare la casella di controllo Password utente predefinita per aggiornare la password dell'utente con privilegi avanzati per il database. Se si desidera mantenere la password predefinita o visualizzare la nuova password immessa, selezionare l'icona

(Mostra password). Per copiare la password negli appunti, utilizzare l'icona

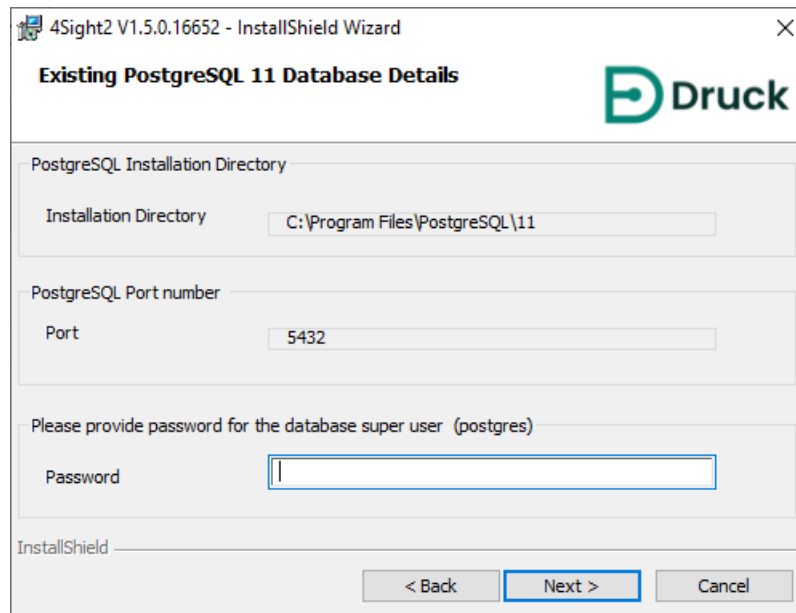
(Copia negli appunti).



Il programma di installazione richiede quindi di registrare nuovamente la password. Dopo avere annotato la password, selezionare **OK**.



2. Questa fase viene visualizzata all'utente solo nel caso in cui il database PostgreSQL sia già installato.



4Sight2 V1.5.0.16652 - InstallShield Wizard

Existing PostgreSQL 11 Database Details

PostgreSQL Installation Directory

Installation Directory

PostgreSQL Port number

Port

Please provide password for the database super user (postgres)

Password

InstallShield

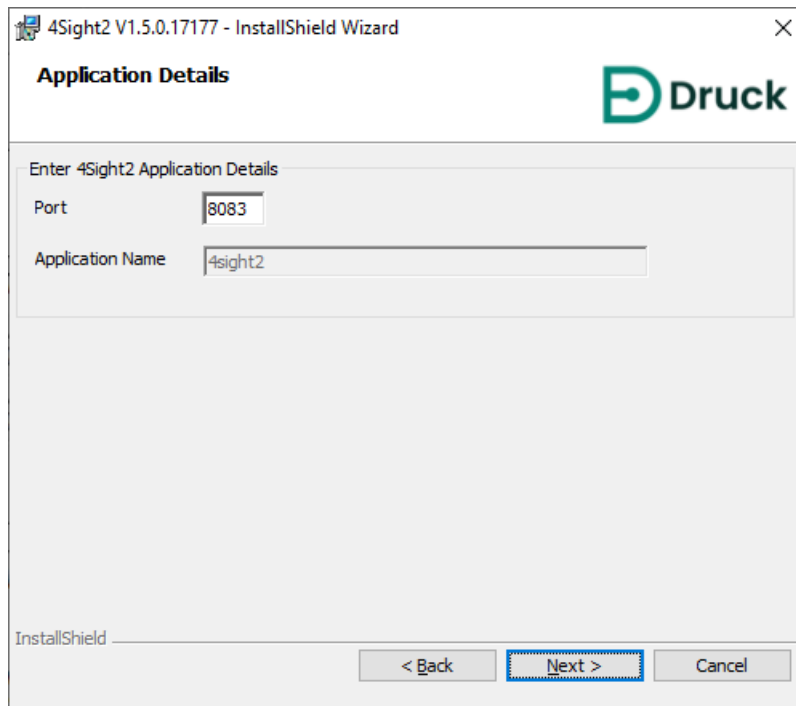
< Back Next > Cancel

Directory di installazione: indica il percorso in cui è installato PostgreSQL. Si tratta di informazioni di sola lettura.

Password: consente di confermare la password dell'utente con privilegi avanzati del database PostgreSQL.

Porta: consente di specificare il numero di porta in uso dal database PostgreSQL per eseguire la richiesta del database.

3. Nella finestra Dettagli dell'applicazione, inserire i dettagli indicati di seguito



Porta: immettere la porta del server Web Tomcat utilizzata dall'applicazione Web 4Sight2 per rispondere alla richiesta HTTP.

Nome applicazione: immettere il percorso del contesto applicativo che si utilizzerà per connettersi all'applicazione 4Sight2 nel browser in uso. Per impostazione predefinita è 4sight2. Nota: se il numero di porta è già occupato, rivolgersi all'assistenza IT. Gli utenti possono anche cambiare il numero di porta, che deve essere annotato per avviare l'applicazione in un secondo momento.

4. Selezionando **Avanti** viene visualizzata la schermata Informazioni sull'utente dell'applicazione.

Informazioni sull'utente dell'applicazione: in questa sezione vengono inseriti il nome dell'utente con privilegi avanzati e la password per accedere all'applicazione 4Sight2.

Nota: questa password sarà necessaria per accedere all'applicazione 4Sight2 quando viene installata.

Informazioni sull'utente del database: in questa sezione vengono inseriti il nome e la password dell'utente del database che verranno utilizzati dall'applicazione 4Sight2 per comunicare con il database PostgreSQL.

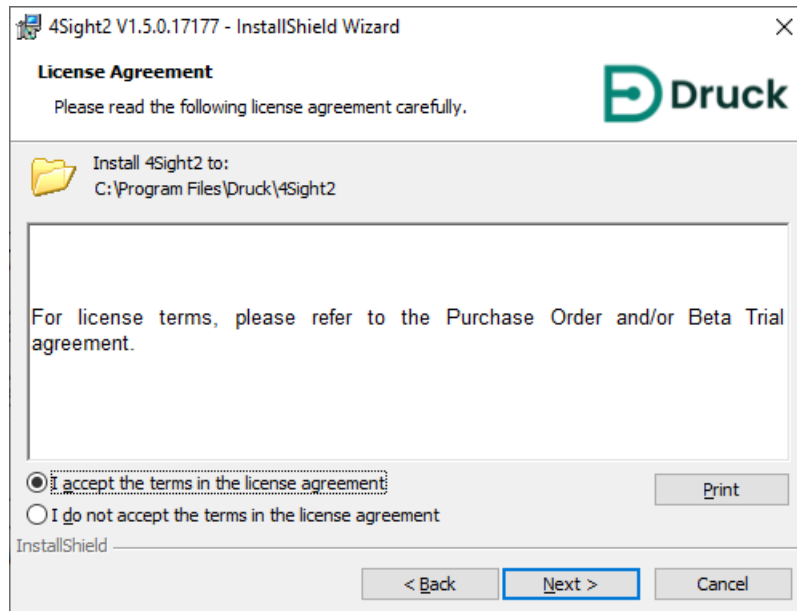


Importante: l'utente deve annotare la password del database. La perdita delle informazioni sulla password può causare un accesso negato o la perdita di dati. Deselezionare la casella di controllo Password utente predefinita per aggiornare la password dell'utente con privilegi avanzati per il database. Se si desidera mantenere la password predefinita o visualizzare la nuova password immessa, selezionare l'icona

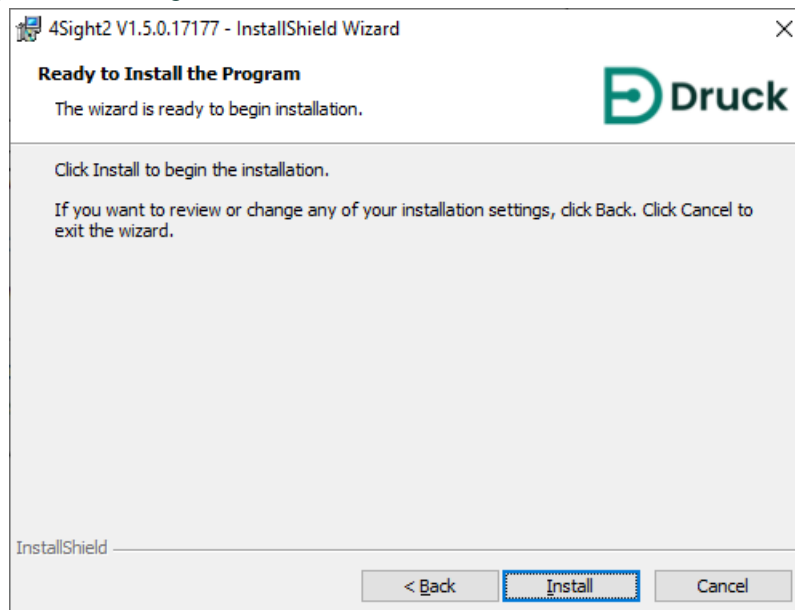
 (Mostra password). Per copiare la password negli appunti, utilizzare l'icona

 (Copia negli appunti).

- Dopo avere letto i termini e le condizioni della licenza, selezionare il pulsante di opzione "Accetto i termini e le condizioni di licenza" e fare clic su **Avanti**.

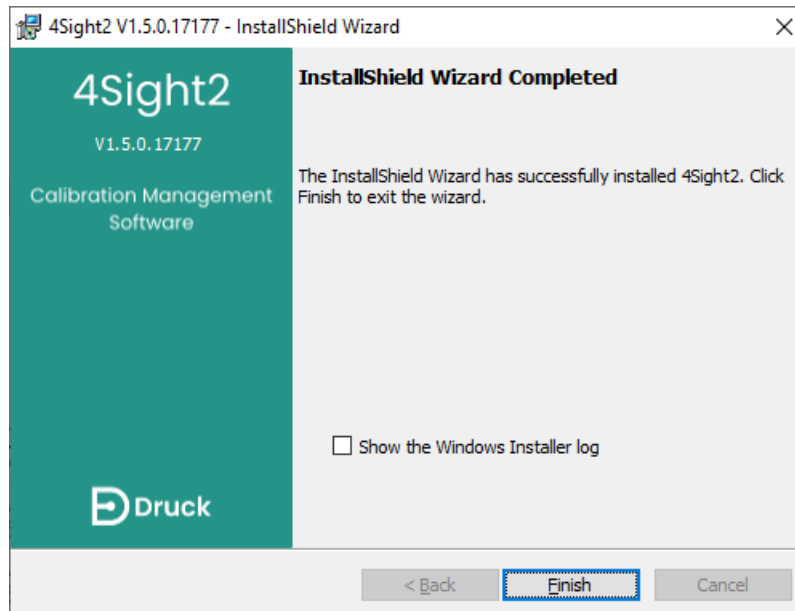


- Fare clic su **Installa** per avviare l'installazione. Verranno installati tutti i pacchetti software relativi all'applicazione 4Sight2 e il database.



Congratulazioni, l'applicazione 4Sight2 è stata configurata.

- Fare clic sul pulsante **Fine** per chiudere la finestra e seguire le istruzioni riportate nella sezione successiva per accedere all'applicazione 4Sight2.



Per accedere a 4Sight2 sul server in modalità locale, portarsi in `http://ComputerName` o `IPAddress:PortNo/ApplicationName`

- **ComputerName:** il nome del PC sul quale è stata installata l'applicazione 4Sight2. Può essere individuato facendo clic con il pulsante destro del mouse sul PC e selezionando Proprietà.
- **IPAddress:** l'indirizzo IP del PC in cui è stata installata l'applicazione 4Sight2. Può essere individuato eseguendo "ipconfig" in una finestra di comando Windows.
- **PortNo:** il numero immesso nel campo Numero porta Tomcat durante l'installazione dell'applicazione.
- **ApplicationName:** il nome immesso nel campo Nome applicazione durante l'installazione dell'applicazione.

Installazione del comunicatore dell'apparecchiatura di prova di 4Sight2

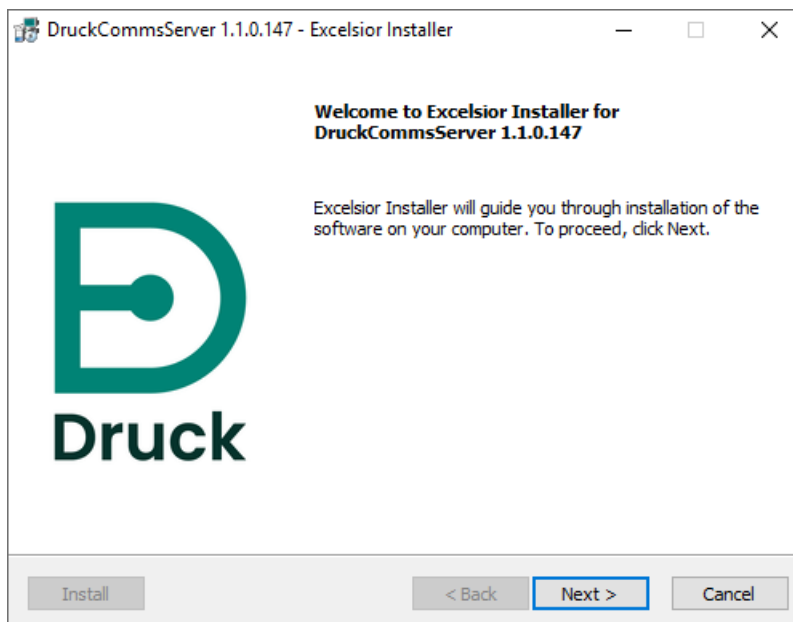
4. Installazione del comunicatore dell'apparecchiatura di prova di 4Sight2

1. Il comunicatore dell'apparecchiatura di prova fornisce agli strumenti Druck i mezzi per comunicare con l'applicazione 4Sight2. Il comunicatore dell'apparecchiatura di prova può essere installato dalla cartella di configurazione di 4Sight2 o può essere scaricato mediante la comunicazione di dispositivi iniziale di 4Sight2. Se il comunicatore dell'apparecchiatura di prova non è disponibile nel file di configurazione, quando l'applicazione 4Sight2 è in esecuzione ed è stato creato un range, portarsi in Calibrazione > Portatile utilizzando il menu di 4Sight2 come utente amministrativo. Per la guida sulla navigazione e la creazione di range, consultare il manuale utente di 4Sight2. Selezionare il pulsante di aggiornamento accanto al menu a discesa delle apparecchiature di prova. Se il comunicatore dell'apparecchiatura di prova non è in esecuzione, viene visualizzato il messaggio di seguito:

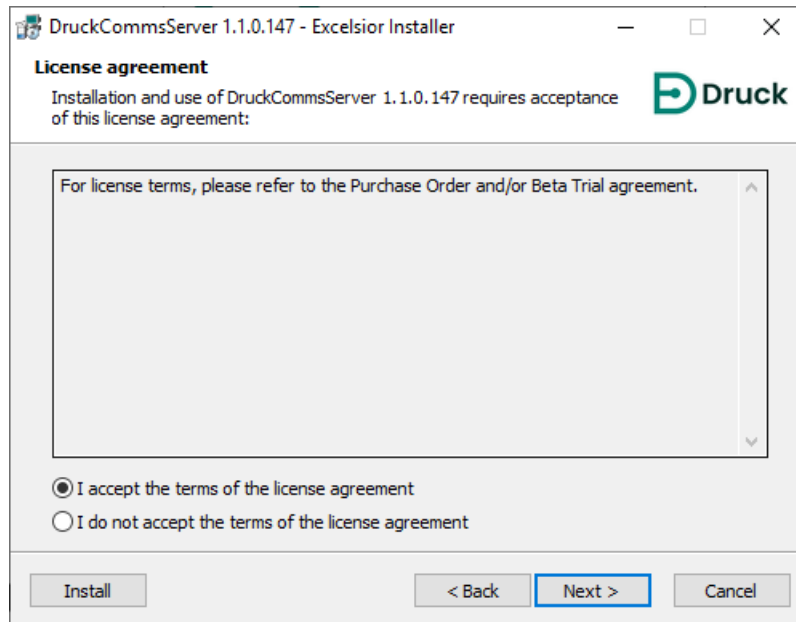
Impossibile comunicare con l'apparecchiatura di prova

Scaricare il pacchetto comunicatore dell'apparecchiatura di prova. Dopo il download, estrarre i file ed eseguire setup.exe per eseguire l'installazione. Per le istruzioni di installazione o per la risoluzione dei problemi, consultare il Manuale di installazione. [Contattare l'Amministratore per assistenza.](#)

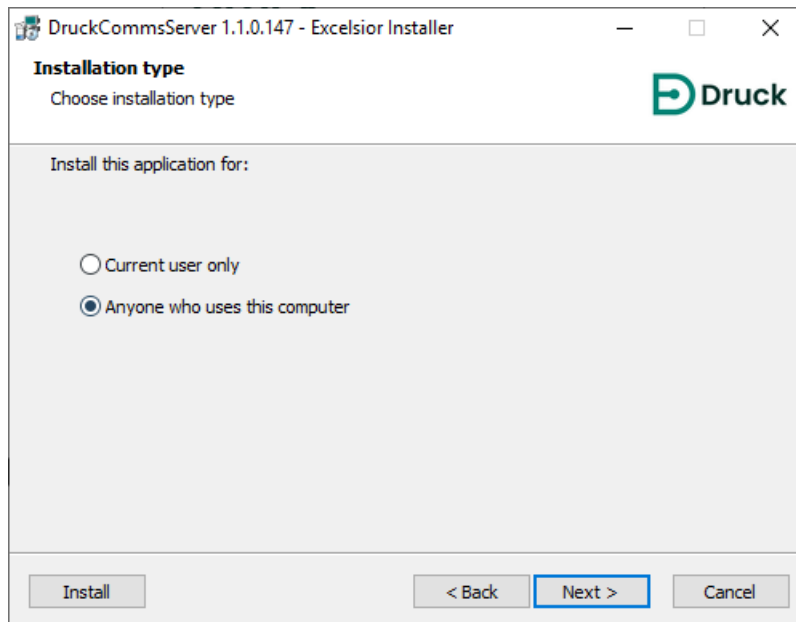
2. Selezionare **Scarica** per ottenere il file di installazione del comunicatore dell'apparecchiatura di prova.
3. I file di installazione del comunicatore dell'apparecchiatura di prova sono visualizzati come file zip CommsServerInstall. Dopo avere scaricato il file zip Comms Server, è possibile seguire la stessa procedura prima o dopo l'installazione di 4Sight2.
4. Estrarre i file dal file zip Comms Server e fare doppio clic sul file setup.exe per eseguire il programma di installazione.
5. Viene visualizzato il programma di installazione DruckCommsServer. Seguire le istruzioni nel programma di installazione o nella presente guida.



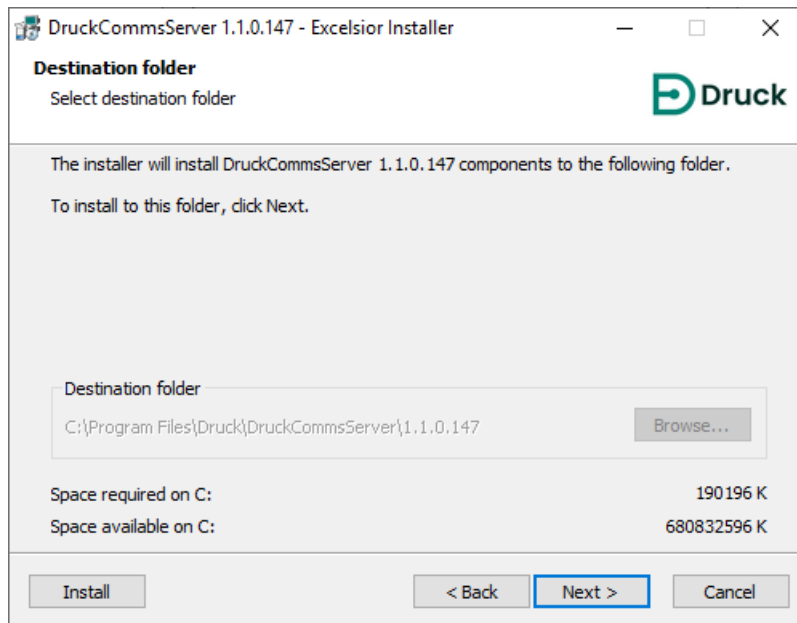
6. Selezionare **Avanti** per visualizzare la schermata del contratto di licenza, leggere i termini e selezionare **Accetto i termini del contratto di licenza**, quindi fare clic su **Avanti** per proseguire.



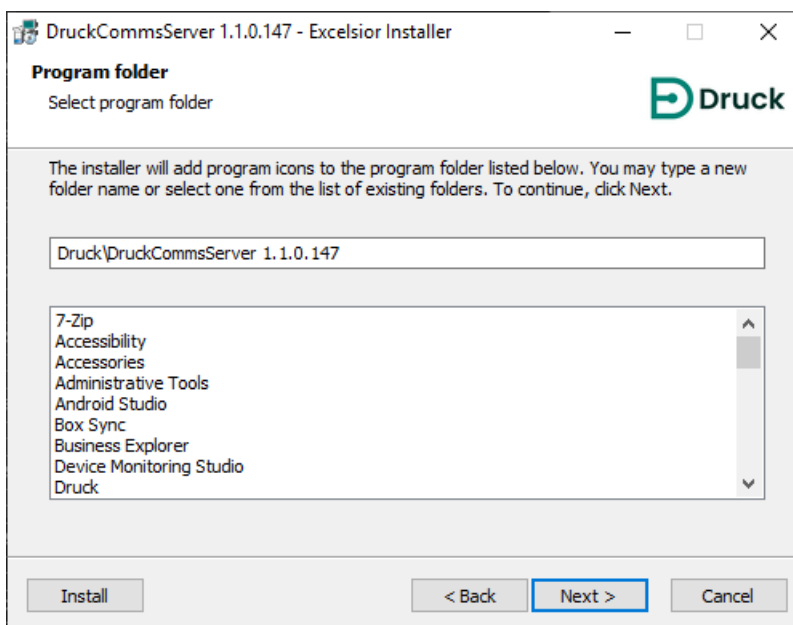
7. Dalla schermata Tipo di installazione, selezionare se si desidera installare CommsServer per tutti gli utenti del PC o solo per l'utente corrente.



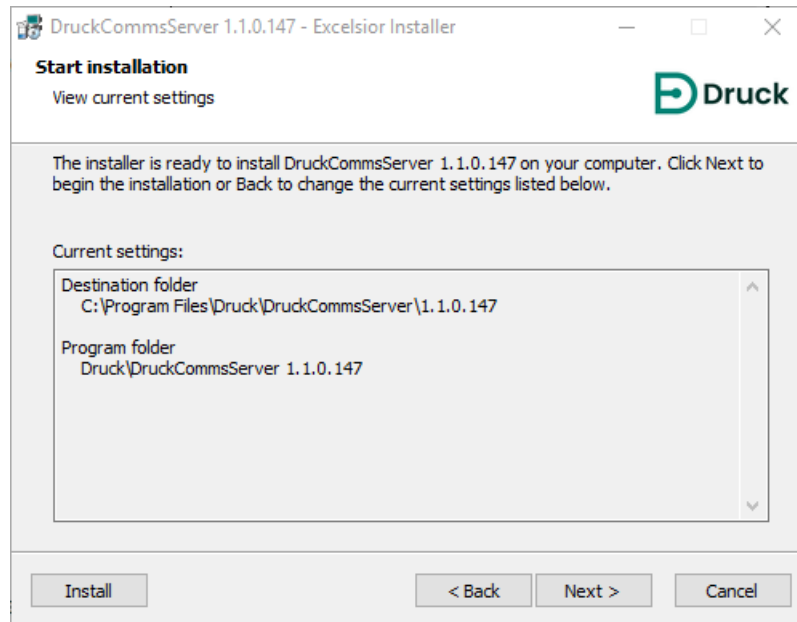
8. La schermata Cartella di destinazione visualizza la cartella in cui verrà installato DruckCommsServer. Per impostazione predefinita è C:\Program Files\Druck\DruckCommsServer\[versione_applicazione]



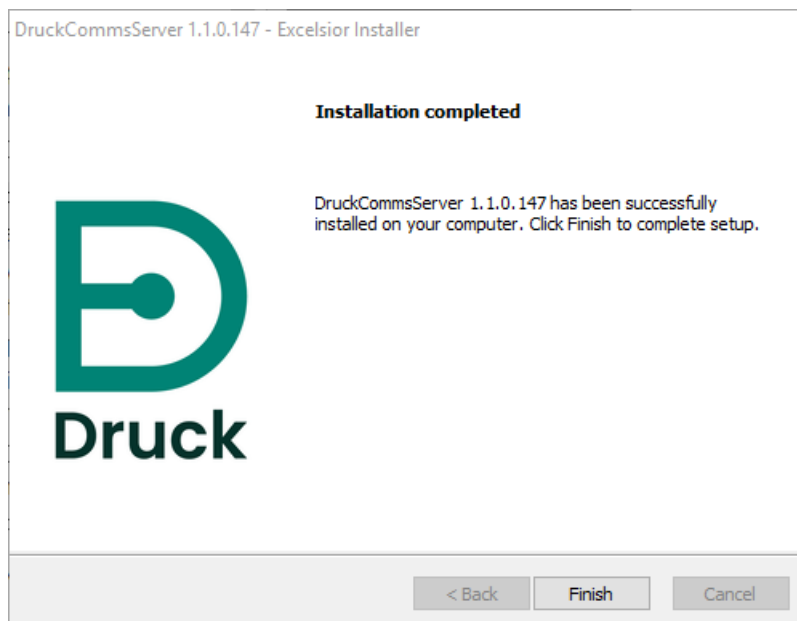
9. La schermata Cartella programma consente di selezionare il punto in cui il programma di installazione aggiunge l'icona del programma verso la cartella del programma.



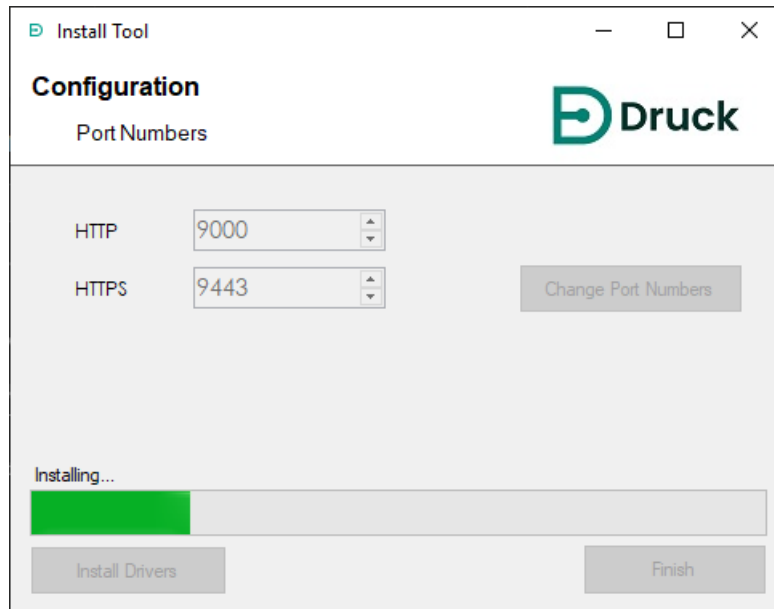
10. Viene quindi visualizzata la schermata Avvia installazione, selezionare **Avanti** per avviare l'installazione.



11. Al termine dell'installazione, selezionare **Fine**.

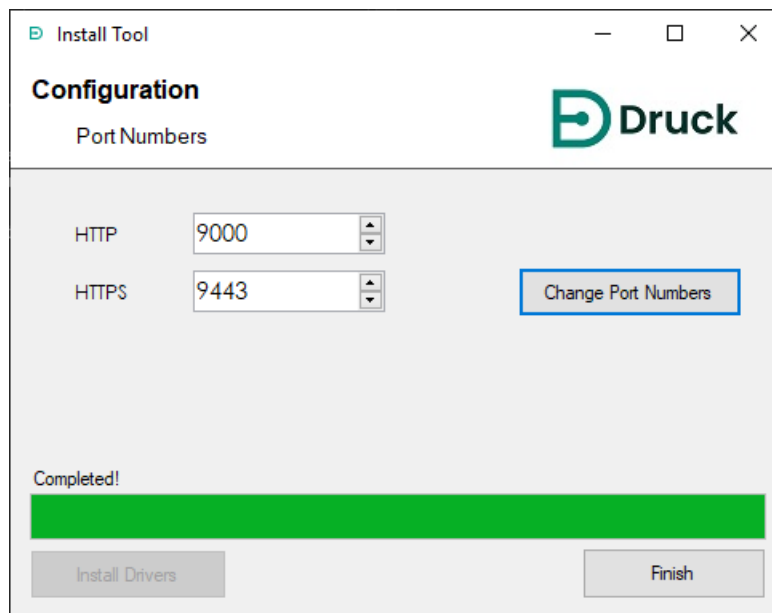


12. Viene quindi visualizzato lo strumento di installazione di CommsServer per l'installazione dei driver aggiuntivi necessari.



13. Nel caso in cui non si sappia se 4Sight2 utilizza numeri di porta alternativi, contattare l'utente amministrativo

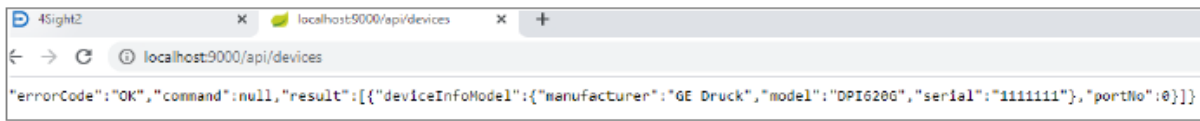
Nota: lo strumento di installazione può essere eseguito separatamente dopo l'installazione per configurare nuovamente tali numeri di porta.



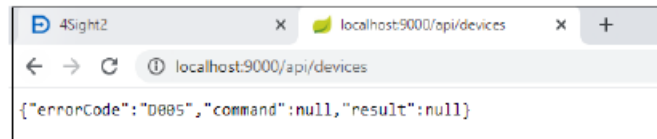
14. Provare l'installazione del comunicatore dell'apparecchiatura di prova immettendo il seguente URL nel browser Web:

`http://localhost:[numero di porta http utilizzato superiore al valore predefinito 9000]/api/devices`

Il browser Web visualizza l'elenco di tutti i dispositivi collegati:



Se non è collegato alcun dispositivo viene visualizzato quanto mostrato di seguito



Nota: i driver necessari per i calibratori di temperatura non vengono configurati automaticamente. Consultare la Sezione 4.3 Configurazione dei driver dei calibratori di temperatura

15. Se l'installazione del driver del dispositivo non viene eseguita correttamente, utilizzare la procedura nella prossima sezione per configurare manualmente i driver necessari.

4.1 Configurazione manuale dei driver

Le impostazioni dei criteri di sicurezza IT possono impedire la configurazione automatica dei driver Druck durante l'installazione. Questo sarà essere evidente se 4Sight2 non è in grado di comunicare con le varie apparecchiature.

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

o



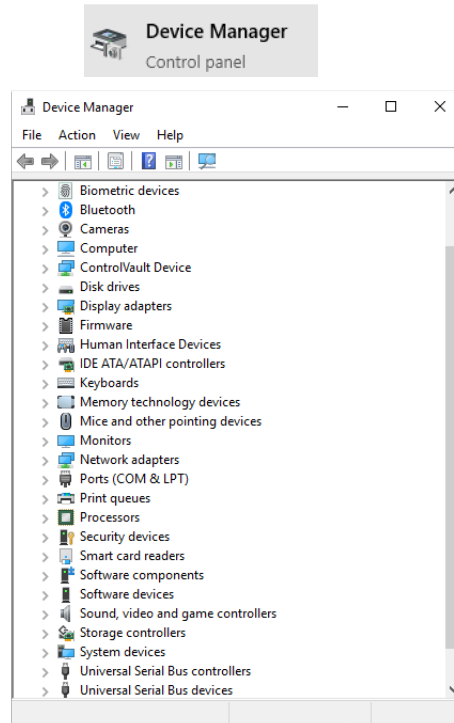
Per risolvere il problema è possibile configurare manualmente i driver Druck. Se non si è sicuri sull'operazione o se è necessaria ulteriore assistenza, rivolgersi al rappresentante IT locale.

4.1.1 Prerequisiti

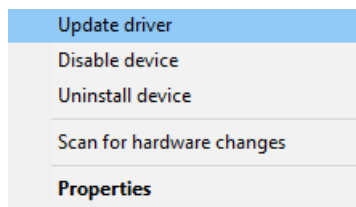
Per installare i driver, è necessaria l'applicazione 4Sight2 installata sul computer o accessibile dal computer. Prima di installare i driver, verificare che sia possibile effettuare l'accesso all'applicazione 4Sight2 dal computer.

Per l'installazione manuale dei driver procedere come indicato di seguito.

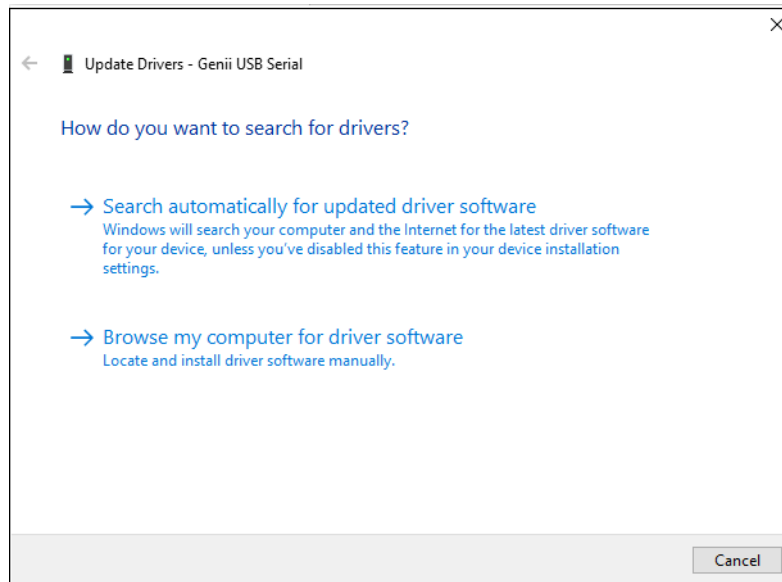
1. Sul desktop, cercare Gestione dispositivi ed eseguirlo.



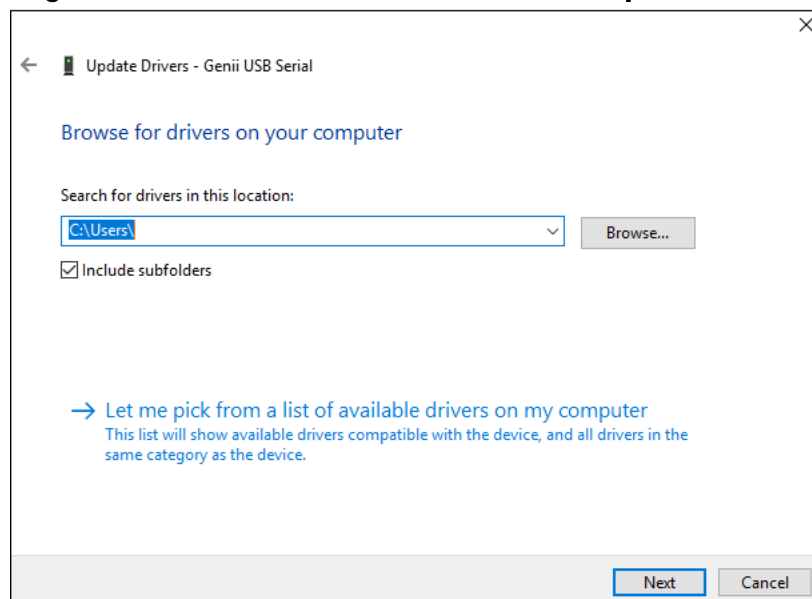
2. Scorrere nell'elenco dei dispositivi USB per trovare i dispositivi non configurati (Dispositivo sconosciuto o Altri dispositivi). Fare clic con il pulsante destro del mouse e selezionare **Aggiornamento software driver**.



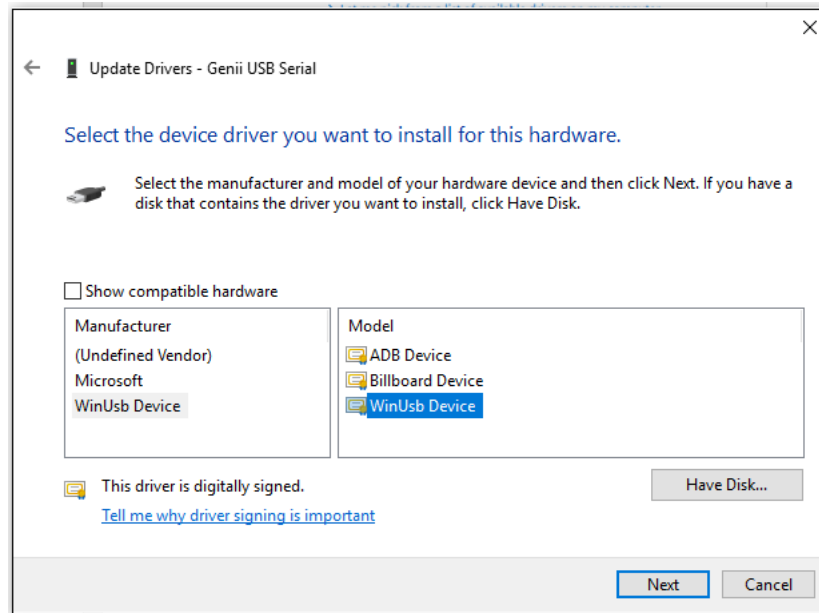
3. Selezionare **Cerca il software del driver nel computer.**



4. Selezionare **Scegli manualmente da un elenco di driver di dispositivo** nel computer.



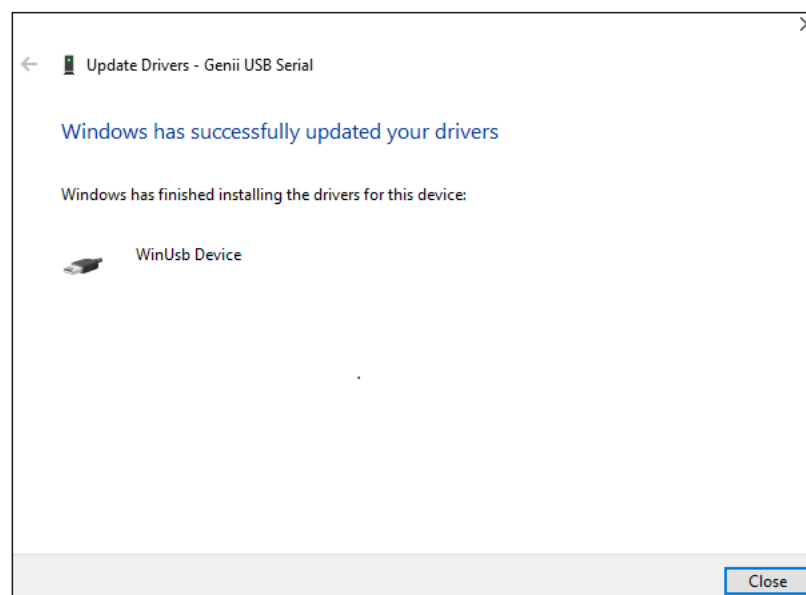
5. Deselezionare **Mostra hardware compatibile** e selezionare **Dispositivo WinUsb** per Produttore e **Dispositivo WinUsb** per Modello.



6. Viene visualizzata l'avvertenza mostrata di seguito. Fare clic su **Sì**.



7. Viene visualizzata una schermata che indica l'aggiornamento riuscito dei driver.



Ripetere la procedura per ogni categoria di dispositivi quando si collega il dispositivo per la prima volta.

Per esempio, se si collegano un PACE e un Genii per la prima volta, può essere necessario ripetere la procedura separatamente per PACE e Genii. Tutte le istanze successive di tutti i dispositivi PACE e Genii dovrebbero funzionare senza che sia necessario effettuare tali impostazioni. Tuttavia, se successivamente si collega una categoria di dispositivi diversa, per esempio DPI611/612, è necessario ripetere la procedura per tale categoria.

4.2 Prova del comunicatore dell'apparecchiatura di prova

1. Effettuare l'accesso a 4Sight2 come Tecnico.
2. Portarsi in **Asset >> Elenco di lavoro**.
3. Selezionare uno o più range e assegnarli al flusso di lavoro di calibrazione portatile o automatica.
4. Fare clic sul pulsante **Aggiorna**.

The screenshot shows the 'Calibrazione portatile' (Portable Calibration) interface. On the left, there is a search bar and a list of test ranges. The main area is titled '1 Seleziona apparecchiatura di prova' (Select test equipment). It includes a 'Porta *' dropdown set to 'USB' and an 'Apparecchiature di prova *' dropdown menu. A red square highlights a refresh icon (circular arrow) next to the dropdown menu. Below the dropdowns are buttons for 'Annulla la calibrazione', 'Reset', 'Cancella memoria apparecchiatura di prova', and 'Continua'. Navigation buttons '<< Indietro' and 'Avanti >>' are also present.

5. Fare clic sull'elenco a discesa **Apparecchiatura di prova**. Se nell'elenco è visualizzato il dispositivo collegato, il comunicatore dell'apparecchiatura di prova è configurato correttamente.

This screenshot shows the same 'Calibrazione portatile' interface, but the 'Apparecchiature di prova *' dropdown menu is now open, displaying a search filter and a list of devices. The device 'DPI620G -- 5262059' is selected. The refresh icon is still visible next to the dropdown menu. The rest of the interface, including the search bar, navigation buttons, and 'Continua' button, remains the same.

4.3 Configurazione del driver del calibratore di temperatura

Per consentire al calibratore di temperatura di comunicare con 4Sight2, è necessario installare un driver FTDI.

1. Scaricare il driver FTDI utilizzando il collegamento indicato di seguito: <https://www.ftdichip.com/Drivers/VCP.htm>.
2. Estrarre il file scaricato dal file zip e salvarlo in una posizione nota nel computer.
3. Portarsi in Gestione dispositivi nel computer.
4. Selezionare Porte (COM e LPT) dall'elenco di dispositivi per visualizzare il calibratore di temperatura.
5. Fare clic con il tasto destro del mouse sul calibratore di temperatura e selezionare l'aggiornamento dei driver.
6. Selezionare Cerca il software del driver nel computer.
7. Selezionare Sfoglia accanto alla casella Specificare il percorso in cui cercare i driver.
8. Selezionare la cartella estratta contenente il driver scaricato.
9. Selezionare Avanti, quindi chiudere.
10. Il driver viene installato.
11. Per provare la comunicazione con un calibratore di temperatura in 4Sight2, portarsi nella calibrazione automatica e verificare che sia possibile selezionare il calibratore di temperatura come Controllore ingresso. In alternativa, eseguire nuovamente il punto 14 della Sezione 4.

Guida all'implementazione

5. Guida all'implementazione

5.1 Architettura di implementazione

L'architettura tipica comprende l'applicazione Web 4Sight2 e il server di autorizzazione e autenticazione utente (UAA, User Authentication and Authorization) in esecuzione sul server Web Tomcat con il database PostgreSQL in esecuzione sullo stesso computer.

L'applicazione Web Browser Client si connette al server 4Sight2, che a sua volta archivia e recupera le informazioni dal database PostgreSQL.

5.2 Implementazione fisica

Si presuppone che l'utente che installa 4Sight2 abbia già predisposto misure di sicurezza informatica in grado di soddisfare i criteri di sicurezza utente e che:

- Il server sia posizionato in un luogo protetto con controllo dell'accesso fisico limitato.
- Il controllo dell'accesso al server sia protetto con accesso autorizzato limitato.
- La rete del server sia protetta con il firewall per consentire accesso limitato alle applicazioni conosciute solo su porte note.
- Le applicazioni vengano eseguite nel relativo contesto e abbiano accesso a database e file system esclusivamente nella relativa cartella.

5.3 Rete

I client vengono connessi mediante browser Web, tramite connessioni Ethernet o una rete wireless. A seconda della larghezza di banda wireless e del numero di dispositivi connessi, sulla rete wireless potrebbe verificarsi una potenziale latenza.

Si consiglia di disabilitare o rimuovere eventuali plug-in ed estensioni del browser installati nel browser.

Il server Web 4Sight2 non deve essere esposto a Internet, gli accessi necessari devono essere forniti tramite Intranet o VPN.

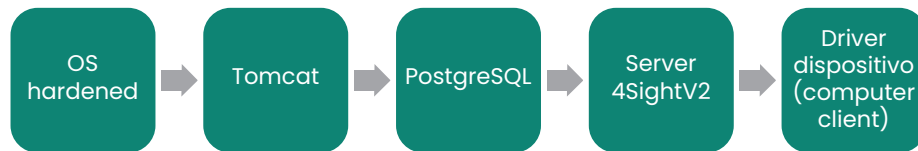
5.4 Sequenza di implementazione

PostgreSQL, Tomcat e Java Runtime sono un prerequisito per l'applicazione 4Sight2. PostgreSQL viene installato come pacchetto separato, mentre gli altri pacchetti vengono installati insieme all'applicazione. Di conseguenza, se PostgreSQL è già installato sul computer utente, per connettersi ed eseguire la configurazione è sufficiente la password dell'utente con privilegi avanzati.

L'installazione richiede diritti di amministratore Windows sul computer. Prima dell'installazione, l'utente deve disporre della password di utente con privilegi avanzati di PostgreSQL, del nome utente e della password di amministratore dell'applicazione nonché del nome utente e della password del database.

La password dell'utente con privilegi avanzati di PostgreSQL è necessaria per creare il database e altre strutture all'interno del server PostgreSQL. L'amministratore dell'applicazione è il primo utente della stessa. È responsabile della creazione di altri utenti e della loro assegnazione a diversi ruoli. L'utente database ha accesso a 4Sight2 e al database UAA. Per accedere al database si utilizzano le credenziali di questo nome utente.

L'applicazione viene pubblicata su una porta del computer. La porta predefinita è 8083 e può essere modificata dall'utente al momento dell'installazione o in un secondo momento. Il contesto applicativo predefinito in Tomcat è 4Sight2.



Per garantire la protezione del sistema operativo, attenersi alla procedura di hardening del sistema operativo conformemente alle linee guida di Microsoft o CIS. La procedura di installazione guida l'utente nell'installazione di PostgreSQL prima di installare il server 4Sight2.

Il comunicatore dell'apparecchiatura di prova viene installato sui computer client quando si collega l'apparecchiatura di prova mediante porte USB. Se il comunicatore dell'apparecchiatura di prova non è già installato sul computer, viene richiesto di scaricarlo dal server 4Sight2 e di installarlo sul computer. Il comunicatore dell'apparecchiatura di prova è in ascolto sulla porta 9000 e può comunicare solo sul livello sicuro.

5.5 Attività post-implementazione

5.5.1 Aggiunta di utenti e gruppi

L'amministratore è responsabile della creazione di diversi utenti, come Supervisore, Tecnico senior, Tecnico e Auditor nell'applicazione. L'amministratore può assegnarli a diversi gruppi predefiniti incorporati. Se sono necessari un maggiore controllo o una maggiore granularità, l'amministratore può creare gruppi personalizzati e assegnare loro accesso specifico.

5.5.2 Password predefinite

Si sta utilizzando la password hardcoded predefinita per l'utente Tomcat nel file ":\Program Files\Druck\4Sight2\<<latest folder number>>\apache-tomcat\conf\tomcat-user.xml".

Si consiglia di modificare la password predefinita e di utilizzare sempre una password conforme alle relative procedure consigliate.

```

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

Per garantire la sicurezza dell'applicazione, sono state implementate le procedure consigliate. Per un livello di sicurezza superiore, attenersi alla seguente procedura:

i file e le cartelle di configurazione sono protetti e, per impostazione predefinita, solo il servizio e i sistemi dispongono dei diritti di accesso. Di conseguenza, prima di tentare di eseguire le operazioni riportate di seguito, l'utente amministratore dispone solo dell'accesso in lettura/scrittura alla cartella C:\Program Files\Druck\4Sight2\<<latest folder number>>\apache-tomcat\conf; aprire quindi il prompt dei comandi con le credenziali dell'utente amministratore.

5.5.3 Comunicazioni protette

Questa sezione fornisce istruzioni per la configurazione di 4sight2 in modalità sicura (nota anche come modalità SSL) utilizzando un certificato autofirmato. Prima di procedere, leggere i presupposti, i termini e le condizioni definiti nell'applicazione 4Sight2. Un certificato autofirmato è un metodo per l'abilitazione di SSL in 4Sight2. In alternativa è possibile

acquistare un certificato CA di terze parti presso molti fornitori, quali Symantec, Digicert e così via.

Nota: la semplice abilitazione di SSL non rende necessariamente protetta l'applicazione. Si tratta di una delle pratiche più comuni per la realizzazione di un'applicazione Web protetta.

5.5.3.1 Presupposti e avvertenze

Affinché le istruzioni di seguito funzionino, si considerano i presupposti di seguito:



Per la generazione di certificati autofirmati è necessario il software OpenSSL per Windows. 4Sight2 presuppone che le leggi nazionali, regionali e dell'organizzazione e le linee guida normative consentano l'utilizzo del software OpenSSL.

- Keytool è un programma di utilità per la gestione di chiavi e certificati fornito da Java, utilizzato per generare diversi componenti coinvolti nella configurazione https. 4Sight2 presuppone che le leggi nazionali, regionali e dell'organizzazione e le linee guida normative consentano l'utilizzo del programma di utilità Keytool.
- Per effettuare le configurazioni di seguito sono necessari i privilegi di amministratore. Per ulteriori informazioni sull'ottenimento dei diritti di amministratore, contattare il proprio reparto IT locale.
- La procedura di seguito richiede conoscenze di base dei processi informatici, quindi si consiglia che sia effettuata dal reparto IT locale o dietro la sua guida.
- I contenuti presentati in questo documento, quali nomi di host, password, URL e percorsi di cartelle, sono unicamente a scopo di riferimento. Accertarsi di modificare i comandi secondo necessità prima della loro esecuzione.
- Le sezioni di seguito descrivono due scenari. Nel primo, il server e il client si trovano nello stesso computer, nel secondo il server e il client si trovano in computer diversi (scenario con client multipli).

5.5.3.2 Procedura per la configurazione dell'applicazione 4Sight2 in https

1. Arrestare 4Sight2 da Windows Services
2. Aprire il prompt dei comandi in **modalità amministratore**.
3. Portarsi nella cartella indicata di seguito nella directory di installazione di 4Sight2 eseguendo il comando di seguito:

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

4. Verificare la presenza di Keytool eseguendo il comando di seguito nel prompt dei comandi:
Keytool -?

Se non è presente, impostare il percorso di ambiente su bin di JRE nella cartella di installazione di 4Sight2, come mostrato di seguito. Aggiornare il percorso corretto secondo la cartella di installazione.

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

5. Per la creazione di un nuovo certificato, passare al punto 6, altrimenti, se esiste già un certificato, effettuare la procedura di seguito:

a. Controllare l'esistenza del file di certificato 4Sight.js nel keystore di Java

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

b. Se il certificato è già installato, eliminarlo.

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


c. Verificare la presenza del file 4SightV2PublicKey.cer ed eventualmente eliminarlo del **"../app/Certificate/4SightV2PublicKey.cer"**

d. Verificare che il certificato esista già nel cacert di Java.

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

e. Se nell'archivio Java esiste il certificato, eliminarlo.

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

6. Creare il nuovo certificato eseguendo il comando di seguito:

keytool -genkey -trustcacerts -keyalg "RSA" -keysize 2048 -validity 1095 -keypass <<KeyPassword>> -alias <<nome host>> -keystore 4Sight.jks -storepass <<StorePassword>> -dname "CN=%COMPUTERNAME%, OU=<<Unità organizzazione>>, O=<<Organizzazione>>, L=<<Località>>, S=<<Stato>>, C=<<Iniziale paese>>" -ext eku:critical=sa

7. Esportare il certificato nel file 4SightV2PublicKey.cer (non modificare nome o percorso)

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

Quando il comando è stato eseguito correttamente, viene visualizzato il messaggio: "Certificato archiviato nel file

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

8. Importare il certificato nel file CACert Java.

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

Dopo la corretta esecuzione del comando, viene visualizzato il messaggio "Certificato aggiunto al keystore".

9. Inserire il certificato nel file di configurazione Tomcat

a. Aprire il file server.xml dalla posizione indicata di seguito.

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

b. Immettere i seguenti dati in server.xml:

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

c. Commentare la sezione di seguito per disabilitare le connessioni http:

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

Nota: se questa parte non viene commentata, l'applicazione non funziona.

10. A questo punto la configurazione https dell'applicazione 4Sight2 è completa.

11. Per provare la configurazione, riavviare il servizio 4Sight2 in Windows Service.

12. Aprire Google Chrome, cancellare la cache del browser e riavviare il browser.

13. Nel browser immettere l'URL di seguito: `https://<<nome-host>>:8443/4sight2`
 - Il primo caricamento dell'URL può richiedere più tempo.
 - Viene visualizzata la schermata "La connessione non è privata"
 - Fare clic sul pulsante **Avanzate** >> collegamento **Procedi a XX**.
 - Se non viene visualizzata la schermata 4sight2, fare clic sul pulsante **Ricarica**.
 - Si viene reindirizzati sulla pagina 4sight2.
 - Nella barra dell'indirizzo è presente un errore "Non sicuro", che viene eliminato dopo la registrazione del certificato in mmc.



5.5.3.3 Procedura per la configurazione di DruckCommsServer in https se installato sul computer server

Vervang waarden in << >> door geschikte gegevens voordat u de opdracht uitvoert.

1. Arrestare DruckCommsServer da Windows Services
2. Aprire il prompt dei comandi in **modalità amministratore**.
3. Verificare la presenza di Keytool eseguendo il comando di seguito nel prompt dei comandi:
Keytool -?

Se non è presente, impostare il percorso di ambiente su bin di JRE nella cartella di installazione di 4Sight2, come mostrato di seguito.

Aggiornare il percorso corretto secondo la cartella di installazione.

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

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

4. Portarsi nella cartella indicata di seguito nella directory di installazione di DruckCommServer eseguendo il comando di seguito:

cd "C:\Program Files\Druck\DruckCommsServer\<< versione Communication Service >>"

5. Verificare l'esistenza di un certificato effettuando la procedura di seguito:
 - a. Verificare che il certificato esista già nel cacert di Java.
keytool -list -alias tomcat -storepass changeit -keystore cacerts
 - b. Se nell'archivio Java esiste il certificato, eliminarlo.
keytool -delete -noprompt -alias tomcat -storepass changeit -keystore cacerts
 - c. Eliminare i certificati preconfigurati da CommsServer forniti con l'impostazione predefinita
del 4Sight.jks
del 4SightV2DeviceMgr.pfx
6. Creare il nuovo certificato eseguendo il comando di seguito:
keytool -genkey -trustcacerts -keyalg "RSA" -keysize 2048 -validity 1095 -keypass <<KeyPassword>> -alias tomcat -keystore CommServer.jks -storepass <<StorePassword>> -dname "CN=localhost, OU=<<Unità organizzazione>>, O=<<Organization>>, L=<<Località>>, S=<<Stato>>, C=<<Iniziale paese>>" -ext eku:critical=sa

7. Esportare il certificato nel file DruckCommServer.cer.
keytool -export -alias tomcat -keystore CommServer.jks -storepass <<StorePassword>> -storetype JKS -file DruckCommServer.cer
 Quando il comando è stato eseguito correttamente, viene visualizzato il messaggio:
 "Certificato archiviato nel file DruckCommServer.cer".
8. Importare il certificato del server di comunicazioni nel file CACert Java.
keytool -import -noprompt -trustcacerts -alias tomcat -storepass changeit -keystore cacerts -file DruckCommServer.cer
 Dopo la corretta esecuzione del comando, viene visualizzato il messaggio "Certificato aggiunto al keystore".
9. Importare il certificato 4Sight nel file CACert Java.
keytool -import -noprompt -trustcacerts -alias <<nome host server>> -storepass changeit -keystore cacerts -file "C:\Program Files\Druck\4Sight2\<<latest folder number>>\app\Certificate\4SightV2PublicKey.cer"
 Dopo la corretta esecuzione del comando, viene visualizzato il messaggio "Certificato aggiunto al keystore".
10. Modificare la password del keystore per application.properties in DruckCommsServer.
 Aprire il file:
 C:\Program Files\Druck\DruckCommsServer\<<Versione Communication Service>>\application.properties e modificare la riga di seguito:
keystore = CommServer.jks
key-store.password= << StorePassword >>
 Nota: << StorePassword >> fa riferimento alla **StorePassword** utilizzata al punto 6.
11. Riavviare i servizi 4Sight2 e DruckCommsServer.

5.5.3.4 Procedura per la configurazione di DruckCommsServer in https se installato su un computer client

1. Il programma di utilità Keytool è compreso nel pacchetto di Java, quindi è possibile installare Java nel computer o controllare la disponibilità di Keytool di Java direttamente senza l'installazione di Java.
2. Arrestare DruckCommsServer da Windows Services
3. Aprire il prompt dei comandi in **modalità amministratore**.
4. Verificare la presenza di Keytool eseguendo il comando di seguito nel prompt dei comandi:
Keytool -?
 In caso contrario, impostare il percorso di ambiente su bin di JRE, se è stato installato Java sul computer, oppure è possibile impostare il percorso verso Keytool come mostrato di seguito.
 Aggiornare il percorso corretto secondo la cartella di installazione.
C:\Program Files\Java\<< versione Java >>\bin
Set Path=%Path%; "C:\Program Files\Java\<< versione Java >>\bin"
5. Ottenere il file **4SightV2PublicKey.cer** dal computer server in cui è installata l'applicazione 4Sight. Questo file si trova nel server come indicato di seguito:
C:\Program Files\Druck\4Sight2\<<latest folder number>>\app\Certificate\4SightV2PublicKey.cer
6. Copiare **4SightV2PublicKey.cer** nel percorso indicato di seguito:

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

7. Ora eseguire i punti da 4 a 8 nella sezione 5.5.3.3.
8. Importare il certificato 4Sight nel file CACert Java.

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

Dopo la corretta esecuzione del comando, viene visualizzato il messaggio "Certificato aggiunto al keystore".

9. Eseguire i punti da 10 a 11 nella sezione 5.5.3.3.

5.5.3.5 Procedura per la generazione di un certificato autofirmato per 4Sight2

1. Scaricare e installare OpenSSL per Windows.
2. Arrestare i servizi 4Sight2 da Windows Services.
3. Creare una nuova cartella dal nome **4Sight2Certificate** nel drive C.
È possibile scegliere qualsiasi posizione o nome di cartella, sempre che si disponga dei diritti di amministratore per tale cartella.
4. Creare un nuovo file nella cartella sopra indicata utilizzando Blocco note e salvarlo come **openssl-ca.cnf**
Copiare i contenuti di seguito nel file e salvarlo.

```

HOME      = .
RANDFILE  = $ENV::HOME/.rnd

#####
#####
[ ca ]
default_ca = CA_default # The default ca section

[ CA_default ]
base_dir    = .
certificate = $base_dir/cacert.pem # The CA certificate
private_key = $base_dir/cakey.pem  # The CA private key
new_certs_dir = $base_dir          # Location for new certs after signing
database    = $base_dir/index.txt  # Database index file
serial      = $base_dir/serial.txt # The current serial number

unique_subject = no # Set to 'no' to allow creation of
                  # several certificates with same subject.

default_days = 1000 # How long to certify for
default_crl_days = 30 # How long before next CRL
default_md    = sha256 # Use public key default MD
preserve     = no # Keep passed DN ordering

x509_extensions = ca_extensions # The extensions to add to the cert

email_in_dn = no # Don't concat the email in the DN
copy_extensions = copy # Required to copy SANs from CSR to cert

#####
#####
[ req ]
default_bits = 4096
default_keyfile = cakey.pem
distinguished_name = ca_distinguished_name
x509_extensions = ca_extensions
string_mask = utf8only
#####
#####
[ ca_distinguished_name ]
countryName = Country Name (2 letter code)
countryName_default = US

stateOrProvinceName = State or Province Name (full name)
stateOrProvinceName_default = Maryland

localityName = Locality Name (eg, city)
localityName_default = Baltimore

```

```

organizationName      = Organization Name (eg, company)
organizationName_default = Test CA, Limited

organizationalUnitName = Organizational Unit (eg, division)
organizationalUnitName_default = Server Research Department

commonName      = [Company Name]
commonName_default = Test CA

emailAddress     = Email Address
emailAddress_default = test@example.com

#####
#####
[ ca_extensions ]

subjectKeyIdentifier = hash
authorityKeyIdentifier = keyid:always, issuer
basicConstraints     = critical, CA:true
keyUsage             = keyCertSign, cRLSign

#####
#####
[ signing_policy ]
countryName          = optional
stateOrProvinceName = optional
localityName         = optional
organizationName     = optional
organizationalUnitName = optional
commonName           = supplied
emailAddress         = optional

#####
#####
[ signing_req ]
subjectKeyIdentifier = hash
authorityKeyIdentifier = keyid,issuer
basicConstraints     = CA:FALSE
keyUsage             = digitalSignature, keyEncipherment

```

Nota: Aggiorna **[Company Name]** sopra e salva il file. Questo è il nome degli emittenti del certificato che apparirà nella console di gestione.

5. Creare un nuovo file nella cartella sopra indicata utilizzando Blocco note e salvarlo come **openssl-server.cnf**

Copiare i contenuti di seguito nel file e salvarlo.

```

HOME      = .
RANDFILE  = $ENV::HOME/.rnd

#####
#####
[ req ]
default_bits      = 2048
default_keyfile   = serverkey.pem
distinguished_name = server_distinguished_name
req_extensions    = server_req_extensions
string_mask       = utf8only

#####
#####
[ server_distinguished_name ]
countryName       = Country Name (2 letter code)
countryName_default = US

stateOrProvinceName   = State or Province Name (full name)
stateOrProvinceName_default = MD

localityName          = Locality Name (eg, city)
localityName_default = Baltimore

organizationName      = Organization Name (eg, company)
organizationName_default = Test Server, Limited

commonName            = [Hostname of server]
commonName_default    = Test Server

emailAddress          = Email Address
emailAddress_default  = test@example.com

#####
#####
[ server_req_extensions ]

subjectKeyIdentifier = hash
basicConstraints     = CA:FALSE
keyUsage             = digitalSignature, keyEncipherment
subjectAltName       = @alternate_names
nsComment            = "OpenSSL Generated Certificate"

#####
#####
[ alternate_names ]

```

```
DNS.1 = [Hostname of server]

# IPv4 localhost
IP.1 = [IP Address of server]

# IPv6 localhost
IP.2 = ::1
```

Nota: aggiornare il nome host e l'indirizzo IPv4 indicati sopra e salvare il file.

6. Aprire il prompt dei comandi con privilegi di amministratore.
7. Portarsi nella cartella 4Sight2Certificate eseguendo il comando indicato di seguito:


```
cd "<<percorso completo verso 4Sight2Certificate >>"
```
8. Impostare la variabile di percorso della cartella bin OpenSSL eseguendo il comando indicato di seguito.


```
Set path=%path%;"<<cartella bin di openssl>>"
```

 Esempio di percorso predefinito:


```
Set Path=%Path%;"C:\Program Files\OpenSSL-Win64\bin"
```
9. Impostare la variabile di percorso della cartella bin di JRE eseguendo il comando indicato di seguito. Nota: il percorso indicato di seguito può essere diverso.


```
Set path=%path%;"C:\Program Files\Druck\4Sight2\<<latest folder number>>\jre\bin"
```
10. Eseguire il comando di seguito per generare i file cacert.pem e cakey.pem


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

 Quando richiesto, immettere i dati del certificato, per esempio paese, stato ecc.
11. Eseguire il comando di seguito per generare i file servercert.csr e serverkey.pem


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

 Quando richiesto, immettere i dati del certificato, per esempio paese, stato ecc.
12. Creare un nuovo file con Blocco note e salvarlo come index.txt. Salvare il file nella cartella 4Sight2Certificate.
13. Creare un nuovo file con Blocco note e salvarlo come serial.txt. Salvare il file nella cartella 4Sight2Certificate.

Aprire il file e immettere **01**. Salvare e chiudere il file.
14. Eseguire il comando di seguito per generare nuovi certificati nei file servercert.pem e serverkey.pem.


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

 Immettere Y per confermare le modifiche; dopo l'esecuzione viene visualizzato un messaggio di database aggiornato.
15. Inserire i file di chiavi esistenti nel formato PFX eseguendo il comando di seguito.


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

 Viene richiesto due volte di inserire la password.

16. Convertire l'archivio PFX in keystore Java ordinato per la posizione bin di JRE indicata sopra, ovvero tomcat/percorso config.

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

Nota: mantenere la stessa password per entrambi gli archivi. Verificare che si punti a 4Sight.jks presente nella cartella config di tomcat come mostrato in precedenza.

Viene richiesto di immettere la password del keystore di destinazione e la password del keystore di origine. Dopo l'esecuzione del comando, viene visualizzato il messaggio "Comando di importazione completato: 1 voce importata correttamente".

17. Esportare il certificato dal keystore Java nel file all'indirizzo:

```
C:\Program Files\Druck\4Sight2\<<latest folder  
number>>\app\Certificate\4SightV2PublicKey.cer  
keytool -export -alias <<nome host>> -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"
```

Nota: verificare che si punti a 4Sight.jks presente nella cartella config di tomcat come mostrato in precedenza. Dopo l'esecuzione viene visualizzato un messaggio di avvenuta archiviazione del certificato.

18. Importare il file di certificato nella cartella cacerts nella directory di installazione di 4sight2.

Nota: il percorso può variare secondo la directory di installazione e la versione di 4sight2

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

Nota: se l'alias che si sta cercando di creare esiste già, eseguire il comando di seguito per eliminarlo, quindi eseguire quanto sopra per creare un nuovo alias:

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

Dopo l'esecuzione del comando viene visualizzato il messaggio "Certificato aggiunto al keystore".

19. Effettuare la modifica indicata di seguito nel file server.xml (presente in C:\Program Files\Druck\4Sight2\<<latest folder number>>\apache-tomcat\conf).

a. Immettere i seguenti dati in server.xml:

```
<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. Commentare la sezione di seguito per disabilitare le connessioni http:

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

20. Questo completa la configurazione https per 4Sight2. Avviare il servizio 4sight2 da Windows Services.

5.5.3.6 Procedura per la configurazione di certificati autofirmati per DruckCommsServer se installato in un computer server

Si presuppone che l'applicazione 4sight2 sia stata convertita in https mediante l'esecuzione della procedura nella sezione 5.5.3.5 e che si disponga dei file indicati di seguito nella cartella

4Sight2Certificate:

- openssl-server.cnf
 - openssl-ca.cnf
 - cacert.pem
 - cakey.pem
 - index.txt
 - serial.txt
 - 4SightV2PublicKey.cer (questo file si può trovare nella cartella C:\Program Files\Druck\4Sight2\<<latest folder number>>\app\Certificate)
1. Creare una nuova cartella dal nome **CommserverCertificate**, copiare i file indicati sopra ed effettuare le modifiche indicate di seguito:
 - openssl-server.cnf

Nella sezione **req** modificare il valore **default_keyfile** in "**DruckCommServerCertKey.pem**".

- In **server_distinguished_name** modificare il valore **commonName** in "**localhost**".
 - In **alternate_names** modificare il valore **DNS.1** in "**localhost**".
 - In **alternate_names** modificare il valore **IP.1** in "**127.0.0.1**".
 - Salvare il file.
- openssl-ca.cnf (non modificare nulla al suo interno)
 - cacert.pem (non modificare nulla al suo interno)
 - index.txt (eliminare tutto il contenuto al suo interno, lasciare il file vuoto)
 - serial.txt (eliminare i contenuti all'interno e lasciare solo la voce 01)
2. Arrestare il servizio DruckCommsServer da Windows Services.
 3. Aprire il prompt dei comandi con privilegi di amministratore.
 4. Portarsi nella cartella **CommserverCertificate** eseguendo il comando indicato di seguito:


```
cd "<<percorso completo verso CommserverCertificate >>"
```
 5. Impostare la variabile di percorso della cartella bin OpenSSL eseguendo il comando indicato di seguito.


```
Set path=%path%;"<<cartella bin di openssl>>"
```

Esempio di percorso predefinito:

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

6. Impostare la variabile di percorso della cartella bin di JRE eseguendo il comando indicato di seguito. Nota: il percorso indicato di seguito può essere diverso.

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

7. Al termine, creare una richiesta di certificato Comm Server mediante il comando di seguito

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

Dopo l'esecuzione del comando, sono presenti una richiesta in **DruckCommServer.csr** e una chiave privata in **DruckCommServerCertKey.pem**

8. Eseguire quindi il comando di seguito per firmare la richiesta csr con il proprio ca:

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

9. In seguito, creare un file PFX con alias **tomcat** per il server delle comunicazioni utilizzando il comando di seguito:

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

10. Convertire l'archivio PFX in keystore Java utilizzando Keytool

Nota: mantenere la stessa password per entrambi gli archivi chiavi.

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

11. Ora importare il certificato in cacert .

a. Eliminare l'alias tomcat esistente fornito per impostazione predefinita con l'installazione

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

b. Dopo avere eliminato l'alias tomcat esistente, importare il certificato in cacerts utilizzando

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

12. Ora è necessario importare la chiave pubblica 4sight nel cacert del server delle comunicazioni per l'autenticazione delle comunicazioni; per farlo eseguire il comando di seguito:

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

13. Al termine sono presenti **DruckCommServer.pfx** e **CommServer.jks** nella cartella **CommserverCertificate** corrente.

Copiare i file e incollarli nella directory "C:\Program Files\Druck\DruckCommsServer\<< versione Communication Service >>\". Modificare **application.properties** dalla stessa posizione. Modificare il valore della proprietà come indicato di seguito

a. Keystore = CommServer.jks

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

c. key-store.type=JKS

5.5.3.6.1 Installazione del certificato in Windows per 4sight e DruckCommsServer

1. Aprire Esegui ed immettere "mmc", quindi premere Invio.
2. Portarsi in File e selezionare Aggiungi/rimuovi snap-in.
3. Dal menu sul lato sinistro selezionare i certificati. Premere Aggiungi, quindi selezionare Account computer >> Avanti >> Fine. Quindi fare clic su Ok.
4. Espandere la sezione relativa ai certificati (Computer locale). Espandere Autorità di certificazione root affidabili.

Fare clic con il tasto destro sulla cartella Certificates >> Tutte le attività >> Importa.

Selezionare cacert.pem >> avanti >> fine.

L'autorità CA personalizzata è stata installata correttamente con autorità affidabile.

Dopo avere effettuato la procedura, avviare il servizio DruckCommsServer.

5.5.3.7 Procedura per la configurazione di certificati autofirmati per DruckCommsServer se installato in un computer client

Per convertire DruckCommsServer in https, è necessario disporre di Keytool di Java e del programma di utilità OpenSSL.

1. Il programma di utilità Keytool è compreso nel pacchetto di Java, quindi è possibile installare Java nel computer o controllare la disponibilità di Keytool di Java direttamente senza l'installazione di Java.
2. Scaricare e installare OpenSSL per Windows.
3. Impostare la variabile di percorso della cartella bin OpenSSL eseguendo il comando indicato di seguito.

Set path=%path%;"<<cartella bin di openssl>>"

Esempio di percorso predefinito:

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

4. Impostare la variabile di percorso della cartella bin di JRE eseguendo il comando indicato di seguito.

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

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

5. Arrestare il servizio DruckCommsServer da Windows Services.
6. Creare una nuova cartella dal nome **CommserverCertificate** nel drive C o in un altro drive desiderato.
7. Ottenere il file di certificato pubblico 4sight2 **4SightV2PublicKey.cer** dal computer server situato nella directory C:\Program Files\Druck\4Sight2\<<latest folder number>>\app\Certificate e copiarlo nella cartella **CommserverCertificate**.
8. Creare **openssl-server.cnf** e **openssl-ca.cnf** eseguendo i punti 4 e 5 della sezione 5.5.3.5 e creare index.txt e serial.txt eseguendo i punti 12 e 13 nella cartella **CommserverCertificate**.
9. Nella cartella CommServerCertificate sono presenti cinque file
 - a. openssl-server.cnf
 - b. openssl-ca.cnf
 - c. index.txt
 - d. serial.txt
 - e. 4SightV2PublicKey.cer

10. Aprire il prompt dei comandi con privilegi di amministratore.

Portarsi nella cartella `CommserverCertificate` eseguendo il comando indicato di seguito:

cd "<<percorso completo verso CommserverCertificate >>"

11. Eseguire il comando di seguito per generare i file `cacert.pem` e `cakey.pem`.
openssl req -x509 -config openssl-ca.cnf -newkey rsa:4096 -sha256 -nodes -out cacert.pem -outform PEM
 Quando richiesto, immettere i dati del certificato, per esempio paese, stato ecc.
12. Modificare il contenuto dei file nella cartella `CommserverCertificate` eseguendo il punto 1 della sezione 5.5.3.6.
13. Eseguire i punti da 7 a 11 della sezione 5.5.3.6.
14. Ora è necessario importare la chiave pubblica `4sight` nel `cacert` del server delle comunicazioni per l'autenticazione delle comunicazioni; per farlo eseguire il comando di seguito:
keytool -import -noprompt -trustcacerts -alias <<nome host server 4sight>> -storepass changeit -keystore "C:\Program Files\Druck\DruckCommsServer\<< versione Communication Service >>\cacerts" -file 4SightV2PublicKey.cer
15. Al termine sono presenti `DruckCommServer.pfx` e `CommServer.jks` nella cartella `CommserverCertificate` corrente.
 Copiare i file e incollarli nella directory `"C:\Program Files\Druck\DruckCommsServer\<< versione Communication Service >>\"`. Modificare `application.properties` dalla stessa posizione. Modificare il valore della proprietà come indicato di seguito
 - a. **Keystore = CommServer.jks**
 - b. **key-store.password = <<KeystorePassword>>**
 - c. **key-store.type=JKS**

5.5.3.7.1 Installazione del certificato in Windows per DruckCommsServer

1. Aprire Esegui ed immettere "mmc", quindi premere Invio.
2. Portarsi in File e selezionare Aggiungi/rimuovi snap-in.
3. Dal menu sul lato sinistro selezionare i certificati. Premere Aggiungi, quindi selezionare Account computer >> Avanti >> Fine. Quindi fare clic su Ok.
4. Espandere la sezione relativa ai certificati (Computer locale). Espandere Autorità di certificazione root affidabili.
 Fare clic con il tasto destro sulla cartella Certificates >> Tutte le attività >> Importa.
 Selezionare `cacert.pem` >> avanti >> fine.
 L'autorità CA personalizzata è stata installata correttamente con autorità affidabile.

Dopo avere effettuato la procedura, avviare il servizio `DruckCommsServer`.

Se si desidera semplicemente controllare l'avvenuta conversione di `DruckCommsServer` in `https`, nella scheda Google Chrome aprire il collegamento di seguito: **`https://localhost:9443/api/devicemanager/version`** (inserire il numero di porta del server di comunicazioni, se è stato modificato, il valore predefinito è 9443)

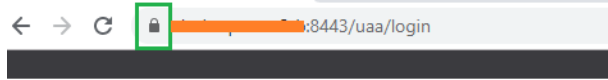
5.5.3.8 Convalida del certificato in 4Sight2

1. Riavviare il PC server.
2. Riavviare i servizi `4Sight2` e `DruckCommsServer` da Windows Services Open
3. Aprire Google Chrome, cancellare la cache del browser e riavviare Google Chrome. Verificare che non siano in esecuzione altre istanze di Google Chrome.
4. Immettere l'URL di seguito nella barra dell'indirizzo e premere Invio.
`Https://<<nome host server>>:8443/4sight2.`

Nota: nell'URL precedente è necessario utilizzare il nome host

- Viene visualizzata la schermata di accesso con l'URL https corretto.

Nota: l'errore rosso è scomparso dalla barra dell'indirizzo. Se il collegamento non è ancora protetto, riavviare il computer e portarsi al punto 3.



Domande frequenti sull'installazione di 4Sight2

6. Domande frequenti sull'installazione di 4Sight2

6.1 Impostazione e installazione

Domanda 1: Ho un'organizzazione in più siti in diverse regioni del mondo. Qual è il modo migliore di impostare 4Sight2?

Risposta: Dipende da come sono mantenuti e gestiti i siti. Se tutti i siti sono mantenuti e gestiti da un hub IT centrale, è possibile installare centralmente singole licenze 4Sight2. Tutti i siti possono accedere a 4Sight2 mediante la rete o LAN. D'altra parte, se sono presenti succursali separate gestite singolarmente, è possibile acquistare più licenze 4Sight2.

Domanda 2: Se acquisto più licenze 4Sight2, queste comunicano tra di loro?

Risposta: No. Ciascuna licenza 4Sight2 è un software diverso isolato con la propria installazione e il proprio database di applicazione. Non esiste comunicazione tra installazioni diverse. Per ulteriori chiarimenti o per discutere di requisiti speciali, rivolgersi al team di 4Sight2.

Domanda 3: Come posso scaricare 4Sight2?

Risposta: È possibile scaricare facilmente 4Sight2 dal sito Web dell'azienda. Di seguito si trova il collegamento.

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

Oppure

È possibile rivolgersi agli uffici vendite ed emettere un ordine di acquisto. Si riceve quindi la versione demo su un dispositivo USB.

Domanda 4: È possibile installare 4Sight2 su un sistema operativo non Windows?

Risposta: No. 4Sight2 è supportato solo per la piattaforma Windows.

Domanda 5: Ho scaricato e installato 4Sight2. Come posso accedere a 4Sight2?

Risposta: 4Sight2 è un software basato sul Web. Di conseguenza sul desktop o nel computer in cui si installa 4Sight2 non vengono generate icone. Per accedere a 4Sight2,

- aprire Google Chrome, incollare l'URL di seguito nella barra degli indirizzi e premere Invio.
- Se 4Sight2 è installato sullo stesso computer, utilizzare `http://localhost:<numero_porta_applicazione>/4sight2`. Se 4Sight2 è installato su un computer diverso nella stessa rete, utilizzare `http://<Nome computer O indirizzo IP>:<numero_porta_applicazione>/4sight2`
- Creare un Preferito in Google Chrome per riferimenti futuri.

Domanda 6: Il programma di installazione di 4Sight2 non riesce a individuare i file del database Postgres

Verificare che il programma di installazione sia stato estratto in un percorso locale e che l'eseguibile venga avviato dalla cartella Disk 1. Verificare che il nome del percorso locale nel quale è stato estratto il programma di installazione non sia lungo poiché questo potrebbe impedire di trovare i file prerequisiti del programma di installazione.

Domanda 7: Cosa accade se il processo viene annullato in qualsiasi fase durante l'aggiornamento?

Risposta: Se in qualsiasi momento l'amministratore annulla il processo di aggiornamento, questo viene riportato alla versione 1.4 e dovrebbe funzionare correttamente. Per effettuare correttamente l'aggiornamento, l'amministratore deve avviare nuovamente il processo di aggiornamento.

Domanda 8: Durante l'installazione dell'applicazione 4Sight2, l'utente riceve il messaggio "Immettere un numero di porta valido. Per conoscere i numeri di porta validi consultare il manuale di installazione"

Risposta: Di seguito si trova l'intervallo di porte non valide, per proseguire con l'installazione scegliere una porta valida

- Le porte da 0 a 1024 sono riservate per la connessione TCP
- Elenco delle porte non sicure: 2049, 3659, 4045, 6000, 6665-6669, 65535

Domanda 9: 4Sight2 con https non funziona nel sistema

Risposta: Rispettare la sintassi del nome di dominio del computer in cui deve essere installata l'applicazione 4Sight2

<dominio> ::= <sottodominio>

<sottodominio> ::= <etichetta> | <sottodominio> "." <etichetta>

<etichetta> ::= <lettera> [[<ldh-str>] <let-dig>]

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

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

<let-dig> ::= <lettera> | <cifra>

<lettera> ::= uno dei 52 caratteri alfabetici da A a Z in

maiuscolo e da a a z in minuscolo

<cifra> ::= una delle dieci cifre da 0 a 9

Nota: nei nomi di dominio sono consentite lettere maiuscole e minuscole. Due nomi con le stesse lettere ma maiuscole e minuscole diverse sono trattati come identici.

6.2 Domande frequenti sul comunicatore dell'apparecchiatura di prova

Domanda 1: Ho completato tutti i passaggi presenti nel manuale di installazione e non vedo ancora il dispositivo nell'elenco.

Risposta: Se l'apparecchiatura di prova non è ancora visibile nell'elenco dopo avere effettuato la procedura, installare nuovamente i driver di 4Sight2. Per farlo, portarsi in **Pannello di controllo >> Programmi e funzionalità** e disinstallare DruckCommsServer dall'elenco. Installare nuovamente il comunicatore dell'apparecchiatura di prova.

Domanda 2: Ricevo un errore "**Nessun dispositivo trovato**"

Risposta: Per risolvere il problema:

- Verificare che il collegamento fisico del dispositivo mediante cavo USB sia corretto. Per verificarlo, portarsi in Gestione dispositivi e individuare il dispositivo nell'elenco. Idealmente si dovrebbe trovare il dispositivo nella sezione Dispositivi Universal Serial Bus. Se il dispositivo è

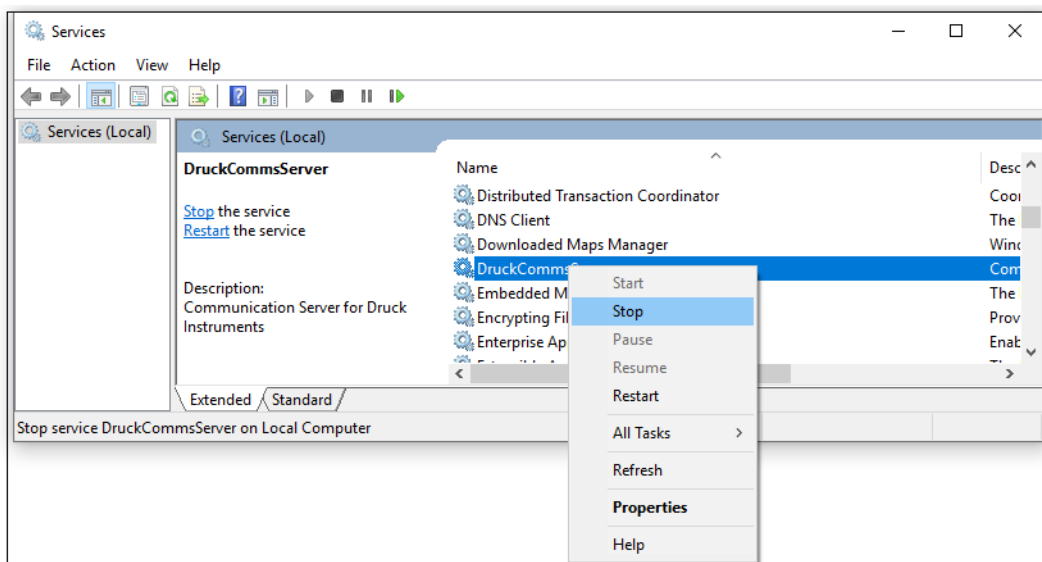
visualizzato in Altri dispositivi, è necessario effettuare le impostazioni indicate sopra per rendere il dispositivo un dispositivo USB.

- Verificare che il dispositivo sia in modalità comunicazione. Vedere il punto 1 sopra.
- Verificare che il percorso del driver sia corretto: C:\Windows\INF... Vedere il punto 2 sopra.

Domanda 3: Ricevo un errore, "**Errore interno del server**" quando faccio clic su **Aggiorna** o quando faccio clic sull'apparecchiatura di prova dall'elenco.

Risposta: Per risolvere il problema,

- Portarsi in Windows Services (noto anche come Services),
- Fare clic con il tasto destro del mouse sul servizio **DruckCommsServer** dall'elenco e fare clic su **Riavvia**.



- Portarsi in 4Sight2 >> Fare clic sul pulsante **Aggiorna**. Nell'elenco dovrebbe essere visualizzato il dispositivo.

Domanda 4: Ricevo un errore, "**Errore di comunicazione**".

Risposta: A volte il software non è in grado di comunicare correttamente con il dispositivo per diversi motivi, quali contatto USB difettoso, dispositivo bloccato, dispositivo occupato nell'effettuazione di altre attività, server occupato in altre attività e così via. Fare nuovamente clic sul pulsante **Aggiorna**: il problema dovrebbe risolversi (provare 2-3 volte)

Tuttavia, se l'errore si presenta spesso, provare a effettuare la procedura di seguito,

- Riavviare il dispositivo (Genii/PACE), verificare che l'operazione possa essere effettuata in sicurezza e che il dispositivo non stia effettuando un'operazione critica. Riprovare. Verificare inoltre che il dispositivo sia ancora fisicamente collegato.

Se la procedura non funziona, seguire le istruzioni al punto 3 sopra e riavviare il servizio **DruckCommsServer**.

Risoluzione dei problemi di installazione

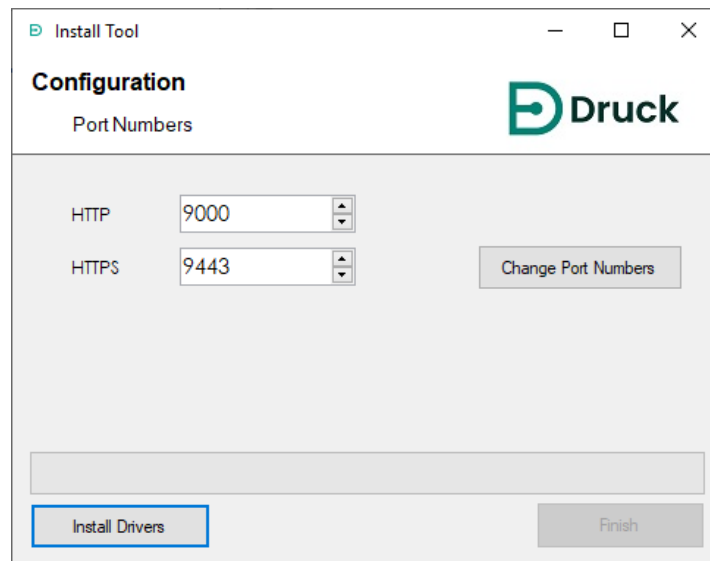
7. Risoluzione dei problemi di installazione

7.1 Problemi di comunicazione dell'apparecchiatura di prova

Utilizzando 4Sight2 per comunicare con un'apparecchiatura di prova, si può rilevare che non viene restituita alcuna apparecchiatura di prova, sebbene si sia verificato che il comunicatore dell'apparecchiatura di prova restituisce la stringa json con una chiamata diretta. Possono essere presenti due problemi principali:

- I numeri di porta sono stati configurati erroneamente. Contattare l'utente amministrativo per sapere quali porte utilizza 4Sight2 per contattare il comunicatore dell'apparecchiatura di prova.

Quando si conoscono le porte da utilizzare, portarsi in C:\Program Files\Druck\DruckCommsServer\[Versione] ed eseguire CommsServerInstallTool.exe



Modificare i numeri di porta e fare clic sul pulsante **Cambia numeri di porta**. Attendere il riavvio del servizio. I numeri di porta sono stati modificati. Selezionare il pulsante **Fine**.

- Il comunicatore dell'apparecchiatura di prova non è configurato per Https, ma 4Sight2 lo è. Contattare l'amministratore e richiedere l'installazione di un certificato autofirmato per il comunicatore dell'apparecchiatura di prova.

7.2 Backup del database Postgres

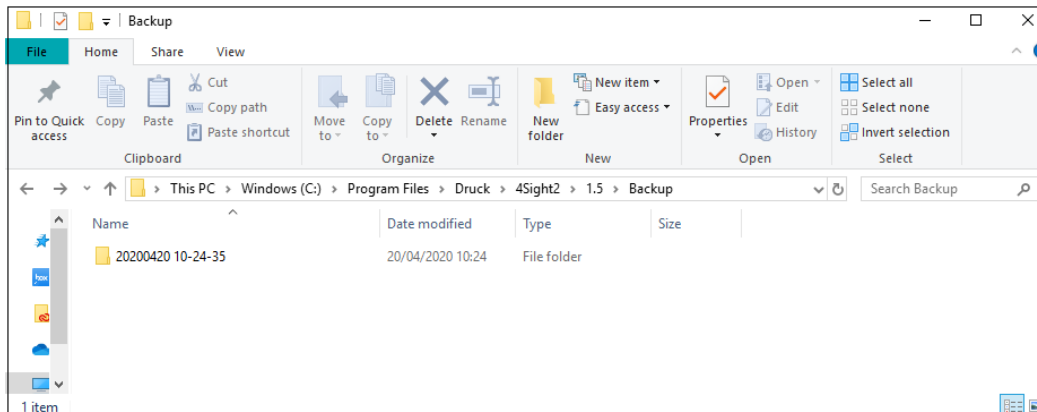
Per informazioni sul backup del database Postgres consultare il manuale utente di 4Sight2 - 123M3138.

7.3 Ripristino del database Postgres

Si presuppone che sia stato effettuato il backup del database utilizzando l'applicazione 4Sight.

L'applicazione 4Sight (versione 1.4 e successive) offre un'interfaccia per l'avvio di un backup (avviato dall'utente/pianificato). L'operazione crea file nella cartella di backup nella directory di installazione di 4Sight sul server. Ciascun backup avviato crea una nuova cartella all'interno della

cartella di backup con il nome nel formato AAAAMMGGHHSS (anno, mese, giorno, ora e secondi), secondo la data e l'ora di completamento corretto del backup.

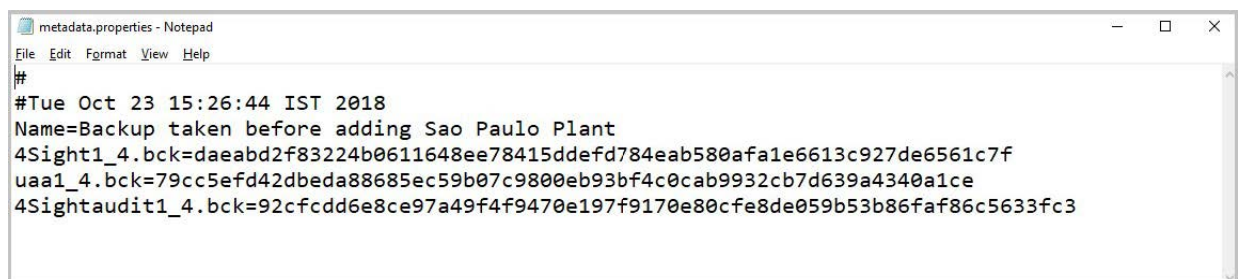


Si consiglia di effettuare il backup dei contenuti della cartella di backup su un supporto separato. Ciascuna cartella contiene 5 file.

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

I file *.bck contengono un suffisso con la versione dell'applicazione 4Sight. Controllare che si stia effettuando il ripristino di un database corrispondente alla versione esatta dell'applicazione. L'applicazione non supporta versioni precedenti o successive del database. Si noti che la versione contiene un carattere di sottolineatura (_) e non un punto (.), ad es. 1_4 e non 1.4. Quando si utilizzano i comandi indicati di seguito nella procedura di ripristino, sostituire <VERSIONE_APPLICAZIONE> con la versione di 4Sight installata.

Il file metadata.properties contiene il nome del backup immesso durante l'avviamento del backup.



Controllo SHA 256

In un backup sono presenti 3 file, uno per ciascun database, con l'estensione .bck. Il file metadata.properties contiene l'algoritmo SHA 256 di ciascun file di backup.

1. Aprire un prompt dei comandi come amministratore e portarsi nella cartella contenente i file di backup selezionati.
2. Utilizzare i comandi di seguito per calcolare l'algoritmo SHA256 di ciascun file


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

- Prima di proseguire con la procedura di ripristino, verificare che l'algoritmo SHA 256 di ciascun file corrisponda all'algoritmo SHA 256 indicato nel file di metadati. Il file di backup è valido per il ripristino se la checksum del prompt dei comandi e la checksum del file di metadati sono identiche. Proseguire con la procedura per il ripristino solo se sono identiche.

7.4 Procedura per il ripristino

- Accedere al server 4Sight come amministratore.
- Trovare la porta su cui è in esecuzione il database Postgres. Si trova nella proprietà `spring.datasource.url` nel file `<DIRECTORY DI INSTALLAZIONE DI 4Sight>\apache-tomcat\webapps\application.properties`. Utilizzare Blocco note eseguito come amministratore per aprire il file. Si tratta del numero appena prima di `4Sight<VERSIONE_APPLICATION>`
- Accedere all'utilità di comando `psql` da un prompt dei comandi eseguito come amministratore, utilizzando l'utente di postgres

```
C:\Program Files\PostgreSQL\11\bin\psql" --port=<PORTA_DB> postgres postgres
```
- L'utente di database utilizzato dall'applicazione si trova nella proprietà `spring.datasource.username` nel file `<DIRECTORY DI INSTALLAZIONE DI 4Sight>\apache-tomcat\webapps\application.properties`. Utilizzare Blocco note eseguito come amministratore per aprire il file.
- Eliminare i database `*_temp`, se presenti, quindi creare i database `*_temp` vuoti eseguendo i comandi di seguito nel prompt `psql`

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

Cambiare il proprietario di database dei tre database indicati sopra in questo utente. Si noti che il nome utente è sensibile alle maiuscole.

```
ALTER DATABASE "4Sight<VERSIONE_APPLICATION>_temp" OWNER TO "<UTENTE_DB>";
ALTER DATABASE "4Sightaudit<VERSIONE_APPLICATION>_temp" OWNER TO "<UTENTE_DB>";
ALTER DATABASE "uaa<VERSIONE_APPLICATION>_temp" OWNER TO "<UTENTE_DB>";
```

- Controllare i file `metadata.properties` dei backup e decidere quale backup si deve ripristinare.
- Aprire un altro prompt dei comandi come amministratore e portarsi nella cartella contenente i file di backup selezionati.

Ripristinare il database dai file `*.bck` nei database `*_temp` utilizzando i comandi indicati di seguito. Se viene richiesta una password, immettere la password dell'utente con privilegi avanzati.

```
"C:\Program Files\PostgreSQL\11\bin\pg_restore" --port=<PORTA_DB> --no-owner --
username=postgres --dbname=4Sight<VERSIONE_APPLICAZIONE>_temp -n public --
role=<UTENTE_DB> 4Sight<VERSIONE_APPLICAZIONE>.bck
```

```
"C:\Program Files\PostgreSQL\11\bin\pg_restore" --port=<PORTA_DB> --no-owner --
username=postgres --dbname=4Sightaudit<VERSIONE_APPLICAZIONE>_temp -n public --
role=<UTENTE_DB> 4Sightaudit<VERSIONE_APPLICAZIONE>.bck
```

```
"C:\Program Files\PostgreSQL\11\bin\pg_restore" --port=<PORTA_DB> --no-owner --
username=postgres --dbname=uaa<VERSIONE_APPLICAZIONE>_temp -n public --
role=<UTENTE_DB> uaa<VERSIONE_APPLICAZIONE>.bck
```

8. Eliminare i database *_old, se presenti, eseguendo i comandi di seguito nel prompt psql


```
DROP DATABASE IF EXISTS "4Sight<VERSIONE_APPLICAZIONE>_old";
DROP DATABASE IF EXISTS "4Sightaudit<VERSIONE_APPLICAZIONE>_old";
DROP DATABASE IF EXISTS "uaa<VERSIONE_APPLICAZIONE>_old";
```
9. Arrestare le applicazioni di servizio 4Sight e pgadmin, se sono aperte.
10. Rinominare database 4Sight esistenti in *_old eseguendo i comandi di seguito nel prompt psql.


```
ALTER DATABASE "4Sight<VERSIONE_APPLICAZIONE>" RENAME TO
"4Sight<VERSIONE_APPLICAZIONE>_old";
ALTER DATABASE "4Sightaudit<VERSIONE_APPLICAZIONE>" RENAME TO
"4Sightaudit<VERSIONE_APPLICAZIONE>_old";
ALTER DATABASE "uaa<VERSIONE_APPLICAZIONE>" RENAME TO
"uaa<VERSIONE_APPLICAZIONE>_old";
```
11. Rinominare i database *_temp in database 4Sight eseguendo i comandi di seguito nel prompt psql.


```
ALTER DATABASE "4Sight<VERSIONE_APPLICAZIONE>_temp" RENAME TO
"4Sight<VERSIONE_APPLICAZIONE>";
ALTER DATABASE "4Sightaudit<VERSIONE_APPLICAZIONE>_temp" RENAME TO
"4Sightaudit<VERSIONE_APPLICAZIONE>";
ALTER DATABASE "uaa<VERSIONE_APPLICAZIONE>_temp" RENAME TO
"uaa<VERSIONE_APPLICAZIONE>";
```
12. Avviare il servizio 4Sight e provare ad accedere come amministratore. Si noti che per effettuare l'accesso deve essere utilizzata la password dell'amministratore al momento dell'effettuazione del backup.

7.5 Procedura di ripristino in seguito a un arresto anomalo di un computer 4Sight2

Presupposti: l'utente ha eseguito un backup del database 4Sight2 prima dell'arresto anomalo. L'utente conosce già il nome utente e la password sia per l'applicazione sia per il database.

1. Configurare il computer con il sistema operativo e i driver di supporto.
2. Installare 4Sight2 sul computer.

3. Durante l'installazione dell'applicazione, specificare lo stesso nome utente e password utilizzati in precedenza per l'applicazione e il database Postgres.

4Sight2 V1.5.0.16652 - InstallShield Wizard

Existing PostgreSQL 11 Database Details

PostgreSQL Installation Directory

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

PostgreSQL Port number

Port: 5432

Please provide password for the database super user (postgres)

Password: []

InstallShield

< Back Next > Cancel

Stessa password dell'installazione precedente

4Sight2 V1.5.0.17177 - InstallShield Wizard

Application Details

Enter 4Sight2 Application User Information

User ID: []

Password: []

Confirm Password: []

Email: []

Enter Database User Information

Use Default User ID/Password Show Password

User ID: 4Sight2Admin

Password: []

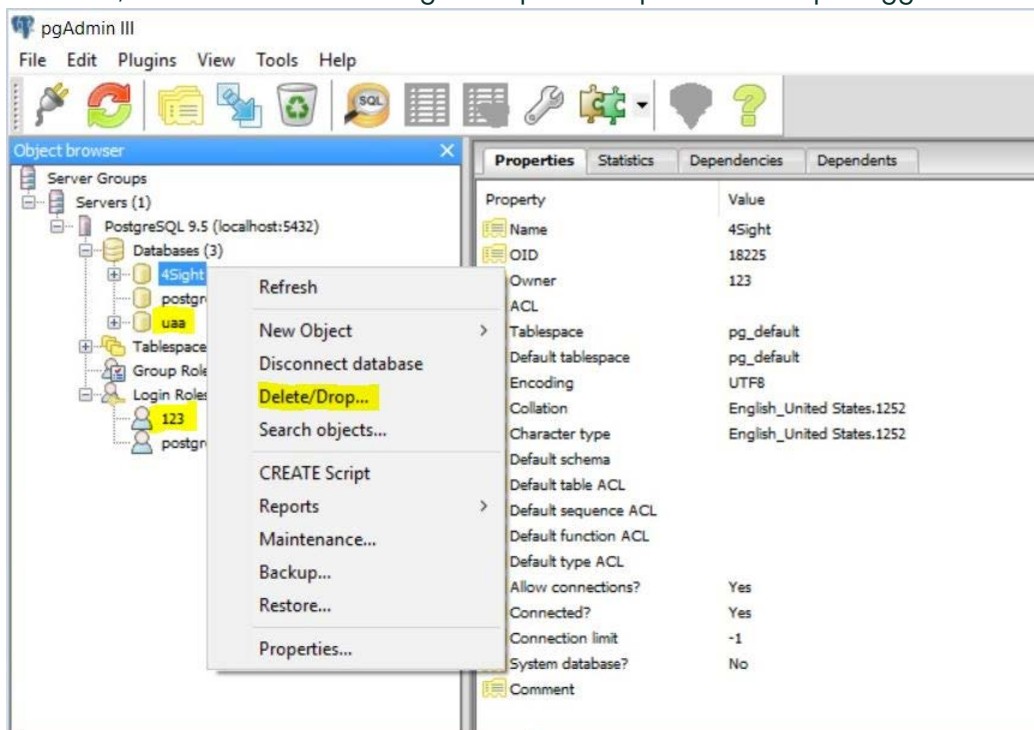
Confirm Password: []

InstallShield

< Back Next > Cancel

Compilare tutti i campi come nell'installazione precedente

- Una volta installata l'applicazione, eliminare il database predefinito creato durante l'installazione dell'applicazione da pgAdmin (fare clic con il pulsante destro del mouse sul database e selezionare Elimina/Rilascia). Se viene visualizzato un errore durante l'eliminazione del database, riavviare il servizio Postgres e ripetere la procedura dopo l'aggiornamento.



- Dopo l'eliminazione del database e dell'utente, attenersi alla procedura riportata di seguito per ripristinare il database come indicato in precedenza dal prompt dei comandi.
- Il database è stato correttamente ripristinato, aprire l'applicazione dal browser e verificare.

7.6 Installazione non riuscita

La tabella di seguito spiega le diverse possibilità di errore durante l'installazione e le relative azioni correttive.

Messaggio di errore	Scenario	Rimedio/azione da intraprendere
"Insufficient disk space available to install 4Sight2 application. Please ensure a minimum of 4096 MB is available. Free Space : available MB."	Errore causato da problema del disco fisso (non è presente lo spazio necessario all'inizio dell'aggiornamento)	L'amministratore deve liberare spazio nel relativo disco ed effettuare nuovamente la procedura di aggiornamento.
"Deployment fail while Migrating database"	Errore causato da problema del disco fisso (non è presente spazio sufficiente dopo l'aggiornamento effettuato correttamente)	L'amministratore deve liberare spazio nel relativo disco ed effettuare nuovamente la procedura di aggiornamento.

Messaggio di errore	Scenario	Rimedio/azione da intraprendere
"Installation failed while migrating Database. Please reinstall 4sight2"	Errore di integrità dei dati durante la copia del database	In questo caso l'amministratore deve rivolgersi all'assistenza clienti. Motivo dell'integrità dei dati inserito nei registri nella posizione [C:\Users\[Nome utente]\AppData\Local\Temp\logs]
"Installation failed while migrating Database. Please reinstall 4sight2"	Errore a causa di integrità dei dati nella fase di aggiornamento dello schema	In questo caso l'amministratore deve rivolgersi all'assistenza clienti. Motivo dell'integrità dei dati inserito nei registri nella posizione 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"	Questo errore si verifica se il programma di installazione non è in grado di ottenere lo stato del servizio.	L'amministratore deve verificare che il servizio 4Sight2 sia in esecuzione.
"Failed to start the 4Sight2 service. Please ensure the 4Sight2 service is present and running"	Errore se l'applicazione è danneggiata, alcuni file sono stati eliminati, la porta è utilizzata da un'altra applicazione, l'utente ha arrestato il servizio ecc.	Se l'amministratore riesce a ottenere lo stato del servizio e se non è in esecuzione per qualche motivo (ad es. applicazione danneggiata, alcuni file sono stati eliminati, la porta è utilizzata da un'altra applicazione, l'utente ha arrestato il servizio ecc.), il sistema cerca di avviare il servizio. Se non è possibile avviare il servizio, l'amministratore deve rivolgersi all'assistenza clienti per risolvere il problema.
"Upgrade of 4Sight2 application is supported from version 1.3 onwards. For earlier version upgrade support please contact Customer Care."	L'aggiornamento non viene effettuato se è installata una versione precedente alla versione 1.3.	L'aggiornamento è possibile solo per la versione 1.3 e successive.
Installer has detected another minor version of PostgreSQL 11. Installer will not continue. Refer to 4Sight2 Installation manual for more details	4Sight2 non è in grado di proseguire l'installazione di 4Sight2 poiché sul computer di destinazione esiste la stessa versione (variante) di PostgreSQL	Opzioni possibili 1. L'utente può scegliere un altro computer 2. L'utente effettua un backup dell'applicazione esistente che utilizza Postgres versione 11.3, disinstalla e distribuisce tale applicazione su un altro computer. Disinstallare Postgres e riavviare l'installazione di 4Sight2

Messaggio di errore	Scenario	Rimedio/azione da intraprendere
Installation failed while upgrading database. Please reinstall 4Sight2. Refer to 4Sight2 Installation manual for more details	Si possono essere verificati alcuni errori interni durante l'aggiornamento, l'utente può ritentare l'installazione	Se il problema persiste, l'utente può condividere i registri di installazione per una migliore comprensione del problema

7.7 Cause generali di errore

Di seguito si trovano alcuni problemi comuni associati alla comunicazione di 4sight2 con l'apparecchiatura Druck mediante USB.

- Il collegamento fisico è allentato o instabile
- Cavi/porte usurati
- Adattatori USB di qualità scadente
- Adattatori/porte USB sovraccarichi
- I dispositivi sono stati in funzione per un lungo tempo e si sono portati in modalità di sospensione
- I dispositivi non sono in modalità di comunicazione
- Software del driver non installato o non aggiornato. Per stabilire la comunicazione con l'hardware è necessaria la stessa versione dell'applicazione 4Sight2 e dei driver.
- Nei dispositivi sono installate versioni di firmware molto datate.

7.8 Disinstallazione di 4Sight2

Attenersi alle istruzioni di seguito se è necessaria l'installazione di una nuova copia di 4Sight2, di una nuova versione di 4Sight2 oppure è necessario disinstallare 4Sight2 a causa di problemi durante l'installazione.



La disinstallazione del componente database PostgreSQL elimina il database 4Sight2 e causa la perdita di dati. La procedura di seguito non crea automaticamente un backup, quindi verificare di avere creato un backup manuale prima di procedere e di avere salvato tale backup in una posizione alternativa nella cartella di installazione di 4Sight2. Consultare la sezione relativa a backup e ripristino del database Postgres del presente manuale.

Se si sceglie di disinstallare solo l'applicazione 4Sight2 e mantenere il database, consultare la parte relativa all'installazione di 4Sight2 del presente manuale. Durante la nuova installazione saranno necessarie le credenziali per l'utente con privilegi avanzati del database. Non cercare di effettuare la disinstallazione se non si dispone di tali credenziali.

Se si desidera effettuare l'aggiornamento della versione di 4Sight2 senza disinstallare il database, **NON** effettuare la procedura di seguito.

1. Portarsi in Pannello di controllo >> Programmi e funzionalità
2. Fare clic con il tasto destro del mouse su 4Sight2 e selezionare Disinstalla.
3. Seguire le istruzioni della procedura guidata di disinstallazione.
4. Fare clic con il tasto destro del mouse su PostgreSQL 11 e selezionare Disinstalla.
5. Seguire le istruzioni della procedura guidata di disinstallazione.
6. La disinstallazione di PostgreSQL non elimina la cartella dei dati. Tale operazione deve essere effettuata manualmente. Eliminare la cartella dei dati, in C:\Program Files\PostgreSQL\11\
 - a. Se si desidera eliminare l'intera cartella PostgreSQL, prima di procedere verificare che tutti i file di backup e gli script siano spostati dalla cartella cestino
 - b. Per impostazione predefinita, i backup del database 4Sight2 vengono creati e salvati nella posizione indicata di seguito: C:\Program Files\PostgreSQL\11\bin
7. Si consiglia di riavviare il computer, se possibile.
8. 4Sight2 è stato disinstallato correttamente.

7.9 Risoluzione dei problemi per le comunicazioni protette

1. Il comando "nome comando" non viene riconosciuto come comando interno o esterno. Per esempio, "keytool" non viene riconosciuto come comando interno o esterno.
- Se si verifica un errore simile, significa che il prompt dei comandi non è in grado di trovare riferimenti al comando specificato nella cartella in cui ci si trova.

Per risolvere il problema, utilizzare il comando di seguito per puntare alla cartella corretta.

Set Path=%Path%;"<<percorso completo della posizione in cui si trova il comando>>"

Per esempio, nell'errore precedente relativo a keytool, è necessario impostare il comando come di seguito,

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

2. Indirizzo IP errato

- Se si riceve un messaggio di errore con questo testo, significa che l'indirizzo IP o il nome host nei file `openssl-ca.cnf` o `openssl-server.cnf` sono errati. Nota: può essere necessario effettuare la correzione in più punti nei file ed eseguire nuovamente i passaggi.

3. Nessun file o directory...

- Se si riceve un messaggio di errore con questo testo, significa che probabilmente il comando eseguito fa riferimento a un nome di file non corretto. Controllare il comando alla ricerca di eventuali errori nei nomi di file e controllare che il file con tale nome sia presente nella cartella, quindi eseguire nuovamente i comandi. Può essere necessario correggere il nome di file nel comando o attenersi alla procedura per generare i file mancanti.
- Questo errore si può verificare per i file `index.txt` e `serial.txt` perché in alcuni casi l'estensione di file viene aggiunta due volte al nome, per esempio `index.txt.txt`.

Modificare il file e salvarlo senza l'estensione `.txt`. Verificare che il file abbia una sola estensione `.txt`.

Procedure consigliate

8. Procedure consigliate

Hardening del server

L'hardening dell'ambiente server deve essere conforme alle linee guida di Microsoft o CIS.

8.1 Tomcat

- Installare Tomcat in una cartella protetta cui abbiano accesso solo gli utenti Ammin o LocalService, come `C:\Programmi (x86)`.
- Installare Tomcat come servizio in esecuzione nell'account LocalService.
- Rimuovere tutto da WebApp, incluse le applicazioni predefinite indesiderate.
- Sostituire la pagina di errore predefinita, ad esempio 404, 403, 500 ecc.
- Applicare HTTPS, abilitare SSL.
- L'applicazione di gestione deve essere eseguita su SSL.
- Utilizzare singoli file di registro per ciascuna applicazione Web.
- Rimuovere il banner del server.
- Abilitare la registrazione dell'accesso.
- Cambiare la porta e il comando di arresto.

8.2 PostgreSQL

- Tutti gli account con privilegi elevati come pgdba, postgres, depez devono essere accessibili solo in locale.
- Verificare la correttezza della sequenza nel file `pg-hba.conf` in modo tale che il diritto di accesso venga assegnato agli utenti corretti.
- Configurare il file `pg-hba.conf` in modo tale che sia possibile connettere il server solo dal computer locale e non attraverso la rete.

8.3 Procedure consigliate per i firewall

Di seguito vengono riportate alcune delle procedure consigliate per i firewall da utilizzare con 4Sight2:

8.3.1 Policy

1. La configurazione dei firewall deve essere coerente con la policy di sicurezza dell'organizzazione.
2. Utilizzare sempre la policy sui privilegi minimi. Rifiutare tutto per impostazione predefinita. Consentire traffico specifico (utilizzando sorgente, destinazione e porta).
3. Inserire regole specifiche e utilizzare regole di eliminazione esplicite.
4. Registrare tutte le azioni, in particolare i tentativi di audit trail non riusciti.

8.3.2 Risorse

1. Monitorare l'utilizzo della memoria.
2. Monitorare l'utilizzo della CPU.
3. Monitorare l'utilizzo della larghezza di banda.
4. Limitare il numero di applicazioni in esecuzione sul computer firewall.

8.3.3 Installazione e manutenzione

1. Limitare l'accesso fisico al computer firewall.
2. Utilizzare l'ID utente univoco per l'amministrazione.
3. Attenersi ai rigorosi criteri di account sul computer.
4. Installare regolarmente patch su sistemi operativi, software applicativo, firmware ecc.
5. Archiviare regolarmente base di regole, configurazione e registri. Documentare tutte le regole e le modifiche apportate in un controllo del codice sorgente.
6. Eseguire test periodici.
7. Rimuovere la regola inutilizzata quando viene eseguita la rimozione delle autorizzazioni per il servizio.
8. Controllare e rivedere le regole a intervalli regolari.
9. Monitorare gli avvisi di sicurezza a intervalli regolari.

8.3.4 Sicurezza avanzata

1. Utilizzare ispezioni con stato.
2. Utilizzare Proxy.
3. Utilizzare l'ispezione e il filtraggio a livello di applicazione.

8.3.5 Protezione interna

1. Disporre di criteri di utilizzo accettabili.
2. Utilizzare un firewall personale per ciascun utente.
3. Utilizzare sistemi di prevenzione delle intrusioni basati su host.
4. Eseguire il monitoraggio della rete.
5. Eseguire il filtraggio dei contenuti.
6. Abilitare il controllo dell'accesso su ogni computer e applicazione.

Sedi degli uffici

Sedi centrali

Leicester, GB

Telefono: +44 (0) 116 2317233

Email: gb.sensing.sales@bakerhughes.com

Australia

Springfield Central

Telefono: 1300 171 502

E-mail: custcare.au@ge.com

Cina

Guangzhou

Telefono: +86 173 1081 7703

Email: dehou.zhang@bakerhughes.com

Cina

Pechino

Telefono: +86 180 1929 3751

Email: fan.kai@bakerhughes.com

Cina

Shanghai

Telefono +86 135 6492 6586

Email: hensenzhang@bakerhughes.com

EAU

Abu Dhabi

Telefono: +971 528007351

Email: suhel.aboobacker@bakerhughes.com

Francia

Tolosa

Telefono: +33 562 888 250

Email: sensing.FR.cc@bakerhughes.com

Germania

Francoforte

Telefono: +49 (0) 69-22222-973

Email: sensing.de.cc@bakerhughes.com

Giappone

Tokyo

Telefono: +81 3 6890 4538

Email: gesitj@bakerhughes.com

India

Bangalore

Telefono: +91 9986024426

Email: aneesh.madhav@bakerhughes.com

Italia

Milano

Telefono: +39 02 36 04 28 42

Email: csd.italia@bakerhughes.com

Paesi Bassi

Hoevelaken

Telefono: +31 334678950

Email: nl.sensing.sales@bakerhughes.com

Russia

Mosca

Telefono: +7 915 3161487

Email: aleksey.khamov@bakerhughes.com

USA

Boston

Telefono: 1-800-833-9438

E-mail: custcareboston@bhge.com

Sedi di servizi e assistenza

Supporto tecnico

Globale

Email: mstechsupport@bakerhughes.com

Brasile

Campinas

Telefono: +55 11 3958 0098, +55 19 2104 6983

Email: mcs.services@bakerhughes.com

Cina

Changzhou

Telefono: +86 400 818 1099

Email: service.mcchina@bakerhughes.com

EAU

Abu Dhabi

Telefono: +971 2 4079381

Email: gulfservices@bakerhughes.com

Francia

Tolosa

Telefono: +33 562 888 250

Email: sensing.FR.cc@bakerhughes.com

Giappone

Tokio

Telefono: +81 3 3531 8711

Email: service.druck.jp@bakerhughes.com

India

Pune

Telefono: +91 213 5620426

Email:

mcsindia.inhouseservice@bakerhughes.com

Regno Unito

Leicester

Telefono: +44 (0) 116 2317107

Email: sensing.grobycc@bakerhughes.com

USA

Billerica

Telefono: +1 (281) 542-3650

Email: namservice@bakerhughes.com