BAKER HUGHES
a GE company

4Sight™ 2

Calibration Management Software

123M3141 Deployment Guide Revision B

Table of Contents

Introduction

Overview

4Sight™ 2 is a calibration management system. The application helps in the following

- Capture the devices information along with the plant and locations inside the enterprise.
- Detail information about the devices, such as serial number, related standard operation procedural documents and manuals. The tag number of an asset is used to indicate where the device is positioned within a location or department
- It also keeps the detail information about the calibrators, such as serial number, when they themselves last calibrated, company and model.
- It helps in developing the Test Procedure for testing these devices.
- It also helps in scheduling these procedure based on the user or asset requirement on which it is placed.
- Storage of calibration data which can be graphically displayed for analysis and used to generate a calibration certificate for audit purposes.

Target Audience

The application is targeted to typically 4 kinds of 4Sight™ 2 roles (and not Windows Groups or Accounts):

Administrators

Administrators are responsible for installation and configuration of the 4Sight™ 2 server. When 4Sight™ 2 server is installed they will have only administrator account. Further administrator will create various groups, users and assign users to group. If required administrators will assign granular permissions to each group or user.

Supervisor

Supervisor is responsible for the calibration management of a plant or number of plants. They are responsible for creating the device information and linking related documentation, such as plant processes or device datasheets, that will assist in the calibration of devices.

They will create the test procedures to be used during calibration, schedule and monitor the health of the devices and approve calibration results.

Technicians

Technicians are responsible for performing the calibration. Calibrations can be performed manually or by downloading a procedure onto a supported portable calibrator. Once the procedure has been downloaded the calibrator is connected to the device to perform the calibration and automatically collate and store the results ready for upload.

For devices, which need to be calibrated manually or using an unsupported 3rd party calibrator, the technician will perform a manual calibration and enter the viewed results.

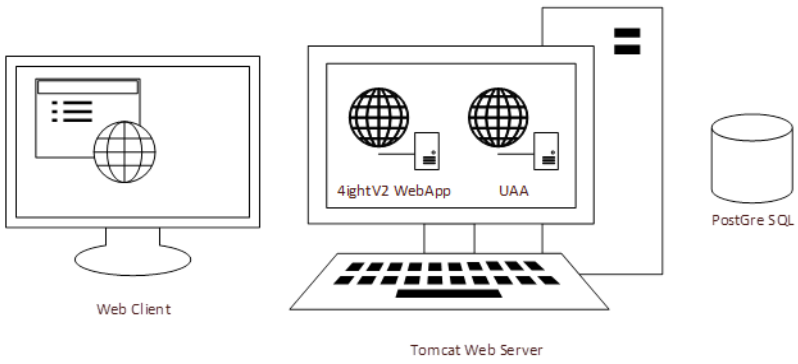
After each calibration, the technician will analyses the results and complete the calibration, providing comments where required, and send the calibration results to the supervisor for approval.

Auditor

They are responsible for auditing the report. In some plant it is mandatory to conduct the audit as a regulatory requirement.

Deployment Architecture

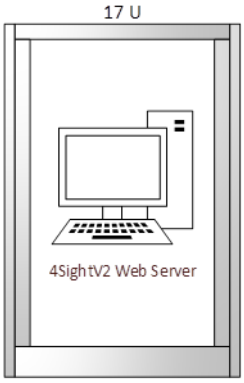
Architecture



Typical architecture include 4Sight™ 2 web application and UAA (User Authentication and Authorization) server running inside the Tomcat Web Server with the PostgreSQL database running on the same machine.

The Browser Client Web Application will connect to the 4Sight™ 2server which in turn stores and retrieves the information from the PostgreSQL database.

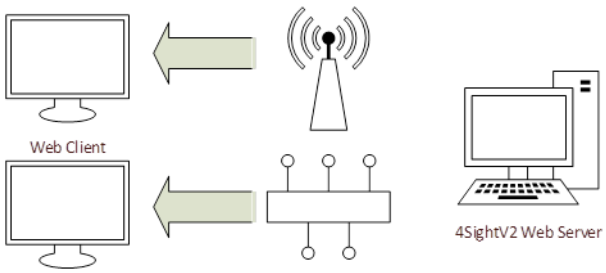
Physical Deployment



We assume that the user installing 4Sight™ 2 has Cyber Security Measures already in place meeting the user security policies, including the following:

- The server is placed in a secure location with physical limited access control.
- Server access control is protected with limited authorize access.
- Server network is protected with the firewall to allow limited access to the well-known applications only on known ports
- The applications run in their own context and have access to database and file systems in their own folder only.

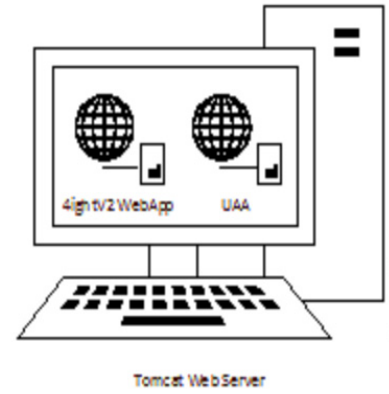
Network



The clients are connected using Web Browsers, either through Ethernet connections or via a wireless network. There could be potential latency on the wireless network depending on the wireless bandwidth and number of devices connected.

It is advisable to disable or remove any browser plugins and extensions installed on the browser

Hardware Requirement



Server Requirement

CPU	Quad Core
Ram	8 GB (32 GB Recommended)
Hard disk	1 TB
Network Speed.	10 Mbps
Operating Systems	Windows 2012 (R2) – Recommended Windows Server 2008 R2
Web Server	Tomcat Server
Database Server	Postgres 9.5

Client Requirement

CPU	Dual Core
RAM	4 GB (8 GB recommended)
Hard disk.	600 GB
Network Speed	10 Mbps
Browser	Google Chrome V58+

Deployment Sequence

PostgreSQL, Tomcat and Java Runtime is prerequisite to the application. PostgreSQL is installed as a separate package while others are package along with the application. So if PostgreSQL is already installed on the user machine then we just need Superuser password to connect and configure it.

The installation requires Windows administrator rights on the machine. Before the installation, the user must have the PostgreSQL superuser password. The Application administrator username & password and Database username & password.

PostGreSQL superuser password is required for creating the database and other structures inside the PostGreSQL server. The Application administrator is the first user of application. He is responsible for creating other users and assigning them different role. The Database user has access to 4Sight™ 2 and UAA database. This username credentials are used for accessing the database.

The application is published on machine port. Default port is 8080, and user can change the port at the time of installation or later. The default application context in Tomcat is 4Sight™ 2.

Follow the Operating System hardening procedure as per Microsoft or CIS guidelines to hardened the OS. The installation procedure will guide to install PostGreSql before installing the 4Sight™ 2 server.

The device drivers are installed on the client machines where we are connecting the portable calibrator using USB ports. If driver is not already installed on the machine, the user is prompted to download the driver from the 4Sight™ 2 server and install it on the machine. The device driver also install a Device Manager service to which the browser client communicates for uploading and downloading the data onto the portable calibrator. The device manager listen to port 9000 and can only communicate on secure layer.

Post-Deployment Tasks

Adding User and Groups

The administrator is responsible for creating different users like Supervisor, Senior Technician, Technician, and Auditor in the application. The administrator can assign them to different built-in default groups. If more control or finer granularity of access is required then administrator can create custom groups and assign specific access to them.

Default passwords

We are using the hardcoded default password for tomcat user in the file "C:\Program Files (x86)\GE Measurement & Sensing\4Sight2\apache-tomcat\conf\tomcat-users.xml".

It is recommended to change the default password and to always use a password which adheres to password best practices.

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

Best practices have been implemented to ensure this application is secure. To achieve additional security please perform the following tasks:-

The configuration files and folders are protected with only Service and Systems having access rights by default. Therefore before attempting to perform the tasks below, the admin user only has read/write access to the C:\Program Files (x86)\GE Measurement & Sensing\4Sight2\conf folder, so open the command prompt with admin user credentials.

Secure Communication

The 4Sight™ 2 is shipped with HTTP as default but it is recommended to change the communication channel to HTTPS using either the Self Signed Certificate or Third Party Certificate.

Before performing any change, stop the 4Sight2 service using the service control manager (Press Windows **->** Start **->** Run **->** Services.msc). Restart the service once the Certificate installations are complete.

Note: Before service restart, make sure the "Local Service" account has full control on C:\Program Files (x86)\GE Measurement & Sensing\4Sight folder and sub folders.

Creating and Installing Self Signed Certificate

1. *Open the command prompt using run as administrator and change to the folder* ***"C:\Program Files (x86)\GE Measurement & Sensing\4Sight2\apache-tomcat\conf".***
2. Make sure JRE is in the path by running the following command.

   Keytool /?

   If JRE is not in the path then add the folder in the path environment variable.
   "C:\Program Files (x86)\GE Measurement & Sensing\4Sight2\jre-1.8\bin"

   Set ***"Path=%Path%;C:\Program Files (x86)\GE Measurement & Sensing\4Sight2\jre-1.8\bin"***
3. If installing new certificate, go to point 5.
4. Otherwise do the following.

   a. Check if the certificate already exists in the java store.

   keytool -list -alias tomcat -storepass <<Password>> -keystore 4Sight.jks

   b. If it is already installed then remove it.

   keytool -delete -noprompt -alias tomcat -storepass <<Password>> -keystore 4Sight.jks

   c. Check and delete if the file 4SightV2PublicKey.cer exists.

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

   d. Check if the certificate already exist in cacert of java.

   keytool -list -alias tomcat -storepass changeit -keystore "../../jre-1.8/lib/security/cacerts"

   e. If the certificate exists then delete using the following command.

   keytool -delete -noprompt -alias tomcat -storepass changeit -keystore "../../jre-1.8/lib/security/cacerts" -file "../../app/Certificate/4SightV2PublicKey.cer"

   Note: Do not change the name of 4SightV2PublicKey.cer certificate file.
5. Create a new certificate with 2048 bit size using the following command.

   keytool -genkey -trustcacerts -keyalg "RSA" -keysize 2048 -validity 1095 -keypass <<KeyPassword>> -alias tomcat -keystore 4Sight.jks -storepass <<StorePassword>> -dname "CN=%COMPUTERNAME%, OU=<<Organization Unit>>, O=<<Organization>>, L=<<Location>>, S=<<State>>, C=<<Country Initial>>" -ext eku:critical=sa

Note: Keysize (2048) depends on the country permissible limit for PKI encryption.

6. Export the certificate public key to the file 4SightV2PublicKey.cer (Do not change the file name and path).

   keytool -export -alias tomcat -keystore 4Sight.jks -storepass <<Password>> -storetype JKS -file "../../app/Certificate/4SightV2PublicKey.cer"

7. Import the certificate into java CACert file.

   keytool -import -noprompt -trustcacerts -alias tomcat -storepass changeit -keystore "../../jre-1.8/lib/security/cacerts" -file ../../app/Certificate/4SightV2PublicKey.cer

8. Make entry of the certificate into Tomcat configuration file.

   a. Open the file ***"C:\Program Files (x86)\GE Measurement & Sensing\4Sight2\apache-tomcat\conf\server.xml"***

   b. Make the following entry in server.xml.

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

   c. Comment the following section to disable http connections.

```
<Connector port="8080" protocol="HTTP/1.1"
           connectionTimeout="20000"
           redirectPort="8443" />
```

Installing the Third Party Certificate or CA Signed Certificate

1. Open the command prompt *using run as administrator* and change to the folder **"C:\Program Files (x86)\GE Measurement & Sensing\4Sight2\apache-tomcat\conf".**
2. Make sure JRE is in the path by running the following command.

   Keytool /?

   If JRE is not in the path then add the folder in the path environment variable.
   "C:\Program Files (x86)\GE Measurement & Sensing\4Sight2\jre-1.8\bin"

3. Copy the acquired certificate in the conf folder for installation. Make sure acquired certificate contain private key. Replace the **<<*PrivKeyPass*>>** in the following commands with the private key password.

   It is assumed that certificate is in PFX format with the name **<<*CASignCert.pfx*>>**

4. If self signed or any other certificate is already installed then do the following to remove it. Otherwise go to step 5.

   a. Check if the certificate already exists in the java store.

   keytool -list -alias tomcat -storepass <<Password>> -keystore 4Sight.jks

   b. If it is already installed then remove it.

   keytool -delete -noprompt -alias tomcat -storepass <<Password>> -keystore 4Sight.jks

c. Check and delete if the file 4SightV2PublicKey.cer exists.

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

d. Check if the certificate already exists in cacert of java.

keytool -list -alias tomcat -storepass changeit -keystore "../../jre-1.8/lib/security/cacerts"

e. If the certificate exists then delete using the following command.

keytool -delete -noprompt -alias tomcat -storepass changeit -keystore "../../jre-1.8/lib/security/cacerts" -file "../../app/Certificate/4SightV2PublicKey.cer"

Note: *Do not change the name of 4SightV2PublicKey.cer certificate file.*

5. Get the alias inside the PFX Certificate store.

   keytool -v -list -storetype pkcs12 -keystore <<CASignCert.pfx>> -storepass <<PrivKey-Pass>>

   Note: Search for the Alias in the output and use in place ***<<sourceAlias>>*** in the following command.

6. Import the key in Java key store.

   Keytool -importkeystore -trustcacerts -srckeystore <<CASignCert.pfx>> -srcstoretype pkcs12 -srcstorepass <<PrivKeyPass>> -srcalias <<sourceAlias>> -destkeystore "4Sight.jks" -deststoretype JKS -deststorepass <<Password>> -destalias tomcat

7. Export the certificate public key to the file 4SightV2PublicKey.cer (Do not change the file name and path).

   keytool -export -alias tomcat -keystore 4Sight.jks -storepass <<Password>> -store-type JKS -file "../../app/Certificate/4SightV2PublicKey.cer"

8. Import the certificate into java CACert file.

   keytool -import -noprompt -trustcacerts -alias tomcat -storepass changeit -keystore "..\..\jre-1.8\lib\security\cacerts" -file ../../app/Certificate/4SightV2PublicKey.cer

9. Make entry of the certificate into Tomcat configuration file.

   a. Open the file ***"C:\Program Files (x86)\GE Measurement & Sensing\4Sight2\apache-tomcat\conf\server.xml"***

   b. Make the following entry in server.xml.

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

c. Comment the following section to disable http connections.

<Connector port="8080" protocol="HTTP/1.1"
connectionTimeout="20000"
redirectPort="8443" />

Installing Device Manager Certificate

Device manager by default is installed with the self-signed certificate of 512 bits binded on port 9443 for HTTPS connections and 9000 for HTTP connections. The user has to run the following command if another self-signed certificate needs to be installed for HTTPS connections.

Before performing any change, stop the "4Sight Device Manager" service using the service control manager (Press Windows **—>** Start **—>** Run **—>** Services.msc). Restart the service once the Certificate installations are complete.

1. Open the command prompt using run as administrator and change to the folder **"C:\Program Files (x86)\GE Measurement & Sensing\4Sight2\apache-tomcat\conf".**
2. Make sure JRE is in the path by running the following command.

   Keytool /?

   If JRE is not in the path then add the folder in the path environment variable.
   "C:\Program Files (x86)\GE Measurement & Sensing\4Sight2\jre-1.8\bin"

   Set ***"Path=%Path%;C:\Program Files (x86)\GE Measurement & Sensing\4Sight2\jre-1.8\bin"***
3. If installing new certificate, go to point 5.
4. Otherwise do the following:

   a. Remove the Device Manager java keystore (4SightDM.jks) if already exist.

   del 4SightDM.jks

   b. Remove the PFX file if it already exist.

   del 4SightDM.pfx
5. Create a new certificate with the required keysize (e.g. 2048 bits) and validity period (e.g. 1095 = 3 years). Make sure that the password keypass and storepass is same. Common name should be localhost.

   keytool -genkey -trustcacerts -keyalg "RSA" -keysize 2048 -validity 1095 -keypass <<KeyPassword>> -alias tomcat -keystore 4Sight.jks -storepass <<StorePassword>> -dname "CN=localhost, OU=<<Organization Unit>>, O=<<Organization>>, L=<<Location>>, S=<<State>>, C=<<Country Initial>>" -ext eku:critical=sa

6. Export the certificate to the file 4SightDM.pfx.

   Keytool -importkeystore -trustcacerts -srckeystore 4SightDM.jks -srcstoretype JKS -srcstorepass <<Password>> -srcalias tomcat -destkeystore 4SightDM.pfx -deststore-type pkcs12 -destkeypass <<Password>> -deststorepass <<Password>> -destalias tomcat

7. Import the certificate in Personal Store.

   Certutil -importpfx -f -p <<Password>> 4SightDM.pfx

8. Use the following command to get the thumb print of the certificate.

   set "cmd=certutil -p <<Password>> 4SightDM.pfx ^| find "Cert Has" ^| find "sha1" " FOR /F "tokens=3-22" %f IN (' %cmd% ') DO SET THUM-B_PRINT=%f%g%h%i%j%k%l%m%n%o%p%q%r%s%t%u%v%w%x%y

9. Bind the certificate with the Device Manager Port.

   netsh http del sslcert ipport=0.0.0.0:9443
   netsh http add sslcert ipport=0.0.0.0:9443 certhash=%THUMB_PRINT% appid={ed1b0cd4-d4a7-4744-a4b4-a8fa41678d5d}

Appendix A

Best Practices

Server Hardening

The server environment should be hardened as per Microsoft or CIS guidelines.

Tomcat

- Install Tomcat in secure folder where only admin or LocalService has access, such as *C:\Program Files(x86)*
- Install Tomcat as a service running in LocalService account.
- Remove everything from WebApp, remove the default unwanted applications.
- Replace Default error page, such as 404, 403, 500 etc
- Enforce HTTPS, enable SSL.
- Management application should run on SSL.
- User individual log file for each web application.
- Remove Server banner.
- Enable Access logging.
- Change Shutdown port and command.

PostGreSQL

- All the high privilege account like pgdba, postgres, depesz should be allowed to local login only.
- Make sure sequence is correct in pg-hba.conf file so that the correct users get right access
- Configure the pg-hba.conf so that server can be connected only from the local machine and not through the network.

Firewall Best Practices

Here are some of the firewall best practices which are recommended for use with 4Sight™ 2:

Policy

1. Firewall configuration should be consistent with the Organization Security Policy.
2. Always use Least privilege policy. Deny all by default. Allow specific traffic (using source, destination and port)
3. Place Specific rules first and use explicit drop rules.
4. Log all the actions, specifically failure attempts for audit trail

Resources

1. Monitor memory utilization
2. Monitor CPU utilization
3. Monitor Bandwidth utilization.
4. Limit the number of application running on the Firewall machine

Installation and Maintenance

1. Limit Physical Access to the firewall machine
2. Use unique user id for administration
3. Follow strict account policy on the machine
4. Patch operating systems, application software, firmware etc. regularly.
5. Archive rule base, configuration and logs regularly. Document all rules and changes made in a source control.
6. Perform regular tests.
7. Remove unused rule when service is decommissioned.
8. Audit and review the rules on a regular basis.
9. Monitory security advisories on a regular basis

Additional Security

1. Use Statefull inspections.
2. Use Proxies
3. Use Application level inspection and filtering.

Internal Protection

1. Have Acceptable Usage Policy
2. Personal Firewall for each user
3. Host Based intrusion prevention
4. Network Monitoring
5. Content Filtering
6. Access Control on each computer and application.

Office Locations

Australia

Springfield Central
Phone: 1300 171 502
Email: custcare.au@ge.com

France

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

Germany

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

India

Bangalore
Phone: 1-800-301-62632
Email: cc.ms.india@bhge.com

Italy

Milan
Phone: +39 02 36 04 28 42
Email: mariangela.scarati@bhge.com

Japan

Chuo-ku
Tel: 03-6890-4538
Email: gesensing.japan@bhge.com

Netherlands

Hoevelaken
Phone: +31 334678950
Email: NL.sensing.sales@bhge.com

Russia

Moscow
Phone: +7 495 739 6811
Email: aleksey.khamov@bhge.com

UK

Leicester
Phone: +44 (0) 116 2317233
Email: gb.sensing.sales@bhge.com

USA

Boston
Phone: 1–800-833-9438
Email: custcareboston@bhge.com

Services and Support Locations

Tech Support

Global
Email: mstechsupport@bhge.com

Brazil

Campinas
Phone: +55 11 3958 0098
Email: mcs.services@ge.com

China

Changzhou
Phone: +86 (0) 519-83051779-3
Email: service.mcchina@ge.com

France

Toulouse
Phone: +33 562 888 250
Email: sensing.france.services@ge.com

India

Pune
Phone: +91-2135-620421 to 425
Email: mcsindia.inhouseservice@ge.com

Japan

Niigata
Phone: +81 257 45 5509
Email: kariwa.LScenter@ge.com

UAE

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

UK

Leicester
Phone: +44 (0) 116 2317674
Email: sensing.grobycc@bhge.com

USA

Billerica
Phone: 1-800-833-9438
Email: service.boston@ge.com

bhge.com

123M3141 Revision B | English