Data Integrator

Data Integrator 2017.1

INSTALLATION GUIDE

Copyright Notice

Trademarks & Service Marks

Schlumberger, the Schlumberger logotype, and other words or symbols used to identify the products and services described herein are either trademarks, trade names or service marks of Schlumberger and its licensors, or are the property of their respective owners. These marks may not be copied, imitated or used, in whole or in part, without the express prior written permission of Schlumberger. In addition, covers, page headers, custom graphics, icons, and other design elements may be service marks, trademarks, and/or trade dress of Schlumberger, and may not be copied, imitated, or used, in whole or in part, without the express prior written permission of Schlumberger. Other company, product, and service names are the properties of their respective owners.

ProSource® is a mark of Schlumberger.
An asterisk (*) is used throughout this document to designate other marks of Schlumberger.

Security Notice

The software described herein is configured to operate with at least the minimum specifications set out by Schlumberger. You are advised that such minimum specifications are merely recommendations and not intended to be limiting to configurations that may be used to operate the software. Similarly, you are advised that the software should be operated in a secure environment whether such software is operated across a network, on a single system and/or on a plurality of systems. It is up to you to configure and maintain your networks and/or system(s) in a secure manner. If you have further questions as to recommendations regarding recommended specifications or security, please feel free to contact your local Schlumberger representative.

Contents

Overview

Introduction

Data Integrator helps E&P data managers to collect, find, manage, and transfer data quickly and easily through an HTML 5 based web portal. It addresses the common problem of identifying and visualizing data within an E&P organization.

- **Discover**: Search, browse, and filter data globally across different data sources.
- **Manage**: Manage all data from a single portal.
- **Deliver**: Transfer filtered data to an asset team or domain user.

The key features that Data Integrator provides are listed below:

- Ability to access and connect to heterogeneous data sources, current release supports ProSource & Studio.
- Visualization of seismic surveys and well data using:
    - Data Table
    - Map
    - Log Viewer
- Data transfer and sharing across E&P applications.
- Reduced cycle time-immediate availability of data.

Audience:

This document is applicable to system architects, administrators and technical personnel who want to install a new Data Integrator system. It should be used in conjunction with the Release Notes that accompany this version of Data Integrator.

System requirements

This chapter provide details of the different system requirements needed to install and configure Data Integrator.

The following table lists the minimum and recommended system requirements to run Data Integrator 2017.1

Component	Data Integrator server	Data Integrator client
Operating system	Windows Server 2012 R2	Windows 7 SP1 64-bit Windows 10 64-bit
RAM (Minimum)	8 GB	4 GB
RAM (Recommended)	32 GB or higher	16 GB or higher
CPU (Minimum)	2 Cores, 2.6GHz	2 Cores, 2.6GHz
CPU (Recommended)	16 Cores or higher, 2.6GHz	8 Cores or higher, 3GHz
Minimum disk space for installation	4 GB	not applicable
Browsers	not applicable	Internet Explorer 11 Google Chrome v48 or higher

Licensing

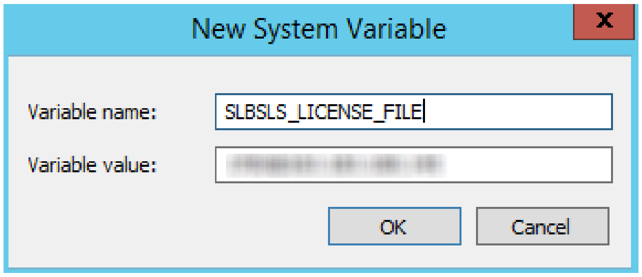
Configure Licensing

Data Integrator uses FlexNet License Manager Software, a network-wide floating license management package. To obtain the necessary licenses for Data Integrator, contact your SIS Customer Support representative. The representative can also provide you with information on:

- Installation and management of FlexNet
- FlexNet implementation options
- FlexNet training programs

After installing the Data Integrator licenses on the FlexLM licensing server, define a system wide environment variable on the Data Integrator server that points to the license server. For example:

```
SLBSLS_LICENSE_FILE=1700@<License Server>
```



Variable name: SLBSLS_LICENSE_FILE

Variable value: [redacted]

Install Data Integrator

This chapter provides information on setting up the Data Integrator environment, including prerequisites and post-installation configuration.

Download the archive

The archive that contains necessary files to install Data Integrator is called **DataIntegratorV2017.1.zip**. The zip file contains **DataIntegrator.msi** and the **Prerequisites** folder. You need to extract the archive to your preferred location.

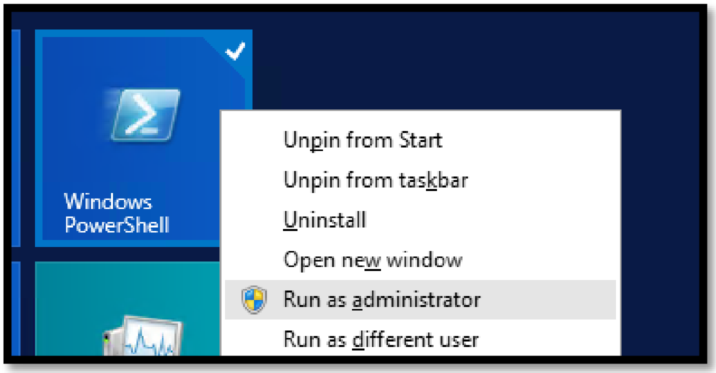
Pre-Installation tasks

Following are the pre-requisite components required to setup Data Integrator.

- .Net4.6.1/4.6.2
- MongoDB 3.4.4 (64 bit)
- MSXML 4.0 SP2
- SQLSysClrTypes for SQL Server 2012 (x64)
- StudioRuntime 2016.2

Above components can be installed by executing `PrerequisiteInstallation.ps1` script. Please follow below mentioned steps to execute the PowerShell script.

1. From the **Start** menu, run **Windows PowerShell** as an administrator.



2. From the PowerShell command line, navigate to the **Prerequisites** directory using the command:

```
cd <Data Integrator Installer folder Location>\Prerequisites
```

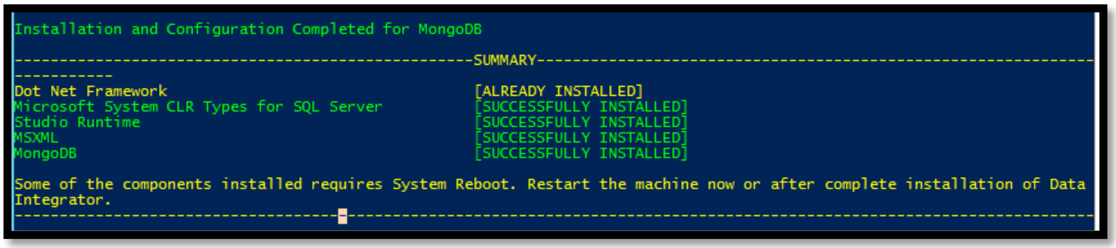
3. Execute the PowerShell script using the command:

```
& .\PrerequisiteInstallation.ps1
```

This command installs and configures the pre-requisites listed above.

Note: If you want to install Data Integrator and MongoDB on a separate server, please refer to Appendix A.

The summary screen is displayed once PowerShell execution is complete.



```
Installation and Configuration Completed for MongoDB

---------------------------------------------------SUMMARY--------------------------------------------------------------
-----------
Dot Net Framework                                  [ALREADY INSTALLED]
Microsoft System CLR Types for SQL Server          [SUCCESSFULLY INSTALLED]
Studio Runtime                                     [SUCCESSFULLY INSTALLED]
MSXML                                              [SUCCESSFULLY INSTALLED]
MongoDB                                            [SUCCESSFULLY INSTALLED]

Some of the components installed requires System Reboot. Restart the machine now or after complete installation of Data
Integrator.
------------------------------------------------------------------------------------------------------------------------
```

MongoDB is installed at a default location C:\Program Files\MongoDB and configured with a default admin user (default password: admin). Please refer to Appendix B for instructions on how to change the admin password.

MongoDB is installed as a Windows service. The configuration file for MongoDB (**mongod.cfg**) is created at default location C:\Program Files\MongoDB.

Additional prerequisites

The following are additional prerequisite components which need to be installed:

- Java Runtime Environment (JRE).
- Tomcat server.
- Web server components (IIS).
- ProSource Front Office (PSFO). Please refer to the *ProSource Installation Guide* to install PSFO.

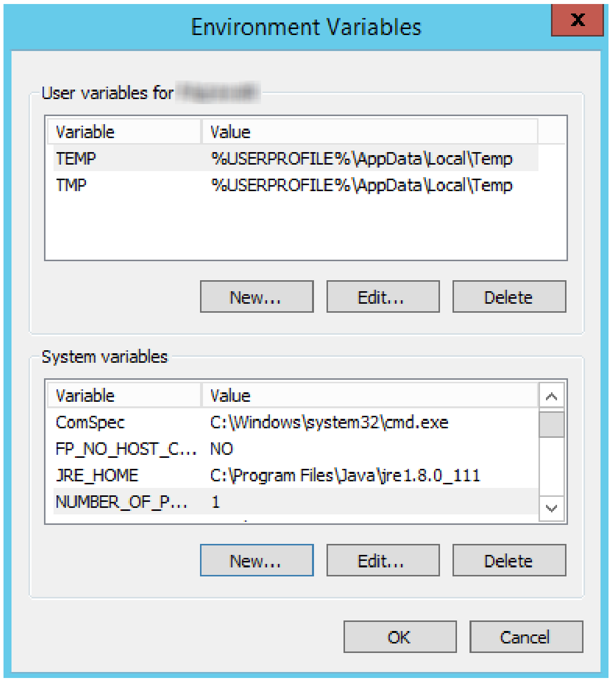
Install Java Runtime Environment (JRE)

1. Download **Java SE Runtime Environment 8u111** from here.

2. Double-click **jre-8u111-windows-x64.exe** file and follow the instructions to install JRE on your system.

3. Right-click **This PC**, select **Properties**, and then select **Advanced system settings** and click **Environment Variables.**

4. In the **Environment Variables** dialog box, click **New**.



Environment Variables

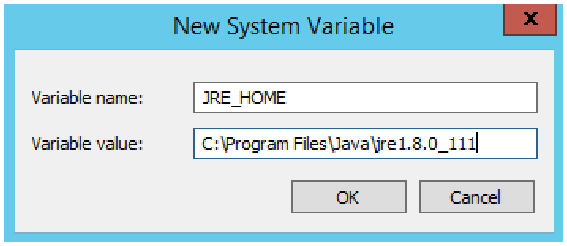
User variables for [redacted]

Variable	Value
TEMP	%USERPROFILE%\AppData\Local\Temp
TMP	%USERPROFILE%\AppData\Local\Temp

System variables

Variable	Value
ComSpec	C:\Windows\system32\cmd.exe
FP_NO_HOST_C...	NO
JRE_HOME	C:\Program Files\Java\jre1.8.0_111
NUMBER_OF_P...	1

5. Enter the **Variable name** as `JRE_HOME` and the **Variable value** as the default location where JRE is installed, and then click **OK**.

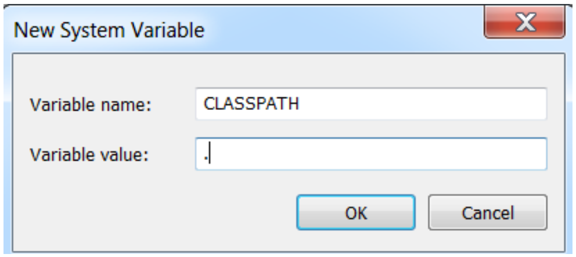


New System Variable

Variable name: JRE_HOME

Variable value: C:\Program Files\Java\jre1.8.0_111

6. Click **New** to add another **Variable name** as `CLASSPATH` and set the **Variable value** as: **.** (dot), and then click **OK**.

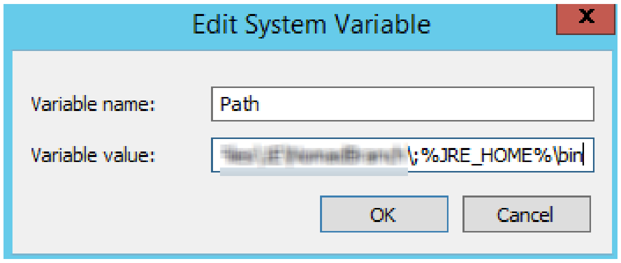


New System Variable

Variable name: CLASSPATH

Variable value: .

7. Select the **Path** environment variable, and then click **Edit.**
8. Append the string `;%JRE_HOME%\bin` at the end, and then click **OK**.



Variable name: Path

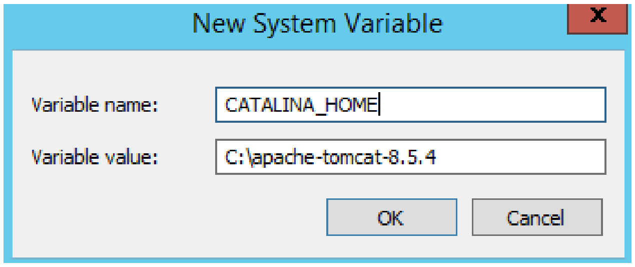
Variable value: [redacted]\;%JRE_HOME%\bin

9. Open the command prompt and run the command **java -version**.
   If it displays the version information, then JRE is correctly installed and configured.

Install and configure the Tomcat service

1. Click here to download the Tomcat 8.5.4 software and then unzip the downloaded zip archive to an appropriate location.

2. Set your environment variables.
   a. Right-click **This PC**, select **Properties**, and then select **Advanced system settings** and click **Environment Variables**
   b. On the **Environment Variables** dialog box, click **New**.
   c. Enter the **Variable name** as `CATALINA_HOME` and set the **Variable value** as the path where the Tomcat folder is downloaded.



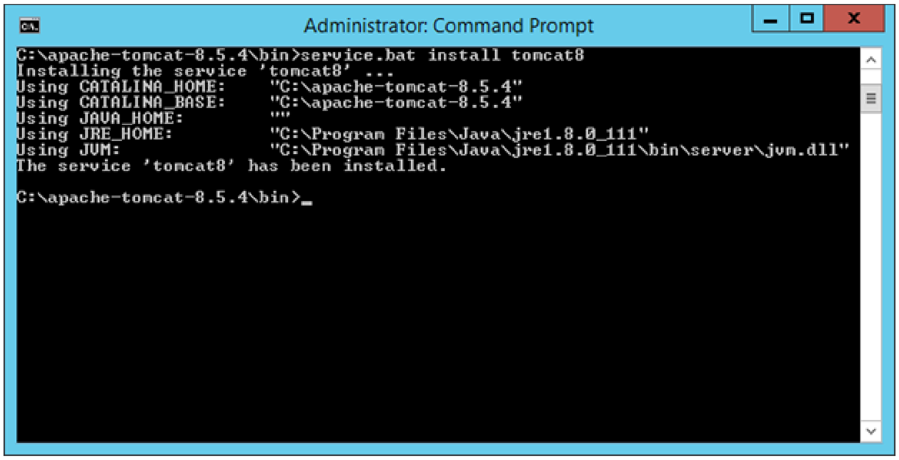
Variable name: CATALINA_HOME

Variable value: C:\apache-tomcat-8.5.4

   d. Select the **Path** environment variable and click **Edit** and then append the string **%CATALINA_HOME%**

3. Open the command prompt as an administrator and execute following commands one by one.
   This installs Tomcat as a Windows service

```
cd %catalina_home%/bin
service.bat install tomcat8
```

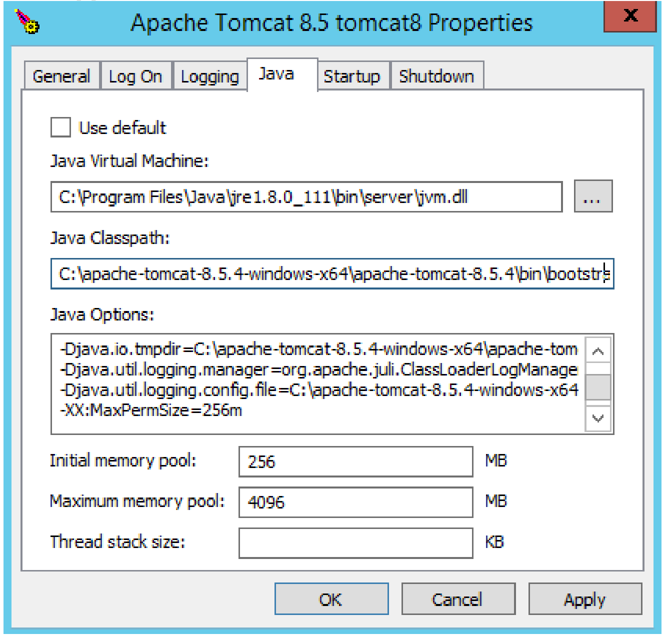


```
C:\apache-tomcat-8.5.4\bin>service.bat install tomcat8
Installing the service 'tomcat8' ...
Using CATALINA_HOME:    "C:\apache-tomcat-8.5.4"
Using CATALINA_BASE:    "C:\apache-tomcat-8.5.4"
Using JAVA_HOME:        ""
Using JRE_HOME:         "C:\Program Files\Java\jre1.8.0_111"
Using JVM:              "C:\Program Files\Java\jre1.8.0_111\bin\server\jvm.dll"
The service 'tomcat8' has been installed.

C:\apache-tomcat-8.5.4\bin>_
```

4. Navigate to <Tomcat_installation_folder>\bin and double-click the **tomcat8w.exe** file. Click **Yes** if prompted for administrator rights.
   The **Apache Tomcat 8.5 tomcat8 Properties** dialog box is displayed.

5. Go to the **Java** tab and set the following options:
   - **Initial memory pool**: 256 MB.
   - **Maximum memory pool**: 4096 MB – It is recommended to set minimum pool size as either 4096MB or 50% of RAM, whichever is higher.
   - In the **Java Options** box, add -XX:MaxPermSize=256m at the end as shown in the image below and click **Apply** and **OK.**



□ Use default

Java Virtual Machine: C:\Program Files\Java\jre1.8.0_111\bin\server\jvm.dll

Java Classpath: C:\apache-tomcat-8.5.4-windows-x64\apache-tomcat-8.5.4\bin\bootstr

Java Options:

```
-Djava.io.tmpdir=C:\apache-tomcat-8.5.4-windows-x64\apache-tom
-Djava.util.logging.manager=org.apache.juli.ClassLoaderLogManage
-Djava.util.logging.config.file=C:\apache-tomcat-8.5.4-windows-x64
-XX:MaxPermSize=256m
```

Initial memory pool: 256 MB

Maximum memory pool: 4096 MB

Thread stack size: KB

6. Go to **Start** and click **Administrative Tools**, and then double-click **Services**.
7. Double-click **Apache Tomcat 8.5 tomcat8** service.
8. On the **Log On** tab, select **This account**. Enter the domain user credentials, which should be the Data Integrator administrator, and then click **Apply.**

Note: Make sure that the same user has administrator access to PSFO projects.

9. On **General** tab, change the **Startup type** to **Automatic**, and then click **Apply**.
10. Click **Start** to start the Tomcat service and then click **OK**
11. Make sure that Tomcat is up and running by launching the URL: http://localhost:8080/ to open the Tomcat page and check the status.

IIS components

Please follow the steps below to install the following mandatory web server (IIS) components.

1. Open **Server manager**.
2. Click **Add roles and Features** and install the components displayed in the table below.

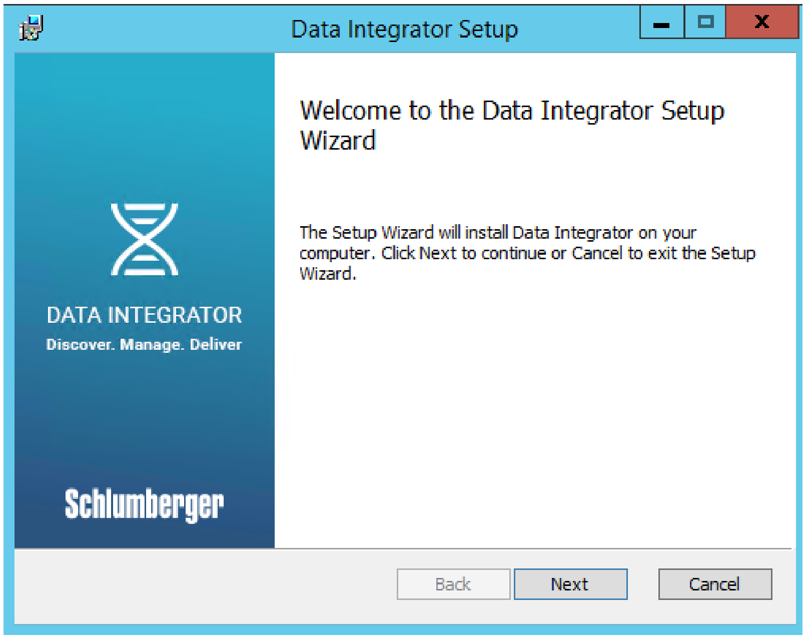
.NET Framework 4.5 Features	Web Server (IIS)	Windows Process Activation Service
• ASP.NET 4.5 • WCF Services o HTTP Activation	Management Tools • IIS Management Console • IIS Management Scripts and Tools Application Development • ASP.NET 4.5 • CGI • ISAPI Extensions • ISAPI Filters • .NET Extensibility 4.5 Common HTTP Features • Default Document • HTTP Errors • HTTP Redirection • Static Content Health and Diagnostics • HTTP Logging Performance • Static Content Compression Security • Basic Authentication • Request Filtering • Windows Authentication	• Configuration APIs • Process Model

Install Data Integrator

Once you have all the prerequisites installed, you can begin installing Data Integrator.

1. Open the command prompt and execute the following command as an administrator.
   ```
   cd <Data Integrator installer folder location>
   ```

2. Execute the following command: `DataIntegrator.msi`
   The **Data Integrator Setup** window is displayed.

   Welcome to the Data Integrator Setup Wizard

   The Setup Wizard will install Data Integrator on your computer. Click Next to continue or Cancel to exit the Setup Wizard.

3. Click **Next.**
   The **End-User License Agreement** dialog box is displayed.

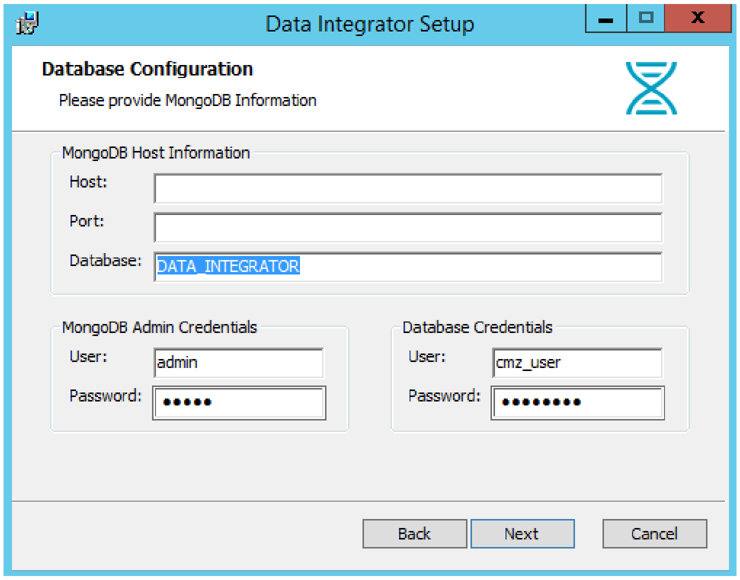
4. Read the license agreement, select the **I accept the terms of this License Agreement** check box, and then click **Next.**

5. Enter the ProSource Front Office URL, and then click **Next.**

6. On the **Database Configuration** dialog box, enter the following details and click **Next.**

Field	Description
Host	IP/Host name of the MongoDB server
Port	Port number on which MongoDB is deployed. By default port number is 27017
Database	Database name for Data Integrator which would be created inside MongoDB

Field	Description
MongoDB Admin Credentials	MongoDB 'admin' database credentials which are required to create the new database for Data Integrator. The credentials displayed below are the default credentials but these can be changed (see Appendix B for more details). **User:** admin **Password:** admin
Database Credentials	New user credentials for the Data Integrator database. This user is created by the installer.



Database Configuration

Please provide MongoDB Information

MongoDB Host Information

Host:

Port:

Database: DATA_INTEGRATOR

MongoDB Admin Credentials

User: admin

Password: •••••

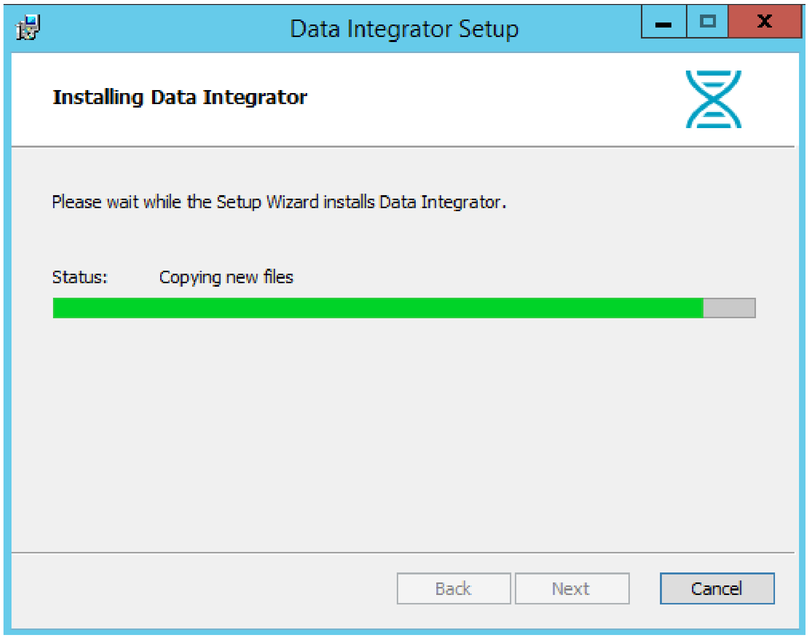
Database Credentials

User: cmz_user

Password: ••••••••

7. In the **Destination Folder** dialog box, select the appropriate local drive path to install Data Integrator, and then click **Next**.

8. In the **Ready to install Data Integrator** dialog box, click **Install**.
   The installation process begins.

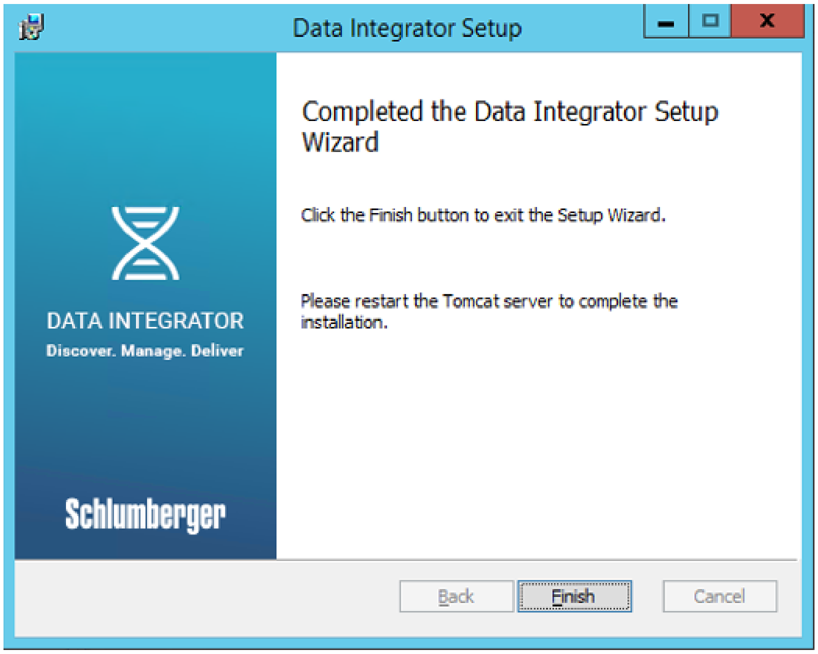


Installing Data Integrator

Please wait while the Setup Wizard installs Data Integrator.

Status: Copying new files

9. Click **Finish** to close the **Data Integrator Setup** wizard.



Completed the Data Integrator Setup Wizard

Click the Finish button to exit the Setup Wizard.

Please restart the Tomcat server to complete the installation.

10. Restart Tomcat.
    a. On the **Start** menu, go to **Administrative Tools**, and then click **Services** to launch the Windows service console.
    b. Right-click **Apache Tomcat 8.5 tomcat8** and select **Restart**.

Verify your installation

Launch the URL: http://<server host name>:8080/DataIntegrator/ to verify if Data Integrator is successfully installed.

Note: Please make sure that the port to access the Data Integrator URL is open, so that users can access the web portal.

Post Deployment Configuration

The following tasks are required and described in this section:

- Configure the ILX Web Service
- Deploy the seismic extension for PSFO
- Configure well log transfer

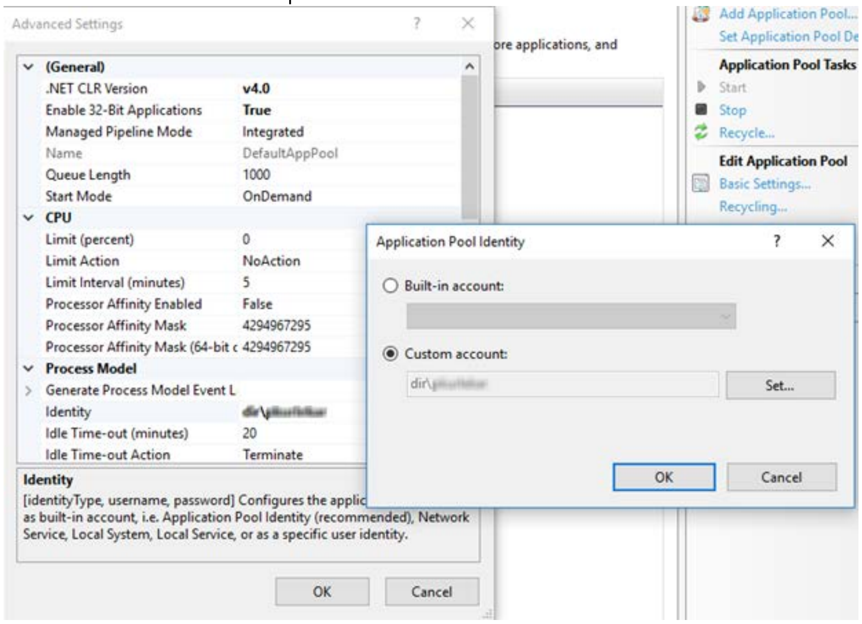
Configure the ILX Web Service

1. From the **Start** menu, select **Administrative Tools** and double-click **Internet Information Services (IIS)** Manager.

2. Click the **Application Pools** and right-click **ILXWSAppPool**, and then click **Advanced Settings**.

3. In the **Advanced Settings** window, click **Identity.**
   The **Application Pool Identity** dialog box is displayed.

4. Select **Custom account** option and click **Set**.



(General)	
.NET CLR Version	**v4.0**
Enable 32-Bit Applications	**True**
Managed Pipeline Mode	Integrated
Name	DefaultAppPool
Queue Length	1000
Start Mode	OnDemand
CPU	
Limit (percent)	0
Limit Action	NoAction
Limit Interval (minutes)	5
Processor Affinity Enabled	False
Processor Affinity Mask	4294967295
Processor Affinity Mask (64-bit c	4294967295
Process Model	
Generate Process Model Event L	
Identity	[redacted]
Idle Time-out (minutes)	20
Idle Time-out Action	Terminate

Identity
[identityType, username, password] Configures the applic as built-in account, i.e. Application Pool Identity (recommended), Network Service, Local System, Local Service, or as a specific user identity.

Application Pool Identity

○ Built-in account:

● Custom account: dir\[redacted]

Set...

5. Enter the **domain\username** and **password** of the Windows server active directory user which already belongs to the local operating system Administrators group.

6. Open command prompt in administrative mode and execute the command `iisreset` to restart the IIS services.

Deploy the seismic extension for PSFO

To deploy the customized entities on PSFO server, follow these steps.

1. Log on to the PSFO server and open the ProSource Front Office installation location. Delete any folder named **SeismicSurveyModules** existing at the locations below (if any):
   - <ProSourceFrontOffice_installation_path> \DataService\ExtensionArchives
   - <ProSourceFrontOffice_installation_path>\DataService\Extensions
   - <ProSourceFrontOffice_installation_path> \PSWebApp\ClientBin\Extensions
2. On the Data Integrator server, copy the **SeismicSurveyModules.zip** file from the <DataIntegrator Installation Path>\Data Integrator\Extensions folder and paste it to the following location on the PSFO server:
   ProSourceFrontOffice_installation_path \DataService\ExtensionArchives

3. Restart IIS for the PSFO server.

Configure well log transfer

Note: For well log transfer, please ensure Data Integration server host file should have ProSource(s) server host name entry in C:\Windows\System32\drivers\etc\hosts.

Contacting Schlumberger

Technical support

Schlumberger has sales and support offices around the world. For technical support related to SIS software, please refer to the contact information given below:

- Schlumberger support portal: https://www.software.slb.com/support
- Customer care center e-mail: customercarecenter@slb.com
- Customer care website: https://customercarecenter.slb.com
- SIS phone support: https://www.software.slb.com/support/contact-details

Appendix A: Set up Data Integrator & Mongo DB on separate servers

In this section steps are provided to configure Data Integrator & MongoDB on separate server machines.

Install MongoDB

1. Copy the **Prerequisites** folder to the server.

2. Launch the windows PowerShell in administrator mode and navigate to the Prerequisites directory using the command:
   ```
   cd <Data Integrator Installer folder Location>\Prerequisites
   ```

3. Run the below command, it would install & configure MongoDB for Data Integrator. Configuration file `mongod.cfg` is kept at default location (C:\Program Files\MongoDB).
   ```
   & .\PrerequisiteInstallation.ps1 -include MongoDB
   ```
   MongoDB is installed at a default location C:\Program Files\MongoDB and configured with a default admin user (default password: admin). Please refer to Appendix B to change the admin password.

To install other prerequisites on DI server

1. Launch the windows PowerShell in administrator mode and navigate to the Prerequisites directory using the command:
   ```
   cd <Data Integrator Installer folder Location>\Prerequisites
   ```

2. Run the below command to install prerequisites for DI excluding MongoDB
   ```
   & .\PrerequisiteInstallation.ps1 -exclude MongoDB
   ```

Appendix B: Change MongoDB admin password

In this section, steps are provided that explain how to change MongoDB credentials.

1. Go to the installation location of Mongo DB.

   Note: By default MongoDB bin folder is C:\Program Files\MongoDB\Server\3.4\bin\

2. Open the **bin** folder and double-click **mongo.exe.** This opens Mongo shell. Copy and paste the following commands one by one and press **Enter**.

   ```
   use admin
   db.auth("admin","<existing password>")
   db.updateUser("admin",{pwd:"<new password>"})
   ```

3. Execute the following command.

   ```
   db.auth("admin","<new password>")
   ```

   If the command returns 1 then it means you have successfully set a new password.

4. Close the Mongo shell.

Appendix C: Configure SSL/HTTPS

Prerequisites

You need to have a valid certificate (**.cer**) file issued by a CA.

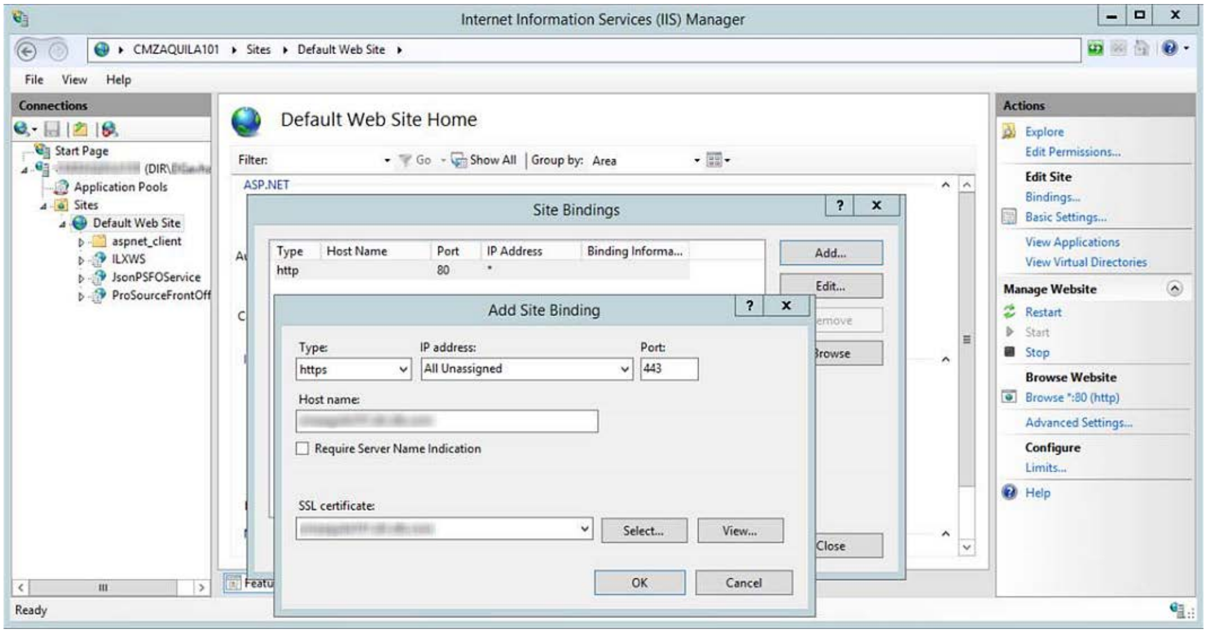
> **Note**: The certificate should be issued to the machine name of the server, else a certificate error may occur.

Deploy SSL certificate on IIS

The steps below explain how to configure SSL on IIS websites.

1. Open **Internet Information Services (IIS**) **Manager**.
2. From your configured connections, in the **Connections** pane, double-click **Server Certificate**.
3. From the **Actions** pane, click **Complete Certificate Request.**
4. In the **Complete Certificate Request** dialog box, click the **ellipses (…)** and navigate to the certificate file (.cer).
5. Specify the **Friendly name** and click **OK**.

   Note: It is recommended to use a fully qualified domain name (fqdn) for the **Friendly name**.
6. To add a binding to the deployed website, select the **Connections** pane, expand the **Sites** folder, and then select the **Default web Site**.
7. In the **Actions** pane, click **Bindings.**
8. In the **Site Bindings** dialog box, click **Add.**
9. In the **Add Site Binding** dialog box, select the **Type** as **https.**



Site Bindings:

Type	Host Name	Port	IP Address	Binding Informa...
http		80	*	

Add Site Binding:

Type: https

IP address: All Unassigned

Port: 443

Host name: [redacted]

☐ Require Server Name Indication

SSL certificate: [redacted]

10. Provide a fully qualified **Host name**.
11. In the **SSL certificate** box, select the name of the certificate that you installed, and then click **OK**.
12. Close **Site Bindings** dialog box

Configure Data Integrator IIS Services with SSL/HTTPS

1. Go to **IIS** and expand the default website, and then right-click **JsonPSFOService** and select **Explore**.

2. Open the **Web.Config** in a text editor.

3. Locate the **<serviceBehaviors>** section, change service metadata to **httpsGetEnabled** as shown below.
   ```
   <serviceMetadata httpsGetEnabled="true" />
   ```

4. Add the <**serviceAuthorization>** tag to this behavior and set **impersonateCallerForAllOperations** to **true**.
   ```
   <serviceAuthorization impersonateCallerForAllOperations="true"/>
   ```

5. Locate the <**bindings**> section, for **<basicHttpBinding**> and <**webHttpBinding>** sections and change **security mode** to **Transport** as shown below:
   ```
   <security mode="Transport">
   ```

6. Update the binding named "BasicHttpBinding_IProjectService" within **<basicHttpBinding>** and add the following lines:
   ```
   <security mode="Transport">
      <transport clientCredentialType="None" />
   </security>
   ```

7. Locate the <**customBinding**> section, and then change the tag **<httpTransport>** to **<httpsTransport >**

Note: Make sure you keep the other attributes in the tag and just change the tag name.

8. Update the **endpoint address** attributes for **UserInformationService.svc, ProjectService.svc, ResourceManager.svc and SeabedService.svc** to use https.

9. Reset **IIS**.

Configure JRE with HTTPS/SSL

1. Open the command prompt as an administrator and execute the following command:
   ```
   cd %JRE_HOME%/bin
   ```

2. Create a keystore with a self-signed certificate by typing the following command:
   ```
   keytool -genkey -alias tomcat -keyalg RSA
   ```

   Note: The command prompts you to provide a new password. For convenience, you can use the same password for all subsequent steps.

   This command creates a keystore at the location: **c:/users/{user}/.keystore**

3. Delete the self-signed certificate from the keystore by typing the following command:
   ```
   keytool -delete -alias tomcat -keystore <key store
   location>/.keystore -storepass <password>
   ```
   This command deletes the stored password from c:/users/{user}/.keystore

4. Following command exports a deployed .cert file to .pfx format.
   a. Open the **Server Certificates** from IIS **.**
   b. Select the certificate which needs to be exported in .pfx format.
   c. Click **Export** in **Action Panel** and specify the location and password.

5. Import the **.pfx** certificate generated in the previous step by typing the following command:
   ```
   keytool -importkeystore -srckeystore <location of the .pfx file>
   -srcstoretype pkcs12 -destkeystore <location of the .keystore
   file> -deststoretype JKS
   ```

6. List the certificate just added using the following command:
   ```
   keytool -list -keystore <location of the .keystore file>
   ```

7. Copy the alias of the certificate listed in the previous step.

8. Change the alias name to Tomcat as follows:
   ```
   keytool -changealias -alias "copied alias" -destalias "tomcat" -
   keypass <password1> -keystore C:\Users\{user}\.keystore -
   storepass <password2>
   ```
   where **password1** is the password used while creating the .pfx file and **password2** is the keystore password.

9. Import this certificate to the JRE as follows:

```
 keytool -import -alias tomcat -file <location of the .cer file>
-keystore "%JRE_HOME%\lib\security\cacerts" -storepass
 <password>
```

Note: Default password is “changeit”

Configure Tomcat with SSL/HTTPS

1. Open the <tomacat directory>\conf\server.xml and add the following block under <Service name="Catalina"> element.

```
<Connector SSLEnabled="true" acceptCount="100" clientAuth="false"
disableUploadTimeout="true" enableLookups="false" maxThreads="25"
port="8443" keystoreFile="keystore_file_path"
keystorePass="password_you_entered"
protocol="org.apache.coyote.http11.Http11NioProtocol"
scheme="https"
   secure="true" sslProtocol="TLS" />
```

   Note: **keystore_file_path** is the location where the .keystore file was generated. **password you_entered** is the password you entered during creation of the keystore.

2. Restart Tomcat services.

MongoDB

Make sure that the certificate files **.pem** and **.der** already exist on the server where MongoBD is deployed.

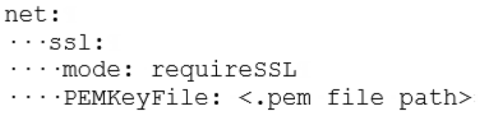
Import keystore for mongo DB

1. Open the command prompt and execute the following command as an administrator to import the certificate file in the keystore:
   ```
   keytool -import -alias mongodb -keystore "C:\Program
   Files\Java\jre1.8.0_111\lib\security\cacerts" -file <filepath for
   .der file> -trustcacerts
   ```
2. Enter a keystore password.
3. In the **Trust this Certificate** dialog box, click **Yes**.
   The confirmation screen is displayed and the certificate is successfully added to the keystore.

Enable SSL for MongoDB

1. Open the **Windows Services management console** and stop the MongoDB service.

2. Update the **mongod.cfg** file located in <Mongodb install path>\ with the contents given below:



```
net:
···ssl:
····mode: requireSSL
····PEMKeyFile: <.pem file path>
```

Note: '.' (dot) character in the above syntax denotes the number of white space characters.

3. Start the MongoDB services again.

Configure PSFO to enable SSL/HTTPS

Following are the minimum required changes for https setup of PSFO service.

Note: To enable https for all the PSFO components, please refer the PSFO documentation.

1. Log on to the PSFO server and Navigate to the PSFO installed directory.

2. Open the < PSFO installed directory>**DataService** folder.

3. Open and edit the **Web.config** file.
   a. Locate the **<services>** section and inside the <endpoint> tag.
   b. Change "**mex"** address **binding** to **mexHttpsBinding** as below:
   ```
   <endpoint address="mex" binding="mexHttpsBinding"
     contract="IMetadataExchange"/>
   ```

Note: Make sure that you change all the <endpoint> tags inside the services section.

4. Locate the <serviceBehaviors> section, and change service metadata to **httpsGetEnabled** as shown below:
   ```
   <serviceMetadata httpsGetEnabled="true" />
   ```

Note: Make sure that you update all the values of **<serviceMetadata>** tag under the **<serviceBehaviors>** section.

5. Locate the <bindings> section, and under <basicHttpBinding>, change the security mode to **Transport** as shown below:

   ```
   <security mode="Transport" />
   ```

   Note: Make sure that you perform this update for all the values under <basicHttpBinding> section.

6. Locate the <customBinding> section, and change the security mode **httpTransport** tag name to **httpsTransport** for all entries within this section, as shown below:

   ```
   <httpsTransport/>
   ```

   Note: Please retain other attributes inside the tags and make sure you change the tag name only.

7. Reset **IIS**.

Configure Data Integrator services with SSL/HTTPS

1. Go to the **config.properties** file placed at **<Installation Path>\DataLoadingApp\config\config.properties>**

2. Change all the URLs from **http** to **https** in the **config.properties** file.

3. Change **mongoSSLFlagDisabled** value to **false**: `mongoSSLFlagDisabled=false.`

4. Close and save the **config.properties** file.

5. Reset **IIS**.

Configure the Data Integrator Web portal with SSL/HTTPS

1. Edit the **config.properties** file located in <**Tomcat path>\webapps\DataIntegrationService\WEB-INF\classes\config.properties**.

2. Change all the URLS in the **config.properties** file from **http** to **https**\

3. Change the **mongoSSLFlagDisabled** value to **false**: `mongoSSLFlagDisabled=false`.

4. Restart the Tomcat service.

   Note: The sample Data Integrator URL: https://<server name>:<port>/DataIntegrator
   Default https port is 8443.