Liquent InSight 6.2 CHF 3 Installation Guide

parexel

Table of Contents

Liquent InSight 6.2 CHF Installation Overview

This guide is a set of installation procedures. To ensure your system integrity, it is essential that you follow all applicable installation instructions.

Liquent InSight certified hotfix (CHF) packages are cumulative. Use the procedures in the following topics to install this CHF on each Liquent InSight server.

Please review the Liquent InSight 6.2 System Support Documentation before starting your migration to the current Liquent InSight 6.2 CHF to ensure that your database and other system hardware and software components are compatible with the upgrade.

Migration Path to a Liquent InSight 6.2 CHF

Follow the migration path to the most current Liquent InSight 6.2 Certified Hotfix, depending on your current installation.

The applicable migration path is the following:

Liquent InSight 6.0 > **Liquent InSight 6.0 CHFs** > **Liquent InSight 6.1** > **Liquent InSight 6.1 CHFs** > **Liquent InSight 6.2** > **Liquent InSight 6.2 CHF 1** > **Liquent InSight 6.2 CHF 2** > **Liquent InSight 6.2 CHF 3**.

The following table lists the upgrade packages that need to be used during the migration to the most recent Liquent InSight 6.2 CHF.

Liquent InSight Version	Upgrade Package
Liquent InSight 6.2	`DB_update6_2_0_0000_0199.zip`
Liquent InSight 6.2 CHF 1	`DB_hotfix6_2_0_chf1_0014.zip`
Liquent InSight 6.2 CHF 2	`DB_hotfix6_2_0_chf2_0060.zip (see 26207 for details)`
Liquent InSight 6.2 CHF 3	`DB_hotfix6_2_0_chf3_0039.zip`

Prepare to Install a Liquent InSight 6.2 CHF

The information presented in this topic contains some general procedures that must be completed prior to installing the specific Liquent InSight 6.2 CHF.

Before you install a Liquent InSight 6.2 CHF, be sure to complete the following procedures:

Procedure Description	Required in this CHF
Save copies of all files that are being replaced to another location, such as a shared network drive.	Yes
As a precaution, backup and save all files associated with your Liquent InSight system that you have modified, even if they are not listed in the instructions in the following topics and are not to be replaced during this upgrade.	Yes
For any customizable files included with this certified hotfix, such as properties files or template files, compare the new files to your existing files (by performing a `diff` procedure, for example) to determine whether changes were made that you need to carry forward to the new files.	Yes
If you have modified the standard overrides in Liquent InSight, contact Technical Support for assistance with preparing your overrides for this upgrade. XML changes will be required and some functionality may be impacted as a result.	Yes
Manual updates to Liquent InSight Data Administration for publishing specifications.	No

Liquent InSight Database Server Installation for 6.2 CHF 3

Prepare to Install the Database Upgrade Script for a Liquent InSight 6.2 CHF

Perform the procedure in this topic to prepare to update your Liquent InSight 6.2 database for each Certified Hotfix (CHF).

Prerequisites

Attention:

- Please note that grants for custom database users are removed during the migration.
- Verify that you are running the Oracle Database installation SQL script on a Windows based computer. If your Oracle Database is hosted by a Unix server, you must run the Oracle Database installation SQL script on a Windows client that can remotely access the database server using Oracle's SQL*Plus.

Before you update the database:

1. Make sure that you completed all the preceding procedures for installing the most recent Liquent InSight 6.2 CHF.
2. Create a backup copy of your database.
3. If you have not updated the database before, or if you are unsure how to upgrade your database script, contact Technical Support before proceeding.

Install the Database Upgrade Script for a Liquent InSight 6.2 CHF

Perform the following procedure to update your Liquent InSight 6.2 database for each CHF.

Prerequisites

The following table lists the Database Upgrade Scripts that must be used to update your Liquent InSight 6.2 database for each CHF. The **Certified Hotfix (CHF) Version** column identifies to which CHF version each script applies.

File Name	Certified Hotfix (CHF) Version	Last Modified Build
`DB_hotfix6_2_0_chf1_0014.zip`	Liquent InSight 6.2 CHF 1	6.2.0.1.0004

File Name	Certified Hotfix (CHF) Version	Last Modified Build
DB_hotfix6_2_0_chf2_0060.zip	Liquent InSight 6.2 CHF 2	6.2.0.2.0069
DB_hotfix6_2_0_chf3_0039.zip	Liquent InSight 6.2 CHF 3	6.2.0.3.0062

To update the database, perform the following procedure to install each database script in the preceding table:

1. Extract the `.zip` file located in the `scripts` directory of the hotfix.
2. Edit the `define.migration` script to fill in the following values:

   SID

   orapath

   dbcommonuser

   dbcommonpass

   dbcommonpath

   password
3. Use the `sqlplus /nolog` command to connect to sqlplus from the directory where the `.zip` file was extracted.
4. At the `sqlplus` prompt, run the `master_pre.sql` by using `@master_pre`.
5. At the `sqlplus` prompt, run the `master.sql` script by using `@master`.
6. Check the log file for errors. If you find errors in the log, contact Technical Support.
7. Restart your database instance after making these changes.

Upgrade to Liquent InSight 6.2

Prerequisites

Verify that you already installed the exact version of a database upgrade script. To determine this, run the following query on your system to compare your installed database scripts to those in the package. Log on to **SQLPLUS** as **System** and type `select * from aud.version_history`.

Note: If you already ran a script, do not run it again.

1. Copy the `database.zip` file from the Database Server installation media to the temp directory you created and extract the ZIP file.
2. Open the `define.migration` file in Notepad.
3. Set the value to the right of the equals sign for the following ID or passwords in the `define.migration` file you are editing.

   Only define the settings from this list that are already present in the `define.migration` file. Do not add any setting to the file from this list.

   - define `sid=name of the database instance for the existing Liquent InSight database`

- define `orapath=database files location`

  `D:\oracle\oraXX\insight` or `\apps\oracle\oradata\insight`

  Note: To prevent connection errors when modifying database execution scripts, because the @ symbol is a value in the Oracle database connection string, enter database passwords containing the character @ using quotes.

  Password `abc@123` should be entered as `'"abc@123"'` (single quotes, double quotes, password, double quotes, single quotes).
  The IDs and passwords are set correctly.

  Default passwords:

- define audpass=aud
- define dmpass=dm
- define ismpass=ism
- define mgrpass=mgr
- define odspass=ods
- define secpass=sec
- define migrationpass=migration
- define jmsadminpass=jmsadmin
- define sharedpass=shared
- define activitipass=activiti
- define syspass=<enter system password for database being upgraded per step action>

4. Close and save the modified `define.migration` file.
5. Open the **command prompt**, type: `sqlplus/nolog` and press Enter.
6. In the `sqlplus` prompt, type `connect database user/database password@sid` and press Enter.
7. After the connection to database is opened, type `@master_pre` in the `sqlplus` prompt and press Enter.
8. After `@master_pre` is complete, type `@master` in the `sqlplus` prompt and press Enter.
9. Once the script is complete, check the database log file for errors.

   This file is generated in the directory where the build script was executed, and should be found in the same directory created previously.

   Note: In case of errors, refer to the *Database Script Error Messages* topic.

   `D:\install\InSightDBUpgrade1\DBupgrade`
10. Optional Step:
    - Open the `define.passwords.alternate` file in Notepad and update passwords values if needed. Save and close file.
11. Optional Step:
    - Open a **command prompt** and navigate to the newly created database folder.

      For Example: cd `D:\Install\InSightDB\database`.
    - Connect to the Liquent InSight 6.2 CHF 3 database as **system** user.
    - At the **command prompt** type: `sqlplus /nolog`.
    - At the `sqlplus` prompt type: `@BLD_FINAL_change_passwords.sql`.

    Script executes updating passwords to Liquent InSight 6.2 CHF 3 defaults.
12. At the `sqlplus` prompt type: `exit`

Liquent InSight Application Server Installation for 6.2 CHF 3

Liquent InSight 6.2 CHF 3 Application Server Installation Prerequisites

Before installing the Liquent InSight 6.2 CHF 3 Application Server, confirm that the Liquent InSight 6.2 CHF 3 Database Server is installed.

Liquent InSight 6.2 CHF 3 Application Server Installation Prerequisites For Liquent InSight Upgrades Only

For the Liquent InSight Application Server, upgrading to Liquent InSight 6.2 CHF 3 is only supported from Liquent InSight 6.2 CHF 2

Before performing any upgrade procedures, do the following:

- Back up your existing Liquent InSight Database.
- Ensure that all users are logged off from the Liquent InSight system and the InSight Manager Service is stopped, as instructed in this script.
- If a customized XML metadata configuration exists in your current installation of Liquent InSight, specific changes to this configuration must be made by Client Enablement when migrating to 6.2 CHF 3. This applies to all licenses and modules, and all configuration XML files (`meta.overrides.xml`, `property_mappings.xml`). Please contact your Technical Support Representative to arrange these upgrade modifications.

Liquent InSight 6.2 CHF 3 Application Server Installation Prerequisites For SharePoint Only

When using Liquent InSight or Liquent InSight Rendering with SharePoint, versioning needs to be turned on in the SharePoint Library(s) in use for Liquent InSight Rendering to render documents without error. To do this, select your library in SharePoint, then choose **versioning settings** and select **Create major and minor versions**.

Ensure that the **Require documents to be checked out before they can be edited?** option is set to **No**.

Attention:

- Any Java application (32-bit or 64-bit) that uses Global Java Variables will cause performance issues and/or cause failures with the Liquent InSight Application. Examples of this are Altiris or Tivoli.

- Liquent InSight is shipped with the out-of-the-box security configuration for JBOSS. Please note that the *profile* that is used is *all*. If you need to secure the JMX console, follow the instructions provided at https://community.jboss.org/wiki/SecureTheJmxConsole.

Preparing to Install the Liquent InSight 6.2 CHF Application Server

The procedure described in this topic is applicable to each Liquent InSight 6.2 Certified Hotfix (CHF) unless otherwise is stated.

You must perform the following procedure on each Liquent InSight server before you install the Liquent InSight 6.2 CHF application server.

To prepare for the installation:

1. Verify the following for the installation service account:

Permissions	Full `read/write` on server (i.e., in the **Administrator** group).
Account	The account is a Windows domain user account with local administrative privileges.
	The account is the same one used to install all prerequisite software for the server. This account will be referred to as `local administrator`.

2. Verify the correct server time and time zone with the repository system and the Oracle database system. Ensure the time for all servers is the same.
3. Verify that all users are logged off the Liquent InSight system.
4. Stop the InSight Manager service:
   a) Choose **Start** > **Control Panel** > **System and Security** > **Administrative Tools** > **Services**.
   b) Double-click the InSight Manager service.
   c) In the **InSight Manager Service Properties** dialog box, click **Stop** and then click **OK**.

Environment Setup

If you are upgrading to Liquent InSight 6.2 CHF 3, the Environmental Variables addressed in this cycle may already exist. For existing variables, update the values as needed to be compatible with Liquent InSight 6.2 CHF 3.

1. On the Application Server, go to: **Control Panel** > **System** > **Advanced System Settings** > **Advanced**.
2. On the **Advanced** tab, in the **Performance** section, click **Settings**.
3. In the **Performance Options** window, select **Data Execution Prevention**.
4. In the **Data Execution Prevention** tab, select: **Turn on DEP for essential Windows programs and services only**.
5. On the **Advanced** tab, for **Processor scheduling**, select **Programs**. Click **Apply**.
6. On the **Visual Effects** tab, select **Adjust for Best Performance** and then click **OK**.
7. Select **Environment Variables**.
8. Under **System variables**, click the **Path** variable, and then click **Edit**.

9. In the **Variable Value** box, remove any directories that reference JRE, and click **OK**.
   For example: `C:\Oracle\product\XX.XJAV.X\Client_1\jre\1.6.0\bin`
10. Under **System Variables**, select **New**.
11. In the **Variable Name** field, type in caps: `JAVA_HOME`
    a) In the **Variable Value** field, type in the directory of your AdoptOpenJDK installation.

    Note: If `JAVA_HOME` is pointing to older version of JDK, remove that value and type in the directory of your AdoptOpenJDK installation.

    For example: *<installation drive>*`:\Program Files\jdk8u212-b03`
    b) Click **OK**.
12. Select the **Variable Path**.
    a) In the Edit environment variable screen, select **New**.
    b) Type the following: `%JAVA_HOME%\bin`
    c) Click **OK**.
13. Adjust **Java.Security**
    a) Apply the following changes required in the **java.security** file under **jdk** installation from the **disabledAlgorithms** list.
    For example: `C:\jdk8u202-b08\jre\lib\security\java.security file`.
    b) Open the **java.security** file. Search the section **jdk.tls.disabledAlgorithms** and remove **anon** for it. Save the file.
    For example:
    - *jdk.tls.disabledAlgorithms=SSLv3, RC4, DES, MD5withRSA, DH keySize < 1024, *
    - EC keySize < 224, 3DES_EDE_CBC, anon, NULL

    should be changed into:
    - *jdk.tls.disabledAlgorithms=SSLv3, RC4, DES, MD5withRSA, DH keySize < 1024, *
    - *EC keySize < 224, 3DES_EDE_CBC, NULL*
14. Under **System variables**, select **New**.
15. In the **Variable Name** field type (in capital letters): `INSIGHT_HOME`
    a) In the **Variable Value** field, enter the directory of your Liquent InSight installation.
    For Example:`C:\InSightManager`
    b) Click **OK**.
16. Under **System variables**, select **New**.
    a) In the **Variable Name** field, type in caps: `DFC_CONFIG`
    b) In the **Variable Value** field, enter the directory where the `dfc.properties` file resides.
    For example: `c:\Documentum\config`
    c) Click **OK**.
17. On the **Environment Variables** window click **OK**, and then on the **System Properties** window click **OK**.
18. Open the **Command prompt** as Administrator and navigate to the `bin` directory within the *<installation drive>*`:\InSightManager` folder. Type `Install_Insight_Service.bat`, and press **Enter**.
    For example: `C:\InSightManager\bin\Install_InSight_Service.bat`
19. In Microsoft Explorer, navigate to the *<installation drive>*`:\InSightManager\bin` folder and open the `run.conf.bat` file. Update the section for the memory allocation pool parameters so the XMS and XMX settings are 70% of the OS memory:
    (if OS memory is 16GB) set:
    - Xms11200m –Xmx11200m
    - Update the section Garbage Collection to increase memory size.

    (if OS memory is 16 GB):

- rem # Garbage Collection settings
- set JAVA_OPTS=%JAVA_OPTS% -XX:+UseConcMarkSweepGC -XX:+CMSClassUnloadingEnabled –
- XX:+ScavengeBeforeFullGC –
- XX:NewSize=3754m –
- XX:MaxNewSize=3754m

Note: These examples are baseline parameters, your optimal settings may vary.

20. Reboot the server.
21. Log on as the local administrator.

Restart the Liquent InSight Manager Service

After you install the components and make the other recommended modifications for Liquent InSight 6.2 CHF, restart the Liquent InSight Manager service on your Liquent InSight application server.

To restart the Liquent InSight Manager service:

1. Select **Start** > **Control Panel** > **Administrative Tools** > **Services**.
2. Double-click the **Insight Manager** service.
3. In the Liquent InSight Manager Service **Properties** dialog box, click **Start** and then click **OK**.

Replacing InSightManager for a Liquent InSight 6.2 CHF

The procedure below is applicable to each Liquent InSight 6.2 Certified Hotfix (CHF) unless otherwise is stated.

Prerequisites

To install Liquent InSight 6.2 CHF, first replace InSightManager.

To replace InSightManager:

1. Move your `InSightManager` folder to another location, such as a shared network drive, for backup purposes.

   If you have modified any properties files contained in `InSightManager`, you will need them later in this procedure.
2. Unzip the `InSightManager.zip` file from the Liquent InSight 6.2 CHF installation media into the root directory of *<intallation drive>*.
3. Copy the contents of the `DTDs` directory (i.e., only the files) and the `Templates` directory (i.e., the folder and the files) from the installation media to the respective `DTDs` and `Templates` directories.

   A *DMS* is recommended over a file system.

   Remember the following:

   - When entering the location, the file path is case sensitive.
   - If you are importing the contents into a docbase, be sure that the file extensions are preserved in the names of the files. That is, the files should still have a name that ends in either `.zip` or `.properties`.

Furthermore, the contents of the `DTD` directory should be copied or imported into the last folder specified in the path.

- If you customized the existing Letter and A4 template files for TOC generation (`TOCTemplate.doc`, `A4TOCTemplate.doc`, and `UCTOCTemplate.doc`), you will need to apply your customizations to the new TOC template files. This step must be performed only if new templates have been added and/or the existing templates have been updated.

4. Be sure to account for any customizations made to your current properties files. If you have customized properties files, compare your backup copies of those files with those provided in the certified hotfix package. Add your customizations to the certified hotfix properties files in the directory `<installation drive>:\InSightManager\server\all\conf\insight`, as needed:

`EctdResources.properties`
`meta.overrides.xml`
`OverridesResources.properties`
`propertyMappings.xml`
`StudyReportResources.properties`
`property_mappings.xml`
`DMSEnterprise.properties`
`%\InSightManager\server\all\conf\bindingservice.beans\META-INF\bindings-jboss-beans.xml`

5. Copy the following files containing your configurations from the `InSightManager` backup folder to the new `InSightManager` folder:

`<installation drive>:\InSightManager\server\all\conf\login-config.xml`
`<installation drive>:\InSightManager\server\all\deploy\oracle-ds.xml`
`<installation drive>:\InSightManager\bin\run.conf.bat`
`<installation drive>:\InSightManager\server\all\conf\insight\insight.var`
`<installation drive>:\InSightManager\server\all\conf\insight\license.xml`

Liquent InSight Configuration for 6.2 CHF 3

Liquent InSight Configuration

1. Locate the `insightConfig.bat` file in the *<installation drive>*`\InSightManager\server\all\conf\insight` installation directory and double-click the file.

   Note: If `insightConfig.bat` fails to run, add a reference to `java.exe` from the JDK package to the Path environment variable.

2. Enter the appropriate values in the **LIQUENT InSight Configuration** Wizard. For Tab **Basic Settings** > **Server Settings** section:

Machine	*<appsrvr>*
Port	8080

   Warning: Liquent InSight will not run if the port specified is in use by another application. Ensure that any applications that use the specified port (example – Windows IIS) are not running on the server.

   Note: If you change the port number from the default 8080, you must also change the `Connector port = "8080"` setting in the `C:\InSightManager\server\all\conf\bindingservice.beans\META-INF\bindings-jboss-beans.xml` file.

3. Enter the appropriate values in the **Database Settings** section:

Database Server Type	Oracle
Database Server	*<server-oracle>*
Database Port	1521
Instance Name	*<sid-base>*
User Name	insight_user
Password	*<password>*

4. Enter the appropriate values in the **DefaultDS** section:

DefaultDS User Name	jmsadmin
DefaultDS Password	*<password>*

   Note: After the Liquent InSight installation is complete, you can arrange with your Database Administrator to change the DefaultDS password to a unique value. Once the password is changed in the database, you must reconfigure the `insight.var` file with the new password by running `insightConfig.bat` again.

5. **Note:** Perform this step only if your installation includes the Liquent InSight Workflow Integrations license.

Choose one of the below defined values and enter the appropriate one in the **Workflow Settings** section. When entering the location, the file path is case-sensitive.

Workflow Definition Location

System	Workflow Definition Location
Documentum	`dctm://docbase/cabinet/foldername`
Livelink	`llin://repositoryname/workspace/folderpath`
File System	`//servername/servershare/foldername`
SharePoint	`shpt://repository/foldername`

6. Enter the appropriate values in the **Mail Settings** section:

Enable Notifications	`True`
Notification 'From' Address	For example: `<insight@liquent.com>`
Notification 'From' Name	*`<InSight>`*

7. Enter the appropriate values in the **Assembly Settings** section:

Reference Object Type	*`<dm_document>`*
Assembly Leaves Auto Create	`true`

8. Enter the appropriate values in the **Publishing Settings** section. Preserve case-sensitivity in the file path.

   DMS Type = `Documentum`, `Livelink`, `SharePoint`, `Secure File System` or `File system`

   `eCTD Location =` (When entering the location, the file path is case-sensitive. The DTD location was specified previously.)

Documentum	`dctm://docbase/cabinet/foldername`
Livelink	`llin://repositoryname/workspace/folderpath`
File system	`//servername/servershare/foldername`
SharePoint	`shpt://repository/foldername`
Company Name	*The name of your company*
Additional Documentum Rendition Formats	list of rendition's extensions in addition to 'pdf' for **Documentum** repository only. For example: `c2pdf, xpdf`

Note: The DMS Type and eCTD Location should match the repositories configured in Application Server Installation procedure.

9. This step is optional. Enter the appropriate values in the **SPOR API Settings** section:

Value	Description
`Enable SPOR API for RMS`*`<value>`*	The *<value>* is `false` by default. If you want the loading of RMS values from EMA SPOR REST Server, set this parameter to `true`. For example: `Enable SPOR API for RMS=true`

Value	Description
`Enable SPOR API for OMS <value>`	The *<value>* is `false` by default. If you want the loading of OMS values from EMA SPOR REST Server, set this parameter to `true`. For example: `Enable SPOR API for OMS=true`
`Default interval (minutes)`	The update interval. The service will run in the update interval provided.
`User Name=<user_name>`	The user name and password values must be requested from EMA authority.
`Password=<password>`	The user name and password values must be requested from EMA authority.

10. Enter the appropriate values in the **XEVMPD Settings** section:

Message Character Encoding	`UTF-8`
Formatted Output XML	`true`

Note: Message Character Encoding = UTF-8 or UTF-16 (If you leave this blank, the setting defaults to UTF-8.)

a) Set the following required parameters in `insight.var`:

Parameter	Description
Location for XEVMPD Submission	The path to the previously created and saved EMEA XML file.
Location for XEVMPD Acknowledgement	The path to the import folder from where the service will take files to import. It must also contain a subfolder named "processed". All processed files are moved to that folder by the service.
Defined interval (minutes)	The update interval. The service will run in the update interval provided.

11. **Note:** Perform this step only if your installation includes the Liquent InSight for Analytics license.

Enter the appropriate values in the **WebFocus Security Settings** section:

WebFocus Host	`http://host-name`
WebFocus Port	`25000`
WebFocus URL path	`/ibi_apps/`
Key (enciphering)	`WebFocus-Key`
Token life (sec)	`18000`

12. Enter the appropriate values in the **InSight Rendering Connection Settings** section.

Server	*<IRserver>*
Port	`2861`

- Server = `IR41`
- Port = `2861`

13. On the **Identity Provider Settings** tab, enter the appropriate values for the **LDAP Identity Provider Type**:

LDAP Server	*<insightpdc>*

Base query	`OU=Users,DC=insight`
User query	`CN=Administrator,OU=Users,DC=insight`
Password	*<password>*
Default admin	*<admin>* `CN=security admin,OU=insight Users,DC=insight`
LDAP Port	*389*
Use Secure LDAP	*True/False* (By default the value is False)
Secure LDAP Port	*636*

Note: Populating **LDAP Port**, the usage of the **Secure LDAP** and the**Secure LDAP Port** fields is optional. If they are not populated, then not secured 389 port will be used by default.

14. On the **Cleanup Schedule** tab, enter the appropriate values in the **Cleanup Schedule**.
    `Daily`
15. On the **Help** tab, enter the following value in the **Help Settings** field: `https://help.liquent.com/InSight_6-2-0/index.html`.
16. Select **File** > **Generate File** and **OK** to confirm.
    - The `insight.var` is successfully created in the `..conf\insight` directory with the correct settings.
    - The `oracle-ds.xml` is successfully created in the `..server\all\deploy` directory with the correct settings.

Note: The first generation of files will throw an error as it cannot backup files it is generating.

17. Select **File** > **Exit**.
18. Edit the `mail-service.xml` file located at `C:\InSightManager\server\all\deploy\`.
    Modify the mail.smtp.host and mail.smtp.port property values for the e-mail server name and port to be used for Liquent InSight notifications.

Enable Azure Active Directory (Azure SSO)

1. Locate the `insightConfig.bat` file in the *<installation drive>*`\InSightManager\server\all\conf\insight` installation directory and double-click the file.
   The **Configuration Settings** window appears.
2. In the left top menu of the **Configuration Settings** window, select **File** > **Load File**.
   The current configuration settings are populated to the **Configuration Wizard**.
3. In the left pane, select **Identity Provider Settings**.
4. Populate the following fields:

Field Name	Input Value
Identity Provider Type	`Azure Active Directory`
Application Logout URI	`https://login.microsoftonline.com/common/oauth2/logout?post_logout_redirect_uri=http(s)://{server}:{port}/insight`
Access Token URI	`https://login.microsoftonline.com/{Azure AD Directory ID}/oauth2/token`
Client ID	`<Azure AD Application ID>`

Field Name	Input Value
Client Secret	<The secret Key for Azure App registrations>
Key Discovery URI	https://login.windows.net/common/discovery/keys
User Authorization URI	https://login.microsoftonline.com/*<Azure AD Directory ID>*/oauth2/authorize
Issuer Base URI	https://sts.windows.net
Tenant ID	<Azure AD Directory ID>
SSO Trusted Applications	<CSV of application_ids for service such as InSightX or LES>
Graph API URI	https://graph.windows.net
Graph API Version	1.6
Default Admin	<Registered Azure AD user> For Example: "Name.Surname@corporation.com"
Use Multiple IDPs	<checked if Insight is going to be used with multiple IDP's only, like Azure+Okta>

5. Select **File** > **Generate File**.
   - The `insight.var` is successfully updated in the `..conf\insight` directory with the correct settings.
   - The `oracle-ds.xml` is successfully updated in the `..server\all\deploy` directory with the correct settings.
   - The `login-config.xml` is updated.
6. Select **File** > **Exit**.
   The Configuration Wizard is closed.
7. Restart the InSight service.

Enable Okta IdP for Liquent InSight

1. Locate the `insightConfig.bat` file in the *<installation drive>*`\InSightManager\server\all\conf\insight` installation directory and double-click the file.
   The **Configuration Settings** window appears.
2. On the **Configuration Settings** window, select **File** > **Load File**.
   The current configuration settings are populated to the **Configuration Wizard**.
3. In the left pane, select **Identity Provider Settings**.
4. Populate the following fields:

Field Name	Input Value
Identity Provider Type	Okta
Application Logout URI	https://{Okta Application Issuer}/oauth2/default/v1/logout\?id_token_hint=ID_TOKEN_PLACEHOLDER\&post_logout_redirect_uri=http://{insight server}:{port}/insight
Access Token URI	https://{Okta Application Issuer}/oauth2/default/v1/token
Client ID	{Okta Application Client ID}

Field Name	Input Value
Client Secret	`{Okta Application Client Secret}`
Key Discovery URI	`https://{Okta Application Issuer}/oauth2/default/v1/keys`
User Authorization URI	`https://{Okta Application Issuer}/oauth2/default/v1/authorize`
Issuer Base URI	`https ://{Okta Application Issuer} /oauth2/default`
Base API URL	`https://{Okta Application Issuer}/api/v1`
Authorization API Token	`{Okta Application Token}`
Default Admin	`{Registered Okta IDP user}` For example: `"FirstName.LastName@corporation.com"`
Use Multiple IDPs	`<checked if Insight is going to be used with multiple IDP's only, like Azure+Okta>`

5. Select **File** > **Generate File**.
   - The `insight.var` is successfully updated in the `..conf\insight` directory with the correct settings.
   - The `oracle-ds.xml` is successfully updated in the `..server\all\deploy` directory with the correct settings.
   - The `login-config.xml` is updated.
6. Select **File** > **Exit**.
7. Restart the InSight service.
8. Navigate to **Control Panel** > **Internet Options** and select the **Trusted Sites** on the **Security** tab.
9. Populate the **Add this website to the zone** field with: `https://{OKTA Application Issuer}`.
10. Select **Add**.
11. Select **Close**.
12. Select **OK**.

Enable PingOne IdP with Liquent InSight

1. Locate the `insightConfig.bat` file in the *<installation drive>*`\InSightManager\server\all\conf\insight` installation directory and double-click the file.
   The **Configuration Settings** window appears.
2. On the **Configuration Settings** window, select **File** > **Load File**.
   The current configuration settings are populated to the **Configuration Wizard**.
3. Select **Identity Provider Settings**.
4. Populate the following fields:

Field Name	Input Value
Identity Provider Type	`PingOne`
Base API URL	`https://directory-api.pingone.com/api/directory`
Authorization API Token	`{<Client ID>:<API Key> encoded to Base64}`
Application Logout URI	`https://sso.connect.pingidentity.com/sso/initslo\ ?page=http://{server}:{port}/insight/`

Field Name	Input Value
SAML Metadata	`saml2-metadata-idp.xml`
SAML Entity Id	`urn:test:app:saml`
SAML Keystore File Name	`{PingOne Keystore file}.jks`
SAML Keystore Password	`{Keystore password}`
SAML Key Name	`{Key Name}` For example: `aliasname` aliasname.
SAML Key Password	`{Key password}`
Default Admin	`{Registered PingOne IDP user}` For example: `"aminpingone"`

5. Select **File** > **Generate File**.
   - The `insight.var` is successfully updated in the `..conf\insight` directory with the correct settings.
   - The `oracle-ds.xml` is successfully updated in the `..server\all\deploy` directory with the correct settings.
   - The `login-config.xml` is updated.
6. Select **File** > **Exit**.
7. Locate the `saml2-metadata-idp.xml` file obtained from the **PingOne Application** page to the *<installation drive>*`\InSightManager\server\all\conf\insight` installation directory.
8. Run the Command Prompt (cmd) from *<installation drive>*`\InSightManager\server\all\conf\insight` installation directory. Paste the following command: `keytool -genkey -alias aliasname -keyalg RSA -keystore samlKeystore.jks -keysize 2048`, where {aliasname} is SAML Key Name property value and the samlKeystore.jks is SAML Keystore File Name property value.
9. Press **Enter**.
10. Populate the following fields:

Note: Remember to press **Enter** after each step below.

Field Name	Input Value
Enter keystore password	`{SAML Keystore Password property value}`
Re-enter new password	`{SAML Keystore Password property value}`
What is your first and last name?	`{valid data or leave blank}`
What is the name of your organizational unit?	`{valid data or leave blank}`
What is the name of your organization?	`{valid data or leave blank}`
What is the name of your City or Locality?	`{valid data or leave blank}`
What is the name of your State or Province?	`{valid data or leave blank}`

Field Name		Input Value
What is the two-letter country code for this unit?	CN	{valid data or blank}
	OU	{valid data or blank}
	O	{valid data or blank}
	L	{valid data or blank}
	ST	{valid data or blank}
	C	{valid data or blank}
Is correct?		{y}
Enter key password for		<aliasname> <RETURN if same as keystore password>:{SAML Key Password property value}
Re-enter new password		{SAML Key Password property value}

11. Press Enter and close the **Command Prompt**.
    After performing the actions in the Command Prompt, the `samlKeystore.jks` file is generated.

    Note: The current step is valid only for Java 8 version. For more details follow: https://docs.oracle.com/javase/8/docs/technotes/tools/windows/keytool.html#keytool_option_genkeypair
12. Restart the InSight service.
13. Go to **Control Panel** > **Internet Options** and select the **Trusted Sites** on the **Security** tab.
14. Populate the **Add this website to the zone** field with: `https://login.pingone.com`.
15. Select **Add**.
16. Select **Close**.
17. Select **OK**.

Increase Oracle Connections for InSight Manager

Refer to your Oracle Connection Settings Established when setting up your Liquent InSight Database instance for the actual Max-Pool-Size settings used.

Attention: Please consult with your DBA before making any changes described in this section.

1. Navigate to the directory *<installation drive>*`:\InSightManager\server\all\deploy` and open the file `oracle-ds.xml file` in Notepad.
2. Add the following lines to the two sections specified:

```
<jndi-name>ManagerDS</jndi-name>
<min-pool-size>1</min-pool-size>
<max-pool-size>500</max-pool-size>
```

and

```
<jndi-name>DefaultDS</jndi-name>
 <min-pool-size>1</min-pool-size>
<max-pool-size>500</max-pool-size>
```

3. Save and close the file.
4. Navigate to the directory `X:\InSightManager\server\all\deploy\hornetq` and open the `jms-ds.xml` file in Notepad.
5. Change the max pool size value to `500`.

```
<tx-connection-factory>
   <jndi-name>JmsXA</jndi-name>
   <xa-transaction/>
   <rar-name>jms-ra.rar</rar-name>
   <connection-definition>org.hornetq.ra.HornetQRAConnectionFactory</
connection-definition>
   <config-property name="SessionDefaultType"
type="java.lang.String">javax.jms.Topic</config-property>
   <config-property name="JmsProviderAdapterJNDI"
type="java.lang.String">java:/DefaultJMSProvider</config-property>
   <max-pool-size>500</max-pool-size>
   <security-domain-and-application>JmsXARealm</security-domain-and-
application>
  </tx-connection-factory>
```

6. Save and close the file.
7. Navigate to the directory *<installation drive>*`:\InSightManager\server\all\deploy\jbossweb.sar` and open the file `server.xml` in Notepad.
8. Change the values for max threads to `1000`.

```
  <Connector protocol="HTTP/1.1"
address="${jboss.bind.address}"
port="${jboss.web.http.port}"
redirectPort="${jboss.web.https.port}"
maxPostSize="150000000"
maxThreads="1000"
maxHttpHeaderSize="8192"
acceptCount="100"
enableLookups="false"
connectionTimeout="20000"
disableUploadTimeout="true"
URIEncoding="UTF-8"
compression="on"

compressableMimeType=
"text/html,text/xml,text/javascript,text/css"
  />
```

9. Save and close the file.
10. Navigate to the directory *<installation drive>*`:\InSightManager\server\all\deploy\` and open the file `jca-jboss-beans.xml` file in Notepad.

11. Change the debug attribute to `false`:

```
<!-- Whether to track unclosed connections and close them -->
   <property name="debug">false</property>
```

12. Save and close the file.

Specify the number of prepared statements per connection in an LRU cache keyed by the SQL query (set to zero disables the cache)

Attention: Please consult with your DBA before making any changes described in this section.

1. Navigate to the directory *<installation drive>*`:\InSightManager\server\all\deploy` and open the file `oracle-ds.xml file` in Notepad.
2. Add the following lines to the two sections specified:

```
 <jndi-name>ManagerDS</jndi-name>
 <prepared-statement-cachesize>100</prepared-statementcache-size>
```

and

```
<jndi-name>DefaultDS</jndiname>
 <prepared-statement-cachesize>100</prepared-statementcache-size>
```

Note: It is just example for modifying value `prepared-statementcache-size`. Setting this to zero disables the cache.

3. Save and close the file.

Access Liquent Online Help

Note: Following steps to be performed only for new installation.

Submit your external IP addresses to Parexel.

To use help.liquent.com in a Liquent InSight environment, high-speed Internet access is required from the Liquent InSight client workstation computers. To enable access to help.liquent.com for your Liquent InSight users, you must send the external IP addresses of your Liquent InSight workstations to your Parexel Account Executive or Parexel Technical Support.

External IP addresses can be determined by going to whatismyip.com in a Web browser on the Liquent InSight client computer.

The security model for help.liquent.com is based on IP filtering. Therefore, the external IP addresses of your Liquent InSight users are required to grant access to the site.

The external IP address information will be forwarded to Technical Publications so that the IP filtering settings for the help.liquent.com site can be updated.

Perform tests from your Liquent InSight environment to confirm that help.liquent.com is accessible. For technical issues related to help.liquent.com, please contact Parexel Technical Support.

Additional Configurations

This topic describes the additional functionalities that can be configured for each Liquent InSight 6.2 CHF, unless otherwise is stated.

The following table lists the procedures that can be performed to configure additional features. Carefully review these procedures before moving forward through the installation process.

Topic Name	Topic Location: Liquent InSight 6.2 Installation Guide
Liquent InSightConfiguration	Liquent InSightConfiguration
Enabling Azure Active Directory "Azure SSO" for LIQUENT InSight	Enabling Azure Active Directory "Azure SSO" for LIQUENT InSight
Increasing the Oracle Connections for InSight Manager	Increasing the Oracle Connections for InSight Manager
Accessing Liquent InSight Online Help	Accessing Liquent InSight Online Help
Enabling Change Password Functionality	Enabling Change Password Functionality
Limiting Product Family and Country Tree Expand Range	Limiting Product Family and Country Tree Expand Range
Limiting Assembly Tree Expand Range	Limiting Assembly Tree Expand Range
Limiting the Assembly Tree Search Results	Limiting the Assembly Tree Search Results
Re-configuring the Consumer Count for a Specific Domain	Re-configuring the Consumer Count for a Specific Domain
Remember Last Logged On User	Remember Last Logged On User
eCTD Bulk Import	eCTD Bulk Import
Setting up Document Management Systems (DMS)	Setting up Document Management Systems (DMS)
Adding a SharePoint DMS Server	Adding a SharePoint DMS Server
LIQUENT InSight Application Server Installation Prerequisites For SharePoint Only	LIQUENT InSight Application Server Installation Prerequisites For SharePoint Only
Adding a Livelink DMS Server	Adding a Livelink DMS Server
Adding a Documentum DMS Repository for LIQUENT InSight	Adding a Documentum DMS Repository for LIQUENT InSight
Additional Prerequisites for Documentum System	Additional Prerequisites for Documentum System
Adding a File System DMS Repository for LIQUENT InSight	Adding a File System DMS Repository for LIQUENT InSight
Adding a Secure File System DMS Repository for LIQUENT InSight	Adding a Secure File System DMS Repository for LIQUENT InSight
Adding a Veeva Vault DMS Repository for LIQUENT InSight	Adding a Veeva Vault DMS Repository for LIQUENT InSight

Topic Name	Topic Location: Liquent InSight 6.2 Installation Guide
Increasing the Transaction Timeout	Increasing the Transaction Timeout
Re-extracting Documents and Regenerating TOC for Active Assemblies	Re-extracting Documents and Regenerating TOC for Active Assemblies
Creating or Recreating Assembly File Templates	Creating or Recreating Assembly File Templates
Activating Kendo Window UI	Activating Kendo Window UI
Note: The changes made to the `insight.var` file will take effect after restarting the server.	

Enable Change Password Functionality

An optional functionality of Liquent InSight 6.2 provides the ability to change passwords on the login page.

To enable the change password functionality, the system must have SSL configured and the option `change.password.enable=true` must be set in the `insight.var` file.

To use secure connections, Liquent InSight must be able to validate the certificate presented by an LDAP directory server. To do this you must import the root certificate (the Certificate Authority certificate) into the keystore (the `cacerts` file) for the Java Runtime Environment (JRE) used by Liquent InSight. Run the following command: `install_dir/bin/jre/bin/keytool -import \ -keystore install_dir/bin/jre/lib/security/cacerts \ -file root_certificate_path \ -alias alias`

We recommend you use the `-alias` option to uniquely identify the certificate. The standard password for the `cacerts` file is `changeit`. You must import the root certificate for every LDAP directory server you are using with Liquent InSight. Creating client certificates for use with Microsoft Active Directory will only accept secure connections from Liquent InSight if it has a valid client certificate that has been signed using the Certificate Services on a Windows 2012 R2 Server. You must do this in addition to importing the root certificate, as described above. To do this, you must:

- Generate the key pair for the client certificate
- Generate a Certificate Signing Request (CSR) for the client certificate
- Create the client certificate
- Install the client certificate

Update Backbone Generator Files on IR Server

This procedure should be performed by the Liquent InSight Publishing users only.

1. Unzip `ectd-backbone.zip` from the installation media to a temporary directory.
2. Copy the contents of the *ectd-backbone directory* (for example, only the files) to the following directory on each Liquent InSight Rendering Rendering (IR) server that you set up to connect with Liquent InSight 6.2 CHF 3: `<InSight Rendering installation drive>:\Program Files\Common Files\Liquent \BackboneGeneratorService\3.5\Lib`
3. Restart each server to ensure that each changed Liquent InSight Rendering server detects and uses the changes.
4. Delete the temporary directory created before.

Limit Product Family and Country Tree Search Results

Liquent InSight enables you to set a limit to the number of search results that are displayed when filtering the Product Family and Country trees in the Navigation Pane.

To limit the number of search results that are displayed:

1. Open the `insight.var` file in a text editor.
2. Add the following parameter to the file: `tree.search.result.limit=<limitation value>`.
   Replace <*limitation value*> with a number that specifies the maximum number of search results..
   For example:

`tree.search.result.limit=`	`100`

Note: if the parameter is not specified then the default limitation is 500 nodes is applied.

3. Save the `insight.var` file.

Limit Assembly Tree Expand Range

Liquent InSight enables you to limit the number of nodes that can be expanded in an assembly tree.

The default limit can be overridden by defining a new value in the `insight.var` file.

To define a limit to the number of nodes that can be expanded:

1. Open the `insight.var` file in a text editor.
2. Add the following parameter to the file: `assembly.tree.expand.range.limit=<limitation value>`.
   Replace <*limitation value*> with a number that specifies the maximum number of nodes that can be expanded.
   For example:

`assembly.tree.expand.range.limit=`	`100`

Note: if the parameter is not specified then the default limitation is 1000 nodes is applied.

3. Save the `insight.var` file.

Limit Assembly Tree Search Results

Liquent InSight enables you to search for assembly tree elements in an assembly using the search option on the assembly tree.

The display of the number of assembly tree elements that match the search criteria can be restricted by defining an upper limit in the `insight.var` file.

To limit the number of search results that are displayed:

1. Open the `insight.var` file in a text editor.
2. Add the following parameter to the file: `assembly.tree.search.result.limit=<limitation value>`.
   Replace <*limitation value*> with a number that specifies the maximum number of nodes that can be expanded.
   For example:

assembly.tree.search.result.limit=	100

Note: if the parameter is not specified then the default limitation is 1000 nodes is applied.

3. Save the `insight.var` file.

Enable Data Exchange for Liquent InSight

To use the Data Exchange feature in Liquent InSight, the IP address and domain name must be defined in the `DataExchangeConfig.xml` file.

To enable the Data Exchange feature in Liquent InSight 6.2 CHF 3:

1. Update the `DataExchangeAuthConfig.xml` file with the IP address (IPv4) and/or Name of the your machine in the *<installation drive>*`\InSightManager\server\all\conf\insight\` directory.

```
<constructor-arg index="1">
     <list>
         <value> IP address of the machine </value>
     </list>
  </constructor-arg>

<constructor-arg index="2">
     <list>
         <value> machine.domain.name.com </value>
     </list>
  </constructor-arg>
```

2. Save and close the file.

Re-configure Consumer Count for a Specific Domain

If the consumer count for a specific domain is going to be changed then the `ejb3-interceptors-aop.xml` file should be updated.

1. In the `%INSIGHT_HOME%/server/all/deploy` directory, open the `ejb3-interceptors-aop.xml` file.
2. Under the specific domain description update the following parameters:

value=	*"StrictMaxPool"*
maxSize=	*<value>*
propertyName=	*"maxSession"*
propertyValue=	*<value>*

Note: The maxSize parameter on the StrictMaxPool needs to be the same as the maxSession set on the bean itself.

Enable DFC Class 7.2 Patch 3

1. Stop the InSight Manager service.
2. Go to the `%INSIGHT_HOME%\server\all\lib` folder and remove the following files:

- certj-6.2.1.jar
- configservice-api-16.4.jar
- configservice-impl-16.4.jar
- cryptoj-6.2.2.jar
- cryptojce-6.2.2.jar
- cryptojcommon-6.2.2.jar
- dfc-16.4.jar
- jcm-6.2.0.jar
- jcmFIPS-6.2.0.jar
- util-6.2.2.jar

3. Go to the Liquent InSight installation media and unpack the files from the archive `dfc_7.2.zip` located in the DFC directory to the `%INSIGHT_HOME%\server\all\lib` folder.
   The new DFC class dependencies are copied into the folder.
4. Go to the `%DFC_CONFIG%\` folder and update the **dfc.properties** settings for content provider:

dfc.docbroker.host[0]	`Content_Host`
dfc.docbroker.port[0]	`1489`
dfc.crypto.repository	`DCTM_XX`
dfc.globalregistry.repository	`DCTM_XX`

5. Start the InSight Manager service.

Enable Documentum D2

This procedure is optional and can be performed if Liquent InSight will be used with Documentum D2.

1. Navigate to the following directory: *<installation Drive>*`\InSightManager\server\all\conf\insight`, and double-click the `insightConfig.bat` file.
2. Enter the appropriate values in the **D2 Life Sciences Integration Settings** section:

`D2 DFS URL=`	*<Hyperlink to the Repository>*
`D2 Repository=`	*<Name of the Repository>*
`D2 Username=`	*<username>*
`D2 Password=`	*<password>*

   For example:

`D2 DFS URL=`	*http://d2abcd:8080/efgf/services*
`D2 Repository=`	*D2REP*
`D2 Username=`	*guest*
`D2 Password=`	*changeme*

3. Select **File** from the Main Menu and then select **Generate File** option.
4. Click **OK** to continue.
5. Select **File** > **Exit**.

Remember Last Logged On User

To add the ability for the system to remember the last logged on user in Liquent InSight, do the following:

1. Navigate to the `C:\InsightManager\server\all\conf\insight` folder and open the `insight.var` file in Notepad.
2. Add the following lines to the `insight.var` file:

```
##### LOGIN SETTINGS  #####

login.remember.me=true

login.days.to.remember.me=14
```

3. Save the `insight.var` file.

Note: This information will move to a section of the `insight.var` file titled `ADDITIONAL VALUES` every time the file is regenerated.

eCTD Bulk Import

The bulk import functionality requires specific default values for the number of concurrently running import jobs (default is `3`), and for the frequency that the system checks for a free place in the queue (in seconds, default is `300`). To define the eCTD Bulk Import values for your system:

1. Go to the directory `C:\InSightManager\server\all\conf\insight` and open the `insight.var` file in a text editor.
2. At the bottom of the `insight.var` file, add the following records:

   `#####Bulk Import Settings#####`

   `bulk.ectd.import.limit = 3` (the number of concurrently running import jobs)

   `bulk.ectd.import.update.interval = 300` (frequency of checking if there is a free place in the queue, in seconds)
3. Save the `insight.var` file.

Note: This information will move to a section of the `insight.var` file titled `ADDITIONAL VALUES` every time the file is re-generated.

Enable SSL for Liquent InSight

Due to the complexity of configuring Liquent InSight for use in an SSL (Secure Sockets Layer) environment, all SSL configurations must be done by the Client Enablement team. Outside RSA certificates may be involved, several browser-specific configuration modifications are necessary, and there are multiple ways to set up SSL, some of which Liquent InSight may not be able to support.

Warning: SSL configurations are supported only when they are installed by Client Enablement, and only defects that can be duplicated on a normal Liquent InSight installation will be addressed.

1. To enable SSL, some modifications need to be made to the `%INSIGHT_HOME%/server/all/deploy/jbossweb.sar/server.xml` file.
2. Open the `server.xml` file.
   a) Comment out the following block of code to disable http connections on port 8080 by using the comment tags (<!-- and -->):

```
<Connector protocol="HTTP/1.1"
address="${jboss.bind.address}"

port="${jboss.web.http.port}"
redirectPort="${jboss.web.https.port}"

maxPostSize="150000000"
maxThreads="250" acceptCount="100"
enableLookups="false"

connectionTimeout="20000"
disableUploadTimeout="true"
URIEncoding="UTF-8"

compression="on"
compressableMimeType="text/html,text
/xml,text/javascript,text/css"

/>
```

   b) Uncomment the following block of XML to enable https connections on port 8443 by removing the comment tags (<!-- and -->):

```
<Connector protocol="HTTP/1.1"
address="${jboss.bind.address}"
port="${jboss.web.https.port}"

SSLEnabled="true" scheme="https"
secure="true"

maxPostSize="150000000"
maxThreads="250" acceptCount="100"
enableLookups="false"

connectionTimeout="20000"
disableUploadTimeout="true"
URIEncoding="UTF-8"

compression="on"
compressableMimeType="text/html,text
/xml,text/javascript,text/css"

SSLVerifyClient="none" SSLProtocol="TLSv1"

SSLCertificateFile="${jboss.server.base.dir}/all
/conf/insight/insightcert.pem"

/>
```

3. Update the `insight.var` file:
   - `useSsl=true`
   - `port=8443`
4. Restart the InSight service.

Enable SSL for Liquent InSight Rendering Services Server 4.4

Note: This step is only for Liquent InSight Rendering Services Server 4.4, which works with Liquent InSight Application Server with Enabled SSL.

Ensure that the Liquent InSight 6.2 CHF 3 SSL Application Server certificate is installed for the service account running Liquent InSight on every Liquent InSight Rendering server where the IRS is installed.

Liquent InSight License and Liquent InSight Manager Service Setup

1. Copy your Liquent InSight license file from the Liquent InSight installation media (or obtain it from your Liquent InSight representative) and paste it into the following directory: `C:\InSightManager\server\all\conf\insight`
   a) Rename the file to: `license.xml`
2. Right-click on the Windows **Start** button and select **Run**.
3. Type `services.msc` and press Enter.
4. Right-click the **InSight Manager** service and select **Properties**.
   a) Verify the startup type is **Automatic**.
   b) Click the **Start** button.

   Note: If the service will not start, the `run.conf.bat` file might need to be changed to suit the environment – for details check the `run.conf.bat` at `C:\InSightManager\bin`.
5. Select the **Log On** tab.
6. Choose the option **This Account** and complete the **This Account** and **Password** boxes using the local administrator service account used during installation. Confirm the Password and then click **OK**.
7. **Stop** and **Start** the Service. **Close** the **Server Manager services** window.

Liquent InSight Communication and License Confirmation

Perform the following procedure to configure your Liquent InSight module licenses.

1. Open Internet Explorer and enter the URL for your local server name, and press **Enter**.
   `http://`*`server name`*`:`*`port number`*`/insight`
2. Enter the following values and then click the **Login** button.

- Username: `admin`
- Password: `admin`

3. Open the **Go To** menu.
4. Click the **Security Administration** link.
5. Under the display name, click **admin** (for example) to view privileges.
6. For reference, note your active Liquent InSight license modules by entering `Active` in the line following the component:

   SPT _____

   RDA _____

   RPT _____

   PDM _____

   ELP _____

   PRP _____

   PSP _____ Inactive_____

   IRI _____ Inactive_____

   LIQUENT InSight for Analytics_____

   XEVMPD_____

   LIQUENT InSight Workflow Integration____

   Note: Active modules will have active drop-down lists in the **Access** column of the screen.

7. Logout of Liquent InSight by clicking **Logout** (open door icon) at the top right area of the window.

Set Up Identity Provider

This procedure should be performed if the multi.idp.use flag is set to true only in the insight.var in the<*installation drive*>:\InSightManager\server\all\conf\insight installation directory.

1. Open Internet Explorer and enter the URL for your local server name , and press **Enter**.
   `http://server name:port number/insight`
2. Enter the following values and then click the **Login** button.
   - Username: `admin`
   - Password: `admin`
3. In Liquent InSight, add a DMS server, if it is not added:
   a) Select **Go To > Security Administration**.
   b) Click **Identity Providers**.
   c) To add a new Identity Provider, click the **Create** icon.

   The **Identity Provider** page appears.

What to do next
Refer to *Add Azure IdP*, *Add Okta IdP*, or *Add PingOne IdP*, depending on Identity Provider Type(s) you are adding.

Add Azure IdP

This procedure should be performed if the multi.idp.use flag is set to true only in the insight.var in the<*installation drive*>:\InSightManager\server\all\conf\insight installation directory.

Note: Verify that there are no active Identity Providers (IdP) in the system and you performed all the steps described in *Set Up Identity Provider*.

1. To add a new Azure IdP, add the following information on the Identity Provider page:

Field Name	Input Value
Provider Type	`<Azure Active Directory>`
Identity Provider Name	`<Identity Provider Name>` Any unique name to identify this IDP in Liquent InSight. Example: Azure123
Application Logout URI	`https://login.microsoftonline.com/common/oauth2/logout?post_logout_redirect_uri=http(s)://{server}:{port}/insight`
Access Token URI	`https://login.microsoftonline.com/{Azure AD Directory ID}/oauth2/token`
Client ID	`<Azure AD Application ID>`
Client Secret	`<The secret Key for Azure App registrations>`
Key Discovery URI	`https://login.windows.net/common/discovery/keys`
User Authorization URI	`https://login.microsoftonline.com/<Azure AD Directory ID>/oauth2/authorize`
Issuer Base URI	`https://sts.windows.net`
Tenant ID	`<Azure AD Directory ID>`
SSO Trusted Applications	`<CSV of application_ids for service such as InSightX or LES>`
Graph API URI	`https://graph.windows.net`
Graph API Version	`1.6`

2. **Save**.
   The Azure IdP is added to Liquent InSight.
3. Restart the InSight Manager service.

Add Okta IdP

This procedure should be performed if the multi.idp.use flag is set to true only in the insight.var in the<*installation drive*>:\InSightManager\server\all\conf\insight installation directory.

Note: Verify that there are no active Identity Providers (IdP) in the system and you performed all the steps described in *Set Up Identity Provider*.

1. To add a new Okta IdP, add the following information on the Identity Provider page:

Field Name	Input Value
Provider Type	<Okta>
Identity Provider Name	<Identity Provider Name> Any unique name to identify this IDP in Liquent InSight. Example: Okta123
Application Logout URI	https://{Okta Application Issuer}/oauth2/default/v1/logout\?id_token_hint=ID_TOKEN_PLACEHOLDER\&post_logout_redirect_uri=http://{insight server}:{port}/insight
Access Token URI	https://{Okta Application Issuer}/oauth2/default/v1/token
Client ID	{Okta Application Client ID}
Client Secret	{Okta Application Client Secret}
Key Discovery URI	https://{Okta Application Issuer}/oauth2/default/v1/keys
User Authorization URI	https://{Okta Application Issuer}/oauth2/default/v1/authorize
Issuer Base URI	https ://{Okta Application Issuer} /oauth2/default
Base API URL	https://{Okta Application Issuer}/api/v1
Authorization API Token	{Okta Application Token}

2. **Save**.
   The Okta IdP is added to Liquent InSight.
3. Restart the InSight Manager service.

Adding PingOne IdP

This procedure should be performed if the multi.idp.use flag is set to true only in the insight.var in the<*installation drive*>:\InSightManager\server\all\conf\insight installation directory.

Note: Verify that there are no active Identity Providers (IdP) in the system and you performed all the steps described in *Set Up Identity Provider*.

1. To add a new PingOne IdP, add the following information on the Identity Provider page:

Field Name	Input Value
Provider Type	<PingOne>
Base API URL	https://directory-api.pingone.com/api/directory
Authorization API Token	{<Client ID>:<API Key> encoded to Base64}
Application Logout URI	https://sso.connect.pingidentity.com/sso/initslo\ ?page=http://{server}:{port}/insight/
SAML Metadata	saml2-metadata-idp.xml
SAML Entity Id	urn:test:app:saml
SAML Keystore File Name	{PingOne Keystore file}.jks
SAML Keystore Password	{Keystore password}

Field Name	Input Value
SAML Key Name	{Key Name} For example: aliasname aliasname.
SAML Key Password	{Key password}

2. **Save**.
   The PingOne IdP is added to Liquent InSight
3. Locate the saml2-metadata-idp.xml file obtained from the **PingOne Application** page to the *<installation drive>*\InSightManager\server\all\conf\insight installation directory.
4. Run the Command Prompt (cmd) from *<installation drive>*\InSightManager\server\all\conf\insight installation directory. Paste the following command: keytool -genkey -alias aliasname -keyalg RSA -keystore samlKeystore.jks -keysize 2048, where {aliasname} is SAML Key Name property value and the samlKeystore.jks is SAML Keystore File Name property value.
5. Press **Enter**.
6. Populate the following fields:

Note: Remember to press **Enter** after each step below.

Field Name		Input Value
Enter keystore password		{SAML Keystore Password property value}
Re-enter new password		{SAML Keystore Password property value}
What is your first and last name?		{valid data or leave blank}
What is the name of your organizational unit?		{valid data or leave blank}
What is the name of your organization?		{valid data or leave blank}
What is the name of your City or Locality?		{valid data or leave blank}
What is the name of your State or Province?		{valid data or leave blank}
What is the two-letter country code for this unit?	CN	{valid data or blank}
	OU	{valid data or blank}
	O	{valid data or blank}
	L	{valid data or blank}
	ST	{valid data or blank}
	C	{valid data or blank}
Is correct?		{y}
Enter key password for		<aliasname> <RETURN if same as keystore password>:{SAML Key Password property value}
Re-enter new password		{SAML Key Password property value}

7. Press Enter and close the **Command Prompt**.
   After performing the actions in the Command Prompt, the samlKeystore.jks file is generated.

Note: The current step is valid only for Java 8 version. For more details follow: https://docs.oracle.com/javase/8/docs/technotes/tools/windows/keytool.html#keytool_option_genkeypair

8. Restart the InSight service.
9. Go to **Control Panel** > **Internet Options** and select the **Trusted Sites** on the **Security** tab.
10. Populate the **Add this website to the zone** field with: `https://login.pingone.com`.
11. Select **Add**.
12. Select **Close**.
13. Select **OK**.

Set Up Document Management Systems (DMS)

Liquent InSight enables you to establish multiple DMS servers through the Administration interface.

Use the Liquent InSight Administration interface to add DMS servers and repositories. Repeat the relevant steps in this section to establish multiple DMS servers.

1. On the Windows desktop, click **Start**, type `services.msc`, and press Enter.
2. Go to the **Services** window and confirm that the InSight Manager service is running.
3. Start Internet Explorer and enter the URL for InSight Manager.
   `http://<server name>:<port number>/insight`
4. Enter the following values, then click the **Login** button:
   - Username: `admin`
   - Password: `admin`
5. In Liquent InSight, add a DMS server (if it is not already added):
   a) In the **Go to** menu, select **Technical Administration**.
   b) Click **DMS Server Management**.
   c) Click the **Create** icon to add a new DMS server.
6. Proceed to the next step(s), according to the DMS Server Type(s) you are adding.

Add a SharePoint DMS Server

1. To create a DMS repository in Liquent InSight, the DMS Server must be configured first.
2. Ensure that the network service account on your SharePoint Host server has change rights to the directory specified in the system temp folder. The default directory is: `c:\windows\temp`
3. To add a SharePoint DMS server, add the following information on the **Servers** page:

Parameter	Value
Server Type:	`<SharePoint>`
Server Name:	*`<SharePoint_Server_Name>`* **Note:** Any unique name to identify this server in Liquent InSight (for example: *SP2013*).
Active Flag:	`Y`
Host Name:	*`<SharePoint_Server>`*

Parameter	Value
Port:	80
LIQUENT Webservice URL:	http://SharePoint_Server/SitePages/Home.aspx
Timeout:	

Note: To use a specific site within SharePoint, use a combination of Host Name, Port on DMS Server Management page, and SharePoint Library field from DMS Repository Management page. Example – *http://SharePoint_Server/sites/PD*

To configure the information correctly:

Parameter	Value
Host Name:	http://SharePoint_Server
Port:	80
Share Point Library:	sites/PD

Adding a Livelink DMS Server

1. To create a DMS repository in Liquent InSight, the DMS Server must be configured first.
2. To add a new Livelink DMS server to your Liquent InSight system, add the following information on the **Servers** page.

Parameter	Value
Server Type:	<Livelink>
Server Name:	*<Livelink server name>* **Note:** Any unique name to identify this server in Liquent InSight (for example: *Livelink3*).
Active Flag:	Y
Host Name:	*<Livelink server host name>* **Note:** Name of the machine hosting Livelink. (for example: *livelink3*).
Port:	*<Livelink server portnumber>* **Note:** Default value is 2099. Port is specified in opentext.ini file. The opentext.ini file can be found on the Livelink host in the *<LIVELINK_HOME>*\config directory.

Add a Documentum DMS Repository

1. To create a DMS repository in Liquent InSight, the DMS Server must be configured first.
2. To add a new Documentum DMS repository, add the following information on the **Repositories** page:

Parameter	Value
Server Type:	Documentum
Server Name:	*<Documentum>*
Active Flag:	Y

3. To add a new File System DMS repository, add the following information on the **Repositories** page:

Parameter	Value
Server Name:	*<Server name>*
Active Flag:	Y

Add a Secure File System DMS Repository

1. To create a DMS repository in Liquent InSight, the DMS Server must be configured first.
2. To add a new File System DMS repository, add the following information on the **Repositories** page:

Parameter	Value
Server Name:	*<Server name>*
Active Flag:	Y

Increase the Transaction Timeout (optional)

When running the Prepare for Publish process, if you elect to perform several of the Prepare for Publish options during the process, the process may fail due to a timeout error. This timeout issue can be avoided by increasing the default transaction timeout value.

1. Using Notepad, open the file: `X:\InSightManager\server\all\deploy\Transaction-jboss-beans.xml`.
2. Locate the following section of code:

```
<bean name="CoordinatorEnvironmentBean"
class="com.arjuna.ats.arjuna.common.CoordinatorEnvironmentBean">

<annotation>@org.jboss.aop.microcontainer.aspects.jmx.JMX(name="jboss.jta:name
=CoordinatorEnvironmentBean",
exposedInterface=com.arjuna.ats.arjuna.common.CoordinatorEnvironmentBeanMBean.
class,
registerDirectly=true)</annotation>

<constructor
factoryClass="com.arjuna.ats.arjuna.common.arjPropertyManager"
factoryMethod="getCoordinatorEnvironmentBean"/>

<property name="enableStatistics">false</property>

<property name="defaultTimeout">3600</property>
```

```
</bean>
```

3. The `defaultTimeout` attribute is set to `3600` seconds (one hour) by default. This value can be increased to avoid transaction timeout issues.
4. Save your change and close Notepad.
5. Restart the InSight Manager service.
   a) Click **Start**, type `services.msc`, and press Enter.
   b) Right-click the **Insight Manager** service and choose **Restart**.

Create Assembly File Templates

1. Open Internet Explorer and enter the URL for your local server name and press Enter.
   Example: `http://server name:port number/insight`
2. Enter the following values, then click **Login**.
   Table 1: Create Assembly File Templates

Field Name	Value
Username:	`admin`
Password:	`admin`

3. In the left pane, click the **Assembly Templates** tab. In the **Name** column, click the **eCTD ICH MODULE 2-5 v3.2** template.
4. In the Assembly Attributes toolbar, click the **down arrow**, and then click **Delete** to remove the template.
   If this is a new installation, no templates will be in the system for deletion.
5. In the Liquent InSight menu bar at the top of the page, click: **New** > **Assembly Template**
6. Select **Assembly File** and then browse to the DMS/file system where you imported/copied your templates.
   a) Choose the **eCTD ICH MODULE 2-5 v3.2.xml** assembly template file.
   b) Click **OK**.
   For ELP or PRP module installation, complete *Re-extracting Documents and Regenerating TOC for Active Assemblies*.
   Non Electronic Lifecycle Publishing (ELP) or Paper Review Publishing (PRP) module installation qualification is complete.

Activate Kendo Window UI

1. Navigate to the `C:\InsightManager\server\all\conf\insight` folder and open the `insight.var` file in Notepad.
2. Select section **############ BROWSER INDEPENDENCE SETTINGS ###########**.
   a) For the insight.window.type.kendo variable, set the value as `true`:
   `insight.window.type.kendo=true`
3. Save and close the `insight.var` file.
4. Restart the InSight service.

Configure the Veeva Cache Timeout Setting

The following procedure describes the configuration required to set the appropriate Veeva cache timeout.

To set the Veeva cache timeout value:

1. Navigate to the `C:\InsightManager\server\all\conf\insight` folder.
2. Open the `insight.var` file in a text editor.
3. Update the following parameters:
   - `cache.timeout.dms.document=<veeva document cache timeout value>`. Replace *<veeva document cache timeout>* with an integer value in seconds.
   - `cache.timeout.dms.user=<veeva user cache timeout value>`. Replace *<veeva user cache timeout>* with an integer value in seconds.

   By default, the parameters are set as following:

`cache.timeout.dms.document=`	`180`
`cache.timeout.dms.user=`	`1000`

4. Save the `insight.var` file.

Liquent InSight Client Configuration

Perform the following procedure to configure Internet Explorer settings to work with Liquent InSight.

1. Log on to the client machine as a Local Administrator (with privileges for client installations).
2. Open Internet Explorer.
3. In Internet Explorer, choose **Tools** > **Internet Options**.
4. On the **General** tab, under **Browsing History**, click **Settings** and do the following:
   a) Set **Check for newer versions of stored pages** to **Automatically**.
   b) Set **Amount of disk space to use** to a minimum of 1000 MB.
   c) Click **OK**.
5. On the **Security** tab, confirm that **Internet** is selected in the **Select zone to view or change security**. Click **Custom Level** and define the following settings. Under **Miscellaneous**, do the following:
   a) Set **Allow META REFRESH** to **Enable**.
   b) Set **Submit nonencrypted form data** to **Enable**.
   c) Set **Userdata persistence** to **Enable**.
   d) Click **OK**, and then click **OK** when prompted.
6. When using Liquent InSight in an SSL environment define the following:
   a) On the **Security** tab, confirm that **Internet** is selected in the **Select zone to view or change security**. Click **Custom Level** and define the following settings:
   b) Under **Miscellaneous**, set **Display mixed content** to **Enable**.
   c) Click **OK** and then click **OK** when prompted.
7. On the **Privacy** tab define the following:
   a) Select **Advanced**.
   b) For Windows 7 or 8.1, select **Override automatic cookie handling**.
   c) Select **Always allow session cookies**.
   d) Click **OK**.
   e) Under **Pop-up Blocker**, select **Turn on Pop-up Blocker**.
8. Click **Apply** > **OK** to close the **Internet Options** window.
9. Close Internet Explorer, then log off of the client machine.
10. Verify Google Chrome is installed on the client machine.
11. Verify Microsoft Edge is installed on the client machine.
12. Optional Step: Verify SmartLink Installations
    - Verify LIQUENT SmartLink for PDF 1.8 or 1.8 CHF 1 is installed.
    - Verify LIQUENT SmartLink for Word 1.8 or 1.8 CHF 1 is installed.
    - Logout of the client machine.
13. Optional Step: Add **"OKTA SSO"** to **Trusted sites** .
    - Navigate to **Control Panel -> Internet Options.**.
    - Select **Security -> Trusted sites**.
    - Select **Sites**.
    - Populate the **Add this website to the zone** with: `https://{OKTA Application Issuer}`.
    - Select **Add**.
    - Select **Close**.

- Select**OK**.

14. Optional Step: Add **"PingOne SSO"** to **Trusted sites**.
    - Navigate to **Control Panel -> Internet Options**.
    - Select **Security -> Trusted sites**.
    - Select **Sites**.
    - Populate the **Add this website to the zone** with: `https://login.pingone.com` and `http{s}://{InSight server}`.
    - Select **Add**.
    - Select **Close**.
    - Select**OK**.

Internet Explorer: Enable Drag-and-Drop from Veeva DMS

Perform this setup procedure in the Internet Explorer browser to enable the drag-and-drop function from Veeva DMS.

To enable the drag-and-drop function from Veeva DMS (from a separate Veeva Vault window):

1. In the Internet Explorer browser, navigate to **Settings** > **Internet Options**.
2. In the **Internet Options** pop-up window, open the **Security** tab and click **Trusted Sites**.
3. Do the following for the Trusted Sites:
   a) Clear the **Enable Protected Mode** option.
   b) Click **Sites**. The **Trusted sites** pop-up window opens.
   c) Enter the following one by one and click **Add**: `<Insight Manager URL>` and `<Veeva Vault URL>`.

   Note: You can use your Veeva Vault name to make the configuration specific for one Veeva Vault only. For example: `https://<vault_name>.veevavault.com`, where <vault_name> is the actual Veeva Vault name.

   Replace the <Insight Manager URL> with the InSight server that you use.
   d) Click **Close**.
4. In the **Internet Options** pop-up window, downgrade the **Security level for this zone: All** parameter to **Medium-low**.
5. In the **Internet Options** pop-up window, click **Custom level...**.
   a) In the **Security Settings - Trusted Sites Zone** pop-up window scroll down to the **Miscellaneous** and update the following settings:

Allow dragging content between domains into separate window	**Enable**
Allow dragging content between domains into same window	**Enable**

   b) Click **OK**.
6. Click **Apply** and then click **OK**.

Internet Explorer: Enable Drag-and-Drop from D2/LSRD

Perform this setup procedure in the Internet Explorer browser to enable the drag-and-drop function from D2.

To enable the drag-and-drop function from D2/LSRD (from a separate D2/LSRD window):

Note: Drag-and-drop of multiple objects is not supported. Drag-and-drop functionality is supported if the D2 window is opened in Java mode only. Make sure that you are aware of all the product-specific notes that may apply to the requirements information for OpenText Documentum D2 16.4, please refer to *D2 Release Notes* for more details.

1. In the Internet Explorer browser, navigate to **Settings** > **Internet Options**.
2. In the **Internet Options** pop-up window, open the **Security** tab and click **Local intranet**.
3. Do the following for the Local intranet:
   a) Clear the **Enable Protected Mode** option.
   b) Click **Sites** > **Advanced**. The **Local intranet** pop-up window appears.
   c) Enter the following, one by one, and click **Add**: `<Insight Manager URL>` and `<D2 URL>`.

      Note: You can use your D2 name to make the configuration specific for one D2 only. For example: `http://<d2_name>`, where <d2_name> is the actual D2 repository name.

      Replace the <Insight Manager URL> with the InSight server that you use.
   d) **Close**.
4. In the **Local intranet** pop-up window, click **OK**.
5. In the **Internet Options** pop-up window, downgrade the **Security level for this zone: All** parameter to **Medium-low**.
6. In the **Internet Options** pop-up window, click **Custom level...**.
   a) In the **Security Settings - Local intranet Zone** pop-up window, scroll to **Miscellaneous** and update the following settings:

Allow dragging content between domains into separate window	**Enable**
Allow dragging content between domains into same window	**Enable**

   b) Click **OK**.
7. Click **Apply** and then click **OK**.

Post-Installation Tasks

Prerequisites

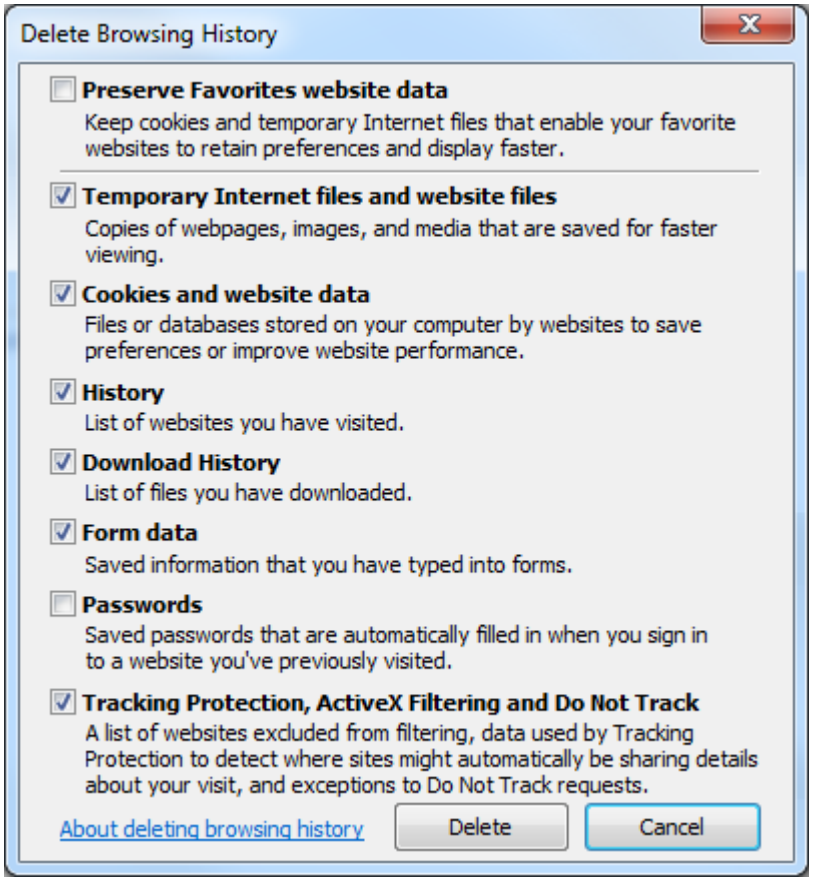
Before you can use any Liquent InSight 6.2 CHF, you must perform post-installation tasks.

Important: After each Certified Hotfix upgrade, Liquent InSight drops and recreates all views. This affects any custom database objects that have been created and granted rights against any of the Liquent InSight database objects. This also affects each customized report (query) which may need to be recreated. If you have any customization applied, you will need to load them back after the upgrade is completed.

After you install Liquent InSight 6.2 CHF:

1. If you customized any properties files before you installed the CHF and you need to maintain the customizations, add your customizations to the new properties files.
2. Create new assembly templates.
3. If you customized any template files before you installed Liquent InSight 6.2 CHF, and you need to maintain the customizations, add your customizations after the certified hotfix template files are installed.
4. Clear temporary Internet files in Internet Explorer.
   a) In the Internet Explorer **Tools** menu, select **Internet Options**.
   b) On the **Internet Options** dialog box, click **Delete**.
   c) On the **Delete Browsing History** dialog box, select the following options and then click **Delete**:

   - Temporary Internet files and website files
   - Cookies and website data
   - History
   - Download History
   - Form data
   - Tracking Protection, ActiveX Filtering and Do Not Track


Delete Browsing History
Preserve Favorites website data
Keep cookies and temporary Internet files that enable your favorite websites to retain preferences and display faster.
Temporary Internet files and website files
Copies of webpages, images, and media that are saved for faster viewing.
Cookies and website data
Files or databases stored on your computer by websites to save preferences or improve website performance.
History
List of websites you have visited.
Download History
List of files you have downloaded.
Form data
Saved information that you have typed into forms.
Passwords
Saved passwords that are automatically filled in when you sign in to a website you've previously visited.
Tracking Protection, ActiveX Filtering and Do Not Track
A list of websites excluded from filtering, data used by Tracking Protection to detect where sites might automatically be sharing details about your visit, and exceptions to Do Not Track requests.
About deleting browsing history
Delete
Cancel

Create Assembly Templates from Template Files

Prerequisites

After you install the new Liquent InSight 6.2 CHF, create assembly templates from the template files that you import.

To create an assembly template from a template file:

1. From a Liquent InSight Web client workstation, log on to Liquent InSight.
2. If a version of the template file already exists in Liquent InSight, delete or rename the existing template file.
   - To delete the existing template - On the Liquent InSight home page, select the **Assembly Templates** tab, then choose the template. On the **More** menu, select **Delete** and then confirm the deletion.
   - To rename the existing template - On the Liquent InSight home page, select the **Assembly Templates** tab, then choose the template. Click the **Edit** icon, update the **Name** field, and click **Save**.
3. Navigate to the **Assembly Templates** tab, and then in the menu bar, click **New** > **Template**.
   The **Create Template** page appears.
4. Select **Assembly File**, browse to the location where you saved your new templates, and then choose the assembly template file.
5. Set **Use Source Assembly Publishing Settings Library** to **Yes**.
6. Set the **Import Publishing Elements** to **Yes**.
7. Click **Next**. The **Assembly Attributes** page appears for the template you created.

DTD Files

To make sure that you have the most current version of each listed DTD file on your system, refer to the **Last Modified Build** column in the table. This column displays the product build number in which the file was introduced or updated.

Component	Customizable	Last Modified Build
\DTDs\au-0-90.zip	No	6.2.0.0.0296
\DTDs\au-0-90-ectd.zip	No	6.2.0.0.0296
\DTDs\au-3-0.zip	No	6.2.0.0.0296
\DTDs\au-3-0-ectd.zip	No	6.2.0.0.0296
\DTDs\au-3-1.zip	No	6.2.0.0.0296
\DTDs\au-3-1-ectd.zip	No	6.2.0.0.0296
\DTDs\au-nees-2-0.zip	No	6.2.0.0.0296
\DTDs\au-nees-2-0-ectd.zip	No	6.2.0.0.0296
\DTDs\ca-1-0.zip	No	6.2.0.0.0296
\DTDs\ca-1-0-ectd.zip	No	6.2.0.0.0296
\DTDs\ca-2-2.zip	No	6.2.0.0.0296
\DTDs\ca-2-2-ectd.zip	No	6.2.0.0.0296
\DTDs\ch-1-0-1.zip	No	6.2.0.0.0296
\DTDs\ch-1-0-1-ectd.zip	No	6.2.0.0.0296
\DTDs\ch-1-1.zip	No	6.2.0.0.0296
\DTDs\ch-1-1-ectd.zip	No	6.2.0.0.0296
\DTDs\ch-1-2.zip	No	6.2.0.0.0296
\DTDs\ch-1-2-ectd.zip	No	6.2.0.0.0296
\DTDs\ch-1-3.zip	No	6.2.0.0.0296
\DTDs\ch-1-3-ectd.zip	No	6.2.0.0.0296
\DTDs\ch-1-4.zip	No	6.2.0.2.0069
\DTDs\ch-1-4-ectd.zip	No	6.2.0.2.0069
\DTDs\eu-1-0.zip	No	6.2.0.0.0296
\DTDs\eu-1-0-ectd.zip	No	6.2.0.0.0296
\DTDs\eu-1-1.zip	No	6.2.0.0.0296
\DTDs\eu-1-1-ectd.zip	No	6.2.0.0.0296
\DTDs\eu-1-2-1.zip	No	6.2.0.0.0296
\DTDs\eu-1-2-1-ectd.zip	No	6.2.0.0.0296
\DTDs\eu-1-3.zip	No	6.2.0.0.0296
\DTDs\eu-1-3-ectd.zip	No	6.2.0.0.0296

Component	Customizable	Last Modified Build
\DTDs\eu-1-4.zip	No	6.2.0.0.0296
\DTDs\eu-1-4-ectd.zip	No	6.2.0.0.0296
\DTDs\eu-2-0.zip	No	6.2.0.0.0296
\DTDs\eu-2-0-ectd.zip	No	6.2.0.0.0296
\DTDs\eu-3-0.zip	No	6.2.0.0.0296
\DTDs\eu-3-0-1.zip	No	6.2.0.0.0296
\DTDs\eu-3-0-1-ectd.zip	No	6.2.0.0.0296
\DTDs\eu-3-0-ectd.zip	No	6.2.0.0.0296
\DTDs\form-1-1.zip	No	6.2.0.0.0296
\DTDs\form-1-1-ectd.zip	No	6.2.0.0.0296
\DTDs\gc-1-2.zip	No	6.2.0.0.0296
\DTDs\gc-1-2-ectd.zip	No	6.2.0.0.0296
\DTDs\gc-1-5.zip	No	6.2.0.0.0296
\DTDs\gc-1-5-ectd.zip	No	6.2.0.0.0296
\DTDs\hr-1-4.zip	No	6.2.0.0.0296
\DTDs\hr-1-4-ectd.zip	No	6.2.0.0.0296
\DTDs\ich-3-2.zip	No	6.2.0.0.0296
\DTDs\ich-3-2-ectd.zip	No	6.2.0.0.0296
\DTDs\jo-1-0.zip	No	6.2.0.3.0062
\DTDs\jo-1-0-ectd.zip	No	6.2.0.3.0062
\DTDs\jp-1-0.zip	No	6.2.0.0.0296
\DTDs\jp-1-0-ectd.zip	No	6.2.0.0.0296
\DTDs\pim-2-1.zip	No	6.2.0.0.0296
\DTDs\pim-2-1-ectd.zip	No	6.2.0.0.0296
\DTDs\schema.properties	Yes	6.2.0.0.0296
\DTDs\stf-2-2.zip	No	6.2.0.0.0296
\DTDs\stf-2-2-3-0.zip	No	6.2.0.0.0296
\DTDs\stf-2-2-3-0-ectd.zip	No	6.2.0.0.0296
\DTDs\stf-2-2-ectd	No	6.2.0.0.0296
\DTDs\th-0-92.zip	No	6.2.0.0.0296
\DTDs\th-0-92-ectd.zip	No	6.2.0.0.0296
\DTDs\th-1-0.zip	No	6.2.0.0.0296
\DTDs\th-1-0-ectd.zip	No	6.2.0.0.0296
\DTDs\us-2-01.zip	No	6.2.0.0.0296
\DTDs\us-2-01-ectd.zip	No	6.2.0.0.0296

Component	Customizable	Last Modified Build
\DTDs\us-2-01-ectd-folder.zip	No	6.2.0.0.0296
\DTDs\us-3-3.zip	No	6.2.0.0.0296
\DTDs\us-3-3-ectd.zip	No	6.2.0.0.0296
\DTDs\za-1-0.zip	No	6.2.0.0.0296
\DTDs\za-1-0-ectd.zip	No	6.2.0.0.0296
\DTDs\za-2-1.zip	No	6.2.0.0.0296
\DTDs\za-2-1-ectd.zip	No	6.2.0.0.0296

Assembly Template Update History

To ensure that you have the most current version of each listed template file on your system, refer to the **Modified/Introduced in Version** column in the **Template Files** table. This column contains information about the template status for every version in the Liquent InSight6.2 branch:

- **No** - template was not updated
- **Yes**- template was updated
- **New** - template introduced or updated
- Blank - template did not exist for the release

Template	Modified/Introduced in Version			
	6.2	6.2 CHF 1	6.2 CHF 2	6.2 CHF 3
	Build 6.2.0.0.0296	Build 6.2.0.1.0004	Build 6.2.0.2.0069	Build 6.2.0.3.0039
templates\510k Template (Sep 2019).xml				
\templates\510k template.xml	No	No	No	No
\templates \A4SampleTOCTemplate.docx	No	No	No	No
\templates\ASEAN ACTD-NeeS.xml	No	No	No	No
\templates\AU eCTD Module 1 v0.90.xml	No	No	No	No
\templates\AU eCTD Module 1 v3.0.xml	No	No	No	No
\templates\AUS Module 1 CTD v2.1.xml	No	No	No	No
\templates\AUS Module 1 CTD-NeeS v2.0 2011.xml	No	No	No	No
\templates\AU Module 1 eCTD v3.1.xml	New	No	No	No
\templates\AU Module 1 NeeS v2.0.xml	New	No	No	No
\templates\Canadian eCTD Module 1 v1.0.xml	No	No	No	No
\templates\Canadian eCTD Module 1 v2.2.xml	No	No	No	No
\templates\Canadian electronic CTA CTA-A-29-May-2013.xml	No	No	No	No
\templates\Canadian electronic CTA.xml	No	No	No	No
\templates\CH eCTD Module 1 v1.0.1.xml	No	No	No	No

Template	Modified/Introduced in Version			
	6.2	6.2 CHF 1	6.2 CHF 2	6.2 CHF 3
	Build 6.2.0.0.0296	Build 6.2.0.1.0004	Build 6.2.0.2.0069	Build 6.2.0.3.0039
\templates\CH eCTD Module 1 v1.1.xml	No	No	No	No
\templates\CH eCTD Module 1 v1.2.xml	No	No	No	No
\templates\CH eCTD Module 1 v1.3.xml	No	No	No	No
\templates\CH eCTD Module 1 v1.4.xml			New	Yes
\templates\CN eCTD Module 1 v1.0.xml				
\templates\CN eCTD ICH Module 2-5 v3.2.xml				
\templates\CN Clinical Study Report (VV5-0).xml				
\templates\CN Nonclinical Study Report (SEND Dataset).xml				
\templates\CN Nonclinical Study Report.xml				
\templates\eCTD ICH Module 2-5 v3.2.xml	No	No	Yes	No
\templates\EAEU Template v1.0.xml				
\templates\EU CTA.xml	No	No	No	No
\templates\EU eCTD Module 1 v1.0 - CP.xml	No	No	No	No
\templates\EU eCTD Module 1 v1.0 - MRP-DCP.xml	No	No	No	No
\templates\EU eCTD Module 1 v1.0 - NP.xml	No	No	No	No
\templates\EU eCTD Module 1 v1.1 - CP.xml	No	No	No	No
\templates\EU eCTD Module 1 v1.1 - MRP-DCP.xml	No	No	No	No
\templates\EU eCTD Module 1 v1.1 - NP.xml	No	No	No	No
\templates\EU eCTD Module 1 v1.2.1 - CP.xml	No	No	No	No
\templates\EU eCTD Module 1 v1.2.1 - MRP-DCP.xml	No	No	No	No

Template	Modified/Introduced in Version			
	6.2	6.2 CHF 1	6.2 CHF 2	6.2 CHF 3
	Build 6.2.0.0.0296	Build 6.2.0.1.0004	Build 6.2.0.2.0069	Build 6.2.0.3.0039
\templates\EU eCTD Module 1 v1.2.1 - NP.xml	No	No	No	No
\templates\EU eCTD Module 1 v1.3 - CP.xml	No	No	No	No
\templates\EU eCTD Module 1 v1.3 - MRP-DCP.xml	No	No	No	No
\templates\EU eCTD Module 1 v1.3 - NP.xml	No	No	No	No
\templates\EU eCTD Module 1 v1.4 - CP.xml	No	No	No	No
\templates\EU eCTD Module 1 v1.4 - MRP-DCP.xml	No	No	No	No
\templates\EU eCTD Module 1 v1.4 - NP.xml	No	No	No	No
\templates\EU eCTD Module 1 v2.0 - CP.xml	No	No	No	No
\templates\EU eCTD Module 1 v2.0 - MRP-DCP.xml	No	No	No	No
\templates\EU eCTD Module 1 v2.0 - NP.xml	No	No	No	No
\templates\EU eCTD Module 1 v3.0 - CP.xml	No	No	No	No
\templates\EU eCTD Module 1 v3.0 - MRP-DCP.xml	No	No	No	No
\templates\EU eCTD Module 1 v3.0 - NP.xml	No	No	No	No
\templates\EU eCTD Module 1 v3.0.1 - CP.xml	No	No	No	No
\templates\EU eCTD Module 1 v3.0.1 - MRP-DCP.xml	No	No	No	No
\templates\EU eCTD Module 1 v3.0.1 - NP.xml	No	No	No	No
\templates\EU eCTD Module 1 v3.0.3 - CP.xml	New	No	No	No
\templates\EU eCTD Module 1 v3.0.3 - MRP-DCP.xml	New	No	No	No
\templates\EU eCTD Module 1 v3.0.3 - NP.xml	New	No	No	No
\templates\EU IMPD template.xml	No	No	No	No

Template	Modified/Introduced in Version			
	6.2	6.2 CHF 1	6.2 CHF 2	6.2 CHF 3
	Build 6.2.0.0.0296	Build 6.2.0.1.0004	Build 6.2.0.2.0069	Build 6.2.0.3.0039
\templates\EU PMF Submission in eCTD.xml	No	No	No	No
\templates\EU VNeeS - Immunological.xml	No	No	No	No
\templates\EU VNeeS - Pharmaceutical.xml	No	No	No	No
\templates\EU VNeeS v2.2 - Immunological.xml	No	No	No	No
\templates\EU VNeeS v2.2 - MRL Maximum Residue Limits.xml	No	No	No	No
\templates\EU VNeeS v2.2- Pharmaceutical.xml	No	No	No	No
\templates\EU VNeeS v2.3 - Immunological.xml	No	No	No	No
\templates\EU VNeeS v2.3 - MRL Maximum Residue Limits.xml	No	No	No	No
\templates\EU VNeeS v2.3- Pharmaceutical.xml	No	No	No	No
\templates\GCC eCTD Module 1 v1.2 - GCC.xml	No	No	No	No
\templates\GCC eCTD Module 1 v1.2 - NP.xml	No	No	No	No
\templates\GCC eCTD Module 1 v1.5 - GCC.xml	No	No	No	No
\templates\GCC eCTD Module 1 v1.5 - NP.xml	No	No	No	No
\templates\HR eCTD Module 1 v1.4 - NP.xml	No	No	No	No
\templates\ICH E3 Clinical Study Report (VV2-2).xml	No	No	No	No
\templates\ICH E3 Clinical Study Report (VV3-0).xml	No	No	No	No
\templates\ICH E3 Clinical Study Report (VV5-0).xml			New	No
\templates\JO eCTD Module 1 v1.0.xml				New
\templates\JP eCTD Module 1 v1.0.xml	No	No	Yes	No
\templates\JP eCTD Module 2-5 v3.2.xml	No	No	No	No

Template	Modified/Introduced in Version			
	6.2	6.2 CHF 1	6.2 CHF 2	6.2 CHF 3
	Build 6.2.0.0.0296	Build 6.2.0.1.0004	Build 6.2.0.2.0069	Build 6.2.0.3.0039
\templates\MD - IMDRF (HC) IVD Template.xml				
\templates\MD - IMDRF nIVD Template.xml				
\templates\Nonclinical Study Report (SEND Dataset).xml	No	No	No	No
\templates\Nonclinical Study Report.xml	No	No	No	No
\templates\PMA Template (Feb 2019).xml				
\templates\PMA Template.xml	No	No	No	No
\templates\ROW CTD Module 1.xml	No	No	No	No
\templates \SampleCoverPageTemplate.docx	No	No	No	No
\templates \SampleOverlayTemplate.docx	No	No	No	No
\templates \SampleTOCTemplate.docx	No	No	No	No
\templates\Saudi Arabia CTD Module 1 v1.0.xml	No	No	No	No
\templates\TH eCTD Module 1 v0.92.xml	No	No	No	No
\templates\TH eCTD Module 1 v1.0.xml	No	No	No	No
\templates \UCSampleCoverPageTemplate.docx	No	No	No	No
\templates \UCSampleOverlayTemplate.docx	No	No	No	No
\templates \UCSampleTOCTemplate.docx	No	No	No	No
\templates\US eCTD Module 1 v2.01.xml	No	No	No	No
\templates\US eCTD Module 1 v3.3.xml	No	No	Yes	No
\templates\ZA eCTD Module 1 v1.0.xml	No	No	No	No
\templates\ZA eCTD Module 1 v2.1.xml	No	No	No	No

Index