LIQUENT InSight 6.2 Installation Guide

Table of Contents

Liquent InSight 6.2 Installation Guide....1
LIQUENT InSight 6.2 Installation Guide....1
Liquent InSight Database Server Installation....1
LIQUENT InSight 6.2 Database Server Reference Documents....1
LIQUENT InSight 6.2 Database Server Prerequisites....1
Oracle Database Requirement....2
Oracle Configuration Assistant Settings....2
LIQUENT InSight Supporting Documentation....4
Type of Installation....4
Prerequisite Installation Procedure....4
LIQUENT InSight Database Setup – New Installation....4
LIQUENT InSight Oracle Database Setup – Upgrade Installation v6.1 to v6.1 CHF 4....5
Upgrade to LIQUENT InSight 6.2....7
Liquent InSight Application Server Installation....8
LIQUENT InSight 6.2 Application Server Reference Documents....8
LIQUENT InSight 6.2 Application Server Installation Prerequisites....8
LIQUENT InSight 6.2 Application Server Installation Prerequisites For LIQUENT InSight Upgrades Only....8
LIQUENT InSight Application Server Installation Prerequisites For SharePoint Only....9
Installing LIQUENT InSight Application Server....9
Additional Prerequisites for Documentum Systems....11
Enable Data Exchange for LIQUENT InSight....11
Environment Setup....11
Liquent InSight Configuration....12
LIQUENT InSight Configuration....12
Enable Azure Active Directory (Azure SSO) for LIQUENT InSight 6.2....16
Increasing the Oracle Connections for InSight Manager....17
Accessing LIQUENT Online Help....18
Adding Additional Functionality to InSight Manager....18
Enable SSL for LIQUENT InSight....22
LIQUENT InSight License and LIQUENT InSight Manager Service Setup....23
LIQUENT InSight Communication and License Confirmation....23
Setting up Document Management Systems (DMS)....24
Increase the Transaction Timeout (optional)....27
Re-extracting Documents and Regenerating TOC for Active Assemblies....27

Create Assembly File Templates..... 28
Activate Kendo Window UI..... 28
LIQUENT InSight Client Configuration..... 29

Liquent InSight 6.2 Installation Guide

LIQUENT InSight 6.2 Installation Guide

The LIQUENT InSight 6.2 Installation Guide describes the procedures for installing LIQUENT InSight 6.2.

It includes sections about the steps required for implementing LIQUENT InSight 6.2 Database Server, Application Server, and Client.

For best results, we recommended using the PAREXEL Client Enablement team to guide and assist you through the installation process.

Liquent InSight Database Server Installation

LIQUENT InSight 6.2 Database Server Reference Documents

This document specifies the implementation steps required for implementing LIQUENT InSight 6.2 Database Server.

Reference Documents

- *LIQUENT InSight 6.2 Release Notes*
- *LIQUENT InSight 6.2 System Support Documentation (SSD)*
- *LIQUENT InSight 6.2 Data Migration Document and Database Migration Release Notes*

LIQUENT InSight 6.2 Database Server Prerequisites

For LIQUENT InSight Upgrades Only

The following table reflects the information applicable for the LIQUENT InSight upgrades only.

LIQUENT InSight Version	Migration Path Description
LIQUENT InSight 6.2	Upgrade is supported from LIQUENT InSight 6.1 or later CHFs, using the appropriate migration path.
LIQUENT InSight 6.1	Upgrade is supported from LIQUENT InSight 6.0 CHF 3 or later, using the appropriate migration path.
LIQUENT InSight 6.0	Upgrade is supported from LIQUENT InSight 5.1 CHF 2 or later, using the appropriate migration path. • For upgrading to LIQUENT InSight 6.0 from LIQUENT InSight 5.1 CHF 2 customers should perform the pre-migration tasks described in the *LIQUENT InSight 6.0 Data Migration Document*. • Before upgrading to the LIQUENT InSight 6.0 CHF 1, customers should perform the post-migration tasks as described in the *LIQUENT InSight 6.0 Data Migration Document*.

LIQUENT InSight Version	Migration Path Description
LIQUENT InSight 5.1 CHF 2	Upgrade is supported from LIQUENT InSight 5.1 CHF 1 only.
LIQUENT InSight 5.1 CHF 1	Upgrade is supported from LIQUENT InSight 5.1 GA only.

Note:

- The grants for custom database users are removed during the migration.
- The creation of the UUID for applications during migration requires Oracle JVM to be enabled on the Oracle Database Server. If Oracle JVM is not enabled, please contact Technical Support.

Oracle Database Requirement

Confirm that your system meets the Oracle database requirement specified in the *LIQUENT InSight Database Server Specifications*.

Oracle Database Settings

Consider the following recommendations before installing the LIQUENT InSight database.

Oracle dedicated server

PAREXEL respects the need to install database schemas on an Oracle server under many different configurations. PAREXEL fully supports the LIQUENT InSight database schema installed to a single, non-shared, Oracle database instance. For migration and support reasons, configurations where the LIQUENT InSight database schema is installed to a shared Oracle database instance are provided with CONDITIONAL support only. A definition of conditional support is available on the Customer Portal under the platform support policies document.

Furthermore, due to the batch processing and transaction sizes executed by LIQUENT InSight, the Oracle Shared Server configuration, also known as the Multi-threaded Server or MTS configuration, is not supported by LIQUENT InSight. Your Oracle environment must be set to the Dedicated Server configuration.

Oracle Configuration Assistant Settings

When completing the **Oracle Configuration Assistant** wizard to create a database instance for LIQUENT InSight, use the following settings as directed.

Oracle has many settings that a DBA can modify after implementation. PAREXEL does not test every possible configuration scenario. Unless otherwise noted, the Oracle database settings are assumed to be standard out-of-the-box settings at the time of installation. As the size of database grows and additional information becomes available, PAREXEL understands that some database settings may need to be adjusted by your DBA to optimize performance.

Required Settings

- `redo log size = 500M`
- `undo tablespace` must be adequately sized: If you are running a supported version of Oracle (see *LIQUENT InSight 6.2 SSD*), confirm you are using the auto management of the undo tablespace.
- `database character set = Unicode (AL32UTF8)`
- `national character set = UTF8 (Unicode 3.0 UTF-8 Universal character set)`
- `connection mode = Dedicated Server Mode`

- workarea_size_policy = AUTO
- the default tablespace users must be created before installing LIQUENT InSight
- a TEMP tablespace must be created in Optional settings
- set instance connections to (see *show parameters sessions* below)

The following are suggested settings for improving performance depending on the system load in your environment. PAREXEL does not have metrics to provide, but informal testing has shown that these settings can improve performance.

- sga_max_size = 1500MB (Oracle scope=spfile)
- sga_target = 1500MB
- alter system set db_file_multiblock_read_count = 128 scope=BOTH;
- alter system set optimizer_mode = ALL_ROWS scope=BOTH;
- alter system set optimizer_index_caching = 100 scope=BOTH;

Establish the maximum number of Oracle sessions you would like to make available for LIQUENT InSight use. This value may be directly tied to the maximum number of users you will have working on your system. The current session count can be determined by keying the following command into the SQL command line:

- show parameters sessions;

If the current setting is deemed too small, please consult with your DBA to increase this value. Retain this value for use when setting up your LIQUENT InSight Application Server.

Oracle Configuration Update

The following Oracle configuration upgrade must be performed on your database server before migrating any data and before installing LIQUENT InSight 6.2.

Please note the following descriptions and settings when performing the Oracle configuration update:

- MAX_STRING_SIZE controls the maximum size of VARCHAR2, NVARCHAR2, and RAW data types in SQL.
- STANDARD means that the length limits for Oracle Database releases prior to Oracle Database 12c apply (for example, 4000 bytes for VARCHAR2 and NVARCHAR2, and 2000 bytes for RAW).
- EXTENDED means that the 32767 byte limit introduced in Oracle Database 12c applies.
- The COMPATIBLE initialization parameter must be set to 12.0.0.0 or higher to set MAX_STRING_SIZE = EXTENDED.
- You can change the value of MAX_STRING_SIZE from STANDARD to EXTENDED. However, you cannot change the value of MAX_STRING_SIZE from EXTENDED to STANDARD.

Increasing the Size of VARCHAR2, NVARCHAR2, and RAW Columns in a Non-CDB

To increase the maximum size of VARCHAR2, NVARCHAR2, and RAW columns in a non-CDB:

1. Shut down the database.
2. Restart the database in **UPGRADE** mode.
3. Change the setting of *MAX_STRING_SIZE* to EXTENDED.
4. Run the rdbms/admin/utl32k.sql script. You must be connected AS SYSDBA to run the script.
5. Restart the database in **NORMAL** mode.

   The utl32k.sql script increases the maximum size of the VARCHAR2, NVARCHAR2, and RAW columns for the views where this is required. The script does not increase the maximum size of the VARCHAR2, NVARCHAR2, and RAW columns in some views because of the way the SQL for those views is written.
6. Run the rdbms/admin/utlrp.sql script to recompile invalid objects. You must be connected AS SYSDBA to run the script.
7. Restart the database in **NORMAL** mode.

LIQUENT InSight Supporting Documentation

Before executing the Database Server script, be sure to obtain a copy of the following supporting documentation:

- *LIQUENT InSight 6.2 Release Notes*
- *LIQUENT InSight 6.2 System Support Documents (SSD)*
- *LIQUENT InSight 6.2 Data Migration Document*

All database server scripts must be run from a Windows OS machine connected to the Oracle database.

The creation of the UUID for applications during migration requires Oracle JVM to be enabled on the Oracle Database Server. If you cannot enable Oracle JVM, please contact Technical Support for assistance.

Type of Installation

This document includes instructions for both new and upgrade installations.

1. Determine the implementation type to be performed.
2. For both types of installation, perform the Prerequisite Installation Procedure.

Prerequisite Installation Procedure

Before performing either a new installation or an upgrade installation, do the following prerequisite procedure.

1. Verify the following for the installation user account:
   - Full read/write permissions on server
   - That this account is the same one used to install all prerequisite software for the server

   Note: Administrator permission is required.
2. Verify that the required software components have been installed.
   - Verify that the Oracle environment is set to the **Dedicated Server** configuration.
3. Verify that a general database instance been created on the database server for the Application Server (new installation).
4. Verify that the character encoding for the Database Server database instance is Unicode (AL32UTF8), and the national character encoding is UTF8 – Unicode 3.0 UTF-8 Universal character set CESU-8 compliant.
5. Verify that the installer has access to the installation media for the Application Server.

LIQUENT InSight Database Setup – New Installation

If you are upgrading from an existing version and not performing a new installation, go to section *LIQUENT InSightOracle Database Setup - Upgrade Installation.*

1. On the computer where you are running the installation script, check the system registry to verify it is set to `AL32UTF8`.

   Under - `HKEY_LOCAL_MACHINE\SOFTWARE\ORACLE\KEY_OraDb12C_home1\NLS_LANG`

   `AMERICAN_AMERICA.AL32UTF8`

   Note: `KEY_OraDb12C_home1` name might be different based on the computer you are running the installation script from and also the version of Oracle installed.
2. On the computer where you are running the installation script, create a temporary install directory.

   The installation script can be run either directly on the database server or remotely from a client running Windows with Oracle SQL*Plus installed on it.

`D:\Install\InSightDB`

a) For remotely running the script, change the `listener.ora` file:
`SID_DESC = (GLOBAL_DBNAME = <dbName>)(ORACLE_HOME = D:\oracle\product\12.*.*\dbhome_1)(SID_NAME =<dbSID>)`

Note: 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.

3. Copy the `database.zip` file from the Database Server installation media to the temp directory you created, and extract the ZIP file into that directory.
4. Open a **command prompt** and navigate to the newly created `database` folder.
`cd D:\Install\InSightDB\database`
5. At the **command prompt** type: `sqlplus /nolog`
   - Ensure that the forward slash (`/`) character is included when the above statement is input.
   - The `build.sql` script can be run by the system user only from the sql prompt.
6. Open the file `define.install` in Notepad from the newly created `database` folder.
7. Enter correct values for the specified parameters:
   - define `sid=dbSID`
   - define `syspass=*syspass*`
   - define `sysuser=system user`
   - define `orapath=path of DB Instance location`
8. At the `sql>` prompt type: `@build.sql`
The build process starts and the `sid` prompt appears.
9. After the script is complete, check the `buildlog.lst` for errors. This file is generated in the directory where the build script was executed, and should be in the same directory previously created.
`D:\Install\InSightDB\database`
There should be no errors on the log except for those relating to:
   - Dropping indexes that do not exist
   - Dropping roles that do not exist
   - Dropping users that do not exist
   - Dropping/deleting tablespaces that do not exist
   - Connect errors that occur at the beginning of the script as attempts are made to connect as users that do not exist.

Note: All database passwords are validated at the beginning of the migration script. If you received the error message `ORA-01017: invalid username/password; logon denied` and the script terminates without connecting, correct the password values that you defined.

10. Close the **command prompt**.

LIQUENT InSight Oracle Database Setup – Upgrade Installation v6.1 to v6.1 CHF 4

The cycle must be repeated for each script run when migrating your database to the current version. Start at the version of LIQUENT InSight you are running, and run the applicable SQL scripts in the order shown to bring your LIQUENT InSight database up to the current release:

InSight versions: **6.1** > **6.1 CHF 1** > **6.1 CHF 2** > **6.1 CHF 3** > **6.1 CHF 4**

Note: For every migration cycle review a migration document applicable for your migration path. All migration documents are available as PDFs in the *Data Migration Documents* topic.

1. Based on the version of InSight from which you will be starting the upgrade, execute pre-migration steps if they are defined for your migration path.
2. Back up your existing Database Server database.
3. Verify that all users are logged off the InSight system and stop the InSight Manager service.
4. Based on the version of LIQUENT InSight from which you will be starting the upgrade, note the ZIP files containing the migration scripts that you need to run:
   - DB Upgrade 61 to 61 CHF1
   - DB Upgrade 61 CHF 1 to 61 CHF2
   - DB Upgrade 61 CHF 2 to 61 CHF3
   - DB Upgrade 61 CHF 3 to 61 CHF4
5. On the computer where you are running the installation script, create as many temporary install directories as needed. The installation script can be run either directly on the database server or remotely from a client running Windows with Oracle's SQL*Plus installed on it.

   `D:\Install\InSightDBUpgrade1`

   `D:\Install\InSightDBUpgrade2`

   `D:\Install\InSightDBUpgrade3`

   Note: 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.
6. Copy and unzip the DB `DB upgrade.zip` file from the Database Server installation media to the `temp` directory.
7. Navigate to the newly created extraction folder.
   `cd D:\Install\InSightDBUpgrade1\DBupgrade`
8. Open the `define.migration` file in Notepad.
9. 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 settings 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`

   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=sgared`
   - define `activitipass=activity`
   - define `syspass=<enter system password for database being upgraded per step action>`

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).

10. Close and save the modified `define.migration` file.
11. Open the **command prompt** from the directory where the `.zip` file was extracted. In the command prompt:
    a) Type `sqlplus/nolog`.
    b) Press `Enter`.
12. At the **SQL>** prompt, type `connect database user/database password@sid` and press **Enter**.
    - After the connection to the database is established, at the **SQL>** prompt, type `@master_pre` and press **Enter**.

    When the SQL script begins, you are returned to the **sqlplus** prompt.
13. After `master_pre` is completed, at the **SQL>** prompt type `@master` and press **Enter**.
14. From the command prompt type `sqlplus/nolog`. At the **sqlplus** prompt type `@master.sql`.
    The upgrade process starts and you are returned to the sqlplus prompt.
15. 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.
    `D:\install\InSightDBUpgrade1\DBupgrade`

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

16. Based on the version of LIQUENT InSight from which you will be starting the upgrade, execute post-migration steps if they are defined for your migration path.

Upgrade to LIQUENT InSight 6.2

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.

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).
4. Open the **command prompt**, type: `sqlplus/nolog` and press Enter.

5. In the `sqlplus` prompt, type `@master.sql` and press Enter.
6. 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`
7. Optional Step:
   - Open the `define.passwords.alternate` file in Notepad and update passwords values if needed. Save and close file.
   - At the `sqlplus` prompt type: `exit`

Liquent InSight Application Server Installation

LIQUENT InSight 6.2 Application Server Reference Documents

The following topics describe the implementation steps required for implementing LIQUENT InSight 6.2 Application Server.

Reference Documents

- *LIQUENT InSight 6.2 Release Notes*
- *LIQUENT InSight 6.2 System Support Documentation (SSD)*

LIQUENT InSight 6.2 Application Server Installation Prerequisites

Before installing the LIQUENT InSight 6.2 Application Server, confirm that the LIQUENT InSight 6.2 Database Server is installed.

LIQUENT InSight 6.2 Application Server Installation Prerequisites For LIQUENT InSight Upgrades Only

For the LIQUENT InSight Application Server, upgrading to LIQUENT InSight 6.2 is only supported from LIQUENT InSight 6.1 CHF4

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. 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.

Attention: 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 JBOSS articles below:

- https://developer.jboss.org/docs/DOC-12190
- https://developer.jboss.org/thread/64874

LIQUENT InSight 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.

Installing LIQUENT InSight Application Server

Observe that some instructions are for upgrade installations only and are not necessary for new installations, and some instructions are optional depending on your document management system (DMS).

1. Verify the following for the installation service account:
   - Full read/write permissions on server (i.e. in Administrator group).
   - The account is a Windows domain user account with local administrative privileges.
   - That this account is the same one used to install all prerequisite software for the server. This account will be referred to as local administrator.
2. To turn UAC off in windows 2012 R2, you must change the registry key: `HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Policies\System`
   a) **EnableLUA** from a `1` (on) to a `0` (off)
   b) Restart the Windows 2012 R2 Server

   Note: Changing the **EnableLUA** value required for installing/uninstalling LIQUENT InSight Service in 2012R2, without changing installing/uninstalling the service, will return an Error message.
3. Verify the correct server time and time zone with the repository system and the Oracle database system, so that the times for all servers are the same.
4. Be sure that you have read the supporting documentation listed at the beginning of this document.
   - If performing an upgrade, proceed to the next step.
   - For all other installations, proceed to step 8.
5. Verify that all users are logged off the LIQUENT InSight system.
6. Remove the InSight Manager service.
   a) Click **Start**, type `services.msc` and press **Enter**.
   b) Double-click the InSight Manager Service.
   c) In the InSight Manager Service **Properties** dialog box, click **Stop** and then click **OK**.
   d) Navigate to the `C:\InsightManager\bin` folder and double-click `Uninstall_InsightManager_Service.bat` to remove the InSight Manager service.
   e) Refresh the **Services management** window and confirm the InSight Manager Service is no longer available.

7. Rename your old `InSightManager` folder to: `InSightManagerOLD`
8. Unzip the `InSightManager.zip` file from the LIQUENT InSight installation media into the root directory of the local drive `C:`, creating an `InSightManager` folder on the local drive.
9. Copy/import the contents of the `DTDs` directory (i.e. only the files) and the `Templates` directory (i.e. folder and files) from the LIQUENT InSight installation media to a location on a universally accessible repository.

   A DMS is recommended over a file system. This information will be used in a later step when you enter the path to the location in the `insightconfig.bat` entry page.

Documentum	`dctm://docbase/cabinet/foldername`
Livelink	`llin://repositoryname/workspace/folderpath`
File system	`//servername/servershare/foldername`
SharePoint	`shpt://repository/foldername`

   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` and `A4TOCTemplate.doc`), you will need to apply your customizations to the new TOC template files.
10. Verify appropriate TCP/IP network access. (Make note of the following hostnames for reference.)
    a) Ping the Application Server by hostname.
    LIQUENT InSight
    b) Record the hostname of the Application Server: _____
    c) Record the hostname of the Content Server Broker: _____
    d) If the Application Server is going to be communicating with a Database on another network server; ping that server by hostname.
    e) Record the hostname of the Database Server: _____
11. Verify that the required software components have been installed. See the *LIQUENT InSight 6.2 System Support Document (SSD)*.
12. Verify that the Regional Options setting on the server hosting the LIQUENT InSight Application Server is set to **U.S**.
13. **Note:** This step is optional.

    If the LIQUENT InSight Application Server will communicate with a Documentum DMS, the Docbase needs to recognize the Printer Text File format (`prn`) and the SAS Transport File format (`xpt`). Arrange with your Documentum administrator to create the `prn` and `xpt` format types in any Docbases that LIQUENT InSight access.
14. **Note:** This step is optional.

    If the LIQUENT InSight Application Server will communicate with a Livelink DMS, several Livelink attributes must be set to Queryable.
    a) In Livelink Administrator, under **Search Administration**, select **Open the System Object Volume** and log on.
    b) Select **Enterprise Data Source Folder** and then open the list next to `Enterprise Search Manager` and choose `Properties`.
    c) Select the **Regions** tab and ensure that the following have **Queryable** selected:

OTCurrentVersion	OTObject
OTDataID	OTOwnerID

OTModifyDate	OTVersion
OTName	OTVersionName

Additional Prerequisites for Documentum Systems

The following prerequisites must exist for systems using Documentum.

- FOR 7.2 DCTM Systems Only: LIQUENT InSight requires a Global Repository on the content server.
- If it does not already exist, create a Global Repository on the content server.

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:

1. Update the `DataExchangeConfig.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.

Environment Setup

If you are upgrading to LIQUENT InSight 6.2, 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.

1. On the Application Server, go to **Control Panel** > **System** > **Advanced System Settings** > **Advanced** tab.
2. On the **Advanced** tab, in the **Performance** section, click **Settings**.
3. In the **Performance Options** window, select the **Data Execution Prevention** tab.
4. In the **Data Execution Prevention** tab, select: **Turn on DEP for essential Windows programs and services only**.
5. On **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 JDK installation.
       For example: `<installation drive>:\Program Files\Java\jdk1.8.0_XXX`
    b) Click **OK**.

12. Select **New** under **System variables**.
13. In the **Variable Name** field type in caps: `INSIGHT_HOME`
    a) In the **Variable Value** field, enter the directory of your LIQUENT InSight installation.
    For Example:`C:\InSightManager`
    b) Click **OK**.
14. 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**.
15. On the **Environment Variables** window click **OK**, and then on the **System Properties** window click **OK**.
16. 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`
17. 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.
18. Reboot the server.
19. Log on as the local administrator.

Liquent InSight Configuration

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 **LDAP Settings** section:

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`

Please ensure that the step 18 is also completed to set up the notifications properly.

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

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

9. 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*

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

10. 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`
`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.

11. 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.

12. **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) =	`1800`

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

Server =	*<IRserver>*
Port =	`2861`

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

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. In the main menu, select **File** > **Generate File** and click **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: First generation of files will throw an error as it cannot backup files it is generating.
17. In the main menu, 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) for LIQUENT InSight 6.2

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 opens.
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 **Azure SSO Settings** menu.
4. Select **Enable SSO**.
5. Populate the following fields:

Field Name	Input Value
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`

6. 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.
7. Select **File** > **Exit**.
   The Configuration Wizard is closed.
8. Locate the `insight.var` file in the *<installation drive>*`\InSightManager\server\all\conf\insight` installation directory and open for editing.
   The `insight.var` file is open.
9. Select parameter user.source=ldap and change the value to "azure".
10. Select parameter user.default.admin= CN\=admin,OU\={OrgUnit},DC\={domain controller},DC\=local and change value to registered Azure AD user. For Example: Name.Surname@corporation.com
    The value is changed.

Note: This user is assigned for first login into the system with enabled Azure SSO.

11. Save all the changes in `insight.var` file and close the file.
12. Restart the InSight service.

Increasing the 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 *<installation drive>*`:\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.

Accessing LIQUENT Online Help

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.

Adding Additional Functionality to InSight Manager

Enabling Change Password Functionality

An optional functionality of LIQUENT InSight 6.2 provides users with 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's 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 2008/2012 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

Updating the Backbone Generator

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 server that you set up to connect with LIQUENT InSight 6.2: `<InSight Rendering installation drive>:\Program Files (x86)\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.

Limiting Product Family and Country Tree Expand Range

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>`
   For example: `tree.search.result.limit=100`

   Replace *<limitation value>* with a number that specifies the maximum number of nodes that can be expanded.

   Note: if the parameter is not specified then the default limitation is 500 nodes.
3. Save the `insight.var` file.

Limiting 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>`
   For example: `assembly.tree.expand.range.limit=100`

   Replace *<limitation value>* with a number that specifies the maximum number of nodes that can be expanded.

   Note: if the parameter is not specified then the default limitation is 1000 nodes.
3. Save the `insight.var` file.

Limiting the 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>`
   For example: `assembly.tree.search.result.limit=100`

   Replace *<limitation value>* with a number that specifies the maximum number of nodes that can be expanded.

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

1. Update the `DataExchangeConfig.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-configuring the 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.

Enabling Documentum D2 for LIQUENT InSight

This procedure is optional and can be performed if LIQUENT InSight is going to 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.

Enabling SSL for LIQUENT InSight Rendering Services Server

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 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.

Setting up Document Management Systems (DMS)

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 management** 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>

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

Adding a File System DMS Repository for LIQUENT InSight

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:	*`<FileSystem 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`

Adding a Veeva Vault DMS Repository for LIQUENT InSight

1. To create a DMS repository in LIQUENT InSight, the DMS Server must be configured first.
2. Log on as an administrator.
3. In the menus, click **GO TO** > **Technical Administration**.
4. In the **Available Options** list, click **DMS Repository Management**.
5. In the **Repositories** view, click the **Create** icon.
6. In the **Server Name** drop-down list select the **Veeva System Server**.
7. In the repository **Name (Docbase)** field, type the name of the Veeva Vault repository.
8. The Active Flag field is set to **Y**, for Yes, so the repository is active as soon as it is added. After you add the repository, you can deactivate it and reactivate it.
9. If you want a different repository name to be displayed in the DMS **Browse** window, in the **Label** field enter the name.
10. In the **Vault URL** field, type the Veeva Vault URL in the format: `https://<vault_name>.veevavault.com` , where `<vault_name>` is the actual Veeva Vault name.
11. In the **Repository User** and **Repository Password** fields, type the credentials for accessing the repository.
12. If you want to enable the LIQUENT InSight users who can access the repository to force new renditions and extractions, in the **Force New Renditions and Extractions** field, click **Yes**.

    Forcing new renditions and extractions means creating missing document renditions and extractions and overwriting document renditions and extractions in the repository.
13. To restrict access to the repository, in the **Limit Access to Specific Users** field, click **Yes**, and do any of the following:

- Restrict access to specific users. In the **Allow Selected Users** section, in the **Access Limited** box, select users. Then click the arrows (**>>**) to move the users to the **Access Allowed** box.
- Restrict access to specific groups. In the **Allow Selected Groups** section, in the **Access Limited** box, select groups. Then click the arrows (**>>**) to move the groups to the **Access Allowed** box.
- Restrict access to users with specific roles. In the **Allow Selected Roles** section, in the **Access Limited** box, select roles. Then click the arrows (**>>**) to move the roles to the **Access Allowed** box.

14. To save the new DMS repository, click **Save**.

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**.

Re-extracting Documents and Regenerating TOC for Active Assemblies

Perform the following procedure for Electronic Lifecycle Publishing (ELP) or Paper Review Publishing (PRP) module installation.

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

Field Name	Value
Username:	admin
Password:	admin

3. Open an active assembly, and then select an attached document in the assembly tree.
4. In the **Document Attributes** pane to the right, confirm that the **Extraction Exists** flag is set to **No** before continuing.
5. Select the top node of the assembly tree in the **tree navigation** pane to the left.
   a) In the **Assembly Attributes** toolbar, click the **down** arrow, and then click **Prepare to Publish**.
6. Select **Generate TOCs** and **Generate Missing Renditions and Extractions**, **Render Generated TOCs** and **Special Sheet Templates** to regenerate TOCs during the Prepare to Publish process. Leave all other options unselected.
   a) Click **OK**,and run the Job Requests report to confirm the process is completed successfully.
7. Repeat this procedure to generate extractions and TOCs for all active assemblies.

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.

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.

Index

A

Assembly *19*, *20*

I

Installation *1*–*5*, *7*, *9*, *11*, *12*, *16*–*29*

N

Navigation *19*

P

Prerequisites *1*, *8*, *9*

R

References *1*, *8*