This license agreement ("License Agreement") sets forth the terms and conditions that govern the distribution and use of the HBM UK Ltd software documentation (the "HBM Software Documentation"), including any and all derivative works. Any unauthorized distribution or use of the HBM Software Documentation is strictly prohibited.

Licensee hereby acknowledges and agrees to the following terms and conditions of this License Agreement for its use of the HBM Software Documentation:

HBM UK Ltd grants the Licensee who accepts and abides by the terms of this License Agreement a non-exclusive, non-transferable, royalty-free, and revocable license to the HBM Software Documentation. Unless otherwise indicated, all HBM Software Documentation are copyrighted and owned by HBM UK Ltd and are the property of HBM UK Ltd. They are licensed to you and for your use only as an individual who has purchased the software ("Licensee"). Notwithstanding this License Agreement, the Licensee shall not have a license to the trademarks, logos, or any other intellectual property of HBM UK Ltd and/or its affiliates or Licensor(s).

Licensee may print a single copy of the HBM Software Documentation for his/her reference. Licensee may reprint the HBM Software Documentation, as needed, if the original printed copy is damaged and/or destroyed.

Except as provided above, no part of the HBM Software Documentation, either text or image, may be used for any purpose other than Licensee’s own personal use and reference as a learning aid. Therefore, the reproduction, modification, creation of derivative works, storage in a retrieval system, or retransmission, in any form or by any means, electronic, mechanical or otherwise, for reasons other than Licensee’s personal use, is strictly prohibited.

Certain photos and images in the HBM Software Documentation are used under non-transferable licenses obtained by HBM UK Ltd and/or its affiliates and are owned by its Licensor(s) ("Licensor"). Images depicting photos of actual persons are licensed to HBM UK Ltd and/or its affiliates and the signed model releases for these images are on file with the Licensor(s). HBM UK Ltd makes no copyright claims on these images. All ownership and intellectual property rights to the HBM Software Documentation are reserved by either HBM UK Ltd and/or its affiliates or its Licensor(s).

DISCLAIMER: THE HBM SOFTWARE DOCUMENTATION IS PROVIDED “AS IS” WITHOUT WARRANTIES OF ANY KIND, EITHER EXPRESS OR IMPLIED, INCLUDING, BUT NOT LIMITED TO: 1) ANY IMPLIED WARRANTIES OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE, OR NON-INFRINGEMENT OF INTELLECTUAL PROPERTY; 2) ANY WARRANTY THAT THE HBM SOFTWARE DOCUMENTATION WILL CONFORM TO SPECIFICATIONS; 3) ANY WARRANTY THAT THE WORK WILL BE ERROR FREE OR VIRUS FREE. IN NO EVENT SHALL HBM UK LTD, ITS AFFILIATES, DISTRIBUTORS, CONTRACTORS, AGENTS, AND ITS LICENSOR(S) BE LIABLE FOR ANY DAMAGES, INCLUDING, BUT NOT LIMITED TO, DIRECT, INDIRECT, SPECIAL OR CONSEQUENTIAL DAMAGES, ARISING OUT OF, RESULTING FROM, OR IN ANY WAY CONNECTED WITH THE HBM SOFTWARE DOCUMENTATION, WHETHER OR NOT BASED UPON WARRANTY, CONTRACT, TORT, OR OTHERWISE, WHETHER OR NOT LOSS WAS SUSTAINED FROM, OR AROSE OUT OF THE RESULTS OF, OR USE OF, THE HBM SOFTWARE DOCUMENTATION. LICENSEES AGREE TO WAIVE ANY AND ALL CLAIMS AGAINST HBM UK LTD, ITS AFFILIATES, DISTRIBUTORS, CONTRACTORS, AGENTS, AND ITS LICENSOR(S), AND SHALL INDEMNIFY, DEFEND AND HOLD HARMLESS HBM UK LTD, ITS AFFILIATES, DISTRIBUTORS, CONTRACTORS, AGENTS, AND ITS LICENSOR(S) FOR ANY AND ALL LIABILITIES, CLAIMS, DEMANDS, DAMAGES, EXPENSES OR LOSSES THAT MAY ARISE FROM THE LICENSEE’S USE OR DISTRIBUTION OF THE HBM SOFTWARE DOCUMENTATION, INCLUDING ANY LIABILITIES OR DAMAGES FROM DERIVATIVE WORKS OR OTHER PRODUCTS BASED ON, OR RESULTING FROM, THE USE THEREOF.

This License Agreement is subject to change without notice and does not represent any commitment on the part of HBM UK Ltd and/or its affiliates to the Licensee, including any commitment to maintain or update the HBM Software Documentation. The names of companies, products, people, characters, and/or data mentioned in the HBM Software Documentation are not intended to represent any real individual, company, product or event, unless otherwise noted. Any rights not expressly granted herein are reserved for HBM UK Ltd.

TRADEMARKS:
ReliaSoft, Synthesis Platform, Weibull++, ALTA, DOE++, RGA, BlockSim, RENO, Lambda Predict, XFMEA, RCM++ and XFRACAS are all trademarks of ReliaSoft Corporation
GlyphWorks, VibeSys, DesignLife and the nCode logos are all trademarks of HBM UK Ltd.

Other product names and services identified in the HBM Software Documentation are trademarks belonging to their respective trademark holders, and are used for illustration purposes. Their use in no way conveys an endorsement or other affiliation with HBM UK Ltd and/or its affiliates.
Synthesis Enterprise Portal Implementation Guide

This document provides instructions to implement ReliaSoft Synthesis Enterprise Portal (SEP) by HBM Prenscia for your organization.

1.1 SEP System Architecture

SEP is a web-based application that serves the needs of engineering teams of any size. The system is based on the .NET Framework and is designed to be n-tier, scalable, distributable, robust and able to be deployed across multiple servers or on a single computer.

Server Requirements

If you plan to host the database and website on the same server, you will need:

- Windows 2008 R2 or newer
- .NET 4.6
- IIS with support for serving ASP.NET
- SQL Server 2008 or newer OR Oracle 10g or newer (32-bit and 64-bit versions of all, full version only)

Client Requirements

Once the website has been implemented, users can access it with any web browser that supports the following doctype.

<!DOCTYPE html PUBLIC "-//W3C//DTD XHTML 1.0 Transitional//EN" "http://www.w3.org/TR/xhtml1/DTD/xhtml1-transitional.dtd">

This includes Internet Explorer, Chrome, Firefox or Safari residing on a Windows operating system, a Mac operating system or a tablet (such as iOS, Android, etc.).

1. If the site is private (e.g., http://InternalServer/SEP), the system administrator may need to provide users with instructions for how to access the website on the internal network from their mobile devices (e.g., via VPN or some other method).
These are the same requirements as the XFRACAS failure reporting, analysis and corrective action system. Both systems can be deployed together on the same database and web server(s).

1.2 Prepare the Database Server - SQL Server or Oracle

The ReliaSoft desktop applications, XFRACAS and the Synthesis Enterprise Portal (SEP) are all designed to connect with the same data repository on either SQL Server or Oracle.

If you need to establish a new data repository, the following considerations apply for preparing the database server.

Later, you will use the admin utility to either create the database or connect the website to an existing database. (See Section 1.6 and Section 1.7.)

If you are setting up for SQL Server:

- Make sure you have the latest version of SQL Server running. To do this, run the following query in Query Analyzer: "Select @@version". This should return a value like “Microsoft SQL Server 2005 - 9.00.3042 (Intel X86)” or “Microsoft SQL Server 2008 R2 - 10.50.1617 (X64),” depending upon which SQL Server service pack you have installed.

- Make sure you know the SQL Server Name. This is a local server name or IP address so the IIS machine with the .NET application can connect to the database. These instructions assume that you will use a default instance of SQL Server to host the ReliaSoft database (e.g., SERVERNAME). If not, you will need to specify the instance when you enter the server name (e.g., SERVERNAME\INSTANCENAME).

If you are setting up for Oracle:

- For easier support, we recommend to have installed the SQL Worksheet (available with the Enterprise edition) or Oracle SQL Developer (free to download from the Oracle website).

1.3 Prepare the Web Server - IIS

To prepare the web server prior to installing the SEP application, you will need to make sure the IIS Web Server role and services are installed, and also prepare for SSL protection if applicable.
IIS Roles and Features

Install the Web Server (IIS) role (if it is not already installed) and make sure it has the following role services installed. (*Instructions are provided below the table for Windows 2016, 2012 and 2008.*)

<table>
<thead>
<tr>
<th>Windows 2016 or 2012</th>
<th>Windows 2008</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Web Server:</strong></td>
<td><strong>Web Server:</strong></td>
</tr>
<tr>
<td>✓ Common HTTP Features</td>
<td>✓ Common HTTP Features</td>
</tr>
<tr>
<td>✓ Default Document</td>
<td>✓ Static Content</td>
</tr>
<tr>
<td>✓ Directory Browsing</td>
<td>✓ Default Document</td>
</tr>
<tr>
<td>✓ HTTP Errors</td>
<td>✓ Directory Browsing</td>
</tr>
<tr>
<td>✓ Static Content</td>
<td>✓ HTTP Errors</td>
</tr>
<tr>
<td>✓ Health and Diagnostics</td>
<td>✓ Application Development</td>
</tr>
<tr>
<td>✓ HTTP Logging</td>
<td>✓ ASP.NET</td>
</tr>
<tr>
<td>✓ Custom Logging</td>
<td>✓ .NET Extensibility</td>
</tr>
<tr>
<td>✓ Logging Tools</td>
<td>✓ ASP</td>
</tr>
<tr>
<td>✓ Request Monitor</td>
<td>✓ ISAPI Extensions</td>
</tr>
<tr>
<td>✓ Application Development</td>
<td>✓ ISAPI Filters</td>
</tr>
<tr>
<td>✓ .NET Extensibility 4.5 or 4.6</td>
<td>✓ Server Side Includes</td>
</tr>
<tr>
<td>✓ Application Initialization (if Windows Server 2016)</td>
<td>✓ Health and Diagnostics</td>
</tr>
<tr>
<td>✓ ASP</td>
<td>✓ HTTP Logging</td>
</tr>
<tr>
<td>✓ ASP.NET 4.5 or 4.6</td>
<td>✓ Logging Tools</td>
</tr>
<tr>
<td>✓ ISAPI Extensions</td>
<td>✓ Request Monitor</td>
</tr>
<tr>
<td>✓ ISAPI Filters</td>
<td>✓ Custom Logging</td>
</tr>
<tr>
<td>✓ Server Side Includes</td>
<td>✓ Security</td>
</tr>
<tr>
<td>✓ Request Filtering</td>
<td>✓ Windows Authentication</td>
</tr>
<tr>
<td>✓ IP and Domain Restrictions</td>
<td>✓ Request Filtering</td>
</tr>
<tr>
<td>✓ Windows Authentication</td>
<td>✓ IP and Domain Restrictions</td>
</tr>
<tr>
<td>✓ Performance</td>
<td>✓ Performance</td>
</tr>
<tr>
<td>✓ Static Content Compression</td>
<td>✓ Static Content Compression</td>
</tr>
<tr>
<td>✓ Dynamic Content Compression</td>
<td>✓ Dynamic Content Compression</td>
</tr>
<tr>
<td>✓ Security</td>
<td>✓ Management Tools:</td>
</tr>
<tr>
<td>✓ Management Tools:</td>
<td>✓ IIS Management Console</td>
</tr>
<tr>
<td>✓ IIS Management Console</td>
<td></td>
</tr>
</tbody>
</table>
On Windows Server 2012 or 2016:

Note that if you do not already have the required version of the .NET Framework installed, you will need to have the operating system installation media available when you install the Web Server (IIS role). The required file is in the sources/sxs folder.

1. Open the Server Manager.
2. Click the Manage menu, choose Add Roles and Features and proceed through the wizard.
   a. If the role is already installed, you can expand the node, review the services that are already installed and select additional services if applicable.
   b. If the role is not already installed, accept any prompts to install required features and proceed to the Web Server (IIS) > Role Services page where you can select the services you need to install.
4. At the end of the wizard, click Install.

On Windows Server 2008:

1. Open the Server Manager.
2. If the Web Server (IIS) role is not installed, view the Roles page and, under Roles Summary, click Add Roles. Follow the wizard to install the role and services.
3. If the Web Server (IIS) role is already installed, view the Roles > Web Server (IIS) page. Under Role Services, review the services that are already installed. If you need to add service(s), click Add Role Services and follow the wizard.

SSL Certificate

If you want the website to use HTTPS for secure communication (SSL/TLS), you must have a digital certificate. Later, you will use this certificate to create the binding for the website. (See Section 1.8 on page 6.)

If you don’t purchase a third-party certificate, you can create your own certificate via another method, such as generating a self-signed certificate via IIS Manager or using the Active Directory Certificate Services role installed on the server.

1.4 Establish a Service Account for the Application (if applicable)

If the database is on SQL Server, we recommend establishing a service account (e.g., “SynUser”) that the website will use to connect to the ReliaSoft database as well as any other external databases that may be used to create “custom connection” dashboards in the Synthesis Data Warehouse (SDW). This account must meet several requirements:

- Active Directory account
- Password does not expire (recommended)
- A user in SQL Server assigned to a public server role, with at least the db_datareader and db_datawriter roles for the ReliaSoft database (if the database does not yet exist, you will need to add the roles via SQL Server after you create it in Section 1.6)
- At least db_datareader role for any other SQL Server databases that will be used by SDW custom connections

If you plan to use this account as a database connection for Open buttons, it must also meet the requirements for an “impersonation user” for all computers that will run desktop applications—specifically, it must be on a trusted domain and it cannot be a local admin, domain admin or member of any Windows admin group (see Section 1.14 on page 11).
1.5 Install the Website and Activate the License

After you have prepared the database and web server(s), you can log in to the web server as an administrator and perform the following steps in the order specified. User Account Control (UAC) can either be left on or turned off for this installation.

1. Run the Synthesis Enterprise Portal setup (e.g., SEP18.exe) and follow the steps in the wizard to create the website and install the activation and admin tools.

2. From Start, search for “SEP 2018 Activation” then run the product activation tool and follow the steps to activate your license.

The license will be registered to a specific e-mail address, which will receive the notification required to activate the license. This will be the same address for all stages of license usage from development/staging to production. Choose an address that someone who changes the hardware on the server will have access to. If the hardware changes for any reason, the license will need to be reactivated in order to get SEP back up and running.

If you already have a database that the website will use, skip ahead to Section 1.7.

1.6 Create the ReliaSoft Database (if Applicable)

If applicable, you can use the admin utility on the web server to create or upgrade the database that your SEP website will use.

Log in to Windows with an Appropriate Account

Before creating a new ReliaSoft database, make sure that you are logged in to Windows with an account that is appropriate for your implementation. This will depend on the database platform and which ReliaSoft applications will connect to the database, now and in the future. The following considerations apply:

- For SQL Server implementations, the account logged in to Windows will create the database and must be able to create objects under the default dbo schema. (For Oracle, you will be prompted to specify the schema and admin login.)

- For ReliaSoft desktop applications and the SEP website, the user who creates the database will receive the first Synthesis Platform user account with full admin permissions for those applications. You can later use this account to create as many other admin accounts as needed and they will all have the same permissions in desktop applications and SEP.

- For XFRACAS, the user who creates the database will receive a special IT/admin-only account within the website that:
  - does not count against the number of users allowed by your XFRACAS license
  - by default, has full permissions within the site’s Admin interfaces
  - will not be visible as a regular user in the site’s User interfaces (i.e., incidents, actions, etc.)

The special account will need to be used on an ongoing basis for some specific IT/admin activities for the XFRACAS website, such as updating database tables, rolling out new permissions to other admin users, bulk data imports (so imported records are not assigned to a particular user), etc.

If you cannot identify a single person who will be available to perform these tasks on an ongoing basis, we recommend to use a shared service account for this purpose.

Create or Upgrade the Database

From Start, search for “SEP 2018 Admin” and open the admin utility.

1. Click either **New Version 2018 Enterprise Repository** or **Upgrade Version 9/10/11 Repository** and enter the details required to create or upgrade the database.
2. If you want to create additional Synthesis Platform user accounts at this time (for access to the ReliaSoft desktop applications or the SEP website), click Manage Synthesis Users. XFRACAS user accounts can only be created from within the website.

**Assign Roles in SQL Server for Application Service Account (if Applicable)**

Finally, if you created a new database on SQL Server, you must make sure the application service account (i.e., the account that the website will use to connect to the database) has the required roles assigned in SQL Server. For requirements, Section 1.4 on page 4.

**1.7 Update the SEP Configuration File**

After you have installed the website, activated the license and established a database, the next step is to update the configuration file on the web server.

From Start, search for “SEP 2018 Admin” and open the admin utility. Then click Update SEP Configuration File.

1. On the Connection tab:
   - **Connection Info** - Enter the required details for the database that the website will connect to. If you used the admin utility to create the database, this will be entered automatically.
     Select Encrypt Connection String if you want to hide the connection string information within the web configuration file.
   - **User Impersonation (SQL Server)** - If the database is on SQL Server, enter the credentials that the SEP website will use to connect. For requirements, see Section 1.4.
     Select Encrypt Impersonation Identity if you want to hide the credentials within the web configuration file.

2. On the Settings tab:
   - **Request timeout** sets how long IIS waits for a request to the application to finish processing. Typically, this will not need to be changed for an SEP implementation.
   - For a SQL Server implementation, select Encrypt communication if you want to encrypt the connection between the application and the database.
     - Select Trust server certificate if the server has a self-signed certificate.

   **NOTE:** If you want to encrypt the connection for an Oracle implementation, you must set the encryption type to either "requested" or "required" for the Oracle database. For more information, please consult the Oracle documentation (e.g., https://docs.oracle.com/cd/B19306_01/network.102/b14268/asoconfig.htm#i1007808).

   - If a Secure Socket Layer (SSL) certificate has been implemented for the SEP website, select Yes for HTTP Cookies Require SSL if you also want the browser cookies to require SSL (an additional level of security).

**1.8 Post-Installation Steps on the Web Server**

After installation, there are additional settings that you may need to configure on the web server to fit your particular implementation.

If you need to make changes to address OWASP security concerns, see Section 1.19.

**1.8.1 Start the Synthesis Service (if applicable)**

The Synthesis Service is an optional utility that is installed with SEP. If you want to use the service to send alerts for Synthesis Platform actions based on calendar date (e.g., when the action is due in X days), you will need to configure
the repository settings to fit your organization's particular needs (as discussed in Section 1.15 on page 13) and make sure the service is running on the web server.

To start the Synthesis Service on the SEP web server:

1. From **Start**, search for “Services” and open the Services window.
2. In the list of local services, right-click **SynthesisService** and select **Properties**.
3. On the **Log On** page, enter the credentials for an account that the service can run as. We recommend to use an account that does not expire, such as the application service account discussed in Section 1.4 on page 4.
4. On the **General** page, set the **Startup type** to either “Automatic” or “Automatic (Delayed Start).” Then click **Start**.

The current status of the service (Running, Not Running or Not Found) will be displayed on the SEP Admin page.

By default, this service is configured to not run for a period from 8 pm to 10 pm each day that can be used for routine database maintenance and backups (**StopProcessingTime** = 20:00:00 and **MinutesToHoldProcessing** = 120). If you need to change these settings, you can edit serviceConfig.xml on the web server. By default, this file is installed in the “bin” folder for the SEP website (e.g., C:\inetpub\wwwroot\SEP\bin). Other settings in this file will be updated automatically when you make changes in the SEP Configuration File (see Section 1.7 on page 6).

### 1.8.2 HTTPS for Secure Communication

If you want to use HTTPS for secure communication (SSL/TLS) and you already have a certificate for the website (as discussed in Section 1.3 on page 2), do the following:

1. In the Connections pane of the IIS Manager, open the **Sites** node under the server name. Click the **Default Web Site**.
2. In the **Actions** area on the right side of the window, click the **Bindings** link and then click the **Add** button in the Site Bindings window that appears.
3. Add a site binding of type https and specify your digital certificate. Close the Site Bindings window.
4. Return to the Connections pane and click the **SEP** site.
5. Under IIS, double-click the **SSL Settings** icon. Select **Require SSL** and **Ignore**, then click **Apply**.

*If you need to use this with the TLS 1.2 protocol, also see Section 1.8.6 on page 9.*

### 1.8.3 IIS Application Pool Identity (if applicable for SDW Dashboards)

If you need to prepare the SEP website to display Synthesis Data Warehouse (SDW) dashboards based on custom connections to external Access databases (or to external SQL Server databases if the ReliaSoft database is on Oracle), you may wish to set a service account (e.g., “SynUser”) as the IIS application pool identity (see Section 1.4). This is not recommended if your website is public.

1. In the Connections pane of the IIS Manager, click **Application Pools**.
2. Right-click the website’s application pool and choose **Advanced Settings** on the shortcut menu.
3. For the **Identity** property, click the **...** button to open the Application Pool Identity window. Select the **Custom account** option and click **Set** to open the Set Credentials window. Enter the account credentials (domain/username) for the service account and click **OK**.

Note that for Access databases with the *.accdb file type, the dashboard can only be displayed if the database was created with the same version of Microsoft Office (32-bit or 64-bit) that is installed on the web server (for SEP) or on the individual user's computer (for ReliaSoft desktop applications).
To ensure that the dashboard will display regardless of which version of Microsoft Office is installed, use the *.mdb file type instead.

### 1.8.4 Release and Recycle Memory

For large systems or systems with a high transactional load, an “Out of Memory” error can occur when the request for pages exceeds the system’s capability to release and recycle the memory with the default IIS settings. The settings provided below will force IIS to recycle the memory usage and handle the memory usage better so that the “Out of Memory” error does not occur. Note that being too aggressive with regard to how memory is recycled can slow down the response of the system. Typically, memory is recycled when the application pool and the server are not busy. Forcing memory recycling to happen more often can take up processor cycle time when the application is still busy, thus slowing down system performance. The following settings have been tested to prevent the error occurring while making the minimum possible impact on performance.

1. In the Connections pane of the IIS Manager, click **Application Pools**.
2. Right-click the system’s application pool and choose **Recycling** on the shortcut menu.
3. In the Application Pool Recycling Settings window that appears, specify the following settings:
   - In the Fixed Intervals area, select **Regular time intervals** and enter **1740**.
   - In the Memory Based Maximums area, select **Private memory usage** and enter **1,024,000**.
     a. Click **Next**.
     b. Select to log the following events and click **Finish**:
        - **Regular time intervals**
        - **Private memory usage**
        - **Unhealthy ISAPI**

### 1.8.5 Limits for Uploads, Buffering and Requests

You will need to specify some limits for uploads, buffering and requests to suit your needs for the website (e.g., if you are running very large reports and find that they do not respond, if you are unable to upload large files, etc.).

1. In the Connections pane of the IIS Manager, click the **SEP** site. Under Management, double-click **Configuration Editor**.
2. In the Section drop-down list, choose **system.webServer/asp**.
   - Under limits:
     - The **maxRequestEntityAllowed** value sets the maximum file size that can be uploaded to the server. This is set during installation to 4,194,304 bytes (or ~4 MB).
     - The **bufferingLimit** value sets the size of the buffer that holds the response sent back to the client. This is set during installation to 4,194,304 bytes (or ~4 MB).
3. In the Section drop-down list, choose **system.webServer/caching**.
   - The **maxResponseSize** value sets the maximum file size that can be returned to the client. This is set during installation to 262,144 bytes (or ~262 KB).
4. In the Section drop-down list, choose **system.web/httpRuntime**.
   - The **maxRequestLength** value specifies the limit for the input stream buffering threshold, in kilobytes. This is set to 4096 KB by default.
5. Return to the Connections pane, click the **SEP** site. Under IIS, double-click **Request Filtering**.
6. In the Actions panel, click the **Edit Feature Settings** link.
   - The **Maximum allowed content length** value specifies the maximum length of content in a request, in bytes. This is set to 30000000 bytes (or ~30 MB) by default.

### 1.8.6 Enable TLS 1.2 Protocol for HTTPS (on Windows 2008 or 2012)

If you are using HTTPS for secure communication and you wish to enable TLS 1.2, the same protocol must be enabled for the database server, the web server and .NET on the web server. *(Also note that if you are using a digital certificate, it must be SHA-256 or higher.)*

If your web server and database server are both Windows 2016, the TLS 1.2 protocol will be enabled by default. If either server is Windows 2008 or 2012, add the following registry keys:

```markdown
Windows Registry Editor Version 5.00

[HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\SecurityProviders\SCHANNEL\Protocols]

[HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\SecurityProviders\SCHANNEL\Protocols\SSL 2.0]
[HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\SecurityProviders\SCHANNEL\Protocols\SSL 2.0\Client]
"DisabledByDefault"=dword:00000001

[HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\SecurityProviders\SCHANNEL\Protocols\TLS 1.0]
[HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\SecurityProviders\SCHANNEL\Protocols\TLS 1.0\Client]
"Enabled"=dword:00000000

[HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\SecurityProviders\SCHANNEL\Protocols\TLS 1.1]
[HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\SecurityProviders\SCHANNEL\Protocols\TLS 1.1\Client]
"DisabledByDefault"=dword:00000000

[HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\SecurityProviders\SCHANNEL\Protocols\TLS 1.1\Server]
"DisabledByDefault"=dword:00000000

[HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\SecurityProviders\SCHANNEL\Protocols\TLS 1.2]
[HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\SecurityProviders\SCHANNEL\Protocols\TLS 1.2\Client]
"DisabledByDefault"=dword:00000000

[HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\SecurityProviders\SCHANNEL\Protocols\TLS 1.2\Server]
"DisabledByDefault"=dword:00000000
```
1.9 Set up Synthesis Platform User Accounts and Permissions

After the database has been created, you can use any of the desktop applications or the Synthesis Admin utility to create Synthesis Platform user accounts and set access permissions. You must create an account for anyone who will be able to edit or view data in the ReliaSoft desktop applications or SEP. (User accounts for XFRACAS are managed separately.)

- In the ReliaSoft Admin tool on the web server, click the Manage Synthesis Users button.
- In the ReliaSoft desktop applications (e.g., Weibull++, XFMEA, etc.), first open the database and then choose File > Manage Repository > Users and Security.

If your organization uses Microsoft Active Directory, you can save time by importing user information from the directory to create the user accounts.

For more information, please consult the “Security Options” topics in the desktop application help files (e.g., http://help.synthesisplatform.net/weibull_alta18/security_options.htm).

1.10 Assign SEP Access to Users

After the Synthesis Platform user accounts have been created, you can use the SEP website to specify which users will have access to the web portal.

Click the SEP Admin link in the top-right corner of the website and then use the Select SEP Users section to specify which user accounts will have website access.

The counters above the user table identify how many more SEP users are allowed under your current license.

1.11 Enable Publish to Synthesis Enterprise Portal

Some SEP-related features in ReliaSoft desktop applications (e.g., the ability to publish analysis summaries, workbooks, reports, etc.) will be visible only if the Enable publish to Synthesis Enterprise Portal option is set to “Yes” for the database.

This can be set from the SEP Admin page in the website or from the Repository Settings window in any of the desktop applications:

Enable publish to Synthesis Enterprise Portal:
(this option can also be set by admin users in the desktop applications)
- YES
- NO
1.12 Configure Custom Content for Home

The optional “Custom Content” area in the SEP home page enables your organization to integrate a banner or other custom content into the site, if desired. This can be configured from the SEP Admin page in the website.

The SEPDefault.htm file is installed in the CustomContent folder under the root directory for the SEP website. You can choose to edit this file on the web server or replace it with a URL to another web page.

Configure 'Custom Content' for the home page:

- Visible: ✔
- Height in pixels: 100

Caption: Title of the Panel in the Home Page

- Use SEPDefault.htm on the application web server
- Use a page from another website (HTTP only)
  http://www.mysite.com/banner_page.htm

NOTE: If the content of the page is taller than the specified height in pixels, users with IOS devices will not be able to scroll.

1.13 Configure URLs for Links to Actions in SEP

When an SEP website is implemented for an enterprise database, the action alert e-mails and portal messages generated by any of the ReliaSoft applications can include links to view the action details in SEP. The applications build the links based on the settings specified on the SEP Admin page in the website. If an administrator has not specified an IIS prefix, the action alerts will not include links to SEP.

- SEP Server - IIS Prefix - enter the server name and folder for the website that you see in the browser's Address bar (e.g., servername/SEP).
- Website Uses SSL (https for URLs) - select Yes if the web server has been configured with a Secure Socket Layer (SSL) certificate for the SEP website and the URLs need to start with https rather than http.

If these settings do not match your website configuration, the links attached to the action alerts will give an error message when users attempt to open the page in a web browser (e.g., “File or directory not found,” “Access forbidden” or “This page can't be displayed”).

1.14 Configure Open Buttons

When users view published analysis summaries and FMEAs in SEP, the Open buttons make it easy to open the full analysis in a relevant desktop application.

1.14.1 Database Connection for Open Buttons (Oracle)

For an Oracle database, the Open buttons always use the same database connection specified for the website (see Section 1.7 on page 6).

1.14.2 Database Connection for Open Buttons (SQL Server)

For a SQL Server database, you can choose one of the following options on the SEP Admin page:

- No impersonation – the buttons will attempt to connect using the domain\username that is currently logged in to Windows. In order to use the desktop applications, each user must have an individual or group login.
• **Same as SEP Configuration File** – the buttons will use the same impersonation account as the website (see Section 1.4 on page 4).

• **Specify impersonation account for Open buttons** – the buttons will use the impersonation account that you specify.

### 1.14.3 Remote ReliaSoft

You can configure SEP to be able to run the applications on a remote server without having to install and update software on each client computer. If Remote ReliaSoft is enabled for your implementation, the User Preferences page gives each user the option of whether to launch the applications on the remote server or generate locator links.

**Requirements**

- A Windows server that can be configured with Microsoft Remote Desktop Services (RDS) and RDP RemoteApp, or multiple RDS servers and a “broker” that distributes the requests. When planning your hardware requirements, you can estimate the following typical memory requirements per application per session. For example, a server with 32 GB RAM could support approximately 30 simultaneous ALTA users, or 100 simultaneous Lambda Predict users, and so on.

<table>
<thead>
<tr>
<th>Application</th>
<th>Estimated Memory Requirement per Session (MB)</th>
</tr>
</thead>
<tbody>
<tr>
<td>ALTA</td>
<td>1000</td>
</tr>
<tr>
<td>RGA</td>
<td>1000</td>
</tr>
<tr>
<td>Weibull++</td>
<td>900</td>
</tr>
<tr>
<td>BlockSim</td>
<td>500</td>
</tr>
<tr>
<td>RENO</td>
<td>500</td>
</tr>
<tr>
<td>XFMEA</td>
<td>400</td>
</tr>
<tr>
<td>RCM++</td>
<td>400</td>
</tr>
<tr>
<td>RBI</td>
<td>300</td>
</tr>
<tr>
<td>MPC</td>
<td>300</td>
</tr>
<tr>
<td>Lambda Predict</td>
<td>300</td>
</tr>
</tbody>
</table>

- Sufficient RDS license seats (purchased from your preferred Microsoft vendor).

- ReliaSoft desktop applications installed and kept up-to-date on the RDS server(s). Locally hosted licensing is recommended (Token-based or Floating). If you do not already have a locally hosted license server for ReliaSoft and nCode software, see instructions at [https://www.reliasoft.com/locally-hosted-licensing](https://www.reliasoft.com/locally-hosted-licensing).

**Set Up the RDS Server(s) and Create a Connection File**

Note that this document provides partial instructions focused on the settings that will affect your ability to generate a connection file that can be used within SEP. If you are not familiar with the steps required to install and configure Remote Desktop Services, you may need to consult documentation/support provided by Microsoft.

1. Install the ReliaSoft desktop applications and configure the locally hosted licensing.
2. In the Windows Server Manager, make sure the required “Remote Desktop Services” roles are installed:

<table>
<thead>
<tr>
<th>Windows 2016 or 2012</th>
<th>Windows 2008</th>
</tr>
</thead>
<tbody>
<tr>
<td>• Remote Desktop Session Host</td>
<td>• Remote Desktop Session Host</td>
</tr>
<tr>
<td>• Remote Desktop Connection Broker</td>
<td>• Remote Desktop Services Manager</td>
</tr>
<tr>
<td>• Remote Desktop Web Access</td>
<td>• Remote App Manager</td>
</tr>
</tbody>
</table>

3. In Remote Desktop Session Host, configure your Remote Desktop license (CALs) and any other settings that are appropriate for your implementation.

   - In Windows 2016 or 2012, in the Windows Server Manager under Remote Desktop Services, create a Session Collection. In the collection, use Publish RemoteApp Programs and follow the wizard. In the Properties window, make sure the Parameters setting is set to “Allow any command line parameters.”
   - In Windows 2008, follow the wizard in the RemoteApp Manager. Make sure the Arguments setting is set to “Unrestricted.”

5. Create and save an *.rdp file that contains the connection information for the ReliaSoft Launcher.
   - In Windows 2016 or 2012, open RDWeb (e.g., https://servername/RDWeb) in a web browser (other than Internet Explorer) and save the connection file.
   - In Windows 2008, click the Create .rdp File link in the RemoteApp Manager.

   **Note:** SEP will use the *.rdp file that you provide as a template, and it will add settings that allow the ReliaSoft Launcher to open a specific ReliaSoft application, project and analysis. If your RDS server is configured to use digital certificates, you may need to edit the file (e.g., in Notepad or another text editor) before uploading to SEP. Specifically, if a certificate was added to the end of the file, it must be removed.

**Enable “Remote ReliaSoft” in SEP Admin**

1. On the SEP Admin page under Remote ReliaSoft, click Browse to find and upload the RDP template that contains the connection information for the ReliaSoft Launcher (created in step 5 above).
2. Click Save (at the top of the page) to upload the file to the database.
3. Click Test Remote ReliaSoft. Depending on your browser settings, this will either download or open an *.rdp file, or prompt you to choose. When you open the file, the ReliaSoft Launcher should run on the remote server.
4. After you confirm that the template is working properly, select the Open Applications via Remote Desktop Services (RemoteApp) check box and click Save (at the top of the page).

1.15 Configure Synthesis Service for Alerts Based on Calendar Date

A ReliaSoft database can be configured to send alerts when a Synthesis Platform action is created, modified or ready to be reviewed. These alerts are sent to any user who is subscribed to “watch” the action, and they can be delivered via e-mail, SMS text message or Synthesis Platform message, depending on each user's preference. (See “Watches and Alerts” in the documentation for any ReliaSoft desktop application.)

New in Version 2018, the Synthesis Service allows you to send additional alerts based on calendar date, if desired. If the service is running on the SEP web server, you can use the SEP Admin page to specify when the service will trigger “Action Due” alerts.

- **Service Status** indicates whether the service was Running, Not Running or Not Found at the time when the page loaded.
- **Alert when action is due in [x] days** - if selected, enter the number of days before the action completion date (due date) to send the first alert.
  - **Remind every [x] days until the action is complete** - if selected, the service will continue to send reminders until the action is complete. Enter the number of days between alerts.
  
  For example, if this is set to 21 days and 7 days, the service will send the first reminder 3 weeks before the due date and then continue to send reminders every week until the action is completed.

- **From Address for E-mail Alerts** - e-mail alerts sent by the service will be “from” this address.

### 1.16 Configure Links Between XFRACAS and SEP

If your organization implements both SEP and XFRACAS for the same enterprise database, you can use the Admin Preferences page in XFRACAS (Admin > Configure > Preferences) to enable links between the two websites.

- **SEP to XFRACAS:**
  - Specify the XFRACAS Server - IIS Prefix (e.g., servername/XFRACAS)

- **XFRACAS to SEP:**
  - Specify the Synthesis Enterprise Portal Server - IIS Prefix (e.g., servername/SEP)
  - Set Synthesis - Display Synthesis Enterprise Portal (SEP) Command to True

### 1.17 Allow Aqira Users to Access SEP

nCode Aqira by HBM Prenscia allows your organization to manage and share nCode fatigue and durability analyses via the web.

New in Version 2018, Aqira users are entitled to access the Synthesis Enterprise Portal without requiring an SEP license seat. To enable this access:

1. On the SEP Admin page under nCode Aqira, specify:
   - **Aqira URL** (e.g., http://servername/aqira/)
   - **Aqira Admin Username**
   - **Aqira Admin Password**

2. Click **Test Aqira Login**. If the settings are valid, the page will display “Success” after the test completes.

3. Select the **Allow Aqira users to log in to SEP** check box.

4. Click **Save** (at the top of the page) to save the new settings.

When the feature is enabled, SEP’s menu will include a link to the Aqira login page. In addition, when an active Aqira user attempts to access SEP, the application will check for a Synthesis Platform user account:

- If an account does not exist, it will be created automatically with the “Aqira” security group. (This group will always have at least “read” access to projects that use “repository-level security.” Any user with permission to edit security groups in ReliaSoft desktop applications can change these permissions to fit your needs.)
- If an account exists and is active, the user can access SEP with the permissions specified for the existing account.
- If an account exists but is inactive, the user cannot access SEP.

### 1.18 Distribute SEP Website Link to All Users

Once the web portal has been implemented, users can access the site with any web browser that supports the following doctype. If the site is private (e.g., http://InternalServer/SEP), the system administrator may need to
provide users with instructions for how to access the website on the internal network from their mobile devices (e.g., via VPN or some other method).

<!DOCTYPE html PUBLIC "-//W3C//DTD XHTML 1.0 Transitional//EN" "http://www.w3.org/TR/xhtml1/DTD/xhtml1-transitional.dtd">

1.19 Additional IIS Configuration Changes for Enhanced Security

This section provides recommendations to address issues that may be identified if you choose to scan your web server for Open Web Application Security Project (OWASP) security concerns.

For some of the issues listed here, you will need to install the URL Rewrite tool, available at http://www.iis.net/downloads/microsoft/url-rewrite.

The tasks performed in the IIS Manager should be done at the default web site level (i.e., in the Connections pane, open the Sites node under the server name and click Default Web Site). Alternatively, the model web.config code provided in Section 1.19.1 on page 17 summarizes the changes made in the IIS Manager. If you make these changes directly in the web.config file in the root folder for your website, you can skip the steps shown here in italics.

Web Server Default Welcome Page
1. From the wwwroot directory, remove iisstart.htm, welcome.png and the asp_client folder.

Clickjacking: X-Frame-Options Header Missing
1. In the IIS Manager Home page, double-click HTTP Response Headers.
2. In the Actions area, click Add. Enter X-Frame-Options as the name, and SAMEORIGIN as the value.

OPTIONS Method Is Enabled
1. In the IIS Manager Home page, double-click Request Filtering.
2. On the HTTP Verbs tab, click Allow Verb in the Actions area and enter Options in the Deny Verb window.

Microsoft IIS Version Disclosure
1. In the following Registry key, create a dWORD entry called DisableServerHeader and set the value to 1:
   HKLM\SYSTEM\CurrentControlSet\Services\HTTP\Parameters
2. In the IIS Manager Home page, double-click URL Rewrite.
3. In the Actions area, click View Server Variables, then click Add and enter RESPONSE_SERVER in the text box.
4. Add an outbound rule to rewrite the RESPONSE_SERVER server variable as blank.
   a. In the Actions area, click Back to Rules and then click Add Rule(s).
   b. In the Add Rule(s) window, click Blank rule in the Outbound rules category and click OK.
   c. Create the outbound rule using the following settings:
      - Name: Response Server
      - Precondition: None
      - Matching scope: Server Variable
      - Variable name: RESPONSE_SERVER
      - Variable value: Matches the Pattern
      - Using: Regular Expressions
      - Pattern: .+
• Action type: Rewrite
• Action Properties:
  o Value: <leave this field empty>
  o Replace existing server variable value: Selected

**ASP .NET Version Disclosure**

1. In the IIS Manager Home page, double-click **URL Rewrite**.
2. In the **Actions** area, click **View Server Variables**, then click **Add** and enter **RESPONSE_X-ASPNET-VERSION** in the text box.
3. Add an outbound rule to rewrite the **RESPONSE_X-ASPNET-VERSION** server variable as blank.
   a. In the **Actions** area, click **Back to Rules** and then click **Add Rule(s)**.
   b. In the Add Rule(s) window, click **Blank rule** in the **Outbound rules** category and click **OK**.
   c. Create the outbound rule using the following settings:
      • Name: x-ASPNet
      • Precondition: None
      • Matching scope: Server Variable
      • Variable name: RESPONSE_X-ASPNET-VERSION
      • Variable value: Matches the Pattern
      • Using: Regular Expressions
      • Pattern: .+
      • Action type: Rewrite
      • Action Properties:
         o Value: <leave this field empty>
         o Replace existing server variable value: Selected

**X-Powered-By Header**

1. In the IIS Manager Home page, double-click **HTTP Response Headers**.
2. Select the **X-Powered-By** header and click **Remove**.
3. In the IIS Manager Home page, double-click **URL Rewrite**.
4. In the **Actions** area, click **View Server Variables**, then click **Add** and enter **RESPONSE_X-POWERED-BY** in the text box.
5. Add an outbound rule to rewrite the **RESPONSE_X-POWERED-BY** server variable as blank.
   a. In the **Actions** area, click **Back to Rules** and then click **Add Rule(s)**.
   b. In the Add Rule(s) window, click **Blank rule** in the **Outbound rules** category and click **OK**.
   c. Create the outbound rule using the following settings:
      • Name: X-Powered
      • Precondition: None
      • Matching scope: Server Variable
      • Variable name: RESPONSE_X-POWERED-BY
      • Variable value: Matches the Pattern
      • Using: Regular Expressions
      • Pattern: .+
1.19 Additional IIS Configuration Changes for Enhanced Security

- Action type: Rewrite
- Action Properties:
  - Value: <leave this field empty>
  - Replace existing server variable value: Selected

Custom Errors

1. In the IIS Manager, open the Configuration Editor.
2. In the Section drop-down list, choose system.web/customErrors.

1.19.1 Default Website Root web.config Changes

```xml
<?xml version="1.0" encoding="UTF-8"?>
<configuration>
    <system.web>
        <customErrors mode="RemoteOnly"/>
    </system.web>
    <system.webServer>
        <httpProtocol>
            <customHeaders>
                <remove name="X-Powered-By"/>
                <add name="X-Frame-Options" value="SAMEORIGIN"/>
            </customHeaders>
        </httpProtocol>
        <security>
            <requestFiltering>
                <verbs>
                    <add verb="OPTIONS" allowed="false"/>
                </verbs>
            </requestFiltering>
        </security>
        <rewrite>
            <outboundRules>
                <rule name="Response Server">
                    <match serverVariable="RESPONSE_SERVER" pattern=".+"/>
                    <action type="Rewrite"/>
                </rule>
                <rule name="X-Powered">
                    <match serverVariable="RESPONSE_X-POWERED-BY" pattern=".+"/>
                    <action type="Rewrite"/>
                </rule>
                <rule name="x-ASPNet">
                    <match serverVariable="RESPONSE_X-ASPNET-VERSION" pattern=".+"/>
                    <action type="Rewrite"/>
                </rule>
            </outboundRules>
        </rewrite>
    </system.webServer>
</configuration>
```
1.20 Other FAQs

1.20.1 Can we implement replication for a ReliaSoft database?

XFRACAS, SEP and the ReliaSoft desktop applications cannot be deployed with bi-directional database replication (*peer-to-peer replication* or *merge replication*). The applications are designed for use with a single back-end database; they do not handle conflict detection and resolution.

It may be possible to use a ReliaSoft database with uni-directional replication (*transactional replication* or *snapshot replication*). However, this is likely to affect the performance of the application(s) and you must test on your own to evaluate the impact in your particular situation. **This type of use is not recommended or supported by ReliaSoft.**

For the purpose of disaster recovery, we recommend to establish a regular schedule for *database backups* and *transaction log backups*. These backups can be stored in a location that is protected from potential failure of the application's database server. If an issue occurs, you can restore the most recent database backup (e.g., nightly) and then restore subsequent transaction logs up to the point right before the failure.