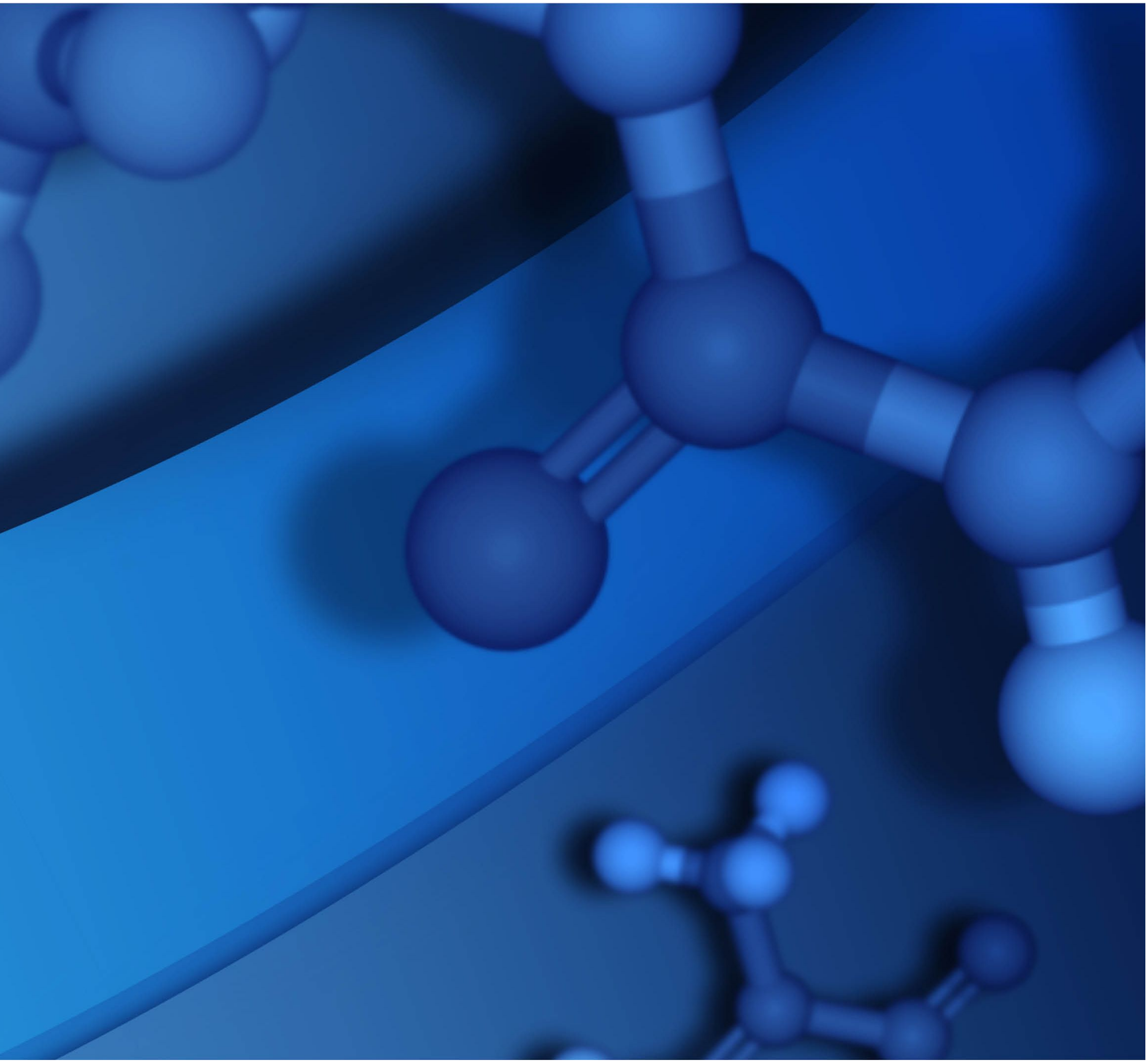
INSTALLATION AND CONFIGURATION GUIDE

BIOVIA FOUNDATION HUB 2021 HF1



Copyright Notice

Acknowledgments and References

To print photographs or files of computational results (figures and/or data) obtained by using Dassault Systèmes software, acknowledge the source in an appropriate format. For example:

> "Computational results were obtained by using Dassault Systèmes BIOVIA software programs. BIOVIA Foundation Hub was used to perform the calculations and to generate the graphical results."

Dassault Systèmes may grant permission to republish or reprint its copyrighted materials. Requests should be submitted to Dassault Systèmes Customer Support, either by visiting https://www.3ds.com/support/ and clicking **Call us** or **Submit a request**, or by writing to:

Dassault Systèmes Customer Support
10, Rue Marcel Dassault
78140 Vélizy-Villacoublay
FRANCE

Contents

Chapter 1: Overview

This guide describes how to deploy and perform an initial configuration of BIOVIA Foundation Hub, which is a key part of BIOVIA Foundation.

Once deployed, you can use Foundation Hub to administer your BIOVIA Foundation deployment.

For details about administering Foundation Hub, see the *BIOVIA Foundation Hub Administration Guide*, which is available in PDF format and from the **?** Help icon on the Foundation Hub toolbar.

IMPORTANT! Do not copy and paste commands from this guide to the command window. Copy to a text editor first and check that the hyphens are correct.

Note: `<hub_install>` is the root of the BIOVIA Foundation Hub installation.
On Windows this is typically:
`C:\Program Files\BIOVIA\Foundation`
On Linux this depends on the location of your Foundation Hub installation, but may be:
`[Home]/BIOVIA/Foundation`

What is BIOVIA Foundation?

BIOVIA Foundation refers to the integrated scientific environment to which BIOVIA applications (including Pipeline Pilot) are connected. BIOVIA Foundation includes the Pipeline Pilot protocol execution engine (to support extension of BIOVIA applications that run Pipeline Pilot protocols), implements security and administration of users, and includes Foundation Hub, amongst other capabilities.

What Is Foundation Hub?

Foundation Hub serves as the authentication provider for all connected foundation applications and enables session management, single sign-on, and single-sign out across BIOVIA applications.

- **Admin and Settings:** Manage security, resources such as equipment, organization, and location information, and settings for Foundation Hub and other BIOVIA applications. For more information, see the *BIOVIA Foundation Hub Administration Guide*.
- **Landing Page:** The BIOVIA Landing page provides a dashboard for managing tasks, viewing notifications, and monitoring equipment that requires calibrationFor more information, see the *Foundation Hub User Guide*.
- **Quick Access to Applications:** Click the **Applications** link in the Foundation Hub toolbar to access BIOVIA applications and any additional links configured for your organization. For more information, see the *BIOVIA Foundation Hub Administration Guide*.

Toolbar Links

The toolbar at the top of Foundation Hub contains the following tools:

🏠	Opens the BIOVIA Landing page
▦	Opens the BIOVIA Applications menu

🔔	Opens a list of your notifications
⚙	Opens Admin and Settings
?	Opens a menu of help options
👤	Access User Settings or Sign out.

Who Should Install Foundation Hub?

The following applications *require* Foundation Hub when installed as part of the Collaborative Science suite:

- Insight
- Insight for Excel
- QSAR Workbench
- Biotherapeutics Workbench
- Workbench Framework

The following applications *require* Foundation Hub when installed as part of the Unified Lab Management suite:

- Workbook
- Notebook
- Experiment (EKB)
- Compose and Capture
- Request
- CISPro
- Chemical and Biological Registration

> **Note:** Legacy EKB Upgrades support Foundation Hub, but do not require it.

The following applications support Foundation Hub, but do not require it:

- Pipeline Pilot
- Materials Studio
- Discovery Studio
- Draw

Which Applications Require BIOVIA Foundation?

The following BIOVIA applications require BIOVIA Foundation Hub:

- BIOVIA Compose and Capture
- BIOVIA Workbook
- BIOVIA Request

The following Pipeline Pilot applications use binstore:

- BIOVIA Insight
- BIOVIA Biological Registration
- BIOVIA Chemical Registration
- BIOVIA QSAR Workbench

The following applications may be run as standalone applications. If they are deployed with Unified Lab Management (ULM), they must connect to Foundation Hub:

- BIOVIA Pipeline Pilot
- BIOVIA CISPro
- BIOVIA Notebook
- BIOVIA Experiment

Foundation Hub Deployment Options

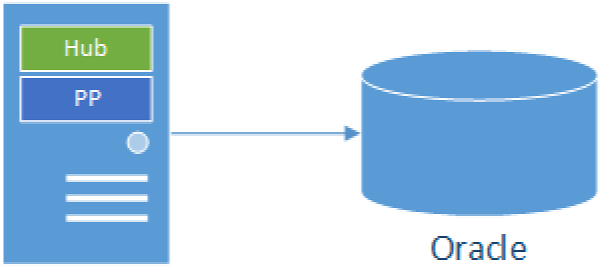
BIOVIA Foundation can be installed on a single node (for example, standalone server) or in various high-availability topologies. Pipeline Pilot, Foundation Hub and other applications communicate through RESTful web services over HTTP and HTTPS. The following sections describe example deployment topologies for standalone server and high availability needs.

Tip: Installing on a shared file system is not recommended.

Standalone Server

The following are possible configuration for Pipeline Pilot and BIOVIA Foundation Hub:

- BIOVIA Foundation can be installed entirely on a single node that includes Pipeline Pilot and BIOVIA Foundation Hub servers.



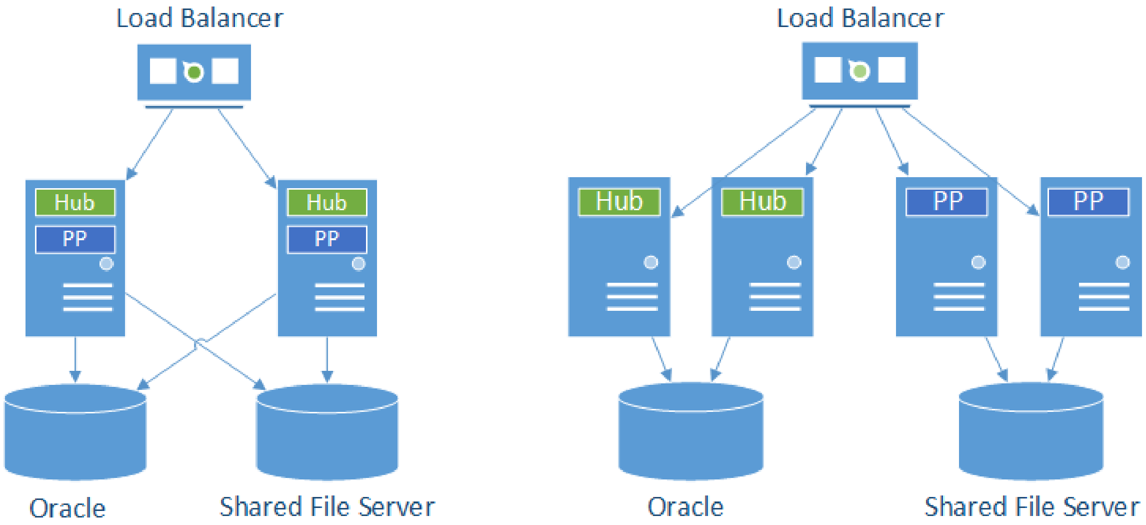
Pipeline Pilot and Foundation Hub installed on the same node.

- You can install Pipeline Pilot and BIOVIA Foundation Hub on separate servers.
- You can have a single Foundation server authenticating multiple Pipeline Pilot servers.

Load Balancing

Load balancing distributes incoming HTTPS requests across web servers in a server farm, which helps avoid overloading any one server.

A separate load balancer is required to distribute incoming HTTPS requests across a group of servers. This provides high availability and scalability to handle high concurrent usage. Use this deployment model to deliver services for large-scale production applications.



High-availability configuration that deploys Pipeline Pilot and Foundation Hub instances on shared servers or separate nodes.

Note: See the Pipeline Pilot Help Center for more detailed information about configuring high-availability deployments. From the Pipeline Pilot Server Home Page (`http://localhost:9944` by default), click **Help Center (Administrators)** and expand the **Reference Guides** section to access the *Pipeline Pilot Server Installation Guide* and *Pipeline Pilot Server Deployment Guide*.

Oracle Database

BIOVIA Foundation Hub maintains all application data in a separate Oracle database. Use Oracle RAC for high availability of the data layer. Foundation Hub configuration files must be aligned and each node registered in the application registry.

Using Ansible Software

BIOVIA supports using Ansible to manage installations and upgrades for Foundation Hub, Pipeline Pilot, CISPro, Compose and Capture, and Workbook. For details, see the *Ansible Installation Guide for BIOVIA*. This document is included in the zipped product documentation for ULM, which is available from the Dassault Systèmes Download Platform alongside the product installers.

Chapter 2: Foundation Hub Installation Checklists

Review the following pre-installation, installation, and post-installation checklists carefully before starting and use them to keep track of your progress. If you have any questions, visit https://www.3ds.com/support/.

If you are upgrading from a previous version of Foundation Hub, refer to Chapter 5: Upgrading Foundation Hub.

Pre-Installation Checklist

Review this checklist carefully before starting installation and use it to keep track of your progress.

Step	Details	Done?
1. Review the security recommendations.	See Security Considerations.	□
2. Choose a standalone or load-balanced deployment.	See Foundation Hub Deployment Options. **Tip:** If the deployment is load-balanced, document the URL and port assignments for Foundation Hub on the load balancer.	□
3. Obtain servers that meet requirements and set up administrative accounts.	Obtain servers that meet the system requirements for the BIOVIA applications they will host and obtain an administrator account for each server with full administrative permissions. See *Foundation Hub System Requirements* and the system requirements documentation for your applications. **IMPORTANT!** ■ Install the Foundation Hub on the local disk. Installing on a shared file system is not recommended. ■ For Windows, you must have administrator privileges. ■ For Linux, you must have root access.	□
4. Set up an Oracle database and schema.	Set up an Oracle database and Oracle schema (account) that meet the system requirements. See Chapter 3: Creating a Foundation Hub Database Schema in Oracle.	□

Step	Details	Done?
5. Obtain a valid license.	Make sure you have a valid license file. Licenses are made available when the software is purchased. If you need assistance with licenses, contact Dassault Systèmes Customer Support. You will be prompted for a license during installation.	□
6. Check for port conflicts on the servers that will host Foundation Hub or on the load balancer.	By default, Foundation Hub uses the following ports: ■ 9953 (HTTPS) ■ 9954 (HTTP) ■ 9955 (Shutdown) **Tips:** ■ If the deployment is load-balanced, make a note of the URL and port assignments for Foundation Hub on the load balancer. ■ You can download a netstat utility (Windows and Linux) to check your network for port availability.	□
7. Obtain SSL certificates for application servers	Use certificates from a trusted Certificate Authority for production systems. See Chapter 7: Working with Certificates.	□
8. Prepare for SPNEGO/Kerberos	If you are planning to authenticate with SPNEGO/Kerberos, review Configuring SPNEGO/Kerberos Authentication.	□

Installation Checklist

Step	Details	Done?
1. Install Foundation Hub.	See Chapter 4: Installing Foundation Hub or Chapter 5: Upgrading Foundation Hub.	□
2. Configure Foundation Hub settings.	Configure the Web Server, Database, Authentication, and Certificate settings: ■ Configuring Foundation Hub on a Single Server ■ Configuring Foundation Hub for Load Balancing	□
3. Configure additional Foundation Hub servers if load balancing.	See Adding Subsequent Load-Balanced Foundation Hub Servers.	□
4. Test the load-balanced configuration.	See Testing Load-Balanced Foundation Hub Servers.	□

Post-Installation Checklist

Step	Details	Done?
1. Provision users.	See Setting Up User Authentication.	□
2. Install Pipeline Pilot and the FoundationSSO package.	■ Foundation 2021 HF1 requires Pipeline Pilot 2021. If it is not already installed, upgrade Pipeline Pilot to 2021. Refer to the *Pipeline Pilot Installation Guide* and *Pipeline Pilot Admin Portal Guide* included within the Pipeline Pilot documentation zip file. ■ For Foundation Hub 2021 HF1, install the separate *FoundationSSO* package on the Pipeline Pilot server. This package contains Pipeline Pilot components and protocols required for Foundation Hub 2021 HF1. For details about installing the FoundationSSO package, see Installing the FoundationSSO Package for Pipeline Pilot. ■ Set **Authentication Method** to **Foundation**.	□
3. Install the remaining BIOVIA applications.	Install the remaining BIOVIA applications. See the installation documentation available with the installation artifacts for more information.	□
4. Update the registered	From the **Pipeline Pilot Admin Portal > Reports > Foundation Applications**, click **Update**	□

Step	Details	Done?
applications in Pipeline Pilot.	**Applications**.	
5. Configure site data and equipment.	Use the **Foundation Hub Server Admin Portal > Admin and Settings** area to configure site data and laboratory instruments and equipment. See the *Foundation Hub Administration Guide* for details about further configuration and managing Foundation Hub: 1. Open a browser and navigate to `http://<hub name>:9954`. 2. Click the help icon ? in the navigation bar and choose **Admin Guide**.	□

Chapter 3:
Creating a Foundation Hub Database Schema in Oracle

Foundation Hub requires an Oracle database that meets the tablespace and other requirements listed in the *Foundation Hub System Requirements*.

IMPORTANT!

- The database server should be on the same local area network as the Foundation Hub server; there should be very low (less than 1 ms) latency between the database and the Foundation Hub server.
- It is important to keep your Oracle database password up to date in Foundation Hub. See Resetting Your Oracle Password. If the password expires or has been changed without following these instructions, you will need to manually update it in the configuration file. See Chapter 12: Troubleshooting.
- If you are upgrading, the required permissions must be granted before upgrading.
- Ensure table compression is *disabled* for the Foundation Hub tablespace.

Oracle Database User

The database *must* be configured with a user that has the following privileges:

- create table
- create session
- create sequence
- create synonym
- create view
- alter session

To avoid interruption to your system's operations, it is recommended that the user is configured with a profile for which passwords do not expire.

Installation Script

Note: For environments where Foundation Hub is to be used as part of Unified Lab Management, it is recommended to start with a large default tablespace size of 25 G. For small test or development environments or where Foundation Hub is not part of ULM, a smaller value of 1 or 2 G is sufficient.

Note the following values:

- `<hub tablespace>` is the name of the tablespace where the Foundation Hub schema will be installed.
- `<path to data file>` is the location of the of the database data file.
- `<hub schema>` is the user with access to the `<hub tablespace>`.
- `<password>` is the password for the schema owner.

```
CREATE TABLESPACE <hub tablespace> DATAFILE '/<path to data file>/Hub.dbf'
SIZE 25G AUTOEXTEND ON NEXT 1G MAXSIZE UNLIMITED EXTENT MANAGEMENT LOCAL
SEGMENT SPACE MANAGEMENT AUTO;

CREATE USER <hub schema> IDENTIFIED BY <password> DEFAULT TABLESPACE <hub
tablespace> TEMPORARY TABLESPACE TEMP;

GRANT CREATE SESSION, ALTER SESSION, CREATE SEQUENCE, CREATE TABLE,
CREATE SYNONYM, CREATE VIEW to <hub schema>;

ALTER USER <hub schema> QUOTA UNLIMITED ON <hub tablespace>;
```

Example

This example uses the following values:

- `<hub tablespace>` is `HUB_TS`.
- `<path to data file>` is `C:\hubdata\Hub.dbf`.
- `<hub schema>` is `HUB_OWNER`.
- `<password>` is `HUBPWD`, you should always customize this to a secure value.

```
CREATE TABLESPACE HUB_TS DATAFILE 'C:\hubdata\Hub.dbf' SIZE 25G AUTOEXTEND
ON NEXT 1G MAXSIZE UNLIMITED EXTENT MANAGEMENT LOCAL SEGMENT SPACE
MANAGEMENT AUTO;

CREATE USER HUB_OWNER IDENTIFIED BY HUBPWD DEFAULT TABLESPACE HUB_TS
TEMPORARY TABLESPACE TEMP;

GRANT CREATE SESSION, ALTER SESSION, CREATE SEQUENCE, CREATE SYNONYM, CREATE
TABLE, CREATE VIEW to HUB_OWNER;

ALTER USER HUB_OWNER QUOTA UNLIMITED ON HUB_TS;
```

(Recommended) Preventing Password Expiration

By default, Oracle user passwords expire after 180 days, which would require you to reset your Oracle password for Foundation Hub on a regular basis. To avoid manual updates or an out-of-date password error, you can prevent the Oracle database password from expiring. You have several options for how to configure this setting. For example:

- You can update the default profile so that passwords do not expire.

  ```
  ALTER PROFILE default LIMIT PASSWORD_LIFE_TIME UNLIMITED;
  ```

- If your organization's policies do not allow updates to the default profile, you can create a separate profile for the Oracle database user and configure that profile so that passwords do not expire.

  ```
  CREATE PROFILE <hub profile> LIMIT
       PASSWORD_REUSE_TIME UNLIMITED
       PASSWORD_LIFE_TIME UNLIMITED;

  ALTER USER <hub schema> PROFILE <hub profile>;
  ```

Tip: For more information on managing security and password settings for database users, see the Oracle documentation for your database version. For example, see Managing Security for Oracle Database Users and Password Settings in the Default Profile for Oracle version 19c.

Testing

To test the schema, log into SQL*Plus as the schema owner of Foundation Hub to ensure a successful connection.

Resetting Your Oracle Password

You must keep the Oracle database password up to date in Foundation Hub. It is recommended that you configure the Oracle database user so that the password does not expire. If you need to reset the Oracle password, follow these instructions.

> **Note:** If the password expires or has been changed without following these instructions, you will need to manually update it in the configuration file. See Chapter 12: Troubleshooting.

1. Open **Admin and Settings > Hub Configuration** and click **Edit**.
2. Set the **Data Source Password** field to the *new* Oracle schema password.
3. Click **Save**. ***Do not*** close the browser and ***do not*** click **Restart Server**.
4. In Oracle, set the Foundation Hub schema owner’s *new* password and commit.
5. On the **Admin and Settings > Hub Configuration** page, click **Restart Server**.

Chapter 4: Installing Foundation Hub

IMPORTANT! If you are upgrading, see Chapter 5: Upgrading Foundation Hub.

Pre-Installation

1. Before you begin, carefully review the Installation Checklist.

   Notes:
   - Side-by-side installation is not supported.
   - Install the Foundation Hub on the local disk.
   - For Windows, you must have administrator privileges.
   - For Linux, you must have root access.

2. Make sure you have a valid license file. Licenses are made available when the software is purchased. If you need assistance with licenses, contact Dassault Systèmes Customer Support.

   You will be prompted for a license during installation.

3. Check for port conflicts. The installer has a feature that allows you to check for port conflicts. If you need to use ports that differ from the defaults, be ready to specify the alternate ports during installation. Foundation Hub uses the following ports by default:
   - 9953 (HTTPS)
   - 9954 (HTTP)
   - 9955 (Shutdown)

4. Obtain and extract the installer archive for your operating system from the Dassault Systèmes Download Platform:
   - **Windows:** `BIOVIA_<version>.Foundation<version>_Win64.zip`
   - **Linux:** `BIOVIA_<version>.Foundation<version>_Linux64.tgz`

     ```
     tar -xpvzf
     ```

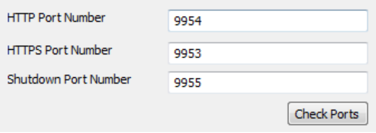
Installing

Tip: BIOVIA supports using Ansible to manage installations and upgrades for Foundation Hub, Pipeline Pilot, CISPro, Compose and Capture, and Workbook. For details, see the *Ansible Installation Guide for BIOVIA*. This document is included in the zipped product documentation for ULM, which is available from the Dassault Systèmes Download Platform alongside the product installers.

1. In the extracted folder, run the installer:
   - **Windows:** Double-click `Foundation2021HF1.exe`.
   - **Linux:** From the command line, run:

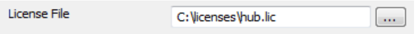
     ```
     $ sh Foundation2021HF1.bin
     ```

2. Proceed through the setup dialogs.
   a. When prompted for ports, click **Check Ports** to check for conflicts with the default ports for Foundation Hub (9954, 9953, and 9955):



HTTP Port Number: 9954
HTTPS Port Number: 9953
Shutdown Port Number: 9955

   b. Provide the path to the license in the License File field:



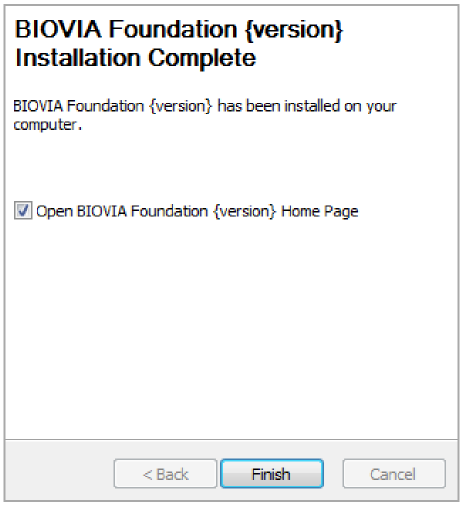
License File: C:\licenses\hub.lic

> **Note:** The license should contain keys for all licensed BIOVIA applications for your site, for example, Foundation Hub, Compose and Capture, and Workbook.

3. On Linux, a boot script starts the *BIOVIA Hub Server <version>* service whenever the computer is restarted. Run the following command as root to install the boot script. Otherwise, the service will have to be started manually each time the machine is restarted:

```
<hub_install>/bin/daemon.sh install
```

4. Continue until your installation is complete. On the last page of the wizard, keep the option to open the home page checked and click **Finish**:



BIOVIA Foundation {version}
Installation Complete

BIOVIA Foundation {version} has been installed on your computer.

☑ Open BIOVIA Foundation {version} Home Page

If you encounter issues during installation, check the log files here: **Admin and Settings > Settings > Logging** or `install.log` in the installation directory.

5. Configure Foundation Hub as a single server or continue installing additional load-balanced Foundation Hub servers:
   - If you are installing on a single server, configure your server now. See Configuring Foundation Hub on a Single Server.
   - If you are installing a load-balance configuration:
     a. Continue installing or updating Foundation Hub on additional servers. See Adding Subsequent Load-Balanced Foundation Hub Servers.
     b. Configure your master load-balanced server and copy the configuration files to the other load-balanced servers. See Configuring Foundation Hub for Load Balancing.
6. Continue with Chapter 8: Post-Installation Steps.

Installing Silently from the Command Line (Windows)

1. Log on to the destination computer as an administrator.
2. Extract the `BIOVIA_<version>.Foundation<version>_Win64.zip` file.
3. In the extracted folder, locate the `Silent.ini` file.

   The `Silent.ini` file is set to upgrade any existing installation by default.

   To force a new installation, edit `Silent.ini` and set `Upgrade=no`.
4. Run the following command as an administrator:

   ```
   Foundation<version>.exe /S /D=<hub_install>
   ```

   Notes:

   - The default installation path for Foundation Hub is `C:\Program Files\BIOVIA\Foundation\Hub`.
   - Do **not** use quotes in the `/D` argument even if there are spaces in the path.
5. Verify the upgrade has succeeded by checking on the service status. To do this, see Managing the Foundation Hub Service .

Checking the Installation

1. If the BIOVIA Foundation Hub web page does not open automatically after the upgrade, open a browser and navigate to:

   `https://<hubserver>:9953/foundation/hub`

   or a different port if you specified a non-default port during installation.
2. Log in as a Foundation Administrator.
3. Open **Admin and Settings > Settings > Applications**.
4. In the **Foundation Hub** row in the table, verify that the **Application Version** is listed as 2021 HF1.

Chapter 5:
Upgrading Foundation Hub

The section provides detailed instructions for upgrading BIOVIA Foundation and an overview for upgrading the remaining applications.

Refer to **Upgrade Paths** in the *Foundation Hub 2021 HF1 Product Release Document* for a list of earlier releases and any interim releases to which you must upgrade before you upgrade to *Foundation Hub 2021 HF1*.

IMPORTANT!

- Renew and update your certificates before they expire, or you will not be able to log in to Foundation Hub or any applications that rely on it for authentication. If you need to update or replace certificates, see Updating Certificates.
- Before you upgrade, refer to **Upgrade Paths** in the *Foundation Hub 2021 HF1 Product Information Document* to ensure that no interim upgrades are required to upgrade from your current release to 2021 HF1.

Overview

The following is the general order of upgrades for BIOVIA applications installed as part of a suite. For details, see Notes and Best Practices for Upgrading, Upgrading, and Post-Upgrade below.

Tip: BIOVIA supports using Ansible to manage installations and upgrades for Foundation Hub, Pipeline Pilot, CISPro, Compose and Capture, and Workbook. For details, see the *Ansible Installation Guide for BIOVIA*. This document is included in the zipped product documentation for ULM, which is available from the Dassault Systèmes Download Platform alongside the product installers.

1. Notify users and stop all BIOVIA application services.
2. Upgrade the Foundation Hub server.
3. Upgrade Pipeline Pilot.
4. For Foundation Hub 2021 HF1, install the separate *FoundationSSO* package on the Pipeline Pilot server. This package contains Pipeline Pilot components and protocols required for Foundation Hub 2021 HF1. For details about installing the FoundationSSO package, see Installing the FoundationSSO Package for Pipeline Pilot.
5. Upgrade the remaining BIOVIA applications.
6. If an application service stopped in Step 1 did not restart as part of the upgrade process, start the service manually.

Notes and Best Practices for Upgrading

- BIOVIA supports using Ansible to manage installations and upgrades for Foundation Hub, Pipeline Pilot, CISPro, Compose and Capture, and Workbook. For details, see the *Ansible Installation Guide for BIOVIA*. This document is included in the zipped product documentation for ULM, which is available from the Dassault Systèmes Download Platform alongside the product installers.
- Before you upgrade, refer to **Upgrade Paths** in the *Foundation Hub 2021 HF1 Product Information Document* to ensure that no interim upgrades are required to upgrade from your current release to

2021 HF1.

- If you are upgrading a Pipeline Pilot Server connected to Foundation Hub, do not disconnect Pipeline Pilot Server before upgrading. You should stop services for ALL BIOVIA applications before upgrading Foundation Hub, but do not remove the applications from Foundation Hub or change the Pipeline Pilot authentication to something other than Foundation.
- Your configuration from the previous installation will be preserved after the upgrade of Foundation Hub.
- Side-by-side installation of different versions of Foundation Hub is not supported.
- Make sure you have a valid license file. Licenses are made available when the software is purchased. If you need assistance with licenses, contact Dassault Systèmes Customer Support.

  You will be prompted for a license during installation.
- Perform database checks. See Database Checks.
- Notify users that the services for BIOVIA applications will be stopped and restarted during the upgrade. Ask them to log out of all BIOVIA applications and refrain from using them until after the upgrade.
- Upgrade Foundation Hub before upgrading Pipeline Pilot OR any other BIOVIA application.

Database Checks

- The `CREATE SYNONYM` privilege is required for Foundation Hub 2018 SP1 or newer. See Chapter 3: Creating a Foundation Hub Database Schema in Oracle.
- Make sure the database schema includes all of the permissions covered in Creating a Foundation Hub Database Schema in Oracle.
- In Oracle, log in as the Foundation Hub schema owner to ensure the schema is functional and back up your Oracle database.

Upgrading

1. Follow Notes and Best Practices for Upgrading.
2. Stop the services for BIOVIA applications:
   - Applications that rely on Foundation Hub (such as BIOVIA Compose Service, BIOVIA CISPro, and Vault Services)
   - Pipeline Pilot services
   - BIOVIA Hub Server <version>service
3. Archive and rename the log files:
   a. Archive the log files in the `<hub_install>\logs` folder by copying and pasting them into a temporary folder so that you can access them until your upgrade is successful.
   b. In the `<hub_install>\logs` folder, rename `install.log`, so that a new log file is generated when you upgrade to 2021 HF1. Otherwise, the log messages will be appended to the existing `install.log` during the upgrade which makes them difficult to review.
4. Obtain and extract the installer archive for your operating system from the Dassault Systèmes Download Platform.

   - **Windows:** `BIOVIA_<version>.Foundation<version>_Win64.zip`
   - **Linux:** `BIOVIA_<version>.Foundation<version>_Linux64.tgz`

     ```
     tar -xpvzf
     ```

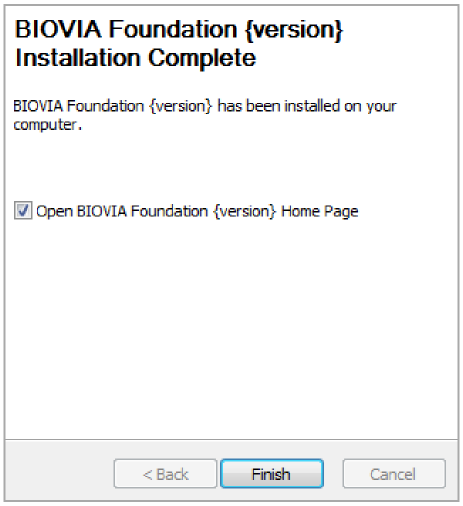
5. In the extracted folder, you can install Foundation Hub using the following methods:
   - **Windows:** Do one of the following:
     - Double-click `Foundation<version>.exe` to run the installer.
     - To install silently on Windows from the Command Line, see Installing Silently from the Command Line (Windows).
     - To install silently on Windows using Ansible software, see Using Ansible Software.
   - **Linux:** From the command line, run:

     ```
     $ sh Foundation<version>.bin
     ```

     In Linux, a boot script starts the BIOVIA Hub Server 2021 HF1 service whenever the computer is restarted. If you did not install the boot script in the previous installation or if you have changed the installation location, run the following command as root:

     ```
     <hub_install>/bin/daemon.sh install
     ```

6. When the installation is complete, keep the option to open the home page checked and click **Finish**:

   BIOVIA Foundation {version} Installation Complete

   BIOVIA Foundation {version} has been installed on your computer.

   ☑ Open BIOVIA Foundation {version} Home Page

   The BIOVIA Hub Server 2021 HF1 service restarts automatically after the upgrade.

   If you encounter issues during installation, check the `hub.log` and `install.log` files in the installation directory.

Upgrading Load-Balanced Foundation Hub

Follow these instructions if you are upgrading load-balanced Foundation Hub.

1. Follow Notes and Best Practices for Upgrading.
2. Ensure that the BIOVIA Hub service is stopped on each Foundation Hub server machine.
3. Upgrade the first Foundation Hub server. For details, see Upgrading.
4. Ensure that you are able to open the URL for the load balancer and sign in to Foundation Hub.

5. Complete the upgrade of all other load-balanced Foundation Hub Server machines one at a time. Each upgrade must be fully completed on the Foundation Hub server machine before you upgrade the next Foundation Hub server machine.
6. Ensure that you are able to open the URL and sign in to Foundation Hub on each server machine.

Post-Upgrade

1. Check that Foundation Hub was upgraded successfully.
   a. If the BIOVIA Foundation Hub web page does not open automatically after the upgrade, open a browser and navigate to:

      ```
      https://<hubserver>:9953/foundation/hub
      ```

      or a different port if you specified a non-default port during installation.
   b. Log in as a Foundation Administrator.
   c. Open **Admin and Settings > Settings > Applications**.
   d. In the **Foundation Hub** row in the table, verify that the **Application Version** is listed as 2021 HF1.
2. Foundation Hub 2021 HF1 requires Pipeline Pilot server 2021. If Pipeline Pilot is a version prior to Pipeline Pilot 2021, upgrade Pipeline Pilot to 2021 or higher.

   After the upgrade, restart the Pipeline Pilot service. If it does not restart automatically after the upgrade, and then update the registration of BIOVIA Pipeline Pilot in **Pipeline Pilot Admin Portal > Reports > Foundation Applications > Update Applications**.
3. For Foundation Hub 2021 HF1, install the separate *FoundationSSO* package on the Pipeline Pilot server. This package contains Pipeline Pilot components and protocols required for Foundation Hub 2021 HF1. For details about installing the FoundationSSO package, see Installing the FoundationSSO Package for Pipeline Pilot.
4. Upgrade the BIOVIA applications that rely on Pipeline Pilot, and then manually update the application's registration in **Pipeline Pilot Admin Portal > Reports > Foundation Applications > Update Application**s.
5. Upgrade any remaining BIOVIA applications.
6. If an application service that was stopped during the upgrade does not restart automatically, start the service manually.
7. Check the registered applications in Foundation Hub. Open **Admin and Settings > Settings > Applications**.

Chapter 6:
Configuring Foundation Hub

The approach that you should take when configuring Foundation Hub depends on whether you are:

- Configuring Foundation Hub on a Single Server
- Configuring Foundation Hub for Load Balancing

> **IMPORTANT!** Review Security Considerations before configuring your installation.

Configuring Foundation Hub on a Single Server

1. Open the Foundation Hub Configuration page:

   a. Open a browser and navigate to the Foundation Hub Landing Page, for example:
   `https://<hubserver>:9953`

   b. Click **Settings** ⚙ **> Hub Configuration.**

2. Complete the **Web Server Configuration** fields:

   - **Host Name:** Provide the name of the host. The default is the fully qualified server host name.

     > **Note:** If the host name changes, you can edit this setting in the `app-config.groovy` file. See Troubleshooting.

   - **HTTP**, **HTTPS**, and **Shutdown Ports:** Change the ports if needed. The defaults are:
     - HTTP: 9954
     - HTTPS: 9953
     - Shutdown: 9955
   - **Reverse Proxy HTTP and HTTPS URLs:** Provide the URL of the reverse proxy server that fronts this Foundation Hub application.

     > **Notes:**
     > - For a load-balanced server, the URL contains the HTTP and HTTPS ports. For example:
     >   `<hub_lb_server>.mycompany.com:9953`
     >   `<hub_lb_server>.mycompany.com:9954`
     > - If you are configuring the load balancer to use HTTPS only, include the HTTPS URL in both the HTTPS URL and HTTP URL fields.
     > - Only specify if the Foundation Hub is installed behind a reverse proxy.

   - **Session Inactivity Timeout:** Set the length of inactivity before a user session becomes locked and requires a password. Specify the time in days (d), hours (h), or minutes (m). The default is 30m.
   - **Session Global Timeout:** Set the length of a session before the user must log in again regardless of inactivity. Specify the time in days (d), hours (h), or minutes (m). The default is 8h.
   - **Validate Login Return Url:** Select this check box to allow redirects only to known endpoints after login. This is selected by default.
   - **Environment Label:** Enter text to display in the toolbar to identify the environment (for example, Test or Production).

- **3DDashboard Hosted:** To use a 3DX Platform application header and color scheme for this installation of Foundation Hub, select this check box. This check box is unselected by default, and is intended for use only by Dassault Systèmes support personnel.

3. Complete the **Database Configuration** fields:
   - **Data Source URL:** Provide the JDBC URL to your Oracle database. On restart, Foundation Hub checks the schema status and creates the necessary schema and data modifications to prepare the database for use. If you are connecting to a previously used schema, only necessary modifications are made. The following is an example of an Oracle JDBC connection string: `jdbc:oracle:thin:@//<oracle server name>:<port>/<service name>`
   - **Data Source Username and Password:** Provide the Oracle schema username and password in which Foundation Hub data is stored.

     You must keep the Oracle database password up to date in Foundation Hub. It is recommended that you configure the Oracle database user so that the password does not expire. If you need to reset the Oracle password, see Resetting Your Oracle Password.

     > **Note:** If the password expires or has been changed without following these instructions, you will need to manually update it in the configuration file. See Chapter 12: Troubleshooting.

4. Hazelcast is *not* enabled by default. Do not change the **Hazelcast Configuration** settings unless instructed by Dassault Systèmes Customer Support.
5. Complete the **Certificate Configuration** fields:

   > **Notes:**
   > - For more information about certificates, see Chapter 7: Working with Certificates.
   > - This is not needed if the load balancer has an SSL Certificate Keystore installed.
   > - Although not required, it is highly recommended to install a valid trusted keystore because some BIOVIA applications such as Workbook and CISPro may not connect to Foundation Hub properly without one.

   - **Hub SSL Certificate Keystore Path:** Provide the path to the JKS format keystore file.
   - **Keystore Password:** Include the password for the keystore or the path to the truststore JKS certificate file, which must contain the load balancer's public key.

     Leave this blank if the Foundation Hub server has a valid signed SSL certificate issued by a recognized Certificate Authority (CA).
   - **Keystore Alias:** Provide the keystore alias. This is required if the specified keystore file has multiple certificate entries.
6. Complete the **Authentication Provider** fields:
   - Foundation Hub authentication: Set **Authentication** to **Hub**. For more information, see Setting Up User Authentication.
   - 3DPassport authentication: Set **Authentication** to **Passport**, set **Server Url** to the 3DPassport server, and then choose whether to use the **Primary Authenticator** option:
     - If you choose the **Primary Authenticator** option, users are directed to the 3DPassport - Login page.
     - If you leave **Primary Authenticator** unselected, users are directed to a sign in dialog box with an option to authenticate using Foundation Hub or 3DPassport.

     See Setting Up User Authentication with 3DPassport.

- SPENGO/Kerberos authentication: Set **Authentication** to **Hub**, and choose **Enable Kerberos Authentication**, see Configuring SPNEGO/Kerberos Authentication and complete the following information:
  - **Service Principal:** Provide the full name of the service principal including the service type prefix (for example, `HTTP/`) and the server's fully qualified domain name (for example, `HTTP/<server FQDN>`).
  - **Realm Name:** Provide the name of the Kerberos realm. This is usually the server domain in upper-case.
  - **Key Tab Location:** Include the path to the keytab file you copied to the server.

7. Leave **Application Monitoring** settings disabled unless instructed by Dassault Systèmes Customer Support to turn them on.
   - **Enable Melody:** Select the checkbox to diagnose issues such as performance and system load.
   - **Enable Tomcat Http Access Logging:** Select the checkbox to log the remote host/IP address URL and response codes. Logs are created in <hub_install>/logs. See Foundation Hub Logging.
8. Click **Save**.
9. Click **Restart Server**. The service restarts and provisions the database schema. The restart may take several minutes.
10. Continue with Chapter 8: Post-Installation Steps.

Configuring Foundation Hub for Load Balancing

A load-balanced or web farm configuration consists of a load balancer and multiple servers. The load balancer is a virtual server shared between all other servers, it acts as a reverse proxy and distributes network or application traffic across a number of servers. Load balancers are used to increase capacity (concurrent users) and reliability of applications.

A load-balanced set of Foundation Hub servers must all have identical configurations in every respect.

You can configure Foundation Hub for load balancing after the initial installation. BIOVIA Foundation Hub supports load balancing when encrypted traffic (HTTPS) is passed through the load balancer.

Refer to the documentation for your load balancing software for more information. Load balancing Foundation Hub is not supported with SSL termination.

For information on configuring a load-balanced set of Pipeline Pilot Servers, refer to the Load Balancing Pipeline Pilot chapter of the *Pipeline Pilot Server Installation Guide*.

Requirements

To prepare a load-balanced configuration, you require:

- The fully qualified domain name and IP address of the load-balanced Foundation Hub server, for example:

  ```
  <hub_lb_server>.mycompany.com
  192.168.2.100
  ```

  Where *<hub_lb_server>* is the hostname of the load-balanced Foundation Hub server.

- The server names for each server. For example:

  ```
  <hubserver1>.mycompany.com
  <hubserver2>.mycompany.com
  <hubserver3>.mycompany.com
  ...
  ```

- The same ports should be available and open on the load-balanced Foundation Hub server and all other Foundation Hub servers.

  The default Foundation Hub ports are 9953, 9954, and 9955.

  This ensures that a load-balanced server address redirects to the other servers properly, for example:

  `https://<hub_lb_server>.mycompany.com:9953/foundation/hub`

- A shared network folder that you can use to transfer files between Foundation Hub server machines to ensure that they are identical across the load-balanced configuration. For example:

  `\\networkshares\hubshares`

  You will use this to store:

  - The SSL certificate and the truststore JKS certificate file if required.
  - The Kerberos keytab file (if you are using Kerberos for authentication).
  - Configuration files: `app-config.groovy` and `tomcat.properties`

Configuring the Primary Load-Balanced Foundation Hub Server

First, configure a primary Foundation Hub ready for load balancing. You will record this configuration and then configure other Foundation Hubs identically.

IMPORTANT! Record the values used for the these settings. You must use the same values on subsequent load-balanced Foundation Hub servers.

1. Open the Foundation Hub Configuration page as an administrator:
   a. Open a browser and navigate to the Foundation Hub Landing Page (for example, `https://<hubserver1>:9953`).
   b. Click ⚙.
   c. Open **Settings > Hub Configuration**.
   d. Click **Edit**.
2. Complete the **Web Server Configuration** fields:
   - **Host Name:** Provide the name of the host. The default is the fully qualified server host name.

     Note: If the host name changes, you can edit this setting in the `app-config.groovy` file. See Troubleshooting.

   - **HTTP**, **HTTPS**, and **Shutdown Ports:** Change the ports if needed. The defaults are:
     - HTTP: 9954
     - HTTPS: 9953
     - Shutdown: 9955
   - **Reverse Proxy HTTP and HTTPS URLs:** Provide the URL of the reverse proxy server that fronts this Foundation Hub application.

Notes:

- For a load-balanced server, the URL contains the HTTP and HTTPS ports. For example:

  `<hub_lb_server>.mycompany.com:9953`

  `<hub_lb_server>.mycompany.com:9954`
- If you are configuring the load balancer to use HTTPS only, include the HTTPS URL in both the HTTPS URL and HTTP URL fields.
- Only specify if the Foundation Hub is installed behind a reverse proxy.

- **Session Inactivity Timeout:** Set the length of inactivity before a user session becomes locked and requires a password. Specify the time in days (d), hours (h), or minutes (m). The default is 30m.
- **Session Global Timeout:** Set the length of a session before the user must log in again regardless of inactivity. Specify the time in days (d), hours (h), or minutes (m). The default is 8h.
- **Validate Login Return Url:** Select this check box to allow redirects only to known endpoints after login. This is selected by default.
- **Environment Label:** Enter text to display in the toolbar to identify the environment (for example, Test or Production).
- **3DDashboard Hosted:** To use a 3DX Platform application header and color scheme for this installation of Foundation Hub, select this check box. This check box is unselected by default, and is intended for use only by Dassault Systèmes support personnel.

3. Complete the **Database Configuration** fields:

   - **Data Source URL:** Provide the JDBC URL to your Oracle database. On restart, Foundation Hub checks the schema status and creates the necessary schema and data modifications to prepare the database for use. If you are connecting to a previously used schema, only necessary modifications are made. The following is an example of an Oracle JDBC connection string: `jdbc:oracle:thin:@//<oracle server name>:<port>/<service name>`
   - **Data Source Username and Password:** Provide the Oracle schema username and password in which Foundation Hub data is stored.

     You must keep the Oracle database password up to date in Foundation Hub. It is recommended that you configure the Oracle database user so that the password does not expire. If you need to reset the Oracle password, see Resetting Your Oracle Password.

   Note: If the password expires or has been changed without following these instructions, you will need to manually update it in the configuration file. See Chapter 12: Troubleshooting.

4. Hazelcast is *not* enabled by default. Do not change the **Hazelcast Configuration** settings unless instructed by Dassault Systèmes Customer Support.
5. Complete the **Certificate Configuration** fields:

   Notes:

   - For more information about certificates, see Chapter 7: Working with Certificates.
   - This is not needed if the load balancer has an SSL Certificate Keystore installed.
   - Although not required, it is highly recommended to install a valid trusted keystore because some BIOVIA applications such as Workbook and CISPro may not connect to Foundation Hub properly without one.

  - **Hub SSL Certificate Keystore Path:** Provide the path to the JKS format keystore file.
  - **Keystore Password:** Include the password for the keystore or the path to the truststore JKS certificate file, which must contain the load balancer's public key.

    Leave this blank if the Foundation Hub server has a valid signed SSL certificate issued by a recognized Certificate Authority (CA).
  - **Keystore Alias:** Provide the keystore alias. This is required if the specified keystore file has multiple certificate entries.

6. Complete the **Authentication Provider** fields:
   - Foundation Hub authentication: Set **Authentication** to **Hub**. For more information, see Setting Up User Authentication.
   - 3DPassport authentication: Set **Authentication** to **Passport**, set **Server Url** to the 3DPassport server, and then choose whether to use the **Primary Authenticator** option:
     - If you choose the **Primary Authenticator** option, users are directed to the 3DPassport - Login page.
     - If you leave **Primary Authenticator** unselected, users are directed to a sign in dialog box with an option to authenticate using Foundation Hub or 3DPassport.

     See Setting Up User Authentication with 3DPassport.
   - SPENGO/Kerberos authentication: Set **Authentication** to **Hub**, and choose **Enable Kerberos Authentication**, see Configuring SPNEGO/Kerberos Authentication and complete the following information:
     - **Service Principal:** Provide the full name of the service principal including the service type prefix (for example, `HTTP/`) and the server's fully qualified domain name (for example, `HTTP/<server FQDN>`).
     - **Realm Name:** Provide the name of the Kerberos realm. This is usually the server domain in upper-case.
     - **Key Tab Location:** Include the path to the keytab file you copied to the server.
7. Leave **Application Monitoring** settings disabled unless instructed by Dassault Systèmes Customer Support to turn them on.
   - **Enable Melody:** Select the checkbox to diagnose issues such as performance and system load.
   - **Enable Tomcat Http Access Logging:** Select the checkbox to log the remote host/IP address URL and response codes. Logs are created in <hub_install>/logs. See Foundation Hub Logging.
8. Click **Save** and then **Restart Server**. The service restarts and provisions the database schema.

   Notes:
   - The restart may take several minutes.
   - You can restart the server manually. See Chapter 9: Managing the Foundation Hub Service .
9. Copy the SSL certificate to the shared network folder so that it can be transferred to other load-balanced Foundation Hub servers. For example:

   ```
   \\networkshares\hubshares
   ```
10. If you are using Kerberos authentication, copy the keytab file to the shared network folder so that it can be transferred to other load-balanced Foundation Hub servers.

11. Navigate to the `<hub_install>\conf` directory on your primary Foundation Hub server machine. Copy the following files to the shared network folder so that they can be transferred to other load-balanced Foundation Hub servers:
    - `app-config.groovy`
    - `tomcat.properties`

    > **IMPORTANT!** After you have installed and configured the load-balanced Foundation Hub servers, remove any files from the shared network folder to prevent unauthorized access.

Adding Subsequent Load-Balanced Foundation Hub Servers

Repeat these steps for each subsequent Foundation Hub server that is included in the load-balanced configuration.

1. Stop the *BIOVIA Hub Server <version>* service on all previously installed and configured Foundation Hub servers.
2. Install BIOVIA Foundation Hub on the next server that you want to use in the load-balanced configuration.
3. Stop the *BIOVIA Hub Server <version>* service on the new Foundation Hub server.
4. Navigate to the `<hub_install>\conf` directory on your new Foundation Hub server machine and make a backup of the following files:
    - `app-config.groovy`
    - `tomcat.properties`
5. Navigate to the network shared folder and copy the following files to the location on your new Foundation Hub server that is equivalent to where they are stored on your primary Foundation Hub server:
    - `app-config.groovy`
    - `tomcat.properties`
6. Edit the `tomcat.properties` file on the new Foundation Hub server and change the `host` value to the fully qualified domain name for this Foundation Hub server.
7. Edit the `app-config.groovy` file on the new Foundation Hub server and change the URLs in `hubSelfRegistration` to the fully qualified domain names for this Foundation Hub server.
8. Copy the SSL certificate and the truststore JKS certificate file (if required) from the network shared folder to the same location on the new Foundation Hub server as where they are stored on the primary Foundation Hub server.
9. If you are using Kerberos authentication, copy the keytab file from the shared network folder to the same location on the new Foundation Hub server as where it is stored on the primary Foundation Hub server.
10. Start the *BIOVIA Hub Server <version>* service on this Foundation Hub server.
11. Open the Foundation Hub Configuration page as an administrator user:
    a. Open a browser and navigate to the Foundation Hub Landing Page (for example, `https://<hubserver1>:9953`).

    b. Click ⚙.

    c. Open **Settings > Hub Configuration**.

12. Click **Edit** and complete the **Web Server Configuration** fields as described in Configuring Foundation Hub on a Single Server.
    - **Reverse Proxy URLs:** The URL of the load balancer server that provides access to this Foundation Hub and its HTTP and HTTPS ports.
13. Set all the other **Web Server Configuration** fields to the same values as used on the primary Foundation Hub server.
14. Set all the **Database Configuration** fields to the same values as used on the primary Foundation Hub server.
15. Set all the **Certificate Configuration** and **Enable Kerberos Authentication** fields to the same values as used on the primary Foundation Hub server.
16. Click **Save** and then **Restart Server**. The service restarts and provisions the database schema.

Testing Load-Balanced Foundation Hub Servers

Once you have installed and configured the load-balanced Foundation Hub servers, you can test the configuration by checking the load balancer URL one node at a time:

1. Turn on the load balancer and all of the nodes.
2. Verify that you can access the load balancer URL without an error: `https://<host:port>/foundation/hub`.
3. Turn off all nodes except one.
4. Verify that you can still access the load balancer URL without an error: `https://<host:port>/foundation/hub`.
5. Turn off the node you verified and turn on another and repeat the test. Do this for the remaining nodes.

Changing from a Single Node to a Load-Balanced Installation

Follow these directions to change from a single-node installation to a load-balanced Foundation Hub installation:

1. Configure the load-balanced servers.
2. Open a browser and navigate to the Foundation Hub page: `https://<hubserver1>:9953`.
3. Go to **Admin and Settings > Settings > Hub Configuration** and click **Edit**.
4. Set **Reverse Proxy HTTP URL** and **Reverse Proxy HTTPS URL** to the load balancer URLs (with port numbers).
5. **Save** and **Restart**.
6. Navigate to the Pipeline Pilot Administration Portal: `https://<pp_server>:9943/admin`.
7. Go to **Security > Authentication**.
8. Change the **Foundation Server URL** to the load balancer URL.
9. Click **Save**.

Chapter 7:
Working with Certificates

BIOVIA Foundation Hub communicates with clients over HTTPS using Apache Tomcat 8 web server. Apache Tomcat supports Secure Sockets Layer (SSL) or Transport Layer Security (TLS) that provides both server authentication and message encryption to keep client communications secure.

To enable SSL or TLS, you must provide a keystore file containing a public and private key certificate pair. The certificates include the external IP address of your Foundation Hub server or load balancer.

IMPORTANT! You must renew and update your certificates before they expire or you will not be able to log in to Foundation Hub or any applications that rely on it for authentication. If you need to update or replace certificates, see Updating Certificates.

Certificate Requirements

- The certificate should be digitally signed by a recognized Certificate Authority (CA) such as your corporate IT department or a root authority such as Verisign.
- You must set the **Name** and **Issued To** properties of the certificate to the Fully Qualified Domain Name (FQDN) of the server machine.

Setting up a Trust Relationship for Outbound Traffic

You can set the truststore policy for outbound SSL connections from the Foundation Hub Application Settings page:

1. Navigate to **Admin and Settings > Settings > Applications > Application Settings > Foundation Hub**.
2. Choose the **Truststore**:
   - **Manual certificate management:** SSL certificates are validated and you can manually import self-signed certificates.
   - **Auto import certificates during setup:** SSL certificates are validated and self-signed or certificates from authentication providers such as LDAP or 3DPassport are imported automatically.
   - **Ignore invalid certificates:** Invalid SSL certificates are ignored and SSL connections are always successful (not secure).
3. Click **Save**.

Setting up a Trust Relationship for Inbound Traffic

You must perform these steps to enable secure communication between the Foundation Hub server and the application servers.

1. Obtain a certificate from a recognized signing authority (VeriSign for example) or enterprise IT. PKCS12 (`.pfx`) is a common format.
2. Import the private and public keys from the certificate into the Foundation Hub server keystore JKS file.

3. Configure Foundation Hub to point to the keystore JKS file. See Configuring Foundation Hub on a Single Server or Configuring Foundation Hub for Load Balancing.

Java Keytool Utility

Foundation Hub includes the Java keytool utility for working with certificates and Java keystore files. Pipeline Pilot also includes the openssl command-line utility that can convert various certificate formats. The full capabilities of these tools is beyond the scope of this document, but the following commands may be useful.

Common Java Keytool Commands

Access the keytool command in the JRE directory:

- `<hub_install>/jre/windows/bin/keytool.exe`
- `<hub_install>/jre/linux/bin/keytool`

Commands

Tip: Do not copy these commands directly from this document to the command prompt.

- Generate a Java keystore and key pair:

  ```
  keytool -genkey -alias [domain] -keyalg RSA -keystore keystore.jks -
  keysize 2048
  ```

- Generate a certificate-signing request (CSR) for an existing Java keystore. The CSR will is sent to a CA for counter-signature:

  ```
  keytool -certreq -alias [domain] -keystore keystore.jks -file [domain].csr
  ```

- Import a root or intermediate CA certificate to an existing Java keystore:

  ```
  keytool -import -trustcacerts -alias root -file [file].crt -keystore
  keystore.jks
  ```

- Import a signed primary certificate to an existing Java keystore:

  ```
  keytool -import -trustcacerts -alias [domain] -file [domain].crt -keystore
  keystore.jks
  ```

- Generating a keystore and self-signed certificate (for development use only) requires several steps.

  Use openssl to generate an RSA private key and a certificate signing request:

  ```
  openssl genrsa -des3 -out hub_SSLcertificate.key 1024
  openssl req -new -key hub_SSLcertificate.key -out hub_SSLcertificate.csr
  ```

  Remove the passphrase from the key:

  ```
  cp hub_SSLcertificate.key hub_SSLcertificate.key.org
  openssl rsa -in hub_SSLcertificate.key.org -out hub_SSLcertificate.key
  ```

  Generate a self-signed certificate:

  ```
  openssl x509 -req -days 365 -in hub_SSLcertificate.csr -signkey hub_
  SSLcertificate.key -out hub_SSLcertificate.crt
  ```

  Import the key and certificate:

  ```
  keytool -importkeystore -destkeystore hub_SSLOutkey.jks -srckeystore hub_
  SSLcertificate.p12 -srcstoretype pkcs12
  ```

- Check the contents of a PKCS12 PFX file:

```
keytool -list -v -keystore [file].pfx -storetype PKCS12 -storepass [pass]
```

Additional Resources

- Overview for configuring SSL or TLS: https://tomcat.apache.org23/tomcat-8.0-doc/index.html

  Portecle (application for creating, managing and examining keystores, keys, and certificates): http://portecle.sourceforge.net
- KeyStore Explorer (graphical interface for working with keytool commands): http://keystore-explorer.sourceforge.net
- Common keytool commands: https://www.sslshopper.com/article-most-common-java-keytool-keystore-commands.html

Updating Certificates

Follow these steps if you need to update or replace your certificate on a Foundation Hub server.

> **Note:** The new or updated certificate will have new properties such as thumbprint. So you must recreate the keystore file in Foundation Hub.

> **IMPORTANT!** You must renew and update your certificates before they expire or you will not be able to log in to Foundation Hub or any applications that rely on it for authentication.

These steps are also applicable if a certificate is replaced on the server (such as, replace a self-signed certificate with a certificate from a Trusted Certificate Authority, or if the name of the server or company changes, which prompts a new certificate.

1. Create the keystore file for the new certificate. See Chapter 7: Working with Certificates.
2. Stop the *BIOVIA Hub Server <version>* service. See Chapter 9: Managing the Foundation Hub Service . If you are updating certificates in a load-balanced environment, stop all services.
3. Navigate to the Foundation Hub configuration directory. For example:

   `<hub_install>\Hub*conf*\"`
4. Make a copy of `tomcat.properties` and edit the original file as follows:
   a. Update the path to the new keystore file.
   b. Replace the encrypted password string with the actual password.
   c. Delete the filename referenced by `truststore.path` and delete the `truststore.password` value:

   ```
   truststore.path=
   truststore.password=
   ```

   d. Save the file.
5. Start the *BIOVIA Hub Server <version>* service. See Chapter 9: Managing the Foundation Hub Service .
6. Log in to the BIOVIA Landing Page as an Administrator user.
7. Open **Applications > Admin and Settings > Settings > Hub Configuration**.
8. Enter the password in the keystore field. If necessary, update the path for the new keystore file.

9. Save the configuration and restart the server when prompted. Restarting will encrypt the password in the `tomcat.properties` file. Restarting without saving does not encrypt the password in this file.
10. After the restart, the BIOVIA Landing Page is displayed again. Log out and log in again as an Administrator user.

    There should not be any certificate errors.
11. Click the lock icon in the browser's URL and select the option to view the certificate. It should show the updated certificate.
12. Repeat steps 3-10 for each server if you are using Foundation Hub in a load-balanced configuration.

Chapter 8:
Post-Installation Steps

When you have completed the initial installation of Foundation Hub, perform the following steps.

Set Up User Authentication

Configure user authentication using LDAP, SPNEGO/Kerberos, or 3DPassport. See Setting Up User Authentication.

Install Pipeline Pilot and the Remaining Applications

1. Install Pipeline Pilot and set Foundation as the external user directory on the **Security > Authentication** page of the Pipeline Pilot Admin Portal.

   See the *Pipeline Pilot Installation Guide* and *Pipeline Pilot Administration Guide*.
2. For Foundation Hub 2021 HF1, install the separate *FoundationSSO* package on the Pipeline Pilot server. This package contains Pipeline Pilot components and protocols required for Foundation Hub 2021 HF1. For details about installing the FoundationSSO package, see Installing the FoundationSSO Package for Pipeline Pilot.
3. Install the remaining BIOVIA applications.
4. Update the registered applications in Pipeline Pilot. On the **Reports > Foundation Applications** page of the Pipeline Pilot Admin Portal, click **Update Applications**.

   > **Note:** Internet Explorer caches some Pipeline Pilot Server Administration Portal pages. If **Update Applications** is not available, refresh the page.
5. Check the registered applications in Foundation Hub. Open **Admin and Settings > Settings > Applications**.

Installing the FoundationSSO Package for Pipeline Pilot

After installing or upgrading Pipeline Pilot for use with Foundation Hub, install the separate *FoundationSSO* package on the Pipeline Pilot server. This package includes components and protocols required for Foundation Hub 2021 HF1 and associated applications.

> **Note:** In a load-balanced environment, install the package on each Pipeline Pilot server.

Windows

1. Obtain the zipped installer for your operating system: `BIOVIA_<version>.BIOVIAFoundationSSO<version>_Win64.zip`
2. Extract the zipped installer on the machine where you have installed or updated Pipeline Pilot.
3. In the extracted folder, double-click `\bin\scitegicsetup.exe` to run the installer. Follow the installer windows:
   a. **Verified and Ready:** This dialog appears when a compatible version is found. Click **Add/Remove Products**.

b. **Confirm Your License:**

- If you installed or upgraded Pipeline Pilot with a valid license, the dialog indicates **The existing license is valid**. Click **Next**.
- If the installer does not find a valid license, click **Browse** and navigate to a Pipeline Pilot license that enables you to use the FoundationSSO package. Click **Next**.

c. **Select product(s) to install:** The FoundationSSO package includes items to be installed in **Pipeline Pilot Core** and the **Pipeline Pilot Compose Collection**. Keep these items selected. It is recommended that you **Back up the XMLDB**.

d. **Running Applications:** If the Pipeline Pilot services are running, you will be prompted to stop them. Click **Stop Services**.

e. **Assign Ports for Apache Web Server:** Keep the HTTP and HTTPS ports as defined when you installed or upgraded Pipeline Pilot.

f. **Confirm Your Add/Remove:** Click **Next**.

g. **Confirm Apache Login:** Click **Next**.

h. **Completed:** Click **Finish**.

Linux

1. Obtain the installer archive for your operating system: `BIOVIA_<version>.BIOVIAFoundationSSO<version>_Linux64.tgz`
2. Extract the installer archive on the machine where you have installed or updated Pipeline Pilot:

   ```
   tar -xpvzf BIOVIA_<version>.BIOVIAFoundationSSO<version>_Linux64.tgz
   ```

3. In the extracted folder, run `sciinstall` as the non-root user that owns the Pipeline Pilot directory tree (Apache).

   ```
   .\sciinstall
   ```

4. When a message informs you that the operating system is supported, enter **y** to continue.
5. When prompted to **Enter the target directory for the server installation**, enter the directory where your Pipeline Pilot server is installed. This is the `<pps_install>` directory referenced in the Pipeline Pilot Installation Guide.
6. Confirm the path for your existing server installation.
7. You will be prompted regarding your license file. If the license file is valid, press **Enter** to continue. The server will be stopped.
8. Verify that there are items to be installed in **Pipeline Pilot Core** and the **Pipeline Pilot Compose Collection** is listed to be installed. Press **Enter** to continue the installation.
9. At the end of the installation, when prompted to start the Pipeline Pilot server service, press **Enter**.

Setting Up User Authentication

You can configure user authentication using LDAP, SPNEGO/Kerberos, or 3DPassport.

- For SPNEGO/Kerberos authentication, see Configuring SPNEGO/Kerberos Authentication.
- For LDAP authentication, configure one or more User Directories. See Adding LDAP User Directories.
- 3DPassport is Dassault Systèmes' user authentication server. To set up 3DPassport authentication, see Setting Up User Authentication with 3DPassport.

IMPORTANT! After setting up user authentication, change the password for the scitegicadmin user.

> **Note:** Foundation Hub does not enforce unique usernames for multiple domains. If a user is not able to sign in, he or she may be using a username that is duplicated in a different domain. Ask the user to sign in while specifying the domain name. For example `<domain>\username`.

Adding LDAP User Directories

> **Note:** Lightweight active directories where the service is not connected directly to the domain controller such as Active Directory Application Mode (ADAM)/Active Directory Lightweight Directory Services (AD LDS) are not supported.

1. Navigate to the Foundation Hub Landing Page, for example:
   `https://<hubserver>:9953/foundation/hub`
2. Click ⚙.
3. Open **Settings > User Directories**.
4. Click the **Add User Directory** (plus) icon.
5. Complete the **User Directory** information:
   - **Name:** Add the name of the user directory.
   - **User Directory is active:** Choose whether this directory is being used currently for user authentication.
   - **Authentication Order:** If there are multiple user directories defined, this field determines the order used to evaluate credentials when no domain is provided during sign in. Lower values take higher precedence.

     The servers can be unrelated or they can be different sub-domains of a root domain. They should not be a list of replicated LDAP servers that have the same user base. When a user directory authenticates a user, the user entry in Foundation Hub is distinct for that user, so in the case where the same user name exists in multiple directories, they are treated as distinct users in Foundation Hub.
   - **Update User Account Data on Sign In:** If there have been changes to the user's account data in the User Directory (first name, last name, full name, email address, etc.), update the user's account when they sign in. See Authentication Settings Matrix for details about how authentication settings affect sign in for different scenarios.

     > **Note:** This setting is affected by **Admin and Settings > Applications > Application Settings > Foundation Hub > Security > Update User Account Data on Sign In**.
6. Complete the **Server Configuration** information:
   - **Server:** Add the full server name for the LDAP server. Use **Find LDAP Server** to find an LDAP server on the network. The address should begin with `ldap://` or `ldaps://`. We recommend that you use the LDAPS URL to secure communication between Foundation Hub and the LDAP server.
   - **Search Base:** Search base from which to authenticate users. This must be a base distinguished name. See Performance Considerations.
   - **Principal** and **Principal Password:** Include the name of the principal account that will be used to look up users. This must be a distinguished name for a user that has rights to authenticate with and read from the user directory.
   - **User Directory Type:** ActiveDirectory by default. GenericLDAP is also supported.

- **User Object Classes:** Comma separated list of attribute values of LDAP objectClass field. This is primarily used to determine if the object is a user (for example, `user,person`).
- **Follow Referrals:** See Performance Considerations.
- **Kerberos Integration:** Choose this if you are using SPNEGO or Kerberos. See Configuring SPNEGO/Kerberos Authentication.

7. Check the **Attribute Mappings** information. These map directory attribute data to Foundation Hub attributes. The default values are based on the **User Directory Type** that you have chosen for the user directory:
   - Username
   - Email
   - External Id
   - Full Name
   - First Name
   - Last Name
   - Group Attribute

   > **Tip:** The settings in the **Attribute Mappings** have a significant impact on the day-to-day use of BIOVIA applications. Use an LDAP tool like Softera or JXplorer to inspect user attributes in your directory before completing this section.

8. Click **Test Connection**. If the connection test is successful, click OK.
9. Configure **Permitted Groups** and **Custom Query Filter** if desired. See Permitted Groups and Custom Query Filter.
10. If you are configuring a load-balanced environment, restart the Foundation Hub server by navigating to **Settings > Hub Configuration** and clicking **Restart Server**.
11. Set up a synchronization schedule and synchronize the user data for the user directory. See Synchronizing LDAP Users.

Permitted Groups and Custom Query Filter

The Permitted Groups and Custom Query Filter fields are only available by opening and editing a user directory that you have created.

1. Open **Admin and Settings > Settings > User Directories**.
2. Click the user directory you just created to open it.
3. Click **Edit** and edit the following fields as desired:
   - **Permitted Groups:** List of fully qualified LDAP groups. The Field will search for entered group names within the previously defined Search Base. Users that are a member of ANY of the defined groups will be part of the user synchronization. The filter will be constructed based on the defined value of the Group Attribute in the User Dirctory. For example:

     ```
     CN=Admins,OU=Groups,OU=OrganizationalUnit1,DC=example,DC=org
     CN=PowerUsers,OU=Groups,OU=OrganizationalUnit1,DC=example,DC=org
     (Group Attribute = memberOf)
     ```

   - **Custom Query Filter:** Additional query that allows you to define a filter without predefined attribute mapping. For example: `(&(!objectClass=computer)(employeeID=*))`.
4. Click **Save**.

Example Filter

You can use the **User Object Classes**, **Permitted Groups**, and **Custom Query** filter fields to filter the results when synchronizing users. In these instructions, the following were provided as examples:

- **User Object Classes:**`user,person`
- **Permitted Groups:**

  ```
  CN=Admins,OU=Groups,OU=OrganizationalUnit1,DC=example,DC=org
  CN=PowerUsers,OU=Groups,OU=OrganizationalUnit1,DC=example,DC=org
  (Group Attribute = memberOf)
  ```

- **Custom Query Filter:** `(&(!objectClass=computer)(employeeID=*))`.

These settings result in the following filter:

```
(&(sAMAccountName=*)(&(objectClass=user)(objectClass=person))
(|(memberOf=CN=Admins,OU=Groups,OU=OrganizationalUnit1,DC=example,DC=org)
(memberOf=CN=PowerUsers,OU=Groups,OU=OrganizationalUnit1,DC=example,DC=org))
(&(!objectClass=computer)
(employeeID=*)))
```

Performance Considerations

How you choose to configure your User Directories could have an impact on the performance of authentication requests and user synchronization. Consider the following when setting up user directories to improve performance:

- Restrict your search base to the deepest point in the directory tree that contains all of the users you want instead of targeting it at the root. Depending on where the majority of your users reside in the directory, you may want to consider setting up more than one user directory, each targeted at a different search base beneath your root. When a user authenticates, the directory must be searched in order to lookup the user. Narrowing the search bases can drastically reduce the amount of time it takes to find the user in the directory. A single directory targeted at a search base potentially containing thousands more users increases the time it takes to find the user.
- Set **User Object Classes** to filter out Groups, Computers, or other arbitrary non-user entries (for example, `user,person`).
- Avoid using **Follow Referrals**. When resolving referrals, transparent connections are created to other servers. Each of the referred servers is searched by root.

Synchronizing LDAP Users

You must create the user directory and then edit it to set up a user synchronization schedule.

Note: Applications > Application Settings > Foundation Hub > Allow Automatic User Provisioning must be enabled in order for the synchronization to be able to add new user accounts.

Setting the Synchronization Schedule

1. Open **Admin and Settings > Settings > User Directories**.
2. Click the user directory you just created to open it.
3. Click **Edit**.
4. Choose whether to **Enable User Synchronization on Schedule**.

5. Set the **Schedule**:
   - **Days of the Week**: Choose which days of the week to synchronize.
   - **Hours:** Specify which hours of the day to synchronize. The time should be whole numbers based on a 24-hour clock. Enter a comma-delimited list to specify multiple hours. For example, `2, 14` would schedule a synchronization for 2 AM and 2 PM.
   - **Minutes Past Hour:** Specify the minutes past the hour you want to run the synchronization. Keep this set to 0 to schedule it to run at the beginning of the hours specified. Use a comma-delimited list to specify multiple runs per hour.
6. Choose **Delete Missing Users** to delete users that are in the Foundation Hub database, but no longer in the external user directory.
7. Set the **Page Size** to the batch size of users to synchronize per request. See your user directory help to view the request limit.
8. Click **Save**.
9. Manually synchronize the users for the first time.

Manually Synchronizing the Users

Once you have set the synchronization schedule, you can manually synchronize for the first time and any time thereafter as needed. Note that the **Synchronize Users Now** button is not exposed until you have set the synchronization schedule.

1. Open **Admin and Settings > Settings > User Directories**.
2. Click the user directory you just created to open it.
3. In User Synchronization, click **Synchronize Users Now**.

Configuring SPNEGO/Kerberos Authentication

If you are planning to authenticate with SPNEGO/Kerberos, review these instructions before configuring Foundation Hub.

Support

- SPNEGO/Kerberos is supported for Foundation Hub installed on Windows.
- SPNEGO/Kerberos is only supported for Windows Active Directory.

Prerequisites

You will need to gather the following if you need to set up SPNEGO/Kerberos authentication for Foundation Hub:

1. Obtain a Kerberos key tab file and copy it to the local disk of the Foundation Hub server.
2. Obtain the name of the Service Principal which includes the service type prefix (for example, HTTP/) and the server's fully qualified domain name (for example, `HTTP/<server FQDN>`). Consider setting up your own Active Directory environment to work with Hub Kerberos Authentication.
3. Obtain the name of the Kerberos realm. This is usually the server domain in upper-case.

Setup

1. Configure the Foundation Hub and choose to **Enable Kerberos Authentication**. You will need to provide **Service Principal**, **Realm Name**, and **Key Tab Location**. See Configuring Foundation Hub on a Single Server or Configuring Foundation Hub for Load Balancing.

2. Set up one or more User Directories and enable Kerberos Integration. See Adding LDAP User Directories.
3. When finished, if you are configuring a load-balanced environment, restart the Foundation Hub server by navigating to **Settings > Hub Configuration** and clicking **Restart Server**.
4. Configure the browsers. See Configuring Browsers for SPNEGO/Kerberos.

Configuring Browsers for SPNEGO/Kerberos

Firefox

1. Type `about:config` in the address field.
2. In filter/search, type `negotiate`.
3. Set `network.negotiate-auth.trusted-uris` to the full server address. Use https for all communication (recommended).

Internet Explorer

Open **Tools > Internet Options > Security tab** and add the Foundation Hub server to the list in **Local intranet**.

Chrome

- **Windows:** Open **Tools > Internet Options > Security tab** and add the Foundation Hub server to the **Local intranet** list.
- **Linux:**
  - Use the following command-line parameters:

    ```
    --auth-server-whitelist="*.example.com"
    --auth-negotiate-delegate-whitelist="*.example.com"
    ```

  - Use https for all communication (recommended).
  - Type the following to check the policy: `//policy/`

Using Chrome Policy Files (Linux Only)

You can configure Chrome on Linux to read JSON format policy files from the following directory: `/etc/opt/chrome/policies/managed`

```
{
       "AuthServerWhitelist" : "*.example.org",
       "AuthNegotiateDelegateWhitelist" : "*.example.org",
       "DisableAuthNegotiateCnameLookup" : true,
       "EnableAuthNegotiatePort" : true
}
```

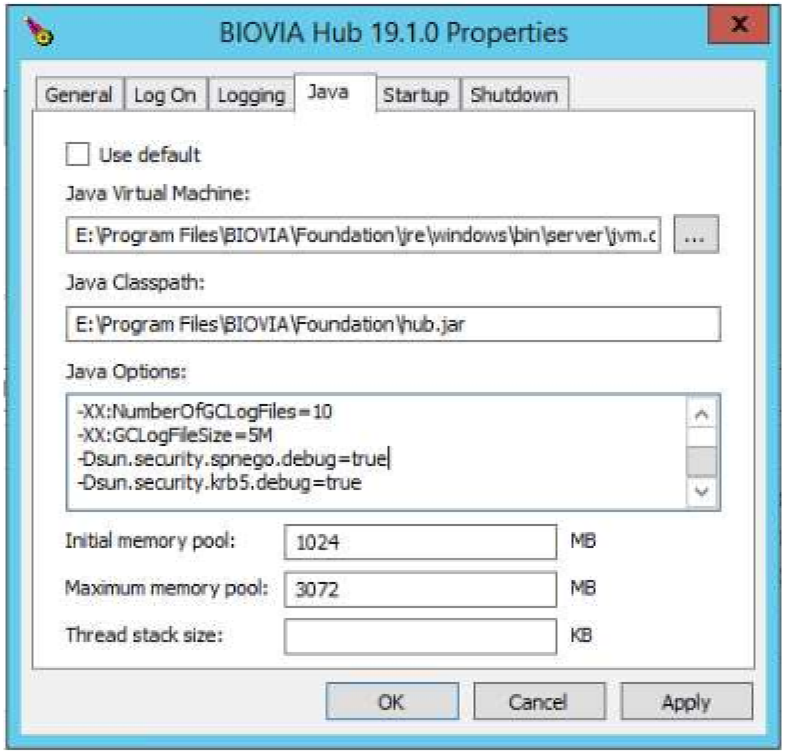
Troubleshooting SPNEGO/Kerberos Setup

You can start investigating issues you are having by turning on the JVM debug options.

Set the Java Virtual Machine Debug Options

1. Start the service manager: `<hub_install>\bin\manage.bat`
2. In the **Java** tab, set the following **Java Options**:

   ```
   -Dsun.security.spnego.debug=true
   -Dsun.security.krb5.debug=true
   ```



☐ Use default

Java Virtual Machine: E:\Program Files\BIOVIA\Foundation\jre\windows\bin\server\jvm.c

Java Classpath: E:\Program Files\BIOVIA\Foundation\hub.jar

Java Options:

```
-XX:NumberOfGCLogFiles=10
-XX:GCLogFileSize=5M
-Dsun.security.spnego.debug=true
-Dsun.security.krb5.debug=true
```

Initial memory pool: 1024 MB

Maximum memory pool: 3072 MB

Thread stack size: KB

3. Restart the Foundation Hub server:
   a. Open **Settings > Hub Configuration**.
   b. Click **Restart Server**.
4. Review `<hub_install>\logs\stdout`.

Error Messages:

LDAP User Search Failure

If you notice LDAP failures in the log file, check your User Directory configuration. You may not be in the same user directory's domain scope.

Check the KeyTab File

The following Java command shows the keytab file entry.

> **Note:** The Principal must exactly match with your Principal Name + "@" + Realm Name of your Foundation Hub configuration (they are case-sensitive).

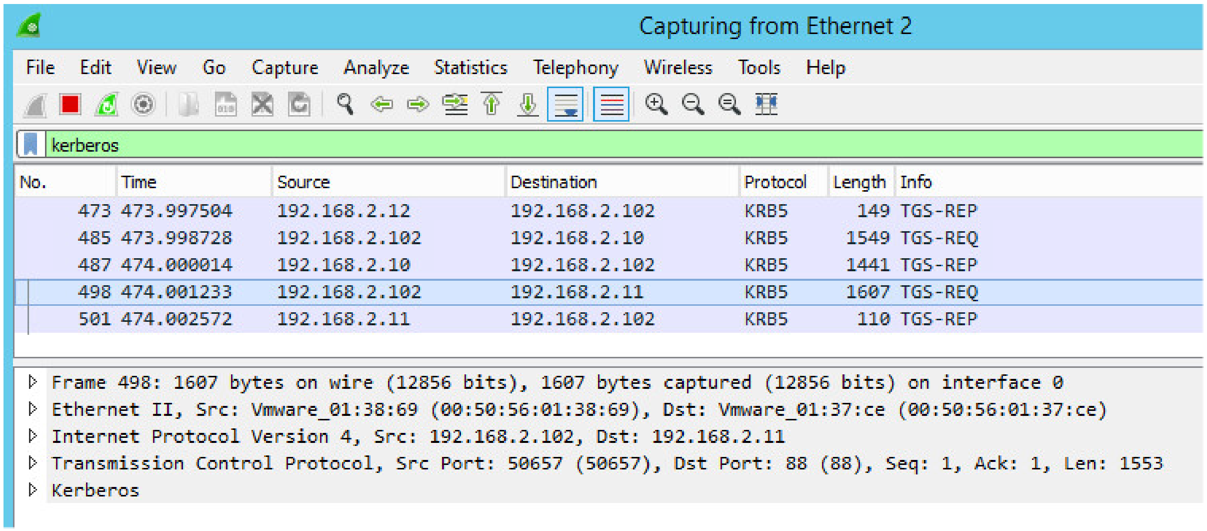
```
% <Java home>\bin\ktab -k <keytab path> -l -e -t

Keytab name: <keytab path>
KVNO Timestamp Principal
---- --------------- ------------------------------------------------------------------------
12 12/31/69 4:00 PM HTTP/server1.west.biovia.com@WEST.BIOVIA.COM (1:DES CBC mode with CRC-32)
12 12/31/69 4:00 PM HTTP/server1.west.biovia.com@WEST.BIOVIA.COM (3:DES CBC mode with MD5)
12 12/31/69 4:00 PM HTTP/server1.west.biovia.com@WEST.BIOVIA.COM (23:RC4 with HMAC)
12 12/31/69 4:00 PM HTTP/server1.west.biovia.com@WEST.BIOVIA.COM (18:AES256 CTS mode with HMAC
SHA1-96)
12 12/31/69 4:00 PM HTTP/server1.west.biovia.com@WEST.BIOVIA.COM (17:AES128 CTS mode with HMAC
SHA1-96)
```

Browser URL Mismatch

The hostname part of your Service Principal must exactly match your Browser's URL.

Sniff Network Packets

Use a network sniffer such as Wireshark on the client machine that you use for your browser to diagnose issues with packets.



kerberos

No.	Time	Source	Destination	Protocol	Length	Info
473	473.997504	192.168.2.12	192.168.2.102	KRB5	149	TGS-REP
485	473.998728	192.168.2.102	192.168.2.10	KRB5	1549	TGS-REQ
487	474.000014	192.168.2.10	192.168.2.102	KRB5	1441	TGS-REP
498	474.001233	192.168.2.102	192.168.2.11	KRB5	1607	TGS-REQ
501	474.002572	192.168.2.11	192.168.2.102	KRB5	110	TGS-REP

```
▷ Frame 498: 1607 bytes on wire (12856 bits), 1607 bytes captured (12856 bits) on interface 0
▷ Ethernet II, Src: Vmware_01:38:69 (00:50:56:01:38:69), Dst: Vmware_01:37:ce (00:50:56:01:37:ce)
▷ Internet Protocol Version 4, Src: 192.168.2.102, Dst: 192.168.2.11
▷ Transmission Control Protocol, Src Port: 50657 (50657), Dst Port: 88 (88), Seq: 1, Ack: 1, Len: 1553
▷ Kerberos
```

Strange Hub Service Account Name

This error can occur if there is a mismatch between the Domain userPrincipalName and the user logon name for the Foundation Hub Service. Using the SetSPN command can overwrite the Domain userPrincipleName, creating the mismatch. Ensure that the user login name is correct.

To ensure that the user logon name is correct:

1. From the Windows Services console, right-click BIOVIA Hub Server *<version>* and click **Properties**.
2. Under the **Account** tab, ensure that the **User logon name** matches with the Domain **userPrincipleName**. If there is a mismatch, request your IT department to fix this attribute.

Setting Up User Authentication with 3DPassport

3DPassport is Dassault Systèmes' user authentication server for the 3DS Platform. Setting up Foundation Hub for 3DPassport Authentication delegates the authentication to a 3DPassport server. Roles, Groups, and Permissions for BIOVIA applications are still managed in Foundation Hub. Local Foundation Hub users (for example, scitegicadmin) cannot authenticate with 3DPassport. It is therefore recommended to assign the Hub System Administrator and Security Manager Role to a user account able to sign in using 3DPassport. During the sign in, 3DPassport and Foundation Hub exchange user information and session data which requires a SSL trust relation between the servers both ways.

Configuring Foundation Hub to use 3DPassport Authentication

Set Foundation Hub to authenticate users using 3DPassport from the Hub Configuration Page. If you did not set Foundation Hub to use 3DPassport during the configuration steps, do the following:

1. Navigate to **Admin and Settings > Settings > Hub Configuration**.
2. Click **Edit**.
3. In the **Authentication Provider** fields, set **Authentication** to **Passport**.
4. Set **Server Url** to point to the 3DPassport server.

5. Choose whether to use the **Primary Authenticator** option:
   - If you choose the **Primary Authenticator** option, users are directed to the 3DPassport sign in dialog box.
   - If you leave **Primary Authenticator** unselected, users are directed to a sign in dialog box with an option to authenticate using Foundation Hub or 3DPassport.
6. Click **Save** and then **Restart Server**.

Configuring a 3DPassport user with Foundation Hub Admin Privileges

1. Check if you can sign in to Foundation Hub using 3DPassport user credentials. Navigate to:
   ```
   https://<hub server>:9943/foundation/hub
   ```
2. Sign in with your 3DPassport account.
   - If login fails, auto-provisioning is turned off. You must create the user manually in Foundation Hub as described later.
   - If login is successful, you are redirected back to the BIOVIA Landing Page. Click the **Applications** icon and choose **Admin and Settings** to check if your account has admin privileges (existing domain users). If you see the error "This account is not authorized...", you will need to configure the 3DPassport credentials with admin privileges.
3. To create the user or assign admin privileges:
   a. Use the following URL for local Foundation Hub authentication and sign in using the default scitegicadmin/scitegic credentials.
      ```
      https://<hub server>:9953/foundation/hub/security/auth?local=true
      ```
   b. If the 3DPassport user does not exist, create it in Foundation Hub from **Admin and Settings > Security > Users**.
   c. Navigate to **Admin and Settings > Security > Roles** and add your 3DPassport user to the **Hub System Administrator** and **Security Manager** roles.
   d. Log out and then sign in to Foundation Hub normally using your 3DPassport credentials that you added to the Hub System Administrator and Security Manager roles. Check that you can now access the Admin and Settings area.

SSL Certificate for 3DPassport

The 3DPassport server and the Foundation Hub server must have a trust relationship set up between them. Include the SSL certificate for the Foundation Hub server in the 3DPassport server's Truststore, and include the SSL certificate for the 3DPassport server in the Foundation Hub server's Truststore.

- **Foundation Hub truststore:** From Foundation Hub **Admin and Settings**, set **Settings > Applications > Application Settings > Foundation Hub > SSL Truststore Policy** to **Auto import certificates during setup** to automatically import the 3DPassport server certificate to the Foundation Hub truststore. See Working with Certificatesto import it manually.
- **3DPassport truststore:** See the 3DPassport server documentation.

Authentication Settings Matrix

The following table describes the expected results of a sign in attempt based on these authentication settings and whether the directory administrator has moved the user to a different domain. Note that these results are the same regardless of whether the user signs in with just their username or signs in to a specific domain in the format DOMAIN/Username.

- **Allow Automatic User Provisioning:** Determines whether authenticated users are automatically added from the IP. This option is available in **Admin and Settings > Settings > Applications > Application Settings > Foundation Hub**.
- **Update User Account Data on Sign In:** Determines whether users are updated at sign in with the user information provided by the authentication provider (LDAP or 3D Passport). This option is available in **Admin and Settings > Settings > Applications > Application Settings > Foundation Hub**.
- **New Domain in Same User Directory:** Determines whether the user directory administrator has moved the user to a different domain within that directory.

Allow Automatic User Provisioning	Update User Account Data on Sign In	New Domain in Same User Directory	Result	Details
Off	Off	Yes	Sign in fails	Authorization succeeds but the domain name in the user record cannot be matched or updated.
Off	On	Yes	Sign in succeeds	Authorization succeeds and the user record is updated with the new domain value.
Off	Off	No	Sign in fails	Authorization succeeds but cannot match the user record to the domain.
Off	On	No	Sign in fails	Authorization succeeds but cannot update the account to the new user directory.
On	Off	Yes	Sign in fails	Authorization succeeds but cannot match or update the domain name in the user record.
On	On	Yes	Sign in succeeds	Authorization succeeds and user record is updated with the new domain value.
On	Off	No	A new account is created	Auto-provision creates a new account because the username does not match an existing user record in the new User Directory in Foundation Hub.
On	On	No	A new account is created	Auto-provision creates a new account is because the username does not match an existing user record in the new user directory in Foundation Hub.

Change the Default Password

After completing the Foundation Hub installation, BIOVIA recommends you locate the user *scitegicadmin* and change its password. You should also create an Administrator account separate from the default *scitegicadmin* account.

1. In Foundation Hub, navigate to **Applications > Application Settings > Users**.
2. Click **scitegicadmin**.
3. Click **Edit**.
4. In the **Password** field, type a new password.
5. Click **Save**.

Deploying in a Regulated Environment

If you are deploying in a regulated environment (for example, GxP), you may want to turn off the **Allow Automatic User Provisioning** option in the Foundation Hub Settings. This option, which is turned on by default, automatically adds authenticated users from configured user directories.

1. From the Foundation Hub navigate to **Applications > Application Settings > Foundation Hub**.
2. Click **Edit**.
3. Set **Allow Automatic User Provisioning** to **No**.

> **Note:** You will not be able to use the scheduled synchronization feature when **Allow Automatic User Provisioning** is set to **No**.

Installing and Upgrading BIOVIA CDS Client Add-ins

BIOVIA provides add-ins for the Empower and Chromeleon Chromatography Data System (CDS) clients.

The BIOVIA add-ins enable the CDS clients to export results to the Foundation Hub measurement store so that Foundation Hub users can execute data acquisition tasks that require the CDS results. They also enable the CDS clients to import Foundation Hub samples and standards for populating their native sample set methods and sequences.

Install the BIOVIA CDS add-ins as described in this section, and then configure equipment that uses them as described in the *Foundation Hub Equipment Guide*, which is available in the zipped documentation file.

License Requirements

To use the BIOVIA CDS add-ins, you must have the following licenses:

- Empower or Chromeleon license

  > **IMPORTANT!** An SDK Runtime license is required for each Chromeleon account that will use the BIOVIA Chromeleon add-in. Use the Chromeleon Administration Console to ensure that **SDK Runtime** is listed under **License Manager > License Overview > Client Licenses**. The BIOVIA menu items for using CDS data are disabled if this license is missing.

- BIOVIA Empower client add-in or BIOVIA Chromeleon client add-in license.
- Foundation Hub license.
- Foundation Hub Equipment license.

For version requirements, see the *Foundation Hub System Requirements*.

Required Permissions

The following permissions are required to use the CDS add-in import and export functionality:

- To import data from Foundation Hub to CDS:
  - Sequences > Copy Sequence
  - Sequences > Modify Sequence
  - Sequences > Manage Sequence Variables
  - Injections > Modify Finished Or Interrupted Injections
  - Injections > Add New Injections
- To export data from CDS to Foundation Hub:
  - Electronic Report > Export Electronic Report

Installing a New Instance of the Chromeleon Client Add-in

1. Obtain the Chromeleon add-in installer, `ChromeleonClientAddin.exe`.
2. Copy the installer to the Chromeleon client machine.
3. On the client machine, right-click `ChromeleonClientAddin.exe` and select **Run as Administrator**.
4. When prompted, identify which Foundation Hub server to use and provide the Foundation Hub administrator credentials.
5. After installation completes, open Foundation Hub **Admin and Settings > Equipment Adapters** and ensure that the Chromeleon adapter is listed.
6. Configure and test equipment for Chromeleon in Foundation Hub. See the *Foundation Hub Equipment Guide*.

Adding Multiple Foundation Hub Servers for Chromeleon

1. Locate the Chromeleon `Addins` directory. By default it is located here: `C:\Program Files (x86)\Thermo\Chromeleon\bin\AddIns`.
2. Make a copy of the `BIOVIA.Chromeleon.Addin` folder and rename it by including a suffix of the name of the server to connect to. For example, `BIOVIA.Chromeleon.Addin - dev.example.com`.
3. Open a command shell and navigate to the new folder.
4. Delete `registration.json`.
5. Run the following command:

   ```
   .\register.exe https://<dev.example.com:port>
   https://<dev.example.com:port> <user name> <password>
   ```

   This generates a new `registration.json` file.
6. Open `BIOVIA.Chromeleon.Addin.addin` in an XML editor.
7. Change the `/Addin/Header/Id` element to a unique value. For example, `BIOVIA.Chromeleon.Addin.1`.
8. Change both `Addin/Extension/InProcessCommand@name` attributes to a value that identifies the server to connect to. For example, `BIOVIA - Get Samples from ONE Lab [dev.example.com]`.

Installing a New Instance of the Empower Client Add-in

1. Obtain the Empower add-in installer `EmpowerClientAddin.exe`.
2. Copy the installer to the Empower client machine.
3. From there, run `EmpowerClientAddin.exe` as Administrator.
4. When prompted, specify the Foundation Hub server to be used and the Foundation Hub administrator credentials.
5. Verify the installation. From the Foundation Hub server, open **Admin and Settings > Equipment Adapters** and check that the Empower adapter is listed.
6. Configure equipment for Empower in Foundation Hub. See the *Foundation Hub Equipment Guide*.

Adding Multiple Foundation Hub Servers for Empower

1. Locate the Empower Add-in installation directory by using the following command:

   ```
   wmic product get installlocation,name | find "BIOVIA Empower Client Add-in"
   ```

2. Make a copy of the folder and rename it by including a suffix of the name of the server to connect to. For example:

   ```
   Empower Addin - dev.example.com
   ```

3. Open a command shell in the new folder.
4. Delete the `registration.json` file in the new folder.
5. Execute `register.exe` in the new folder with the correct arguments. For example:

   ```
   .\register.exe https://dev.example.com:9953 https://dev.example.com:9953
   hubadmin password
   ```

   This generates a new `registration.json` file.

6. Run `regedit.exe` to open the Windows Registry Editor.
7. Navigate to the following key folder: **HKEY_LOCAL_MACHINE > SOFTWARE > Wow6432Node > Waters > Empower > Toolkit > CustomPrograms**.
8. Right-click **ProjectWindow** and choose **Modify**.
9. Add a new value of type `String`:
   - Set **name** to `Program<n>` where <n> is the next number in the sequence. For example, If the highest value name is `Program2`, the name should be `Program3`.
   - Set **data** to:

     ```
     "Send to Measurement Store - <server>"
     "<path>\Biovia.Empower.ResultsExtractor.exe" /v:%v /u:%u /x:%x /p:%p
     /t:%t /r /t:%t
     ```

     where:

     - <path> is the path to the copied folder.
     - `<server>` is the name of the server to connect to.

       For example, if you copied the `Empower Addin` folder into `e:\apps\biovia\Empower Addin - dev.example.com`, and the server is `dev.example.com`, then the value data in the Windows Registry should be:

```
"Send to Measurement Store - dev.example.com"
"e:\apps\biovia\Empower Addin -
dev.example.com\Biovia.Empower.ResultsExtractor.exe" /v:%v /u:%u
/x:%x /p:%p /t:%t /r /t:%t
```

10. Repeat the previous step with the following exceptions:
    - Specify the path to `BIOVIA.Samples.exe` instead of `Biovia.Empower.ResultsExtractor.exe`.
    - Specify `Get Samples from ONE Lab` instead of `Send to Measurement Store`.

    For example:

    ```
    "Get Samples from ONE Lab - dev.example.com" "e:\apps\biovia\Empower
    Addin - dev.example.com\BIOVIA.Samples.exe" /v:%v /u:%u /x:%x /p:%p /t:%t
    ```

Upgrading the Chromeleon and Empower Client Add-ins

Tip: Be sure to notify users that the client machine will be down during the upgrade. Note that upgrading the Chromeleon and Empower client add-ins will not affect the CDS server.

1. Use the Windows Programs and Features control panel to uninstall the old version of the CDS add-in.
2. Install the new CDS add-in. See Installing a New Instance of the Chromeleon Client Add-in and Installing a New Instance of the Empower Client Add-in.
3. Test the new version of the CDS add-in.

Configure Site Data and Equipment in Foundation Hub

Use the **Foundation Hub Admin and Settings** area to configure additional data including locations and laboratory equipment. For details about further configuration and managing equipment, see the *Foundation Hub Equipment Guide*, which is available in the zipped documentation file.

Chapter 9: Managing the Foundation Hub Service

You can manage the Foundation Hub service by using the Windows Services console or Foundation Hub command-line tools.

Windows Services Console

You can use the Windows Services console to view services that run as Windows services, to identify the logon account to use for each such service, and to start, stop, and restart services. Foundation Hub includes a service named *BIOVIA Hub Server <version>*.

Foundation Hub Command Line Tools

Command-line tools provide the same features as the Windows Services Console. However, the command line also simplifies the process of customizing the service memory settings and start-up parameters.

- **Start the service**
  - **Windows:** `<hub_install>\bin\startService.bat`
  - **Linux:** `sudo bin/daemon.sh start`
- **Stop the service**
  - **Windows:** `<hub_install>\bin\stopService.bat`
  - **Linux:** `sudo bin/daemon.sh stop`
- **Restart the service**
  - **Windows:** `<hub_install>\bin\restartService.bat`
  - **Linux:** `sudo bin/daemon.sh restart`
- **Uninstall the service:** Stop the service before installing. On Linux, you will need to manually remove the installation directory. See Uninstalling Foundation Hub.
  - **Windows:**`<hub_install>\bin\uninstall.bat`
  - **Linux:** `sudo bin/daemon.sh uninstall`

Chapter 10: Uninstalling Foundation Hub

Note: If you are using Foundation Hub as your authentication server in Pipeline Pilot, be sure to change your authentication settings in the Pipeline Pilot Admin Portal on the **Security > Authentication** page.

Windows

Navigate to the Foundation Hub installation directory and run the uninstaller:

```
uninst.exe
```

The uninstaller will stop the Foundation Hub services, but will leave the configuration and log files.

Linux

1. Stop the service:

   ```
   daemon.sh stop
   ```

2. Uninstall the service as a root user:

   ```
   sudo daemon.sh uninstall
   ```

3. Remove the installation directory:

   ```
   rm -rf installDir
   ```

4. Remove the following:

   ```
   rm /etc/init.d/Hub
   rm /etc/rc.d/rc*.d/Hub
   ```

Chapter 11: Cloning the Foundation Hub Environment

Foundation Hub provides a **cloneconfig** utility that allows you to clone existing environment registry settings, make changes to reflect the new environment, and import it to a new system. Follow the procedures here to export the source configuration of the source environment and then import it into the target environment.

Exporting the Configuration from the Source Environment

1. Test the Foundation Hub source environment to make sure it is working properly.
2. Export the `cloneconfig.xml` file from the source environment. See Exporting cloneconfig.xml.
3. Shut down the source environment Foundation Hub services. See Managing the Foundation Hub Service .
4. Export the source environment Oracle DMP for the Foundation Hub schema. See Exporting the Source Environment Oracle DMP.

Exporting cloneconfig.xml

The `cloneconfig` endpoint consolidates all the application, installation, and node URL data into an XML file.

1. Navigate to the Foundation Hub installation to be cloned.
2. Point to the `cloneconfig` XML endpoint:

   `https://<original Hub>/foundation/hub/api/v1/cloneconfig`
3. Save `cloneconfig.xml`.

Exporting the Source Environment Oracle DMP

You can use any method you prefer to export your Oracle database or schema, such as Oracle data pump utilities, machine snapshots, and imaging techniques.

Best Practices

- Stop all Foundation Hub services before exporting the original schema.
- If you are using the Oracle Data Pump utilities, use the parallel option if the schema is very large, (for example, several hundred GB).
- Export all BIOVIA schemas that belong to the same environment simultaneously. For example, if you have Foundation Hub and Compose installed, export both schemas simultaneously (for example , `expdp schemas=hub,compose` when using Oracle Data Pump utilities.)
- If exporting schemas simultaneously using Oracle Data Pump utilities, use the `flashback_time=systimestamp` parameter.

Importing the Configuration to the Target Environment

1. Prepare the target environment infrastructure, including a application server and database server.
2. If your target environment already has Foundation Hub installed, shut down the target environment Foundation Hub services. See Managing the Foundation Hub Service .

3. Import the Oracle DMP into the target environment Oracle Database server.
4. Copy `cloneconfig.xml` into the Foundation Hub base directory and edit it to reflect the new environment. See Editing cloneconfig.xml.

   If you are cloning a load-balanced environment, you only need to do this for one node. The information in `cloneconfig.xml` is imported into the database on startup and is shared among all of the nodes.
5. Edit the target environment configuration files to reflect the new environment:
   - `app-config.groovy`: Update `hubSelfRegistration.nodeRootUrl` and `hubSelfRegistration.nodeSslRootUrl`.
   - `tomcat.properties`: Update host.

   If you are cloning to a load-balanced environment, copy the updated files to all nodes.
6. Restart target environment Foundation Hub services. The `cloneconfig.xml` file will automatically be parsed, timestamped, and moved to a folder called `imported_configurations`.

   IMPORTANT! Do not restart the target environment Foundation Hub services without editing `cloneconfig.xml` to reflect the new environment first.

7. Change the application label to distinguish the cloned instance from the original installation.

   IMPORTANT! Do not perform this step before restarting the target environment as required in step 6.

   a. From the target environment, open .**Admin and Settings > Applications**
   b. Click the row for Foundation Hub.
   c. Click **Edit**.
   d. Change the text in the **Label** field.
   e. Click **Save**.
   f. Repeat steps b through e for other applications listed in **Admin and Settings > Applications**.
8. Verify the target environment functionality.

Note: It is highly recommended that you firewall network traffic between your environments, especially if the source environment is a production environment.

Editing cloneconfig.xml

1. Change the `rootUrl` and `sslRootUrl` fields for the Applications and Nodes to point to the new location.
2. Make additional changes as needed. See Examples.

   IMPORTANT!
   - Do not edit the origin section. This origin section is designed to prevent corruption of the source database.
   - Do not edit the application names or application labels.
   - Do not create new applications.
   - Do not use invalid URLs.
   - Do not edit Session Inactivity Timeout or Session Global Timeout fields. Change those in the target environment in **Admin and Settings > Hub Configuration**.

Cloneconfig Fields

- **origin:** Schema information of the source database. Do not edit these fields. This origin section is designed to prevent corruption of the source database schema. If you try to import `cloneconfig.xml` into a Foundation Hub server that is using the same Oracle schema information in `app-config.groovy`, Foundation Hub will abort to prevent modification of the schema.

  > **Note:** An error is thrown if the schema data in the `cloneconfig` file matches the server you are importing to.

- **application:** Represents a unique installation. The installation and application properties are combined to a single application header.
  - **name/label:** Name and label fields from the application. Do not edit these fields. The application name and label are used to identify the records in the Foundation Hub database schema to modify. If an Installation has multiple applications associated with it, the first application's name and label are used. For example if you want to change the Pipeline Pilot URL, it may be listed under BIOVIA Draw since Draw was also registered on that Pipeline Pilot server.
  - **rootUrl/sslRootUrl:** Application's rootUrl and sslRootUrl fields.
  - **nodes:** List of nodes associated with each installation.
    - **node:** Unique node for the installation.
      - **rootUrl:** Root URL of the node.
      - **sslRootUrl:** SSL root URL of the node.

Examples

- Valid cloneconfig.xml
- Removing an Application
- Removing Nodes
- Adding Nodes
- Editing URLs

Valid cloneconfig.xml

```
<?xml version="1.0" encoding="UTF-8"?>
<applications>
  <origin>
    <schema>Schema Name</schema>
    <server>jdbc:oracle:thin:@//host:port/source</server>
  </origin>
  <application>
    <name>Application 1 Name</name>
    <label>Application 1 Label</label>
    <rootUrl>http://app1:port</rootUrl>
    <sslRootUrl>https://app1:port</sslRootUrl>
    <nodes>
      <node>
        <rootUrl>http://node1:port</rootUrl>
        <sslRootUrl>https://node1:port</sslRootUrl>
      </node>
      <node>
        <rootUrl>http://node2:port</rootUrl>
        <sslRootUrl>https://node2:port</sslRootUrl>
      </node>
    </nodes>
  </application>
  <application>
    <name>Application 2 Name</name>
    <label>Application 2 Label</label>
    <rootUrl>http://app2:port</rootUrl>
    <sslRootUrl />
    <nodes />
  </application>
  <application>
    <name>Application 3 Name</name>
    <label>Application 3 Label</label>
    <rootUrl>http://app3:port</rootUrl>
    <sslRootUrl>https://app3:port</sslRootUrl>
    <nodes />
  </application>
</applications>
```

Removing an Application

```
<?xml version="1.0" encoding="UTF-8"?>
<applications>
  <origin>
    <schema>Schema Name</schema>
    <server>jdbc:oracle:thin:@//host:port/source</server>
  </origin>
  <application>
    <name>Application 1 Name</name>
    <label>Application 1 Label</label>
    <rootUrl>http://app1:port</rootUr>
    <sslRootUrl>https://app1:port</sslRootUrl>
    <nodes />
  </application>
  <application>
    <name>Application 2 Name</name>
    <label>Application 2 Label</label>
    <rootUrl>http://app2:port</rootUrl>
    <sslRootUrl>https://app2:port</sslRootUrl>
    <nodes />
  </application>
</applications>
```

To remove Application 2, remove the `<application>` block that contains that application:

```
<?xml version="1.0" encoding="UTF-8"?>
<applications>
  <origin>
    <schema>Schema Name</schema>
    <server>jdbc:oracle:thin:@//host:port/source</server>
  </origin>
  <application>
    <name>Application 1 Name</name>
    <label>Application 1 Label</label>
    <rootUrl>http://app1:port</rootUr>
    <sslRootUrl>https://app1:port</sslRootUrl>
    <nodes />
  </application>

</applications>
```

Removing Nodes

```
<?xml version="1.0" encoding="UTF-8"?>
<applications>
 <origin>
    <schema>Schema Name</schema>
    <server>jdbc:oracle:thin:@//host:port/source</server>
 </origin>
 <application>
    <name>Application 1 Name</name>
    <labelApplication 1 Label</label>
    <rootUrl>http://app1:port</rootUrl>
    <sslRootUrl>https://app1:port</sslRootUrl>
    <nodes>
      <node>
        <rootUrl>http://node1:port</rootUrl>
        <sslRootUrl>https://node1:port</sslRootUrl>
      </node>
      <node>
        <rootUrl>http://node2:port</rootUrl>
        <sslRootUrl>https://node2:port</sslRootUrl>
      </node>
    </nodes>
  </application>
  <application>
    <name>Application 2 Name</name>
    <label>Application 2 Label</label>
    <rootUrl>http://app2:port</rootUrl>
    <sslRootUrl>https://app2:port</sslRootUrl>
    <nodes />
  </application>
</applications>
```

To remove node one:

```
<?xml version="1.0" encoding="UTF-8"?>
<applications>
 <origin>
    <schema>Schema Name</schema>
    <server>jdbc:oracle:thin:@//host:port/source</server>
 </origin>
 <application>
    <name>Application 1 Name</name>
    <labelApplication 1 Label</label>
    <rootUrl>http://app1:port</rootUrl>
    <sslRootUrl>https://app1:port</sslRootUrl>
    <nodes>
      <node>
```

```
        <rootUrl>http://node2:port</rootUrl>
        <sslRootUrl>https://node2:port</sslRootUrl>
      </node>
    </nodes>
  </application>
  <application>
    <name>Application 2 Name</name>
    <label>Application 2 Label</label>
    <rootUrl>http://app2:port</rootUrl>
    <sslRootUrl>https://app2:port</sslRootUrl>
    <nodes />
  </application>
</applications>
```

To remove both nodes:

```
<?xml version="1.0" encoding="UTF-8"?>
<applications>
 <origin>
    <schema>Schema Name</schema>
    <server>jdbc:oracle:thin:@//host:port</server>
 </origin>
 <application>
    <name>Application 1 Name</name>
    <labelApplication 1 Label</label>
    <rootUrl>http://app1:port</rootUrl>
    <sslRootUrl>https://app1:port</sslRootUrl>
    <nodes />
  </application>
  <application>
    <name>Application 2 Name</name>
    <label>Application 2 Label</label>
    <rootUrl>http://app2:port</rootUrl>
    <sslRootUrl>https://app2:port</sslRootUrl>
    <nodes />
  </application>
</applications>
```

Adding Nodes

In this example, neither application has nodes:

```
<?xml version="1.0" encoding="UTF-8"?>
<applications>
  <origin>
    <schema>Schema Name</schema>
    <server>jdbc:oracle:thin:@//host:port/source</server>
  </origin>
  <application>
    <name>Application 1 Name</name>
    <label>Application 1 Label</label>
    <rootUrl>http://app1:port</rootUrl>
    <sslRootUrl>https://app1:port</sslRootUrl>
    <nodes />
  </application>
</applications>
```

To add nodes to Foundation Hub:

```
<?xml version="1.0" encoding="UTF-8"?>
<applications>
 <origin>
    <schema>Schema Name</schema>
    <server>jdbc:oracle:thin:@//host:port/source</server>
  </origin>
  <application>
    <name>Application 1 Name</name>
    <label>Application 1 Label</label>
    <rootUrl>http://app1:port</rootUrl>
    <sslRootUrl>https://app1:port</sslRootUrl>
    <nodes />
  </application>
  <origin>
    <schema>Schema Name</schema>
    <server>jdbc:oracle:thin:@//host:port/source</server>
  </origin>
  <application>
    <name>Application 1 Name</name>
    <label>Application 1 Label</label>
    <rootUrl>http://app1:port</rootUrl>
    <sslRootUrl>https://app1:port</sslRootUrl>
    <nodes>
      <node>
        <rootUrl>http://node1.port</rootUrl>
        <sslRootUrl>https://node1:port</sslRootUrl>
      </node>
      <node>
        <rootUrl>http://node2.port</rootUrl>
        <sslRootUrl>https://node2:port</sslRootUrl>
      </node>
    </nodes>
  </application>
</applications>
```

Editing URLs

```
<?xml version="1.0" encoding="UTF-8"?>
<applications>
  <origin>
    <schema>Schema Name</schema>
    <server>jdbc:oracle:thin:@//host:port/source</server>
  </origin>
  <application>
    <name>Application 1 Name</name>
    <label>Application 1 Label</label>
    <rootUrl>http://originalhost:port</rootUrl>
    <sslRootUrl>https://originalhost:port</sslRootUrl>
    <nodes>
      <node>
```

```
        <rootUrl>http://originalnode1:port</rootUrl>
        <sslRootUrl>https://originalnode1:port</sslRootUrl>
      </node>
    </nodes>
  </application>
  <application>
    <name>Application 2 Name</name>
    <label>Application 2 Label</label>
    <rootUrl>http://host:port</rootUrl>
    <sslRootUrl>https://host:port</sslRootUrl>
    <nodes />
  </application>
</applications>
```

Edit the URLs to change them. Check that they are valid before using the `cloneconfig.xml` file.

```
<?xml version="1.0" encoding="UTF-8"?>
<applications>
  <origin>
    <schema>Schema Name</schema>
    <server>jdbc:oracle:thin:@//host:port/source</server>
  </origin>
  <application>
    <name>Application 1 Name</name>
    <label>Application 1 Label</label>
    <rootUrl>http://newhost:port</rootUrl>
    <sslRootUrl>https://newhost:port</sslRootUrl>
    <nodes>
      <node>
        <rootUrl>http://newnode1:port</rootUrl>
        <sslRootUrl>https://newnode1:port</sslRootUrl>
      </node>
    </nodes>
  </application>
  <application>
    <name>Application 2 Name</name>
    <label>Application 2 Label</label>
    <rootUrl>http://host:port</rootUrl>
    <sslRootUrl>https://host:port</sslRootUrl>
    <nodes />
  </application>
</applications>
```

Chapter 12: Troubleshooting

Foundation Hub generates standard log files that you can use to troubleshoot issues with the installation. See the following for tools that are available with Foundation Hub for troubleshooting purposes:

- Foundation Hub Logging
- Using PuTTY to Test ConnectivityUsing PuTTY to Test Connectivity

General Issues

My license expired and I cannot access the Admin and Settings page to update it

Problem: A valid license is required to access the Admin and Settings page. If your license is expired, you cannot access the **License Files** page to add an updated license file.

Solution: You must manually copy the license file to the installation directory and restart the Foundation Hub service.

Licenses are made available when the software is purchased. If you need assistance with licenses, contact Dassault Systèmes Customer Support.

1. Navigate to the installation folder for Foundation Hub. For example: `C:\Program Files\BIOVIA\Foundation\hub`.
2. Remove the expired license file (`.lic`) from the installation folder and from the `imported_licenses` folder if it exists.
3. Copy the updated license file to the installation folder.
4. Restart the *BIOVIA Hub Server <version>* service. See Managing the Foundation Hub Service .
5. Repeat for each Foundation Hub server node if you are working with a load-balanced environment.

Load-balanced Pipeline Pilot nodes are no longer registered with Foundation Hub after upgrading Pipeline Pilot

Check for missing load-balanced Pipeline Pilot nodes. If you are upgrading from 2017 to 2018 and have load-balanced Pipeline Pilot servers, there is a known issue that may have caused existing nodes registered with the installation to be removed:

1. Navigate to **Admin and Settings > Settings > Applications**.
2. Find the row for **Pipeline Pilot**, click the link in the **Installation** column, and check for a list of your load-balanced Pipeline Pilot nodes.
3. If they are missing, click **Edit**, click **Add** under **Nodes**, and then add the fully qualified URL (HTTP) and fully qualified secure URL (HTTPS) for each Pipeline Pilot node.

Cannot start the Foundation Hub because the Oracle password has expired

1. Make a backup of the Foundation Hub configuration file:
   `<hub_install>\conf\app-config.groovy`
2. Make the following changes to the original configuration file:
   - Change the Data Source Password to the new Oracle Password.
   - Comment out the line that references `.passwordEncryptionCodec`.
3. Save the file and restart Foundation Hub.
4. In Foundation Hub, open **Admin and Settings > Hub Configuration** and click **Edit**.
5. Set the **Data Source Password** field to the new Oracle schema password again and **Save**. Saving will re-enable encryption.

Also If you know in advance that you will be resetting your Oracle schema password, see Resetting Your Oracle Password.

Equipment and instrument features are not enabled as expected

Check that you have a license for equipment and instrument functionality in **Settings > License Files**. If you add a license file, you *do not* need to stop or restart the Foundation Hub service.

Licenses are made available when the software is purchased. If you need assistance with licenses, contact Dassault Systèmes Customer Support.

Foundation Hub does not start, no error or redirect

There may be no access to the database because the credentials or URL changed, or there may be a port conflict. Check `hub.log` to confirm. See Foundation Hub Logging.

- To resolve a database connection string issue, see Resolving an Invalid Database Connection String.

Issues manually editing configuration files

See Reverting Foundation Hub to the Default Configuration.

Timeout while attempting to restart the Foundation Hub Server

Restart the server manually. See Chapter 9: Managing the Foundation Hub Service .

The log file was not updated or saved

Check that there is enough disk space. See *Foundation Hub System Requirements*.

3DPassport Issues

Single log out not working when using 3DPassport authentication

The 3DPassport server and the Foundation Hub server must have a trust relationship set up between them. Include the SSL certificate for the Foundation Hub server in the 3DPassport server's Truststore, and include the SSL certificate for the 3DPassport server in the Foundation Hub server's Truststore.

Directed to 3DPassport login page and cannot sign in

Authentication was set to Passport on the Hub Configuration page.

If you do *not* plan to use 3DPassport for authentication, update the Hub Configuration to not use Passport for Authentication:

1. Use the following URL to use local authentication instead of 3DPassport:

   ```
   https://<hub server>:9953/foundation/hub/security/auth?local=true
   ```

2. Navigate to **Admin and Settings > Settings > Hub Configuration** and set **Authentication** to **Hub**.

If you do plan to use 3DPassport for authentication, you need to create the user and/or set up permissions for the user account. See Setting Up User Authentication with 3DPassport.

User cannot sign in

Foundation Hub does not enforce unique usernames for multiple domains. If a user is not able to sign in, he or she may be using a username that is duplicated in a different domain. Ask the user to sign in while specifying the domain name. For example `<domain>\username`.

Foundation Hub Logging

Note: Each node in a load-balanced deployment has its own log file. To figure out if an error occurred you must check all log files.

Viewing Log Files

1. Open **Settings > Logging**.
2. Click **Download Current Log File** or **Download All Log Files**.
3. See `<hub_install>/logs/hub.log`.

Editing Logging Settings

To manage Foundation Hub application logging, navigate to **Admin and Settings > Settings > Logging** and click **Edit**:

- **Application Logging Level:** Choose from **Debug**, **Info**, and **Warn** to set the level of verbosity. It is recommended that you leave the level set to **Warn**.
- **Log SQL Statements:** Logs a line for each SQL statement executed against the database. This option is verbose. It is not recommended for normal operation.
- **Log SQL Statement Parameters:** Logs a line for each parameter of each SQL statement executed against the database. This option is extremely verbose. It is not recommended for normal operation.
- **Download Current Log File:** Retrieves the active `hub.log` file from the server.
- **Download All Log Files:** Retrieves the current `hub.log` file, all archived log files (up to a maximum of ten) as well as the most recent `stderr` and `stdout` log files.
- **Output Elapsed Times:** Includes the time elapsed for various operations such as GET, PUT, and POST. This provides profiling information.
- **Include System Information:** Includes the system information (for example, host operating system and Java system information).

Tomcat Logging

Apache Tomcat logs additional information in its own log files:

- `stdout` (standard output)
- `stderr` (standard error)

Tomcat Http Access Logging

You can turn on Tomcat Http Access Logging in **Settings > Hub Configuration > Enable Tomcat Http Access Logging**.

Foundation Hub will record all requests processed by the server. With this enabled the following information is written to an access_log file in the log folder:

- Remote host name (or IP address if enableLookups for the connector is false)
- Date and time, in Common Log Format
- First line of the request (method and request URI)
- HTTP status code of the response
- User session ID
- Time taken to process the request, in milliseconds
- Time taken to commit the response, in milliseconds
- Current request thread name

Note: These log files are not cleaned up automatically. If you plan to use this feature, it is recommended that you include regular cleanup as part of your business process.

Java Garbage Collection Logs

Timestamped logs for Java garbage collection are created in `<hub_install>/logs`. These log files are not cleaned up automatically. It is recommended that you include regular cleanup as part of your business process.

Using PuTTY to Test Connectivity

Installations of Foundation Hub include the PuTTY terminal emulator, which you can use to test network connectivity of equipment and devices.

Running PuTTY

Access PuTTY here: `<hub_install>\util\putty\win64`.

Accessing PuTTY Documentation

See the PuTTY documentation: https://www.chiark.greenend.org.uk/~sgtatham/putty/docs.html.

Resolving an Invalid Database Connection String

The Foundation Hub validates the Database Configuration during the initial save of the server configuration. Issues with the connection string (Datasource URL, Username, and Password) are reported to the UI and logged to `<hub_install>/logs/hub.log`.

For example:

```
2015-02-10 10:14:58,203 [tomcat-exec-2] ERROR application.Foundation
HubConfigSingletonService  - An error occurred establishing a database
connection. ORA-01017: invalid username/password; logon denied
```

After configuration, if the database credentials or the URL has changed and the Foundation Hub can no longer access the database, an error is reported to `hub.log`.

For example:

```
2015-02-10 11:45:09,313 [localhost-startStop-1] ERROR pool.ConnectionPool  -
Unable to create initial connections of pool.

java.sql.SQLException: ORA-01017: invalid username/password; logon denied
```

This causes the *BIOVIA Hub Server <version>* service to fail to start.

You can change the username and URL values directly in `<hub_install>\conf\app-config.groovy`. However, the password is encrypted during the configuration step and additional steps are required.

Changing the Database Password

1. Stop the *BIOVIA Hub Server <version>* service. See Chapter 9: Managing the Foundation Hub Service .
2. Edit `<hub_install>\conf\app-config.groovy` and comment out or remove the following line:

   ```
   passwordEncryptionCodec='com.accelrys.platform.utils.DatasourceCodec'
   ```
3. Change the encrypted **Data Source password** string to the to the actual plaintext password for the **Data Source** user.
4. Start the Foundation Hub and navigate to the **Administration > Foundation Hub Configuration** page.
5. Edit the configuration and re-enter the new password in the **Data Source Password** field.
6. Click **Save** and **Restart Server**.

The Foundation Hub server re-enables password encryption and writes the database password as an encrypted string to the `app-config.groovy` file.

Alternatively you can revert the Foundation Hub configuration to default (see Reverting Foundation Hub to the Default Configuration) and re-run the configuration process.

Reverting Foundation Hub to the Default Configuration

Run the following command:

```
<hub_install>\bin\resetConfiguration.bat
```

Or:

```
<hub_install>/bin/resetConfiguration.sh
```

The command performs the following steps:

1. Copy the current configuration files to `<hub_install>/conf/backup`.
2. Overwrite pre-existing backups.
3. Delete the existing configuration files, and replace them with template versions.

Note: After restarting, the browser is redirected to the Foundation Hub Configuration Page.

Updating the Password in the Keystore After a Certificate Change

If users cannot log in to Foundation Hub, a possible reason is that the certificate expired or was updated, but the configuration was not updated. Use these steps to correct the situation and log in.

To update the configuration file:

1. Create the Java keystore file for the new certificate. See Chapter 7: Working with Certificates.
2. Open the `<Install Hub folder>\config\` file , open the `tomcat.properties` file, and locate the keystore.path in the file.
3. Back up the file `tomcat.properties` file. If you run Foundation Hub in a load-balanced environment, back up this file on each additional server.
4. Move or copy the newly created file to the name and location of the keystore.path identified in Step 2.
5. Stop the Foundation Hub service.
6. Edit the file `<Install Hub folder>\config\tomcat.properties` by changing the entry under keystore.password. Replace the encrypted password string with the current password in clear text.
7. Start the Foundation Hub service.
8. If you are running in a load-balanced environment, repeat Steps 5-7 (stop the service, edit the file, and restart the service).
9. To verify that the certificate has been changed, do the following:
   a. Access `https:\\<FQDN>:9953\foundation\hub` and check the certificate.
   b. Check to see if users can now log on.
   c. After users have logged on, check to see if the `cleartext` password in each `tomcat.properties` file has been overwritten with the encrypted password.

Appendix A: Security Considerations

BIOVIA Foundation Hub supports a variety of configuration options and settings that can help protect your data from security vulnerabilities. When planning your deployment, consider the following recommendations to help prevent unauthorized access to data and malicious computer attacks. Additionally, your deployment configuration should be validated by security experts and comply with policies within your organization.

We strongly recommend that you install critical patches (including security patches and hot fixes) for all systems as soon as they become available, so you can keep your Foundation Hub environment as secure and up-to-date as possible. To verify if you should upgrade to a major or minor release of an operating system or database, refer to the *BIOVIA Foundation Hub System Requirements* or contact Dassault Systèmes Customer Support.

We also assume the administrator of the Foundation Hub system has a basic understanding of security, and understands how to harden servers and databases.

TLS Support

Foundation Hub uses TLS version 1.2 or higher. To ensure Foundation Hub uses the most secure TLS service cipher suites, disable older TLS versions such as 1.0 and 1.1. When Foundation Hub is used with any other BIOVIA applications, ensure that both Foundation Hub and those BIOVIA applications use the same TLS Version.

If you have a third-party application using a weaker protocol that needs to connect to Foundation Hub, contact Dassault Systèmes Customer Support for assistance.

Considerations and Recommendations

Consideration	Recommendations	More Information
Server Security		
Server Infrastructure	■ Deploy your Foundation Hub server behind a firewall, load balancer, or another network device that protects it from unwanted network traffic. ■ For your production deployment, using a load balancer as a reverse proxy is the recommended deployment pattern.	■ Load Balancing ■ Configuring Foundation Hub for Load Balancing
Server Authentication and Authorization	Only authorized IT staff should have access to the application server machine.	
Server Configuration	Install virus-scanning software in locations from which files are uploaded to Foundation Hub, including network locations that store files for equipment readings.	

Consideration	Recommendations	More Information
SSL Certificates	To secure communication between the server and any client connecting via SSL in your deployment of Foundation Hub, obtain and install a trusted SSL certificate from a recognized Certificate Authority.	Working with Certificates
Encryption	■ Configure your deployment to use SSL over HTTPS for network communications. Foundation Hub uses TLS 1.2 or higher to encrypt network communications. ■ Consider blocking HTTP access at the load balancer or reverse proxy to force all traffic to be sent over HTTPS.	■ TLS Support ■ Configuring the Hub on a Single Server (step 2) ■ Configuring the Primary Load-Balanced Server (step 2)
Application Configuration (Server)	■ To ensure that users are not forwarded to untrusted sites and only trusted sites receive security tokens, keep the **Validate Login Return Url** setting enabled (enabled by default). The allowlist includes any URL aliases for applications that you register with Foundation Hub. ■ Set the **Session Inactivity Timeout** and **Session Global Timeout** intervals according to your organization's security policies	■ Configuring the Hub on a Single Server (step 2) ■ Configuring the Primary Load-Balanced Server (step 2)
Application Security		
Authentication	■ For most production deployments, configure Foundation Hub as the authentication provider. Alternatively, if you are running within the 3DEXPERIENCE Platform, configure authentication to use 3DPassport. ■ Use LDAP to connect Foundation Hub user accounts with your corporate directory, allowing users to log in with their standard network user accounts. ■ For your production deployment, use only LDAP accounts, and do not use local accounts in the Foundation Hub database. This setup ensures that all credentials are subject to the password and other standard account policies for your organization.	Setting Up User Authentication

Consideration	Recommendations	More Information
Authorization	■ Create an administrator account and then disable or change the password for the *scitegicadmin* account. The default password for the *scitegicadmin* account is the same used for all BIOVIA applications. ■ Configure appropriate permissions, roles, groups, and collaborative spaces to follow the principle of least privilege. All access rights and permissions are enforced within the Foundation Hub application.	■ Change the Default Password ■ Managing Security in the *BIOVIA Foundation Hub Administration Guide*
Database Security		
Database Authentication and Authorization	■ Configure the database user with the required permissions. ■ Users in the system do not require direct database access. All database access is through the application server.	Creating a Foundation Hub Database Schema in Oracle

Dassault Systèmes Support Resources

For additional resources or to contact Dassault Systèmes Customer Support, visit the Support portal:

https://www.3ds.com/support/

From this portal, you can:

- Call or email Dassault Systèmes Customer Support
- Submit a request
- Download installers
- Access hardware and software requirements
- Access Knowledge Base
- Access Communities and Twitter feeds