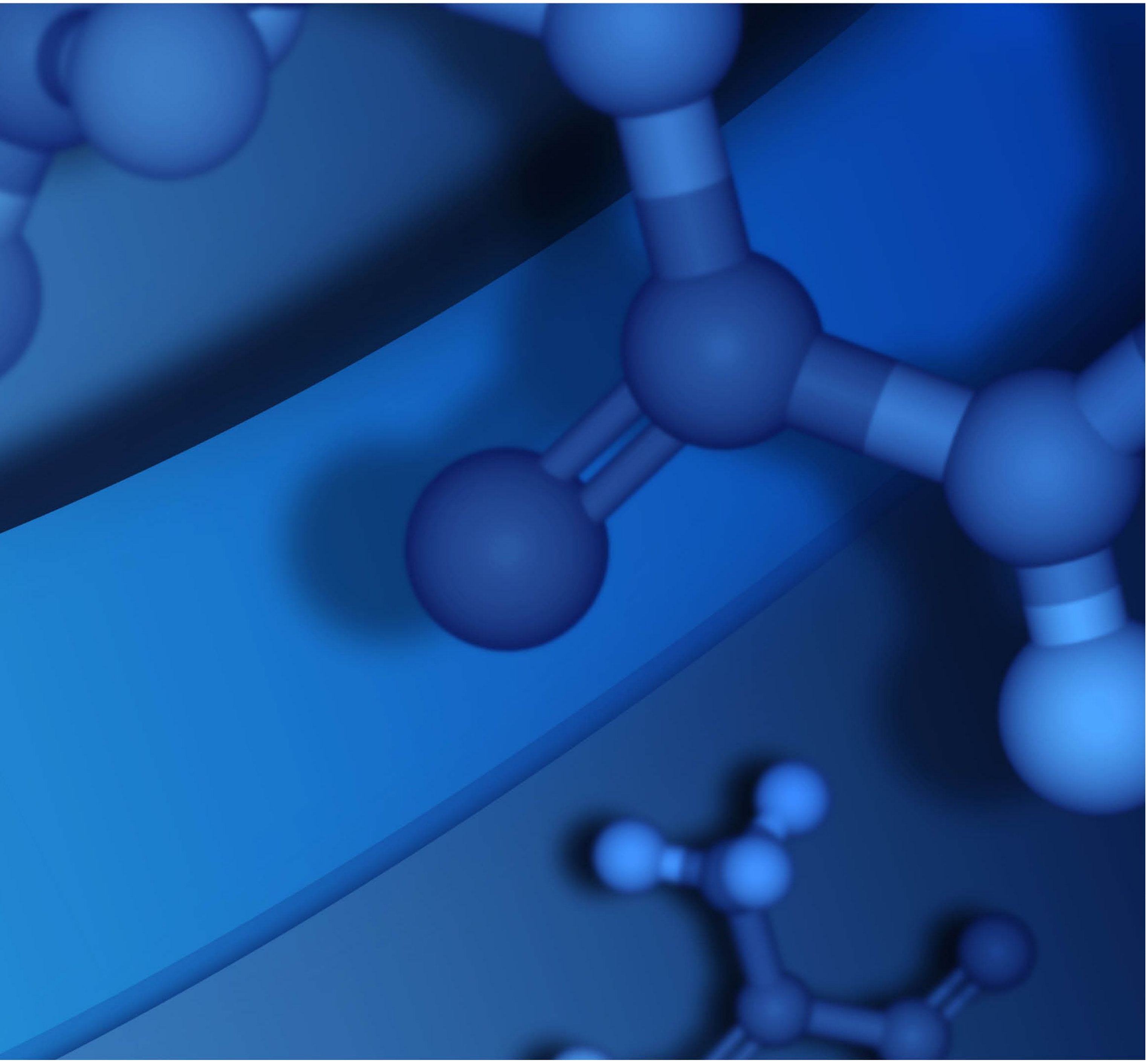
VAULT SERVER INSTALLATION GUIDE

BIOVIA WORKBOOK 2021



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 Workbook 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

Installation Overview

Vault Server is the BIOVIA Workbook component that interfaces between end users on Workbook client systems and the Workbook Oracle data repository on a database server.

This guide describes how to set up and install the Workbook 2021 Vault Server.

This Overview provides a summary of the installation process and provides flowcharts that depict the overall workflow.

Installation Process Overview

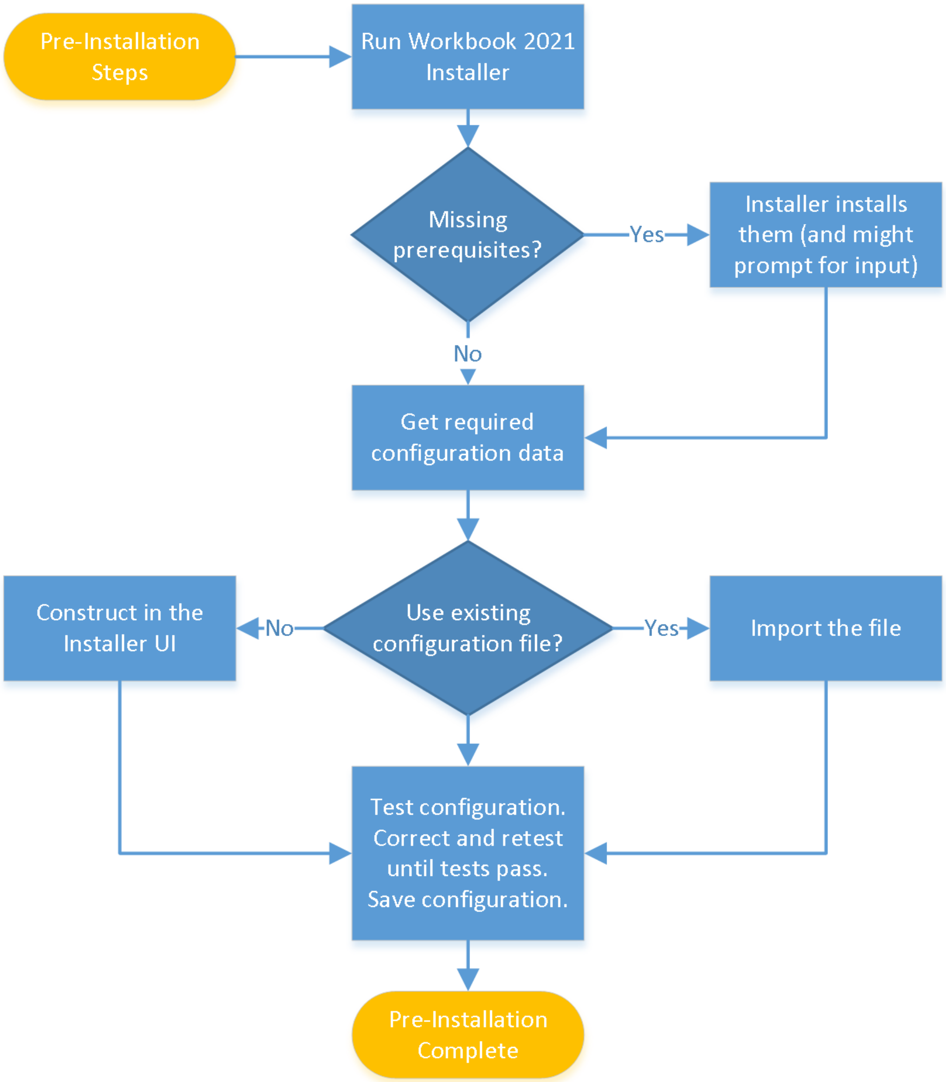
Regardless of whether you are upgrading from a previous release or creating a greenfield deployment of Workbook 2021, it is important to perform this sequence of tasks:

1. Perform prerequisite tasks such as gathering configuration details and preparing your environment for your new installation or upgrade, as described in Chapter 1: Prerequisite Tasks.
2. Run the Workbook Installer to perform pre-installation configuration and testing tasks and to install the software, as described in Chapter 2: Running the Workbook 2021 Installer and shown in the following diagrams:
   - Pre-Installation Flowchart on page 2
   - Installation Flowchart on page 3

   Alternatively, you can install or upgrade not only Workbook, but also Pipeline Pilot, Compose and Capture, and CISPro, by using Ansible scripts. For information about performing a scripted installation, see the *Ansible Scripting Installation Guide for BIOVIA 2021*. This guide is included in the ULM documentation zip file on the Dassault Systèmes Download Platform.
3. Perform required post-installation tasks such as configuring ADM and installing other Workbook components, as described in Chapter 3: Post-Installation Tasks and shown in Post-Installation ADM Configuration Flowchart on page 4.
4. Perform additional tasks such as configuring your load-balanced environment and installing related BIOVIA applications that you need for Workbook 2021 to function correctly in your environment. For more information, see the following:
   - Appendix A: Configuring Load Balanced Environments
   - Appendix B: Integration with BIOVIA Chemical Registration
   - Appendix C: Integration with BIOVIA CISPro

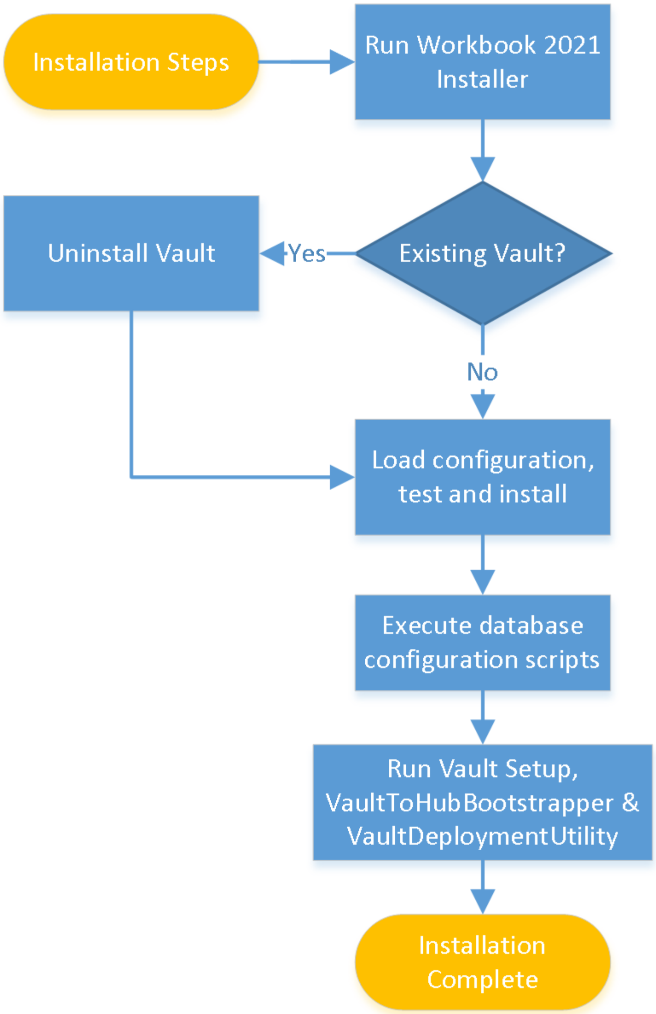
Pre-Installation Flowchart

The following flowchart depicts the pre-installation workflow, which you perform using the Workbook Installer as described in Chapter 2: Running the Workbook 2021 Installer.


Pre-Installation Steps
Run Workbook 2021 Installer
Missing prerequisites?
Yes
Installer installs them (and might prompt for input)
No
Get required configuration data
Use existing configuration file?
No
Construct in the Installer UI
Yes
Import the file
Test configuration. Correct and retest until tests pass. Save configuration.
Pre-Installation Complete

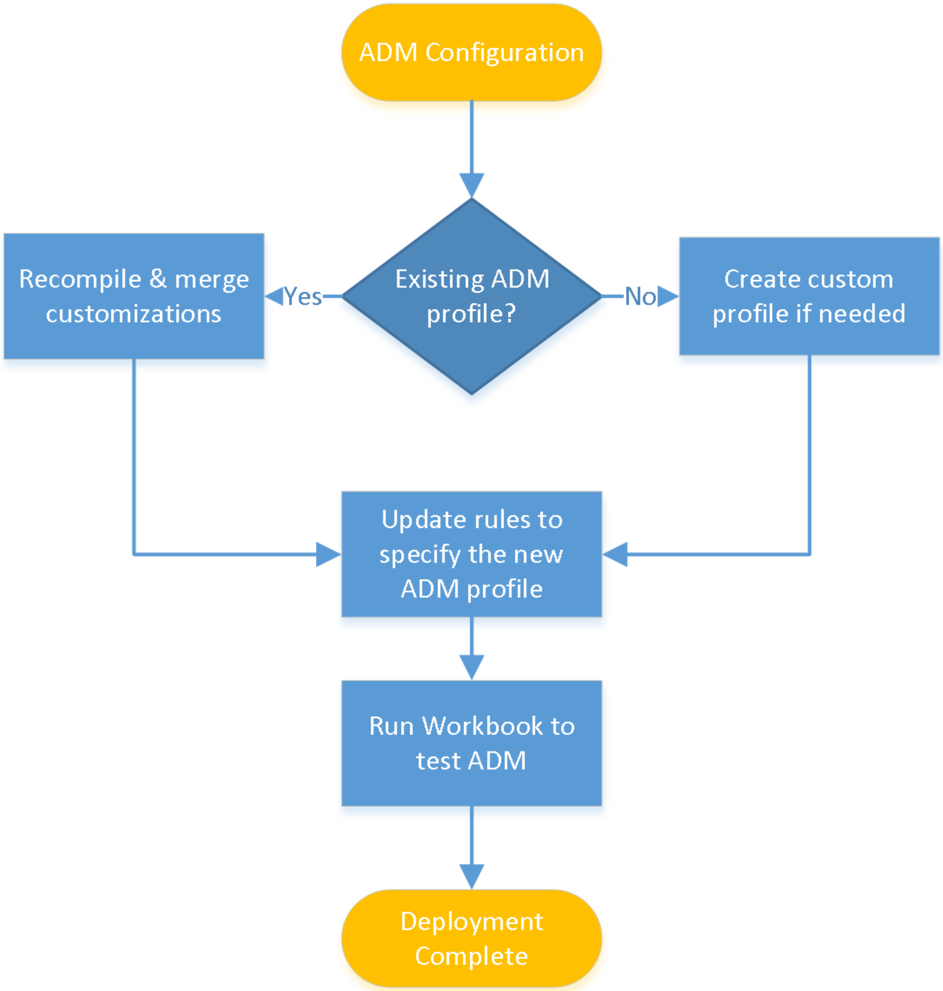
Installation Flowchart

The following flowchart depicts the installation workflow, which you perform using the Workbook Installer as described in Chapter 2: Running the Workbook 2021 Installer.


Installation Steps
Run Workbook 2021 Installer
Existing Vault?
Yes
Uninstall Vault
No
Load configuration, test and install
Execute database configuration scripts
Run Vault Setup, VaultToHubBootstrapper & VaultDeploymentUtility
Installation Complete

Post-Installation ADM Configuration Flowchart

The following flowchart shows the workflow for configuring ADM, which is one of the post-installation tasks described in Post-Installation Tasks on page 26.


ADM Configuration
Existing ADM profile?
Yes
Recompile & merge customizations
No
Create custom profile if needed
Update rules to specify the new ADM profile
Run Workbook to test ADM
Deployment Complete

Chapter 1: Prerequisite Tasks

Perform the prerequisite tasks described in this chapter before you do either of the following:

- Create a new installation of Workbook 2021.
- Upgrade an earlier Workbook installation to Workbook 2021.

Both upgrades and new installs require all tasks in this chapter, except those marked **Upgrade Only** or **New Installs Only**. Even with an upgrade, however, ensure that the configuration is still valid.

These tasks are required for all installation methods: Workbook Installer, silent, and Ansible.

Verify System Requirements and Gather Resources

Perform the following preparation tasks before you start the other pre-installation tasks in this chapter:

1. Ensure that your system meets all requirements described in the *BIOVIA Vault Server 2021 System Requirements*, which is included in the `BIOVIA Workbook_Vault_2021_Documentation.zip` file.

   > **IMPORTANT!** The Workbook Installer checks for certain prerequisites and does not allow you to proceed if any are missing.

2. Review the BIOVIA Workbook 2021 *Product Release Document* (PRD) to:
   - Become familiar with the features in this release.
   - (Upgrades Only) In the Upgrade Paths section, identify any interim versions that you must install prior to upgrading from your current version to Workbook 2021.
3. Fill out the configuration data in the installation worksheets in Appendix A, or obtain and update the following files from a previous deployment of Workbook:
   - `workbook_config.xml` (output from the last deployment)
   - `*.parameters` (used as input for the last deployment)

   When you run the Workbook Installer, you can import an updated version of either of these files, or you can manually enter the required configuration data, using the worksheets or a previous configuration file for reference.
4. Obtain the `.PFX` certificate file and corresponding password for your Vault server or load balancer, if applicable.

   For details, see Configuring a Load Balanced Vault Server Environment on page 39.
5. Ensure that the license file that includes your Workbook license is uploaded to Foundation Hub and is still valid. From Foundation Hub, navigate to **Admin and Settings > Settings > License Files**. Note that your Workbook license might be combined with licenses for other BIOVIA products in a single license file if you licensed the products at the same time.
6. Install the SSL certificate in your trusted root store on the Vault server.

   For details, see Importing a SSL Certificate PFX File into the Trusted Root Store on page 79.

Prepare the Microsoft Windows Server

> **IMPORTANT!**
> Workbook 2021 requires a server on which IIS is not configured to support any other applications. Consequently, a new installation of Workbook 2021 typically requires a new server, rather than a server whose operating system has been upgraded to Windows Server 2019 or 2016. To use a server on which IIS is configured to support other applications, the applications must be migrated and their IIS configurations must be removed. For assistance, contact Dassault Systèmes Customer Support.
>
> To upgrade an earlier version of Workbook to Workbook 2021, the earlier version must be a supported version and the installation must be fully functional.

To prepare the Microsoft Windows Server that will host your Vault Server installation, perform the following tasks.

1. Install or upgrade the server as described in the appropriate Microsoft article:
   - Windows Server 2016 System Requirements (https://docs.microsoft.com/en-us/windows-server/get-started/system-requirements)

- Install, upgrade, or migrate to Windows Server 2019 (https://docs.microsoft.com/en-us/windows-server/get-started-19/install-upgrade-migrate-19)

2. Apply all critical Windows updates.
3. Install anti-virus software and then run a full scan to ensure there are no viruses on the server.
4. Add the server to the appropriate domain.
5. Ensure that the user who will install Vault Server has "Write" access to the following path:

   `C:\ProgramData`
6. Provide the Network Service account user with "Write" access to the system\temp folder as described in Provide "Write" Access to the System Temp Folder on page 7.
7. Remove the `IUSR_VaultServer_computer` account from the Guests group.
8. (Optional) Install .NET Framework 3.5.

   The Workbook Installer installs the .NET Framework 3.5, if it is not already installed.

   If you want to install it in advance, use a method described in the following article: Microsoft .NET Framework 3.5 Deployment Considerations (https://docs.microsoft.com/en-us/windows-hardware/manufacture/desktop/microsoft-net-framework-35-deployment-considerations).
9. Set the User Account Control (UAC) to its lowest setting (**Never Notify)**.

   You can reset UCA to your preferred setting after you complete the installation.

Provide "Write" Access to the System Temp Folder

Ensure that the Network Service account user has "write" access to the Windows System temp folder:

1. Determine the location of the folder.
   a. Select **Start** > **Control Panel** > **System and Security** > **System**.
   b. Click the **Advanced** tab and then click **Environment Variables**.
   c. In the **System variables** pane, note the value of **TEMP** variable, for example C:\WINDOWS\TEMP.
2. In Windows Explorer, right-click the temp folder, select **Properties**, and then click the **Security** tab.
3. In **Temp Properties**, in **Group or user names**, determine whether the **NETWORK_SERVICE** account user is listed and has **Write** access.
   - If the user is listed and already has **Write** access, this task is complete.
   - If the user is listed, but without **Write** access, click **Advanced**, click **Change Permissions**, and select the **Modify** permission to complete this task.
   - If the user is not listed:
     a. Click **Edit**, and then click **Add**.
     b. From **Locations**, find and select the server and then click **OK**.
     c. In **Select Users, Computers, or Groups**, in **Object Name**, type **`NETWORK SERVICE`** and click **Check names** to ensure that it is found.
     d. Select the **Write** permission.

Install and Configure Prerequisite BIOVIA Applications

Vault Server and the Workbook client application use Foundation Hub for single sign-on authentication. Foundation Hub and Pipeline Pilot Server must be correctly configured for SSL security using TLS1.2 and strong cryptography. Pipeline Pilot Server must also be configured for domain authentication via Foundation Hub—SAML is not supported. For configuration details, see the relevant product installation guides.

To install the prerequisite BIOVIA applications:

1. Refer to the *Workbook 2021 System Requirements* document to determine compatible versions of the following prerequisite applications:
   - BIOVIA Foundation Hub
   - BIOVIA Pipeline Pilot Server
   - BIOVIA Direct
2. If a compatible version of these applications is not already installed, obtain the appropriate installation archives and documentation zip files, extract the relevant product installation guides, and continue.
3. If needed, install or upgrade Foundation Hub and then install or upgrade Pipeline Pilot Server, on your application server or servers.

   You can install these applications on the same or on different servers.
4. Log in to the Pipeline Pilot Administration Console and ensure that Workbook is listed under **Reports > Installed Packages**.
5. If needed, install or upgrade BIOVIA Direct on your database server, either before or after Step 2.

Extract the Installation Files and Scripts

Extract `BIOVIA_Workbook_2021.zip` to the default temporary folder, `C:\BIOVIA\Workbook`, or to another folder whose path contains **no spaces**.

The `BIOVIA_Workbook_2021.zip` file contains the installers and scripts required for the following Workbook components:

- Vault Server
- Vault Administration Console
- Workbook client components
- Workflow Designer
- Query Service Security Plug-in

Notes:
This *Vault Server Installation Guide* focuses on Vault Server, but also provides instructions for installing Vault Administration Console and Workflow Designer. For more informationm see Installing Other Workbook Components on page 70.

For additional details about the installers and scripts in BIOVIA_Workbook_2021.zip, see Installation Files and Scripts in BIOVIA_Workbook_2021.zip on page 70.

Install the Vault Administration Console

Before you start the Workbook Installer, install the Vault Administration Console on the Vault server, or on a system from which the server can be accessed. This tool is required for troubleshooting issues that might arise during the installation process.

If you are upgrading, you must remove the currently installed version before you install the new version.

For details, see Installing and Uninstalling the Vault Administration Console on page 71.

Create a Vault Admin Account and Add it to Foundation Hub (New Installs Only)

Before you install Vault Server, you must create an account to serve as the Vault Global Administrator account.

To set up this account:

1. In your Microsoft Windows directory domain, create a valid user account to serve as the Vault Global Administrator.

   Notes:
   - Consider using an Active Directory Administrator account with standard domain user privileges that you can share across your network.
   - Avoid spaces and special characters in the password, as described in Characters to Avoid in Passwords.

2. In Foundation Hub, add the Vault Global Administrator user account to any BIOVIA Foundation Hub group that has a permission level of at least **Foundation | Logon**.

   During installation, when you run the VaultToHubBootstrapper utility, the utility automatically adds the Vault Global Administrator user account to the Foundation Hub Vault Global Administrators group, which provides all other required permissions.

Unsupported Password Characters

Avoid using the following special characters in your Vault Global Administrator Account password. If you use them, the Workbook Installer will fail when it attempts to run the Vault Deployment Utility, and you will have to exit and run the utility manually, as described in Manually Running the Vault Deployment Utility on page 83.

Special character	Escape sequence
blank space	" "
double quote (")	""""
single quote (')	^'
carat (^)	^^
ampersand (&)	^&
open angle bracket (<)	^<
closed angle bracket (>)	^>
pipe (|)	^|

Configure Workbook to Use BIOVIA Direct 2021 (Upgrades Only)

Perform the following steps to enable Workbook to use Direct 2021:

1. Install Direct 2021 as described in the *BIOVIA Direct Installation Guide*.
2. Use SQL*Plus to connect to the SymyxDB Workbook database schema.
3. Enable the `SymyxDb` Workbook schema to work with Direct 2021 by entering the following commands:

   ```
   execute mdlaux.unsetup;
   execute c$DIRECT2021.mdlauxop.setup;
   ```

4. Verify that the Direct version is now 2021 by entering the following command:

   ```
   select mdlaux.version from dual;
   ```

5. Repeat steps 2 through 4 to enable the `SymxDBUser` schema to work with Direct 2021.
6. Reconnect to the `SymyxDb` Workbook schema and upgrade the molecule and reaction domain indexes by entering the following commands:

   ```
   select mdlaux.upgradeindexes_prepare from dual;
   select mdlaux.upgradeindexes_upgrade from dual;
   ```

   Your output should be similar to the following:

   ```
   UPGRADEINDEXES_UPGRADE
   ------------------------------------------------
   Created index: ALLCHEMRXNS_CHEM
   Created index: ALLCHEMSTRUCS_CHEM
   ```

   If you encounter any errors, contact Dassault Systèmes Customer Support.

7. Validate the domain indexes by using the following commands:

   ```
   column index_name format a20
   column ityp_owner format a15
   select index_name, status, domidx_status, ityp_owner from user_indexes
   where index_type = 'DOMAIN';
   ```

   The output should list each index status as **VALID** and each Index Owner as **C$DIRECT2021**:

   ```
   INDEX_NAME           STATUS   DOMIDX_STATU ITYP_OWNER
   -------------------- -------- ------------ ---------------
   ALLCHEMSTRUCS_CHEM   VALID    VALID        C$DIRECT2021
   ALLCHEMRXNS_CHEM     VALID    VALID        C$DIRECT2021
   VAULTTEXT_TEXT       VALID    VALID        CTXSYS
   ```

Verify the Installation of Oracle Text

Note: To perform this task, use an account with DBA privileges to log in to SQL*Plus on the database server.

Vault Server and the RAS data warehouse component require Oracle Text for indexing and retrieving content.

To verify that Oracle Text has been installed:

1. Log in to the Oracle instance that will host the RAS data warehouse.
2. Start SQL*Plus.
3. Verify that the CTXSYS username exists by executing the following command:

   ```
   select username from dba_users where username = 'CTXSYS'
   ```

   If the username does not exist, Oracle Text is not installed. Refer to your Oracle documentation for instructions.
4. (Optional) If the CTXSYS account is locked and DBAs might need to log in as CTXSYS to work with packages owned by CTXSYS, unlock it and reset its password by executing the following command:

   ```
   alter user ctxsys identified by new_ctxsys_password account unlock;
   ```

Disable Auto-Acceptance of SQL Profiles

To avoid a known Oracle defect, disable automatic acceptance of SQL profiles:

1. Log in to SQL*Plus as SYS, as sysdba, or as System.
2. Execute the following command to determine if SQL profile acceptance is automatic:

   ```
   select parameter_value from dba_advisor_parameters where task_name = 'SYS_
   AUTO_SQL_TUNING_TASK' and parameter_name = 'ACCEPT_SQL_PROFILES';
   ```
3. If the output of the command is **True**, execute the following query to change it to **False**:

   ```
   BEGIN
   DBMS_SQLTUNE.SET_TUNING_TASK_PARAMETER('SYS_AUTO_SQL_TUNING_TASK', 'ACCEPT_SQL_
   PROFILES', 'false');
   END;
   /
   ```

Install and Verify ODAC

Workbook requires a specific Oracle Database Access Components (ODAC). To obtain them, you must have an Oracle Support contract and Support Identifier.

To download and install ODAC:

1. Browse to the download page for **ODAC Developer Downloads - Oracle Universal Installer**:

   http://www.oracle.com/technetwork/topics/dotnet/downloads/odacdev-4242174.html
2. Accept the license agreement.
3. In the list of versions, select **ODAC 12.2.0.1.1 - 431,571,252 bytes - August 6, 2018**, and then click **Download**.
4. On the **Sign in** page, enter the Oracle account username and password that are linked to your organization's Oracle Support Identifier, and then click **Sign in**.
5. After the download is complete, extract the contents of `ODTwithODAC122011.zip` to a temporary folder.
6. Click **setup.exe** to start the installer.
7. Work through each screen in the installer, making sure to select the following:
   - On the **Available Product Components** screen, select the check box for **Oracle Data Provider for .NET**. Clear the check boxes for the other Product Components.
   - On the **ODP.NET (Oracle Data Provider for .NET)** screen, select the check box for **Configure ODP.NET and/or Oracle Providers for ASP.NET at machine-wide level**.

To verify your ODAC installation:

1. In a text editor, open the file **`sqlnet.ora`** in `Oracle_Client_Home\network\admin:`
   - Verify that the sqlnet.authentication_services setting is as follows:

     ```
     sqlnet.authentication_services = (NONE)
     ```
   - If a names.directory_path line, exists, verify that it is commented out by a hash tag character (#):

     ```
     # names.directory_path = (TNSNAMES, EZCONNECT)
     ```
2. Check System > System Properties > Advanced > Environment Variables to verify that the **Path** system environment variable points to `ORACLE_Client_HOME\network\admin`.

   By default, when you upgrade an existing Oracle Client installation, Oracle creates a new Home folder instead of reusing the existing home folder.
3. (Optional) Create an environment variable called `TNS_ADMIN` that points to `ORACLE_Client_HOME\network\admin`.

   > **Note:** To use a Transparent Network Substrate (TNS) alias to connect to the database, you must have a `tnsnames.ora` file. For more information, see the *Oracle Net Services Installation Guide*.
4. Test the network connection to the Oracle database by using SQL*Plus or the SQL Worksheet to execute a test query.

Chapter 2:
Running the Workbook 2021 Installer

After you complete the prerequisite tasks described in Chapter 1: Prerequisite Tasks, you can run the Workbook Installer, **workbook2021.exe**. The Installer helps you perform two sets of tasks:

- **Pre-installation tasks**, which consist of installing any missing prerequisites, entering or importing your configuration data, and testing log-ins, connections, and other functions that use this data.
- **Installation and setup tasks**, which consist of uninstalling your existing Vault Server software (if you are upgrading), running database setup and migration scripts, and then running VaultSetup, the Vault-to-Hub Bootstrapper, and the Vault Deployment Utility.

Tip: Pre-installation tasks can require multiple iterations and troubleshooting. You must enter, test, correct, and re-test configuration data until all tests have passed. Start your pre-installation tasks "n" days before your planned deployment date, where "n" is an adequate amount of time to fix problems with areas such as database schema design, database access, certificates, and so on.

This chapter provides an overview of the series of Workbook Installer screens, and then explains how and when to use each screen. For a more general overview of installation tasks and flowcharts that depict pre-installation, installation, and an important post-installation task, see Installation Overview.

Workbook Installer Screen Overview

The Workbook Installer displays a series of screens for performing different functions.

IMPORTANT! The order of the screens, particularly for upgrades, does **not** reflect the order in which you must execute their functions. Use the **Next** and **Back** buttons to skip and later return to screens like the Uninstallation screen that appear before you are ready to use them.

The following summarizes the screens and their functions:

1. **Various Start-up Screens**. Use them to do the following:
   a. Enter information that the Installer requires to install missing prerequisites, if prompted for such information.
   b. Run the Vault Server uninstaller, if you are upgrading. Skip this screen until you have entered the Workbook configuration data on a later screen, the Installer reports that all tests have passed, and you are ready to install Workbook 2021. Then return to this screen.
   c. Select the version to install.
   d. Extract the setup files.
2. **Workbook Configuration Screen**. Use this screen to perform these pre-installation tasks:
   a. Enter your configuration data, either manually by using the UI, or by importing a configuration file.
   b. Perform tests to determine whether the Installer can successfully use the configuration data.
3. **Database Configuration Screen**. Use this screen to execute a series of database configuration scripts.

   IMPORTANT! If you are upgrading, complete the following tasks before you execute the scripts:
   a. Tasks described in Part C. Perform Final Pre-Installation Tasks (Upgrades Only) on page 22.
   b. Navigate back to the Installer's Uninstall screen and uninstall your existing version of Workbook.
4. **Vault Setup Screen**. Use this screen to run the following:
   - Vault Setup
   - VaultToHubBootstrapper
   - VDU

Part A. Start the Workbook Installer, Select Options, and Extract the Files

Start the Workbook Installer and work your way through its screens to the file extraction screen:

1. In the folder into which you extracted `BIOVIA_Workbook_2021.zip` (by default `C:\BIOVIA\Workbook`), start the Workbook Installer, **`Workbook2021.exe`** by right-clicking and choosing **Run as Administrator**.
2. On the *Welcome* screen click **Next**.
3. If the Installer prompts you for input to install a missing prerequisite, provide the requested input. After all prerequisites are installed, click **Next**.
4. If the **Existing Vault** screen appears, click **Next** to skip it.
   - If you are not finished with pre-installation data entry and testing tasks, click **Next** to skip the uninstallation process and proceed to the Installer's Workbook Configuration screen.

     Also skip uninstallation if you are using the Installer for its configuration testing capabilities, rather than to install or upgrade Workbook.
5. In the *Workbook2021 Installation Setup* screen:
   - In the **Features** tab, select **Workbook2021**.
   - In the **Temporary Folder** tab, browse to the temporary folder in which you extracted `BIOVIA_Workbook_2021.zip`, and then click **Next**.
6. In the *Ready to Install* screen, click **Extract Files**, wait for this extraction process to complete, and then click **Next** and proceed to Part B. Enter and Test Workbook Configuration Data on page 15 .

Tip: The file extraction process does not overwrite existing Workbook configuration files. Consequently, you can re-run the Installer and re-extract files at any time without losing your previously entered configuration data.

Part B. Enter and Test Workbook Configuration Data

After the extraction completes, the Workbook Installer displays the **Workbook Configuration** screen.

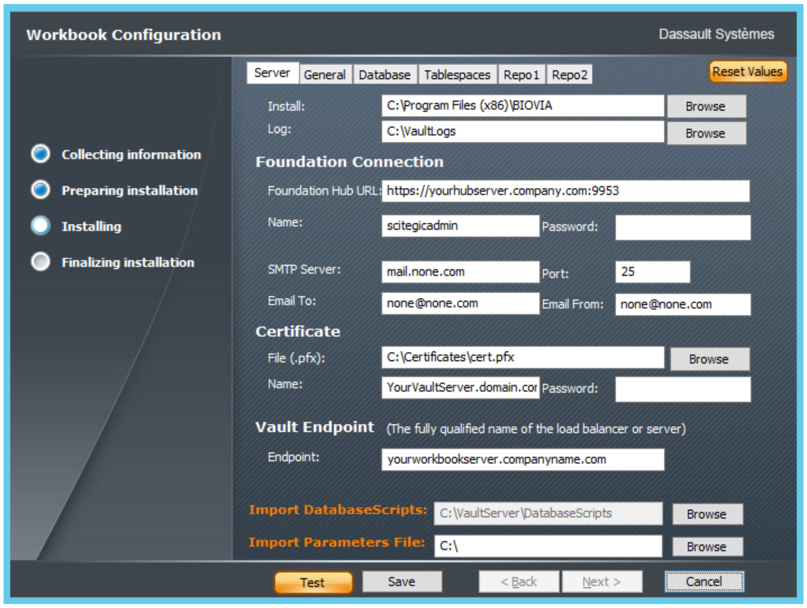
Tips:

- You can click **Save** at any time to save your configuration data. After saving, you can close the Workbook Installer and restart it at a later time without losing the data.
- You can discard your configuration data and recover the default values by clicking **Reset Values**.
- The values you enter in this screen are used in the **`workbook_config.xml`** file.
- For additional details, see Database Configuration Files on page 75.

Manually Entering Workbook Configuration Data

To manually enter configuration data, perform the following steps. To import a configuration file, see Importing Workbook Configuration Data on page 20.

1. On the **Server** tab, configure the following fields:



Install: C:\Program Files (x86)\BIOVIA

Log: C:\VaultLogs

Foundation Hub URL: https://yourhubserver.company.com:9953

Name: scitegicadmin

Password:

SMTP Server: mail.none.com

Port: 25

Email To: none@none.com

Email From: none@none.com

File (.pfx): C:\Certificates\cert.pfx

Name: YourVaultServer.domain.cor

Password:

Endpoint: yourworkbookserver.companyname.com

Import DatabaseScripts: C:\VaultServer\DatabaseScripts

Import Parameters File: C:\

a. In the **Install** field, accept the default `C:\ProgramFiles(x86)\BIOVIA` or browse to a different folder. This folder is referred to in the rest of this guide as the `<install_folder>`.

b. In **Logs**, accept the default `C:\VaultLogs` or browse to a different folder.

c. Under **Foundation Connection**,

- In **Foundation Hub URL**, use the following syntax to specify the HTTPS URL for BIOVIA Foundation Hub or for the load balancer:

  `https://<Fully-qualified server name>:<port_number>`

  The default HTTPS port number is **9953**.

- In **Name** and **Password**, enter the name and password of the administrator account used to log in to Foundation Hub.

- In **SMTP Server**, enter the name of your SMTP server, for example, mail.mycompany.com.

- In **Port**, enter the port number used for the SMTP connection.

- In **Email To**, enter the email address of the Workbook or Vault administrator or administrative user group to notify if certain Vault or RAS issues occur, for example VaultAdmins@mycompany.com.

- In **Email From**, enter the email address to list as the sender of automated notifications, for example VaultServer@mycompany.com

d. Under **Certificate**,

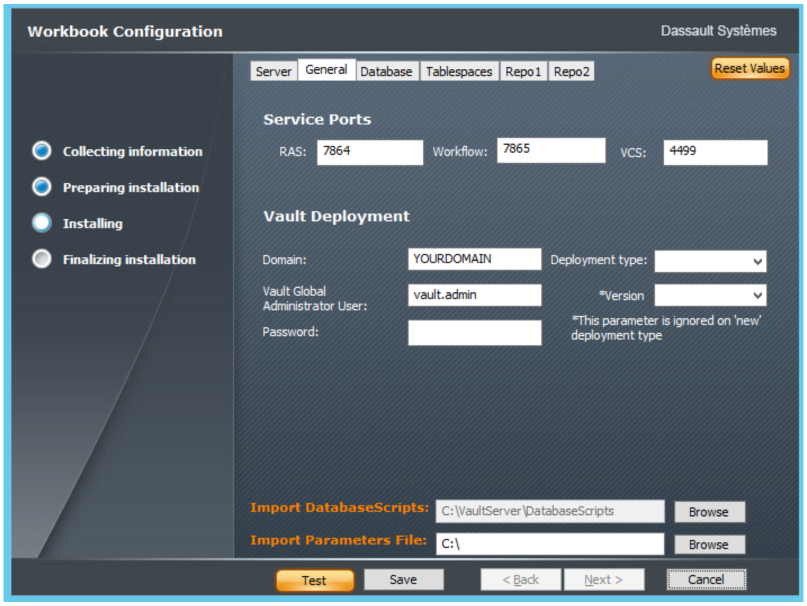
- In **File (.pfx)**, enter the path and name of the Vault Server machine's .pfx certificate file. In a load-balanced configuration, identify the .pfx for the load balancer machine.

- In **Name**, enter the fully-qualified domain name of the Vault Server host machine or virtual machine that users must enter in the Workbook client application's login screen.

- In **Password**, enter the password for the certificate's .pfx file.

e. Under **Vault Endpoint**, in **Endpoint**, enter the same value you entered in the **Name** field under **Certificate**.

2. On the **General** tab, configure the following fields, which correspond to parameters in the `\DatabaseScripts\vaultvariables.siteconfig` file.



Service Ports

RAS: 7864 Workflow: 7865 VCS: 4499

Vault Deployment

Domain: YOURDOMAIN

Deployment type:

Vault Global Administrator User: vault.admin

*Version

*This parameter is ignored on 'new' deployment type

Password:

Import DatabaseScripts: C:\VaultServer\DatabaseScripts

Import Parameters File: C:\

a. Under **Service Ports**, accept the default values for **RAS**, **Workflow**, and **VCS** (Tomcat Vault Client Service).

   The wizard checks for conflicts when you click either **Save** or **Install**. If a conflict is reported, select another port and save again.

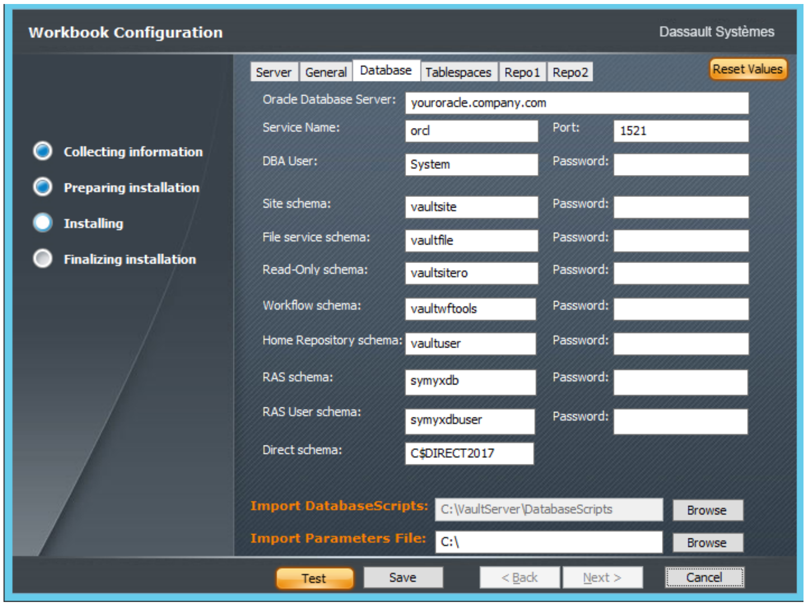
b. Under **Vault Deployment**, in **Domain**, replace the default domain with the domain name to use for your installation.

c. In **Vault Global Administrator Account** and **Password**, enter the name and password of the Vault Global Administrator.

   This account must exist in Foundation Hub and must be a member of a Foundation Hub group that has the **Foundation|Logon** permission. For more information, see Create a Vault Admin Account and Add it to Foundation Hub (New Installs Only) on page 9.

d. In **Deployment Type**, select **New** or **Upgrade**. If you are upgrading, you must also select the correct **Version** from which you are upgrading.

3. On the **Database tab,** configure the following fields, which correspond to parameters used by the following database configuration files:
   - `variables.db.config`
   - `vaultvariables.siteconfig`
   - `variables.RAS.config`
   - `variables.fileservice.config`
   - `vaultvariables.wftools.config`



Oracle Database Server: youroracle.company.com

Service Name: orcl   Port: 1521

DBA User: System   Password:

Site schema: vaultsite   Password:

File service schema: vaultfile   Password:

Read-Only schema: vaultsitero   Password:

Workflow schema: vaultwftools   Password:

Home Repository schema: vaultuser   Password:

RAS schema: symyxdb   Password:

RAS User schema: symyxdbuser   Password:

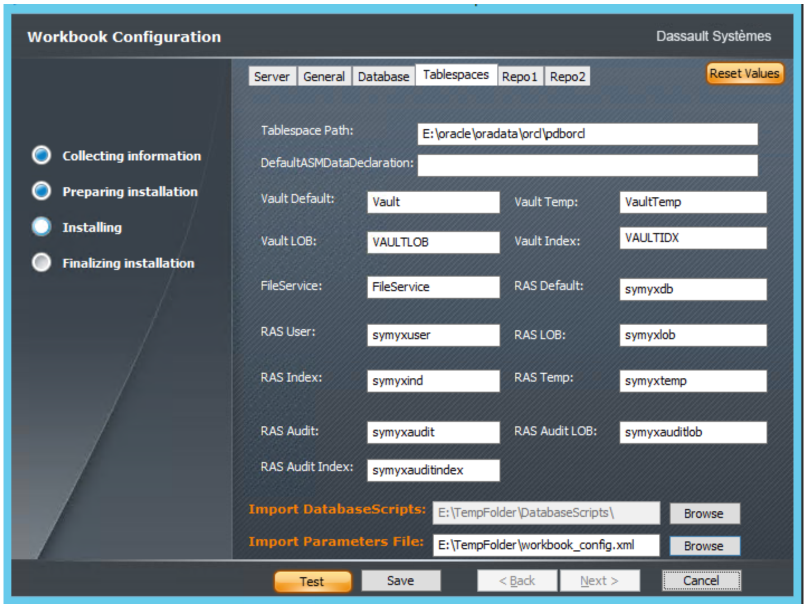
Direct schema: C$DIRECT2017

Import DatabaseScripts: C:\VaultServer\DatabaseScripts

Import Parameters File: C:\

   a. In the **Oracle Database Server** field, enter the Oracle server name.
   b. In **Service Name**, enter the name that clients can use to connect to the database.
   c. In **Port**, enter the port number of the database connection.
   d. In **DBA User** and **Password**, enter the name and password of the Vault database administrator.
   e. In **Site schema** and **Password**, enter the name and password of the Site schema account, for example, vaultsite.
   f. In **File service schema** and **Password**, enter the name and password of the **File Service Schema** account, for example, vaultfile.
   g. In **Read-Only schema** and **Password**, enter the name and password of the Site read-only user, for example, vaultsitero.
   h. In **Workflow** and **Password**, enter the name and password of the Workflow account, for example, vaultwftools.
   i. In **Home Respository schema** and **Password**, enter the name and password of the home repository schema account, for example, vaultuser.
   j. In **RAS schema** and **Password**, enter the name and password of the RAS schema user, for example, symyxdb.
   k. In **RAS User schema** and **Password**, enter the name and password of the RAS user account, for example, symyxdbuser.
   l. In **Direct schema**, enter the name of the Direct user account.

4. On the **Tablespaces** tab, configure the following fields, which correspond to parameters in `\DatabaseScripts\variables.setup.config`.



Tablespace Path: E:\oracle\oradata\orcl\pdborcl

DefaultASMDataDeclaration:

Vault Default: Vault

Vault Temp: VaultTemp

Vault LOB: VAULTLOB

Vault Index: VAULTIDX

FileService: FileService

RAS Default: symyxdb

RAS User: symyxuser

RAS LOB: symyxlob

RAS Index: symyxind

RAS Temp: symyxtemp

RAS Audit: symyxaudit

RAS Audit LOB: symyxauditlob

RAS Audit Index: symyxauditindex

Import DatabaseScripts: E:\TempFolder\DatabaseScripts\

Import Parameters File: E:\TempFolder\workbook_config.xml

a. In the **Tablespace Path** field, enter the Oracle data files path. Use forward slashes for Linux servers.

b. In **DefaultASMDataDeclaration**, enter the ASM Data Declaration.

> **Note:** If the ASM Data Declaration is specified, it will overwrite the existing Tablespace Path field. If the Tablespace Path is blank, the ASM Data Declaration is required.

c. In **Vault Default**, enter the name of the default Vault tablespace, for example, Vault.

d. In **Vault Temp**, enter the name of the Vault temporary tablespace, for example, VaultTemp.

Some users find it best to use the standard TEMP tablespace.

e. In **Vault LOB**, enter the name of the Vault LOB tablespace, for example, VAULTLOB.

f. In **Vault Index**, enter the name of the Vault index tablespace, for example, VAULTIDX.

g. In **FileService**, enter the name of the Vault FILE tablespace, for example, FileService.

h. In **RAS Default**, enter the name of the default RAS tablespace, for example, symyxdb.

i. In **RAS User**, enter the name of the RAS user tablespace, for example, symyxuser.

j. In **RAS LOB**, enter the name of the RAS LOB tablespace, for example, symyxlob.

k. In **RAS Index**, enter the name of the RAS index tablespace, for example, symyxind.

l. In **RAS Temp**, enter the name of the temporary RAS tablespace, for example, symyxtemp.

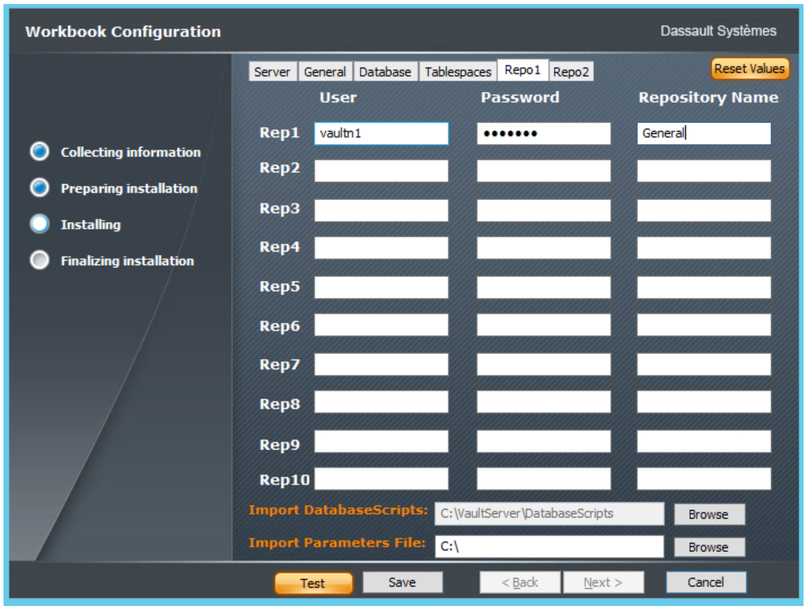
Some users find it best to use the standard TEMP tablespace.

m. In **RAS Audit**, enter the name of the RAS audit tablespace, for example, symyxaudit.

n. In **RAS Audit LOB**, enter the name of the RAS audit tablespace for the LOB tablespace, for example, symyxauditlob.

o. In **RAS Audit Index**, enter the name of the RAS audit tablespace for the index tablespace, for example, symyxauditindex.

5. If needed, on the **Repo1** and **Repo2** tabs, configure the following fields, which correspond to versioned Vault repository parameters in `\DatabaseScripts\variables.nb#.config`.



	User	Password	Repository Name
Rep1	vaultn1	•••••••	General

Import DatabaseScripts: C:\VaultServer\DatabaseScripts

Import Parameters File: C:\

a. In the **Rep1 - Rep 10** rows, enter the user name, password, and repository name for up to ten versioned repositories.

IMPORTANT! You cannot use the single quote (') character in the Repository Name field.

b. To configure up to ten more repositories, use the **Repo2** tab.

6. Proceed to Saving and Testing Workbook Configuration Data on page 21.

Importing Workbook Configuration Data

To import an existing configuration file, for example `C:\VaultConfig<server>.parameters` or `workbook_config.xml`, perform the following steps. To manually enter the data, see Manually Entering Workbook Configuration Data on page 15.

1. On the **Server** tab in the Workbook Installer's Workbook Configuration screen, click **Browse** next to **Import Parameters File**, and find and select the file. When prompted for the password, enter the password for Foundation.

2. Click the **General** tab and enter the following values under **Vault Deployment**:

   a. For **Password**, enter the password of the Vault Global Administrator.

   b. In **Deployment Type**, select **New** or **Upgrade**. If you are upgrading, you must also select the correct **Version** from which you are upgrading.

3. Click the **Database** tab and make any needed changes to the parameter values for the database configuration files.

   a. For **Password**, enter the password for Oracle.

4. Click the **Tablespaces**, **Repo1**, and **Repo2** tabs, and make any necessary changes.

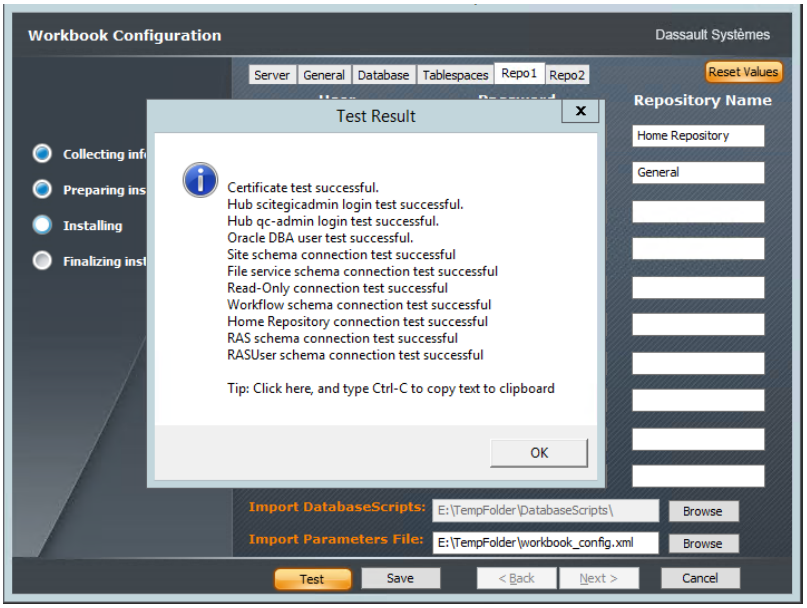
> **Note:** If the ASM Data Declaration is specified, it will overwrite the existing Tablespace Path field. If the Tablespace Path is blank, the ASM Data Declaration is required.

5. Proceed to Saving and Testing Workbook Configuration Data on page 21.

Saving and Testing Workbook Configuration Data

After you enter or import the configuration data, save and test it:

1. Review each tab, correct any incorrect values, and then click **Save**. The Workbook Installer saves the values in the `workbook_config.xml` file.
2. Click **Test** and review the results.
   - The Workbook Installer conducts several tests, verifies that the Foundation Administrator can securely log in to Foundation, and then displays the name and result for each test that it conducts.
   - If a test fails, correct the relevant parameters, save your corrections, and then click **Test** again. Repeat until the **Test Result** message lists each test as successful.



Test Result

```
Certificate test successful.
Hub scitegicadmin login test successful.
Hub qc-admin login test successful.
Oracle DBA user test successful.
Site schema connection test successful
File service schema connection test successful
Read-Only connection test successful
Workflow schema connection test successful
Home Repository connection test successful
RAS schema connection test successful
RASUser schema connection test successful

Tip: Click here, and type Ctrl-C to copy text to clipboard
```

Repository Name: Home Repository; General

Import DatabaseScripts: E:\TempFolder\DatabaseScripts\

Import Parameters File: E:\TempFolder\workbook_config.xml

3. If you are performing an upgrade, perform the steps in Part C. Perform Final Pre-Installation Tasks (Upgrades Only) on page 22.

   Otherwise skip to Part D. Perform the Installation Tasks on page 23.

Part C. Perform Final Pre-Installation Tasks (Upgrades Only)

Before you start the uninstallation and installation steps of an upgrade, perform these steps:

1. Ensure that users have checked in their experiments and logged out of Workbook.
2. Open the Windows Server Manager and choose **Configuration > Services**, and stop the Vault services in the following order:
   - Vault Client Service
   - Vault Hub Synchronization Service
   - Vault Message Processing Service
   - Vault Workflow Service
   - Vault Tomcat Server Service
3. Back up your entire Vault database, including Vault and RAS data.

   > **Note:** Backing up the database requires privileges to use Oracle export utilities or other backup software.

4. Move all existing log files from `C:\VaultLogs` to a different folder.

   When you upgrade, new empty logs are created in the `C:\VaultLogs` folder.
5. Use the Workbook Installer to uninstall your existing Vault Server software:
   a. Navigate to the Installer's **Existing Vault** screen and click **Uninstall Existing Vault**.
   b. In the *Uninstall* screen, click **Uninstall**.
   c. Click **Finish** and then click **Next**.
   d. Click **Show Logs** and examine the uninstall log, `<temp_install_folder>:\VaultLogs\Uninstall.log`.
6. Proceed to Part D. Perform the Installation Tasks on page 23.

Part D. Perform the Installation Tasks

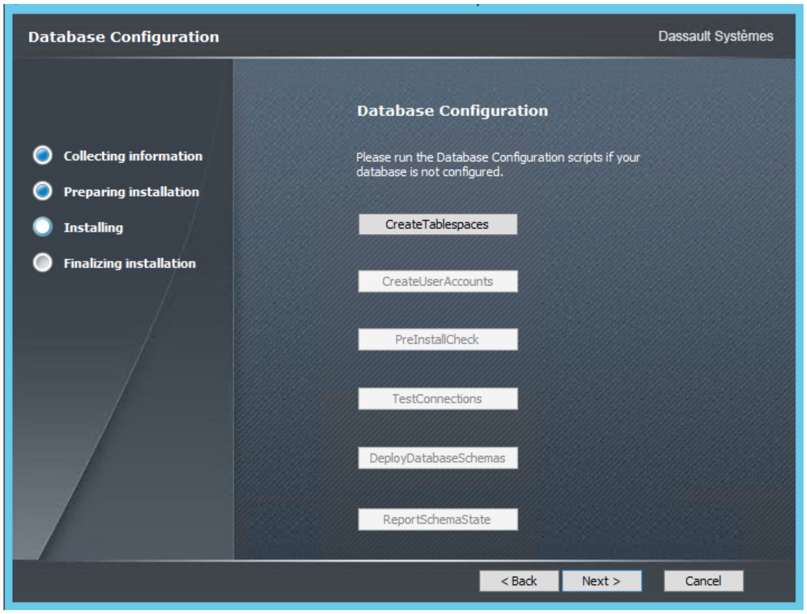
The installation tasks include running the database scripts and running Vault Setup, the Vault-To-Hub Bootstrapper, and VDU.

You can use the Workbook Installer to perform these tasks manually. Alternatively, you can run `WorkbookSilentInstall.bat`, which executes them in a mode that requires no user intervention.

Performing the Installation Tasks Using the Workbook Installer

To use the Workbook Installer to perform the installation tasks, follow these steps. To use a batch file, skip to Performing the Installation Tasks Using the Silent Installer on page 25.

1. Run each script listed on the **Database Configuration** screen. Each script must finish before you can execute the next one.



Please run the Database Configuration scripts if your database is not configured.

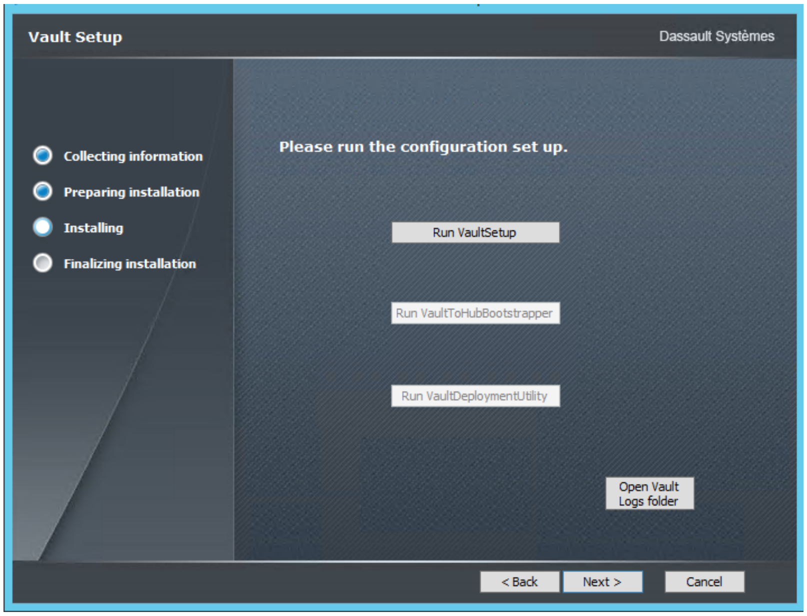
   a. Monitor the command window used to run each script and press any key when prompted to continue.

   b. View the log file for each script. The Workbook Installer displays the log file in your default text editor.

   > **IMPORTANT!** If your default text editor is Notepad++, your system might hang when you attempt to close a log file and start the next script. If this happens, close all open tabs in Notepad++, change your default text editor, and then rerun the script.

   c. If the Installer displays a red "X" next to a script, correct the errors identified in the log file and then rerun the script. You cannot continue until the green "Success" check mark appears.

d. After all scripts have successfully completed, click **Next** to proceed to the **Vault Setup** screen.



2. On the **Vault Setup** screen, execute each option and ensure that a green "Success" check mark instead of a red "X" appears next to the option. Each option can take several minutes to run.

   If an option fails, click **Open Vault Logs folder**, find the error in the relevant log file, resolve it, and then rerun the option. The log files are:

   - `Install.log`
   - `VaultToHubBootstrapper.Debug.log`
   - `Vault Deployment Utility.Debug.log`

     This log identifies password errors and other types of errors. To resolve password errors, return to the Workbook Configuration screen and ensure that the **Vault Global Administrator** password entered on its **General** tab is correct. If the password is correct, ensure that it does not contain any special characters. The Workbook Installer cannot install the Vault Deployment Utility if this password uses special characters, but you can run it without using the Installer.

     For more information, see Create a Vault Admin Account and Add it to Foundation Hub (New Installs Only) on page 9 and Manually Running the Vault Deployment Utility on page 83.

3. After the Vault Deployment Utility completes successfully, click **Next**.
4. In the *Workbook 2021 Setup Complete* screen:

   a. Read any messages about post-installation steps. For details, see the next chapter.

   b. Ignore **Clear dead messages** and click **Finish**.

Performing the Installation Tasks Using the Silent Installer

Exit the Workbook Installer and perform the following steps to start the silent installer, which installs Vault Server without the need for user intervention.

1. Open a command-line prompt and change directories to the folder to which you extracted `BIOVIA_Workbook_2021.zip`.
2. Execute the following command:

```
 WorkbookSilentInstall.bat -config C:\temp\workbook2021
\workbook_config.xml
```

Chapter 3:
Post-Installation Tasks

Perform the post-install tasks described in this chapter after you do either of the following:

- Create a new installation of Workbook2021.
- Upgrade an earlier Workbook installation to Workbook2021.

Both upgrades and new installs require all tasks in this chapter, except those marked **Upgrade Only** or **New Installs Only**. Even with an upgrade, however, ensure that the configuration is still valid.

These tasks are required for all installation methods: Workbook Installer, silent, and Ansible.

Verify the Vault Server Installation

Perform the following steps to verify that Vault Server was successfully installed:

1. Verify that the Vault Web Service and the Vault Web Private Service were successfully installed:

   a. Select **Apps > BIOVIA > Vault Web Service** and verify that a web page titled **"VaultServerService" Service** displays and does not report errors.

   b. Select **Apps > BIOVIA > Vault Web Service Vault Web Private Service** and verify that a web page titled **"VaultServerPrivateService" Service** displays and does not report errors.

   > **Note:** The URLs for both web services include the /6.6/ node regardless of which version is installed.

2. Verify that the Deployment Manager was successfully installed:

   Select **Apps > BIOVIA > Deployment Manager** and verify that the Deployment Manager (DM) web page opens and does not report any errors.

3. Verify that the RAS Service was successfully installed:

   a. In Internet Explorer, navigate to **Tools > Internet Options**, click the **Security** tab, and set **Internet security** to **Medium-High**.

   b. Select **Apps > BIOVIA > Vault RAS Status** and verify that a web page titled "Renaissance Application Server" is displayed.

Assign Deployment Profiles to Users

The Workbook installation step that runs the VDU publishes three new deployment profiles that all use the same new deployment package.

- For new installations, the offline profile is assigned to all users by default so that all users can log in. An administrator can update the ADM rules to assign different profiles to different groups of users.
- For upgrades, the VDU does not alter the profile assignments. Users continue to receive their previously assigned profile until an administrator updates the ADM rules.

> **IMPORTANT!**
>
> - For some releases, previous packages are incompatible with the upgraded Vault server. Consequently, the ADM rules must be reassigned before users can log in.
> - If you use an ADM package that includes different assemblies or run-time redirects, then you must reapply these customizations to the new ADM package.

For more information, see the *Workbook Deployment Manager Guide*.

Enable Full-text Searching on Linux Servers

> **Note:** In BIOVIA Workbook, full-text searching in both an embedded file section and in the spreadsheet section does not work on a database server that uses the Linux x86-64 system.

To enable full-text searching on a Linux-based server:

1. Modify the LD_LIBRARY_PATH using one of the following:

   For C Shell (csh or tcsh):

   ```
   setenv LD_LIBRARY_PATH $ORACLE_HOME/ctx/lib:$LD_LIBRARY_PATH
   ```

   For Bourne shell (sh), Bash shell (bash), or Korn shell (ksh):

   ```
   export LD_LIBRARY_PATH=$ORACLE_HOME/ctx/lib:$LD_LIBRARY_PATH
   ```

   For example:

   ```
   LD_LIBRARY_
   PATH=/app/oracle/product/11.2.0.4/ctx/lib:/app/oracle/product/11.2.0.4/l
   ib32:/opt/ Symyx/direct90/bin11
   ```

2. Run the following command to verify that the LD_LIBRARY_PATH environmental variable is set correctly:

   ```
   echo $LD_LIBRARY_PATH
   ```

3. Restart both the Oracle database and the listener.

Install the BIOVIA Workbook Client

For new installations, install the BIOVIA Workbook Client on your users' client systems, as described in the *BIOVIA Workbook Client Installation Guide.*

If you are upgrading, check the *Vault Server System Requirements* to determine whether upgrading your client systems is required. Most releases of Vault Server are backward-compatible with earlier releases of the Workbook Client.

Import Workbook Example Templates

To enable Workbook users to use example experiment templates supplied with Workbook, import the `.voexp` files for the templates that you want to make available. Each `.voexp` file contains a set of example templates.

> **Note:** For upgrades, skip this step unless the new release contains new or updated templates that you want to use. Consult the *Product Release Document* (PRD) for more information.

To import the `.voexp` files:

1. Log in to Workbook using an account that has Templates Transfer permission.
2. Create a destination folder in which to store the templates, for example `WorkbookDefaultTemplates2021`.
3. In Notebook Explorer, click **Create** > **Import** > **From voexp** and navigate to the following folder:

   \<install_folder>VaultDeploymentUtility\ExperimentTemplates

   where <install_folder> is the folder in which the Workbook Vault Server components were installed (by default, `C:\Program Files (x86)\BIOVIA\WorkbookInstall`).
4. In the **Import** dialog,
   a. Click the **Action** column.
   b. Select the first `.voexp` file below, select your destination folder, and click **Import**.
      - AnalyticalChemistryTemplates
      - CIMSTemplates
      - CISProTemplates
      - ExternalDocumentConversionTemplates
      - FormulationTemplates
      - NotebookExampleTemplates
      - SyntheticChemistryTemplates

   c. Repeat for `.voexp` file that contains templates you want.

Install BIOVIA Workflow Designer (Optional)

BIOVIA Workflow Designer enables you to create and publish custom workflows for BIOVIA Workbook users.

For installation instructions, see Installing and Uninstalling Workflow Designer on page 72.

Change Settings in the Lookup Service (Optional)

Enter Your Database Web Service License Key (Optional)

If you want Workbook users to be able to import chemical names and structures from the BIOVIA DiscoveryGate Database Web Service, replace its placeholder license key in the Lookup Service application permission.

Tip: To use a command-line utility to add or update permission configurations for services and applications, see "Using the Import/Export Application Permissions Utility" in the *Vault Server Administration Tools Guide*. The command-line utility enables you to easily export all editable application permissions, edit them using a text editor, tokenize them for use on more than one Vault Server if needed, and then re-import them into the same or a different Vault Server.

To use the Vault Administration Console to enter your Database Web Service license key:

1. Open the Vault Administration Console and log on to Vault Server as a member of the Vault Global Administrators group.
2. Expand the server node and select **Application Permissions**.
3. Double-click **LookupService**, and then click the **Configuration** tab.
4. In the **ResolverXML** row, click the **Value** column.
5. In the configuration file editor, replace the placeholder license key (`DG_LICENSE KEY_NEEDED`) with your own license key, and then click **OK** to save your changes.

```
<Configuration>
  <Property
name="URL">https://www.discoverygate.com/webservice/1.2/DGWS</Property>
  <Property name="MoleculeFlags">IDENTIFICATION,PROCUREMENT_
PROPERTIES,SOURCE_SUMMARY</Property>
  <Property
name="QueryProperties">Material.Name,Material.Structure,TestPropertySet.
CASNumber</Property>
  <Property name="ReplaceExistingPropertyValues">True</Property>
  <Property name="MaxNumberResults">10</Property>
  <Property name="LicenseKey">DG_LICENSE KEY_NEEDED</Property >
  <Property name="DataSourceOrder">CHEMSEEK, ACD, CINDEX</Property>
</Configuration >
```

6. Exit the Vault Administration Console.

Change the Resolver Order in the Lookup Service (Optional)

By default, the DiscoveryGate Database Web Service resolver is used before the OpenEye resolver, the data is filtered, and only unique result sets are displayed. You can change this order to use the OpenEye resolver first, so that the name and structure are retrieved with OpenEye, and molweight and formula are computed using Cheshire scripts on the Material Property Structure change event.

Tip: To use a command-line utility to add or update permission configurations for services and applications, see "Using the Import/Export Application Permissions Utility" in the *Vault Server Administration Tools Guide*. The command-line utility enables you to easily export all editable application permissions, edit them using a text editor, tokenize them for use on more than one Vault Server if needed, and then re-import them into the same or a different Vault Server.

To use the Vault Administration Console to change the default order of resolvers, perform the following steps:

1. Open the Vault Administration Console and log on to Vault Server as a member of the Vault Global Administrators group.
2. Expand the Vault Server node and select **Application Permissions**.
3. In the **LookupService| MaterialInfoManager Properties** dialog, select the **Configuration** tab.
4. Click the **Value** column of the **ResolverXML** row.
5. Copy and paste the contents of the ResolverXML into a text editor. The default XML is similar to the following:

```
<?xml version='1.0' encoding='utf-8'?>
<MaterialInfoLookUp>
  <Resolver name= 'Symyx.Notebook.DiscoveryGateMaterialInfoLookup.
   RefDataWebServices.DiscoveryGateWebServiceResolverWithMolName,
   Symyx.Notebook.DiscoveryGateMaterialInfoLookup,
   Version=6.9.0.xxx, Culture=neutral,
   PublicKeyToken=fb4b5791c48b7e8a'>
  </Resolver>
  <Resolver name='Symyx.Framework.MaterialInfoLookup.
   OpenEye.OpenEyeResolver, Symyx.Framework.MaterialInfoLookup,
   Version=6.9.0.xxx, Culture=neutral,
   PublicKeyToken=fb4b5791c48b7e8a'>
  </Resolver>
</MaterialInfoLookUp>
```

6. Swap the positions of the OpenEye element and DiscoveryGate elements the file:

```
<?xml version='1.0' encoding='utf-8'?>
<MaterialInfoLookUp>
  <Resolver name='Symyx.Framework.MaterialInfoLookup.
   OpenEye.OpenEyeResolver, Symyx.Framework.MaterialInfoLookup,
   Version=6.9.0.xxx, Culture=neutral,
   PublicKeyToken=fb4b5791c48b7e8a'></Resolver>
  <Resolver name='Symyx.Notebook.DiscoveryGateMaterialInfoLookup.
   RefDataWebServices.DiscoveryGateWebServi ceResolverWithMolName,
   Symyx.Notebook.DiscoveryGateMaterialInfoLookup,
   Version=6.9.0.xxx, Culture=neutral,
   PublicKeyToken=fb4b5791c48b7e8a'></Resolver>
</MaterialInfoLookUp>
```

7. Remove the extra spaces or blank lines from the end of the XML string.
8. Copy and paste the updated configuration file into the Value box of the ResolverXML row.
9. Click **OK** to save your changes.
10. Click **OK** to close the dialog.

For more information about the Lookup Service, contact Dassault Systèmes Customer Support.

Change the Data Source Search Order (Optional)

The default search order for the DiscoveryGate Database Web Service resolver is:

1. CHEMSEEK
2. ACD

You can reverse this order, if needed.

> **Tip:** To use a command-line utility to add or update permission configurations for services and applications, see "Using the Import/Export Application Permissions Utility" in the *Vault Server Administration Tools Guide*. The command-line utility enables you to easily export all editable application permissions, edit them using a text editor, tokenize them for use on more than one Vault Server if needed, and then re-import them into the same or a different Vault Server.

To use the Vault Administration Console to change the default search order, perform the following steps:

1. Open the Vault Administration Console and log on to Vault Server as a member of the Vault Global Administrators group.
2. Expand the Vault Server node and select **Application Permissions**.
3. In **Application Permissions**, double-click **LookupService**.
4. In the **LookupService| MaterialInfoManager Properties** dialog, click the **Configuration** tab.
5. Click the **Value** column of the `Symyx.Notebook.DiscoveryGateMaterialInfoLookup.RefDataWebServices.DiscoveryGateWebServiceResolverWithMolName` row.
6. Open the XML configuration file and scroll to the `Configuration` section:

```
<?xml version="1.0" encoding="UTF-8"? > < MaterialInfoResolver
name="DiscoveryGate">
.
.
.
<Configuration>
<Property
name="URL">https://www.discoverygate.com/webservice/1.2/DGWS</Property>
<Property name="MoleculeFlags">IDENTIFICATION,PROCUREMENT_
PROPERTIES,SOURCE_SUMMARY</Property>
<Property
name="QueryProperties">Material.Name,Material.Structure,TestPropertySet.
CASNumber</Property>
<Property name="ReplaceExistingPropertyValues">True</Property>
<Property name="MaxNumberResults">10</Property>
<Property name="LicenseKey">DG_LICENSEKEY_NEEDED</Property>
<Property name="DataSourceOrder">CHEMSEEK, ACD, CINDEX</Property>
</Configuration>
</MaterialInfoResolver>
```

7. Change the setting of the `DataSourceOrder` property to put CHEMSEEK before ACD:

```
<Property name="DataSourceOrder">ACD, CHEMSEEK, CINDEX< /Property >
```

8. Save and close the XML file.

Configure Pipeline Pilot Server Settings

This section explains how to configure Pipeline Pilot Server for use with Workbook.

Configuring Pipeline Pilot Global Properties (New Installs Only)

Set the ConfigFilePath property in Pipeline Pilot:

1. Log in to the Pipeline Pilot Administration Console.
2. Select **Setup > Global Properties**.
3. In the Package list, select **BIOVIA Workbook** and note the **ConfigFilePath**.
4. Change the location of ConfigFilePath to the following:
   `<pps_install>\apps\scitegic\notebook\dataroot\`
5. Click **Update**.

Granting Permissions for Pipeline Pilot Integration (New Installs Only)

The Vault/Users group requires five permissions to support Workbook's integrated Pipeline Pilot features. If these permissions are missing, Workbook users cannot run any protocols in custom scripts, export the audit history, or use the **Analyze** tab.

Assign the required permissions as follows:

1. Log in to the Foundation Hub.
2. Add the **Vault/Users** group to the **Foundation/Everyone** group, so that Vault/Users group members inherit the required permissions from the **Foundation/Everyone** group:
   - Platform/Logon
   - Platform/PipelinePilot/Logon
   - Platform/RunProtocol
   - Platform/WebPort/Logon
3. Add the remaining required permission, **Vault/RunProtocol**, to the **Vault/Users** group.

Configuring Pipeline Pilot RunProtocol Settings (New Installs Only)

To enable Workbook users to run standard and customer-specific Pipeline Pilot protocols, you must configure the `RunProtocol` application permission.

Tip: To use a command-line utility to add or update permission configurations for services and applications, see "Using the Import/Export Application Permissions Utility" in the *Vault Server Administration Tools Guide*. The command-line utility enables you to easily export all editable application permissions, edit them using a text editor, tokenize them for use on more than one Vault Server if needed, and then re-import them into the same or a different Vault Server.

To use the Vault Administration Console Console to configure the Pipeline Pilot Client `RunProtocol` settings, perform the following steps:

1. Open the Vault Administration Console and log on to Vault Server as a member of the Vault Global Administrators group.
2. Expand the Vault Server node and select **Application Permissions**.
3. In **Application Permissions**, select the `PipelinePilot.RunProtocol` permission, and click **Properties**.

4. In the **PipelinePilot.RunProtocol** dialog, select the **Configuration** tab.
5. For the **Value** of the **Endpoint**, type the HTTPS URL for the fully-qualified domain name for the Pipeline Pilot server, for example: `https://<`*`fully-qualified PipelinePilot_server_name`*`>:9943`.

Re-registering the Pipeline Pilot Application (Upgrades, Only)

After an upgrade, ensure that the Pipeline Pilot application version is re-registered in Foundation Hub to reflect the new version of Pipeline Pilot.

If has not been re-registered, the audit history and other features in Workbook will fail.

Creating the Vault Site and RAS Data Source

To create the Vault Site and the RAS data source:

1. Log in to the BIOVIA Pipeline Pilot Administration Portal.
2. In Admin Pages, select **Setup** > **Data Sources**.
3. Click **Add Data Source**.
4. In **Name**, enter **RAS**.
5. In **Description**, type a description of the data source.
6. From the **Type** list, select **ODBC (PP)** as the connection option.
7. From the **Driver** list, select **Oracle**.
8. From the **Driver Version** list, select **Latest**.
9. In **Server**, enter the fully-qualified domain name of the Oracle database server.
10. In **Port**, enter the port number of the Oracle database server.
11. In **Service Name**, enter the name of the Oracle database service.
12. In **DB Username**, enter the name of the RAS User schema owner (for example, symyxdbuser).

    Note: The Optional DB Username and Optional DB Password are required.

13. In **DB Password**, enter the password associated with the user name.
14. Click **Save**.
15. To verify that the data source is valid, click **Test**.
16. Repeat steps 3 through 15 to create a data source named **VAULT_SITE**. For the **DB Username**, and password, use the credentials for the Vault site read-only schema owner (for example, vaultsitero).

Configuring Users, Groups, and Permissions in Foundation Hub

After Vault Server 2021 is installed, use BIOVIA Foundation Hub to configure users, groups, and permissions for the Vault Server and Workbook client users.

For more information, see Configuring Workbook User Accounts, Groups, and Permissions on page 80.

Integrating Workbook with Other BIOVIA Products

See the following appendices for information about integrating Workbook with other BIOVIA products, if needed for your site.

- Integration with BIOVIA Chemical Registration on page 41
- Integration with BIOVIA CISPro on page 49

Appendix A:
Configuring Load Balanced Environments

About Vault Server Load Balancing

A load balanced or web farm configuration consists of a load balancer and multiple servers. The load balancer is a virtual server that is shared by all other servers, and that acts as a reverse proxy to distribute network and application traffic across the servers in the farm. Load balancers increase capacity (concurrent users) and reliability of applications.

Workbook requires the following server components, all of which can be load balanced:

- BIOVIA Vault Server
- BIOVIA Pipeline Pilot Server
- BIOVIA Foundation Hub

For information about load balancing Pipeline Pilot Server and Foundation Hub, see the following:

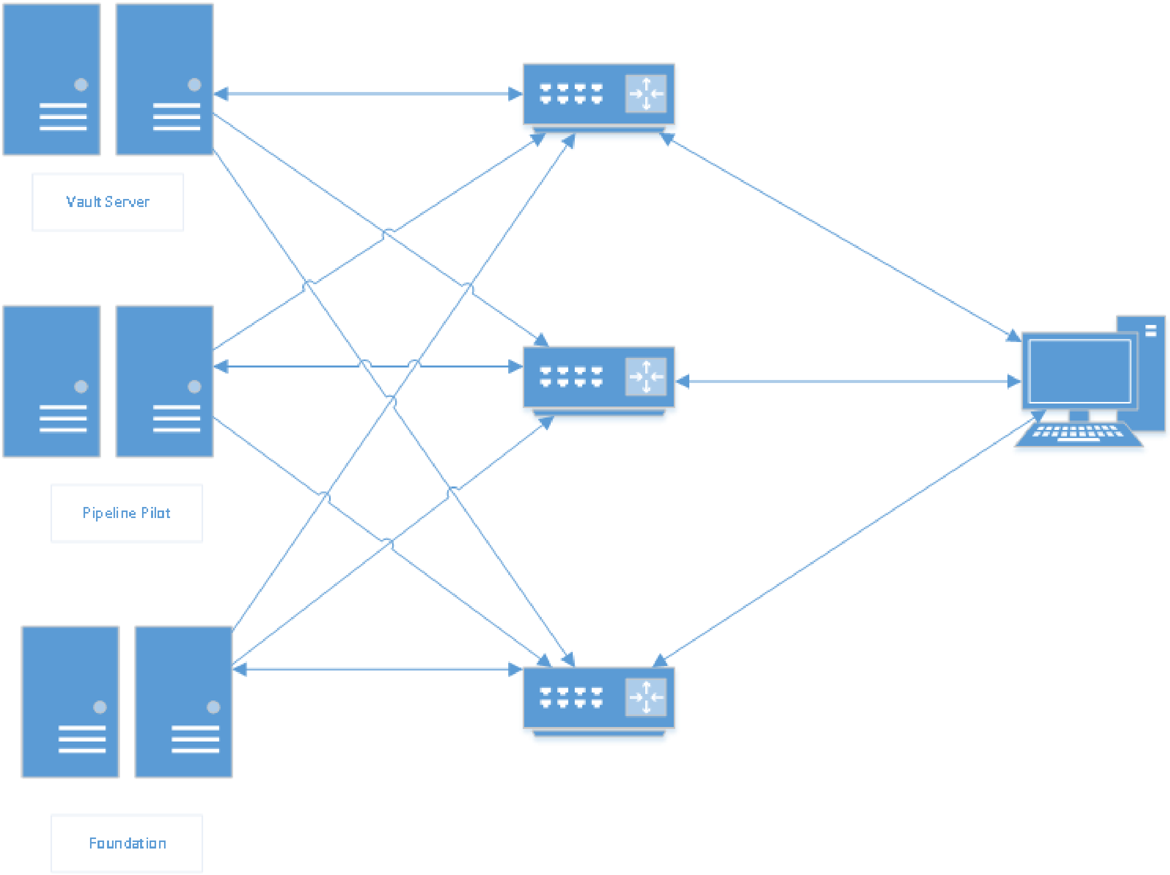
- *Pipeline Pilot Server Installation Guide*
- *Pipeline Pilot Server Deployment Guide*
- *Foundation Hub Installation Guide*

All servers that will be load balanced must have equivalent configurations and must be secured with SSL using TLS 1.2 and strong cryptography.

BIOVIA recommends you employ the following load-balanced configuration.

Example Configuration:

Install each component on separate servers – a Pipeline Pilot server, a Vault server, and a Foundation Hub server. Each server type requires a separate load-balancer address.



Contact Dassault Systèmes Customer Support for advice about which configuration is best for your environment.

Load balancing is complex and can result in functional or performance problems.
Verify that Workbook, Foundation Hub, Pipeline Pilot, and are working correctly with good performance before you implement load-balancing.

Load Balancer Prerequisites

Requirement	Description
Port information	You must know the ports used by Vault Server, Foundation Hub, and Pipeline Pilot. Vault Server uses ports 80, 443, 4499, and 7864. Pipeline Pilot Server uses ports 9944 and 9943. Foundation Hub uses port 9953, 9954, and 9955. If you do not know the port numbers configured on your system, see Viewing the Port Numbers Used by Vault Server on page 82.
Load balancers	Verify that the load balancers ports are open.
Certificates	Obtain a certificate from a trusted Certificate Authority (CA) for the load balancer. Foundation Hub, Vault Server, and the Pipeline Pilot instances use the certificate for SSL communication using TLS 1.2. ■ Use the fully-qualified domain name (FQDN) in the certificate for the server, for example, `mynotebook.mycompany.com`. ■ Make the certificate available as a Personal Information Exchange (PFX) file in the PKCS #12 format and obtain the file's password.
Certificate Store	Install the certificates in the local computer Trusted Root certificate store on each server. For information, see Importing a SSL Certificate PFX File into the Trusted Root Store on page 79.

Shared Folder Location	Create a shared folder on your network and ensure that all Pipeline Pilot Servers that you will configure for load balancing can access it. Create subfolders for the **User**, **Jobs**, and **Shared Public Directory** Pipeline Pilot directories. For example:
	`\\networkshares\shareduser`
	`\\networkshares\sharedjob`
	`\\networkshares\sharedpublic`
	Do not use a shared folder for the Pipeline Pilot XMLDB. The XMLDB directory stores protocols and components specific to the server. For more information, see the Pipeline Pilot Help Center's Server Maintenance topics under **Managing the XMLDB** and the Load Balancing Pipeline Pilot chapter in the *Pipeline Pilot Server Installation Guide*.

Configuring Vault Server to Use Load-Balanced Foundation Hub and Pipeline Pilot Server Environments

> **Note:** In these instructions, `<installation_directory>` indicates the BIOVIA Vault Server installation location. The default location is `C:\Program Files (x86)\BIOVIA\Vault`.

To configure Vault Server to use load-balanced Pipeline Pilot Server and Foundation Hub environments:

1. Stop Vault services. See Stopping the Vault Services on page 73.
2. Verify that you can log in to Pipeline Pilot using the load-balancer URL for Foundation Hub.
3. Configure each Vault Server machine to use the load-balanced URL for Foundation Hub authentication by editing the following configuration files on each machine:
   - `<installation_directory>\WebService\web.config`
   - `<installation_directory>\DeploymentManager\web.config`
   - `<installation_directory>\Rest\web.config`

   a. Back up each file.

   b. Change the `uri` value in each file to the Foundation Hub load-balancer that provides authentication. For example:

```
<authentication defaultAuthenticationProviderForSigning="AEP">
   <uri>https://Workbook.biovia.com:9953</uri>
   <cache-time>00:05</cache-time>
</authentication>
```

4. On each Vault Server machine, start the Vault services. See Starting the Vault Services on page 73.
5. Configure each Vault Server machine to use the load-balanced URL for running Pipeline Pilot protocols by editing the following configuration files:
   - `<installation_directory>\WebService\web.config`
   - `<installation_directory>\DeploymentManager\web.config`
   - `<installation_directory>\Rest\web.config`

   a. Back up each file.

   b. Change the `uri` value in each file to the Pipeline Pilot Server load-balancer, for example:

```
<authentication defaultAuthenticationProviderForSigning="AEP">
   <uri>https://mynotebook.mycompany.com:9943</uri>
   <cache-time>00:05</cache-time>
</authentication>
```

Configuring a Load Balanced Vault Server Environment

Note: In these instructions, `<installation_directory>` indicates the BIOVIA Vault Server installation location. The default location is `C:\Program Files (x86)\BIOVIA\Vault`.

To configure a load balanced Vault Server environment:

1. Stop the Vault services on each Vault Server computer. See Stopping the Vault Services on page 73.
2. Copy the load balancer's PFX file from the Certificates folder to the `<installation_directory>\VaultClientService\conf` folder, and then name the file `vault.pfx`.
3. Edit the `server.xml` file, verify that the path for the `keystoreFile` and `keystorePass` are correct for the load balancer PFX file. For example:

```
<Connector
  protocol="org.apache.coyote.http11.Http11NioProtocol"
  connectionTimeout="20000" port="4499"
  maxThreads="200"
  scheme="https" secure="true" SSLEnabled="true"
  keystoreFile="C:\Program Files
(x86)\BIOVIA\Vault\VaultClientService\conf\vault.pfx"
  keystorePass="mypassword"
  keystoreType="PKCS12"
  clientAuth="false"
  sslProtocol="TLS" />
```

4. On each Vault Server machine, configure IIS to use the **`vault.pfx`** certificate for authentication as follows:
   a. Open the **Internet Information Services (IIS) Manager**.
   b. Edit the site bindings by changing the bindings for port 443 to **`vault.pfx`**.
5. Restart the Vault services. See Starting the Vault Services on page 73.
6. Open a browser on a computer where BIOVIA Workbook is installed to test load balancing.
7. Enter the URL for the load-balancer server in the browser. The default IIS website page should open without certificate errors.
8. Log in to Workbook to connect to the load-balancer server.

Load Balancer Reference

Issue	Scenario and Recommendation
Use session persistence	The user remains on the same Pipeline Pilot or BIOVIA Vault Server IP address for the duration of their BIOVIA Workbook interaction. The load balancer requires session affinity to bind a user's session to a specific application instance.
Use the client's true source IP address	BIOVIA Vault Server needs to know the client's source IP address, and does not support Network Address Translation.
Identify servers in alternate DNS list	BIOVIA Vault Server does not need an alternate DNS list.
Understand load balancer methods	Use the round robin DNS load balancing method. BIOVIA has not tested other methods.
Mitigate a single point of failure with Pipeline Pilot Shared folders	You can mitigate the single point of failure issue by providing file system fail-over through third-party devices such as RAID systems or disk arrays.
Perform environment monitoring	You should monitor all BIOVIA Vault Server services. Investigate service failures and occasions when the server is taken out of the load balancing pool.
Determine which server is accessed behind the load balancer	You can determine which BIOVIA Vault Server is accessed by testing the environment: 1. Shut down all servers except one, then log in to the BIOVIA Workbook client to ensure that the load balancer servers are working. 2. Perform this testing process on all of the servers. 3. For monitoring use of the servers over time, check your load balancer logs or your Microsoft IIS and BIOVIA Vault Server logs.
Identify server used by the BIOVIA Workbook client	Check your load balancer logs to determine the server used by the client: 1. You can copy the **Show Environment** protocol from **`Web Port Examples\Generic\Show Environment to Web Services\Workbook\Analysis`** with Load Balancer Configuration 1. 2. Use the Pipeline Pilot Client to copy **Show Environment to Web Services\Workbook\Analysis** folder. 3. You can run this protocol from the BIOVIA Workbook, Notebook Explorer Analysis tab.

Appendix B:
Integration with BIOVIA Chemical Registration

You can integrate Workbook with Chemical Registration if you have a Chemical Registration license and Pipeline Pilot 2021 with Chemical Registration is deployed with the `Fetch External Data` option enabled.

If Chemical Registration and Workbook connect to the same Pipeline Pilot server, Vault Server can use the RunProtocol Application permission to access Chemical Registration.

If Chemical Registration is on a different Pipeline Pilot server, you must create a new Application Permission to run protocols on that server, as described in Adding ChemRegRunProtocol Permission on page 47. You must also update the experiment template to use that permission for the action buttons.

Setting Up the Pipeline Pilot Server

The *Fetch External Data* component is installed as part of the Notebook Component Collection to the `Components\Laboratory\Notebook\ChemReg Integration` folder of the Pipeline Pilot Client.

After you install the integration software, you must copy this component to the `Components\Web Applications\ChemicalRegistration\Custom Extensions` folder of the Pipeline Pilot Client component tree

1. On the Pipeline Pilot Client, navigate to the `ChemReg Integration` folder in the component tree.
2. Double-click the *Fetch External Data* component to add the component to a new protocol.
3. Select the component in the protocol, right-click and select **Save As**.
4. Navigate to the following folder:

   `Components\Web Applications\ChemicalRegistration\Custom Extensions`
5. Save the customized *Fetch External Data* component in the `Custom Extensions` folder.

Setting Up User Authentication

If BIOVIA Chemical Registration uses a BIOVIA Pipeline Pilot installation on a different server than BIOVIA Vault Server, you must create a new application permission in the BIOVIA Foundation Hub to run the Chemical Registration protocols from Workbook. The alternate server must have both the Chemical Registration and BIOVIA Workbook protocols.

To set up user authentication for the Chemical Registration and BIOVIA Workbook integration to work on a Pipeline Pilot:

- Use SSL to connect to the Pipeline Pilot.
- Define the endpoint using HTTPS.
- Update the Synthetic Chemistry – ChemReg experiment template to start using the newly created application permission.
- Configure the **Register** and **Update** toolbar buttons, BIOVIA Workbook, for the synthetic chemistry section before scientists can begin to use the BIOVIA Workbook and Chemical Registration integration protocols.
- Use domain authentication in Pipeline Pilot to support both Chemical Registration and BIOVIA Workbook in Active Directory or local Windows accounts. Verify that the user names and passwords for Chemical Registration and BIOVIA Workbook are synchronized.

Assigning Permissions

To set up BIOVIA Workbook users with permissions to use BIOVIA Chemical Registration:

1. Log in to Foundation Hub as an Administrator.
2. Click on Settings > Admin and Settings > Groups
3. Click on the desired Workbook Group and then click **Edit**.
4. Under Permissions, assign the appropriate Chemical Registration permissions to the Group.

   For more information, see the *BIOVIA Foundation Hub Administration Guide*.
5. Click **Save**.

Limitations

- Users can register only one material at a time. If a user selects multiple materials and clicks on the **Register** button, then the following error displays to the user:

  "Simultaneous registration of multiple instances is not currently supported. Please a select a single substance and re-submitted for registration."
- If the user does not select any materials, and clicks the **Register** button, the following message displays:

  "Please select a single substance and re-submit for registration."

Integration Components

The Pipeline Pilot Client components and protocols listed below are required to integrate BIOVIA Workbook and BIOVIA Chemical Registration. The components and protocols are installed on the Pipeline Pilot Server after the Workbook Component Collection is installed.

Fetch External Data

Chemical Registration can populate the registration forms with data from external systems. You can configure the pre-populate registration forms with appropriate values to enabled access from a URL. The *Fetch External Data* component controls the data population for the registration forms.

To access and run the component, save the custom *Fetch External Data* component in the `Components\Web Applications\Chemical Registration\Custom Extensions` folder of the Pipeline Pilot Client component tree.

Fetch Registration Data

The *Fetch Registration Data* component is used by the *Fetch ChemReg Data* protocol to get registration data for a BIOVIA Workbook material from Chemical Registration.

Read ChemReg Configuration

The *Read ChemReg Configuration* component is used to read configuration data for the *Register Material* and *Fetch ChemReg Data* protocols.

Search and Fetch Registration Data

The *Search and Fetch Registration Data* component is used by the *Fetch Registration Data* component to connect to the Chemical Registration database and execute queries on the database.

Integration Protocols

The following Pipeline Pilot Client protocols are required for the integration of BIOVIA Workbook and BIOVIA Chemical Registration.

Finish Chemical Registration

The *Finish Chemical Registration* protocol is called when the BIOVIA Workbook user clicks the **Update**, **Register**, and **Close** buttons in experiments using the Synthetic Chemistry - ChemReg experiment template.

Finish Chemical Registration sends the Chemical Registration data back to the BIOVIA Workbook experiment containing the Synthetic Chemistry - ChemReg section after a material has been registered.

Register Material

The *Register Material* protocol is configured to work with the Register dynamic toolbar button of the Synthetic Chemistry – ChemReg experiment template. The **Register** button launches the Chemical Registration application and populates the data sent by BIOVIA Workbook to the Chemical Registration page.

Fetch ChemReg Data

The *Fetch ChemReg Data* protocol is configured with the BIOVIA Workbook Dynamic Toolbar's **Update** button in the Synthetic Chemistry - ChemReg experiment template. *Fetch ChemReg Data* is used to get the available Chemical Registration data for all materials in the Synthetic Chemistry section.

Field Mappings

If you customized the BIOVIA Chemical Registration data model, you must also customize the field mappings between BIOVIA Workbook experiment and the Chemical Registration database. The BIOVIA Workbook mapping configuration files are set up to work with the default Chemical Registration data model.

The field mapping configuration is defined in files located on the BIOVIA Pipeline Pilot in the following directory:

`<PPS_installation_directory>\apps\scitegic\notebook\dataroot`

These files are:

- `Notebook-To-ChemReg-PropertyMapper.xml`
- `ChemReg-To-Notebook-PropertyMapper.xml`

Workbook to Chemical Registration Mapping

You can configure BIOVIA Workbook fields to the Chemical Registration fields in the `Notebook-To-ChemReg-PropertyMapper.xml` file. When Chemical Registration is launched from BIOVIA Workbook, material data fields from BIOVIA Workbook are mapped to corresponding fields on the registration page of Chemical Registration.

In each `<PropertyMapping>` element in `Notebook-To-ChemReg-PropertyMapper.xml`, there are two child elements:

- `<NotebookProperty>` contains the BIOVIA Workbook field name
- `<ChemRegProperty>` contains the Chemical Registration attribute

When mapping fields always enter the BIOVIA Workbook field name in the `<NotebookProperty>` element, and the Chemical Registration data model element in the `<ChemRegProperty>` element. For example, the following example shows the mappings of the Materials Name property from BIOVIA Workbook to the IupacName property in Chemical Registration.

```
<PropertyMapping>
  <NotebookProperty>Material::Name</NotebookProperty>
  <ChemRegProperty>IupacName</ChemRegProperty>
</PropertyMapping>
```

IMPORTANT! If any of the vocabulary controlled fields in Chemical Registration are required fields, then you must synchronize the Chemical Registration fields with the equivalent fields in BIOVIA Workbook. If the required fields are not mapped to BIOVIA Workbook, scientists cannot register materials using values supplied by a BIOVIA Workbook experiment.

Tips:

- Define property tags in the following order: `<NotebookProperty>`, then `<ChemRegProperty>`.
- The `<NotebookProperty>` name must match the Property name as it appears after the data has been read by the *Notebook Table Reader*, a BIOVIA Workbook component that reads the data exported from the BIOVIA Workbook.
- For Chemical Registration properties that are populated with field values from the Background Form, use the same BIOVIA Workbook property name.
- Fields added to the BIOVIA Workbook Background Form. You must map the fields to the corresponding Chemical Registration fields using the field name in the Background Form. The `<ChemRegProperty>` name is equivalent to the field name as defined in the Chemical Registration database.
- The integration of BIOVIA Workbook and Chemical Registration supports one to one field mappings. You cannot map complex data structures to a single field in Chemical Registration. For example, you need to map a quantity value individually for the value, unit, and sig-fig, even though it is a single field in BIOVIA Workbook.

For more information refer to the "Configure the Chemical Registration Dynamic Toolbar" topic in the BIOVIA Workbook online help.

Chemical Registration to Notebook Mapping

Chemical Registration data for a material is updated in BIOVIA Workbook using the *Fetch ChemReg Data* protocol. The mapping of the Chemical Registration field to its corresponding BIOVIA Workbook field is configurable by editing the `ChemReg-To-Notebook-PropertyMapper.xml file`.

You can define a default start page number for the Chemical Registration application when launched from BIOVIA Workbook by extending the mapping in the `ChemReg-To-Notebook-PropertyMapper.xml` file.

Field Mapping Configuration Files

Notebook-To-ChemReg-PropertyMapper.xml

The `Notebook-To-ChemReg-PropertyMapper.xml` configuration file contains the following default field mappings:

```
<?xml version="1.0" encoding="utf-8"?>
<NotebookChemRegMapping>
<PropertyMapping>
  <NotebookProperty>Material::Structure</NotebookProperty>
  <ChemRegProperty>Chemistry</ChemRegProperty>
</PropertyMapping>
<PropertyMapping>
  <NotebookProperty>Material::Name</NotebookProperty>
  <ChemRegProperty>IupacName</ChemRegProperty>
</PropertyMapping>
<PropertyMapping>
  <NotebookProperty>AccelrysTableSection::RowId</NotebookProperty>
  <ChemRegProperty>OriginID</ChemRegProperty>
</PropertyMapping>
<PropertyMapping>
  <NotebookProperty>ActualAmount::CalcMass___Number</NotebookProperty>
  <ChemRegProperty>Lot/Quantity</ChemRegProperty>
</PropertyMapping>
<PropertyMapping>
  <NotebookProperty>ActualAmount::CalcMass___Unit</NotebookProperty>
  <ChemRegProperty>Lot/Quantity__unit</ChemRegProperty>
</PropertyMapping>
<PropertyMapping>
  <NotebookProperty>txtUser</NotebookProperty>
  <ChemRegProperty>Lot/Scientist</ChemRegProperty>
</PropertyMapping>
<PropertyMapping>
  <NotebookProperty>txtID</NotebookProperty>
  <ChemRegProperty>Lot/Notebook/ID</ChemRegProperty>
</PropertyMapping>
<PropertyMapping>
  <NotebookProperty>cbProject</NotebookProperty>
  <ChemRegProperty>Project</ChemRegProperty>
</PropertyMapping>
<PropertyMapping>
  <NotebookProperty>txtExperimentStartDate</NotebookProperty>
  <ChemRegProperty>Lot/DatePrepared</ChemRegProperty>
</PropertyMapping>
</NotebookChemRegMapping>
```

ChemReg-To-Notebook-PropertyMapper.xml

The `ChemReg-To-Notebook-PropertyMapper.xml` configuration file contains the following default field mappings:

```
<?xml version="1.0" encoding="utf-8"?>
<NotebookChemRegMapping>
<PropertyMapping>
  <NotebookProperty>MaterialRegistration::Response</NotebookProperty>
  <ChemRegProperty>GemsInstance/Lifecycle</ChemRegProperty>
</PropertyMapping>
<PropertyMapping>
  <NotebookProperty>MaterialRegistration::SubmissionDate_SYS
  </NotebookProperty>
  <ChemRegProperty>GemsInstance/createdDate</ChemRegProperty>
</PropertyMapping>
<PropertyMapping>
  <NotebookProperty>MaterialRegistration::BatchId</NotebookProperty>
  <ChemRegProperty>GemsInstance/Label</ChemRegProperty>
</PropertyMapping>
<PropertyMapping>
  <NotebookProperty>MaterialRegistration::NormalizedStructure
  </NotebookProperty>
  <ChemRegProperty>Chemistry</ChemRegProperty>
</PropertyMapping>
</NotebookChemRegMapping>
```

Document Vocabularies

BIOVIA recommends keeping the vocabularies for common fields between Workbook and Chemical Registration synchronized.

In Chemical Registration, the *Project* field is a list of value the user can selects when creating or editing a project. In Workbook, the Synthetic Chemistry – ChemReg experiment template has a *Project* field in the Background Form section. The Workbook *Project* field is also a list of values that the user selects.

If you map the Chemical Registration *Project* field to the Workbook *Project* field the values in both fields should must match.

If Bloodpressure is added to the Chemical Registration *Project* field vocabulary, then Workbook *Project* field must contain the same value using the same word spacing and capitalization. If these values are not synchronized then the populated values fail validation in Chemical Registration.

In the example above, if the Workbook *Project* field vocabulary has Blood Pressure as two words with different capitalization, and the Chemical Registration *Project* field has Bloodpressure as one word and only capitalizes the *B*, the validation fails because Blood Pressure is evaluated as two different vocabulary terms.

Adding ChemRegRunProtocol Permission

If BIOVIA Chemical Registration and BIOVIA Vault Server use different BIOVIA Pipeline Pilot Servers, you must configure Vault Server to run protocols on the Pipeline Pilot server used for Chemical Registration.

> **Tip:** To use a command-line utility to add or update permission configurations for services and applications, see "Using the Import/Export Application Permissions Utility" in the *Vault Server Administration Tools Guide*. The command-line utility enables you to easily export all editable application permissions, edit them using a text editor, tokenize them for use on more than one Vault Server if needed, and then re-import them into the same or a different Vault Server.

To use the Vault Administration Console to add the ChemRegRunProtocol Permission, perform the following steps:

1. Open the Vault Administration Console and log on to Vault Server as a member of the Vault Global Administrators group.
2. Expand the Vault Server node and select **Application Permissions**.
3. In the **Actions** pane, select **Add**.
4. In the **New Permission** dialog, in the **Application** field, type **PipelinePilot**.
5. In the **Permission** field, type **ChemRegRunProtocol**.
6. Click **OK**.
7. In Application Permissions, select **PipelinePilot|ChemRegRunProtocol** and click **Properties**.
8. In **PipelinePilot|ChemRegRunProtocol Properties**, click the **Configuration** tab.
9. In **Name**, type **Endpoint**, and in **Value**, type the endpoint URL to look similar to the following: `https://server_name:port_number`, for example, `https://myChemReg_PPserver:9943`, and then click OK.
10. Click the **Name** heading to add a second line in the **Configuration** tab.
11. In the blank line, in **Name**, type **ProtocolRoot**.
12. In **Value**, type **Protocols/Web Services/Workbook/Experiment** and click **OK**.

You must assign users that are able to run Chemical Registration from Vault Server to the **PipelinePilot |ChemRegRunProtocol** permission. For more information, see Assigning Users or Groups to the ChemRegRunProtocol Permission on page 48.

Assigning Chemical Registration Permissions

On BIOVIA Pipeline Pilot, you must assign one or more roles to users and groups to enable running the integration of BIOVIA Chemical Registration and BIOVIA Workbook.

1. Log in to the BIOVIA Foundation Hub using administrator credentials.
2. Navigate to **Admin and Settings > Security > Groups**.
3. Assign one or more BIOVIA Workbook users or groups the appropriate Chemical Registration group (s):
   - `Chemical Registration/Administrators`
   - `Chemical Registration/Basic`
   - `Chemical Registration/Bulk`
   - `Chemical Registration/Chemist`
   - `Chemical Registration/Editor`
   - `Chemical Registration/Registrar`
   - `Chemical Registration/Users`.

Note: For more information, see the *Chemical Registration Administration Guide.*

Assigning Users or Groups to the ChemRegRunProtocol Permission

To run BIOVIA Chemical Registration from BIOVIA Workbook 2021 when the applications are installed on different servers, you must assign the `PipelinePilot|ChemRegRunProtocol` permission to users or groups in the Vault Administration Console. You must also change the protocol to use the Chemical Registration server as the endpoint.

To assign users or groups to the ChemRegRunProtocol permission:

1. In the Vault Administration Console, log in to the BIOVIA Vault Server using your administrator credentials.
2. Expand the Vault Server and select **Groups** or **Users**.
3. In **Groups** or **Users**, select the **group** or **user** to receive permission to run Chemical Registration protocols from Vault Server and click **Properties**.
4. In the **Group** or **Users Properties** dialog, click the **Permissions** tab.
5. In the **PipelinePilot|ChemRegRunProtocol** row, click **Allow** and click **OK**.

Appendix C: Integration with BIOVIA CISPro

Workbook determines how to access CISPro and how to map CISPro data to Workbook fields by using a CISPro material information resolver. This resolver, like those you might have for other external systems, provides the necessary integration information in the form of configuration XML.

The **MaterialInfoManager** Vault Server application permission hosts the configuration XML for CISPro. You access and edit this XML to meet your site-specific requirements by using the Vault Administration Console, which provides access to all Vault application permissions. For more information about this tool and about application permissions, see the *Vault Server Tools Administration Guide*.

Version Compatibilities, Constraints, and Prerequisites

Version Compatibilities

IMPORTANT! The configuration XML can vary based on the version of CISPro that you use. If you upgrade to a version of CISPro that requires different configuration XML than your previous version, you must update your configuration XML accordingly.

The following table lists CISPro versions that can be integrated with Workbook 2021 and indicates whether you must update your existing XML configuration when you upgrade to these CISPro versions.

CISPro Version	Requires updates to Configuration XML?	Feature Notes
2020 SP1	Yes	CISPro 2020 SP1 introduced a faster API that requires changes to the configuration XML. The new configuration XML also added support for retrieving CISPro information from the Material and ReceiptLot levels, instead of from only the Container level. This XML is represented in Example Configuration XML for CISPro 2020 SP1 and Later on page 55.
2020 SP1 HF1 or later	No, unless you want to use new features	CISPro 2020 SP1 HF1 does not require changes to the configuration XML provided for CISPro 2020 SP1. This release added support for retrieving custom CISPro properties. To use this feature, customers can modify the 2020 SP1 configuration XML as described in Step 3d of Upgrading a Customized CISPro Material Resolver Configuration on page 52.

Integration Constraints and Prerequisites

You can integrate CISPro and Workbook only if:

- CISPro and Vault Server use the same Foundation Hub for authentication.
- The CISPro site is configured to require SSL using TLS 1.2 and strong cryptography.
- You are a member of the Vault Global Administrators group.
- You have the `Templates Transfer` application permission, if you intend to import CISPro objects into Workbook.

Workbook users can retrieve data from CISPro only if they belong to a group that has the MaterialInfoManager permission set to **Allow**.

Obtain the following required information before you configure the resolver:

- Your CISPro customer ID
- URL of the CISPro web client
- Your Foundation Hub client ID

Editing the CisProMaterialInfoResolver XML

To enable Workbook users to search the CISPro database, you must replace placeholder values for CISPro web client URL, CISPro Customer ID, and Foundation Hub client ID in the configuration XML used for CISPro.

> **Tip:** To use a command-line utility to add or update permission configurations for services and applications, see "Using the Import/Export Application Permissions Utility" in the *Vault Server Administration Tools Guide*. The command-line utility enables you to easily export all editable application permissions, edit them using a text editor, tokenize them for use on more than one Vault Server if needed, and then re-import them into the same or a different Vault Server.

To use the Vault Administration Console to update the configuration XML, perform the following steps:

1. Open the Vault Administration Console and log on to Vault Server as a member of the Vault Global Administrators group.
2. Under Console Root, expand the Vault Server node and select **Application Permissions**.
3. In **Application Permissions**, double-click **LookupService**.
4. In **LookupService > MaterialInfoManager Properties**, click the **Configuration** tab.
5. Click the **Value** cell next to **Biovia.Notebook.CisProMaterialInfoLookup.CisProInventoryMaterialInfoResolver** XML and resize the resulting edit window to see more of the XML.
6. Copy the XML to the Clipboard (**Ctrl+A**, **Ctrl+C**), paste (**Ctrl+V**) it into Notepad or another external text editor, and save it as **`XML.backup`** in case you need to recover it later.
   - For a description of the XML elements, refer to Resolver XML Element Descriptions on page 58.
   - To see example configuration XML, refer to Example Configuration XML for CISPro 2020 SP1 and Later on page 55.
7. In a different text editor window, copy the XML again and make the following required changes to its <Configuration> element properties:
   - Change the **URL** property value to the URL of your CISPro web client:

     ```
     <Property name='URL'>https://<mycispro.web_client_
     URL>/cispro</Property>
     ```
   - Change the **CustomerId** property value to the Customer ID that you use to log in to the CISPro web client.

     <Property name='CustomerId'><mycompany_customerID></Property> <Configuration>

     > **Note:** The CISPro web client displays the **CustomerId** after the at (@) symbol in your user account name, for example, cispro_username@**mycustomerID**.
   - Change the **FoundationAppNameOrClientId** property value to match the value in the **Name** field in Foundation Hub **Admin and Settings > Settings > Applications** > **Inventory**.
8. If needed, change the values for the following additional Configuration element properties:
   - **ReplaceExistingPropertyValues**

     Indicates whether scanned barcode values imported from CISPro can overwrite existing property values in the material row. *True* allows overrides, *False* prevents them.

- **SearchGridColumnOrder**

  Comma-delimited list of fully qualified property keys in the form *`PropertySetKey.PropertyKey`* to display as columns in the Material Import dialog search results grid.

- **MaxNumberOfResults**

  Maximum number of results to retrieve from CISPro when using the Material Import dialog box.

9. If necessary, insert elements to identify any custom CISPro fields that Workbook users require.

   For details, see Upgrading a Customized CISPro Material Resolver Configuration on page 52.

10. Select your modified XML and copy it to the Clipboard (Ctrl+A, Ctrl+C).
11. Return to the Vault Administration Console edit window and replace its XML with your modified XML.
12. Click **OK** to save your changes and close the edit window.
13. Click **OK** to close the Properties dialog box.

Upgrading a Customized CISPro Material Resolver Configuration

The XML configuration documents for the old and new CISPro resolvers are similar. Use the old XML as the foundation for your upgrade.

To upgrade customized configuration XML:

1. For each property name in your old configuration XML, identify the name required by the new CISPro inventory material resolver. Keep in mind that the names are case-sensitive, and that any date fields must use the `datefield_utc` property to support correct handling of timezones.

   The following table provides a partial list of standard property names. If your configuration identifies custom CISPro fields to use in Workbook, you can identify them by their `customProperties.` prefix.

   IMPORTANT! Retrieving custom CISPro property values for use in Workbook negatively impacts performance. Retrieve a custom property only if that property is essential to your Workbook users.

Old CISPro Material Resolver Property	New CISPro Inventory Material Resolver Property
Material	material.name
Notes	Notes
Structure	material.structure
CAS No	material.casNo
Quantity	quantity
Concentration	concentration
Location	location.fullPath
Status	status
Expiration Date	receiptLot.expirationDate_utc
Specific Gravity	material.specificGravity

Old CISPro Material Resolver Property	New CISPro Inventory Material Resolver Property
Manufacturer Lot No	receiptLot.manufacturerLotNo
Manufacturer	receiptLot.manufacturer_name
Barcode	barcode

2. In each XPATH query, replace each instance of '**old name**' with the new name:

   //x:Properties/x:ObjectClassCollectionModel.EntityModel.Property[x:PropName='**old_name**']/x:Gestalt

   For details, see Referencing CISPro Property Names in XPATH Queries on page 54.

   > **Note:** `x:PropName` and `x:ObjectClassPropName` are interchangeable.

3. If you need to retrieve property data from a level other than **container**:

   a. Identify each property and the level from which to retrieve it by prefixing the property name with the level name, plus a period. For example, the table in Step 1 identifies properties from three levels:

   - Four from the `material` level: `material.name`, `material.structure`, `material.casNo`, and `material.specificGravity`
   - Three from the `receiptLot` level: `receiptLot.manufacturerLotNo`, `receiptLot.manufacturer_name`, and `receiptLot.expirationDate_utc`.
   - One from the `location` level: `location.fullPath`

   The names of the levels are case-sensitive.

   b. In the XML, replace <Property name="**SelectFields**"> with <Property name="**ExpandLevels**">, and insert a comma-separated list of the levels that you need. For example:

   ```
   <Property name="ExpandLevels">material,receiptLot,location</Property>
   ```

   c. To minimize performance impacts, insert a `$select` attribute for each level that identifies *only* the specific properties that you need from that level. For example:

   ```
   <Property name="ExpandLevels">
    material($select=nodetypeid,name,structure),
    receiptLot($select=nodetypeid,manufacturerLotNo,manufacturer_
   name,expirationDate_utc),
    location($select=nodetypeid,fullPath)
   </Property>
   ```

   d. If you use CISPro 2020 SP1 **HF1** or later and want to retrieve custom properties from a level, insert the `$expand=customProperties` attribute. You cannot do this for earlier versions. Example that retrieves all custom properties from the container and material levels:

   ```
   <Property name="ExpandLevels">
    material($select=nodetypeid,
   name,structure;$expand=customProperties),
    receiptLot($select=nodetypeid,manufacturerLotNo,manufacturer_
   name,expirationDate_utc),
    location($select=nodetypeid,fullPath)
    location($select=nodetypeid,fullPath),
   customProperties
   </Property>
   ```

4. Update each `SearchType` key value by replacing the old name with the new name and level. The following table shows some examples.

Old Key Value	New Key Value
<SearchType key='Barcode'...	<SearchType key='barcode'...
<SearchType key='CAS No'...	<SearchType key='**material**.casNo'...
<SearchType key='Tradename'...	<SearchType key='**material**.tradename'...

Referencing CISPro Property Names in XPATH Queries

XPATH queries that reference CISPro property names must use the following format:

```
//x:Properties/x:ObjectClassCollectionModel.EntityModel.Property[x:
PropName='expandLevel.propName']/x:Gestalt
```

Where:

- `x:PropName` and `x:ObjectClassPropName` are interchangeable.
- `expandLevel` is required only if the data is not from the container level.
- `propName` is the case-sensitive CISPro property name.
- Valid names for standard container properties and expandable levels are identified in the CISPro Inventory API help index, which is available on your CISPro server at the following url:

  ```
  http://<cispro_
  server>/cispro/inventory/apihelp/index#!/Containers/Containers_Get
  ```

- If you defined custom CISPro properties, reference them by prefixing their names with `customProperties`. For example, to reference a custom property called MyCustomPropName, use:

  ```
  customProperties.MyCustomPropName
  ```

  Custom property names, like standard property names, are case-sensitive.

  > **Note:** With CISPro 2020 HF1 and later, you can retrieve custom CISPro properties. To do so, map the properties in the configuration XML by adding `$expand=customProperties` to the `ExpandLevels` property.

Example Mapping Queries

- Map the “status” property of the container level from CISPro:

  ```
  //x:Properties/x:ObjectClassCollectionModel.EntityModel.Property
  [x:PropName='status']/x:Gestalt
  ```

- Map the “casNo” property of the material level from CISPro:

  ```
  //x:Properties/x:ObjectClassCollectionModel.EntityModel.Property
  [x:PropName='material.casNo']/x:Gestalt
  ```

- Map the material level custom property “Color” from CISPro:

  ```
  //x:Properties/x:ObjectClassCollectionModel.EntityModel.Property
  [x:PropName='material.customProperties.Color']/x:Gestalt
  ```

- Map the container level custom property “Part Number” from CISPro:

  ```
  //x:Properties/x:ObjectClassCollectionModel.EntityModel.Property
  [x:PropName='customProperties.Part Number']/x:Gestalt
  ```

The following value for the `ExpandLevels` parameter supports the retrieval of all four properties from the previous examples:

```
material
($select=nodetypeid,casNo;$expand=customProperties),customProperties&amp;
$select=nodetypeid,nodeid,guid,displayName,nodetypename,barcode,status&amp
;$orderby=nodeid desc
```

Example Configuration XML for CISPro 2020 SP1 and Later

The following example configuration XML for CISPro 2020 SP1 and later is provided in the Workbook 2020 installation package as a file called `ExampleCisProMaterialInfoLookupConfiguration.xml`.

To upgrade to CISPro 2020 SP1 or later, you must upgrade your configuration XML by replacing the property values shown in **red** with site-specific values, as described in Editing the CisProMaterialInfoResolver XML on page 51. To capitalize on the enhancements in this version, such as obtaining custom fields for use in Workbook and obtaining fields at levels below the container level, see Upgrading a Customized CISPro Material Resolver Configuration on page 52.

```
<?xml version="1.0" encoding="utf-8" ?>
<MaterialInfoResolver name="CISPRO">
    <PropertySet name="Material">
        <Property
name="Name">//x:Properties/x:ObjectClassCollectionModel.EntityModel.Property
[x:ObjectClassPropName='material.name']/x:Gestalt</Property>
        <Property
name="Comments">//x:Properties/x:ObjectClassCollectionModel.EntityModel.Property
[x:ObjectClassPropName='notes']/x:Gestalt</Property>
        <Property
name="Structure">//x:Properties/x:ObjectClassCollectionModel.EntityModel.Property
[x:ObjectClassPropName='material.structure']/x:Gestalt</Property>
        <Property
name="CASNumber">//x:Properties/x:ObjectClassCollectionModel.EntityModel.Property
[x:PropName='material.casNo']/x:Gestalt</Property>
        <Property
name="MW">//x:Properties/x:ObjectClassCollectionModel.EntityModel.Property
[x:PropName='molecularWeight']/x:Gestalt</Property>
        <Property name="InitialAmount">
            <xpath
path="//x:Properties/x:ObjectClassCollectionModel.EntityModel.Property
[x:ObjectClassPropName='quantity']/x:Gestalt">
                <matchingPatterns />
                <unitMatchingPatterns>
                    <pattern unit="LITER">\d+\s*(L)</pattern>
                    <pattern unit="MICROLITER">\d+\s*(µL)</pattern>
                    <pattern unit="MICROLITER">\d+\s*(uL)</pattern>
                    <pattern unit="MILLILITER">\d+\s*(mL)</pattern>
                    <pattern unit="GRAM">\d+\s*(g)</pattern>
                    <pattern unit="KILOGRAM">\d+\s*(Kg)</pattern>
                    <pattern unit="KILOGRAM">\d+\s*(kg)</pattern>
                    <pattern unit="MILLIGRAM">\d+\s*(mg)</pattern>
                    <pattern unit="MICROGRAM">\d+\s*(µg)</pattern>
                    <pattern unit="MICROGRAM">\d+\s*(ug)</pattern>
                    <pattern unit="UNDEFINED">\d+\s*(\w*)</pattern>
                </unitMatchingPatterns>
            </xpath>
        </Property>
    </PropertySet>
    <PropertySet name="FormulationMaterial">
```

```
        <Property name="Purity" formatterKeys="GetMassPercent">
            <xpath
path="//x:Properties/x:ObjectClassCollectionModel.EntityModel.Property
[x:ObjectClassPropName='concentration']/x:Gestalt">
                <matchingPatterns />
                <unitMatchingPatterns>
                    <pattern unit="MASSPERCENT">\d+\s*(wt%)</pattern>
                    <pattern unit="MASSPERCENT">\d+\s*(mass%)</pattern>
                </unitMatchingPatterns>
            </xpath>
        </Property>
    </PropertySet>
    <PropertySet name="ReactionMaterial">
        <Property name="PurityConcentration">
            <xpath
path="//x:Properties/x:ObjectClassCollectionModel.EntityModel.Property
[x:ObjectClassPropName='concentration']/x:Gestalt">
                <matchingPatterns />
                <unitMatchingPatterns>
                    <pattern unit="MOLELITER">\d+\s*(mol/L)</pattern>
                    <pattern unit="MOLELITER">\d+\s*(M)</pattern>
                    <pattern unit="MMOLG">\d+\s*(mmol/g)</pattern>
                    <pattern unit="MOLMG">\d+\s*(mol/mg)</pattern>
                    <pattern unit="MOLKG">\d+\s*(mol/kg)</pattern>
                    <pattern unit="NMOLKG">\d+\s*(nmol/kg)</pattern>
                    <pattern unit="MMOLKG">\d+\s*(mmol/kg)</pattern>
                    <pattern unit="UMOLKG">\d+\s*(µmol/kg)</pattern>
                    <pattern unit="UMOLG">\d+\s*(µmol/g)</pattern>
                    <pattern unit="MOLPERHUNDREDGRAM">\d+\s*(mol/100g)</pattern>
                    <pattern unit="MOLG">\d+\s*(mol/g)</pattern>
                    <pattern unit="MOLML">\d+\s*(mol/mL)</pattern>
                    <pattern unit="MMOLELITER">\d+\s*(mmol/L)</pattern>
                    <pattern unit="MLMMOL">\d+\s*(mmol/mL)</pattern>
                    <pattern unit="UMOLEULITER">\d+\s*(µmol/µL)</pattern>
                    <pattern unit="MOLEPM3">\d+\s*(mol/m³)</pattern>
                    <pattern unit="UMOLELITER">\d+\s*(µmol/L)</pattern>
                    <pattern unit="NMOLELITER">\d+\s*(nmol/L)</pattern>
                    <pattern unit="PMOLELITER">\d+\s*(pmol/L)</pattern>
                    <pattern unit="MASSPERCENT">\d+\s*(wt%)</pattern>
                    <pattern unit="MASSPERCENT">\d+\s*(mass%)</pattern>
                    <pattern unit="MASSFRACTION">\d+\s*(mass fraction)</pattern>
                    <pattern unit="MASSFRACTION">\d+\s*(m/m)</pattern>
                    <pattern unit="GG">\d+\s*(g/g)</pattern>
                    <pattern unit="MILLIGRAMKG">\d+\s*(mg/kg)</pattern>
                    <pattern unit="NANOGRAMKG">\d+\s*(ng/kg)</pattern>
                    <pattern unit="GRAMPERHUNDREDGRAM">\d+\s*(g/100g)</pattern>
                    <pattern unit="MILLIGRAMG">\d+\s*(mg/g)</pattern>
                    <pattern unit="KGPERKG">\d+\s*(kg/kg)</pattern>
                    <pattern unit="KGPERG">\d+\s*(kg/g)</pattern>
                    <pattern unit="KGPERHUNDREDGRAM">\d+\s*(kg/100g)</pattern>
                    <pattern unit="GRAMPERKG">\d+\s*(g/kg)</pattern>
                    <pattern unit="MICROGRAMKG">\d+\s*(µg/kg)</pattern>
                </unitMatchingPatterns>
            </xpath>
        </Property>
    </PropertySet>
    <PropertySet name="Container">
        <Property name="Barcode" isSource="true">//x:Name</Property>
    </PropertySet>
    <PropertySet name="InventoryCisPro_SYS">
```

```
        <Property name="InventoryId">//x:Id</Property>
        <Property
name="Location">//x:Properties/x:ObjectClassCollectionModel.EntityModel.Property
[x:ObjectClassPropName='location.fullPath']/x:Gestalt</Property>
        <Property
name="Status">//x:Properties/x:ObjectClassCollectionModel.EntityModel.Property
[x:ObjectClassPropName='status']/x:Gestalt</Property>
        <Property name="IsExpired"
formatterKeys="ToDateTime,IsExpired">//x:Properties/x:ObjectClassCollectionModel.Entity
Model.Property[x:ObjectClassPropName='receiptLot.expirationDate_
utc']/x:Gestalt</Property>
        <Property
name="SpecificGravity">//x:Properties/x:ObjectClassCollectionModel.EntityModel.Property
[x:PropName='material.specificGravity']/x:Gestalt</Property>
    </PropertySet>
    <PropertySet name="AnalyticalMaterial">
        <Property
name="LotNumber">//x:Properties/x:ObjectClassCollectionModel.EntityModel.Property
[x:ObjectClassPropName='receiptLot.manufacturerLotNo']/x:Gestalt</Property>
        <Property
name="Manufacturer">//x:Properties/x:ObjectClassCollectionModel.EntityModel.Property
[x:ObjectClassPropName='receiptLot.manufacturer_name']/x:Gestalt</Property>
        <Property
name="ExpiryDate">//x:Properties/x:ObjectClassCollectionModel.EntityModel.Property
[x:ObjectClassPropName='receiptLot.expirationDate_utc']/x:Gestalt</Property>
    </PropertySet>
    <Configuration>
    <Property name='URL'>https://ServerName/cispro</Property>
    <Property name='FoundationAppNameOrClientId'>Inventory</Property>
    <Property name="ReplaceExistingPropertyValues">True</Property>
    <Property name="MaxNumberOfResults">200</Property>
    <Property name="SearchGridColumnOrder"> InventoryCisPro_
SYS.InventoryId,Container.Barcode,Material.Name,InventoryCisPro_
SYS.Status,InventoryCisPro_SYS.Location,InventoryCisPro_
SYS.SpecificGravity,AnalyticalMaterial.ExpiryDate,Material.InitialAmount,Material.Comme
nts
    </Property>
    <Property name="ContainerIdentifierXPath">//x:Id</Property>
    <Property
name="ContainersXPath">/x:ObjectClassCollectionModel/x:Entities/*</Property>
    <Property name="ExpandLevels"> location($select=nodetypeid,fullPath),material
($select=nodetypeid,name,structure,casNo,specificGravity),receiptLot
($select=nodetypeid,manufacturerLotNo,manufacturer_name,expirationDate_
utc)&amp;$select=nodetypeid,nodeid,guid,displayName,nodetypename,barcode,notes,molecula
rWeight,quantity,concentration,status&amp;$orderby=nodeid desc
    </Property>
    <Property name="RequestTimeout">300000</Property>
    <Property name='CustomerId'>CUSTOMERID</Property>
    </Configuration>
    <SearchTypes>
        <SearchType key="barcode" searchExecuterKey="" displayText="Barcode List"
instructionText="Search Criteria: Enter one barcode per line" />
        <SearchType key="material.casNo" searchExecuterKey="" displayText="CAS# List"
instructionText="Search Criteria: Enter one CAS# per line" />
        <SearchType key="material.tradename" searchExecuterKey="" displayText="Name
List" instructionText="Search Criteria: Enter one name per line" />
        <!--
            <SearchType key="status" searchExecuterKey="" displayText="Status List"
instructionText="Search Criteria: Enter one status per line"/>
            <SearchType key="material.supplier_name" searchExecuterKey=""
```

```
displayText="Supplier List" instructionText="Search Criteria: Enter one supplier per
line"/>
        -->
    </SearchTypes>
    <QueryValidators defaultKey="~">
        <QueryValidator key="WildcardsDisallowed" type="py" modelVariableName="model"
errorVariableName="error">
            <![CDATA[
import clr
import sys

for name in model.Names:
  if name.Contains("*"):
    error = "Wildcards cannot be used for this search type."
               ]]>
        </QueryValidator>
    </QueryValidators>
    <SearchExecuters>
        <SearchExecuter key="General" type="py" modelVariableName="model"
outputVariableName="outVar">
            <![CDATA[
import clr
import sys

outVar = model.ResolverLookupPair.Resolver.PerformContainerSearch(model.SearchTypeKey,
model.Names)
               ]]>
        </SearchExecuter>
    </SearchExecuters>
    <Namespaces>
        <namespace prefix="x"
uri="http://schemas.datacontract.org/2004/07/ChemSW.Api.Controllers"></namespace>
        <namespace prefix="y"
uri="http://schemas.datacontract.org/2004/07/ChemSW.Nbt.PropTypes"></namespace>
        <namespace prefix="z"
uri="http://schemas.microsoft.com/2003/10/Serialization/Arrays"></namespace>
    </Namespaces>
    <Formatters>
        <Formatter key="GetMassPercent" type="py" inputVariableName="inVar"
outputVariableName="outVar">
            <![CDATA[
import clr
import sys
import re

outVar = ''

try:
```

Resolver XML Element Descriptions

The default XML for the CISPro contains the following elements, property sets, properties, and attributes. You must update the property and attribute values that are listed in red in Example Configuration XML for CISPro 2020 SP1 and Later on page 55; updates to other elements are optional.

- **`MaterialInfoResolver` element**
  - **name attribute**

    Specifies the name of the material import extension to configure. The value is the value that is expected by CISPro in the resolver code.

  - **`displayName` attribute**

    An optional name that identifies the resolver to the user in Workbook.

- **`PropertySet` element**

  Contains property elements that map CISPro results to Workbook properties.

  - **name attribute**

    Specifies the name of the Workbook property set that receives the CISPro data.

- **`Property` element**

  Specifies a CISPro result value mapping to corresponding Workbook property.

  - **`value`**

    Represents an XPATH query into the CISPro XML result set to identify the data to import into the Workbook property. You can define any namespace prefixes required by the XPATH in the Namespaces element. XPATH queries are case-sensitive.

  - **name attribute**

    Specifies the name of the Workbook property within the containing property set that receives the CISPro data.

  - **`isSource` attribute**

    Specifies the value applied to one property to identify it as the property that contains the CISPro identifier to query. The legal value is true.

  - **`formatterKeys` attribute**

    Specifies an optional, comma delimited list of formatter keys that indicate how the CISPro data is formatted before the import into Workbook. The data might have one or more formatters applied. When multiple formatters are used, they are applied in the order listed. For more information, see the `Formatter` element.

    - **xpath element**

      Applies only to mappings that require unit matching.

      - **path attribute**

        Specifies an XPATH query into the CISPro XML result set that identifies the data to import into the Workbook property. You can define any namespace prefixes required by the XPATH in the Namespaces element. . XPATH queries are case-sensitive.

  - **`matchingPatterns` element**

    DO NOT USE

  - **`unitMatchingPatterns` element**

    Contains pattern elements that map CISPro units to Workbook units.

    - **`pattern element`**

      A CISPro to Workbook unit mapping.

    - **`value`**

      Specifies a Regular Expression pattern that matches a CISPro result value expressed in a specific unit.

    - **`unit` attribute**

      The Workbook unit key that identifies the unit matched by the Regular Expression pattern.

- **`Namespaces` element**

  The list of namespaces as required by the `Property` element value XPATH.

  - **`Namespace` element**

    A namespace prefix to URI mapping.

    - **`prefix` attribute**

      A unique prefix that identifies the namespace within the XPATH.

    - **`uri` attribute**

      The URI of the namespace.

  - **`SearchTypes` element**

    Contains SearchType elements that define the available search types in the material import dialog.

    - **`SearchType` element**

      A available search type, which corresponds to an item in the material import dialog Types list.

    - **`key` attribute**

      Represents a user defined key to uniquely identify the search type.

    - **`searchExecuterKey` attribute**

      Specifies the key of the user defined search executer used to execute the search. Omitting this key indicates the use of the default container search executer. See the matchingPatterns element.

    - **`queryValidatorKeys` attribute**

      One or more comma delimited query validator keys that are applied to the query parameters to ensure validity. Omitting this attribute indicates the use of the default query validator. See the matchingPatterns element.

    - **`displayText` attribute**

      The display text appearing in the material import dialog Type list.

    - **`instructionText` attribute**

      The instruction text displayed in the material import dialog when the search type is selected.

  - **`QueryValidators` element**

    Contains `QueryValidator` elements that define the available custom query validators.

  - **`defaultKey` attribute**

    Assigns a unique user defined key to the default query validator to reference to in a `queryValidatorKeys` attribute of a `SearchType` element.

  - **`QueryValidator` element**

    Specifies a query validator definition.

  - **`key` attribute**

    A user defined key to uniquely identify the query validator. See SearchType element, queryValidatorKeys attribute.

  - **`type` attribute**

    Identifies the type of query validator. Currently only *py* is supported to specify a Python script.

  - **`modelVariableName` attribute**

    Specifies a user defined name for the variable providing script access to the IMaterialImportModel implementation that defines the query to validate.

  - **`errorVariableName` attribute**

    Specifies a user defined name of the variable that the script sets to contain the validation error message, if any.

  - **CDATA section**

    Contains the Python script that validates a query.

- **`SearchExecuters` element**

  Contains `SearchExecuter` elements that defines how a custom search is executed.

  - **`SearchExecuter` element**

    Defines a custom search executer.

  - **key attribute**

    A user defined key to uniquely identify the search executer. See SearchType element, searchExecuterKey attribute.

  - **type attribute**

    Identifies the type of search executer. Currently only *py* is supported to specify a Python script.

  - **`modelVariableName` attribute**

    Specifies a user defined name for the variable providing script access to the IMaterialImportModel implementation that defines the query to execute.

  - **`outputVariableName` attribute**

    Specifies a user defined name for the variable that the script sets to return the search results. Verify that your search results are the type `List<IDictionary<string, MaterialLookupField>>`. Each dictionary in the list corresponds to a single material container. A dictionary maps fully qualified property keys in the form *`<PropertySetKey>.<PropertyKey>`* to a corresponding `MaterialLookupField`. The utility method `ProcessQueryResults` on the resolver can convert a container result document retrieved from CISPro into the expected search results structure.

- **`Formatters` element**

  Contains `formatter` elements which translate CISPro results into Workbook expected data formats

  - **`Formatter` element**

    A formatter definition.

  - **key attribute**

    A user-defined key to uniquely identify the formatter. See Property element, formatterKeys attribute.

  - **type attribute**

    Identifies the type of formatter. Currently only *py* is supported to specify a Python script.

  - **`inputVariableName` attribute**

    Specifies a user defined name for the variable that contains the `formatter` script’s input value.

  - **`outputVariableName` attribute**

    Specifies a user defined name for the variable that the script sets to return the formatted value.

  - **CDATA section**

    Contains the Python script that effects the format change.

- **`Configuration` element**

  A configuration section specific to the material info resolver which contains Property elements that hold resolver-specific name/value property pairs.

  - **`name` attribute**

    Specifies the name of the property.

  - **`value`**

    Specifies the value of the property.

Configuring the IIS SSL Security Setting

Configure IIS to require SSL for the CISPro site:

1. Start IIS Manager (Start > Administrative Tools > Internet Information Services (IIS) Manager).
2. In the **Connections** pane, expand your Vault Server computer, expand **Default Sites**, and select **CISPro**.
3. In the center pane, double-click **SSL Settings** in the **IIS** group.
4. In the Actions pane, select **Require SSL** and then click **Apply**.
5. Restart **IIS**.

Importing the Inventory CisPro_SYS VOEXP File

If Workbook users require the following CISPro templates, import the `InventoryCisPro_SYS` voexp file:

- CISPro Formulation Experiment
- CISPro Analytical Procedure Experiment

To import this file:

1. Log in to Workbook using an account that has Templates Transfer permission.
2. In Notebook Explorer, click **Create** > **Import** > **From voexp** and select the following:

   \VaultDeploymentUtility\SystemVOexps\StandardPSDs.voexp
3. In the **Import *StandardPSDs.voexp*** dialog box:
   a. Click the **Action** column.
   b. In all rows except the one that contains *InventoryCispro_SYS PSD*, select **Ignore.**
   c. In the *InventoryCisPro_SYS PSD* row, select **Add**.
4. Click **Import**.

Configuring Multiple CISPro Servers

In the Vault Administration Console, configure each BIOVIA CISPro server, identified by the unique key assigned to the Resolver name attributed such as CisPro1 and CisPro2.

> **Tip:** To use a command-line utility to add or update permission configurations for services and applications, see "Using the Import/Export Application Permissions Utility" in the *Vault Server Administration Tools Guide*. The command-line utility enables you to easily export all editable application permissions, edit them using a text editor, tokenize them for use on more than one Vault Server if needed, and then re-import them into the same or a different Vault Server.

To use the Vault Administration Console to configure the servers, perform the following steps:

1. Open the Vault Administration Console and log on to Vault Server as a member of the Vault Global Administrators group.
2. Expand the Vault Server node and select **Application Permissions**.
3. In **Application Permissions**, double-click **LookupService**.
4. In **LookupService|MaterialInfoManager Properties**, click the **Configuration** tab.
5. In the **ResolverXML** row, open the XML editor in the value cell.
6. Add the following line in the **MaterialInfoLookup** configuration:

   ```
   <MaterialInfoLookUp>
      <Resolver name=<unique_CISPro_Name>
       typeName="Biovia.Notebook.CisProMaterialInfoLookup.
       CisProMaterialInfoResolver,
       BIOVIA.Notebook.CisProMaterialInfoLookup,
       Version=<Vault_Version_Number>, Culture=neutral,
       PublicKeyToken="" />
   </MaterialInfoLookUp>
   ```

7. Add a new row in the configuration tab.

   The Name field must match the name used in the previous step.

8. Copy the Value from the pre-existing CISPro row and use it as a template for the new CISPro row. Edit the configuration as described in Editing the CisProMaterialInfoResolver XML on page 51.
9. In the XML configuration of each CISPro server, include the optional `displayName` attribute to identify each CISPro server, for example:

   For example, in the configuration for CisPro1:

   ```
   <MaterialInfoResolver name="CISPRO" displayName="CISPro server #1">
   ```

   In the configuration for CisPro2:

   ```
   <MaterialInfoResolver name="CISPRO" displayName="CISPro server #2">
   ```

10. Click **OK**.

Appendix D:
Security Considerations

The following table lists some basic things to consider to ensure the security of your BIOVIA Workbook installation.

Subject	Key Points	References
Server setup	- Obtain your SSL certificate and create a corresponding `.pfx` file and password for it.	
Load balancing	Configure required ports and TLS 1.2 on the load balancer.	See previous references. For port assignments, also see Viewing the Port Numbers Used by Vault Server on page 82
Configuration parameter management	Use the Vault Configuration Tool to view and maintain ports, passwords, and other configuration settings that are stored on the Vault server.	In the *Vault Server Administration Guide*, see Vault Configuration Tool
Database password management	Encrypt the database passwords.	In the *Vault Server Administration Guide*, see: - Running the Password Replacer Utility - EncryptDBPasswords - Changing the Case of Encrypted Database Passwords
End-user access	Configure the initial users and groups you will need for Workbook. Assign the users to groups. Assign permissions to groups.	In the *Foundation Hub Administration Guide*, see Managing Security

Subject	Key Points	References
Repository setup	- Create separate repositories to segment data needed by separate user groups. - Subscribe users and groups only to the repositories that they are allowed to view. - Assign permissions based on experiment workflows. - Assign user and group access permissions at the folder level within a repository, as needed.	- In the *Vault Server Administration Guide*, see Repository Creation, Monitoring, and Maintenance - In the *Vault Server Administration Tools Guide*, see: - Manage Repository Subscriptions - Assigning Default Templates and Workflow Actor Roles - Defining Workflows - In the Workbook online help, see Assign Folder Permissions
Feature configuration	Set up supported features and integrations by configuring Vault Server application permissions.	- In the *Vault Administration Tools Guide*, see Configuring Application Permissions - In the Workbook online help, see Integrating with Other Products

Appendix E:
Reference Information

This appendix provides reference materials for BIOVIA Vault Server administrators.

Vault Server Installation Worksheets

Use the following worksheets to gather the information required for a new installation of BIOVIA Vault Server. Review and update them as needed before you upgrade an existing installation.

Oracle Database Worksheet

Parameter	Example or Default Value	Value for Your Site
Oracle database information		
ORACLE_HOME path for the Oracle Client	C:\Oracle\product\<version>	
Oracle Database Host name	server_name	
TNS listener port number	1521	
Oracle Database service name (Name of database that hosts the RAS and Vault schemas)	*MyDB.xyz.com*	
Oracle DBA username	SYSTEM	
Oracle DBA password	SYSPASSWORD	
RAS schema information		
RAS schema name and password	symyxdb/password	
RAS schema username and password	symyxdbuser/password	
Vault schema information		
Site schema name and password	vaultsite/password	
Home schema name and password	vaultuser/password	
File service schema name and password	vaultfileserviceuser/password	
Workflow schema name and password	wftools/password	
Vault administrator username	vault.admin	
Domain (Network domain of the Vault administrator. If you use local accounts on the Vault server, use the server name.)	mycompany	
Versioned repository schema name and password	vaultver1/password	
Tablespace information		

Parameter	Example or Default Value	Value for Your Site
RAS default tablespace name	SYMYXDB	
RAS user tablespace name	SYMYXUSER	
RAS temp tablespace name	SYMYXTEMP	
RAS index tablespace name	SYMYXIND	
RAS LOB tablespace name	SYMYXLOB	
RAS audit tablespace name	SYMYXAUDIT	
RAS audit index tablespace name	SYMYXAUDITIND	
RAS audit LOB tablespace name	SYMYXAUDITLOB	
Default tablespace name for Vault schema	VAULTDB	
Index Tablespace name for Vault schema	VAULTIND	
LOB tablespace name for Vault schema	VAULTLOB	

Vault Server Worksheet

Parameter	Example or Default Value	Value for Your Site
Workflow port number	7865	
Vault Server(Tomcat) port number	7864	
Vault Client Service port number	4499	
Mail server parameters		
SMTP server name	server_name	
Default *From* address	server_email_address	
Vault Administrator email	username@yourcompany.com	
Vault directories		
Vault log directory	C:\VaultLogs\	
Pipeline Pilot Server URL	PLP-Server.corp.com:9943	
Foundation Hub server URL	HUB-Server.corp.com:9953	

Installing Other Workbook Components

Installation Files and Scripts in BIOVIA_Workbook_2021.zip

The BIOVIA_Workbook_2021.zip file contains installers for all Workbook components, not just for the Vault Server. When you extract its content, a set of installation-related files and subfolders is created.

It is important to extract the content to a temporary folder whose path contains **no spaces**. The default extraction location is `C:\BIOVIA\Workbook`.

Installation Files for Vault Server and Database Setup

The following installers are extracted to the top level of the temporary folder into which you extracted the BIOVIA_Workbook_2021.zip file.

File Name	Description
Workbook2021.exe	Workbook Installer, also known as the "Super Installer." The Workbook Installer extracts files required for Vault Server, gathers server, database, repository, and other configuration data from you, and then guides you through executing database scripts, installing Vault Server, running the Vault Deployment utility, and running the VaultToHubBootstrapper.
`WorkbookSilentInstall.bat`	Windows batch file that you can use after you enter configuration data in the Workbook Installer, if you want to perform an unattended installation.
`WorkbookSilentInstall.ps1`	Windows PowerShell script that you can use after you enter configuration data in the Workbook Installer, if you want to perform an unattended installation.

Installation Files for Other Client and Server Components

The following installers are extracted to the **`Client and Server Installers`** subfolder of your temporary folder.

File Name	Description
`VaultAdministrationConsoleInstaller.exe`	Vault Administration Console installer
`WorkflowDesignerInstaller.exe`	Workflow Designer installer
`BIOVIA.Workbook.19.1.64bit.msi`	Workbook client x64 installer
BIOVIA.Workbook.19.1.msi	Workbook client x32 installer

- For details about installing the Vault Administration Console, see Install the Vault Administration Console on page 9.
- For details about installing the Workflow Designer, see Install BIOVIA Workflow Designer (Optional) on page 28.
- For details about installing the Workbook client components, see the *Workbook Client Installation Guide*.

Database Scripts

The following scripts are extracted to the `DatabaseScripts` subfolder of your temporary folder. The Workbook Installer prompts you through running these scripts.

File Name	Description
`AddRepository.bat`	Creates a new versioned repository.
`CreateNewRepositoryUser.bat`	Creates the schema owner of a new versioned repository.
`CreateTablespaces.bat`	Creates new tablespaces.
`CreateUserAccounts.bat`	Creates the schema owners for RAS and Vault.
`DelExternalReps.bat`	Deletes external version 5 repositories.
`DeployDatabaseSchemas.bat`	Deploys a new Vault Server database and upgrades Vault Server database.
`ReportSchemaState.bat`	Validates the Vault Server database after it is installed or upgraded.
`Pre-Install CheckScripts\ PreInstallCheck.bat`	Check pre-installation or pre-upgrade state of the server.

Query Service Security Plug-in

The installation file and instructions for this plug-in are extracted to the IDS subfolder of your temporary folder.

Installing and Uninstalling the Vault Administration Console

Installing the Vault Administration Console

To install the Vault Administration Console, perform these steps:

1. (Upgrades Only) Remove the previously installed version. For details, see Installing and Uninstalling the Vault Administration Console on page 71.
2. Navigate to the folder to which you extracted BIOVIA_Workbook_2021.zip, by default `C:\BIOVIA\Workbook`, and then navigate to its `Client and Server Installers` subfolder.
3. Execute `vaultAdministrationConsoleInstaller.exe`.

Uninstalling the Vault Administration Consol

To uninstall the existing version of Vault Administration Console and remove the `ObjectCache` and `Symyx Administrator Tools` folders:

1. Log on to the Vault Server as an administrator.
2. Open the Add/Remove Programs window, select your existing version of Vault Administration Console, click **Remove**, and then click **Yes**.
3. In Windows Explorer, navigate to the `Symx Technologies` folder under `c:\ProgramData.`
4. Under `Symx Technologies` folder, delete the `ObjectCache` subfolder, but do **not** delete any of its other subfolders.

> **IMPORTANT!** Do **not** delete `Symyx Technologies, BIOVIA`, or `LocalStorage` folders. The result is data loss.

5. Navigate to the `Program Files` folder, which will be one of the following:
   - C:\Program Files\Symyx
   - C:\Program Files (x86)\Symyx
   - C:\Program Files\Accelrys
   - C:\Program Files (x86)\Accelrys
   - C:\Program Files\BIOVIA
   - C:\Program Files (x86)\BIOVIA
6. Delete the `Symyx Administrative Tools <version>` folder.

Installing and Uninstalling Workflow Designer

Installing Workflow Designer

To install Workflow Designer:

1. Browse to the `<temp_install_folder>\Client and Server Installers` folder.
2. Right-click the following setup program, and then choose **Run as Administrator**:

   `WorkflowDesignerInstaller.exe`

For more information, see the *BIOVIAWorkflow Designer*online help.

Uninstalling Workflow Designer

Uninstalling Workflow Designer involves removing the program, backing up any customization DLLs and the corresponding config file, and then deleting the `Workflow Designer` folder.

To uninstall Workflow Designer:

1. Use an administrator account to log in to the computer where Workflow Designer is installed.
2. Use Windows **Add/Remove Programs** to remove Workflow Designer, and verify that it is no longer listed after the uninstall process completes.
3. Navigate to `C:\Program Files (x86)\BIOVIA\Workflow Designer` and:
   a. Copy any customization DLLs and the customized `Symyx.Workflow.Designer.exe.config` file to a different folder.
   b. Delete the `Workflow Designer` folder.

Uninstalling BIOVIA Workbook Client

To uninstall the previous version of BIOVIA Workbook client:

1. Use Windows Add/Remove Programs to uninstall BIOVIA Workbook Client Manager, and then verify that it is no longer listed after the uninstall process completes.
2. Check the `C:\WINDOWS\system32` folder for a file called `BiPrnDrv.ocx` file and remove it if it exists.

Starting the Vault Services

Use the Windows Server Manager to start the Vault Server services.

Note: The Oracle instance that BIOVIA Vault Server connects to must be started before the Vault services. If the database is shut down for any reason, stop the Vault services, restart the Oracle instance, and then restart the Vault services.

To start the Vault services:

1. Open the Windows **Server Manager** and choose **Configuration** > **Services**.
2. Start the following services in this order:
   a. World Wide Web Publishing Service
   b. Vault Tomcat Server Service
   c. Vault Workflow Service
   d. Vault Message Processing Service
   e. Vault Hub Synchronization Service
   f. Vault Client Service

Stopping the Vault Services

IMPORTANT! Before you shut down the Oracle database or start an upgrade, ensure that all users are logged off, and then stop the Vault services.

To stop the Vault services:

1. Open the Windows **Server Manager** and choose **Configuration** > **Services**.
2. Stop the following services in this order:
   a. Vault Client Service
   b. Vault Hub Synchronization Service
   c. Vault Message Processing Service
   d. Vault Workflow Service
   e. Vault Tomcat Server Service
   f. World Wide Web Publishing Service

Vault Server Oracle Database

This section contains general information on the Vault Server Oracle database.

About Vault Schema Objects

BIOVIA Vault Server repositories are used to organize data. You can use the repositories to separate data by location, intended use, and application. Repositories are analogous to file shares in a network system. Each repository is stored in a dedicated Oracle user account to provide flexibility in deployment.

BIOVIA Vault Server has five main repositories:

- **Site** is used for system operation.
- **Home** is used for temporary storage.
- **Versioned** is used for permanent data storage.
- **Fileservice** is used for file section content.
- **Workflow Tools** is used to track information for Vault objects.

Repository types are extensible to meet new application needs.

Repositories are represented by the Repository `VaultObject`. This object contains all information needed to describe the operating parameters of the repository, including its Oracle connection information. The following table describes the Vault repository schemas.

Vault Schema	Repository	Description
Site	Yes	Defines the Site repository that stores the system configuration data, including users, groups, repository definitions, assemblies, object locator, add-ins, and workflows. End-user data, such as documents and templates are not stored in the Site repository.
Home (User)	Yes	Defines the Home repository as a location for temporary object storage that are not included in the official intellectual property records of the company. Each user in the Vault is assigned a folder in the Home repository. The folder is the Roaming repository for the user and stores the objects, profile, and other data for the user. The Home repository for the user stores only the latest version of the files. The Home repository allows deletes and synchronization. The Home repository does not allow auditing, workflow, or archiving.
Versioned (Notebook)	Yes	Defines the document management repository in Vault. The Versioned repository tracks changes and preserves version history. A versioned repository stores all versions, allows auditing, workflow, and archiving. The versioned repository does not allow deletes or synchronization.
FILESERVICE	No	Defines the schema for all file section content for documents. The FILESERVICE schema is required.
WorkflowTools (WFTools)	No	Defines the WorkflowTools schema for workflow tracking information for the Vault objects, and all repositories that participate in a workflow. The WorkflowTools schema is required for an operational workflow.

Database Configuration Files

The following database configuration files are used to identify environment-specific details about your database.

variables.db.config

Provides the Oracle server connection information and tablespace names. Tablespace names are optional. BIOVIA recommends that you keep the default tablespace names listed in the `variables.db.config` file.

- **`DbServer`**

  Specify the Oracle Server name.
- **`DbPort`**

  Specify the connection port number.
- **`DbServiceName`**

  Specify the name that clients can use to connect to the database.

variables.RAS.config

- **`RASSchema`**

  Specify the Oracle user account.
- **`RASSchemapass`**

  Specify the Oracle user account's password.
- **`RASUser`**

  Specify the Oracle user account.
- **`RASUserpass`**

  Specify the Oracle user account's password.
- **`DirectUser`**

  Specify the Direct user account.

variables.setup.config

Provides the tablespace location and names.

- **`DefaultTablespacePath`**

  Specify the Oracle data files path.

vaultvariables.siteconfig

- **`SiteUser`**

  Enter the Oracle user account name.
- **`Sitepass`**

  Enter the Oracle user account's password.
- **`uname`**

  Enter the vault.admin account that you defined for the installation.
- **`domain`**

  Replace the `SYMYX IC` domain with the actual domain name for your site.

- **`siterouser`**

  Enter the name for the Site's read-only user.
- **`siterouserpass`**

  Enter the password for the Site's read-only user.

> **Notes:**
> When updating the `vaultvariables.siteconfig` file, do the following:
>
> - Use the Vault Global Administrator account as the network and domain account.
> - Replace the SYMYX IC domain with the actual domain name for your site.
> - Use the Vault Site read-only (`SiteUser.ro`) user name when configuring the Vault Site datasource in Pipeline Pilot.

vaultvariables.nb#.config

Contains variables for the versioned repositories.

- **`RepositoryUser`**

  Enter the Oracle user account name.
- **`Repositorypass`**

  Enter the Oracle account's password.
- **`Repository name`**

  Create a unique repository name surrounded by single quotes (for example, `'PharmaLab'`).

Creating Multiple Repositories

You can create multiple versioned repositories. Create a copy of the `nb#.config` file and replace the pound (#) symbol with the number of each versioned repository. You must use consecutive numbers for the repositories. For example:

- `vaultvariables.nb1.config`
- `vaultvariables.nb2.config`
- `vaultvariables.nb3.config`

When you create unique repository names, surround each name with single quotes (for example, `'Labteam'`).

vaultvariables.user1.config

Contains variables for the Oracle "Home" repository.

- **`RepositoryUser`**

  Enter the Oracle user account name.
- **`Repositorypass`**

  Enter the Oracle user account's password.

vaultvariables.wftools.config

Contains variables for the Workflow repository.

- **`WFToolsUser`**

  Enter the Oracle user account name.
- **`WFToolpass`**

  Enter the Oracle user account password.

variables.fileservice.config

Contains the variables for the FileService repository.

- `FileserviceUser`

  Enter the Oracle user account name.
- `Fileservicepass`

  Enter the Oracle user account's password.

VaultSetup.exe Configuration Reference

The BIOVIA Vault Server setup program, VaultSetup.exe, gathers the information described in this section and stores it in the `workbook_config.xml` file. The Vault Server setup program and database scripts subsequently use the parameters stored in this file to install Vault Server and set up the database.

Server Configuration Parameters

Directories

- `Install`

  Represents the installation directory. The Install field value is populated with the default installation location `C:\ProgramFiles (x86)\BIOVIA`. If you installedVault Server in a different location, update the `Install` field to your current installation directory.
- `Log`

  Specify the directory for the Vault log files. The default location is `C:\VaultLogs`.

Foundation Connection

- `Pipeline Pilot URL`

  Specify the HTTPS URL for the BIOVIA Foundation Hub in the following format:

  `https://<Fully-qualified server name>:<port_number>`

  The default value is 9943. If you used a different port, specify the port number that you used.
- **Foundation Hub URL**

  Specify the HTTPS URL for BIOVIA Foundation Hub or the load balancer in the following format:

  `https://<Fully-qualified server name>:<port_number>`

  The default HTTPS port number is 9953. Use the HTTPS Port that has been specified for Foundation Hub at your site.
- `Name`

  Specify the administrator account name used to log in to Foundation Hub.
- `Password`

  Specify the administrator account password used to log in to Foundation Hub.

SMTP Connection

- `SMTP Server`

  Specify the values for your environment (for example, `mail.mycompany.com`).
- `Port`

  Specify the port number used for the SMTP connection.

- **`Email To`**

  Specify the administrator sender name (for example, `admin@mycompany.com`).
- **`Email From`**

  Specify the administrator recipient name (for example, `admin@mycompany.com`).

Certificate

- **`File (.pfx)`**

  Enter the name or browse to the `.pfx` file which you had generated from the certificate for the Vault middle tier machine in the IIS Manager on the Vault Server machine. If you are using a load-balanced configuration, enter the name of the `.pfx` file of the certificate for the load-balancer.
- **`Name`**

  Enter the Vault Server name that a user would enter in the Workbook client application. For example, this could be the fully qualified domain name (FQDN) of the Vault Server middle tier machine or the virtual server name in a load-balanced configuration.
- **`Password`**

  Specify the password for the `.pfx` file of the certificate.

Service Ports

Default values are already populated for the ports. The Vault Server installer checks if there are any conflicts for these port numbers and reports the conflicts when you click either Save (to save the parameters) or Install. If there are conflicts, select other open ports.

- **RAS**

  Specify the port number for the RAS connection.
- **Workflow**

  Specify the port number for Workflow Service.
- **VCS**

  Specify the Tomcat server port number for the Vault Client Service (VCS).

Vault Endpoint

- **Endpoint**

  Enter the Fully Qualified Domain Name (FQDN) of the Vault Server or the Load-Balancer Server, that is, the name of the Vault Server that a user would enter in the login dialog box for Workbook Client applications.

Database Configuration Parameters

Site Connection

- **`Datasource`**

  Specify the connection string to the Oracle database.
- **`User Name`**

  Specify the name of the Oracle schema.
- **`Password`**

  Specify the password of the Oracle schema.

File Service Connection

- `Datasource`

  Specify the connection string to the Oracle database.
- `User Name`

  Specify the name of the File Service user.
- `Password`

  Specify the password of the File Service user name.

RAS Connection

- `Datasource`

  Specify the connection string to the Oracle database.
- `User Name`

  Specify the name of the Oracle user.
- `Password`

  Specify the password of the Oracle schema.
- `RAS User Name`

  Specify the name of the RAS user.
- `RAS User Password`

  Specify the password of the RAS user.

Workflow Connection

- `Datasource`

  Specify the connection string to the Oracle database.
- `User Name`

  Specify the name of the Workflow Service user.
- `Password`

  Specify the password of the Workflow Service user.

Importing a SSL Certificate PFX File into the Trusted Root Store

To import a PFX certificate:

1. Launch Microsoft Certificates for Local Computer:
   a. Select **Start > Run**.
   b. Type **certlm.msc**.
   c. Press **Enter**.
2. From Action, select **All Tasks** > **Import**.
3. In the Certificate Import Wizard, ensure that Local Machine is selected and click **Next**.
4. On the File to Import page, select the .PFX file and click **Next**.
5. On the Password page:
   a. Type the password for the .PFX file.
   b. Select **Mark this key as exportable** and **Include all extended properties**.

   c. Click **Next**.

6. On the Certificate Store page, select **Place all certificates in the following store**, and click **Browse**.
7. In **Select Certificate Store**, select the **Trusted Root Certification Authorities** and click **OK**.
8. Click **Next** and then click **Finish**.

Configuring Workbook User Accounts, Groups, and Permissions

Use Foundation Hub to configure user accounts, groups, and application permissions for Vault Server and Workbook client users. For details, refer to the *Foundation Hub Administration Guide*.

Predefined Groups and User Accounts

- **Global Administrators**

  Members of this group can manage various aspects of the Vault Server and Workbook client application. This group has **Vault|Administrator** permissions.

  Predefined user accounts that are members of this group include:

  - Message Processing Service, which handles messages for indexing and keeps the Workflow history current
  - Request Management, which manages the laboratory work order process for Workbook users to integrate with BIOVIA Request Management
  - vault.admin, which performs system administration tasks
  - Workflow Service, which manages any custom workflows you have implemented

- **Repository Administrators**

  Members of this group can manage repositories.

- **Vault Services**

  Members of this group can access the Vault Services web pages.

- **Vault Users**

  Members of this group can log in to Vault and Workbook.

Adding User Accounts

To add user accounts, log in to the Foundation Hub with the Global Administrator permissions. In Foundation Hub, create each user account and assign each account to the group that provides the permissions the user requires. You cannot assign permissions directly to individual user accounts.

To add user accounts:

1. Navigate to the Foundation Hub Home page using a URL similar to the following:

   ```
   https://<server_name>.<domain_name>:<port_number>/foundation/hub
   ```

2. Open **Admin and Settings** > **Security** > **Users**, and then click **Add User**.
3. Add a **Last Name**, and optionally **First Name** and **Email**.
4. Choose the appropriate **Account Type**:
   - **Database**: Use for accounts that need direct access to the Vault repository.
   - **Directory**: Use for end-user accounts, which typically correspond to the accounts configured in Windows Active Directory.

> **Tip:** You can use the `add-user.ps1` PowerShell script to quickly create large numbers of user accounts based on existing accounts in Windows Active Directory. This script is installed in `C:\Program Files (x86)\BIOVIA\VaultAdministration\Powershell` when you install the BIOVIA Vault Administration Console. For more information, see the *Vault Server Administration Tools Guide*.

- **Service Account**: Used for accounts that applications rather than individual users require to access Workbook functions.

5. Select the appropriate **Group Memberships** for the user account. The user account inherits all permissions of all groups to which it is assigned.

Editing User Accounts and Configuring Additional Properties

To change a user account's original group membership, inactivate the account, flag it for automated updating by external systems, or link it to additional information in an external system, use the **Edit** option:

1. Open **Admin and Settings** > **Security** > **Users**.
2. Select the user and click **Edit**.
3. Enter any required changes:
   - **Related Groups/Users**: Associate the account with other groups without assigning the account to the groups, and associate it with other users.
   - **Account is active**: Enable or disable the account to allow or prevent it from logging in to Workbook.
   - **Include account in automated updates**: Flag the account to give external systems the ability to access and update it.
   - **External Id**: Enter the ID of an external system that provides additional information about the account.

Adding Vault and Workbook Groups

To add Vault and Workbook groups, log in to the Foundation Hub with Global Administrator permissions.

1. Navigate to the Foundation Hub Home page using a URL similar to the following:

   `https://<server_name>.<domain_name>:<port_number>/foundation/hub`
2. Open **Admin and Settings** > **Security** > **Groups**.
3. Click **Add Group** (⊕).
4. Define the following:
   - **Name:** Give the Group a unique and descriptive name.
   - **Email address:** Email contact for the group.
   - **Description:** Additional information about the group.
   - **External Claims:** Choose an External Claim to assign to the group and click Assign. You can assign more than one to the group. See Managing External Claims.
   - **Member Groups:** Assign one or more existing groups to belong to this group. Users that belong to those groups will belong to this group implicitly.
   - **Member Of:** Assign one or more existing groups for this group to be a member of. Users that belong to this group will belong to those groups implicitly.

- **User Roles**: Assign one or more User Roles for this group.
- **Permissions:** Assign one or more Permissions granted to users that are members of this group.

5. Click **Save.**

Restricting Group Permissions

To restrict group permissions:

1. Open **Admin and Settings** > **Security** > **Groups**.
2. Open the group you want to edit.
3. Click **Edit**.
4. In the **Permissions** area, select the **Denied** check box for the permissions you want to deny to the group.
5. Click **Save**.

Viewing the Port Numbers Used by Vault Server

You can find the port numbers used by Vault Server in the Windows Internet Information Services (IIS) Manager. In the IIS Manager, you can view the port bindings for HTTP and HTTPS. The default ports are 80 and 443.

> **Note:** In these instructions, `<installation_directory>` indicates the BIOVIA Vault Server installation location. The default location is `C:\Program Files (x86)\BIOVIA\Vault`.

The port number used for the Vault Client Service is specified in the Catalina service file `<installation_directory>\VaultClientService\conf\server.xml`, as the value of the `port` attribute in the `Connector` element.

The following example shows the Catalina service element in the `server.xml` file.

```
<Service name="Catalina">
<Connector
  protocol="org.apache.coyote.http11.Http11NioProtocol"
  connectionTimeout="20000"
  port="4499"
  maxThreads="200"
  scheme="https"
  secure="true"
  SSLEnabled="true"
  keystoreFile="C:\Program Files
(x86)\BIOVIA\Vault\VaultClientService\conf\eln.pfx"
  keystorePass="mypassword"
  keystoreType="PKCS12"
  clientAuth="false"
  sslProtocol="TLS" />
```

The port numbers for Pipeline Pilot are specified in the `<pps_install>\install\tokens.config` file. The port numbers are the values in the `port` and `sslport` properties.

Where `<pps_install>` Pipeline Pilot is the installation location, by default this is `C:\Program Files\BIOVIA\PPS`.

The default the Pipeline Pilot port numbers are 9944 and 9943. For more information, see **Reconfiguring Ports** on the Administrators tab in the Pipeline Pilot Help Center.

Manually Running the Vault Deployment Utility

The Vault Deployment Utility adds the required system objects and default templates to the server. Normally, you execute this utility from the Workbook Installer, but you can also run it manually.

To manually run the utility:

1. Open a command window and change directory to the <installation_folder>, by default `C:\BIOVIA\Workbook\VaultDeploymentUtility`

2. Enter the following command:

   ```
   VaultDeploymentUtility <server> <domain>\<administrator-user> <password>
   <deploymentType>
   ```

   where:

   - **`<server>`** is the fully-qualified domain name for the BIOVIA Vault Server.
   - **`<domain>\<administrator-user>` `<password>`** is the domain, username, and password of the Vault Global Administrator account you identified in the `vaultvariables.site.config` file.

     Notes:
     If the password uses any of the special characters identified in the following table, represent them in your command by using the corresponding escape sequence:

Special character	Escape sequence
blank space	" "
double quote (")	""""
single quote (')	^'
carat (^)	^^
ampersand (&)	^&
open angle bracket (<)	^<
closed angle bracket (>)	^>
pipe (|)	^|

   - **`<deploymentType>`** is "new" or "upgrade <version>"

   Examples:

   ```
   VaultDeploymentUtility server1.xyz.com xyz\vault.admin mypassword new
   ```

   ```
   VaultDeploymentUtility server1.xyz.com xyz\vault.admin mypassword
   upgrade 19.1
   ```

3. Leave the Vault Deployment Utility running and periodically check on its progress until it has completed.

   The utility can run for an extended period of time, especially for a new installation. Your command window output should look similar to the following:

   ```
   <deployment type> installation deployment steps starting...
          Begin deployment step (1 of x): Stop Vault Services
          Successful

          Begin deployment step (2 of x): Publishing assemblies from C:\version_
   ```

```
number.x\workbook2021\VaultDeploymentUtility\Assemblies\Assemblies.zip.
        Successful
```

4. When the utility is complete, verify that the command window displays the following:

   `Vault deployment completed successfully.`

5. Verify the following Vault Services are running:
   - Vault Client Service
   - Vault Message Processing Service
   - Vault Tomcat Server
   - Vault Workflow Service

IMPORTANT! If an error occurs, a message similar to *"`At least one deployment step failed`"* is displayed.

Examine the logs for details of the failure. For more information, see the `VaultDeploymentUtility.Debug.log` located in the same folder as the Vault Deployment Utility executable.

If the Vault Deployment Utility stops due to an error, you must fix the problem, rename the `VaultDeploymentUtility.Debug.log`, and re-run the Vault Deployment Utility.