insightsoftware

Hubble Desktop and Web

Administration and Configuration Guide

Version 25.3

August 2025

Contents

Document Information

Notices

Copyright

Disclaimer

This guide is designed to help you to use the Hubble applications effectively and efficiently. All data shown in graphics are provided as examples only. The example companies and calculations herein are fictitious. No association with any real company or organization is intended or should be inferred.

Version History

Date	Revision	Software Version	Comments
30th August, 2025	1.0	25.3	Initial issue for 25.3.

Customer Support

For more information regarding our products, please contact us at https://insightsoftware.com/hubble/.

For upgrade questions, parallel version installations, product support, training, and documentation, contact Professional Services at http://central.insightsoftware.com/ or email HubbleServices@insightsoftware.com.

Hubble Overview

Hubble® is an integrated suite of performance management apps. It offers reporting, analytics and planning in a single, real-time solution that fully understands your ERP. Hubble is built on a simple idea – that things should be easy. Hubble integrates your critical business systems so end users at all levels of the organization have access to live data – extraordinarily fast. With this type of visibility, everyone can easily understand, manage and predict the business. Redundant processes disappear, and a high-performance business can emerge.

Our software provides real-time access to your ERP data. Administrator is used for working with the administration elements of Hubble. This includes the creation and management of database repositories, setting up and managing user profiles and permissions, and implementing individual business preferences.

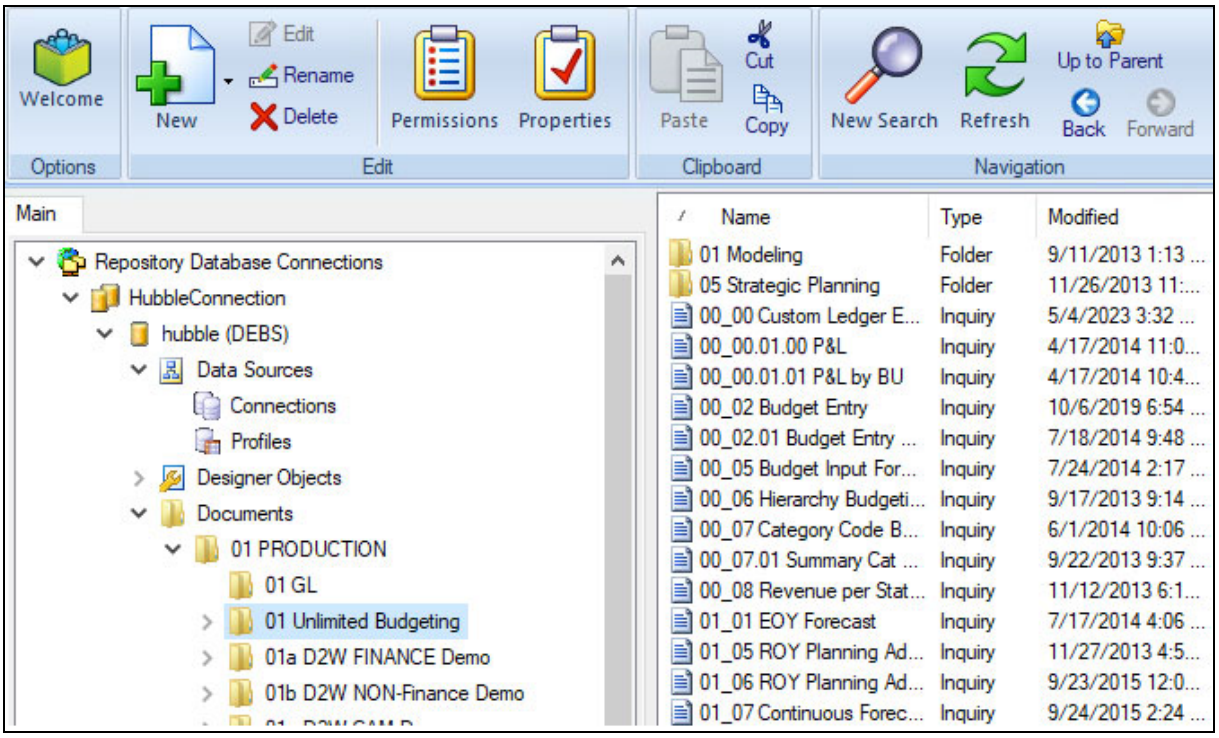
While many of the components in the process are more technical (e.g. the installation of the application, license key management and upgrades), there is considerable functionality that can be made available to business users. In this guide, you will review each of the components depicted in the process flow; however, the focus is primarily on those functions that facilitates managing users, documents, user capabilities and scheduling documents.

Administrator User Interface

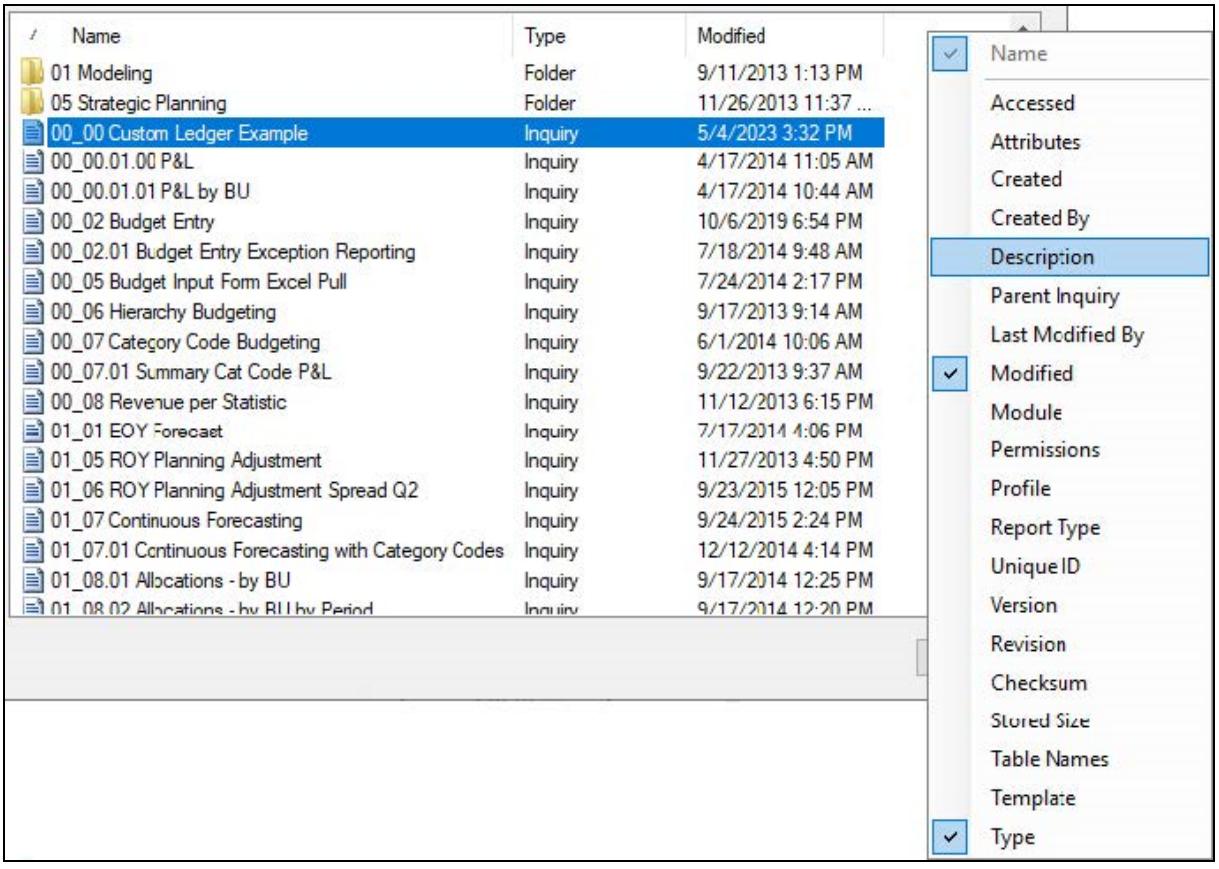
The main parts of the Administrator user interface are:

- **Backstage View** - Accessed by clicking the File menu, from this view you manage your documents
- **Menus** - The different ribbon menu tabs across the top of the screen
- **Filters** - Used to select the data on which to run the inquiry
- **QBE Line** - An additional way to filter on data being returned in the inquiry
- **Inquiry Results** - The results returned after running the inquiry
- **Status Bar** - A customizable bar that displays at the bottom of the screen, showing specific details about the inquiry
- **Zoom Control** - A control used to zoom in and out of the inquiry

Beneath the ribbon menus are a left and a right panel. The right-hand panel of Administrator displays the contents of the selected item from the left-hand panel. The display and tree structure have the same 'look and feel' of the Windows Explorer file management tool.

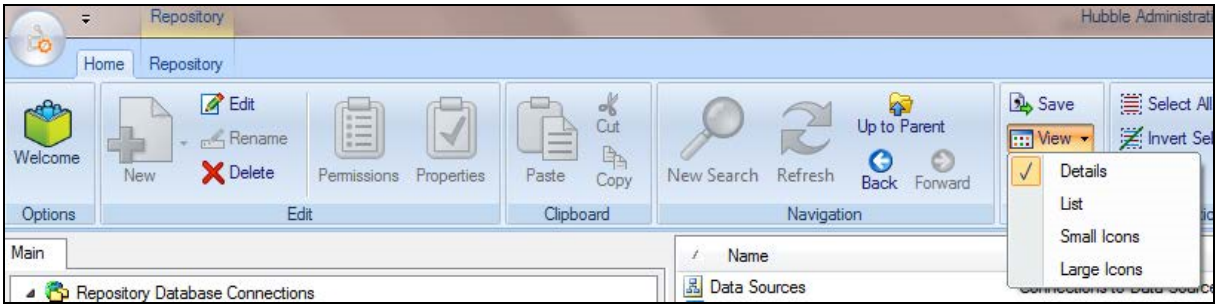


To add a property column to the list of items displayed in the right-hand panel of the dialog, right-click on the headings and select the property from the menu that is then displayed.



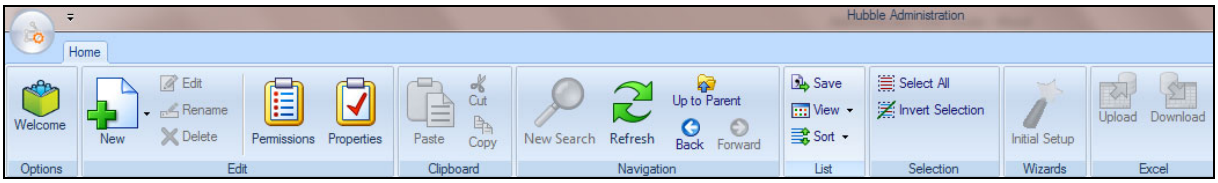
The contents of the ribbon menus are contextual; they change according to the item you in which you are focused. The ribbon buttons are active when they are in color and grayed out when inactive.

Some buttons on the ribbon have a drop-down menu to the right of them, such as the **View** button in the **List** group on the **Home** menu. There are 4 options available from View: Details, List, Small Icons and Large Icons. In this case it means that the information in the right panel can be viewed with details, as a list, or as small or large icons.



Menus

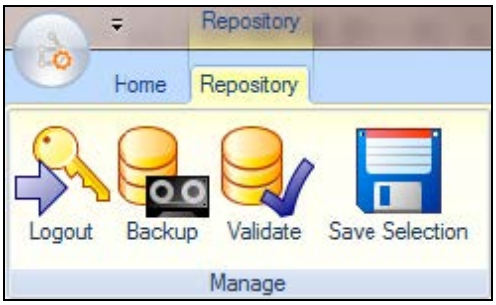
Home Menu



- **New**: Creates a new item within Administrator
- **Edit**: Edits an item
- **Rename**: Renames an item you have created
- **Delete**: Deletes the selection
- **Permissions**: Sets the Permissions for the selected object
- **Properties**: Reviews the properties and use of an object
- **Paste**: Pastes from the clipboard
- **Cut**: Cuts the selected text or element from its current location to the clipboard
- **Copy**: Copies the selected text or element to the clipboard
- **New Search**: Opens the Search tab on the left-hand panel
- **Refresh**: Refreshes the view to reflect any changes you have made
- **Up to Parent**: Moves your selection up the tree directly to the parent level
- **Back**: Goes back to the last selection within the tree
- **Forward**: Goes to your most recent selections after using Back

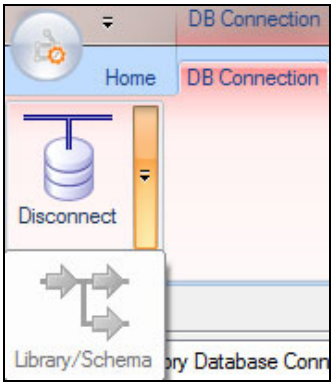
- **Save**: Saves the list you have in the right-hand panel to a .csv spreadsheet compatible (comma separated) file
- **View**: Arranges the right-hand panel by List, Details, Small Icons, Large Icons
- **Sort**: Sorts the elements of the right-hand panel by Name, Type or Modified
- **Select All**: Selects all of the elements within the right-hand panel
- **Invert Selection**: Selects the un-highlighted elements
- **Initial Setup**: accesses the wizard to help you connect to an existing Hubble Repository, or to create a new one
- **Upload**: Uploads a Microsoft Excel® spreadsheet into the Object Repository for use in Budgeting
- **Download**: Downloads a Microsoft Excel spreadsheet from the Object Repository to your local drive

Repository Menu



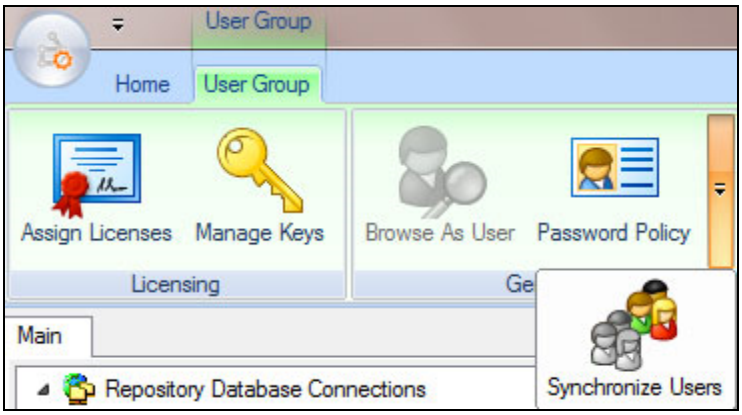
- **Logout**: Login/logout of the currently selected repository
- **Backup**: Backs up the Repository Database
- **Validate**: Validates the Repository connections and settings
- **Save Selection**: Saves the repository selection that Hubble will use upon launching the product. Saves the configuration and allows users to select and switch between repositories that are active.

DB Connection Menu

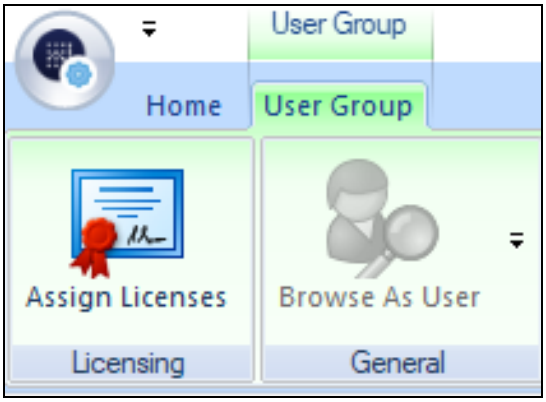


- **Disconnect**: Disconnects from the Repository Database Connection
- **Library/Schema**: Connects to a specific library/schema

User Group Menu for Standard Users

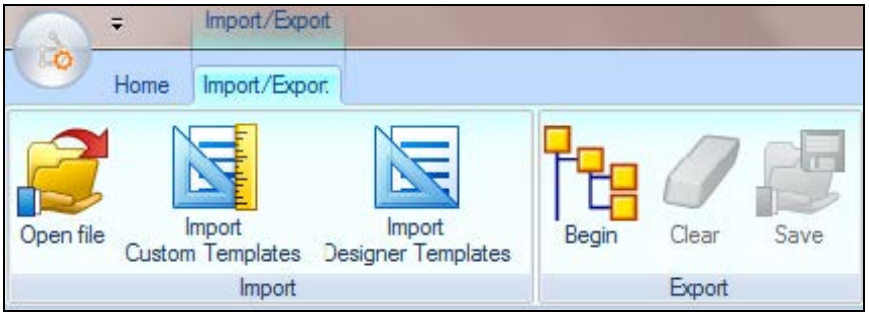


User Group Menu for Platform Users



- **Assign License**: Sets user licenses
- **Manage Keys**: (For Standard Users Only) Manages license keys
- **Browse as User**: Browses the repository as a specific user would view it
- **Password Policy**: Sets password policy for the repository
- **Synchronize Users**: Synchronizes users against the ERP system

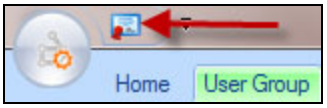
Import/Export Menu



- **Open File** - Imports a repository database file. (Used for customer-created reports and templates, including Designer Express templates.)
- **Import Custom Templates** - Imports an Hubble-created customer custom requisitioned template.
- **Import Designer Templates** - Imports a standard Hubble-created/delivered Designer template.
- **Begin** - Creates a blank repository area for copying multiple objects.
- **Clear** - Clears the repository area created by the **Begin** button.
- **Save** - Saves the repository area and its contents into a repository database file.

Quick Access Toolbar

The **Quick Access Toolbar** (QAT) is located at the top left corner of the screen and it allows you to quickly access the operations you access most frequently, such as **Run** and **Save**.



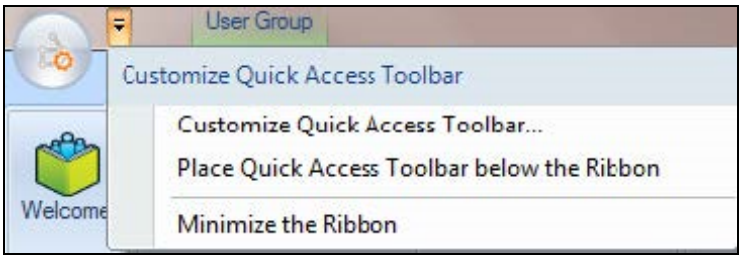
When you click on the arrow to the right of the Quick Access Toolbar, you have 3 options:

- Customize the Quick Access Toolbar
- Place Quick Access Toolbar below the Ribbon
- Minimize the Ribbon

To undo an option in regards to the Quick Access Toolbar - To undo an option, such as the option to place it below the ribbon, click on the drop-down to the right of the **Quick Access Toolbar** and select that option again to deselect it.

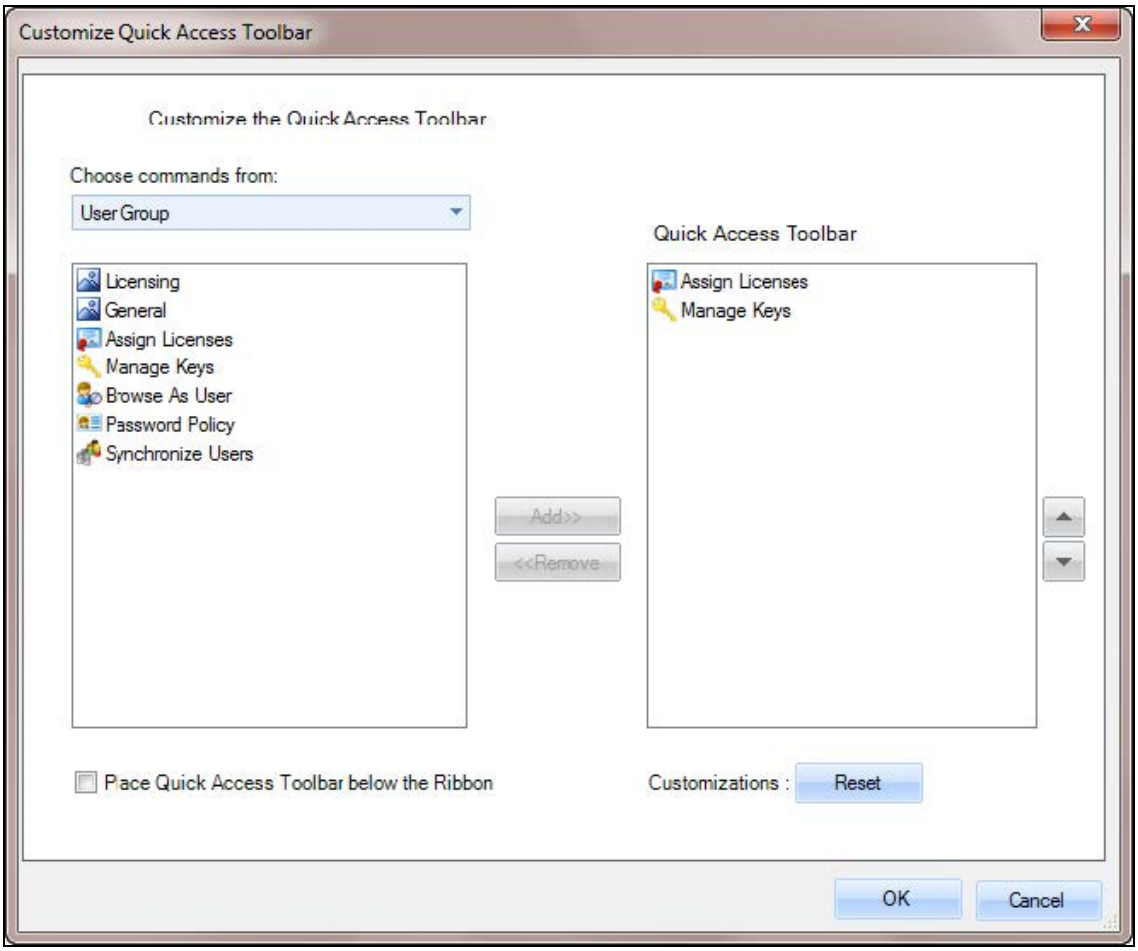
To customize the Quick Access Toolbar, follow these steps:

1. Click on the drop-down menu of the toolbar and select **Customize Quick Access Toolbar**:

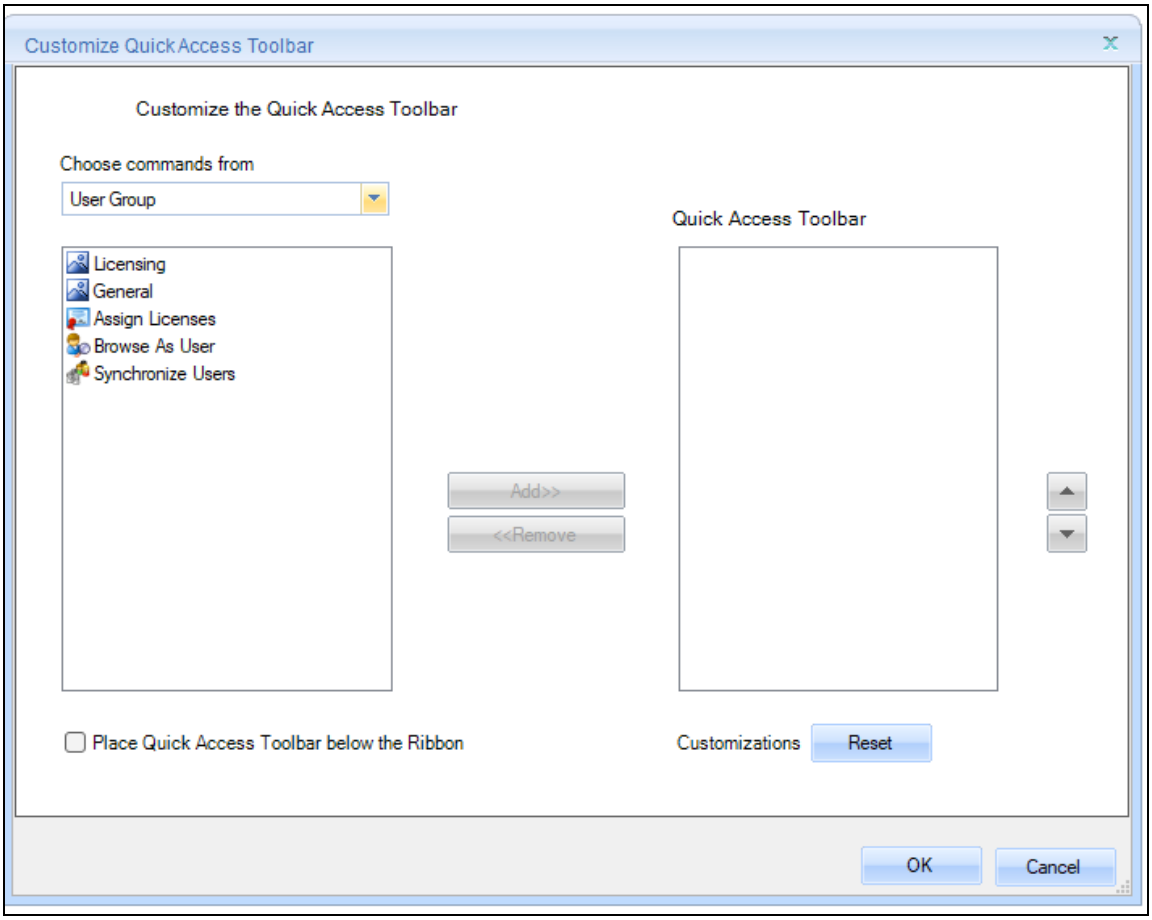


2. Under **Choose commands from**, choose the group under which the button is located on the ribbon, and then select it by moving it to the right hand side. On the right side is a list of all buttons that are currently included in your **Quick Access Toolbar**.

Customize Quick Access Toolbar for Standard Users



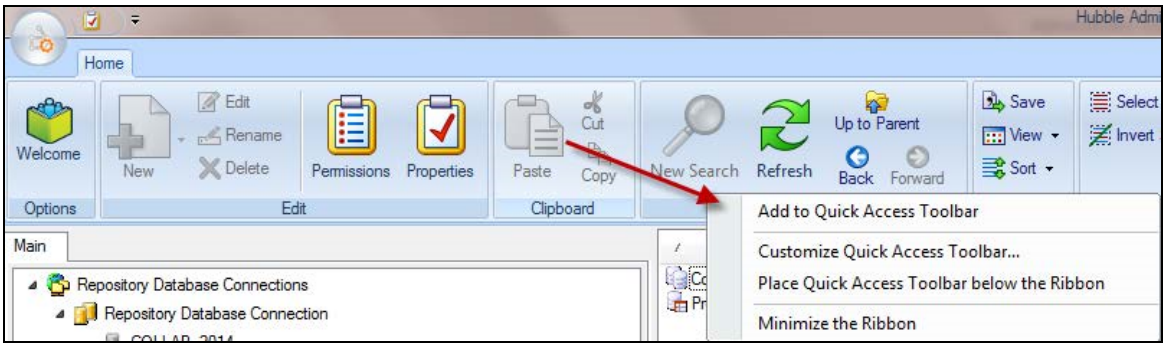
Customize Quick Access Toolbar for Platform Users



3. Click **OK** to save your changes and return to the inquiry.

Shortcut to add commands to the Quick Access Toolbar:

1. Highlight the button/function you wish to add to the **Quick Access Toolbar**, e.g. Paste.
2. Right-click and select **Add to Quick Access Toolbar**:



Licenses Related To User Types And Capabilities

Standard User Licenses

Licenses relate to user types and capabilities as follows:

- **Advanced Distributions (DIS)** – When included in the license key, the web Distribution functionality will be extended to allow HTML distribution, which can additionally be distributed to non-Hubble users via a hyperlink in an email. The DIS key is a user-based license key, but is not assigned to named users. The key operates in defined blocks, for example, 100, 200, and will allow for this number of non-Hubble users to receive distributions. Each unique non-Hubble user will count towards this total.
- **Configurator (CFG)** – A user with a Configurator license has the ability to control the user interface and the templates made available to other Hubble users. Typically, this is a highly experienced user of the underlying ERP system.
- **Console (CON)** – A Hubble Viewer user has the ability to view and run Hubble inquiries created by other users, all in real-time, in order to make timely and better-informed decisions. This product is designed for users who will not be creating reports and do not need the full functionality available to Power users.
- **Currency Restatement (CUR)** – This module provides currency conversion of period balances for the General Ledger, Job Cost, and Advanced Cost Accounting Balances templates.
- **Hubble Analytics (HUA)** is a Global repository license, which means it does not need to be assigned to individual users. Once included in the license key, Hubble web will allow for 8 views to be used per page in a workspace. Without this key, only 1 view can be used per workspace page. When this key is added to a repository the Application Pool on the web server must be recycled.
- **Reporting (RPT)** – Hubble Power users must have this license assigned along with the license(s) for the specific modules for which they should have access.

Platform User Types (Available from version 25.3 onwards)

Platform users are assigned one of three user types through the Platform, which automatically includes specific module assignments:

Designer User

- Automatically includes: DXD, RPT, CFG, HUB modules
- Can be assigned additional modules through Administrator

Power User

- Automatically includes: CON, HU5 modules
- Must have RPT (Reporting) license for module access
- Can be assigned additional modules through Administrator

Viewer User

- Automatically includes: CFG, HUB modules
- Cannot be assigned additional modules beyond default allocation

> **Note:** For Platform users, the user type (Designer/Power/Viewer) is controlled at the Platform level, while additional module assignments are managed through the Hubble Administrator License Assignment screen.

Modules

A module is a grouping of templates that correlates to its respective module within your ERP system, such as Accounts Payable or General Ledger. Via **License Assignments**, administrators determine to which modules Designer and Reporting user should have access.

Our available modules include:

- **Advanced Cost Accounting (ACA)**
- **Accounts Payable (AP)**
- **Advanced Pricing (APR)**
- **Accounts Receivable (AR)**
- **Budgeting (BUD)** - this is for the users that will be actively participating in budgeting/planning within Hubble. If a Power User (CFG, RPT licenses) has this, they will have the ability to create budget input forms. If a Viewer user (CON license) has this, they will be able to use the input forms to enter data.
- **Platform Users - Planning Module Mapping**:
  - **Designer SKU**: Automatically includes DXD, RPT, CFG, BUD, DXE, HUB + All Modules
  - **Power SKU**: Automatically includes RPT, CFG, BUD, DXE, HUB
  - **Viewer SKU**: Automatically includes CON, BUD, DXE, HU5, HU1
- Platform users receive these planning-related modules automatically based on their assigned SKU type, enabling full budgeting and planning functionality within their license tier.
- **Capital Asset Management (CAM)**
- **Cash Management (CM)**
- **Customer Relationship Management (CRM)**
- **Contract Service Billing (CSB)**
- **(Platform-specific) DEP and LAB**: Available exclusively on Platform for all Designer license holders. These modules have the following limitations:
  - DEP works only for users with Designer licenses.
  - LAB includes experimental functionality that works only when provided through Advanced Capabilities.

  - These modules appear in module assignment, but ISW support isn't provided for them.
  - When users hover over or select these modules, they see warnings about the lack of ISW support and are directed to submit feedback through the ISW Ideas Portal.

- **Designer Express (DX)**
- **Designer Express Developer (DXD)**
- **DX Data Entry (DXE)** - provides the ability to use Strategic Planning in Hubble. This functionality enables end users to design a budget or forecasting input form using any table in JD Edwards incorporated with user-defined data collection columns that hold key driver information for robust modeling.
- **Fixed Assets (FA)**
- **General Ledger (GL)**
- **Growers Management (GM)**
- **Homebuilder (HB)**
- **Human Capital Management (HCM)**
- **Human Resources (HR)**
- **Inventory (INV)**
- **Job Cost (JC)**
- **Lease Management (LM)**
- **Master Data (MD)**
- **Manufacturing (MFG)**
- **Manufacturing Resource Planning (MRP)**
- **Projects Accounting (PA)**
- **Payroll (PAY)**
- **Property Management (PM)**
- **Purchasing (POP)**
- **Reconciler (RCL)** - provides access to Reconciler, where users run inquiries built in the Reconciler module
- **Reconciler (REC)** - provides access to the module that is used to edit the Reconciler templates
- **Real Estate Management (REM)**
- **Scheduler (SCH)** - provides access to the Scheduler
- **Subledger Accounting (SLA)**
- **Service Management (SM)**
- **Sales Order Purchasing (SOP)**

- Tax (TAX)
- Timesheet (TS)
- Warehouse Management (WM)

Third Party Product Licenses

Required licenses for third party products are as follows:

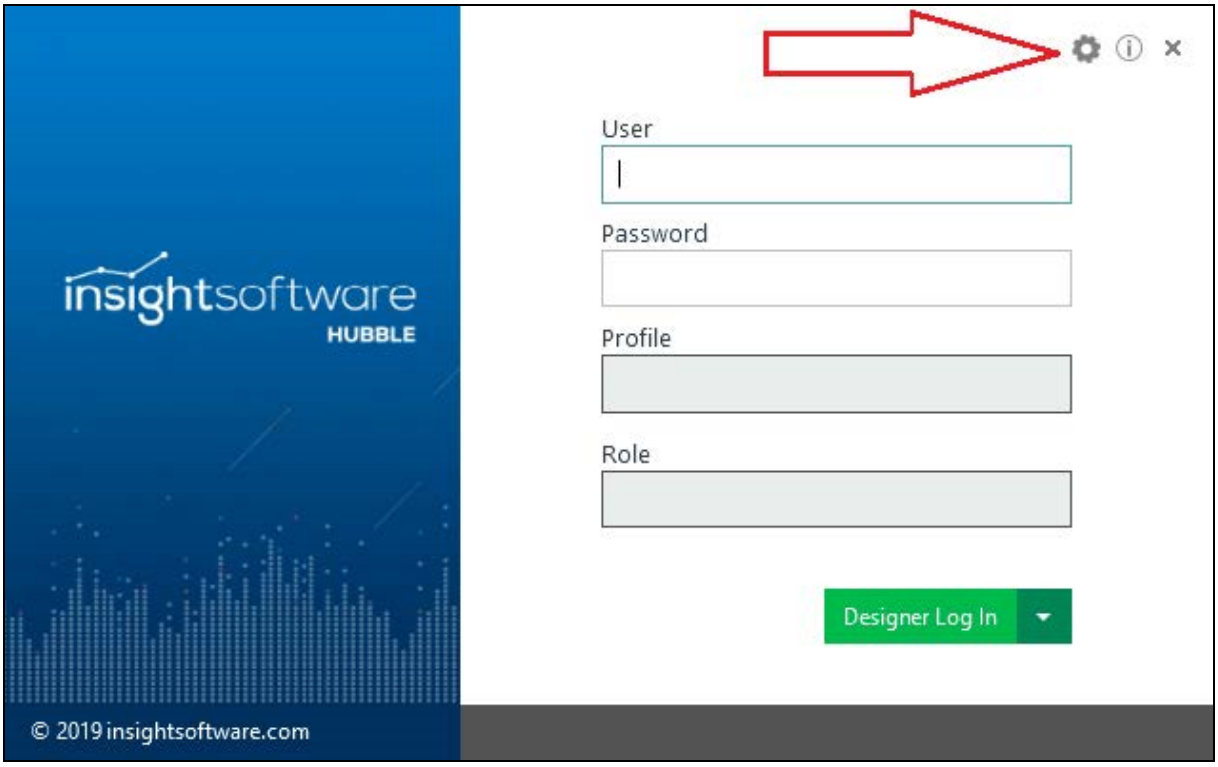
- IMB Optim (OPM)
- QSoftware Security (QSF)

Getting Started With Administrator

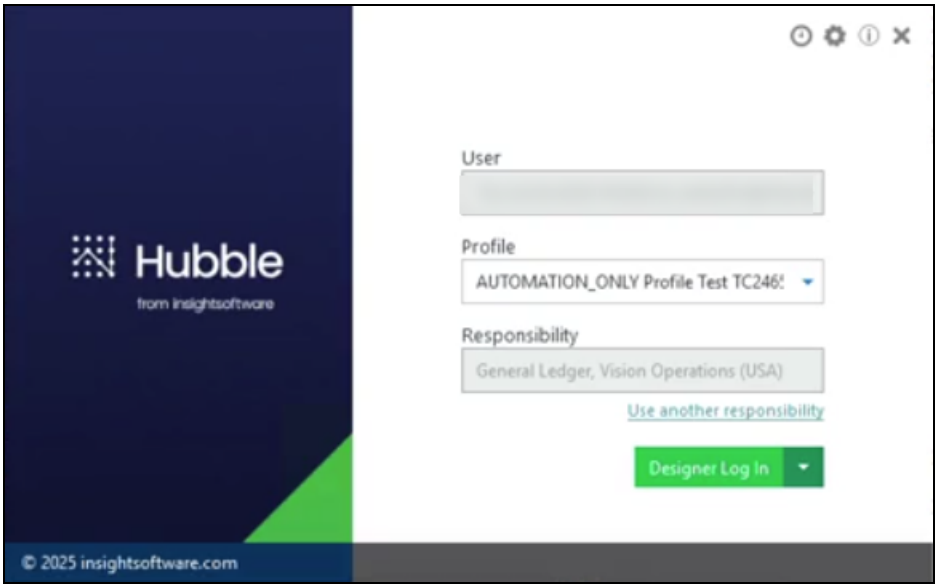
Accessing Administrator

To access the Administrator Application, click on the cogwheel symbol on the Hubble login screen.

Standard Version



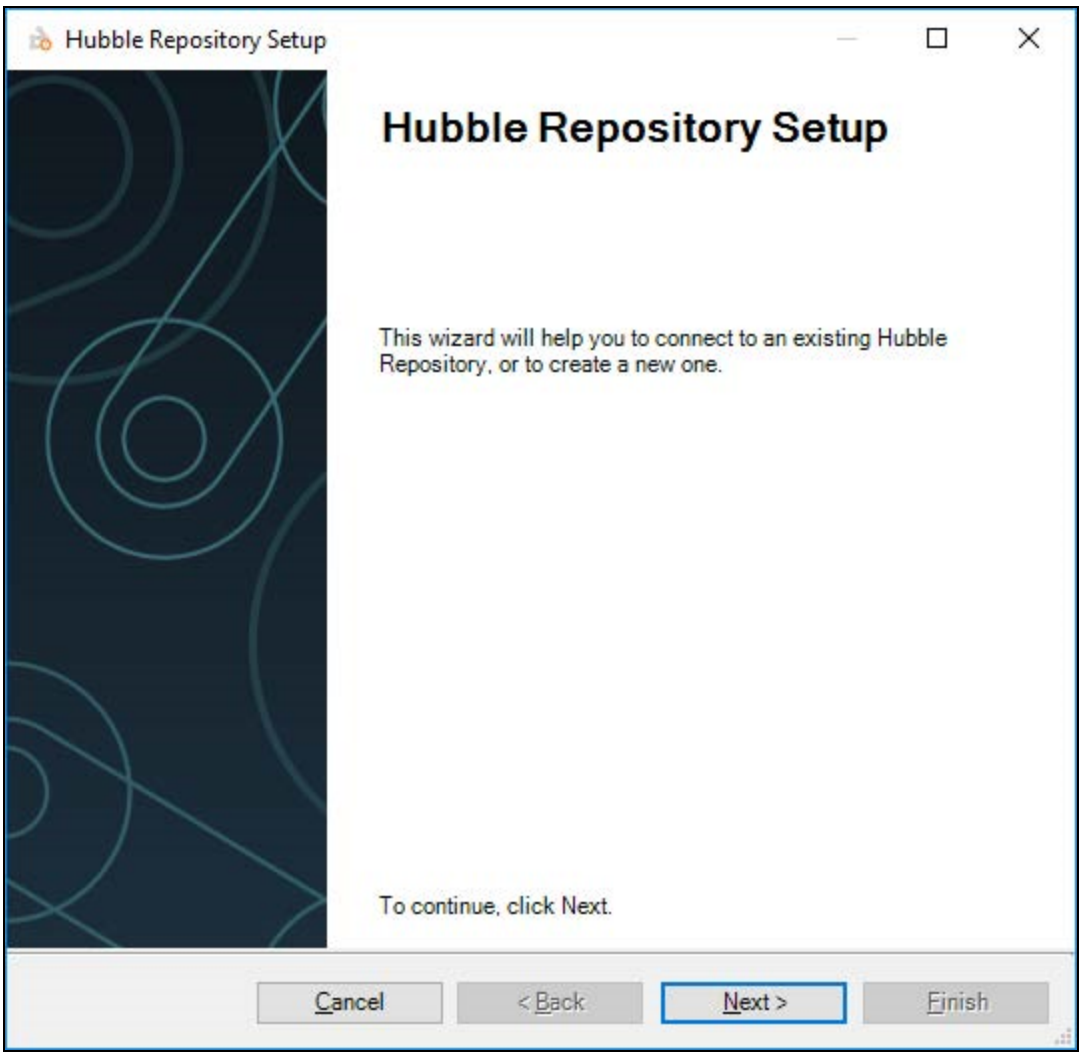
Platform Version



Hubble Repository Setup Wizard

The first time you open Administrator after installing it, the **Hubble Repository Setup** wizard dialog will automatically open.

The **Hubble Repository Setup** wizard is a tool for administrators to setup a connection to the repository.



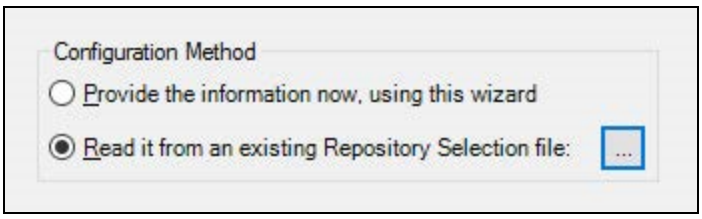
You can close the wizard by clicking **Cancel** or by clicking the **Close Window (X)** on the top right corner of the wizard dialog.

If you close the wizard and need to open it again, click the **Initial Setup** button on the **Home** menu, or click **New** then **Repository** (this option will be disabled if a repository has already been setup.

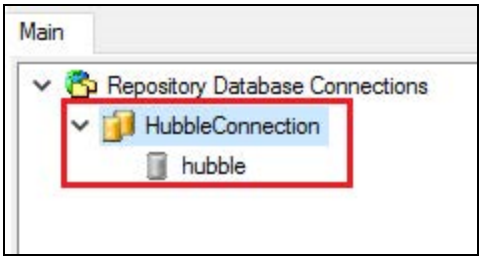
The configuration carried out within the wizard is as follows:

1. When the welcome page of the wizard comes up, click **Next**.
2. In the **Choose Configuration Method** step, choose **Read it from an existing Repository Selection** file and then navigate to the saved .xml file by selecting the radio button and clicking the "..." button.

(The .xml file is commonly found within the Hubble install directory.)



Click **Finish** to close the wizard and create your repository. connection It is then listed in the Main tab. For example:

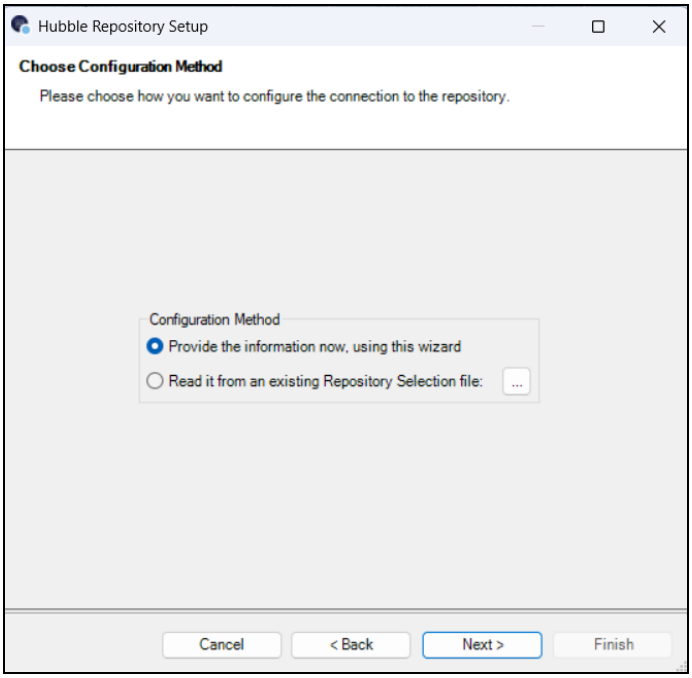


Note: Only one repository can be assigned to a connection. If multiple environments are required, it is recommended that multiple servers are used.

Create A New Repository

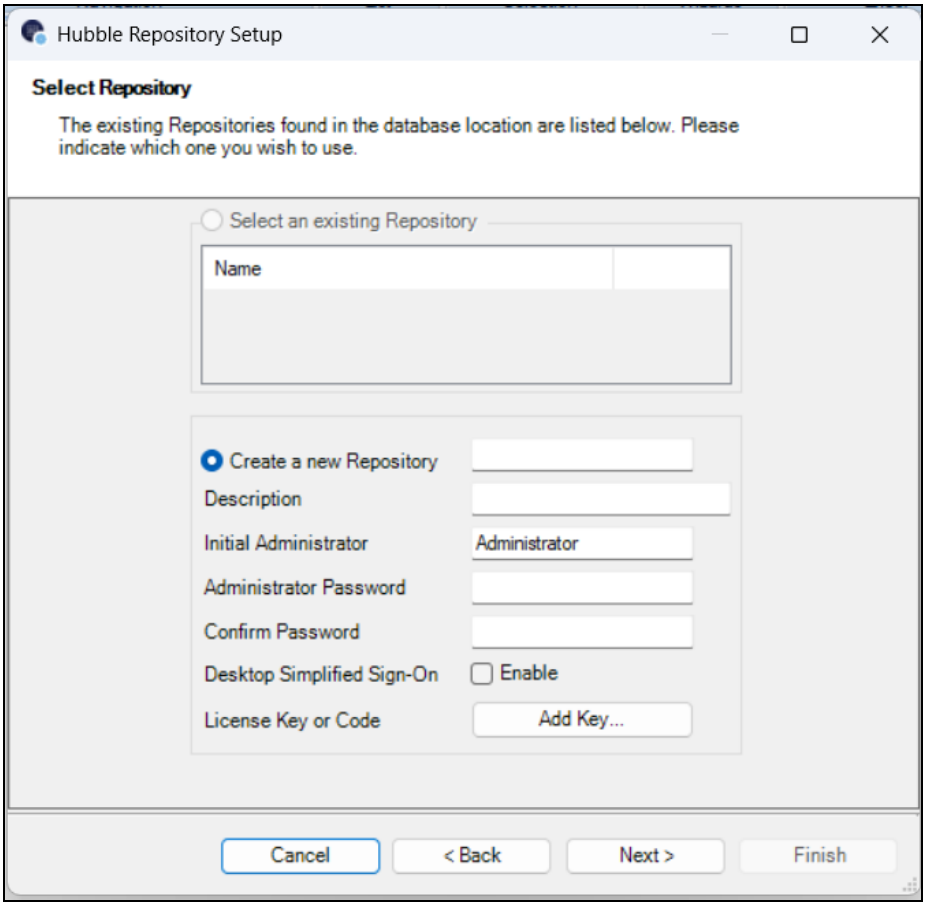
1. Open the HubbleAdministrator application. The **Hubble Repository Setup** wizard will appear. Click **Next**.

2. In the **Choose Configuration Method** step, choose **Provide the information now, using this wizard** option.



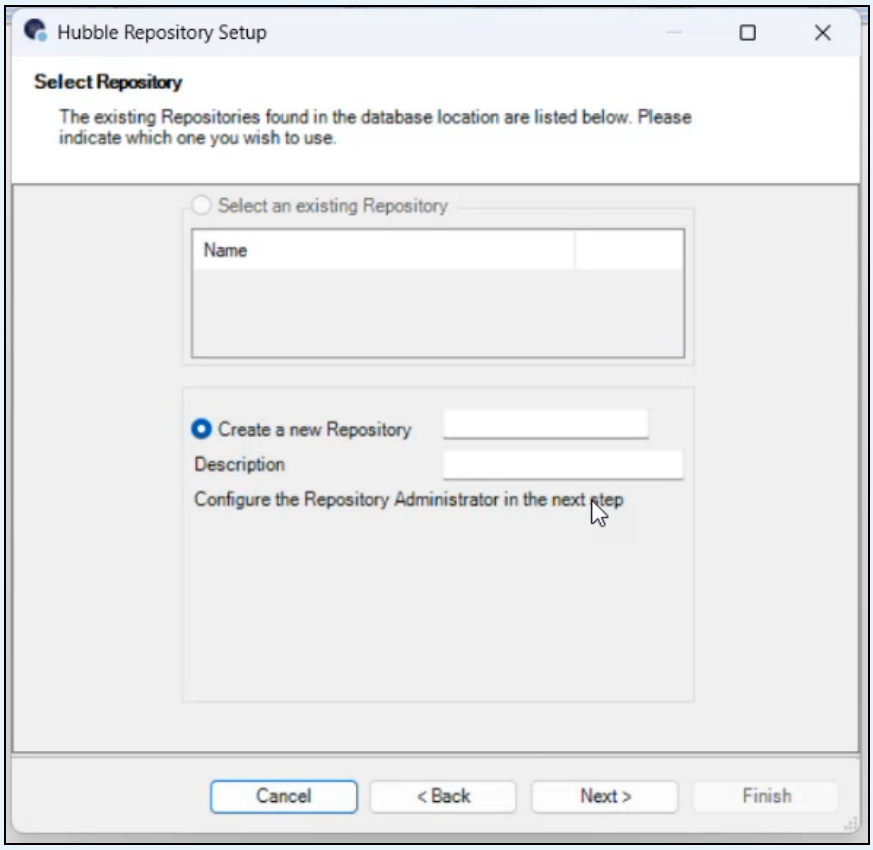
3. In the **Repository Database Connection** screen:
   - In the **Name** field under **Identification**, enter a repository name.
   - (Optional) Enter a description in the **Description** field.
   - From the **Type** drop-down list under **Data Source**, select the database type.
   - Select a provider from the **Provider** list.

   Verify that the **Connect automatically** check box is selected and click **Next**.
4. In the **Repository Database Connection Configuration** screen:
   - Enter the server name in the **Server** field.
   - Select **Use Windows Authentication** under **Login**.
   - Select a database from the **Database** drop-down.
   - Click **Next**.
5. In the **Select Repository** screen:



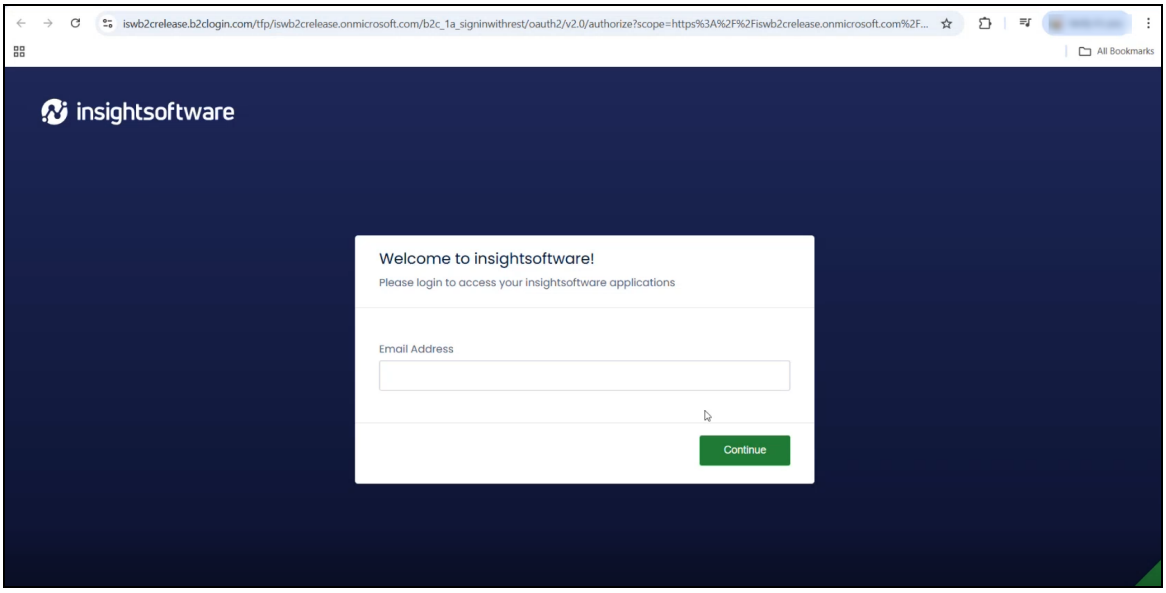
- Choose **Create a new repository**.
- Provide repository details:
  - Repository name
  - **Description (optional)**
  - **Administrator Password**
  - **Confirm Password**

> **Note:** For the Platform version (v25.3 onwards), you no longer enter the password during repository creation.



Click **Next**. For Standard authentication users, the repository is ready for use after this step.

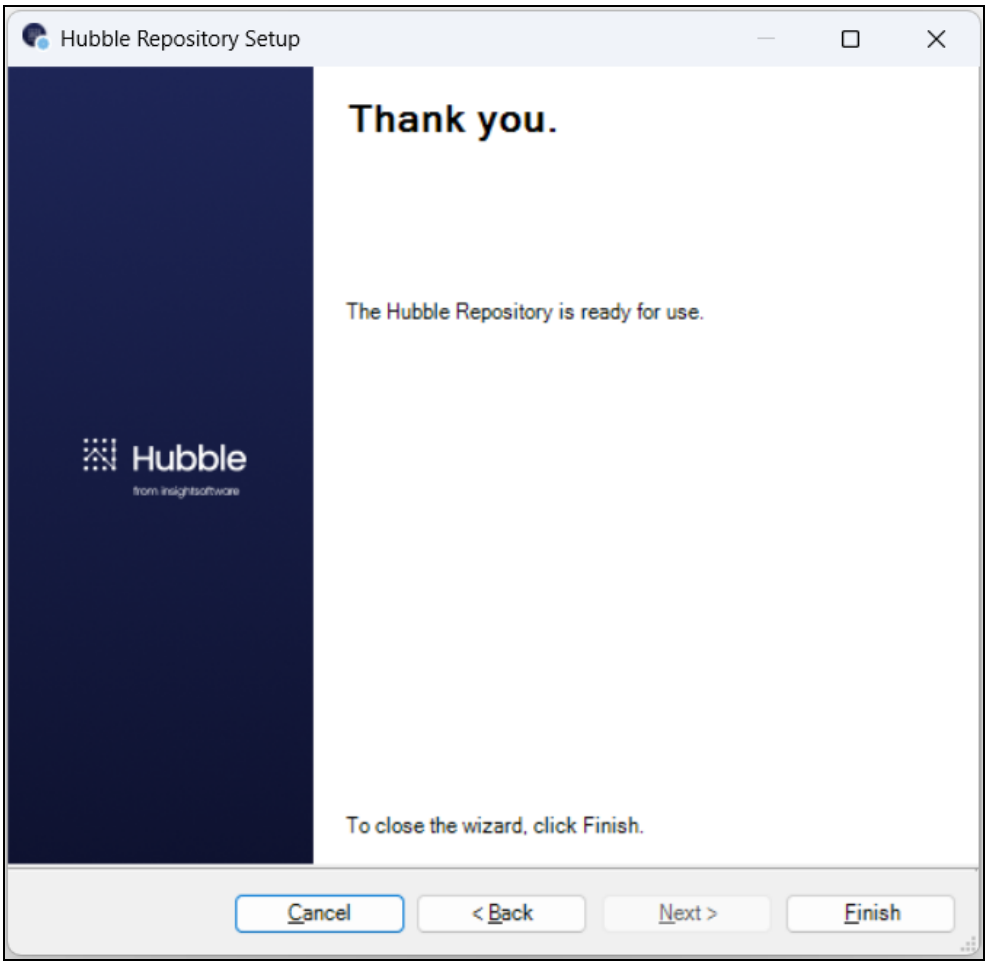
6. For Platform users, click **Next** to be redirected to the Platform authentication page in your browser window.



7. Enter the email address of the user who will be the initial administrator for this repository.

> **Note:** Choose this assignment carefully as this user will have full administrative control over the repository.

8. The system automatically returns to the Administrator tool.



9. After selecting **Finish**, the system prompts you to log in with administrator credentials.

10. Log in using the Platform administrator account you specified during repository creation.

Platform users can now access and use the repository.

Save The Repository Selection File

The Repository Selection File (or RepositorySelection.xml file) defines where the Object Repository is stored and how the software connects to it.

Once a new repository has been created or an existing one selected, the Repository Selection File should be saved in the Hubble directory for subsequent use for all users on that machine.

To save the Repository Selection File in the Hubble directory:

1. In the left panel under Repository Database Connection, right-click on the repository for which you wish to save the Repository Selection File.
2. Select **Save Repository Selection**.
3. A **Save As** dialog will be displayed, allowing you to specify the directory.
4. The file can be copied to other machines in order to use the same Repository selection.

> **Note:** If the `RepositorySelection.xml` file does not exist in the Hubble directory, the Login dialog will display the Initial Setup wizard, which will be used to select or create a repository.

You must be an administrator (having Windows administrative rights) in order to save into the installation folder as it is a protected folder. If you are not a local administrator of the workstation, you are not able to save the xml file into the Program File directory within Administrator.

There are 2 ways you can save the xml file into the install path outside of Administrator:

Option 1: Save the Repository Selection file to an allowed location and then move it into the install path from within Windows Explorer.

1. When saving the Repository Selection file in Administrator, save it to My Documents on your Desktop.
2. Use Windows Explorer to move or copy it to the Hubble installation folder (the default location for the installation folder is under Program Files).

Option 2: Run Administrator with Windows administrative rights.

1. Right-click on the **Administrator** shortcut.
2. Choose **Run as Administrator**.
3. Save the xml file directly into the Hubble installation folder (the default location for the installation folder is under Program Files).
4. If users try to launch Hubble without a RepositorySelection.xml file in the installation folder, an exception message displays.

Sign In To The Repository As A Standard User

If you selected **Standard Authentication** while installing the Hubble Desktop application and installed the standard version of Hubble Desktop, follow the given steps to log into the repository:

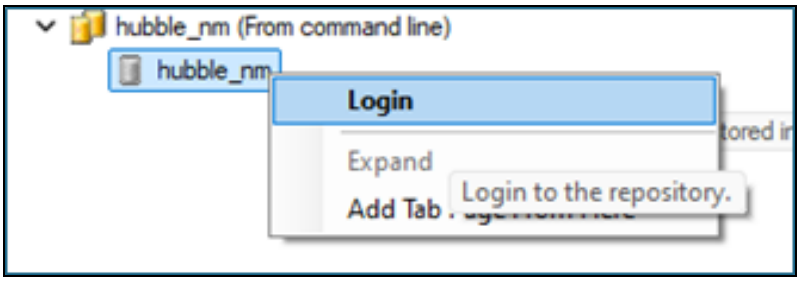
1. After completing the initial setup wizard or manually creating a repository, you will see the **Repository Database Connection** you have just created appear in the left panel of Administrator.
2. Open the **Repository Login** dialog by doing either of the following:
   i. Click on the underlying repository so the Ribbon automatically displays the **Repository** tab. Then click **Login** to open the **Repository Login** dialog.
   ii. Double-click on the repository name to open the **Repository Login** dialog.
3. In the **Repository Login** dialog, enter the login name and password that you specified in the Initial Setup for the Repository (e.g. 'Administrator').

4. Click **Login**. The Repository icon will change from gray to yellow if you have correctly entered in your login credentials.
5. Once Logged in, you can navigate using the + icons in the left-hand panel or click on the folder in the right-hand panel of Administrator.

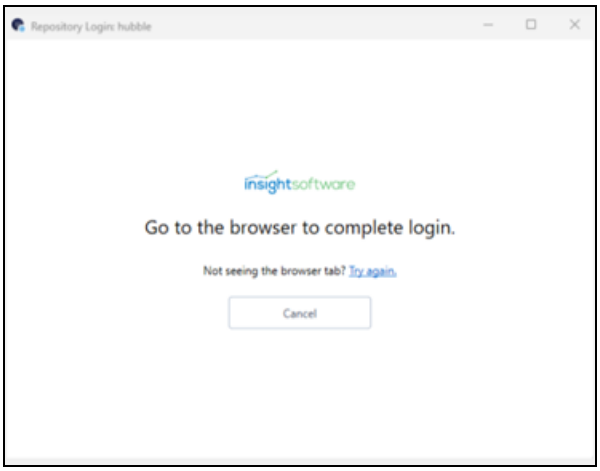
Sign In To The Repository As A Platform User

If you selected **Platform** while installing the Hubble Desktop application and installed the Platform version of Hubble Desktop, follow the given steps to log into the repository:

1. After completing the initial setup wizard or manually creating a repository, you will see the **Repository Database Connection** you have just created appear in the left panel of Administrator.
2. Right click the repository you have created and select **Login**.



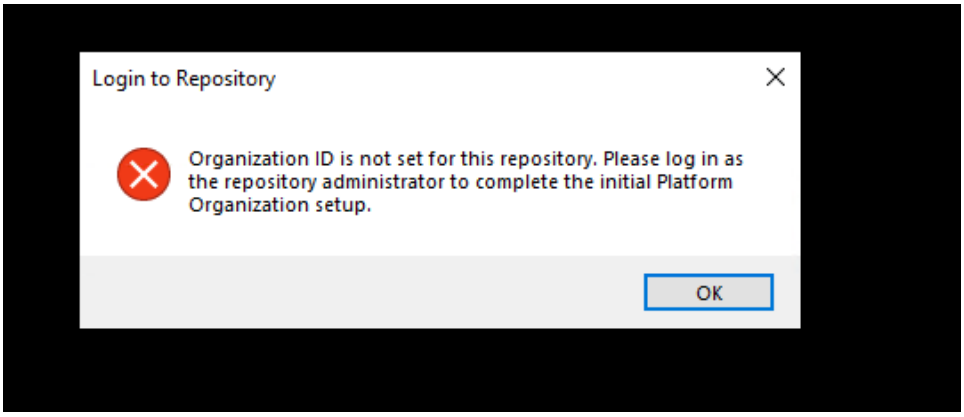
3. The Platform Login is launched in your browser window.



4. Enter your credentials and complete authentication. Upon successful authentication, the system returns you to the Administrator tool.

> **Important:** Sign in with the default administrator user for your first login. Using any other account will result in an error. This mandatory step maps your organization ID to the

repository to ensure smoother user synchronization for your customers.



CRITICAL: Export Users Immediately After Admin Login

Caution: User Role Loss Warning For existing customers, you MUST export users as your first action after logging in as Administrator. Failure to export users immediately will result in permanent loss of user role assignments.

Required Sequence:

1. Migrate Repository
2. Administrator Login
3. IMMEDIATELY export users - Do not perform any other actions before completing this step

Important: This export process is also required to import users onto the Platform. Without completing the export, you cannot proceed with user migration.

Back Up The Repository

During the configuration of the application server, repository backups are scheduled. See the *Hubble Supplementary Deployment Topics Guide* for more information on this.

Alternatively, you can back up the repository manually by following the below instructions. If you do it this way, be sure to save the backup files to a network location that is included with your regular disaster recovery services.

Note: The Administration tool backup only backs-up Desktop objects. It does not backup Web objects (Web objects are stored outside of the Desktop table structure and are bridged with special views).
When the Web version is installed, the Application server will automatically backup the full repository each night.

To back up your repository:

1. Log into your repository if you are not logged in already.
2. Either select the repository you wish to back up and click **Backup** on the Ribbon or right-click on the repository and select **Backup**.
3. You are then prompted to save the RDF file to the location of your choice.

> **Note:** It is recommended to put the backup files into a designated backup folder and in the file name include the specific repository information (such as the repository name) so that you can easily identify the backup files.

The following message is displayed when the backup is complete:

Once a repository is backed up, you can either use the **Import** function to bring in specific items from the backup, or the **Restore** function to bring in all items from the backup.

Restore A Repository From Backup

You can use the **Restore** function to add a new repository to an existing one or create a new one.

1. Log into your repository if you are not logged in already.
2. Right-click on the repository you wish to restore into and select **Restore**.
3. When the **Open File** dialog opens, navigate to and select the Repository Data File (RDF) you want to restore.
4. Click **OK**.
5. When the restore has completed, save the repository selection file to the appropriate Hubble installation path.

The repository being restored will then be appended to the open repository. Any incompatible files will be reported through a message dialog.

When you restore into a repository that has existing data, it adds any new reports that are not currently there. If the same report already exists in the repository and it is in the restore, the restore will *overwrite* the existing report. If a report lives in the repository currently and the restore does not have the report, you will still have the report. If a profile was renamed, a restore will bring it in again with the original name; otherwise it will *overwrite* the profile/connections if they are the same name.

Restoring As Part Of An Upgrade

If restoring from backup as part of an upgrade to Hubble, you will receive a temporary license key which with which you must replace the old permanent license key. Once the upgrade is completed and has been checked as satisfactory, for the standard version, you will receive a new permanent license key to replace this temporary license key. See **License Keys** for further details.

After the upgrade, the profile wizard for each profile must be run. This is so that any new tables included in the upgrade (as listed in the **Table Locations** screen) can be registered. See **Creating New Profiles** for details of the profile wizard.

Change A Repository Organization ID For Platform Users

When To Use This Procedure

Use this procedure only when the Platform account changes or when you create a new account but want to continue using the same repository. In these cases, follow the backend procedure to update the Organization ID.

Overview

When you onboard a client to the Platform, the Platform assigns them a unique Organization ID and Organization Name (for example, 905_Hubble Test). When you create a new repository with Platform integration enabled, you are prompted to provide an email address to authenticate with the platform. The administrator is the person who creates the repository. After the repository is created successfully, the administrator must sign in first. This initial sign-in ensures that the Organization ID is recorded properly in the database.

This procedure describes the manual process for changing a Repository Organization ID for Platform users. While not frequently needed, this process provides a recovery mechanism for situations where Organization IDs must be updated on the Platform.

Background

- During repository initialization, the system creates an organization property in the database with an empty string
- When a Platform administrator creates a repository, the system saves the organization value in the repository database
- For existing repositories, the Platform administrator who created the repository must log in first to complete the organization setup

Prerequisites

- Platform authentication enabled (version 25.3 or later)
- Access to SQL Server Management Studio or DBeaver

- Database administrator permissions
- Current organization ID and new organization ID values

Change The Organization ID

1. Open the repository database using SQL Server Management Studio or DBeaver.
2. Run the following query to verify the current organization ID setting:

```
SELECT * FROM Repositories
```

```
WHERE Section = 'Identities'
```

```
AND Item = 'OrganizationID'
```

```
AND Repository = 'YourRepositoryName'
```

3. Update the organization ID to the new value:

> **Note:** The `settingValue` format is `` `{orgId}_{orgName}` ``.

```
UPDATE Repositories
```

```
SET SettingValue = '945_Hubble Test'
```

```
WHERE Section = 'Identities'
```

```
AND Item = 'OrganizationID'
```

```
AND Repository = 'YourRepositoryName'
```

4. Have the platform administrator log in with the correct organization ID to complete the update.

Important Considerations

- Use this manual recovery process only when necessary.
- The Platform administrator who created the repository must log in first after any organization ID change.
- Platform users cannot log in if their organization ID does not match the repository ID.
- This process applies only to repositories using Platform authentication.

ERP Database Connections

Database Connections For JD Edwards

Create A New Database In Microsoft SQL Server

The steps for creating a new database are listed below; however be aware that these can vary depending on your version of Microsoft SQL Server. The links to documentation based on specific version numbers are listed below. If you still have further questions, please consult your Systems Administrator to complete this task.

From SQL Server Enterprise Manager:

1. Select **New Database**.
2. Provide a database name.
3. Click **OK**.

For detailed steps on creating a database, refer to these instructions: http://msdn.microsoft.com/en-us/library/ms186312%28v=SQL.100%29.aspx

Create A New Database User

The steps for creating a new database user are listed below; however be aware that these can vary depending on your version of Microsoft SQL Server. The links to documentation based on specific version numbers are listed below. If you still have further questions, please consult your Systems Administrator to complete this task.

From SQL Server Enterprise Manager:

1. Connect to the database server where the database has been created.
2. In the left panel, expand **Microsoft SQL Servers**.
3. Expand the **SQL Server Group** to be presented with a list of available servers.
4. Select the server for which you wish to create a user.
5. Expand the server selection.

6. Expand the **Security** folder.
7. Underneath the Security folder, right-click on **Login**.
8. Select **New Login**.
9. On the **General** tab of the **SQL Server Login Properties - New Login** dialog:
   i. Provide a name for the new user.
   ii. Select the **SQL Server Authentication** option.
   iii. Enter the password of your choice.
   iv. For the **default database**, select the database created for the Hubble Object Repository.
10. On the **Server Roles** tab of the **SQL Server Login Properties - New Login** dialog, leave the default selection.
11. On the **Database Access** tab of the **SQL Server Login Properties - New Login** dialog:
   i. Highlight the database created for the Object Repository.
   ii. Check the **Permit** item from the list of databases
   iii. Select the database roles of **public** and **db_owner**.
12. When you click **OK**, you will be asked to re-enter the new user's password.

For detailed steps on creating a database user, refer to these instructions:
http://msdn.microsoft.com/en-us/library/aa337545%28v=SQL.100%29.aspx

SQL Server Authentication Mode

The Microsoft SQL Server Authentication mode must be set to **SQL Server and Windows Authentication**. (If the authentication mode is set to Windows Authentication only, you will not be allowed to log onto the SQL Server database with the designated database user.)

To change the Server Authentication mode in SQL Server 2017, follow these steps:

https://docs.microsoft.com/en-us/sql/database-engine/configure-windows/change-server-authentication-mode

For detailed steps on to do this in other versions of SQL Server, you can link to those instructions from this webpage.

Create An Oracle Schema

Since the process of creating new databases can be done in a variety of ways within Oracle, a step-by-step guide is not provided here. Rather, it is described at an abstract level and you may need to consult your DBA to complete this task.

Prior to installing Hubble, you need to either create a new, empty Oracle database or a new schema within an existing Oracle database. No tables need to be created at this time; the Repository will be populated during the software configuration process.

Create A New Library/Schema In IBM DB2

Depending on the version of DB2 for i (formerly AS/400) you are in, the terminology will be different; what was called 'library' in older versions is now called 'schema' in newer versions.

There are two ways in which you can create the library/schema with a SQL collection, either via SQL or the iSeries Navigator. In either case, the Object Repository *requires that Journaling be enabled for the library/schema*. This is because the database must allow support for database transactions.

Option 1: Create the library/schema using a SQL command:

1. On the AS/400, use the CREATE COLLECTION function. (Do not use the CRTLIB command.)

Example: Create a library/schema called REPOSITORY:

CREATE COLLECTION REPOSITORY

Option 2: Create the library/schema using the iSeries Navigator:

1. Right-click on the library/schema selection.
2. Select **New Library/New Schema**.
3. In the **New Library/New Schema** dialog, add a *name* for the new library/schema.
4. In the list of options:
   i. For older iSeries versions, be sure to activate the option to *Create as a SQL collection*.
   ii. For newer iSeries versions, be sure to **uncheck** the option to *Create as a standard library*.
5. Click **OK** and the library/schema will be created.

Database Connections For Oracle EBS

Create Hubble Schema/Database User

When creating a database connection for Oracle EBS a script must be run which will create a schema (database user) which will enable the Oracle EBS connection to be setup correctly, i.e. so as to provide access to EBS tables create the required views and functions.

The script (script.sql) accompanies every EBS release as part of the installation. It is a lengthy set of SQL and PL/SQL instructions to be run by a DBA before a data source connection can be set up in Administrator and the Profile Wizard used.

The database script is located in the Installation folder and can be accessed once the build is installed.

To run the script:

1. Open SQL Developer and connect to the database as 'SYSTEM' (password = 'Manager').

2. Copy and paste the entire script into the connection window
3. Select All and then Run Statement (Ctrl + Enter).
4. Several fields must then be completed as follows:
   - **Username** - e.g. Q2015_1_40_076, Q2015_1_0_580
   - **Enter Insight Password** - (which is the same as username)
   - **Enter existing Insight username to copy grants from** - Leave it blank unless testing this feature
   - **Enter** - SYSTEM
   - **Temporary tablespace** - TEMP
   - **Name to run script under** - SYSTEM
   - **Password** - Manager
   - **TNS_ADMIN entry** - <blank>

After a moment, the following prompts will be displayed:

- Create Index on FND_TABLES and FND_COLUMNS Y/N? - Y

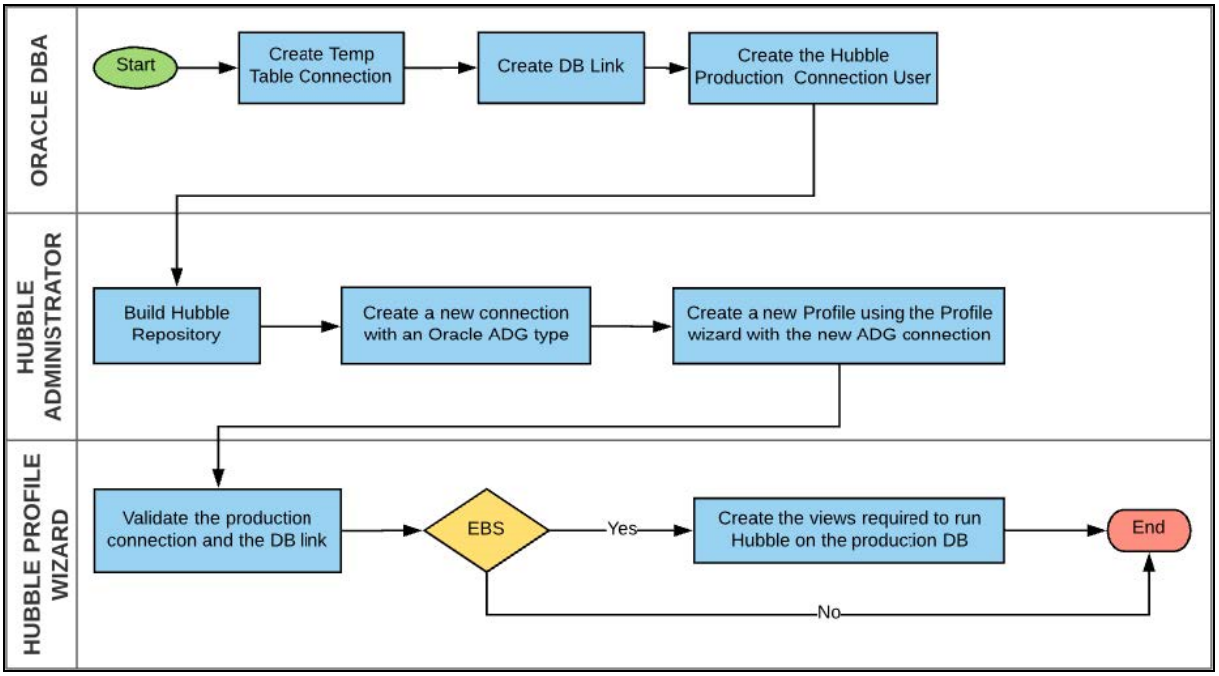
- Create indexes on FA_BOOKS and FA_DISTRIBUTION_HISTORY Y/N? - Y
- Create indexes on PO_HEADERS_ALL and PO_LINES_ALL Y/N? - Y

Once the script is complete. check that the output is error free.

Database Connections For Oracle Active Data Guard (ADG)

Hubble supports the use of an Oracle Active Data Guard (ADG) environment as the reporting DB connection. This allows the DB reporting overhead to be offloaded from the production environment onto an ADG environment copy of the DB.

Configuring Hubble For An ADG Environment



1. **Oracle DBA - Create Temp Table Connection User**. Create the Hubble temp table user on the DB which will be used for the Temp Tables using Script_Remote_Temp_Tables.sql. This will create the remote user used by the DB link which will allow Hubble to create Temp Tables
2. **Oracle DBA - Create DB Link - Create a DB link on the production DB to the Temp Table DB**. This will be replicated onto the ADG environment and will be used to create temp tables when Hubble connects to the ADG environment. Provide the Hubble Administrator with the DB Link name.
   - Create public database link:
     mylink
   - Connect to:
     remote_username
   - Identified by:
     mypassword

- Using:
  'myserver:1521/MYSID'.

3. **Oracle DBA - Create the Hubble Production Connection User**. Run the script.sql on the Production DB to create the reporting connection user that will be replicated to the ADG environment and used by Hubble to run queries. After running script.sql, existing ADG connections will not function correctly until the validations actions from profile creation step of this guide are performed.
4. **Hubble Administrator - Build Hubble Repository**. As described previously under **Installation** The repository can sit on one of our supported DB types e.g. Oracle, SQL Server. It cannot be on the ADG environment but could be on the Production, Temp Table DB or another DB.
5. **Hubble Administrator** - Create a new connection with an Oracle ADG type. This will request details for the Production server details, the ADG server details and the Temp Table Link Name provided by the DBA. Refer to **Creating a New Connection** for further details.
6. **Hubble Administrator**. Create a new Profile using the Profile wizard with the new ADG connection. Refer to **Creating New Profiles** for further details.

Connect To Data Sources

Overview

When you are logged into your repository in Administrator, you will see the **Data Sources** node in the tree structure in the left panel. When you expand this, you see two items:

Connections - stores the information (database type, user name and password) required to connect to your ERP Database(s).

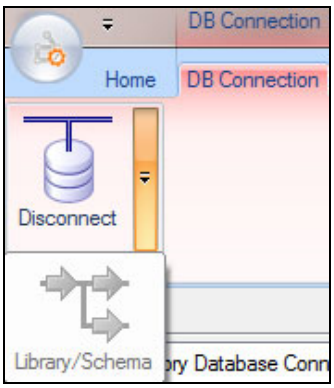
Profiles - designate the Data Source connection(s) to be used in Hubble as well as define the parameters for Hubble to derive correct information from your ERP System.

Create A New Connection

Follow the steps below to create a new database connection:

1. Log into your repository if you are not logged in already.
2. Expand the **Data Sources** node in the left panel.
3. Then either:
   - Right-click on **Connections**, select **New**, then **Repository Database Connection**.
   - Or highlight **Connections**, click the **New** button on the Ribbon and select **Repository Database Connection** to open the **Database Connection** dialog.

4. Configure the connection in the **Database Connection** dialog



   i. **Identification** - set a unique **Name** for this connection (e.g. 'JDE90 Production') and, optionally, set a **Description**.

   ii. **Data SourceType** - specify the **Type** of database in which your ERP Data is located:

i. Microsoft SQL Server®

ii. Oracle

iii. IBM DB2

iv. UDB

v. Qlik (driver used to access IBM Optim archived files)

vi. Local Database file

vii. Oracle ADG

viii. PostgreSQL

   iii. **Data Source Provider** - specify the **Provider** or 'driver' you are using to connect to your ERP data. The options for creating connections are appropriate to the data source type already selected:

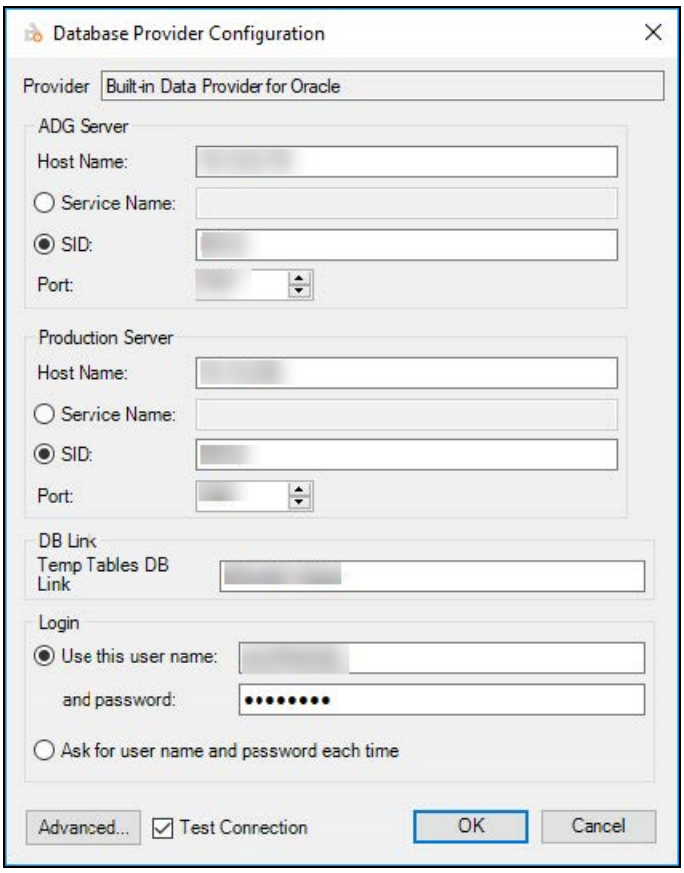
i. SqlClient Data Provider

ii. Built-in Data Provider

iii. OracleClient Data Provider

iv. Data Provider

5. Click **Configure**. The **Database Provider Configuration** dialog is then displayed. For example:



6. The settings in the **Database Provider Configuration** dialog will vary depending on the type of source database the connection is located in (the example above is of the dialog if the Oracle ADG source type was selected).
    i. **If using SQL Server**:
        i. **Server** - select the server on which your database is located or manually type in the location.
        ii. **Login** – specify the details needed to access the server. If you have no password, click the **Blank** checkbox.
        iii. **Database** - select the database on which your ERP data, security, Data Dictionary or UDC tables are stored (whichever this connection is being used for).
        iv. **Test Connection** – mark this option if you want Administrator to verify that all of the connection details are working as expected when you click **OK** in the next step. If there are any errors, a message box will appear and identify them so they can be addressed. When the configuration is working, the **Test Connection** message confirms that it is successful.
    ii. **If using IBM DB2**:
        i. **Server** – specify the Host Name for the database and mark the checkbox if your database version is **pre-V5R3**.

ii. **Login** - specify the login details needed to access the server on which the ERP tables are located. If you prefer to enter the password each time, choose the second option.

iii. **Settings** - specify the Default Library and the names of the Data, Control and Security Libraries.

iv. **Test Connection** – mark this option if you want Administrator to verify that all of the connection details are working as expected when you click **OK** in the next step. If there are any errors, a message box will appear and identify them so they can be addressed. When the configuration is working, the **Test Connection** message confirms that it is successful.

iii. **If using Oracle DB**:

i. **Server** - specify the Host (Server) Name of your server, the Service Name (SID) of the instance you wish to connect to and its Port number.

ii. **Login** - specify the login details needed to access the server. If you prefer to enter the password each time, choose the second option.

iii. **Test Connection** – mark this option if you want Administrator to verify that all of the connection details are working as expected when you click **OK** in the next step. If there are any errors, a message box will appear and identify them so they can be addressed. When the configuration is working, the **Test Connection** message confirms that it is successful.

iv. **If using Database Accelerator**:

i. **Server** - specify the Host (Server) Name of your server and its Port number.

ii. **Login** - specify the login details needed to access the server. If you prefer to enter the password each time, choose the second option.

iii. **Database** - specify the required database name.

iv. **Test Connection** – mark this option if you want Administrator to verify that all of the connection details are working as expected when you click **OK** in the next step. If there are any errors, a message box will appear and identify them so they can be addressed. When the configuration is working, the **Test Connection** message confirms that it is successful.

v. **If using Oracle ADG**:

i. **ADG Server** - specify the Host (Server) Name of your ADG server, the Service Name (SID) of the instance you wish to connect to and its Port number.

ii. **Production Server** - specify the Host (Server) Name of your production server, the Service Name (SID) of the instance you wish to connect to and its Port number.

iii. **DB Link** - enter the name of the DB Link to be used by Hubble to create Temp Tables. See **Database Connections for Oracle Active Data Guard (ADG)** for details.

iv. **Login** - specify the login details needed to access the server. If you prefer to enter the password each time, choose the second option.

v. **Test Connection** – mark this option if you want Administrator to verify that all of the connection details are working as expected when you click **OK** in the next step. If there are any errors, a message box will appear and identify them so they can be addressed. When the configuration is working, the **Test Connection** message confirms that it is successful.

vi. **If using PostgreSQL**:

i. **Server** - specify the Host (Server) Name of your server and its Port number it will use.

ii. **Login** - specify the login details needed to access the server. If you prefer to enter the password each time, choose the second option.

iii. **Database** - specify the required database name.

iv. **Advanced** - click this button and set the following:

i. `SSL Mode` to **Required**.

ii. `Trust Server Certificate` to **True**.

7. Click **OK**.

8. If you require more than one connection to your ERP tables, you will repeat this process for each connection.

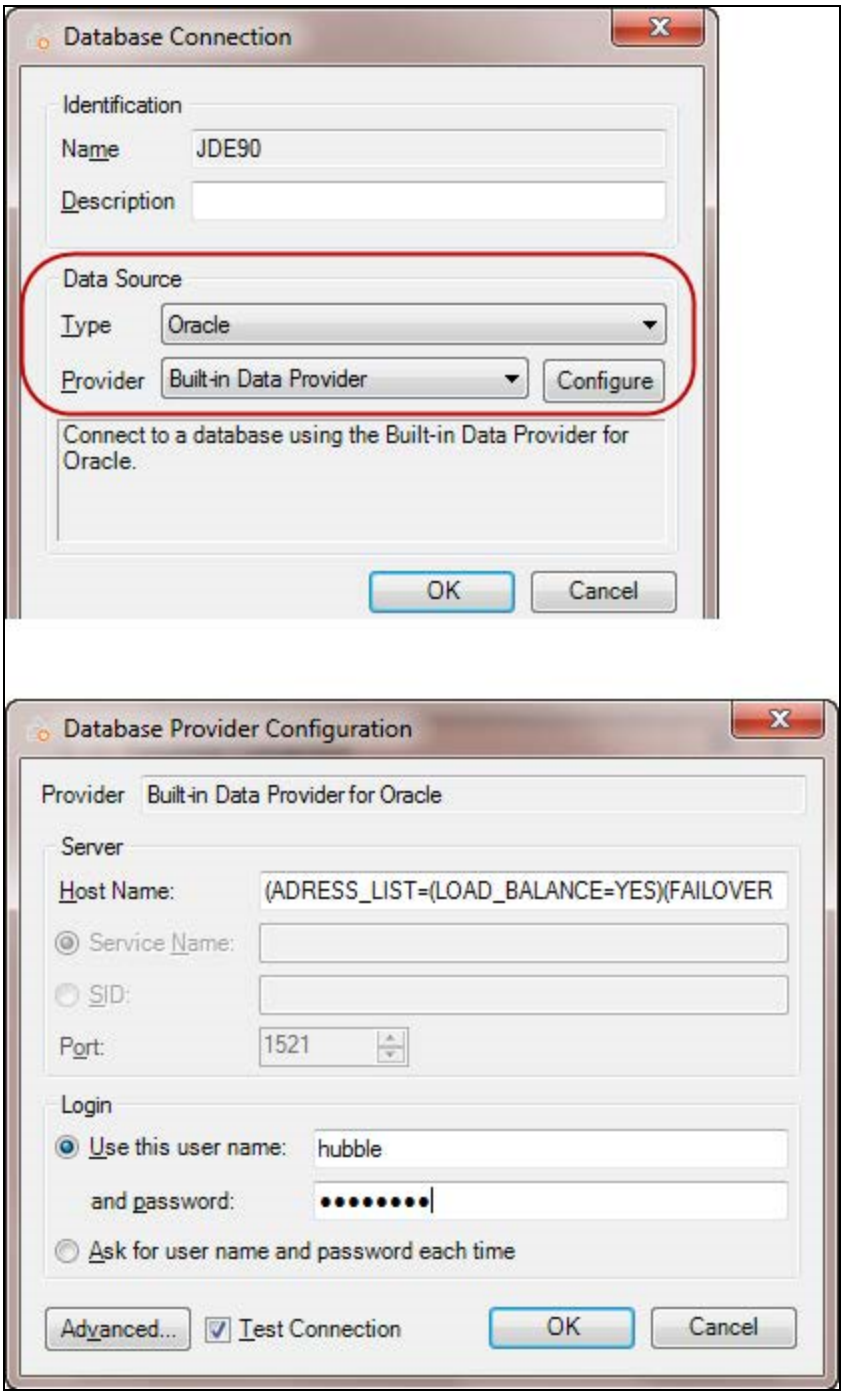
Built-In Data Provider

The advantage of using a built-in data provider is simplicity; it is very simple to set up in Administrator. The SQL Server and Oracle Server Data Providers can be used if using those servers. The ODBC Data Provider requires more maintenance; with this option, you must set up an ODBC data source *on each Hubble installation* instance (server and individual PCs). The ODBCs must be set up *exactly the same* (name, description, and all settings) on each installation.

Load Balancing And Failover Configuration

Load Balancing and Failover Configuration can be done within the Oracle database connection configuration in Administrator. This is to support Oracle Real Application Clusters (RAC), which provides software for clustering and high availability in Oracle database environments.

To configure multiple servers for load balancing or failover, you can specify the TNS description instead of a Host Name in the Oracle Built-in Data Provider setup, such as the example shown below:



For example, if your TNS description is as follows:

```
(DESCRIPTION= (ADDRESS_LIST=
(LOAD_BALANCE=YES) (FAILOVER=YES)
(ADDRESS=(PROTOCOL=tcp)(HOST=servername1)(PORT=1521)) (ADDRESS=
(PROTOCOL=tcp)(HOST=servername2)(PORT=1521))
```

```
)
(CONNECT_DATA= (SERVICE_NAME=acme)
)
)
```

Remove the line breaks, and then cut and paste the description into the **Host Name** field. Following the same example, it would look as shown below:

```
(DESCRIPTION=(ADDRESS_LIST=(LOAD_BALANCE=YES)(FAILOVER=YES)(ADDRESS=(PROT
OCOL=tcp)(HOST=servername1)(PORT=1521))(ADDRESS=(PROTOCOL=tcp)(HOST=serve
rname2)(PORT=1521)))(CONNECT_DATA= (SERVICE_NAME=acme)))
```

Create New Profiles

Once Data Source Connections have been created in Administrator, you can create a Profile that uses these Connections. A Profile can be made up of multiple Connections. This is why the ERP Wizard allows you to create a new Connection or make use of an already existing one. Additionally, for ease of use, a Connection can also be reused by multiple Profiles.

Create A JD Edwards Profile

1. Log into your repository if you are not logged in already.
2. Expand the **Data Sources** node in the left panel.
3. Use one of these options:
   i. Right-click on **Profiles**, select **New**, then **JDE Profile**.
   ii. Highlight **Profiles**, click the **New** button on the Ribbon and select **JDE Profile**.
   iii. Select **Connections**, right-click on a Connection in the right panel and select **Create Profile**.
4. If option a. or b. (above) was selected, the **New ERP Profile** dialog opens. Enter a unique name that identifies this Profile. Click **OK**.
   If option c. was selected, the new profile will automatically be given the same name as the Connection. If a profile with that name already exists, a sequence number will be added to the end of the new profile name to distinguish it.
5. In the Create/Edit ERP Profile Wizard, click **Next**.
6. For clients using JD Edwards, you will next designate the Connections that link Hubble with the JD Edwards database tables. Choose the relevant connection from the previously defined list of available Connections. If a Connection has not been defined, click the **New** button and you will be presented with the Database Connection dialog and from here, a new Connection can be created.

If the JD Edwards Security, Data Dictionary or UDC tables reside in the same database on the same machine as the Data tables, it is possible to use the same Connection for all of these tables. In such instances, the **Same as Data Connection** checkbox should be enabled for the relevant connection and no further connection details need to be provided.

a. **Data Connection** – the Connection that links to the main JD Edwards Data tables, such as F0902 and F0911.

b. **Security Connection** – the Connection that links to the JD Edwards Security tables, such as F0092 and F0093.

c. **Data Dictionary Connection** – the Connection that links to the JD Edwards Data Dictionary table F9201(World) or F9210 (E1).

d. **UDC Connection** – the Connection that links to the JD Edwards UDC Data table, such as F0005.

7. Click **Next**.
8. Select the JD Edwards edition and version to which you will be connecting.
9. Click **Next**.
10. For DB2 for i, there are specific database settings due to restrictions on what can be done with regards to SQL commands and query sizes:
    i. **DB2 / AS/400 Options** - select any of the applicable options. If you use a V5 release of OS400 you do not need to select any of these.
    ii. When enabling the SQL setting **Column Limit**, you will specify a maximum limit on the number of columns allowed in a SQL Query. You can allow the configuration tool to attempt discovery of this value by using the **Detect** option when enabled. Depending on your database and version, the number of columns will differ. It is recommend that you use the Detect functionality and enable the **Column Limit**.
11. Click **Next**.
12. In the **Module Selection** screen, activate the modules and options you wish to use in this Profile. (Note that when applicable, only the modules or Features your organization is licensed for are available to select.)
    i. **Modules**
    ii. **Features**:

i. **Budgeting** - if you have a license for this feature, you can activate it for this Profile.

ii. **Designer Express** - if you have a license for this feature, you can activate it for this Profile.

iii. **DX Data Entry** - this functionality enables you to design a budget or forecasting input form using any table in JD Edwards. If you have a license for this feature, you can activate it for this Profile.

iv. **Currency Restatement** – if you have a license for this feature, you can activate it for this Profile.

v. **Localized Captions** - gives the ability to derive different language captions from the underlying JD Edwards system.

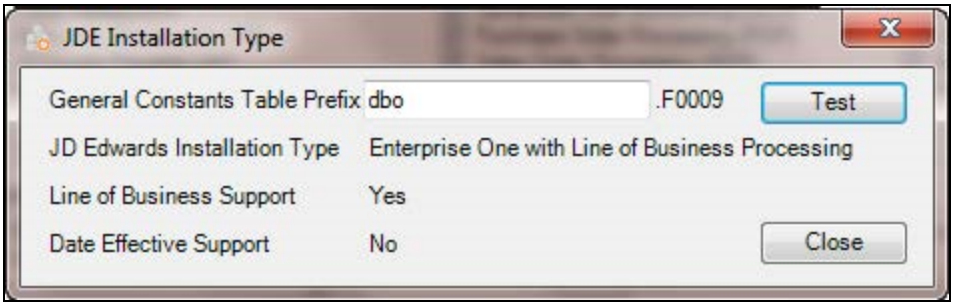
vi. **Attachments** - this features enables you to add attachment columns to reports and link to attachments from the ERP database.

iii. **GL & JC Settings** - Weekly reporting - available if you use this option in JD Edwards, this option is directly related to the Date Fiscal Patterns – 52 Period Accounting Table (F0008B).

iv. **AR & SOP & CRM Settings** - Line of Business Support and Use Date Effective Categories - settings available if you use these Accounts Receivable/Sales Order Processing/Customer Relationship Management options in JD Edwards.

v. **Line of Business Support** – when enabled, Hubble will use the Customer Master by Line of Business Table (F03012). When disabled, Hubble will use the Customer Master Table (F0301).

vi. **Effective Categories** – when enabled, Hubble will be able to derive data from the Customer Date Effective Category Codes Table (F03012A).



Note: If you are unsure whether to enable either of these options, click **Verify**. If you have only one F0009 table, click **Test**. The results will tell you if either is activated in that table. If the F0009 is located in more than one library in your database, identify the table owner/library such as below.

13. Click **Next**. (There will be a pause while the data source is analyzed for relevant control and data tables. The amount of time this process takes will vary depending on the size of the JD Edwards implementation.)

14. If you are using Budgeting and/or the Percent Split functionality, complete the information in the **Budgeting Connection** screen. This is where you define the connection and the database or library where uploaded data will be stored.
    i. **Data Entry** section:

i. **Connection** – identify the connection being used to connect to the Budgeting Repository.

ii. **Database/Library** – identify the database/library being used for the Budgeting Repository. If it has already been initialized, it will be listed in the drop-down box; otherwise, the location must be typed in.

- For SQL Server, enter the name of the database in SQL Server, followed by a period, followed by the database owner username (typically 'dbo').
- For DB2 and Oracle, you only need name of the database/library.

iii. **Repository Prefix** - a repository may contain multiple budgeting repositories. This is controlled on a profile basis. A repository prefix must be added to table names to distinguish them by entering it here or selecting it from the drop-down.

ii. **Budgeting Upload Table section** - You can upload the F0902Z1 using a different connection than the Data Connection (the F0902Z1 can be located on a different server than the

Budgeting Repository and JD Edwards.) Therefore within this section you define which connection is being used to connect to the F0902Z1.

> If using JD Edwards World, you need a 3rd party program to upload the data.

i. **Connection** - identify the connection being used to connect to the F0902Z1 table.

ii. **Upload** - define the name of the database and owner or library name where the F0902Z1 Table is located. (This will be listed automatically if it is visible via the JD Edwards Data Connection; otherwise, enter the database name, followed by a period, followed by the database owner or library name.) If it has already been initialized, it will be listed in the drop-down box; otherwise, the location must be typed in.

- For SQL Server, enter the name of the database in SQL Server, followed by a period, followed by the database owner username (typically 'dbo').
- For DB2 and Oracle, you only need name of the database/library.

iii. **New Connection** - if you wish to have a separate Connection to the location of the F0902Z1 table but have not yet created it, create it by clicking on the **New Connection** button.

15. In the **Select Additional Tables to Configure** screen, select the specific tables needed for Designer Express (if enabled). This screen will not be displayed if the Designer Express feature is not enabled.

i. **Connection** - set how to connect to the Object Librarian Master Table (F9860 in E1 and F9801 World), whether it is the same Hubble Connection as that being used to connect to your JD Edwards Data, or whether it is a different Connection.

ii. **Object Library** - define the library where the F9860/F9801 table resides (allows you to map to tables not configured in the profile).

iii. **Choose Tables** – define the tables which will be used in new templates if they are not already mapped.

i. All available tables are listed in the left panel. To select tables, move them to the right panel either by using the arrows or double-clicking on the specific table in the left panel. Optionally, use the QBE to find any table in order to move it to the right panel. All tables in the right panel will be available.

ii. Tables can be flagged as "non-ERP" so that they are not checked against the data dictionary. To do this, select the tables, click **Table Origin**, and tick the checkboxes of those tables to be flagged as non-ERP.

iii. Click **OK** once all selections have been made.

> **Tip:** It is strongly recommended that you only add the tables you need and that you not add all the tables.

iv. **Import Tables** - import custom data entry tables from an xml file. Imported tables are automatically configured (there is no need to choose them using the **Choose Tables** facility).

i. Click **Clear** to clear the imported tables.

ii. Click **Export** to export them to another file.

16. Click **Next**.

17. In the **Table Locations** screen, define all of the tables needed for Hubble with the appropriate Owner, Library or Schema name.

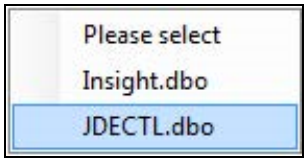
- *If there is uncertainty over any of the table selections explained below, please consult your JD Edwards Administrator*.

The tables available are split between mandatory and optional, both of which can be defined on this screen. The default setting for the table definition is to only show those tables that have multiple selectable prefixes. Click **Show All Tables** to see all database tables. If all tables have the same prefix, this screen will be blank until you check **Show All Tables**.

a. **Table Owners/Library Names** - In the IBM DB2/400 database, this grouping is called a **library**. For Oracle and SQL Server databases, the equivalent of a library is the **Table Owner** (SQL Server) or **schema** (Oracle). A table owner/schema is associated with the database user who owns, and most likely created, the database table. In this Profile Wizard we use the term **Owners/library names** to cover all possibilities.

b. If the correct default libraries have been supplied in the ODBC connection for DB2/400, Oracle or SQL Server, the library prefixes should automatically be completed. Please ensure that all of the tables in the list either have a valid prefix or are set to '**Do not use**' where appropriate. If this is not the case, valid prefixes can be manually entered by' double-clicking on the appropriate prefix field and entering the name manually.

c. To select multiple rows, use either the Shift or Ctrl keys to select the fields with a common owner/table. Highlight the rows and right-click. This will provide you with a selection of **Library Prefix** names that are common to all highlighted tables:



After selecting the common owner/table for the selected fields, you see that the table prefix has changed to the value you selected.

- When all of these prefixes have been applied, click **Next** to continue.
- Click **Next**.
- Define the location of the **Data Dictionary** table and choose whether you want to use any Data Dictionary **overrides**.
- *The Data Dictionary library is an information library that contains data definitions to access when using Hubble. If using EnterpriseOne or World version A81 or higher, the table is F9210. When using World versions lower than A81, the table is F9201. Therefore the syntax will either be <LIBRARY>.F9210 or <LIBRARY>.F9201. In some environments, the database name is needed. In such cases, the syntax will be <DATABASE>.<LIBRARY>.<TABLE>.*
- Click **Next**.
- In the **Test the Configuration** screen, the application tests what has been entered so far in the Profile Wizard. If you wish to see the number of rows returned in each test, mark the checkbox to **Include Row Count Information**.

- Click **Run Test**.
- *If a warning message is received at this point, click the Back button to return to the screen that is relevant to the issue highlighted in the message. Examine and alter those settings that are at fault before returning to test the configuration.*
- Click **Next**.
- In the **Environment and Model Business Unit** screen:
  1. **Environment** – when users sign in to Hubble, the application validates that they have access to the JD Edwards **Environment** defined here. This can be selected from the drop-down list of options or it can be entered manually.
  2. Enter in a JD Edwards **Model Business Unit** to validate object accounts selected by the user.

     > *In JD Edwards, Model Business Units (BU) are identified as such within the Business Unit Master table – F0006. Typically a Model BU will be kept up to date and will contain a complete account structure. A Model BU typically does not have any transactional data.*

     If there is no single model Chart of Accounts but there are separate model balance sheets and model profit and loss accounts, multiple Business Units can be entered. Initially the dialog allows for one General Model Business Unit option, which is then applied to all modules.
  3. Enable the **Override for specific Modules** option if you wish to use a different Model Business Unit for the General Ledger, Job Cost and/or Fixed Asset modules.
  4. Either manually enter the Model Business Unit(s) (comma separated for multiple Models) in the field provided or press the **Search** button to the right of the field to search for and select a Model Business Unit.

     > *If you do not have a complete Model BU available, you may opt to enter an alternative BU (one that is not defined as a Model BU in JD Edwards). If you choose to enter a 'live' Business Unit in this dialog, all users will be able to see the transactional data for that Business Unit.*
- Click **Next**.
- There are several tabs in the **Options** screen:
  1. **Subledger Locations** – using the drop-down list, choose to include or exclude each Subledger type from the Subledger filter. (Optionally, you can use the **Select All** button to select all at once.)
     i. Optionally, mark the option to Use temporary table in Subledger joins.
        - Some clients have experienced reduced performance when joining to JD Edwards Subledger tables in Hubble. This is because the key fields are stored in a different format in the main and Subledger tables. This option can assist with these performance concerns.

     ii. For the A, C and W Subledger types, you can further narrow them down by clicking on the button next to the Sub Type column. When presented with the list to choose from, you can use the Shift and Ctrl keys to multi-select.

     iii. If the Address Book Subledger type has been selected, only include the sub types that are needed as this can dramatically speed up the processing of the Subledger Visual Assist.

     iv. Within the Subledger type `A` – Address Book, it is also possible to select which Address Book record description should be used within Hubble by clicking the Advanced button next

to the Description column. The choices include: Mail Name (WWMLNM from F0111), Alpha Name (WWALPH from F0111) and Alpha Name (ABALPH from F0101).

v. In Hubble, for Subledger Type `S` only, we will suppress all the * selections when retrieving the Structured Subledger type `S` items. The * selection is wildcard searching functionality that can be achieved in the Query by Example (QBE) filters of the Query Assist dialog.

2. **Balance Sheet Overrides** - define which Automatic Accounting Instructions values from the AAI table, F0012, define the start and end items for your balance sheet and profit and loss range of accounts. By default this is GLG2 and GLG5.

   You can change the start and end of the AAI value range that Hubble uses by selecting No Override and using the corresponding drop-down menus. Alternatively, you can select an override. Note that override settings do NOT get written back to your JD Edwards database and therefore they will not modify the values in the Automatic Accounting Instructions table.

   - Select the **Define an override system** option.
   - Click **Override**.
   - In the **Specify Account Ranges** dialog, click **New** to specify the start and end account of your balance sheet account range. (You can also edit and remove account ranges in this dialog.)
   - Click **OK**.

3. **Options: Description Settings** - specify which combination of Object Account and Subsidiary will be used to derive the description value that Hubble will display:
   i. **Model BU/First Subsidiary or Object Account** - this default option uses the configured Model Business Unit for the inquiry result.
   ii. **Exact BU/First Subsidiary or Object Account** - stores in a temporary table the descriptions based upon selections from your Account Master.
   iii. **Exact BU/Blank Subsidiary or Object Account** - joins directly to the F0901 to retrieve the descriptions.
   iv. **Exact BU/Exact Object/Exact Subsidiary**- joins directly to the F0901 to retrieve the descriptions.

4. **Data Settings**:
   i. **Data contains NULL values** - you may disable this option to increase performance if you know that your data definitely does not contain null data.
      - If you are unsure about this setting, please do not change the default setting unless advised by our Support Team.

   ii. **Load Data Dictionary at start-up** - this setting tells the application how to handle data types and padding. When checked, Hubble runs one large query at the time of login in order to cache the Data Dictionary information. When unchecked, whenever Hubble needs to know how to work with an individual item, it runs an individual query to get that information from the Data Dictionary and then caches the result.

   In other words, this option enables you to choose which option is better for your profile: one large query or queries on demand. For sites that host the database remotely, the option being turned on will help with performance as time is lost when queries are continuously

being run as the information is needed.

- If you are unsure about this setting, please do not change the default setting unless advised by our Support Team.

iii. **Financial Year setting** - Financial years in JD Edwards are stored in 2 fields, CTRY (century) and FY (financial year). If you have data for the same year in different centuries, such as 2007 and 2107, you should be using the **Use CTRY and FY** to determine year. Otherwise if you know that your Company's Date Fiscal Patterns (F0008) only span across one century, you will be able to enable the option **Use FY only** to determine year (best performance).

iv. **World Security Options** – available to sites using JD Edwards World, in this dialog you set the following:

v. **Security Settings**:

i. **JD Edwards Business Unit Security** turns on/off Business Unit Security.

ii. **Allow blanks** gives you the option of allowing blanks in the Business Unit Security Settings.

iii. **Implement security using temporary tables (recommended)** - creates temporary tables to handle the JD Edwards security settings. This was added as it can improve inquiry performance times.

iv. **Use Tax ID / Social Security Number Masking** - used in combination with the Advanced Capabilities for Social Security Number Options (Advanced Capabilities: Options > JDE), Hubble can mask the display of Tax IDs / Social Security Numbers (SSNs).

vi. **Connection Settings** allow you to select which security authentication mode you want your users to use as part of the logon process:

i. **Option 1** - uses the username and password of the person logging onto Hubble to verify against the AS/400.

ii. **Option 2** - connects using the username and password defined in the Connection in Administrator but still validates the person logging in (using their user-name and password) against the AS/400.

iii. **Option 3** - connect using option 1; upon failure, connect using option 2.

iv. **Option 4** - same as option 2 except the person logging in is validated in the object repository, not the AS/400.

> **Note:** If Hubble Web functionality is to be used in the project, option **4. system credentials, verify user with Hubble password management setting** must be selected.

5. **Security Options** – available to sites using JD Edwards E1, in this dialog you set the following:
   i. **Use JD Edwards Security** - enables JD Edwards security. The following further settings are available:

i. **GL and JC Balance Templates** - tick these checkboxes as required to apply JDE *ALL Table Security for xxMCU and xxCO columns only to table F0902 for GL and JC balances.

ii. **All Transaction Templates** - tick these checkboxes as required to apply JDE *ALL Table Security for xxMCU and xxCO columns only to table F0911 for transactions.

iii. **DX Reports - Enable Streamline Security** - tick to choose to apply the streamlined security to DX reports.

The *ALL table security is useful in JDE is because applications and reports typically only use one or two tables, and usually both tables do not have the MCU or CO columns.

In the case of templates such as Balances, the above security is applied to the F0902, F0901 (and Company table/F0010 if included). This repetitive security is not necessary and results in a performance impact.

ii. **Implement JD Edwards Security using temporary tables** (recommended) – when selected, Hubble will create temporary tables to handle the JD Edwards security settings. This was added as it can improve inquiry performance times.

iii. **Use Tax ID / Social Security Number masking** - used in combination with the Capabilities for Social Security Number options, Hubble can mask the display of Tax IDs / Social Security Numbers.

iv. **Use Inclusive Row Security to Prevent Table Access (Add/View/Change/Delete all equal N)** - used to enable Inclusive row security, where a role cannot view a table unless explicitly granted access to it.

6. **DB2 Options**– available if your JD Edwards system is using a DB2 database:
   i. **Indices** - this option can improve the performance for Object Account/Subsidiary validation by relying on your indices on the F0901 table. Click the **Test** button to verify that Hubble can use your indices and then check the box as appropriate.
   ii. **Globalization** - this option must be checked if you want double byte for localizations so that the double byte text can be converted to Unicode. Select in the drop-down list the Coded Character Set Identifier which was used when the Asian text was entered into the database. (The conversion will be applied to JD Edwards descriptive columns only, e.g DL01, EX).

7. **Joins** - Within the General Ledger and Job Cost modules, we are using tables F0901 and F0902. This tab allows us to define how we want to join the two files:
   i. **Full Join** - joins on all aspects of an account, i.e. Account I.D, Company, Business Unit, Object Account and Subsidiary. By joining on all of these fields, you are sacrificing speed for integrity due to the additional checks Hubble will need to perform.
   ii. **Account ID Only Join** - only joins on Account ID (which is the same way that JD Edwards joins these tables). This type of join sacrifices integrity for speed. You can check the integrity of your system by running the Account ID Integrity Test under Extended Tests in the Integrity Checker; this will allow you to see if it is safe to use this faster option.

- Click **Next**. Pressing **Cancel** on this screen will result in your profile not being saved.
- Click **Finish**. You will see the **Updating ERP Profile** screen, which runs through a number of process, for example Setup Standard Templates and Setup Budgeting Repository. These processes will load all of the information, templates etc. that will be used by the configured ERP Profile. Once completed, the status bar columns will show as **OK**.
- Click **Close** to exit the screen if it doesn't exit automatically.

- If the process has not updated correctly, the status column will show as Error. This will mean that your profile will not be completed. You will need to fix the error before re-running the process. Double-click on the line to receive further information.
- On completion, your ERP Profile will appear as an item within Profiles.

Create An Oracle Profile

Follow the steps below to create a new Oracle profile:

1. Log into your repository if you are not logged in already.
2. Expand the **Data Sources** node in the left panel.
3. Use one of these options:
   i. Right-click on **Profiles**, select **New**, then **Oracle Profile**.
   ii. Highlight **Profiles**, click the **New** button on the Ribbon and select **Oracle Profile**.
   iii. Select **Connections**, right-click on a Connection in the right panel and select **Create Profile**.
4. If option a. or b. (above) was selected, the **New ERP Profile** dialog opens. Enter a unique name that identifies this Profile. Click **OK**.

   If option c. was selected, the new profile will automatically be given the same name as the Connection. If a profile with that name already exists, a sequence number will be added to the end of the new profile name to distinguish it.
5. In the **Create/Edit ERP Profile** Wizard, click **Next**.
6. Designate the Connection that links Hubble with your Oracle database tables. Choose the relevant connection from the previously defined list of available Connections.

   If a Connection has not been defined, click the **New** button and you will be presented with the **Database Connection** dialog and from here, a new Connection can be created.

   > **Note:** For Oracle ERP data, only one connection is needed to connect to all data. Therefore, only the Data Connection needs to be identified. Set the **Same as Data Connection** checkbox for the Security, Data Dictionary and UDC Connections.
7. If the HR and/or Payroll modules are to be used, an HR Security connection to the APPS schema is required (refer to the *Installation & Maintenance Guide for Oracle EBS DBAs* for details). Select the connection from the **HR Security Connection** list and mark the **Use Data Connection** checkbox.
8. If the selected Data Connection is an Accelerator connection (an Actian Vector database), select a Replication Schema from the **Replication Schema** list.
9. Click **Next**.
10. Select the Oracle EBS version to which you will be connecting.
11. Click **Next**.

12. In the **Module Selection** screen, activate the modules and options you wish to use in this Profile.
    - Only those modules for which your organization is licensed are available to select.
        - Modules
        - Features:
            i. **FSG Row Set Importer** - enables the option to import FSG Row Sets
            ii. **Parent Code Filter Support** -enables users to filter on parent codes. (For example, Account 1000 (Cash) is the parent code and has no postings directly against it. If this option is enabled, users can filter on Account 1000 and see the sum of all its descendants.)

13. Click **Next**.

14. If you are using Budgeting functionality, complete the information in the **Oracle Connectivity (Data Entry Connection)** screen. This is where you define the connection and the database or library where uploaded data will be stored.
    i. **Data Entry Settings** section:

    i. **Connection** – identify the connection being used to connect to the Budgeting Repository.

    ii. **Database/Library** – identify the database/library being used for the Budgeting Repository. If it has already been initialized, it will be listed in the drop-down box; otherwise, the location must be typed in.
        - For SQL Server, enter the name of the database in SQL Server, followed by a period, followed by the database owner username (typically 'dbo').
        - For DB2 and Oracle, you only need name of the database/library.

    iii. **Repository Prefix** - a repository may contain multiple budgeting repositories. This is controlled on a profile basis. A repository prefix must be added to table names to distinguish them by entering it here or selecting it from the drop-down.

    ii. **New Connection** - if you wish to have a separate Connection to the location of the table but have not yet created it, create it by clicking on the **New Connection** button.

15. Click **Next**.

16. In the **Select Additional Tables to Configure** screen, select the specific tables needed for Designer Express (if enabled). This screen will not be displayed if the Designer Express feature is not enabled.
    i. **Choose Tables** – select the tables which will be used in new templates if they are not already mapped.

    i. All available tables are listed in the left panel. To select tables, move them to the right panel either by using the arrows or double-clicking on the specific table in the left panel. Optionally, use the QBE to find any table in order to move it to the right panel. All tables in the right panel will be available.

ii. Click **OK** once all selections have been made. The tables are then configured.

> **Tip:** It is strongly recommended that you only add the tables you need and that you not add all the tables.

17. **Import Tables** - import custom data entry tables from an xml file. Imported tables are automatically configured (there is no need to choose them using the **Choose Tables** facility).
    i. Click **Clear** to clear the imported tables.
    ii. Click **Export** to export them to another file.

17. Click **Next**.

18. In the **Table Locations** screen, define all of the tables needed for Hubble with the appropriate Schema name. If there is uncertainty over any of the table selections explained below, please consult your Oracle EBS Administrator.

The tables available are split between mandatory and optional, both of which can be defined on this screen. The default setting for the table definition is to only show those tables that have multiple selectable prefixes. Click **Show All Tables** to see all database tables. If all tables have the same prefix, this screen will be blank until you check **Show All Tables**.

- **Table Owners/Library Names** - For an Oracle database, this is the schema. A table owner/ schema is associated with the database user who owns, and most likely created, the database table.
- If the correct default libraries have been supplied in the Data Source Connections, the prefixes should automatically be completed. Please ensure that all of the tables in the list either have a valid prefix or are set to '**Do not use**' where appropriate. If this is not the case, valid prefixes can be manually entered by double-clicking on the appropriate prefix field and entering the name manually.
- If a Replication Schema has been specified for the connection, the replicated tables will be displayed with the Replication Schema name as their prefixes.
- To select multiple rows, use either the Shift or Ctrl keys to select the fields with a common owner/table. Highlight the rows and right-click. This will provide you with a selection of **Library Prefix** names that are common to all highlighted table. After selecting the common owner/table for the selected fields, you see that the table prefix has changed to the value you selected.

19. When all of these prefixes have been applied, click **Next** to continue.

20. The mandatory views, synonyms, types and packages required by Hubble are then created. The progress and results of this process is displayed in the wizard.

21. Click **Next** once the process is completed successfully.

22. In this screen, Hubble tests what has been entered so far in the Profile Wizard. If you want to see the number of rows returned for each table, click **Include Row Count Information** prior to running the test.

23. Click **Run Test**. If a warning message is received at this point, click the **Back** button to return to the screen that is relevant to the issue highlighted in the message. Examine and alter those settings that are at fault before returning to test the configuration.

24. If desired, click **Export** to export all test results before continuing.

25. Click **Next**.

26. In the **Profile Options** screen, there are several options:
    i. **Allow expired users to log in** - This enables organizations to allow their expired Oracle EBS users to log on. (While this can be beneficial in terms of efficient use of Oracle licenses, it can raise security concerns and will require manual monitoring by the organization to ensure it is not abused.)
    ii. **Enable EBS Segment and Org Security** - This enables organizations to switch off the reference to the EBS. Org and Segment security for completely open reporting. (This is beneficial for consolidation reporting but can cause security concerns for some organizations and should be treated with caution; once it is switched off, it applies to all users accessing the affected Hubble profile.)
    iii. **Segment filter values from all COAs are made available** – Typically users should see one ledger per responsibility. When this is activated, it allows you to see all ledgers when logging into Hubble.

    > **Important:** This setting is off by default and should remain off except in exceptional circumstances as it causes individual queries to run for each segment for every ledger. This can result in hundreds, if not thousands, of inquiries being run at login.

    iv. **Using Projects time-phased budgeting** – Activate this option if budgeting is done periodically, as in every period/month (time-phased). Leave this option unchecked if the entire budget amount for a project is allocated against a single period.

i. *> For example, if Project ABC runs from April 2012 to April 2015, you can either budget for every month throughout that period (time-phased) or allocate the entire budget to one period, most likely the final one in the life of the project which is April 2015.*

    v. **Apply Parent Code Filtering Support (PCFS) Subset Optimization** - This can be used if there are complex structures, i.e. many parent/child levels within multiple segments.

    This allows you to enter a parent code in the filter and the data returned includes all the child levels associated with the parent code. Similar to a hierarchy, which is a parent/child relationship, you can input the parent code in a filter and once the inquiry runs, all child levels are returned in the inquiry results. However with this option checked, there is no need to create the hierarchy.

    vi. **Load Data Dictionary at start-up** - This setting tells the application how to handle data types and padding. When checked, Hubble runs one large query at the time of login in order to cache the Data Dictionary information. When unchecked, at the time Hubble needs to know how to work with an individual item, the application runs an individual query to get that information from the Data Dictionary and then caches the result.

    In other words, this option enables you to choose which option is better for your profile: one large query or queries on demand. For sites that host the database remotely, the option being turned on will help with performance as time is lost when queries are continuously being run as the information is needed.

    > If you are unsure about this setting, please do not change the default setting unless advised by our Support Team.

27. Click **Next**. Pressing **Cancel** on this screen will result in your profile not being saved.

28. Click **Finish**. You will see the **Updating ERP Profile** screen, which runs the Standard Templates Setup. This process will load all of the information and templates that will be used by the configured ERP Profile. Once completed, the status bar columns will show as **OK**.
29. Click **Close** to exit the screen if it doesn't exit automatically.
30. If the process has not updated correctly, the status column will show as Error. This will mean that your profile will not be completed. You will need to fix the error before re-running the process. Double-click on the line to receive further information.
31. On completion, your ERP Profile will appear as an item within Profiles.

Configure Additional Tables

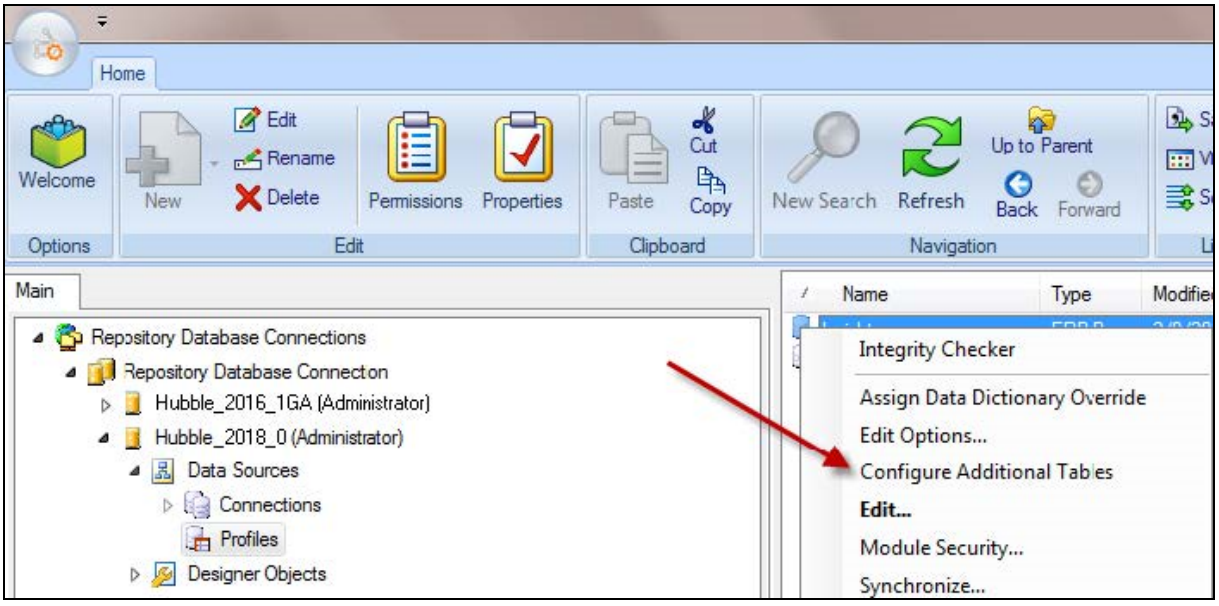
Note: For Oracle EBS Accelerator Users:

If your environment uses Oracle EBS with online patching (R12.2+), you must include the lookup table created by the online patching replication script as a custom table in the profile. This ensures that only the run edition data is used, avoiding duplicates.

Refer to the *Oracle EBS Online Patching Overview* document and Replication Script Guide for detailed steps.

The Configure Additional Tables option for a Profile can be quickly accessed in a Profile by right-clicking on the specific Profile and selecting **Configure Additional Tables**.

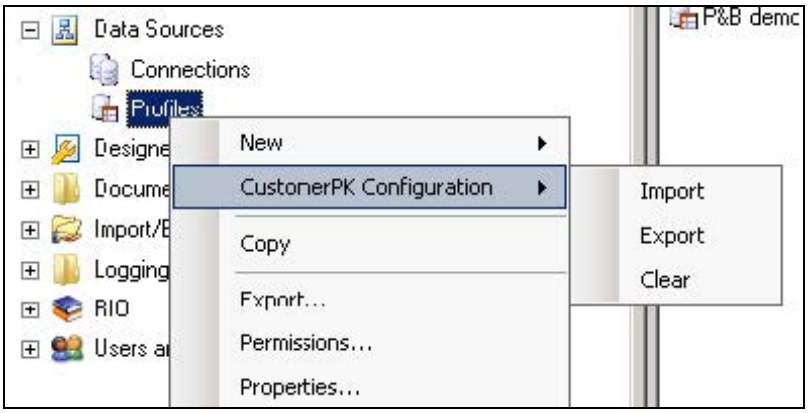
This will display the **Select Additional Tables to Configure** and **Table Locations** screens in the Profile, bypassing the other screens that you would see by going through the full profile wizard.



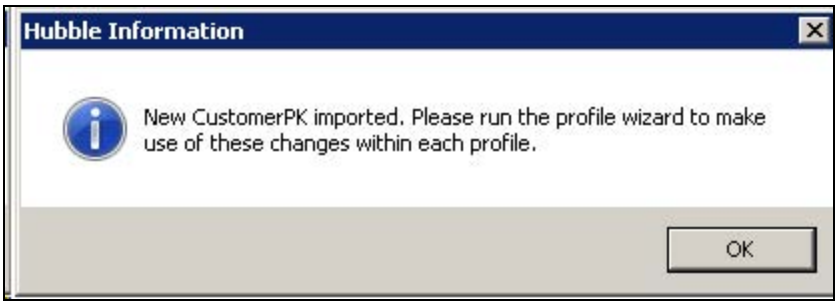
Import And Export The CustomerPK Configuration

The Hubble profile configuration file, CustomerPK.xml, can be imported, exported and cleared.

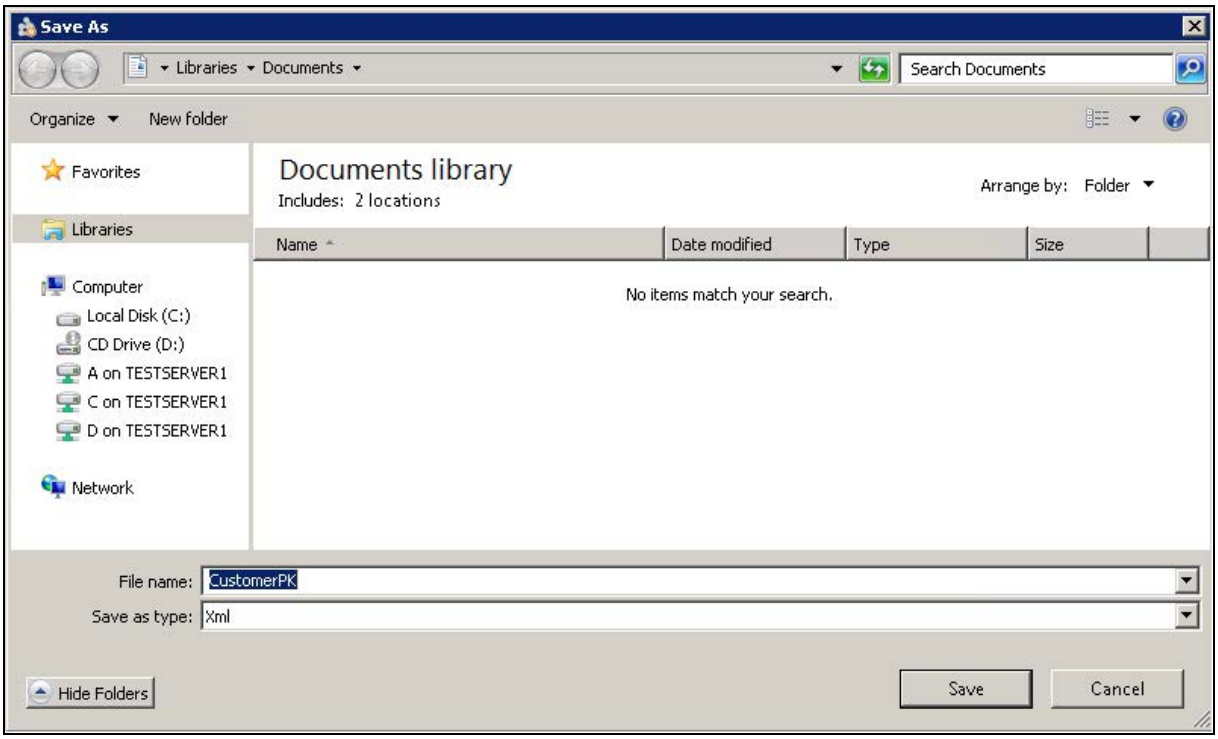
Right-click on **Profiles** and select **CustomerPK Configuration**:



To import a new CustomerPK file, select the **Import** option. The following message is then displayed regarding the profile wizard:

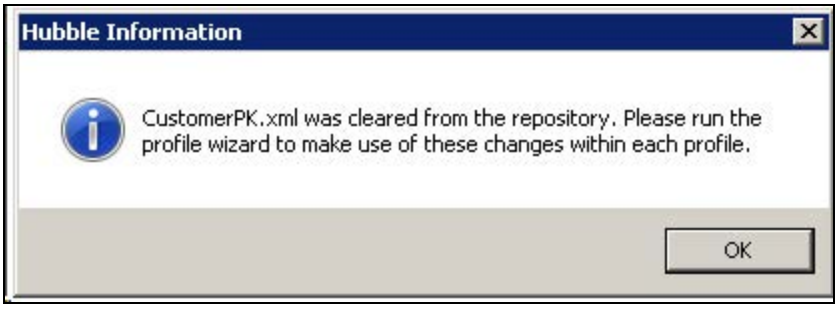


To export the current CustomerPK file, select the **Export** option. You will then be asked where the file is to be saved:



Select the required location and click **Save**.

To clear the current CustomerPK file, select the **Clear** option. The following message is then displayed regarding the profile wizard:



Integrity Checker

The integrity checker is designed to detect any problems or inconsistencies within the database that might interfere with the operation of Hubble.

To run an integrity check:

1. Right-click on a specific profile from the right-hand panel of Administrator.
2. Select **Integrity Checker**.
3. Under **Available Tests**, use the checkboxes to select which tests or groups of tests you want to run. Expand Common and Extended Tests as needed to see the detailed list of tests:
   i. **Common Tests** - recommended tests, which detect common inconsistent settings. These run quickly and can be run as part of the configuration of the database connection.
   ii. **Extended Tests** - additional tests, which may take considerably longer to run, are designed to tackle more complex data issues. We would typically recommend that you run these tests overnight.
4. Click **Run**. The results of the test appear in the bottom panel of the dialog.
5. When the results appear in the bottom-half of the dialog, you can export them to a CSV file by right-clicking on the results panel. If you have Microsoft Excel installed, the results will launch in Microsoft Excel.
6. The feedback from the data integrity tool is divided into two categories:
   i. **Warnings** - these suggest that current database settings may result in unexpected behavior.
   ii. **Errors** - these indicate settings that are not compatible with Hubble and need to change in order to ensure a complete and proper configuration.
7. If there are any errors or warnings, please seek advice from your Systems Administrator.

Account ID Integrity Test

The Account ID test is typically the most commonly used extended integrity test. The Account ID test is particularly helpful in these scenarios:

- Trial balances in Hubble are different from the balances in JD Edwards.
- Transactions displayed in the Hubble Transactions template are not visible in the Hubble Balances template even though they are posted transactions.

In JD Edwards, for a unique Account ID in the Accounts Masters table (F0901), there is only one unique combination of Company, Business Unit, Object Account and Subsidiary. In Hubble, you can set whether the application joins the Balances and Transactions tables the same way or by a full join (this is set in **Profile Options** in Administrator).

When the profile is set to join by Account ID, the join is the same as what is used in JD Edwards and therefore inquiry results will be the same as what is seen in JD Edwards. When the profile is set to a full join between the F0901 and F0902, the join is on Account ID, Company, Business Unit, Object Account and Subsidiary. In this case there can be a discrepancy in data between Hubble inquiries and JD Edwards data. It is slower to perform queries on this join option; however it will point out discrepancies that can then be fixed in your JD Edwards data.

This test is performed across the JD Edwards Balances tables; the inconsistency could be in a single table or multiple tables. Any integrity issues found by running this test need to be fixed in your JD Edwards data.

So for example, you have the following account in the Account Master:

ACCOUNT ID (AID)	CO (CO)	BU (MCU)	OBJ (OBJ)	SUB (SUB)
00000100	00001	1	1110	BEAR

In the Balances or Transactions table you would have postings against the same structure and the transactions balance:

ACCOUNT ID (AID)	CO (CO)	BU (MCU)	OBJ (OBJ)	SUB (SUB)	VALUE
00000100	00001	1	1110	BEAR	100
00000100	00001	1	1110	BEAR	-100

If you sum the values by Company (Co), this would balance to 0:

COMPANY (CO)	VALUE
00001	100
00001	-100
Total for Company 00001	0

And again by Business Unit (MCU), this would also balance to 0:

BUSINESS UNIT (MCU)	VALUE
1	100
1	-100
Total for Business Unit 00001	0

Scenario with incorrect data

If, for example, you have a single Account ID associated with more than one BU:

ACCOUNT ID (AID)	CO (CO)	BU (MCU)	OBJ (OBJ)	SUB (SUB)	VALUE
00000100	00001	1	1110	BEAR	100
00000100	00001	2	1110	BEAR	-100

In this scenario, your trial balance by company would be correct but your trial balance by Business Unit would be inaccurate.

If you sum the values by Company (Co), this would balance to 0:

COMPANY (CO)	VALUE
00001	100
00001	-100
Total for Business Unit 00001	0

However, by Business Unit (MCU), this would not balance to 0:

BUSINESS UNIT (MCU)	VALUE
0	0
1	100
Total for BU1	100

To get the correct result in Hubble, the data must be consistent across the Balances and Transaction tables.

Continuing with the same scenario, the test results for the Account ID integrity test would be as follows:

Account ID Test -- Warning: The following Company, Business-Unit, Subsidiary and Object-Account combinations from table [dbo].[F0902] are linked to more than one Account ID: '00104 - 020713 - - 8300 ', '00104 - 020713 - - 8300 ', '00104 - 020713 - - 8300 '

These results show that in the F0902 file there is more than one account ID present for the combination of Company, Business Unit, Subsidiary and Object Account.

- *Note that the combination of Company, Business Unit, Subsidiary and Object Account is separated by "-" and the complete combinations are comma separated.*

The second test that the Account ID integrity test does is the reverse of the first. It checks to verify that for each Account ID there is only one combination.

Account ID Test -- Warning: The following Account IDs are linked to more than one combination of Company, Business-Unit, Subsidiary and Object-Account: '00055319', '00055327', '00055458', '00055589', '00072477'

Data Dictionary Overrides

Hubble knows to add leading zeros to a company column when the columns data dictionary is set with Display Rule of MASK/0 (F9210.FROWDR = MASK and F9210.FRODR1 = 0) which is why tables with a xxPKCO column will automatically have leading zeros. However, columns like CO, KCO, and KCOO no longer have the Display Rule set with MASK/0 in JD Edwards, so a Profile Data Dictionary Override is needed to add the leading zeros.

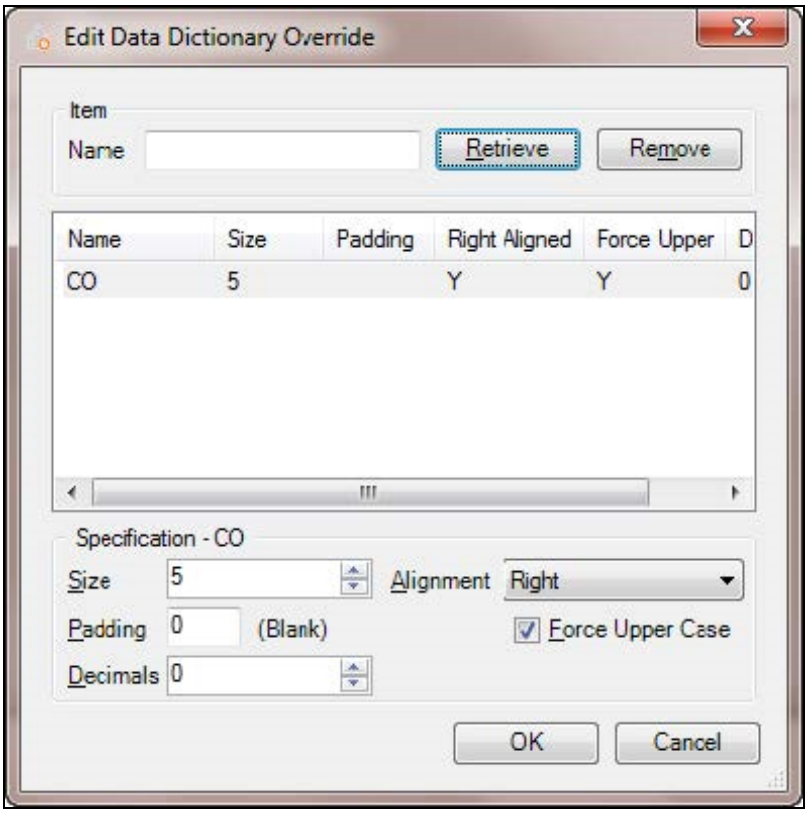
The Data Dictionary Override is designed to override settings held within the JD Edwards Data Dictionary in order to negate any inconsistencies within the database that might interfere with the operation of Hubble. Note that any override set for the profile does not modify the Data Dictionary in your JD Edwards database. The override information is stored within the Hubble Object Repository.

To set up overrides to the Data Dictionary:

1. Log into your repository if you are not logged in already.
2. Expand the **Data Sources** node in the left panel.
3. Click on **Profiles**.
4. In the right panel, right-click on the profile that you wish to amend.
5. Select **Assign Data Dictionary Override**.
6. Using the drop-down menu next to **Use override**, select the override you wish to use.
7. If you need to create a new override, click **Manage**.
8. In the **Data Dictionary Overrides** dialog, click **New**.
9. Enter a name for the new Data Dictionary Override.
10. Click **OK**.
11. Enter the **Name** of the item as entered on the Data Dictionary table, and click **Retrieve** to import the attributes to the override table.
    - *The naming convention for Data Dictionary Overrides ONLY allows for letters, numbers and underscores. Space characters are not valid.*
12. You can now modify the settings for that particular data item. These new settings will be the values used within Hubble once it is restarted.

Example of a Data Dictionary Override

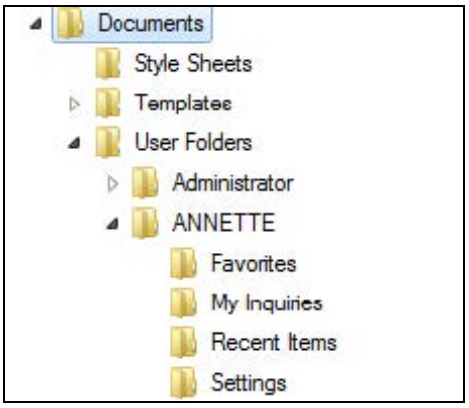
By default, a Data Dictionary Override is set up for column CO so that you do not need to enter in leading zeros if there are less than 5 values in a company number:



The Documents Folder

Overview

Within the **Documents** folder in Administrator there are 3 main folders:



- **Style Sheets** - Used for exports to Microsoft Word.
- **Templates** - Templates for reports, organized by module. Templates include custom templates as well as our Standard Templates. See **Importing the Standard Templates** for further details on that topic.
- **User Folders** - Set of folders for each named Hubble user, each set containing that user's favorites, inquiries, recent items and settings.

Date Fields/Moving Reports

Reports can be moved between folders within a single repository or from one repository to another. Depending on whether they are moved within one repository or between multiple repositories, the dates will vary.

- Created Date
  - When moving from folder to folder on one repository, this date will stay the same, which is the date when the inquiry was originally saved.
  - When moving from one repository to another, the created date will change to the date that it was imported into the new repository.
- Created By
  - Just as with Created Date, within one repository, it will stay the same.
  - When moving from repository to repository, it will change to the user who does the import/ export.
- Modified Date
  - The Modified Date tracks the date the report was last saved.
- Access Date
  - This is the date a report was last opened and run.
  - In order to report on report changes, within the Administrator application, highlight the **Documents** folder and use the New Search functionality to search through reports on a number of different filters and criteria. The **New Search** button is located on the **Home** tab. Refer to the **Search** topic for more details on the search facility.

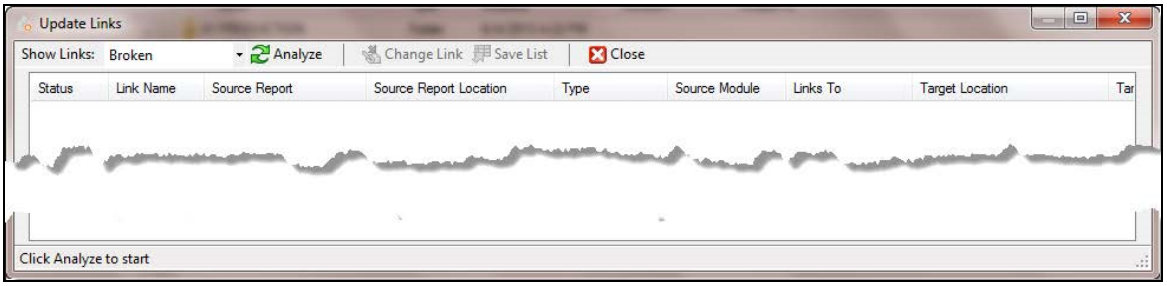
Update Links Functionality

The Update Links functionality allows a user to quickly analyze multiple inquiries and view links between inquiries. You can view all links, only valid links or only broken links. When viewing broken links, you can uncover instances where links to other inquiries/templates are not functional.

To Use The Update Links Functionality

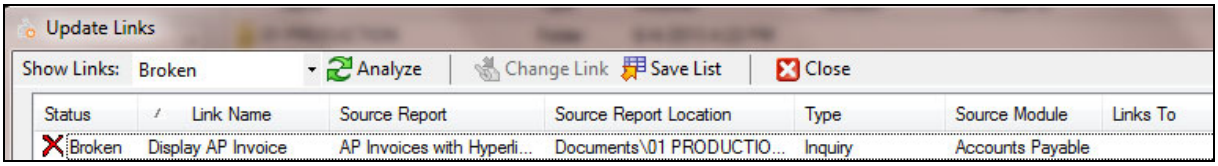
To use the Update Links functionality, follow the steps below:

1. Right-click on a specific document or folder (even the entire 'Documents' Folder) and select **Update Links**.
2. This brings up the **Update Links** dialog:



3. Use the drop-down next to **Show Links** to filter on Broken/Valid/All Links.
4. Click **Analyze**.

The information returned includes the following:



- **Status** – link status (broken or valid).
- **Link Name** – name of the link used within Hubble.
- **Source Report** – the report you are linking from.
- **Source Report Location** – saved location of the source report.
- **Type** – type of document (e.g. template or inquiry).
- **Source Module** – module the source report belongs to.
- **Links To** – the report you are linking to.
- **Target Location** – location of the target/destination report.
- **Target Module** – module the target report belongs to.

To change a link:

1. Highlight a specific row* and click **Change Link**.

   > **Tip:** *If you have multiple reports sharing the same link that you are updating, you can fix them at the same time using multi-select. Select all the affected reports by highlighting them and using the Ctrl key, then selecting Change Link. The link that you change will be updated in all the selected reports.

2. Navigate to the new inquiry you wish to link to.
3. Click **Open**.
4. Back in the **Update Links** dialog, if you click Analyze again you will see the link status has changed.
5. To save the results list in the **Update Links** dialog, click **Save List** to save it as a .csv spreadsheet compatible file.
6. Click **Close** to exit the dialog.

Import And Export Repository Information

Overview

Hubble uses repository data files (RDFs) to store repository information. The import/export function allows you to share items between your Object Repository and your computer via an RDF file.

Import/export functions as a temporary workspace or staging area, so once you have completed the import or export, be sure to clear this workspace.

Examples of when you may use the import function include the following:

- When upgrading or running parallel to an existing Object Repository.
- When you need to restore your Object Repository from a backup.
- When you wish to import the Standard Templates back into Administrator (for example when templates have been overwritten or have not been upgraded).

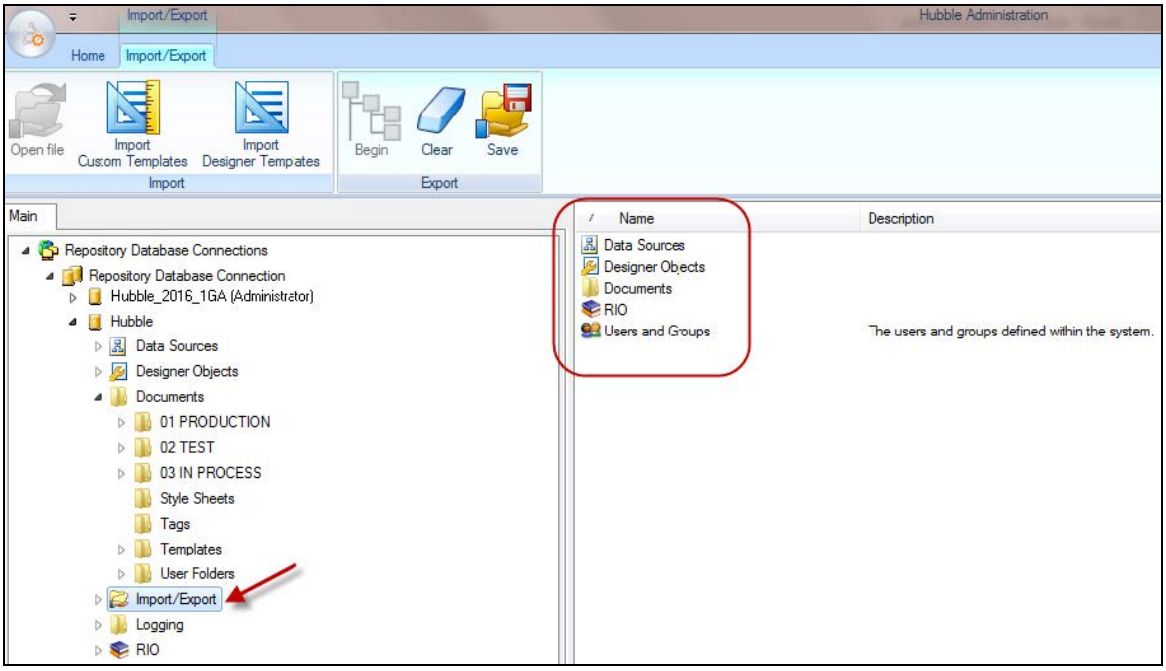
Examples of when you may use the export function include the following:

- When running parallel installs of Hubble.
- When you need to send a particular inquiry to our Customer Support Department for further assistance.

Import Into A Repository

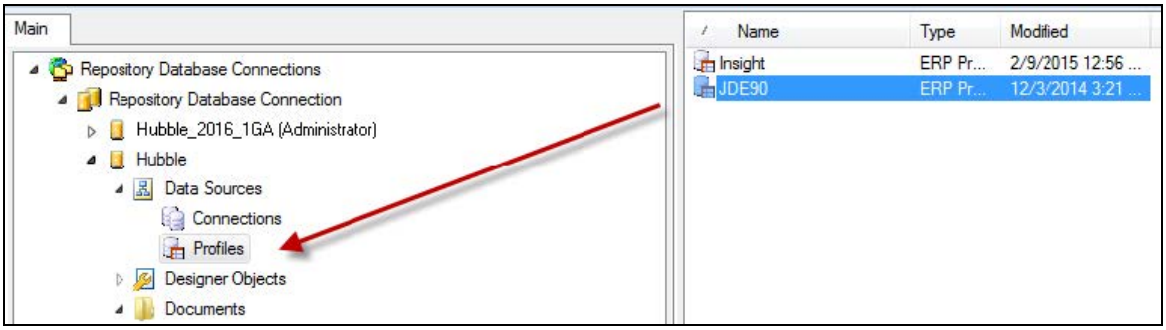
Follow the steps below to import into the repository:

1. Log into your repository if you are not logged in already.
2. Highlight the **Import/Export** node in the left panel and then either right-click and select **Open File** or click **Open File** on the Ribbon.
3. From the **Open File** dialog, navigate to and select the RDF file and click **Open**.
4. The data from the RDF is now in a staging area under **Import/Export**. Everything included is displayed in the right panel:

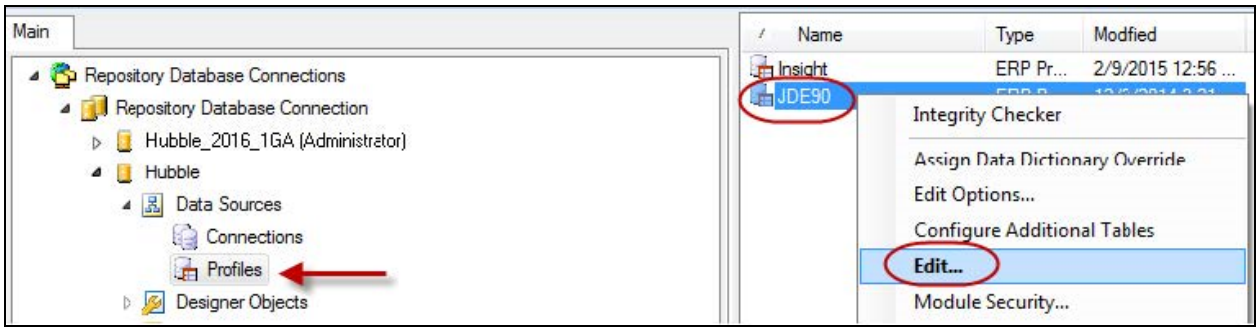


5. You now have the option to either drag and drop or copy each imported object from the holding area to the corresponding object within the Object Repository. This can be done at the highest level of the object tree, such as **Data Sources**, or lower down the tree, such as under **Profiles**.

   (The objects can also be copied to multiple repositories if desired.) If you wish to add all items of one Repository Data File to another, use the **Restore** function instead of the **Import** function.



6. If any profiles have been imported, go through the profile wizard again, making sure all tests are completed successfully. The profile wizard can be access by right-clicking the individual profile, in this example JDE90, and then selecting **Edit**:



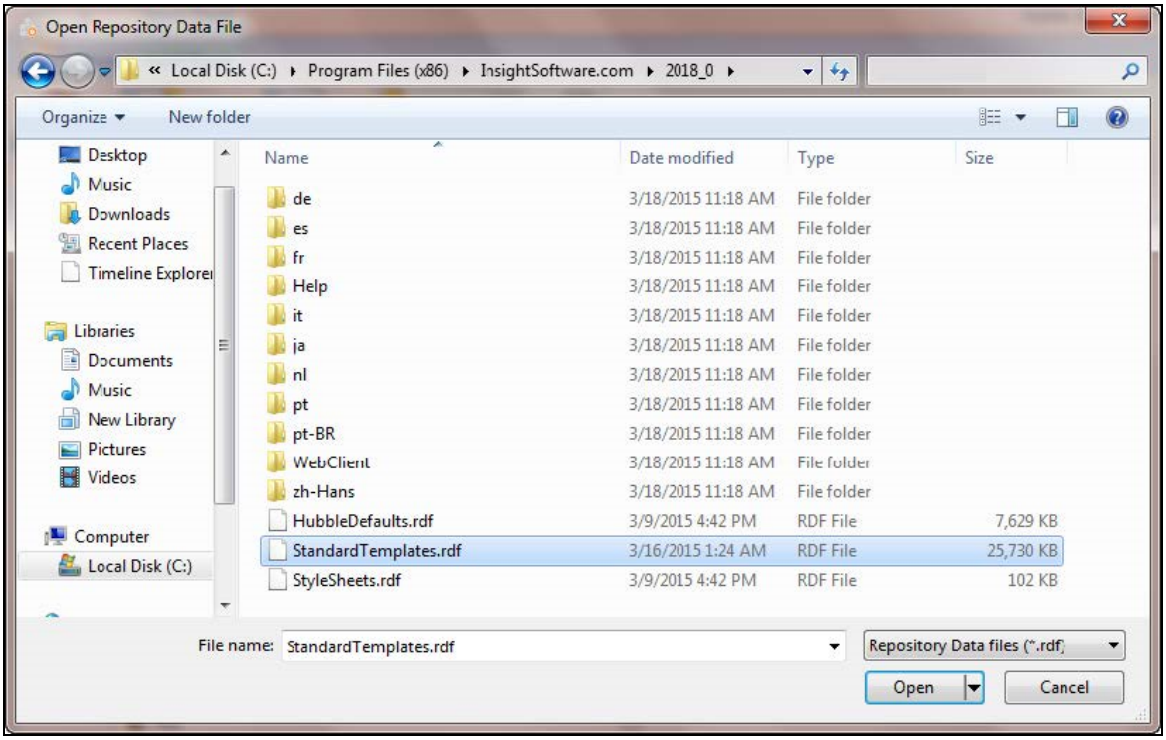
7. Assign Permissions as needed for this object that was just moved into the repository.
8. When finished, be sure to clear the temporary workspace area by highlighting the **Import/ Export** node in the left panel and then either right-clicking and selecting **Clear** or clicking **Clear** on the Ribbon.

Import The Standard Templates

Follow the steps below to import the standard templates into the repository:

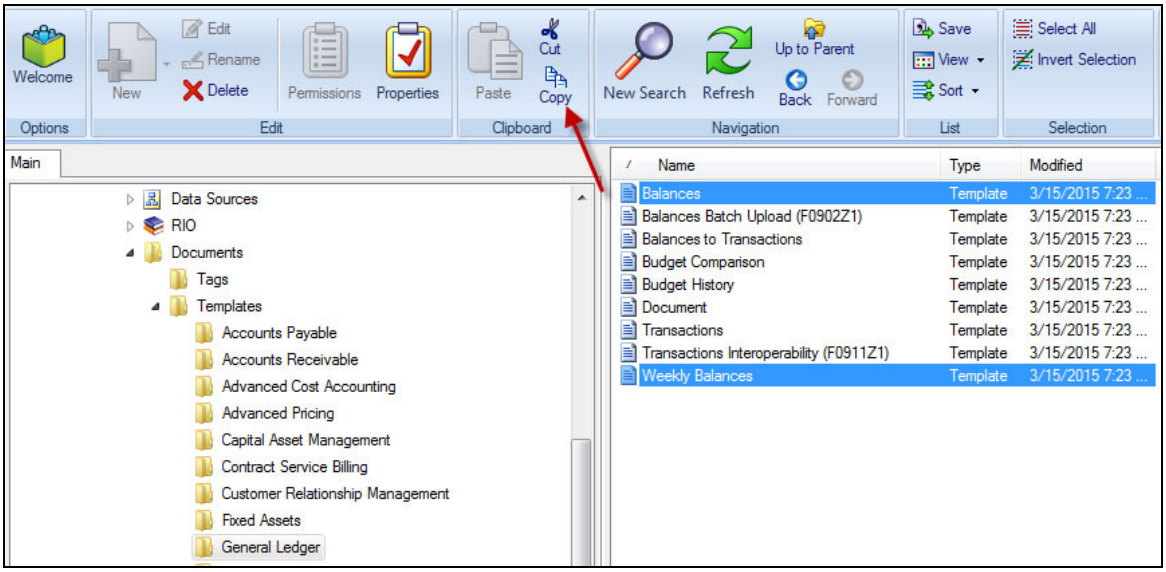
1. Log into your Repository if you are not logged in already.
2. Highlight the **Import/Export** node in the left panel and then either right-click on **Import/Export** and select **Open File** or click **Open file** on the Ribbon.

3. From within the Hubble installation folder, highlight StandardTemplates.rdf and select **Open**:

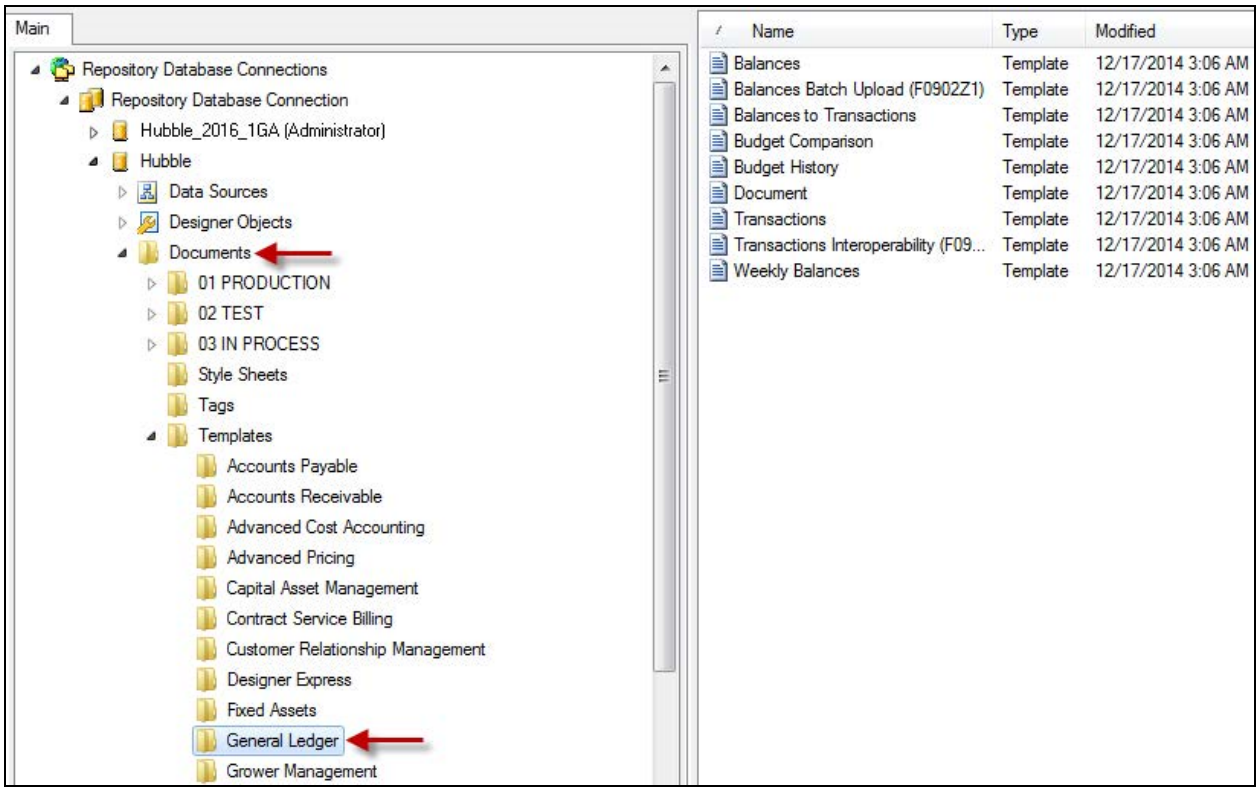


4. On the left panel, expand **Import/Export > Documents > Templates**.

5. In this example, the GL Balances and Weekly Balances templates will be copied. Using the Ctrl key, select both templates and either right-click and select **Copy** or click **Copy** in the Ribbon:



6. Collapse the **Import/Export Folder**, expand **Documents > Templates** in the designated repository and highlight the folder into which you wish to put the templates (in this case the General Ledger folder).



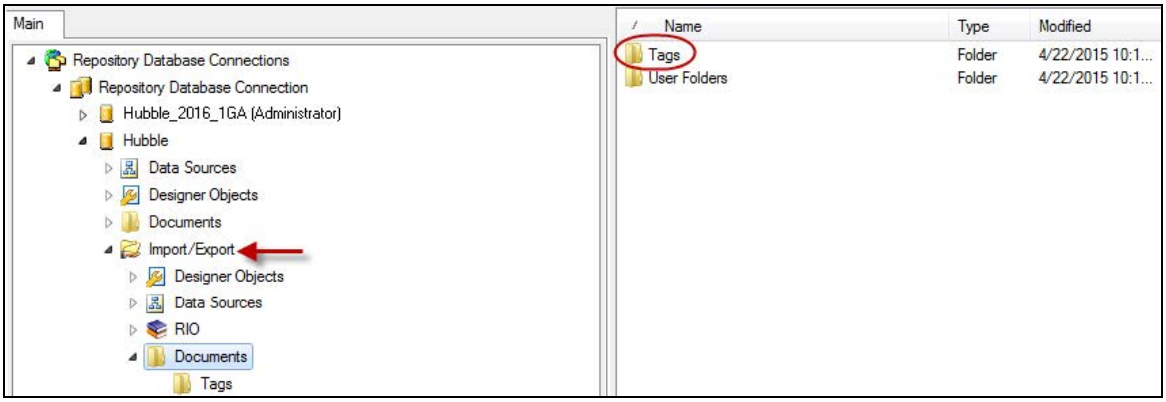
7. Either right-click and select **Paste** or click **Paste** in the Ribbon.
8. When prompted, select **Replace All** to overwrite the old templates.
9. When finished, clear the staging area by selecting the **Import/Export** folder and either right- clicking on **Import/Export** and selecting **Clear** or by clicking **Clear** on the Ribbon.

Export From The Repository

The **Export** function is used to select and save single and multiple Repository elements to a repository data file (RDF). (To export the entire repository, use the **Backup** function instead of the **Export** function.)

1. Log into your repository if you are not logged in already.
2. Highlight the **Import/Export** node in the left panel and then either right-click and select **Begin Export** or click **Begin** on the Ribbon.
3. A blank repository then opens within the **Import/Export** tree. Use this to paste or drag and drop the repository items that you want to export.

   In this example, the 'Tags' Folder was moved into the staging area:



Another way to export single items from the Repository is to:

1. Highlight the item you wish to export.
2. Right-click and select **Export**.
3. When the **Save file** dialog opens, name and select a location to store the data.

Import Custom Templates

A custom template is a Designer-created custom-requisitioned template.

1. In Administrator, focus on the **Import/Export** node.
2. Click **Import Custom Templates** on the ribbon.
3. Navigate to the template (RDF file) you are importing and click **Open**.
4. This will look in the RDF file, find all templates and import them into the *Custom Templates* folder.
5. If the *Custom Templates* folder doesn't exist, it will be created underneath Documents. (You will need to refresh the main Administrator page in order to see it once it is created.)
6. Templates in the Custom Templates folder with a matching Unique ID will be replaced by one being imported. (The import propagates template changes to reports which depend upon the imported templates and have a revision version lower than that of the template.)
7. A progress window will be displayed (similar to that at the end of the profile wizard), which will show importing and propagating progress. It will automatically close once the tasks have completed. If the RDF has none or just a couple of templates to import, it will disappear immediately.

Import Designer Templates

A designer template is a standard Hubble-created/delivered Designer template (created/delivered by our internal Solutions Team).

1. In Administrator, focus on the **Import/Export** node.
2. Click **Import Designer Templates** on the ribbon.
3. Navigate to the template (RDF file) you are importing and click **Open**.

4. This will look in the RDF file and search for designer templates which either have a corresponding template in the repository (matched using the Unique ID) and a revision less than that in the RDF. It also looks for those that do not exist at all in the repository.
5. These templates will be imported to the same corresponding location they were stored in within the RDF, e.g. if RDF location is *Documents**Templates**NewModule**NewTemplate*, and then stores them in the equivalent location in the repository. (The import propagates template changes to reports which depend upon the imported templates and have a revision version lower than that of the template.)
6. A progress window will be displayed (similar to that at the end of the profile wizard), which will show importing and propagating progress. It will automatically close once the tasks have completed. If the RDF has none or just a couple of templates to import, it will disappear immediately.

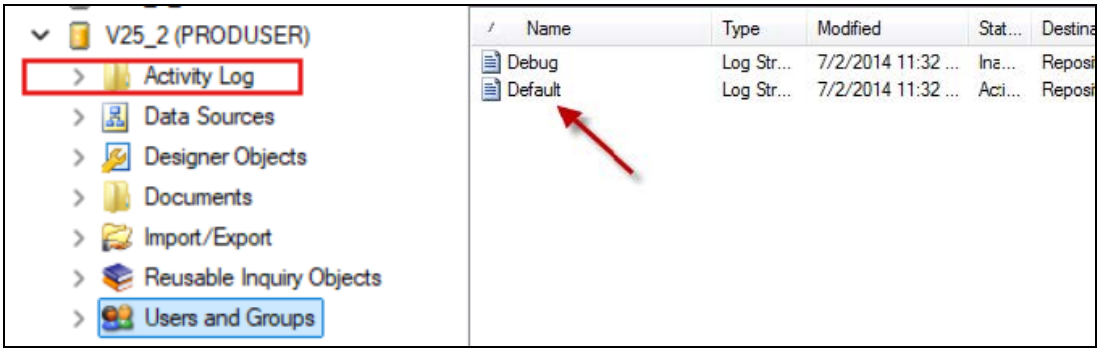
Configure Logging

Overview

The logging functionality, which is set up in Administrator, records events including who did what, when and to whom.

By default, basic logging is enabled at an *informational* level in all new repositories and is stored in a table that is created for that repository. The log will record *when* an inquiry object has been edited, but cannot record the details of what changed (for example formats or calculations).

All repositories have a folder called **Activity Log** that appears in the Administrator. This directory contains one Log Stream called **Default**, as shown in the following screenshot.



The Logging directory can contain multiple log streams which can be enabled or disabled for different logging scenarios. Log Streams can be treated like any other object within the repository in that they can be created, renamed, deleted, copied, etc.

Important: Certain logging settings should only be used for specific situations and are not enabled continuously.

Be aware that setting the Categories to 'All' or setting the Severity to the 'Debugging' level can substantially increase the number of log entries recorded, which will impact the performance of any application within Hubble.

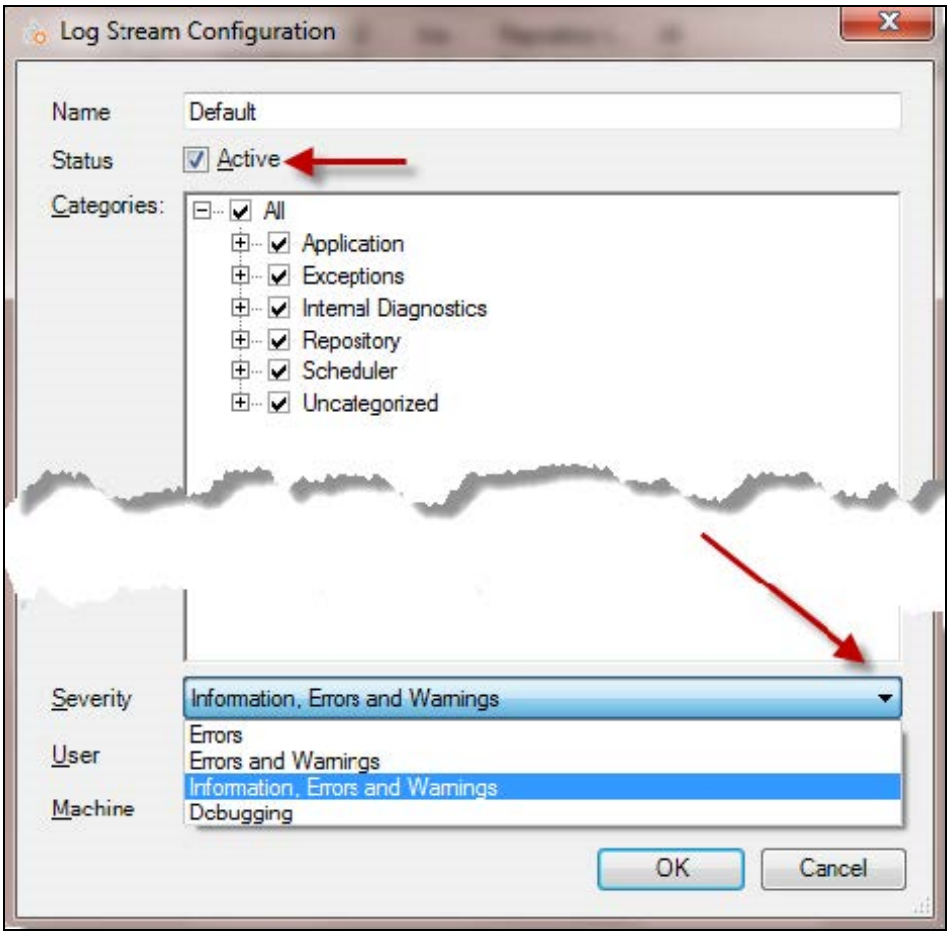
Once you have captured the desired information using the logging functionality, it is extremely important that you set the logging back to the default values.

Setting Up And Modifying Logging Configuration

You can edit a Log Stream to configure the status (active or not) as well as when to log activity according to the type of activity, the severity, the specific user and the specific machine.

To edit a Log Stream:

1. Log into your repository if you are not logged in already.
2. Highlight the **Logging** node in the tree on the left panel.
3. In the right panel, right-click on the Log Stream you wish to edit whether it is the **Default** Log Stream or one you have already created.
4. Click **Edit**. The **Log Stream Configuration** dialog will be displayed:



5. Configure the Log Stream as needed:
   i. **Name**
   ii. **Status** – active/inactive (It is recommended that you do not delete a Log Stream but disable it in case you to re-enable the logging later.)
   iii. **Category** – set logging for specific situations.
   iv. **Severity** - specify the level of information being recorded by the log stream. It is recommended that these logging settings are only used for specific situations and are not enabled continuously.

> Be aware that setting the Categories to 'All' or setting the Severity to the 'Debugging' level can substantially increase the number of log entries recorded, which will impact the performance of Hubble.

v. **User** – optionally, select individual users for logging (user groups cannot be selected). If left blank, it is used for all users.

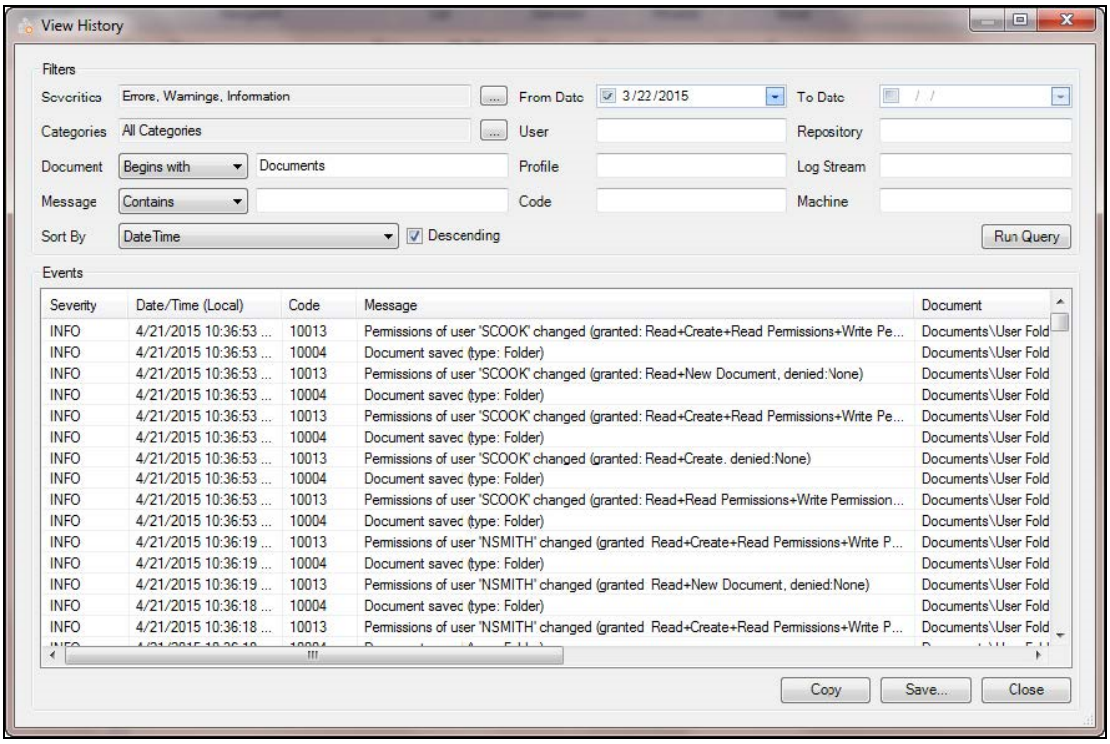
i. Click the "…" button to open the **Select User** dialog.

ii. Select a **User**.

iii. Click **OK** to return to the main dialog.

vi. **Machine** – optionally, specify a PC name so that only activity originating from that PC is logged.

vii. Set thresholds for log generation. When the log count surpasses the specified limit, you receive notifications.



As a Hubble administrator, you have the option to configure an alert threshold while setting up the log stream. Importantly, this field is not mandatory, so you can leave it blank if you prefer not to receive notifications.

viii. When editing a log stream that is used to log activity in Administrator, you must restart the application for the changes to be correctly applied.

> **Note:** Once you have captured the desired information using the logging functionality, it is extremely important that you set the logging back to the default values.

> As mentioned above, you should not continuously enable logging, particularly debugging, as it will impact the performance of any application within Hubble. It should only be set to capture specific information and then disabled once this information has been recorded.

Viewing Logged Activity

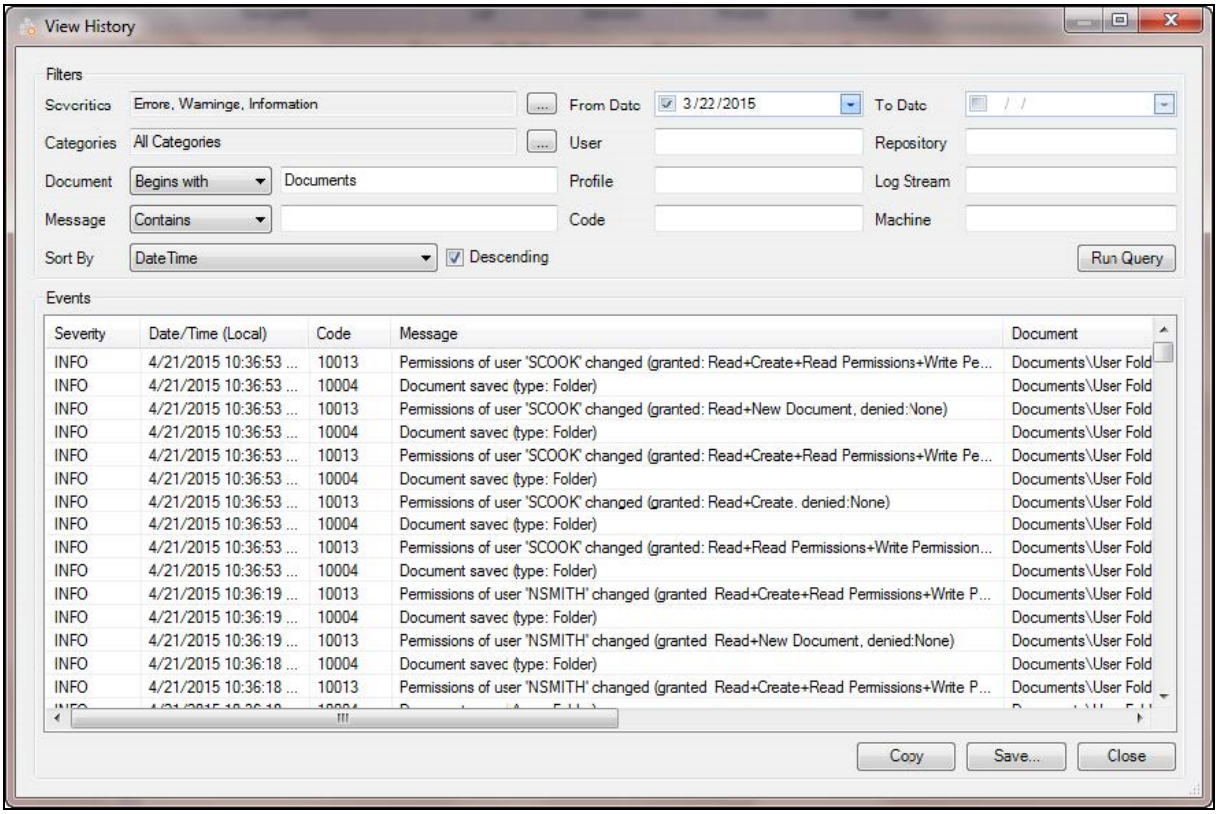
Administrators are automatically entitled to use the View History dialog. Non-administrators must be granted the Logging capability in order to get access to the dialog.

1. Log into your repository if you are not logged in already.
2. Highlight the item for which you wish to view the logging activity. (This can be an individual item such as the Documents folder, if logging had been set up for it, or the Default Log Stream under Logging to include all items.)
3. Right-click on the item and select **View History**.
4. Use the filters to narrow down the data returned:
   i. **Severities** - the required severity level of Errors, Warning, Information or Debug specified in the Log Stream(s).
   ii. **Categories** - the Categories specified in the Log Stream(s).
   iii. **Document** - the Document or Document Folder text. The logged events can be further narrowed down by using the associated drop-down control's options of Equals, BeginsWith, Contains and EndsWith. (For example, Begins With if used in conjunction with Document would return all the logged events associated with all documents, reports and templates stored within the Documents folder.)
   iv. **Message** - specific text within the Message column. The logged events can be further narrowed down by using the associated drop-down control's options of Equals, Begins With, Contains and Ends With.
   v. **Sort By** - set the order of the logged events. Any of the associated filters can be selected and can be sorted by enabling/disabling the Descending checkbox.
   vi. **From Date/To Date** - the date ranges of the activity. Either manually type in the dates or use the down arrow to select dates using the calendar. (You can overwrite the From Date that automatically defaults in.)
   vii. **User** - the specific user making the changes. (Useful when multiple users are accessing the same repository.)
   viii. **Profile** – a specific Profile. (This is particularly useful when diagnosing whether issues are related to a Profile configuration issue.)
   ix. **Code** - the specific (numeric) Code for a function that is included within a Categories group. (You can see the specific codes by looking in the Code column or in the Categories dialog, accessed by clicking on the … next to the Categories filter.)
   x. **Repository** – the specific repository.
   xi. **Log Stream** –the specific Log Stream being used.
   xii. **Machine** – the specific Machine PC/Server.
5. Click **Run Query** to refresh the logged events displayed in the lower half of the dialog.

The **View History** dialog also allows the users to export the logged events via:

- **Copy** - copies any highlighted records into the local computer's clipboard, allowing the user to paste these records into an appropriate program.
- **Save** - save all displayed Logged Events into a CSV file for later analysis.

In the example shown, the selection of the **Document** folder has populated Document in the **Document** Filter. However the pre-population of filters will work with inquiries, templates, report packs, reusable inquiry objects, and profiles.

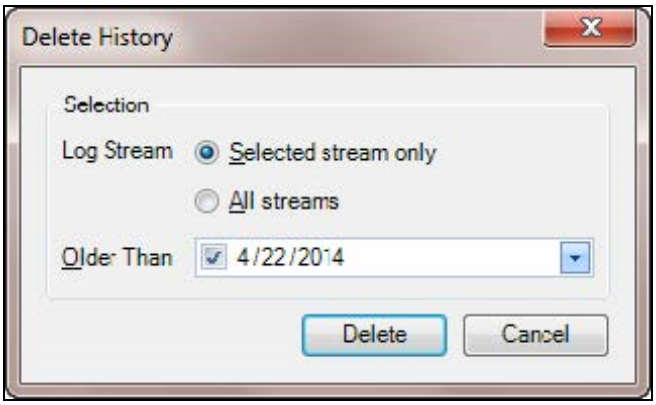


Deleting Logged Activity

Logged data can be purged via the **Delete History** functionality. Individual objects within the repository can have their logged events purged or, alternatively, this can be done by individual Log Streams as shown below:

1. Log into your repository if you are not logged in already.
2. In the left panel, highlight **Logging**.
3. In the right panel, highlight the specific Log Stream for which you wish to delete the logging activity and select **Delete History**.
4. In the **Delete History** dialog, specify:
   i. **Log Stream** – either the selected stream or all streams.
   ii. **Older than** – log streams older than the date specified will be deleted. (If left blank, all entries

will be deleted.) The default date can be overridden.



5. Click **Delete**. The **Hubble Information** dialog that appears tells you how many log entries were deleted.

Reusable Inquiry Objects

From Administrator, you can manage Reusable Inquiry Objects (RIO) by creating new folders and defining Permissions to users/groups for the folders and/or the individual RIO items within the folders. (From Hubble, new folders can be created but permissions can only be set for them through Administrator.)

To create a Reusable Inquiry Objects (RIO) folder:

1. Log into your repository if you are not logged in already.
2. In the left panel, expand the RIO node in the tree structure. You will then see a folder for **Global** as well as folders for any individual profile that has been set up. The **Global** folder holds RIO items that can be used in all profiles.
3. Right-click on the level you wish to create a folder, whether it is Global or a specific profile, and select **New > Folder**.
4. Provide a name for the folder.
5. Assign permissions by right-clicking on a specific folder or an item within a folder and selecting Permissions.

Configure Users And Groups

Note: A user should not be allocated to multiple groups at a time. If a user is added to more than one group, when logging-on they will only ever be assigned the permissions etc. from the first of the groups alphabetically.

Add A User

Under the Users and Groups node within your repository in Administrator, users can be added in one of two ways:

1. Manually
2. Imported and synchronized from your ERP system

> **Note:** For EBS customers, once a valid username is added in Administrator, the application also picks up the responsibilities assigned to the user. Upon logging in to Hubble, the user will select one of these responsibilities.

Create A User Group

In Administrator, you can create groups in which to organize users; this can particularly be useful not just for organizational purposes but also when performing tasks at the group level such as when setting permissions or capabilities.

1. Log into your repository if you are not logged in already.
2. Expand the **Users and Groups** node in the left panel.
3. Highlight the level above which you want to create the new group, whether it be **Everyone** or another level that already exists.
4. Right-click on this level and **New> Group**.
5. In the **Group Definition** dialog, create a name for the group and, optionally, a description. (Leave the **Members** section in this dialog blank for now; it will show the users included in this group after you have added them in at a later step.)
6. Click **OK**.
7. You will now see this group listed in the tree structure under **Users and Groups**.

Edit A Group

Once created, a user group can be deleted. It is important to know that when a group is deleted, all users and groups within it will be deleted as well. The exception to this is for users who also belong to other groups; in that case the user will not be deleted. Additionally, you cannot delete the 'Administrator' or 'Everyone' Groups.

1. Log into your repository if you are not logged in already.
2. Expand the **Users and Groups** node in the left panel.
3. Right-click on the group you wish to delete and select **Delete**.
4. You will be prompted to confirm this action.

Manually Add A New Standard User

You can manually add Hubble users within Administrator. If you manually create a user, you must manually assign permissions for the profiles. (This is different than synchronizing a user when the system automatically assigns permissions for that user to the associated profile.)

1. Log into your repository if you are not logged in already.
2. Expand the **Users and Groups** node in the left panel.

3. Highlight the level above which you want to add the user, whether it be **Everyone** or another level that already exists.
4. Right-click on this level and **New> User**.
5. In the **User Definition** dialog, enter in the requested information and activate the options as desired:
   i. Name [*Hubble username*]
   ii. First Name
   iii. Surname
   iv. Email
   v. Password
   vi. Confirm password
   vii. Enforce password policy
   viii. Enforce password expiration
   ix. User must change password at next login
   x. Enforce account expiration
   xi. Account is disabled
6. Click **OK**.
7. You will now see this user listed in the tree structure under whichever group you placed them in.

Note that:

- Passwords may not be too common, e.g. the password 'password' can no longer be used.
- Passwords may not contain sequences, e.g. 123456 or 111111, qwerty, and abcdef are not allowed.
- The minimum password length is 6 characters.
- The default setting is that new users must change the password when they first login.
- Entry of an email address is mandatory. Upgraded and imported users can still login to Desktop without having the email address, but when the account is edited the Administrator must enter their email address.

> **Note:** Each Hubble user is required to have a valid email address regardless of whether or not they use Web Single-Sign on (SSO).

If a customer is using the Desktop Simplified Sign-On (reduced login) functionality either of these two workflows may be followed:

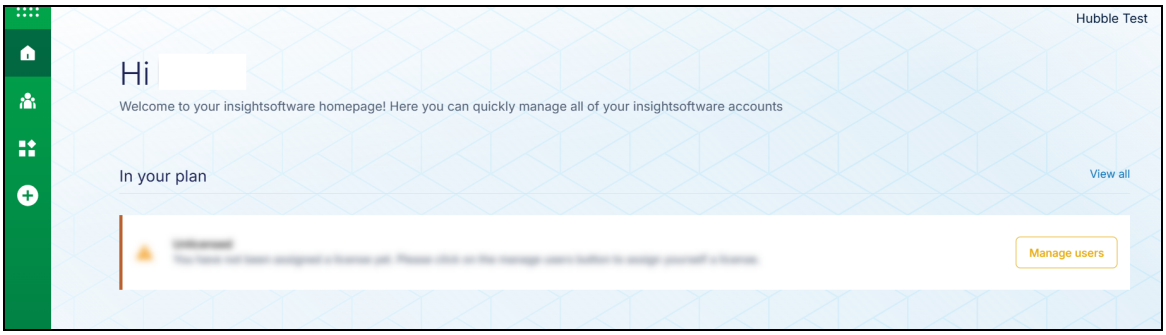
1. The user enters a password once (no change):
   i. The user is created in the Administration tool, logs into Hubble and enters a password 1 time.
   ii. On this login Hubble will record the user's Windows domain user identity.
   iii. On subsequent logins they will not be requested to enter a password.

2. The user never enters a password (small change):
    i. The user is created in the Administration tool and the Administrator sets the Windows domain user so the user never needs to enter a password.
    ii. There is an additional step to enter the users email address, as this is now required when editing the user definition in the Administration tool.

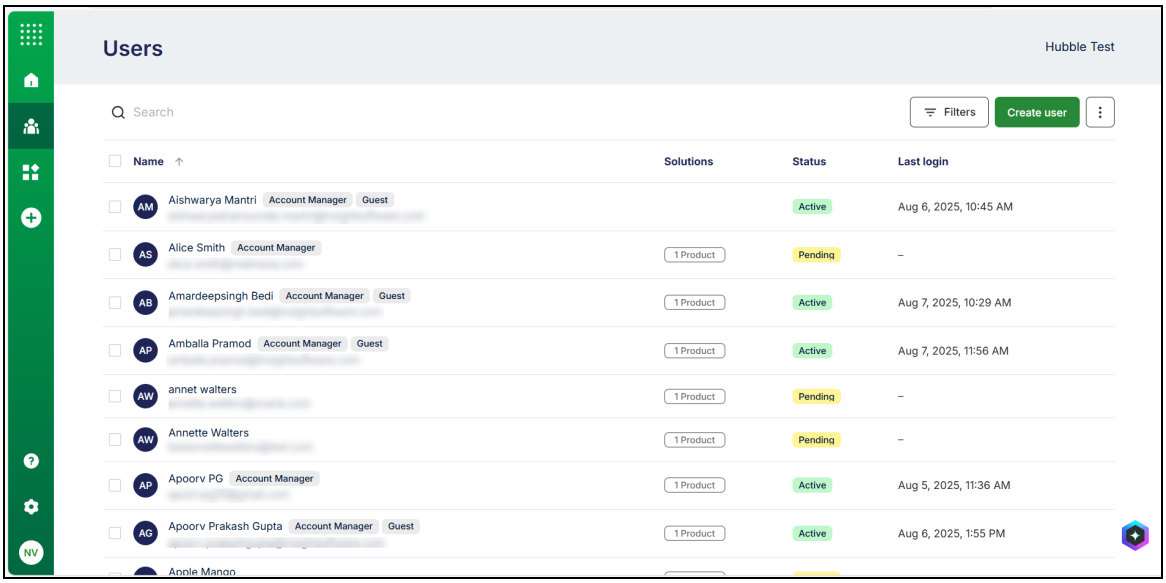
The user can then log in with no password.

Add A Platform User

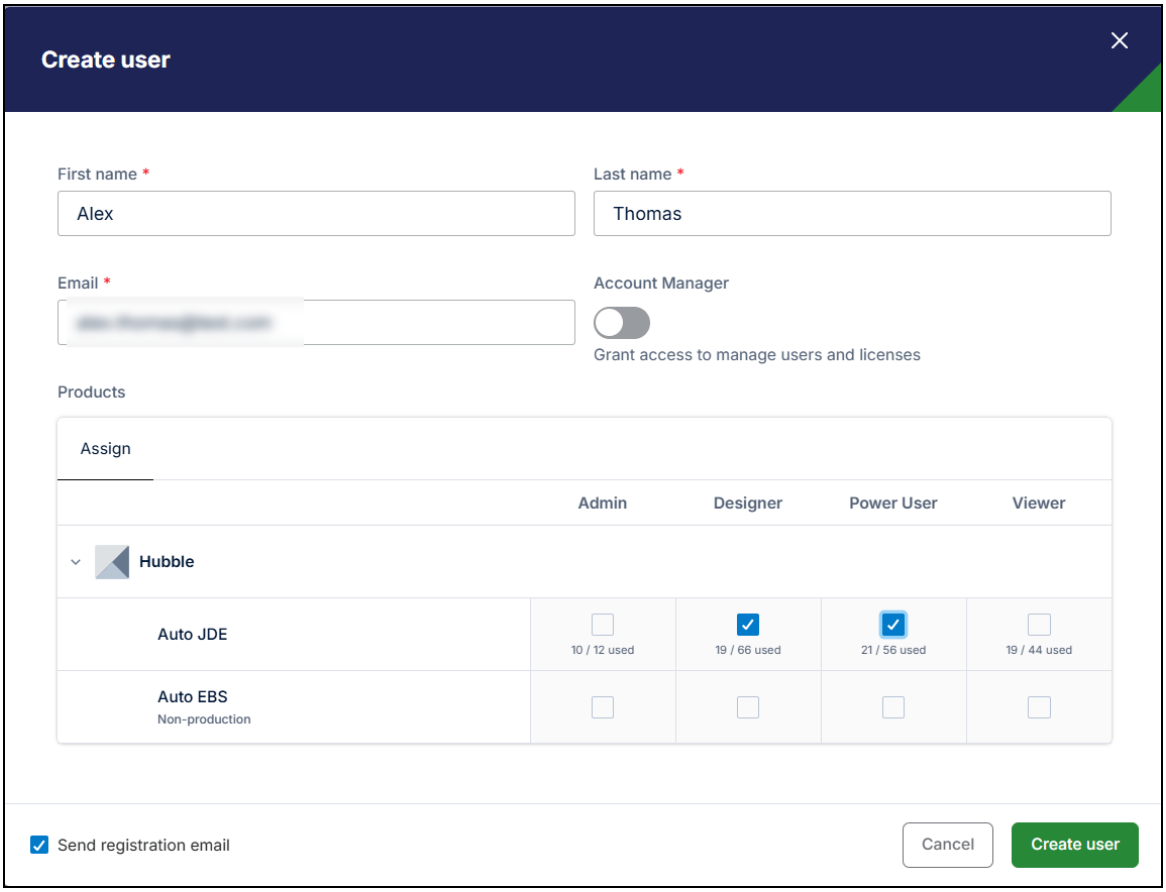
1. Log in to the Platform with administrator credentials.
2. Select **Manage Users** to navigate to the **Users** section.



3. Select the **Create User** button.

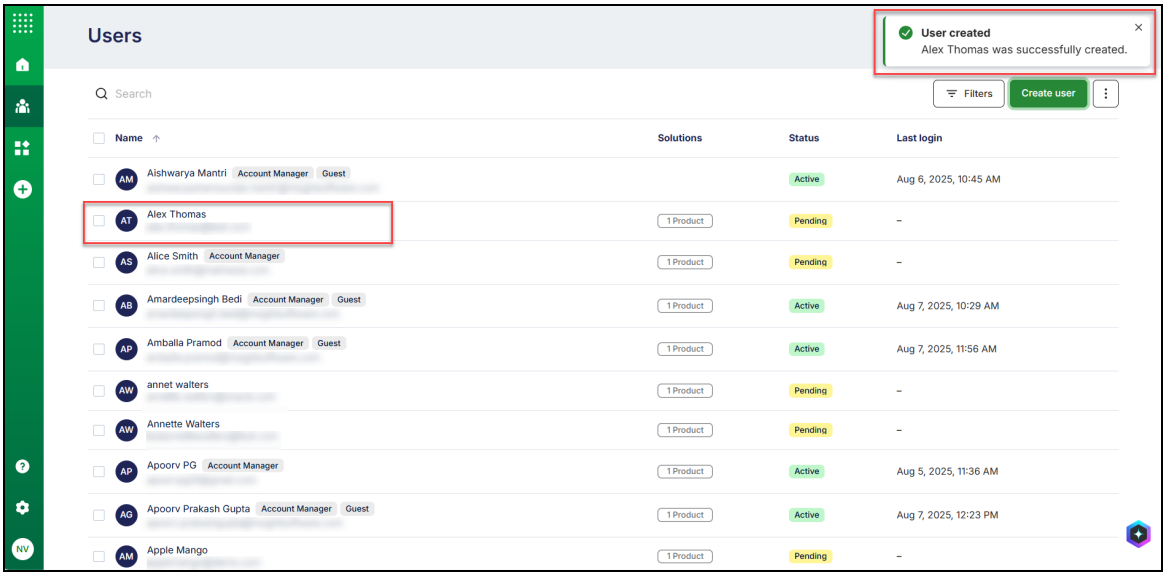


4. Enter the required user information:



- **First name**
- **Last name**
- **Email**

5. Assign a user license type:
   - **Designer**: For users who create and design reports
   - **Power User**: For users who run and modify reports
   - **Viewer**: For users who only view reports
6. Select **Create user** to create the user.



7. Complete user setup by using the **Platform User Sync** tab in the **ERP User Synchronization** window. Select the **Add** action to synchronize the user.

   After Platform user creation, the user appears in Administrator with their email address as the username.

Edit And Delete Users

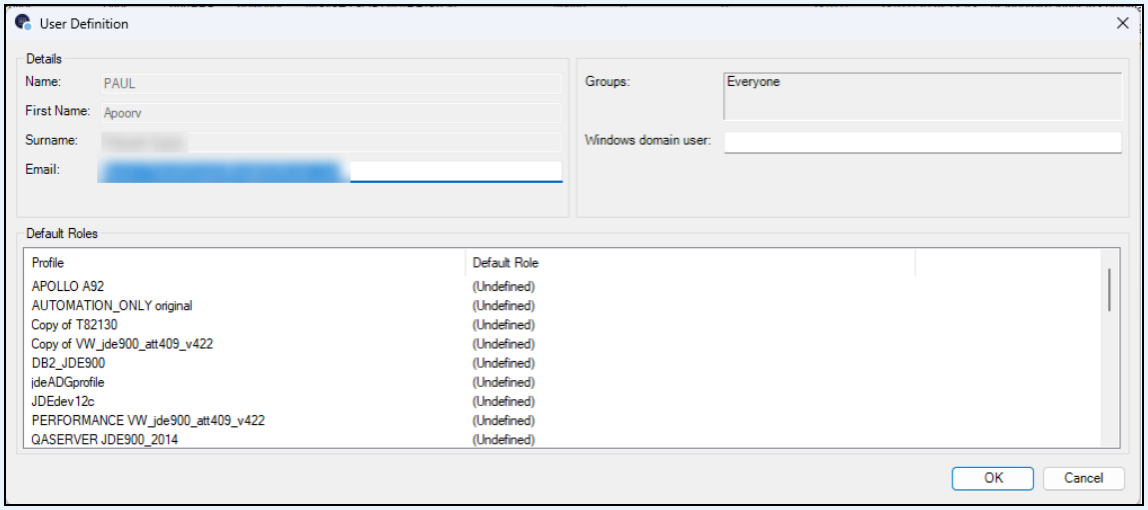
A user profile can be edited after it is created. The only setting that cannot be changed is the user's Hubble username.

> **Note:** You can only delete the **Administrator** User when there is at least one other Administrative Account available (other than **System**). The **System** User cannot be used as a login and cannot be deleted, renamed or moved even by Administrators as it is used for internal operations.

Before deleting a user, you may want to review what is contained within their profile by using the **Browse as User** functionality.

1. Log into your repository if you are not logged in already.
2. Expand the **Users and Groups** node in the left panel.
3. Right-click on the specific user and select **Edit** or **Delete**, depending on which action you wish to do.

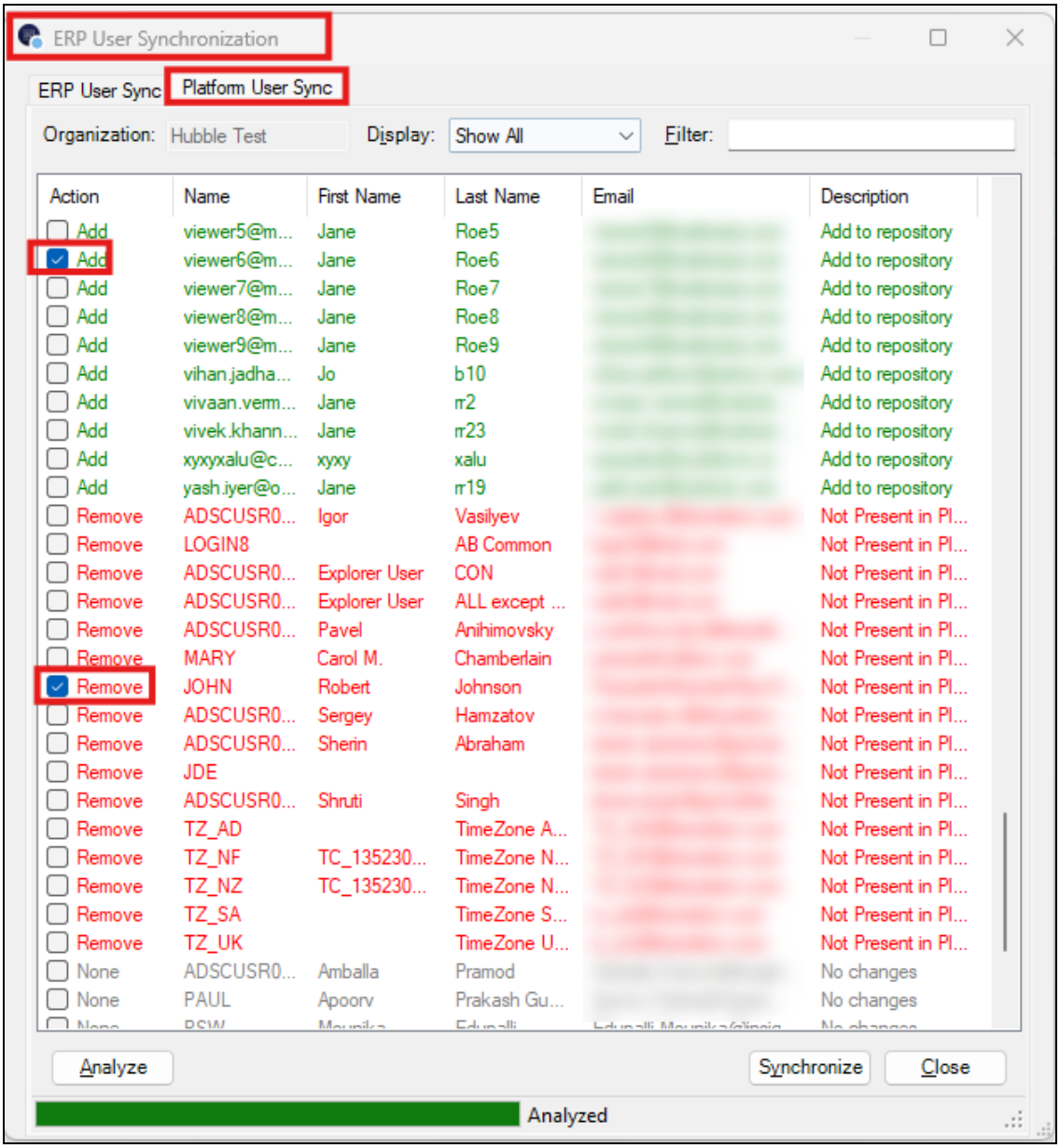
Note: Platform users can only edit the email address field in the **User Definition** window.



Platform User Deletion

For Platform users, after deleting a user from the Platform:

4. Perform synchronization in the Administrator tool to remove the user from the Hubble repository.



5. The deleted user will appear with a **Remove** indicator during synchronization.
6. When prompted to confirm deletion, select **Yes**.
7. Complete the synchronization process to finalize the user removal from Hubble.

Remove Platform User Data For GDPR Compliance

When a Platform user leaves your organization, remove their personal data to comply with GDPR requirements.

Remove User From Platform

1. Sign in to the Platform with administrator credentials.
2. Go to the **User Management** section.
3. Search for the user you want to remove.
4. Select the user, then select **Delete User**.
5. When prompted, confirm the deletion.
6. Verify that the user no longer appears in the platform user list.

Synchronize User Deletion In Hubble

Complete user removal using one of these methods:

Method 1: Platform Synchronization

1. Sign in to the Hubble Administrator tool.
2. In the left panel, select **Users & Groups**.
3. Right-click and select **Synchronize**.
4. In the synchronization window, select the **Platform User Sync** tab.
5. Select **Analyze** to get the current Platform user list.
6. Find the deleted user in the list. The user will show an **Action** status of **Remove**.
7. Select the user, then select **Synchronize**.
8. This marks the user for deletion in Hubble.

Method 2: Direct Deletion from Hubble Repository

1. In the **Users & Groups** section, find the user you want to delete.
2. Right-click the user and select **Delete**.
3. Review the deletion confirmation. The following data will be removed:
   - User profile information
   - Module assignments
   - Access permissions
   - Personal preferences
   - Repository access history
4. Select **Delete** to permanently remove all user data from Hubble.
5. Verify the deletion by searching for the user. No results should appear.

Important Notes

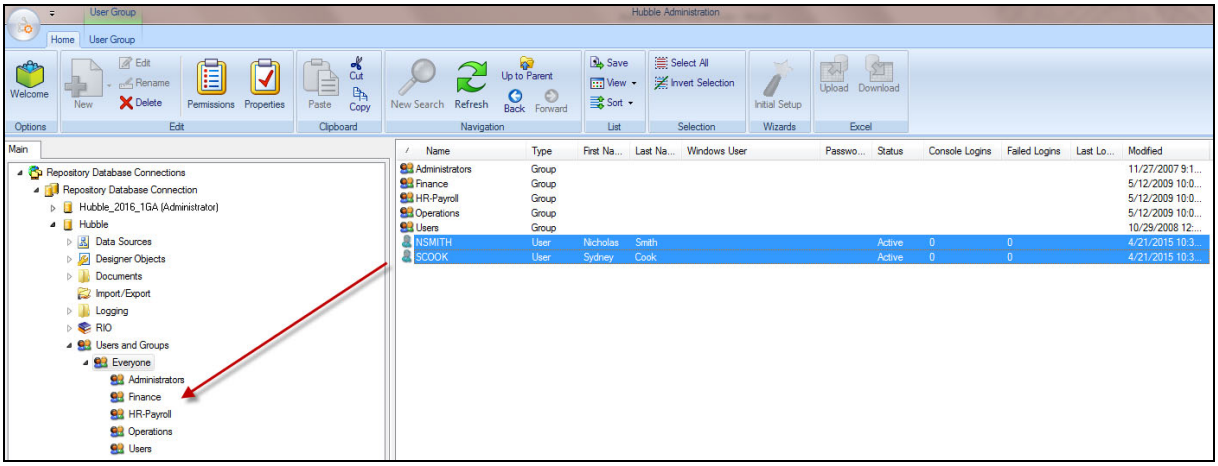
- Platform deletion must occur first to prevent re-synchronization
- Synchronization ensures Platform and Hubble remain aligned
- This process permanently deletes all user data and cannot be undone
- Allow time for synchronization to complete before final deletion
- For immediate deletion needs, proceed directly to Method 2 after Platform removal

Move A User To A Different Group

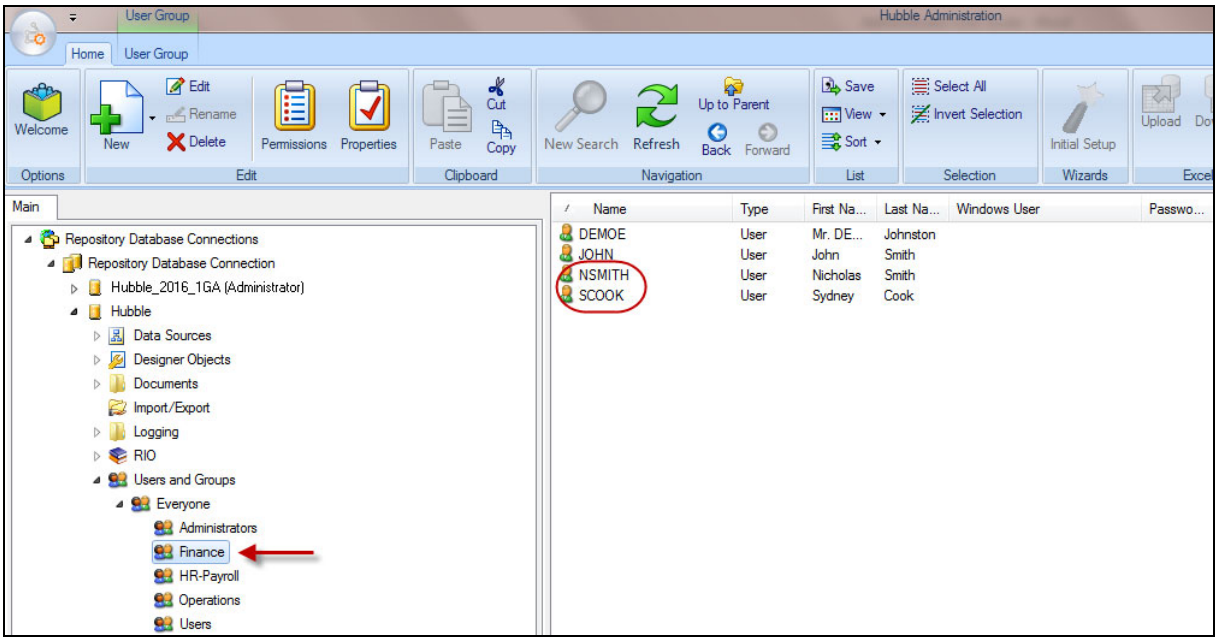
In Administrator you can move users to different user groups by completing the following steps:

1. Log into your repository if you are not logged in already.
2. Expand **Users and Groups** in the left panel.
3. Select **Everyone** (or whichever group the users are currently included in).
4. Highlight the users in the right panel and drag them over to the desired group.

In the example below, we will move 2 users from the Everyone level to the Finance Group. This is done by focusing on the Everyone level, highlighting the 2 users, and then dragging and dropping them from the right panel to the correct group in the left panel:



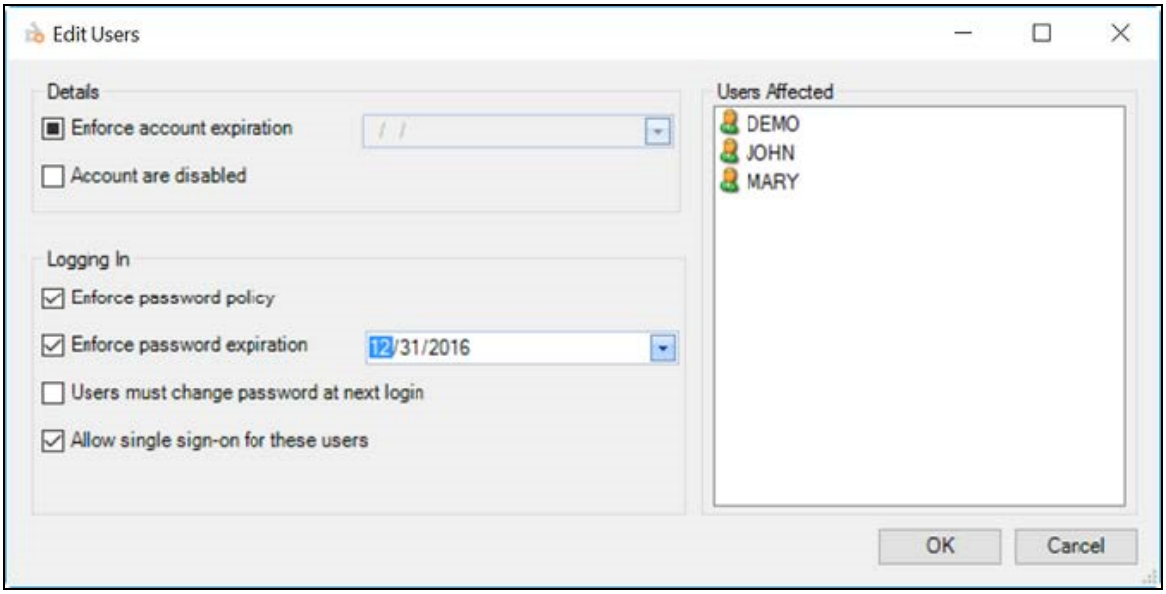
The users now are listed under the Finance Group:



Change The Properties Of Multiple Users For Standard Version

You can edit the user properties for multiple Standard users at once. To do this:

1. Log into the repository (if you are not logged in already).
2. Expand **Users and Groups** in the left-hand panel.
3. Select **Everyone** (or whichever group the users are currently part of).
4. Select multiple users in the right-hand panel using the *Shift* or *Control* key.
5. Right-click and select **Edit**. The **Edit Users** dialog is displayed:



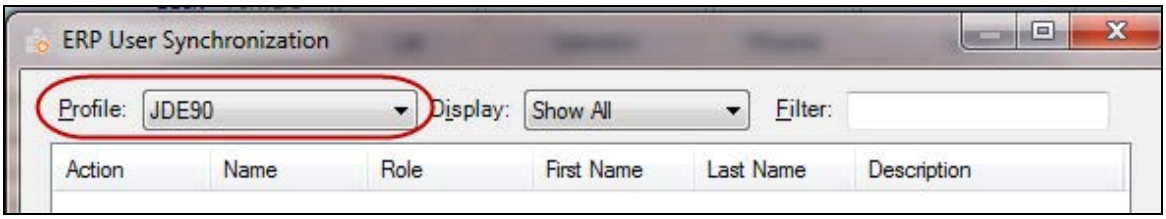
6. Make whichever change is needed within the dialog and click **OK**.

Import And Synchronize Users

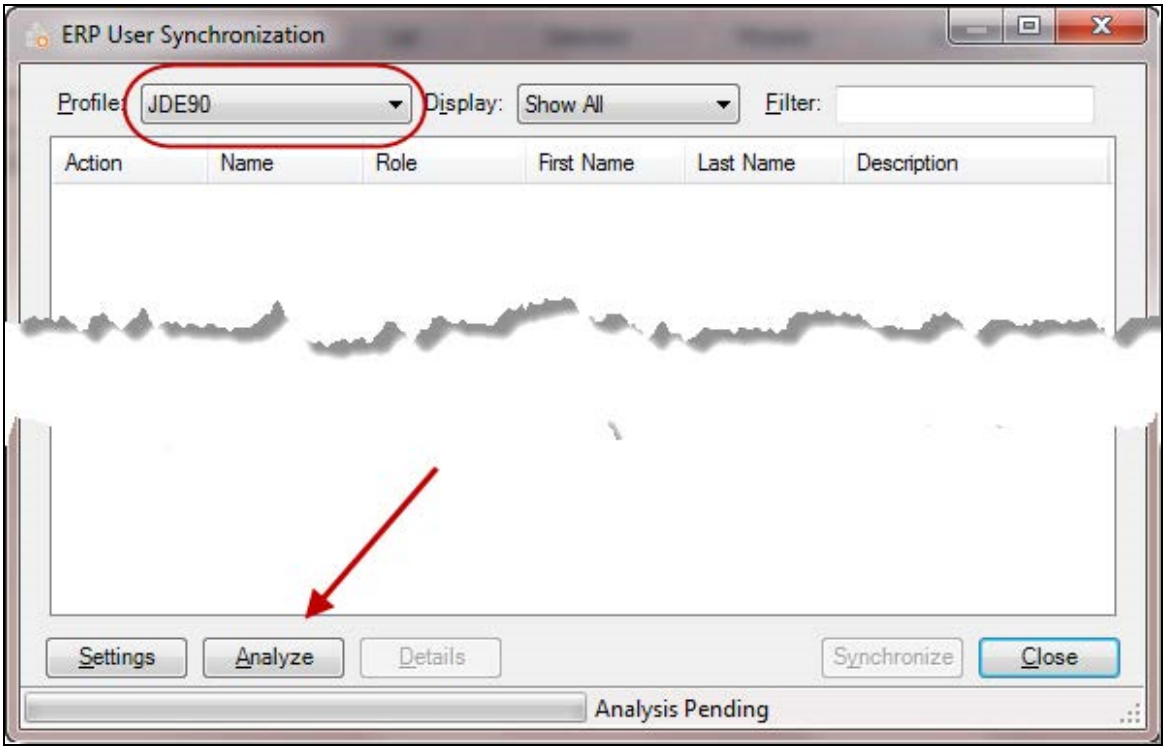
> **Note:** Starting from version 25.3, Platform users can use the **Platform User Sync** option to add non-ERP users directly from the Platform to the repository.

After creating Connections and Profiles, you can import and synchronize user names and information from your Enterprise Resource Planning (ERP) system with Hubble. The synchronization process allows you to check for users not currently stored in the repository and cross-reference user data such as Group or Role information. For Platform authentication users, you can also synchronize users directly from the Platform using the **Platform User Sync** tab, eliminating the need for these users to exist in the ERP system. Any subsequent amendments to Group/Role structures in the ERP system can be mirrored by running the Synchronize tool.

1. Log into your repository if you are not logged in already.
2. Expand the **Users and Groups** node in the left panel.
3. Highlight **Everyone**.
4. Either right-click and select **Synchronize** or click **Synchronize Users** on the Ribbon. (To view it on the Ribbon, you need to click the drop-down menu on the right side in order to see it.)
5. In the upper left-hand corner of the **ERP User Sync** dialog, choose the ERP profile from which you wish to synchronize users.



6. In the bottom left-hand corner of the dialog, click **Settings** to set all synchronization settings prior to bringing in the users. Set the options within **Synchronization Settings** as needed.
   i. **Repository Users** – select from all users or just those from the profile previously defined in the main ERP User Synchronization screen.
   ii. **Profiles** – select to group users under their ERP Role, ERP Group or a specific group within Hubble.
   iii. **Password** – select the default password for each user being synchronized in.
   iv. **Hide password in Details form** – hides the password in the **Details** dialog, accessed from the **ERP User Synchronization** screen (after selecting a specific user).
   v. **Expire passwords for new users** – automatically expire the original passwords for new users so they are forced to create new passwords when logging into Hubble for the first time.
   vi. **Disable new users** – automatically set new users' status to disabled until you enable them individually.
7. Back in the **ERP User Sync** dialog, click **Analyze** to list all users from the defined profile in the upper left corner:



i. Optionally, adjust the **Display** drop-down to show specific users:

i. **Show All** - show all users in your ERP system.

ii. **Show Changes** - show only those users whose ERP information has changed since last being synchronized with Hubble.

iii. **Show Additions** - show only new users who have been added to your ERP system since last synchronizing.

iv. **Show Removals** - show only those users who have been removed from your ERP system since last synchronizing.

v. **Show Updates** - show only those that will be updated when you next synchronize. It is important to show these users prior to synchronizing to verify which users will be updated. You want to uncheck any users that do not need updated because otherwise synchronizing them again changes their existing grouping in Hubble.

vi. **Show Selected** - show only those users who have been selected in the ERP User Synchronization dialog.

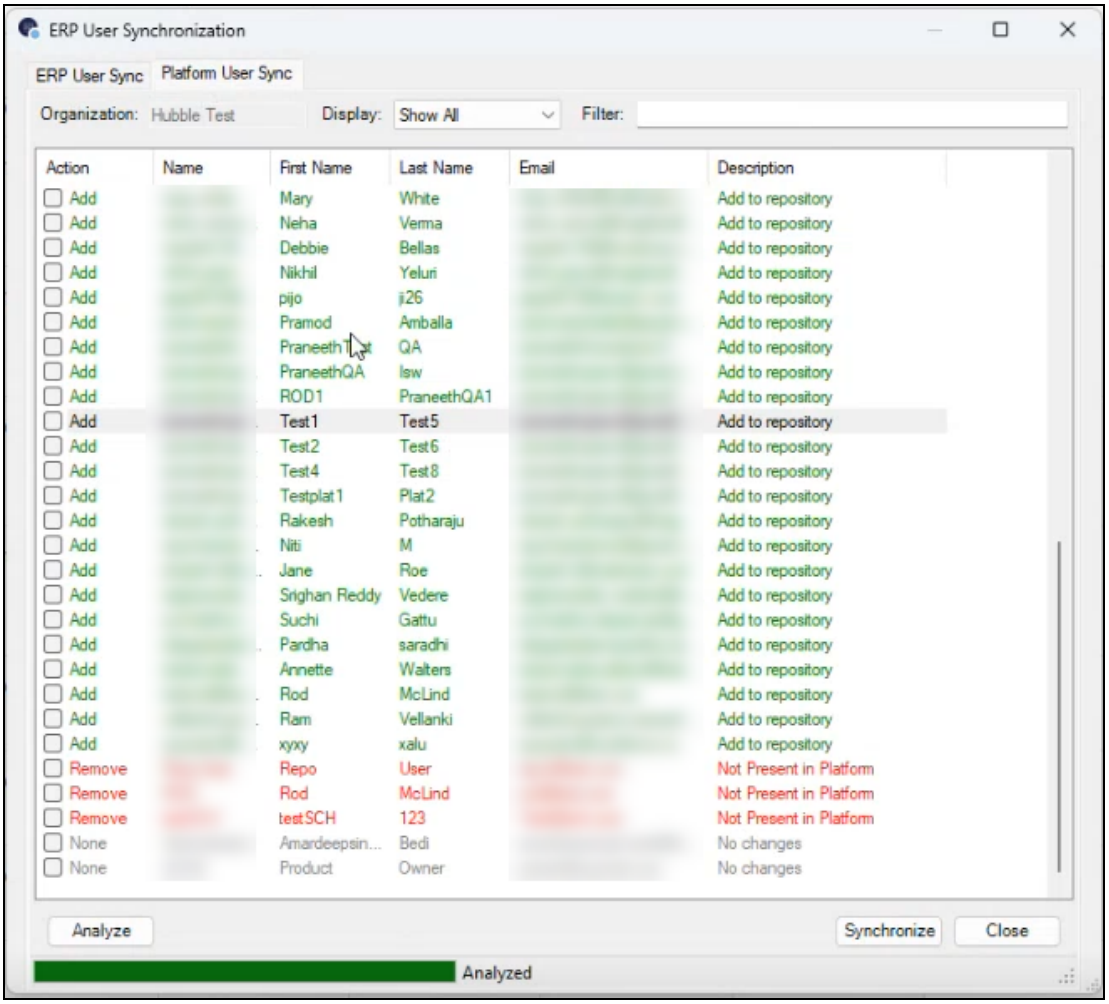
ii. To search for specific users, user the **Filter** in the upper right corner. This will display the specified user.

8. **For Platform Users Only:** If the user already exists in ERP:

- Ensure the Platform user email matches the ERP user email.
- Perform ERP synchronization in Hubble Administrator.

- The system links the ERP user with the Platform user.

The **Platform User Sync** tab enables you to add non-ERP users from the Platform to your repository.



- In the **User Synchronization** window, select the **Platform User Sync** tab.
- Select **Analyze** to retrieve users from the Platform.
- In the results list, select the check box for each user you want to add to the repository.
- Select **Synchronize** to add the selected users.

> **Note:** The synchronization process adds the Platform users to your repository with their existing Platform permissions and roles.

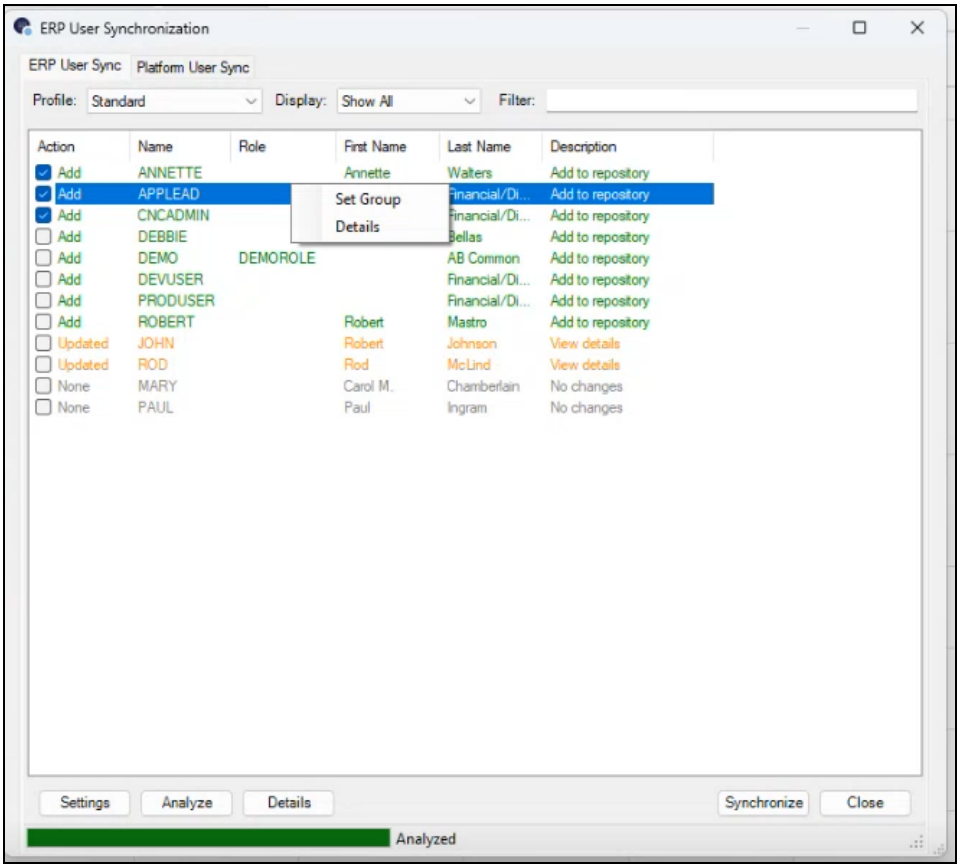
Platform Sync Actions:

- **Add**: Select users to add to repository.

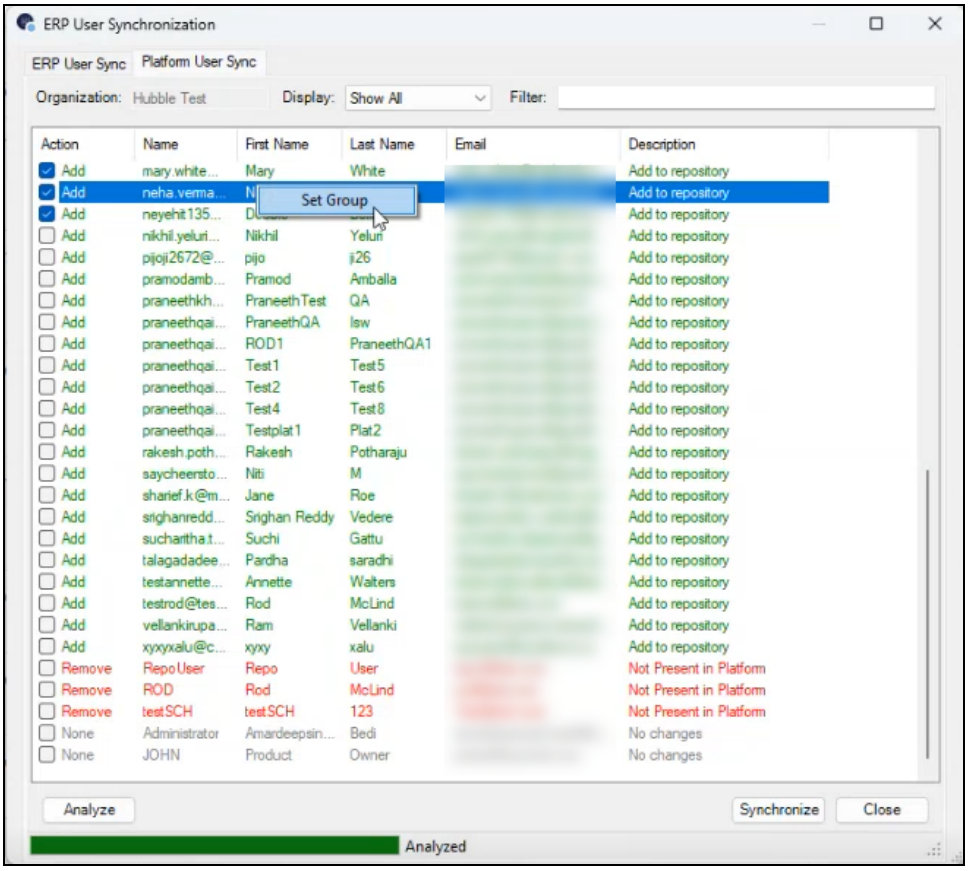
- **Update**: Select users to update the details in repository.
- **Remove**: Select users to remove from repository.
- **None**: No Platform changes detected.

9. Optionally, you can set the group where these users will be placed within the **Users and Groups** folder.
    i. Select all the appropriate users (you can use the Shift/Ctrl keys to select users), right-click and select Set Group:

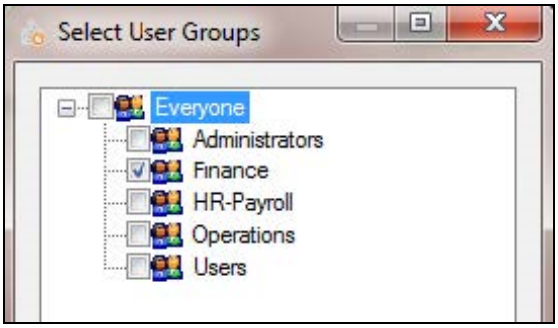
ERP User Sync



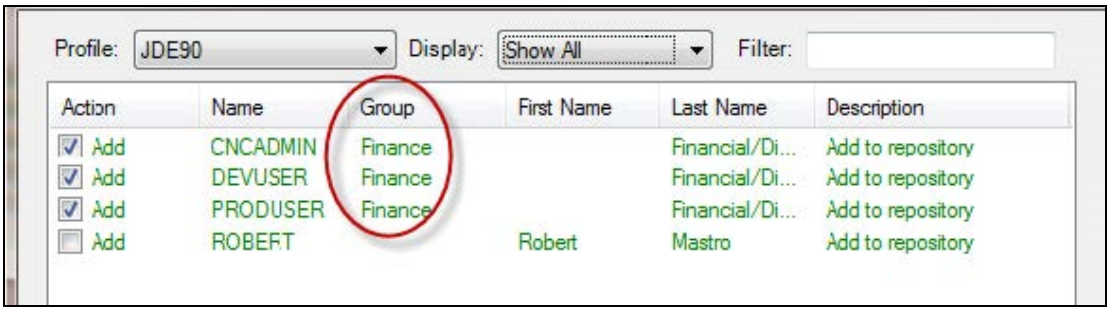
Platform User Sync



ii. Mark the group you wish to place them under and select **OK**:



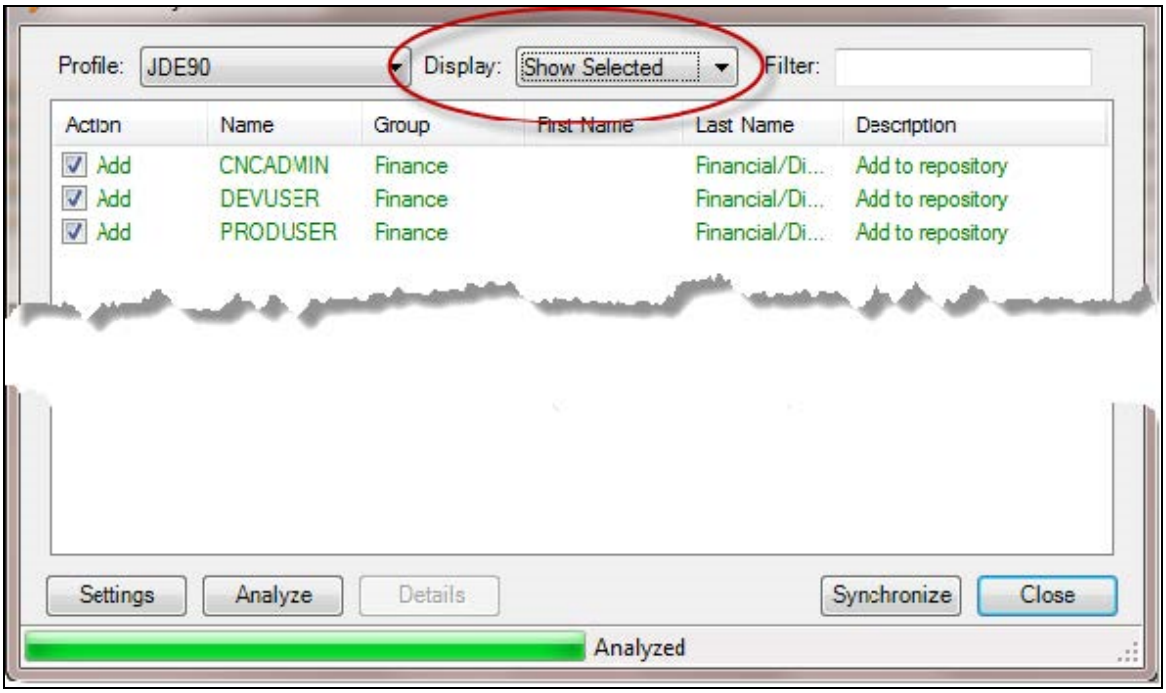
iii. You see their group has changed appropriately:



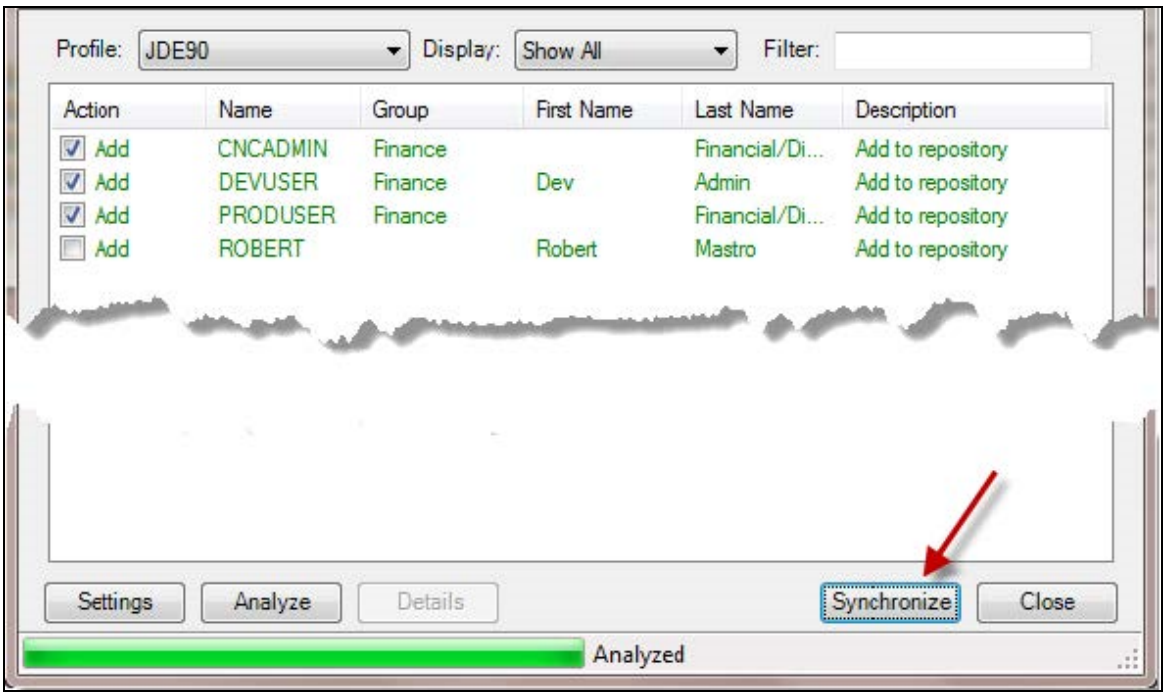
10. To see details about any one user, highlight the user's name and select Details to bring up the Details dialog. You can change settings in here as needed. Click **OK** when finished.

11. Use the Shift/Ctrl keys to select users. Check the boxes next to the users you are synchronizing.

12. Prior to synchronizing, change **Display** to **Show Selected** to confirm which users you are updating. (This way you know only the selected users are being added and users that had already been synchronized will not be synchronized again as they will lose all previously set groupings and permissions.) The users who will be synchronized have check marks next to their names. To prevent any users from being synchronized, uncheck the box next to their names.



13. Click **Synchronize** to synchronize users:



14. Assign licenses as needed.
15. The action status has changed to ‘Added’ or ‘Removed’.
16. Click **Close** to complete the process.

> **Note:** If you change a user name in your ERP system or in Hubble, the synchronization will be lost and the user is treated as a new addition.

Special Cases

ERP Unavailable Scenarios

Users with any status (active, expired, disabled) not present in ERP and not added to Platform:

- Status remains disabled.
- License are not assigned.

Expired User Activation

The Platform does not support user expiration. To activate expired users:

1. Update user details on Platform (such as first name and last name).
2. Run platform synchronization.

3. User status updates according to synchronization workflow.

> **Note:** Account expiration is not available in the user interface. Administrators cannot directly activate expired users without updating Platform details.

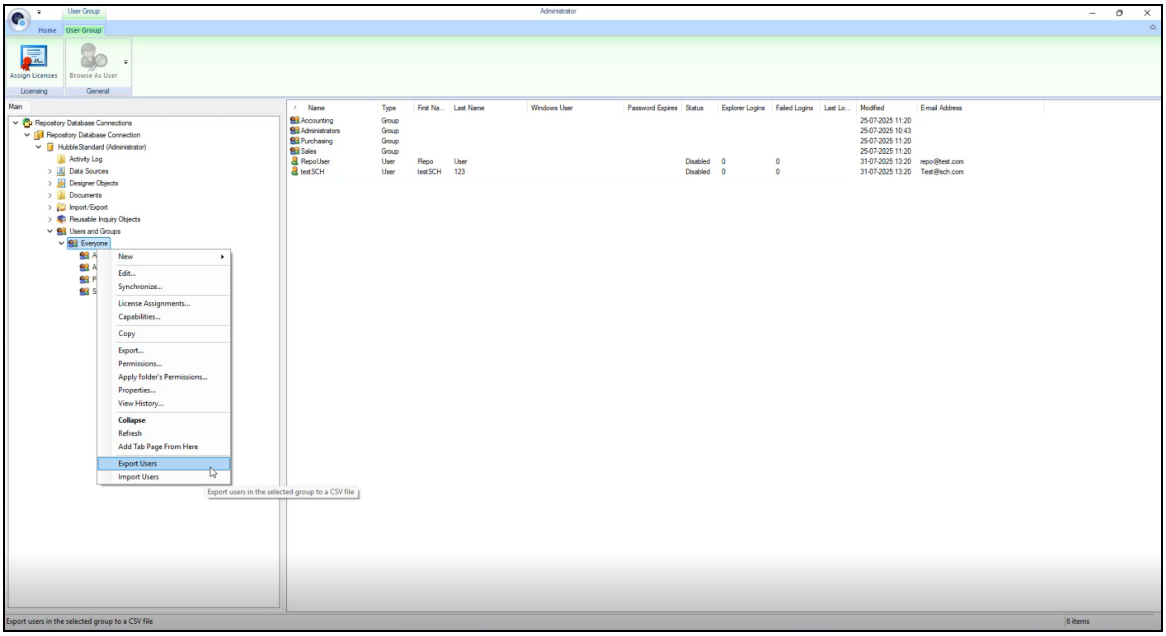
Export And Import Platform Users From Administrator Tool

Export Platform Users

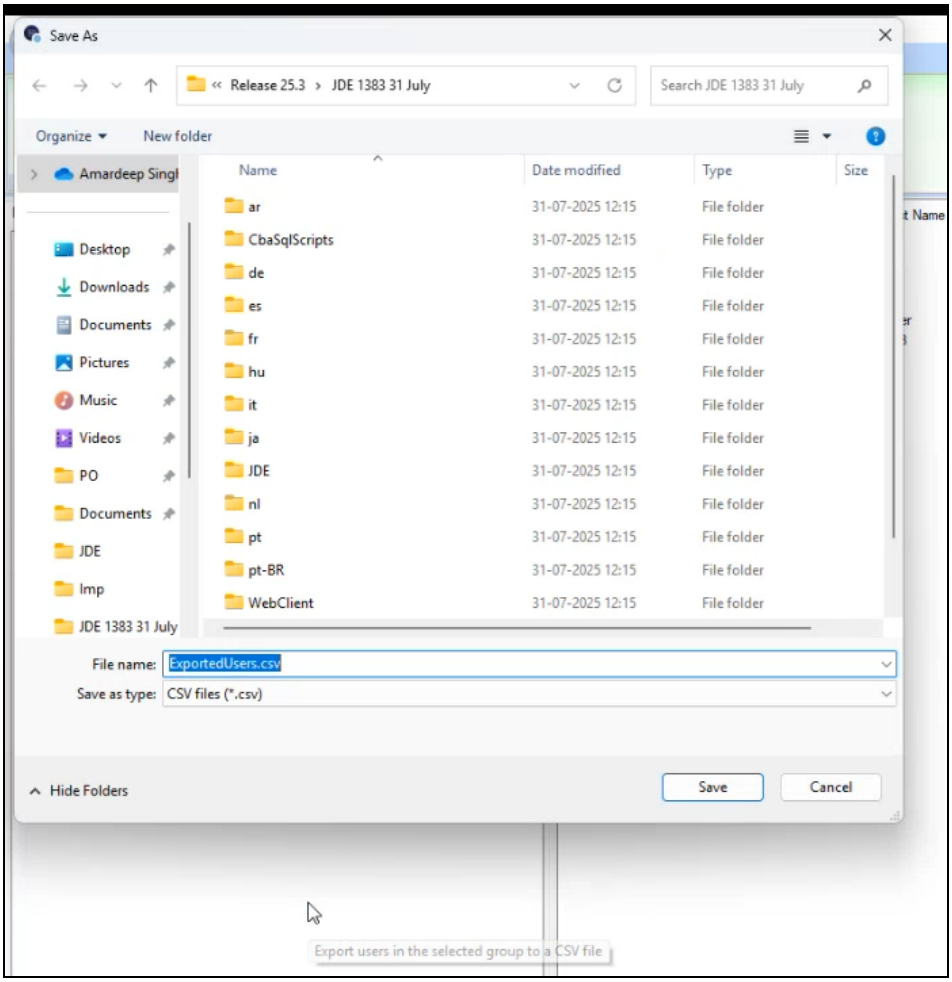
The **Export Users** feature enables you to export all platform repository users to a CSV file for reporting or backup purposes.

To export platform users:

1. In the Administrator tool, navigate to **Users and Groups.**
2. Right-click **Everyone** and select **Export Users**.



3. Select **CSV** as the export format:



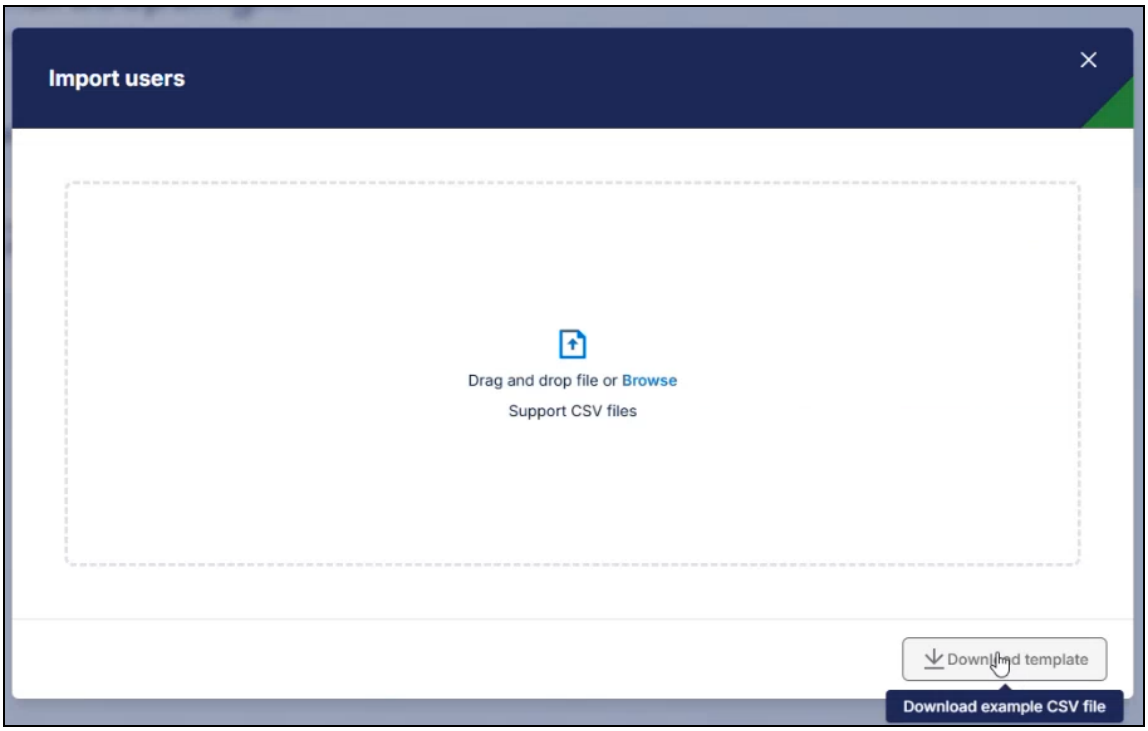
4. Choose the save location and file name.
5. Select **Save** to export the Platform user list.

Import Platform Users

The **Import Users** feature allows you to update Platform user email addresses by importing a modified CSV file.

Import Methods:

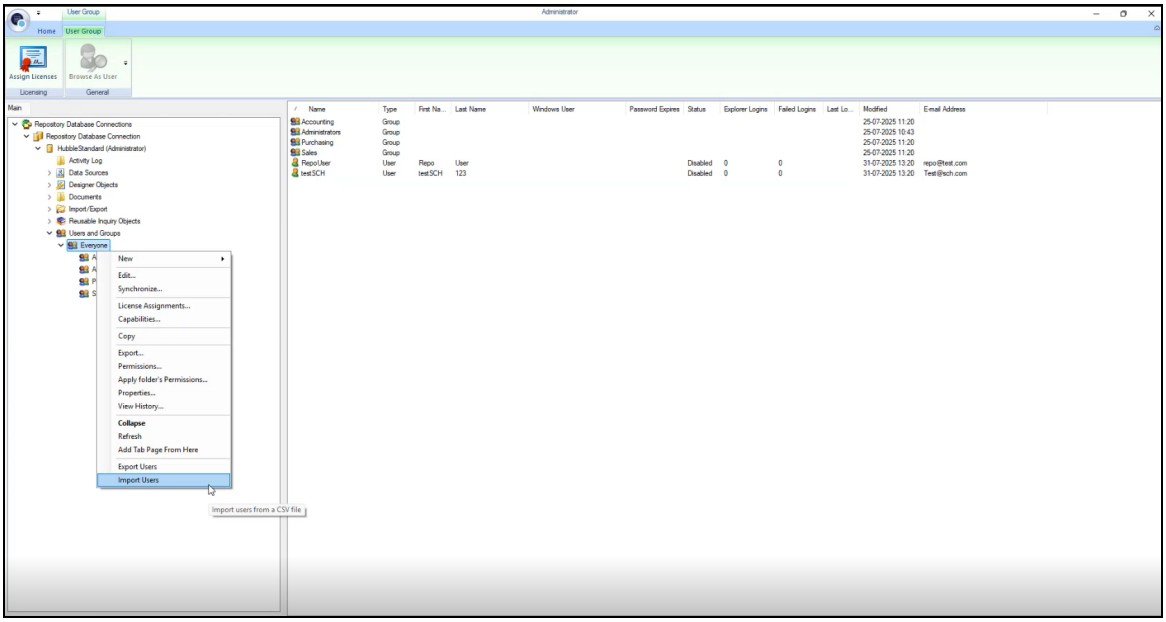
- **For new customers**: Import users directly using the Platform CSV template if you have their details



- **For existing customers**:
  - Export users from the Administrator tool (after installing the Platform version)
  - Add email addresses to the exported file
  - Import using the Platform CSV template

To import platform users:

1. In the Administrator tool, navigate to **Users and Groups**.
2. Right-click **Everyone** and select **Import Users**.



3. In the file selection dialog, browse to and select your CSV file.
4. Select **Open**.
5. The system validates the CSV file for:
   - Correct email format
   - Valid email addresses (using existing email validation rules)
6. If validation succeeds, the system updates user records with the new email addresses from the CSV file.

Important Notes

- Only email addresses can be modified through the import process
- Email validation follows the same rules as manual email entry
- All other user attributes remain unchanged during import
- Export your current user list before importing to maintain a backup

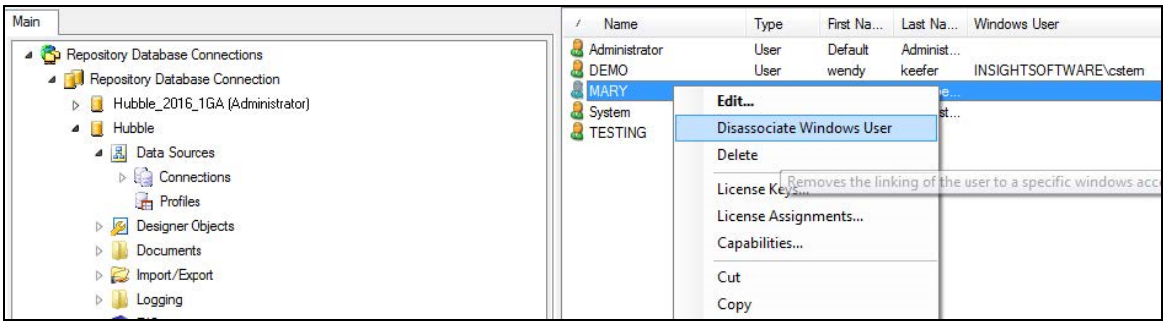
Disassociate A Hubble User From A Windows User

By default, Hubble users are linked to their Windows account. This error is saying that the Hubble username being used to login is associated with a different user account than that which was used to log into Windows.

This error specifically states the current user (current Windows user) and the expected user (expected Windows user), based on the Hubble username being used to login.

Your Hubble Administrator can help determine whether there is a need to disassociate the Windows user account from the Hubble username. This is done from within Administrator as described in the steps below.

1. Log into your repository if you are not logged in already.
2. Expand **Users and Groups** in the navigation tree on the left panel and select **Everyone**.
3. Expand the group that contains the user, highlight the specific user and then right-click and select **Disassociate Windows User**:



4. This user can now log into the Hubble application.

Password Policy

The Password Policy is used to define and manage password protection for Hubble users. A Password Policy can be set for any individual or group. When set at the group level, whether it is Everyone or another group, it will then apply to all users and sub-groups within that group. A password policy defined at a group level can be overridden by a policy set at a lower level. So if settings for an individual user are different than those in the group the user belongs to, the individual user's settings will take precedence.

The Password Policy options, such as minimum length, are enforced only when a password is being changed – they are not retroactive. The default settings in the Password Policy are minimal.

To access view and potentially change settings in the Password Policy:

1. Log into your repository if you are not logged in already.
2. Expand the **Users & Groups** node in the left panel of Administrator.
3. At the level you want to view/edit the Password Policy, such as **Everyone**, right-click and select **Password Policy**.
4. Use the checkboxes to set and define any additional password criteria:
   i. Inherit Policy
   ii. Disable user after failed login attempts
   iii. Restrict password re-use
   iv. Restrict number of times a password can be changed
   v. Set minimum password length
   vi. Enforce password strength

vii. Password should expire after x number of days
viii. Password can be the same as user name
ix. Password can be a dictionary word
x. Password is case-sensitive
xi. Password must contain numerics

5. Click **OK** to make the changes.

Password Strength

Passwords are converted into a rating number (typically between 0 and 100) as follows:

1. Rating = password length in characters * 5.
2. If password contains repeating characters, then rating = rating * 0.75. (An example of a password with repeating character is 'aaa4xup'. Repeating characters at the beginning or end of the password slightly reduces the rating.)
3. If password can be found in a dictionary, then rating = rating * 0.5. (A British dictionary is used currently. There is also an American dictionary available but it is not currently used.)
4. If password contains lower case letters, then rating = rating + lower case letters count, else rating = rating * 0.95.
5. If password contains upper case letters. then rating = rating + upper case letters count, else rating = rating * 0.95.
6. If password contains digits, then rating = rating + (digits count * 2), else rating = rating * 0.9.
7. If password contains punctuation (i.e. ?, ‘, “! characters), then rating = rating + (punctuation count * 2), else rating = rating * 0.9.
8. If password contains symbols (i.e. +,=,%,$,Aœ,\,/,@,#,^,&,| characters), then rating = rating + (symbol count * 2), else rating = rating * 0.9.

Strength bands:

- Weak passwords have a rating is less than or equal to 30.
- Medium passwords have a rating between 30 and 55.
- Strong passwords have a rating between 55 and 80.
- Best passwords have a rating greater than 80.

So, for example, if the password is “drill”, the score would be 5*5= 25 (5 characters * 5) and then 25 *.75 = 18.75. The *.75 is because of repeating characters. Total = 25 + 18.75 = 43.75 (Medium).

We reserve the right to update the algorithm at any time.

User Login And Password

The passwords for users of Hubble are not stored, so they do not need to be encrypted and they are not transmitted during login. Instead, we do what most secure applications do: we calculate a special value which is based on the chosen password, called a hash value, and store that. The hash function (SHA-2/256) is such that it is considered very difficult to deduce the password from the hash value, and each

password has a distinct hash value. When the user logs in, we calculate the hash value of the password they have entered and compare it to the stored hash value. If they are the same, the password is confirmed correct.

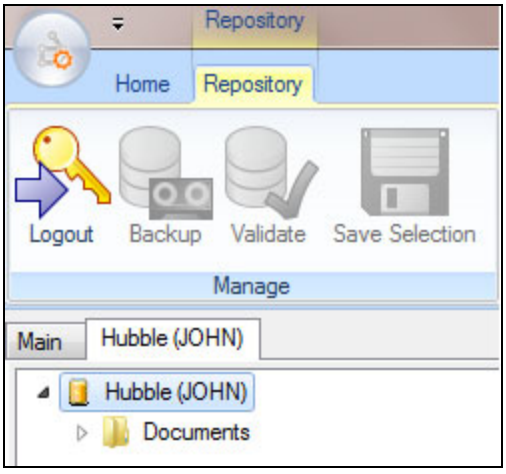
There is another consideration however, which is the login information used for the repository database connection and the ERP database connection. For database connections to the repository and to the ERP database, we store the connection string, which is encrypted using AES / Rijndael with a key size of 256 bits. The connection string typically includes the database username, password, server name, and schema name. Unlike a hash value, the encrypted text can be decrypted by Hubble. The symmetric key for this encryption is stored in source code and thus ends up embedded within the application binary. The encrypted repository connection string is stored in a file on disk on the client PC, in the Hubble installation folder (repositoryselection.xml). The encrypted ERP database connection string is stored in tables in the repository database, within a serialized object: a .NET object serialized to binary format, ZIP compressed, and then base-64 encoded.

Browse As A User

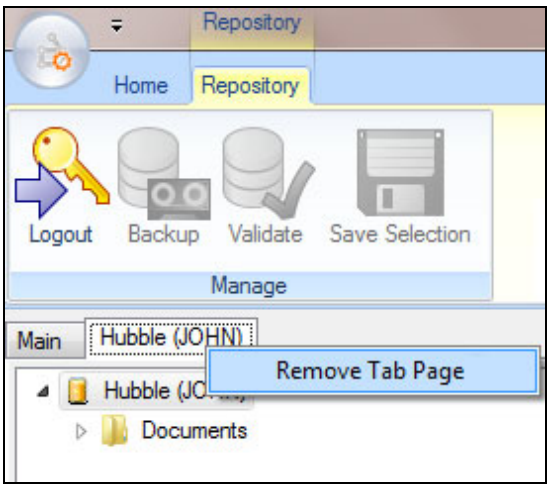
If you want to review what functions and visibility a user has within Administrator, you can use the Browse as User functionality to open a new tab in the left-hand panel of Administrator.

To browse the repository as a specific user:

1. Log into your repository if you are not logged in already.
2. Expand the **Users & Groups** node in the left panel of Administrator.
3. Select the user and either click the **Browse as User** button on the Ribbon or right-click and select **Browse as User**.
4. A new tab, named after the user, will open in the left-hand panel of Administrator. Within this tab, you can see what access this user has. In the example below, user John only has access to the **Documents** folder:



5. To close this tab, right-click and select **Remove Tab Page**:



Changes to the functionality or items that a user has access to in Administrator are done via Capabilities and Permissions.

Set Up Desktop Simplified Sign-On For Standard Users

Overview

Desktop Simplified Sign-On functionality enables Standard users to log into the product without being prompted for a username and password. Our products remember who the user is and automatically logs the user in.

Desktop Simplified Sign-On does not integrate with any outside directory access protocols such as LDAP or Active Directory. Hubble Desktop Simplified Sign-On functionality is self-contained and uses the user's Windows Domain Name as an association to the Hubble Standard user for logging into the product.

> **Note:** The **Desktop Simplified Sign-On** facility is distinct from the **Web Single Sign-On (SSO)** facility. The Web SSO facility is used to simplify access to content for Hubble Web users and to streamline user administration. Web SSO uses the SAML 2.0 standard and an existing SAML ID provider. Refer to the Configuring Single Sign-On with SAML topic in the *Hubble Initial Deployment Guide* for details.

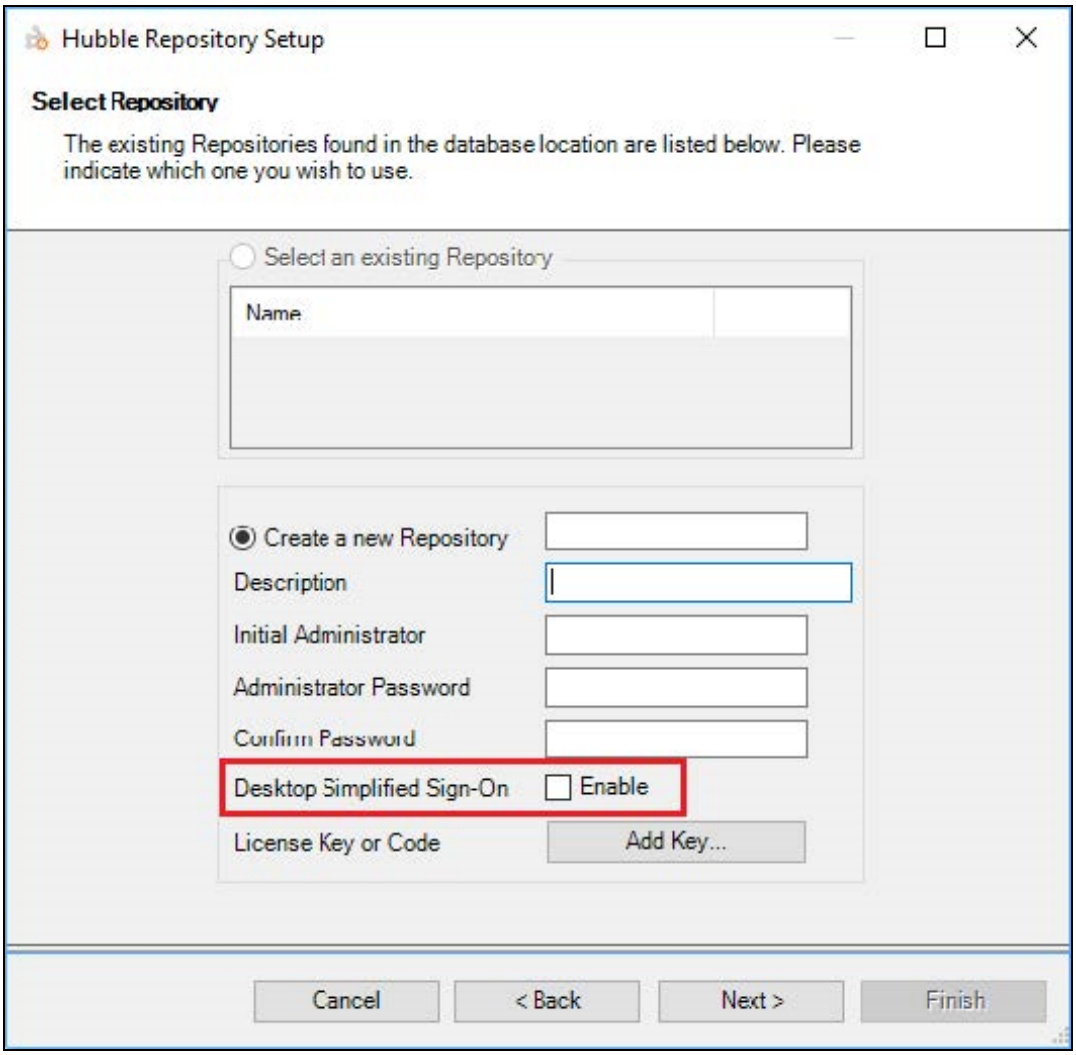
Desktop Simplified Sign-On in JD Edwards World environments - Desktop Simplified Sign-On only works for a JD Edwards World environment when World/AS400 interactive authentication is not required. This is determined in Administrator within the **Connection Settings** for the specific Profile being used. These **Connection Settings** allow you to select which security authentication mode you want your users to use as part of the login process.

The **Connection Settings** are in the **World Security Options** screen within the Profile wizard. Only option 4 (system credentials) can be used with Desktop Simplified Sign-On. Options 1, 2 and 3 are mutually exclusive with Desktop Simplified Sign-On because these options require Hubble to get a password from the user upon logging into their Hubble product.

Enable Desktop Simplified Sign-On

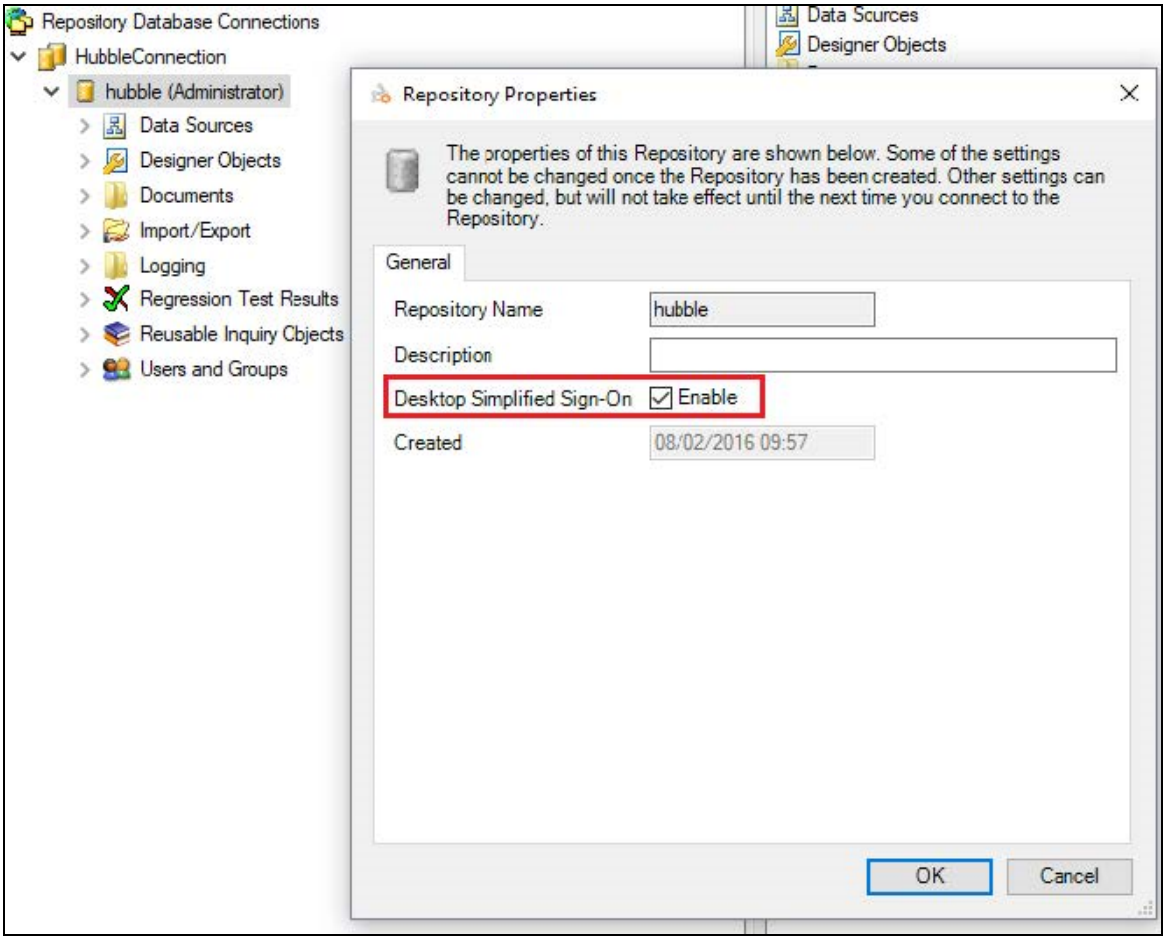
Desktop Simplified Sign-On must first be activated in Administrator at the Repository level. Each Hubble user must also be enabled (this is enabled by default). There are two ways you can activate Desktop Simplified Sign-On for your repository:

1. Use the **Install Setup Wizard** to create a new Repository and check the **Desktop Simplified Sign-On** checkbox as shown below:



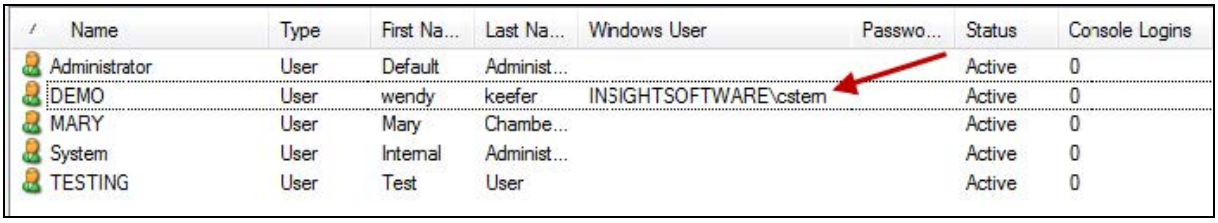
2. Edit your existing Repository. Right-click on your repository after logging into it, click **Edit** to open the **Repository Properties** dialog, and then check the **Desktop Simplified Sign-On** checkbox as

shown below:



Enabling Desktop Simplified Sign-On at the repository is all you need enable this feature. The first time you log into your Hubble product, you will be prompted to key in your username and password information. Once successfully logged in for the first time, you have now defined the association required for Desktop Simplified Sign-On to function. The user's Windows Domain Name has been associated to their Hubble Username. Your administrator can see this association using the

Administrator application. Below you can see that the User DEMO is now associated to the Windows Domain Name of INSIGHTSOFTWARE\cstern:



Name	Type	First Na...	Last Na...	Windows User	Passwo...	Status	Console Logins
Administrator	User	Default	Administ...			Active	0
DEMO	User	wendy	keefer	INSIGHTSOFTWARE\cstern		Active	0
MARY	User	Mary	Chambe...			Active	0
System	User	Internal	Administ...			Active	0
TESTING	User	Test	User			Active	0

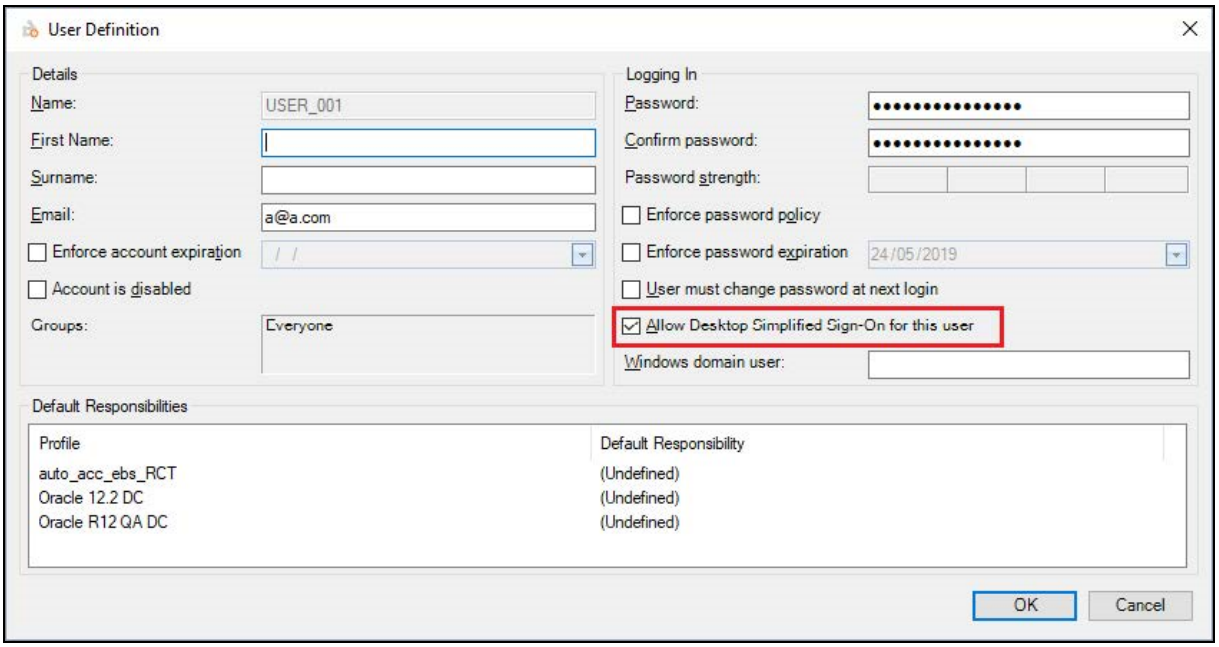
Now each subsequent login to the application will retain this association, thus automatically logging in the user. The user may still need to select a Profile and/or Responsibility to complete the login; however they are no longer challenged for their Username or Password. The user will still need to select their Profile and/or Responsibility in the login dialog.

Activate Desktop Simplified Sign-On At User Level For Standard Users

Desktop Simplified Sign-On is activated at the user level by default. All users are automatically enabled for Desktop Simplified Sign-On by default when:

- Creating new users
- Synchronizing in users from the ERP Profile
- Restoring users from a previous backup

In Administrator, you can see this by editing any user. The checkbox for **Allow Desktop Simplified Sign- On for this user** will be selected.



Desktop Simplified Sign-On And Password Policy

With Desktop Simplified Sign-On switched on, the Hubble passwords in the Object Repository are not needed and not asked for as long as Desktop Simplified Sign-On is operating for the user.

This means that if, for example, you have Hubble Password Policy set for a user's password to expire in 90 days, technically at 90 days the password in the repository is marked as expired. However this does not impact the user because the Hubble password in the repository is not being used. As long as Desktop Simplified Sign-On continues to operate, the user will never know that his/her password has expired.

If for some reason, at some point, Desktop Simplified Sign-On stops operating (switched off, or more than one Hubble account is associated with the same Windows domain account), then the application will ask the user for his/her username and password. If the password has expired, users must enter their old password and create a new one, following the same process as before Desktop Simplified Sign-On was implemented.

Manage Licenses And Assign Modules

Manage License Keys

> **Note:** The **Manage License Keys** functionality is available only for Standard users. Platform users have their licenses managed at the Platform level.

Access License Keys

There are several ways to access the License Keys dialog:

- Within a repository, select the Users and Groups node in the left panel and click the **Manage Keys** button on the Ribbon.
- Within a repository, select the **Users and Groups** node.
- Select **Everyone** (or the level at which you wish to view the license keys), right-click on this group or user and select **License Keys**.
- From within the **License Assignments** dialog, click the **Manage** button.

Within the **License Keys** dialog, you can:

- **Add** new license keys. (Use **Add** to add a brand new license key that is not replacing an existing one, e.g. when adding a license key for the first time or adding a trial license key that is separate from your main license key.)
- **Remove** old license keys.
- **Replace** a license key with another one. (Use **Replace** to replace a license key, e.g. an expired one or one from a previous version, with a new one. When you use this, your existing license assignments are retained and the new key validates that it can accommodate all of your current license assignments.)
- **Details** – view details of the selected key.

Replace A License Key

To use the Update Links functionality, follow the steps below:

1. In the **License Keys** dialog, select the key that you wish to replace.
2. Click **Replace**.
3. When the **Enter Replacement Key** dialog opens, copy and paste in the new license key (clicking **Paste** will paste in whatever was most recently copied).
4. Click **OK**.
5. A replaced license key cannot revoke any existing licenses or license assignments. Therefore, if an incompatible license key is used (one that has less licenses than those that have already been assigned), a message dialog opens to show you which Modules are affected.
6. Click **OK** to close the message.
7. Change the license assignments as needed in **License Assignments**.
8. You can now replace the license key.

Add A New License Key

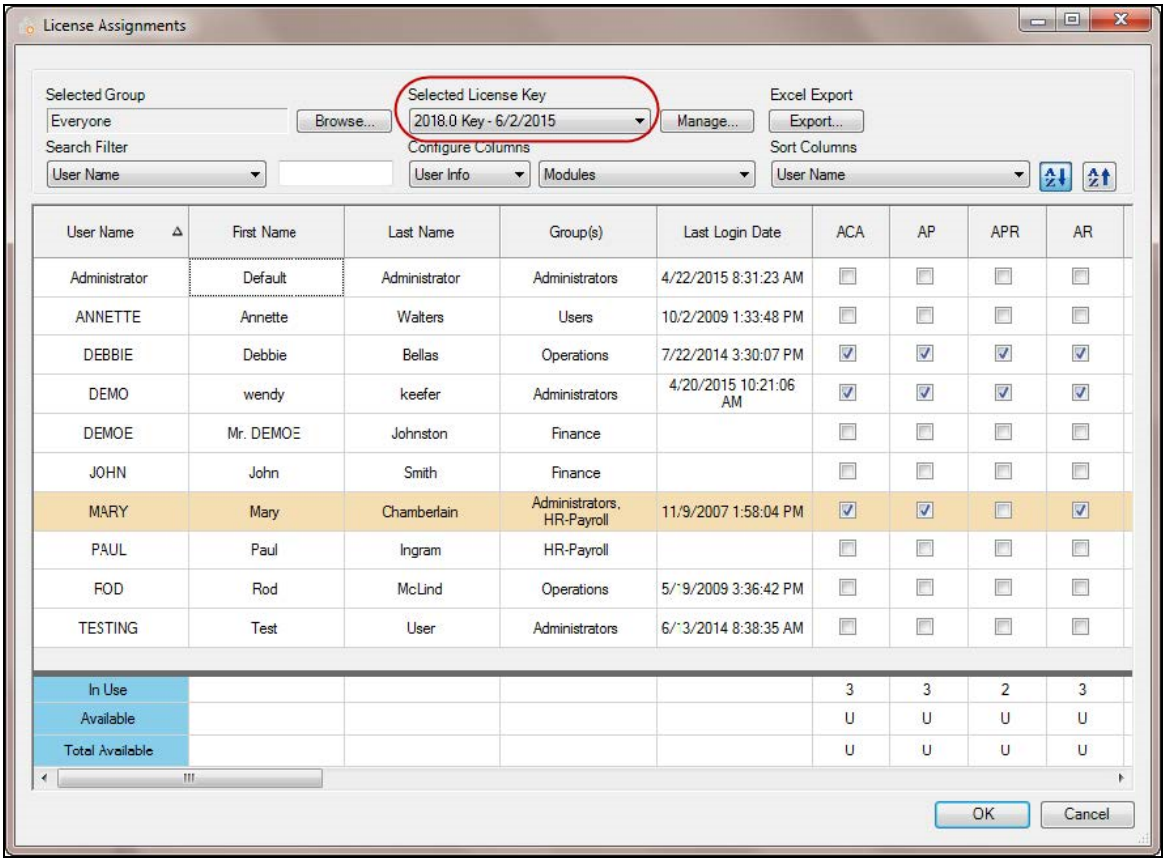
To add a new license keys, follow the steps below:

1. In the **License Keys** dialog, click **Add**.
2. When the **Add Replacement Key** dialog opens, copy and paste in the new license key (clicking **Paste** will paste in whatever was most recently copied.)
3. Click **OK**.

Assign Licenses To Users

Once you have applied a valid license key for Standard users or have logged in as a Platform user, and have users set up in Administrator, you can assign licenses to individual users.

1. Log into your repository if you are not logged in already.
2. Select **Users & Groups** from the left-hand panel of Administrator.
3. Select **Everyone** (or the level at which you wish to view the license keys), right-click on this group or user and either click the Assign Licenses button on the Ribbon or right-click and select **License Assignments**.
4. **For Standard Users Only:** Notice that the **Selected License Key** as displayed in the top middle of the dialog. You can change this as needed to select the license key for which you want to apply licenses.

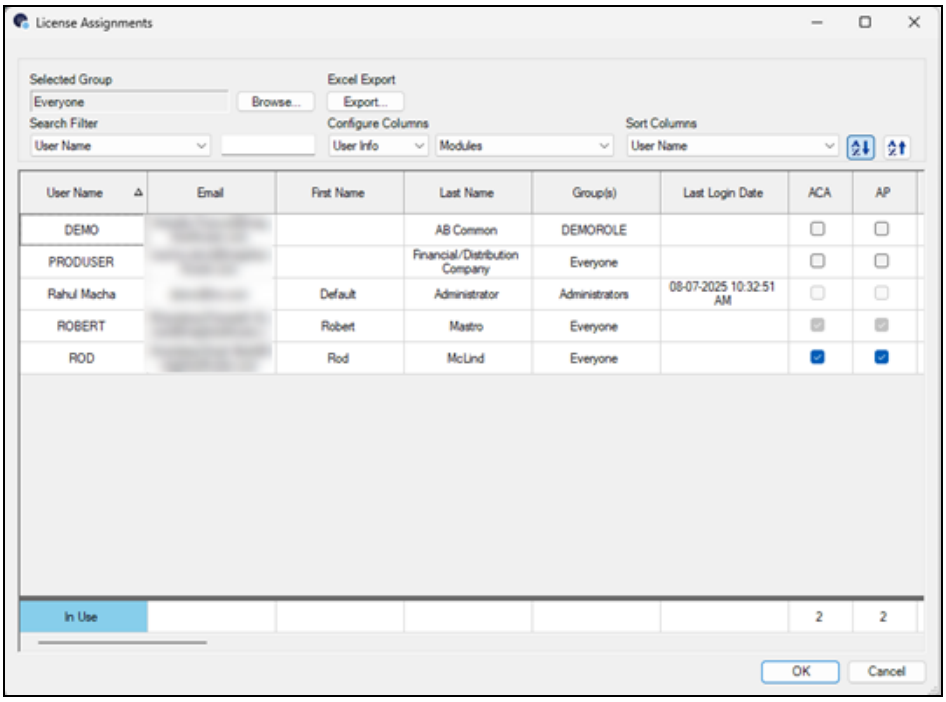


5. License Module information display:

   - **For Standard Users:** The Module information is summarized in the rows listed at the bottom of the table: **In Use**, **Available** and **Total Available**.

   - **For Platform Users:** The Module information is summarized in the **In Use** rows listed at the

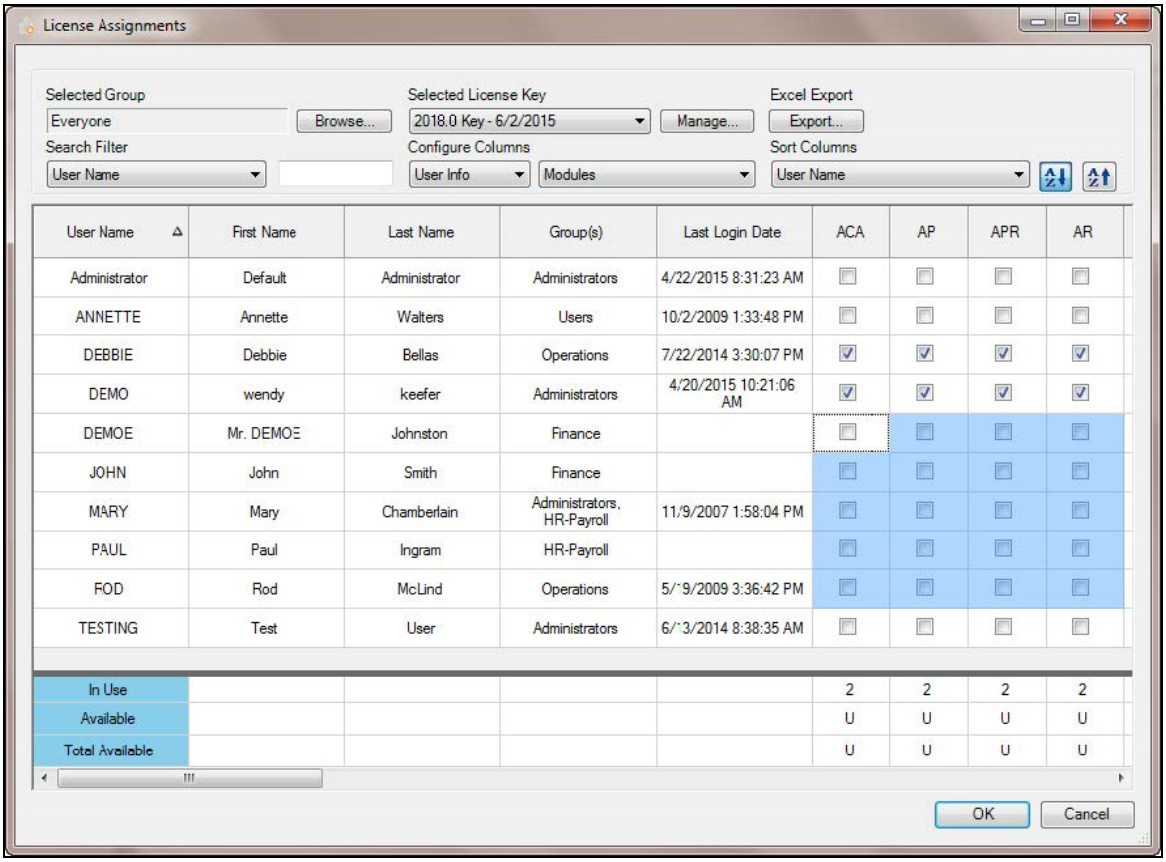
bottom of the table.



6. Assign Modules to users by checking the relevant box in the table, either individually or using multiple selection (click and hold on a cell to the left of the checkboxes and use the mouse to drag the selection across the Module cells that you want to select). The cells will be highlighted in blue, and you can then check or uncheck any cell within the selection to update all of the selected cells.

> **Important:** For Hubble Power users, you must assign the RPT (Reporting) license along with the other license(s) for the specific Modules for which they should have access.

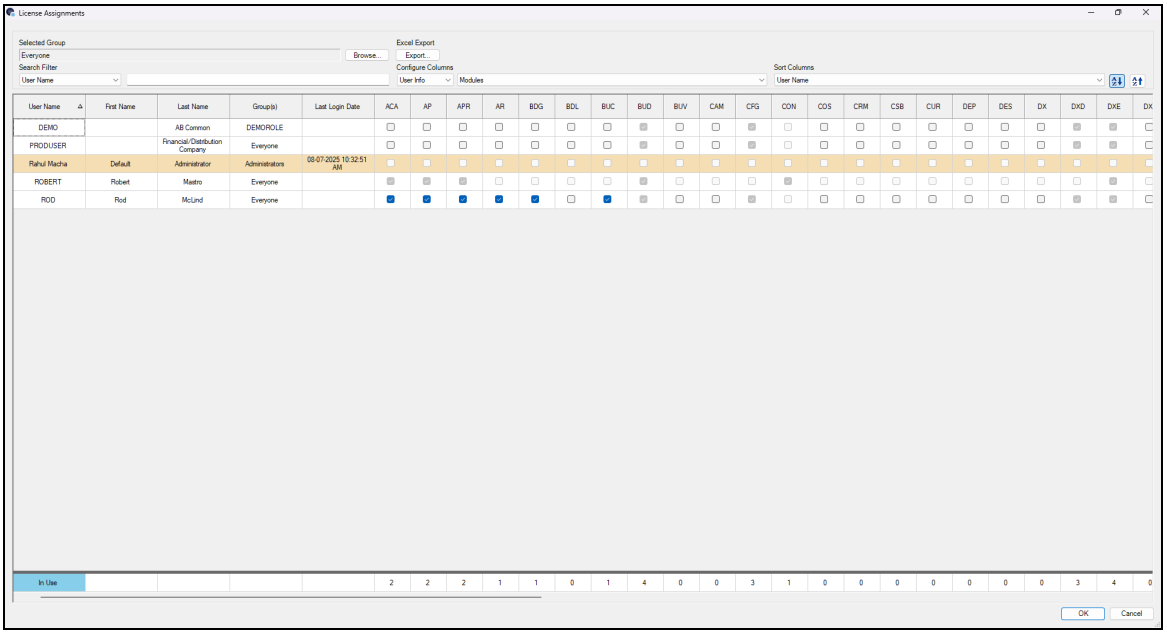
License Assignment for Standard Users



Assign Modules For Platform Users

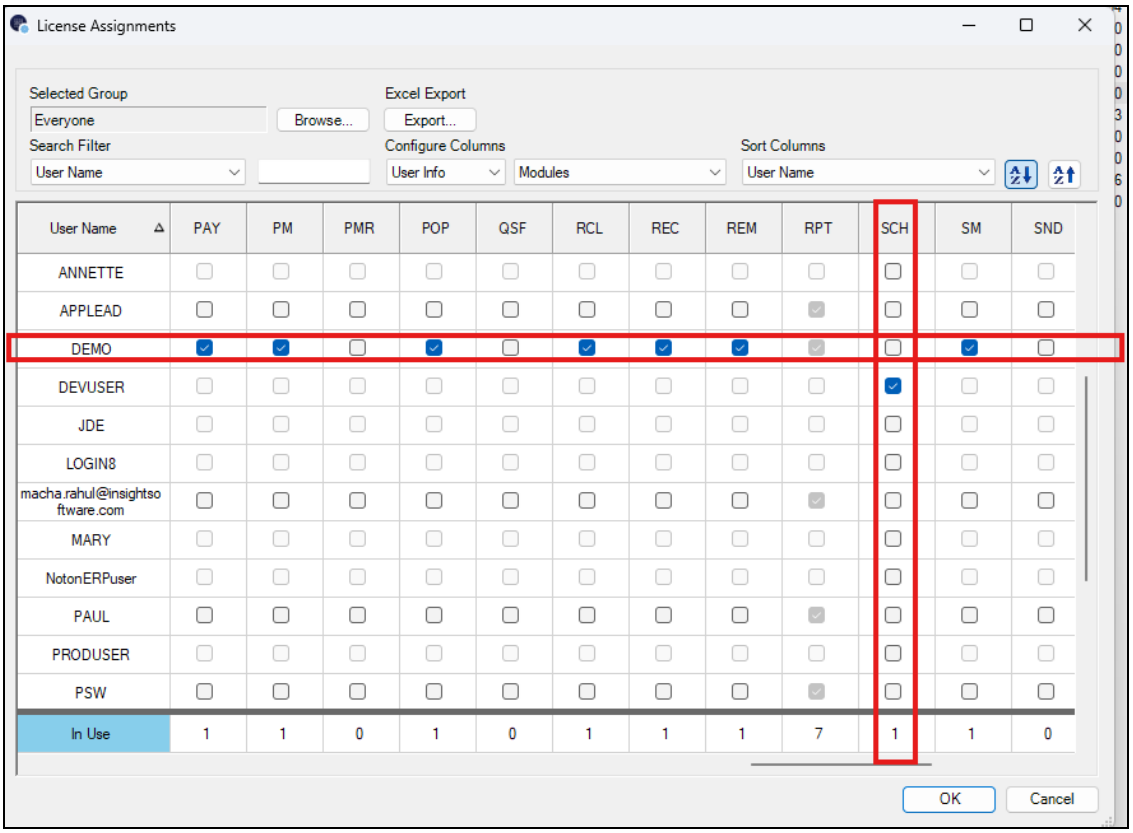
When assigning modules to Platform users, the process differs from Standard users due to pre-configured license types:

1. In Administrator, navigate to **Users & Groups**.
2. Right-click on user/group and select **License Assignments**.
3. The license assignment screen displays:



- Pre-checked modules based on platform license type (grayed out/disabled)
- Additional assignable modules (checkboxes enabled)
- **SCH**: Application-level module, assignable regardless of authentication type (checkbox

enabled)



4. Select additional modules as needed.
   - Designer and Power users can receive additional module assignments
   - Viewer users are restricted to their default modules only
5. Click **OK** to save assignments.

> **Note:** Platform users have base license types (Designer/Power/Viewer) that are controlled at the platform level and automatically include specific modules. Only additional modules can be assigned through the Administrator.

Additional Features

The License Assignment dialog includes the following features:

For Standard Users Only:

Manage: launch the **Manage Keys** dialog to add, remove, or replace license keys.

For Both Standard and Platform Users:

- **Export** - export to a Microsoft Excel Worksheet all displayed information in the **License Assignments** table. (You will be prompted to enter the name and location where the worksheet will be saved. When you review the file in Microsoft Excel, the check boxes appear as 'True' when checked and 'False' when unchecked.)

- **Search Filter** - filter on specific criteria by first selecting the search criteria using the drop-down menu and then entering in the search text in the field to the right of it.

- **Configure Columns** – select/deselect the user information to display as well as the Modules to display in the table.

- **Sort Columns** – select the column to sort by and then whether to sort in ascending or descending order.

Assign Capabilities

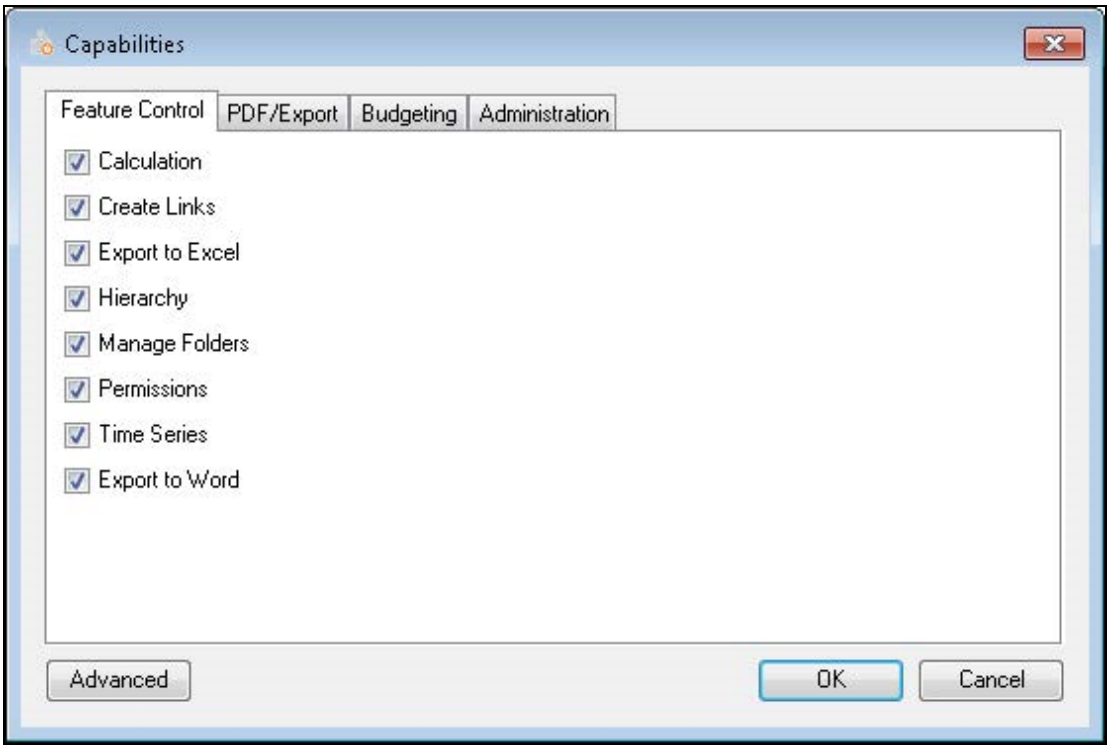
Capabilities Overview

Capabilities are used to manage users' access to functionality within Hubble such as being able to export data, build Hierarchies and Time Series, and other functional elements where you may wish to restrict capabilities to trained or authorized users. Capabilities are also used to assign limited functional rights within Administrator to non-administrators. They can be set at the individual user level or at the group level, whether it be Everyone or other groups.

To access and set **Capabilities**:

1. Log into your repository if you are not logged in already.
2. Select **Users & Groups** from the left-hand panel of Administrator. Expand as needed to view specific groups and/or individuals.
3. Right-click on the specific level (group or individual user) you wish to set Capabilities for and select **Capabilities**.
4. The **Capabilities** dialog opens with default settings, allowing users to manage the different features within Hubble:

i. Basic Capabilities are all those set within the main **Capabilities** dialog.



ii. Advanced Capabilities are accessed by clicking on the **Advanced** Button in the lower left corner of the **Capabilities** dialog.

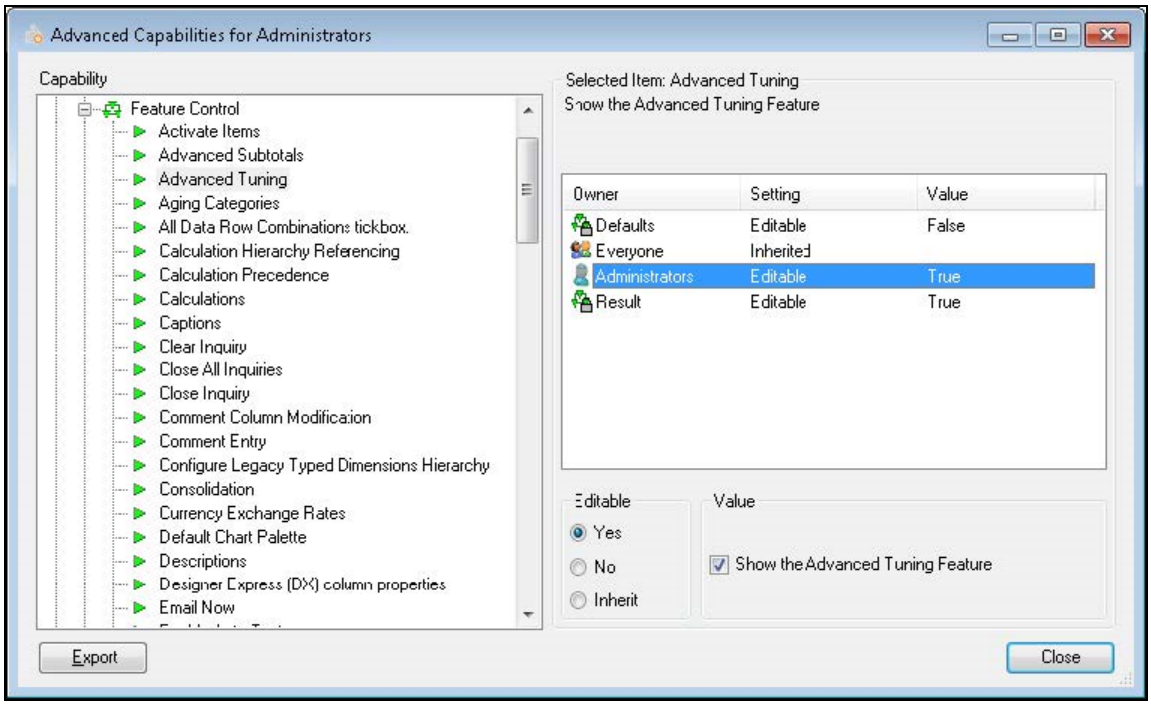
i. Using the tree structure in the left panel of the **Advanced Capabilities** dialog, navigate to and select the specific capability you wish to view/edit.

ii. In the upper right corner of the dialog, select the owner or level at which you wish to set the capability.

iii. The settings in the lower right corner of the dialog vary depending on the capability; set these accordingly. Inherit means that the settings are inherited from the group above. The **Everyone** level inherits the setting from **Defaults**.

iv. Click **Close** once the settings have been made.

For example, navigate to **Feature Control> Advanced Tuning Capability**, which is used for viewing the SQL statement within Hubble. In the Owner section, we are setting it at the **Everyone** level. **Select Editable = Yes** and activate the option to **Show the Advanced Tuning Feature**:



5. Click **OK** to save the settings.
6. Hubble must be restarted in order for changes to be made.

Basic Capabilities

Basic Capabilities are all those set within the main **Capabilities** dialog:

1. **Feature Control** tab – activate/deactivate any of the listed features for the selected user(s), e.g:
    i. **Calculations**
    ii. **Create Links**
    iii. **Export to Excel**
    iv. **Hierarchy**
    v. **Manage Folders**
    vi. **Permissions**
    vii. **Time Series**
    viii. **Export to Word**

2. **PDF/Export** tab – these are the default settings for all inquiries, however can be overridden within individual inquiries:
    i. **PDF Output Location** – the default location for printing and exporting, initially this is %UserDocuments% (this is the logged-in user's My Documents folder).

    i. In recent versions, the location defined here populates in the Export Location field within individual inquiries if the location is blank. (Previously it did not populate but was still used as the default location for printing and exporting.)

ii. Note that %UserDocuments% is the default location for a brand new repository in version 2012.2 and above. If you have an upgraded repository from a previous release and the Print Output Location has been overridden at the Everyone level, that override value remains as the Print Output Location in Administrator. If it was not overridden in the previous release, the new Print Output Location displays as shown above.

iii. For clients who have Hubble installed on a terminal server, it can be changed to be a generic mapped drive that users can change in order to save on their own workstation.

ii. **Reports – Logo Image Location** – the default location for logo images that can be included in PDF outputs, initially this is the installed directory of Hubble.

iii. **Reports – Display Confidential Footnote** – set whether the confidential footnote displays on PDF outputs as well as the text of this footnote.

iv. **Display Repository Location** - set whether the confidential footnote displays on PDF outputs.

v. **Display Profile** – set whether to display the data profile being used on PDF outputs.

3. **Budgeting tab** – set whether to grant specific Budgeting permissions:
   i. **Administrator Permission**
   ii. **Management Permission**
   iii. **Participation**

4. **Administration tab** - grant specific capabilities within Administrator to specific users/groups:
   i. **Features**:

i. **Data Sources** – Allows access to view the connections and profiles (requires additional permissions to edit).

ii. **Reusable Inquiry Objects** – Allows access to RIO.

iii. **Documents** – This should be granted by default for a user's own folder (requires additional permissions if more folders should be included).

iv. **Users and Groups** – Allows access to view **Users and Groups** (requires additional permissions to update or create users/groups).

v. **Import/Export** – Allows access to Export to file but used in conjunction with the Repository Import and Export options, the user will be able to use all functionality.

vi. **Logging** – Allows access to the Logging folder (requires additional permissions to the specific log stream to use the Logging Functionality).

vii. **Module Security** – Allows access to set Module Security (requires read and update permission to the individual profile as well).

viii. **Application Objects** – Allows access to the Designer Objects Folder.

ii. **Repository**:

i. **Backup** – Allows access to back up the Object Repository.

ii. **Restore** – Allows access to restore the Object Repository.

iii. **Validate** – Allows access to validate the Object Repository (this function checks the repository for errors and attempts to fix them).

iv. **Edit** – Allows access to edit the Object Repository.

v. **Delete** – Allows access to delete the Object Repository.

vi. **Import** – Allows access to import in Import/Export.

vii. **Export** – Allows access to export in Import/Export.

iii. **Users and Groups**:

i. **User Licenses** – Grants access to User Licenses. Needs to be used to conjunction with Users and Groups (Features).

ii. **Manage License Keys** – (Applicable for Standard users only) Grants access to Manage License Keys. Needs to be used to conjunction with Users and Groups (Features).

iii. **Synchronize Users** – Grants access to Synchronize Users. Needs to be used to conjunction with Users and Groups (Features).

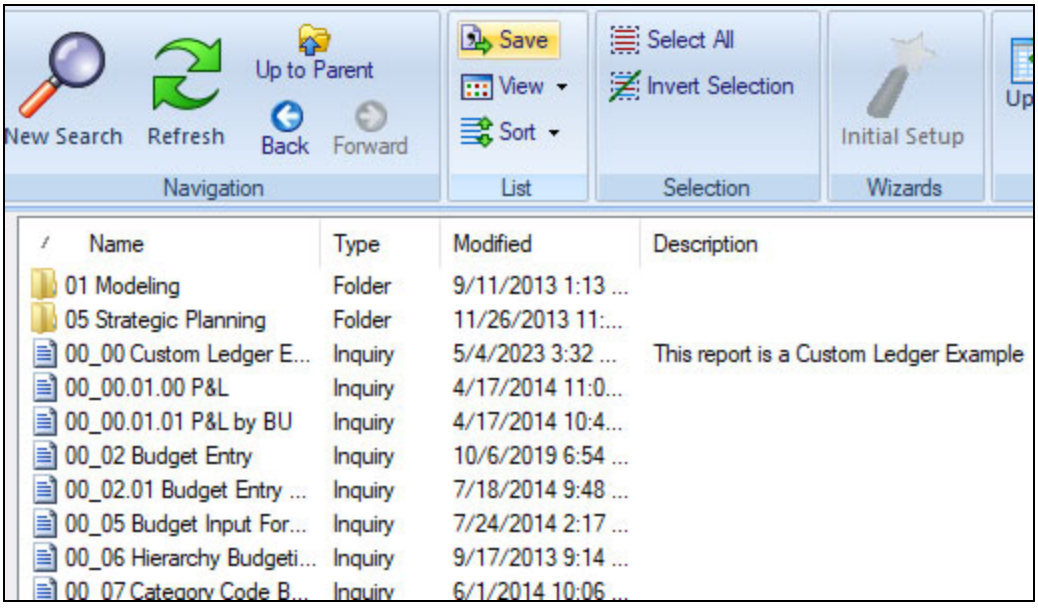
iv. **Basic Capabilities** – Allows access to Basic Capabilities.

v. **Advanced Capabilities** - Allows access to Advanced Capabilities.

Save Folder Data To A .CSV File

The list of folders and files displayed in right-hand panel of the main window can be save to a .csv spreadsheet compatible (comma separated) file.

To export a .csv file, ensure that the required data is displayed in the right-hand panel, and click **Save** on the **Home** menu.



You will then be prompted to enter a name and specify a location for the file.

The .csv file will contain data from each of the columns currently displayed in the right-hand panel. To add columns to the right-hand panel of the dialog, right-click on the headings and select the attribute from the menu that is then displayed.

A .csv file can also be exported for a specific set of data via the Search facility (see below).

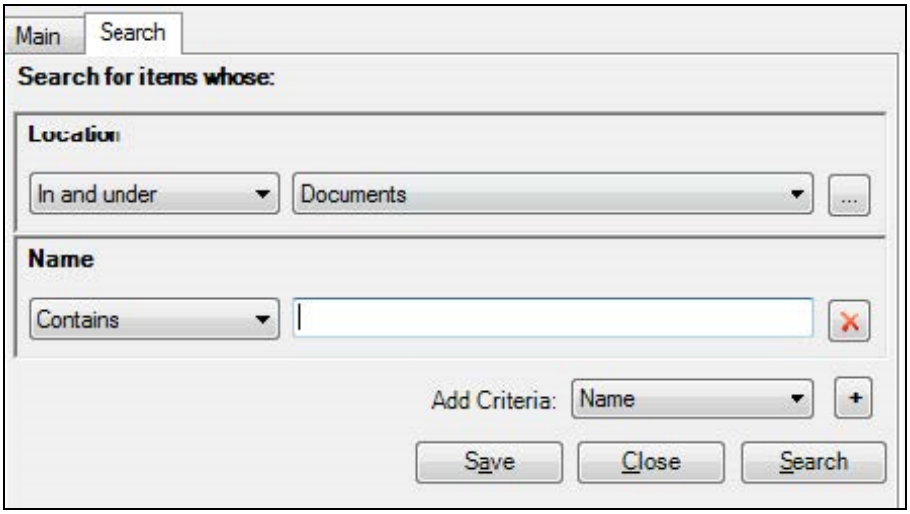
Search

Overview

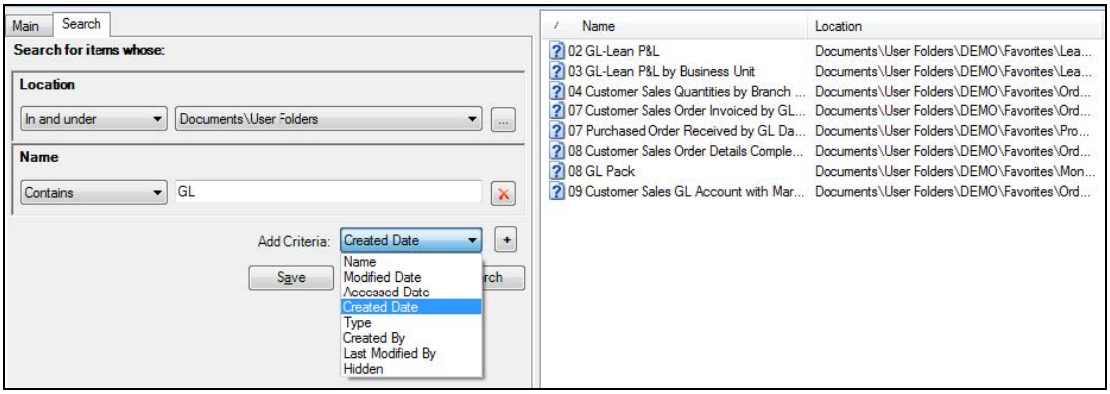
In Administrator, you can search for folders, templates and inquiries. This is particularly useful when items have been misplaced or incorrectly saved. You can also use the Search functionality to perform functions such as save, rename, delete, and export items, as well as create a spreadsheet with all results returned from the search.

To use the search functionality:

1. At the level you wish to search (such as everything under the 'Documents' folder), highlight that folder.
2. Either right-click and select **Search** or click the **New Search** button in the Ribbon.
3. This will open a new tab in the left-hand panel of Administrator called **Search**. Within the search panel you can define the search criteria that you wish to use by selecting the value from the **Add Criteria** drop-down and clicking on the + (add) button:

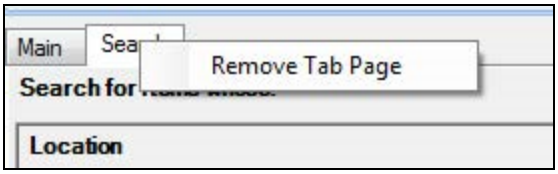


4. You can remove criteria from a search by clicking on the **X** (delete) button to the right of the defined field.
    i. You can also add the same criteria multiple times in order to search for more than one value. This approach will reduce the result set of a search, only showing the results where ALL criteria and values were met.
    ii. When you have defined your criteria, click the **Search** button. The results of your search are displayed in the right-hand panel of the **Search** dialog.



iii. To save a search for reuse, click **Save**. Use the **File Save** dialog to name and locate where you want to place the search.

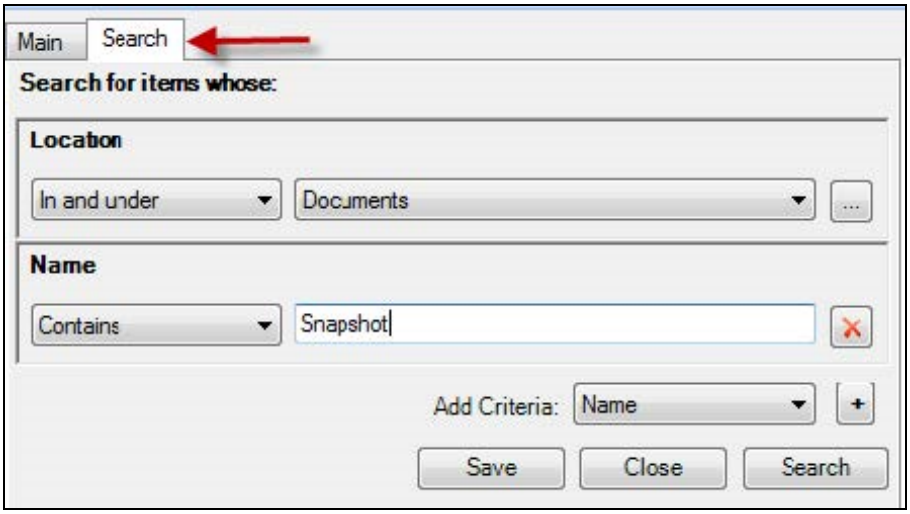
iv. To close the Search Panel, click **Close**. Alternatively, right-click on the tab header, and select **Remove Tab Page**:



Open A Saved Search

In order to open an existing search that you have saved in Administrator:

1. Navigate to the saved search within the **Documents** folder on the left-hand panel of Administrator. (If the file is not showing, you may need to click the **Refresh** button.)
2. In the right-hand panel, right-click on your saved search and then select **Open**.
3. The search will open a new **Search** tab:

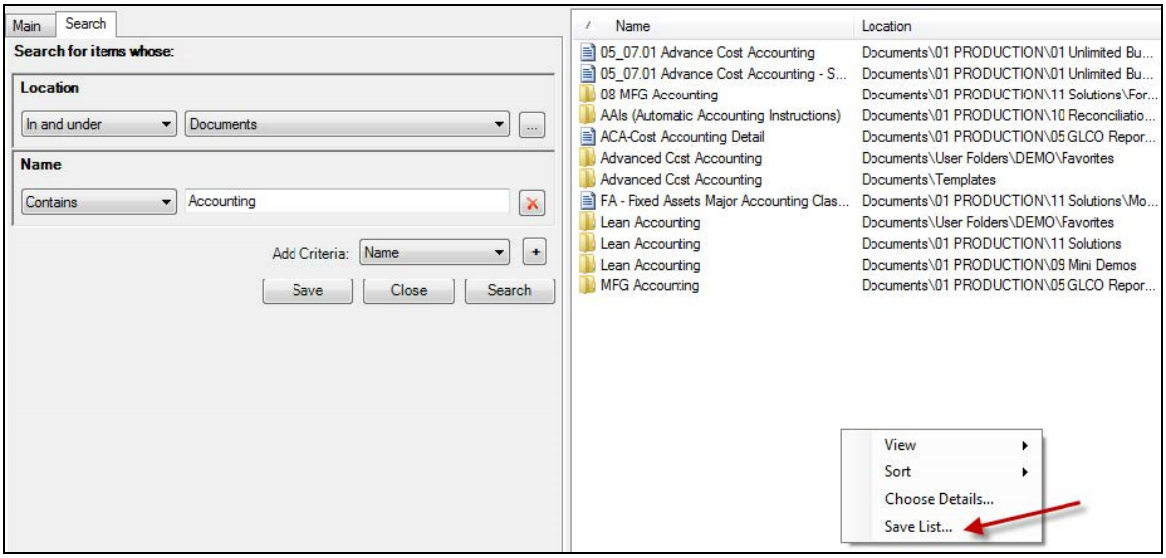


4. You can now use the Search functionality as you normally would.

Export Search Results To Microsoft Excel

You can export any results within the right-hand panel to a .csv spreadsheet compatible file from within Administrator, allowing you enhanced management and maintenance of the repository.

1. Log into the repository if you are not logged in already.
2. Expand the nodes in the tree structure in the left panel as needed in order to view the desired results in the right panel.
3. Once you can view the results you wish to export, right-click within the right-hand panel.
4. Select **Save List**. You can then name, save and open the results within any spreadsheet application.



5. The **File Save** dialog allows you to name and locate where you want to save the results. Upon clicking **Save**, the file will automatically launch within Microsoft Excel (if installed).

Configure Permissions

Overview

While Permissions are used in Hubble to manage which users can do what with inquiries and folders, in Administrator they are also used for any saved objects such as Connections, Profiles, documents, folders and Reusable Inquiry Objects. You can assign Permissions at the individual or group level.

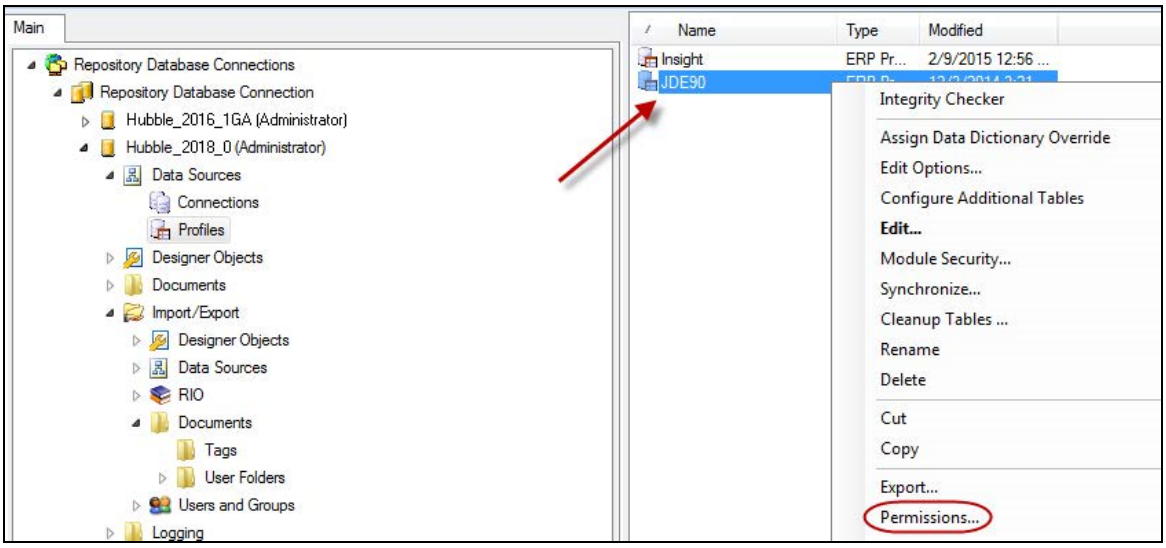
When new Data Sources (Connections and Profiles) are created in Administrator, the Administrator must be sure to grant Read Permissions to the users who need to use those Connections and Profiles when using Hubble. By default, all users other than those in the Administrators Group under **Users and Groups** are *denied* all Permissions to the Data Sources.

When a new folder or document is created, the user who created it is automatically granted all Permissions for that folder or document. Permissions are retained by objects that are renamed or moved, and are deleted when the object is deleted.

Any changes to Permissions made within Administrator will take effect immediately.

To view and potentially edit the Permissions on an object in Administrator:

1. Log into your repository if you are not logged in already.
2. Navigate to the object you wish to view/edit Permissions on.
3. Either right-click on the object and select **Permissions** or highlight the object and select **Permissions** on the Ribbon.
4. This launches the **Permissions** dialog, where you can set Permissions as desired for a user or group of users.

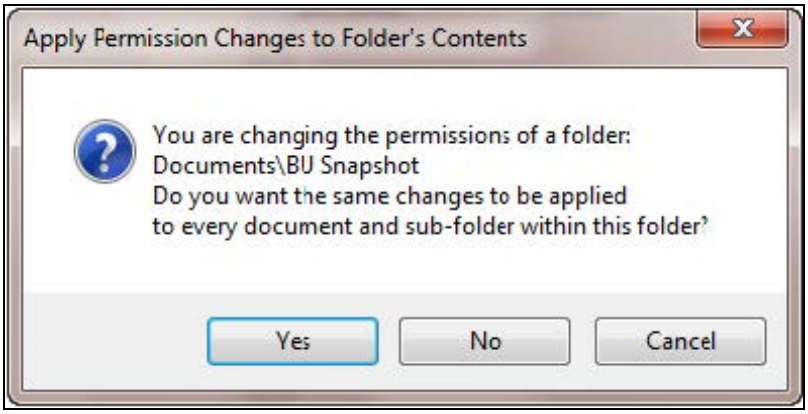


Administrator Permissions

Users who are members of the **Administrators Group** under **Users and Groups** are not subject to permissions and therefore have access and visibility to all stored objects.

Applying Permissions To The Other Items In A Folder

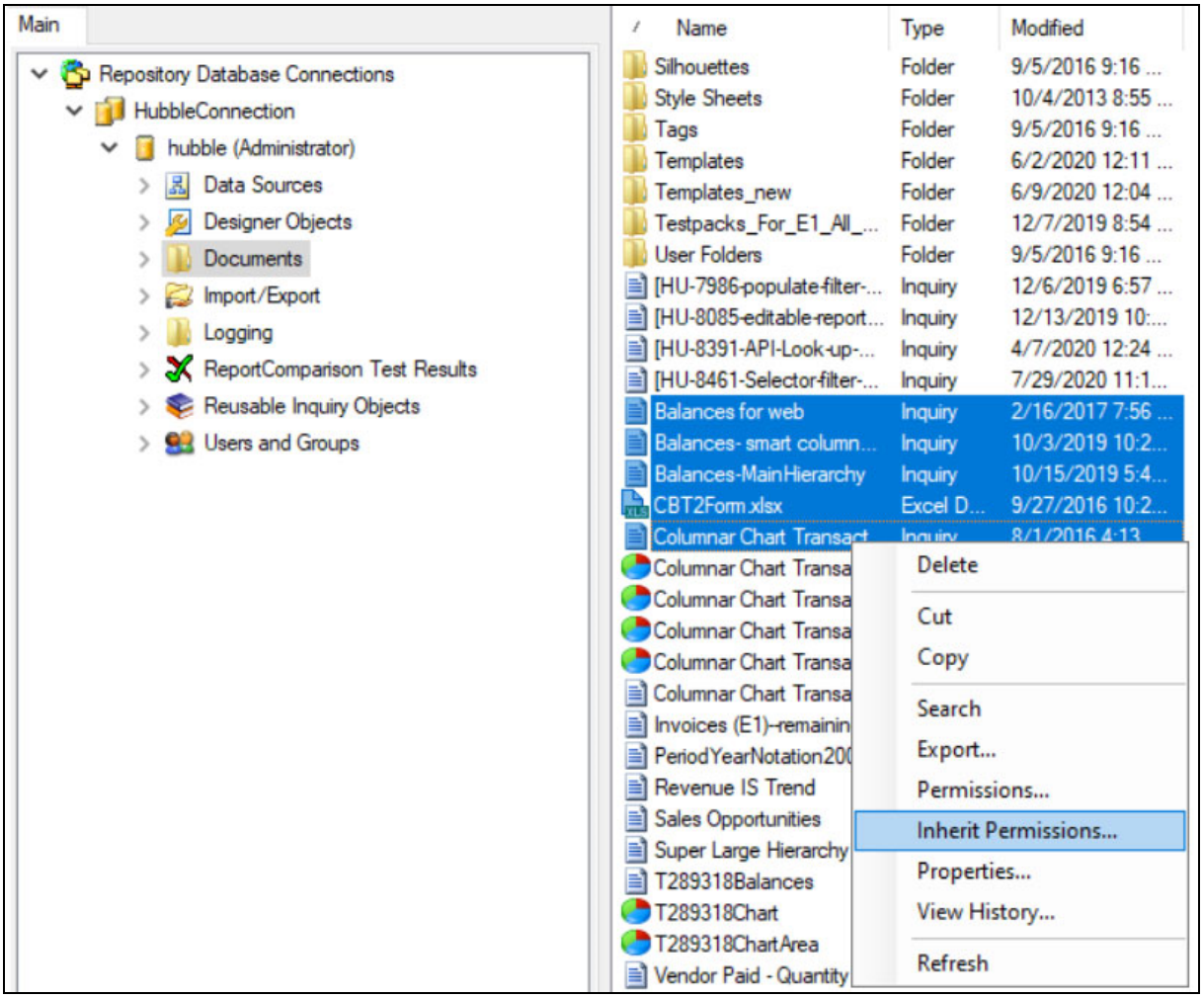
Permissions assigned to a folder are not automatically inherited by documents within the folder; however, any change to the folder can be copied to the folder's contents when the action has been completed. After changing the permissions for a folder and then clicking OK, you are asked whether or not to apply those same changes to every document and sub-folder within this folder:



Answering ‘Yes’ means that the same Permissions will be applied to everything within that folder; answering ‘No” means that the Permissions to the contents in that folder will remain unchanged.

Setting Documents To Inherit Permissions From Parent Folders

Folder permissions are not automatically inherited by the documents or sub-folders in them, but can be copied from a parent folder by selecting the document or documents, right-clicking on them and selecting the **Inherit Permissions** option:



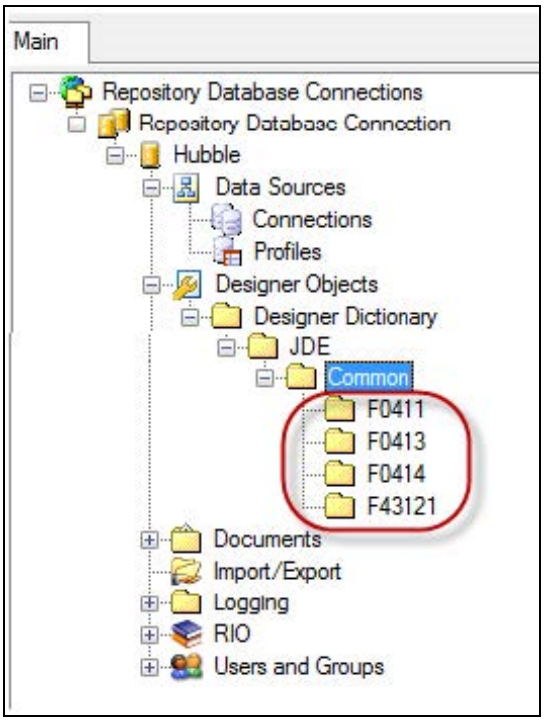
Other Functionality

Designer Express Setup

Default Metadata

When updating the ERP Profile, at the end of the Profile Wizard you will see a task called "**Import Hubble Default Metadata**" being performed. This step can take a while to complete the first time it is being done.

Once you go through the Profile Wizard, you will see an additional folder called "**Common**" that displays along with the folders for each ERP Version Specific profile defined if they were defined in a version prior to 2012.1. This "**Common**" folder is referred to as the **Customer Common Library**:



The Customer Common Folder will be populated for any customer-specific table definitions, for example, custom ERP System Tables.

The final step in the Profile Wizard created, behind the scenes, a folder for the **Hubble Default Library** that is not exposed in the repository. This folder is the one that stores all the Hubble Default Metadata to be used in DX when creating reports.

Designer Dictionary In Designer Express

This is where all the Default Amounts and Quantities (Hubble Default Metadata) are defined and stored. This file is used at the end of the Profile Wizard to bring in behind the scenes all the Hubble Default

Metadata. It is important to note that the HubbleDefaults.rdf file is not imported if the metadata in the repository matches the metadata in the rdf. Hubble checks the date the file was created, the date the file was modified, the file size and the checksum of the file to determine if the file has changed.

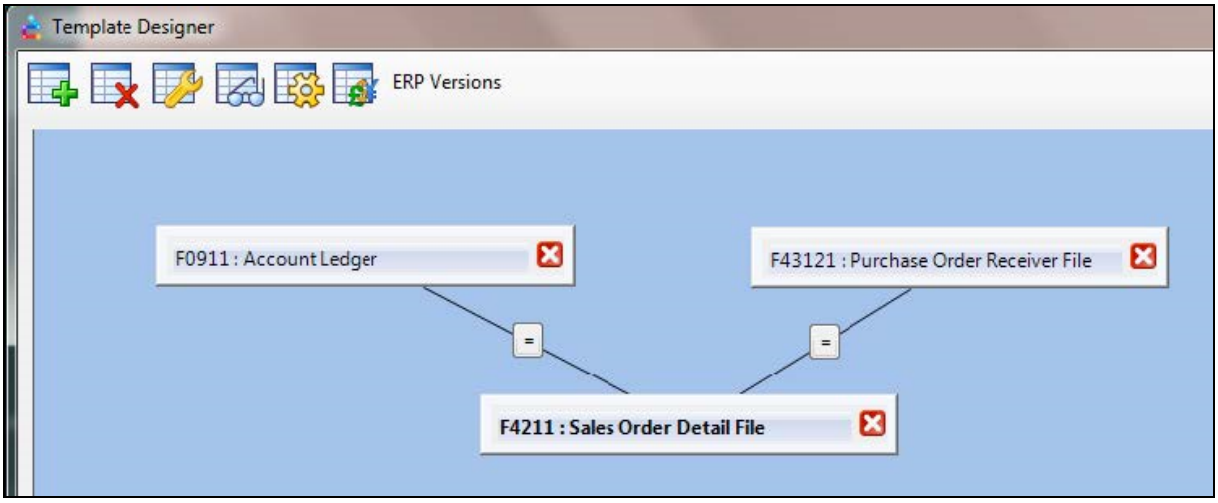
Note that the Hubble Defaults folder does not display in Administrator, however it is there behind the scenes once you have gone through the Profile Wizard.

Minimizing Tables In Template Designer

You can minimize the tables used in Template Designer so that only the table names appear. This is necessary when using many tables in a report so you can display all the tables on one screen within Template Designer.

After you have added a table from within Template Designer, double-click on the table header to minimize the table.

The below example shows all tables being minimized when each table header has been clicked on:



Module Security

Overview

Module Security was created to allow greater control of what a user can see when using the Payroll, Timesheet and Human Resources modules. This feature works in conjunction with the standard security settings provided with JD Edwards products, e.g. Business Unit Security.

The feature is available within Administrator and is attached directly to a profile. By defining security conditions based on fields and values, you can choose what a user can view and ultimately report on. These security conditions can be made against a specific User ID, against a specified group or even a combination of the two.

Brief examples of how the feature can be used include allowing administrative staff to see the contact details of staff while hiding their salary, or allowing the head of a department to only see the employees for whom he is responsible.

It is important to remember that users and groups will inherit permissions from their respective parent groups. In the situation of large numbers of users or groups, we recommend grouping users together with security levels in mind in order to reduce the overall maintenance. When similar level users are in the same group, you can apply the same security settings for the entire group instead of assigning them to individual users.

The application of Module Security only comes into effect when creating/opening a new inquiry. If the user whose security settings you are changing is already in an inquiry which you would like to restrict, the security will not be enforced. The user would need to close out of the inquiry and then reopen it in order for the security to take effect.

Setting Up Module Security

In order to be able to set up Module Security, you must have the following set in Administrator:

1. You must have Read and Update Permissions for the profile on which you will be setting Module Security.
2. You must have the Module Security Capability (accessible in the **Basic Capabilities > Administration tab > Module Security** feature).

Setting Up Module Security For A Profile

To set up module security for a profile, follow the steps below:

1. Log into your repository if you are not logged in already.
2. Expand **Data Sources** in the navigation tree on the left panel and select **Profiles**.
3. In the right panel, right-click on the required **Profile** and select **Module Security**.
4. Within the **Module Security** dialog, set Grant or Deny Permissions to specific users on specific modules:
   i. Select the specific Module using the drop-down menu.
   ii. At the level you wish to set security, highlight that user or group in the left panel
   iii. Click **New**.
   iv. From the drop-down list, select the field to be restricted.
   v. Specify the specific field values to either grant or deny to the selected user(s). (Multiple selections are separated with a comma and ranges are supported using the colon character. Only a single definition can be made per user for any one field.)
   vi. Using the radio button, select either **Granted** or **Denied**.
   vii. Click **OK**.
   viii. Click **OK** again in the main **Module Security** dialog.

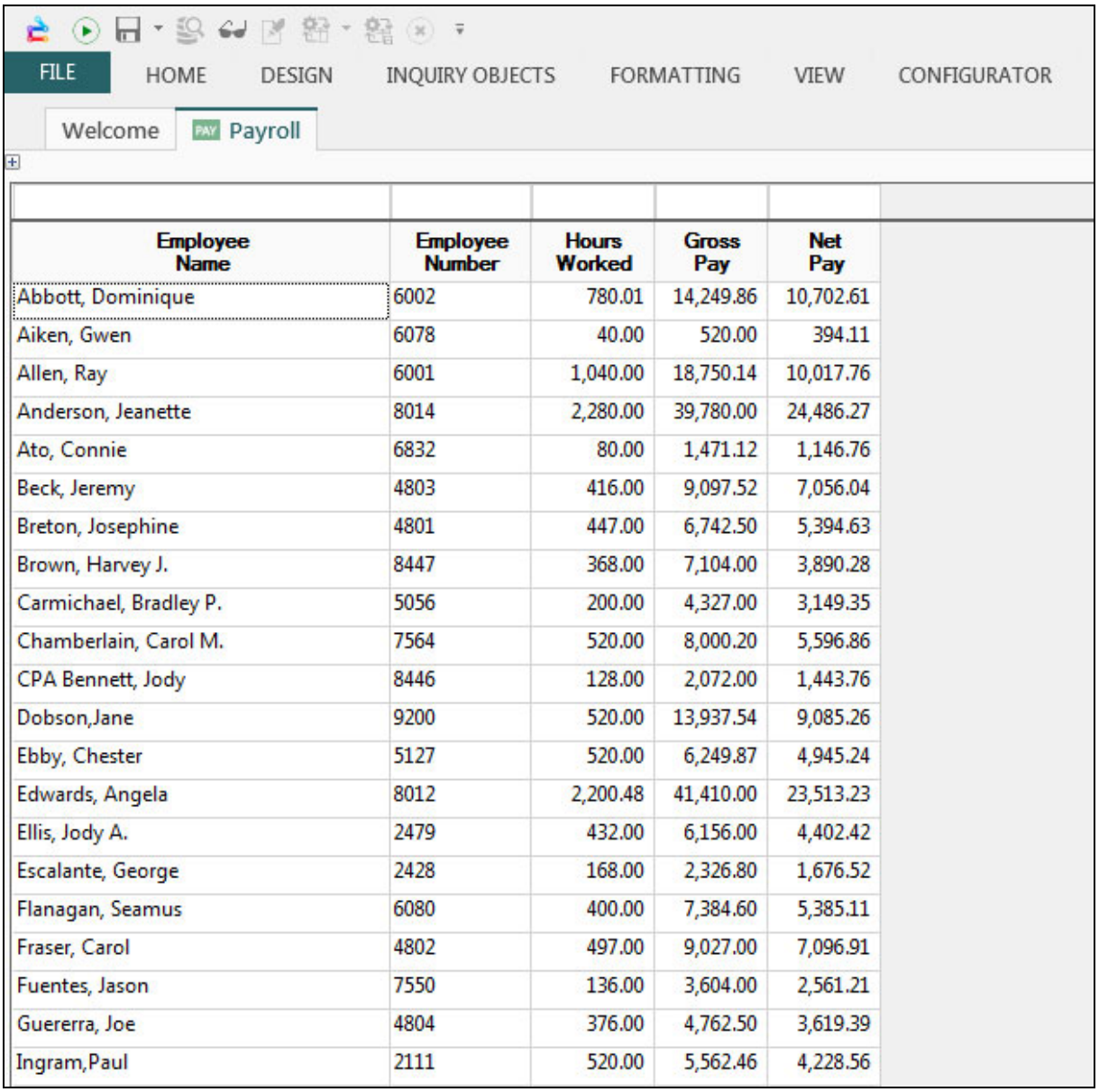
Module Security Examples

While the below examples are very specific in how Module Security can be configured to restrict or allow access to certain values, the logic can be applied to any allowable field.

Example 1: Denying Specific Values

In the first example, we are going to restrict a user from seeing specific employees' payroll details using the **Denied** mode. The result of using Module Security will be shown by comparing the results before and after changing the security.

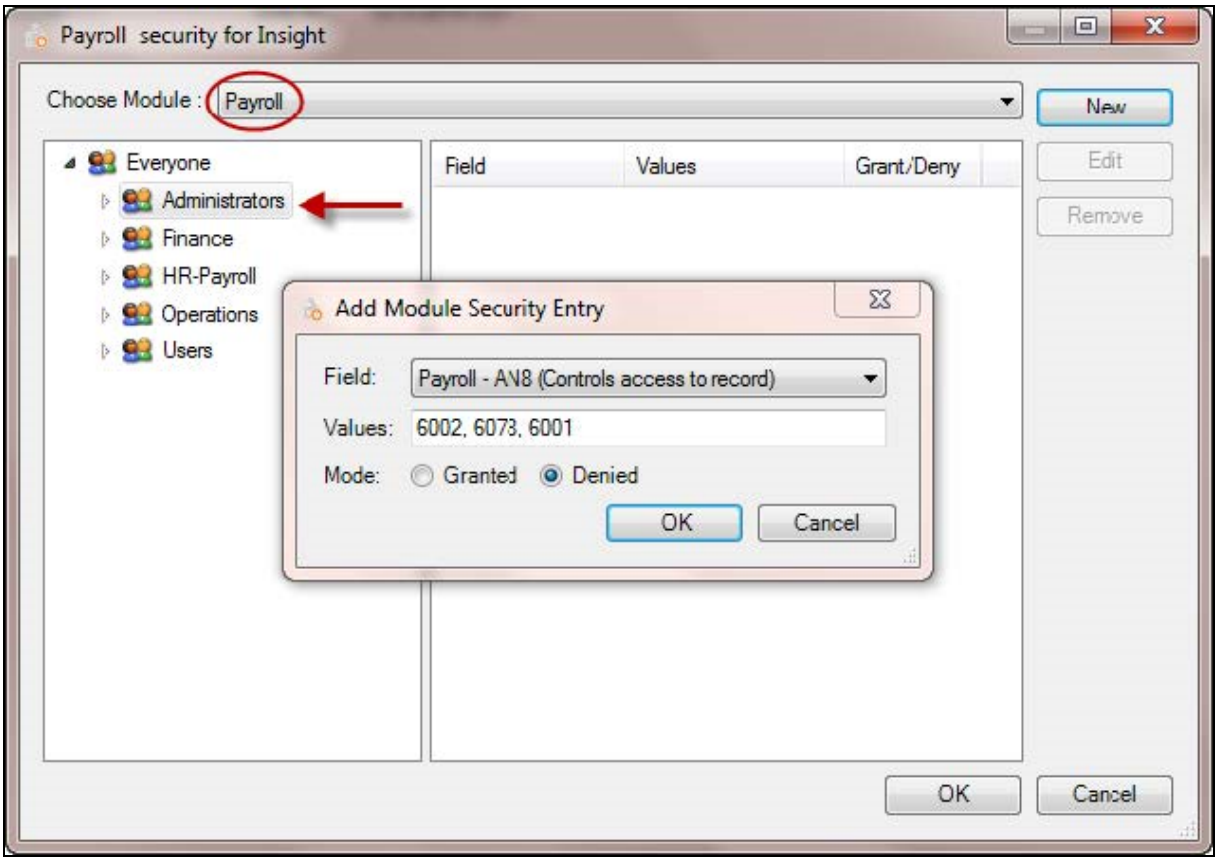
Below is a basic Payroll History inquiry prior to setting security. The filter selections, hidden to maximize the display result set, are left blank to return all results. Additionally all non-essential columns were removed.



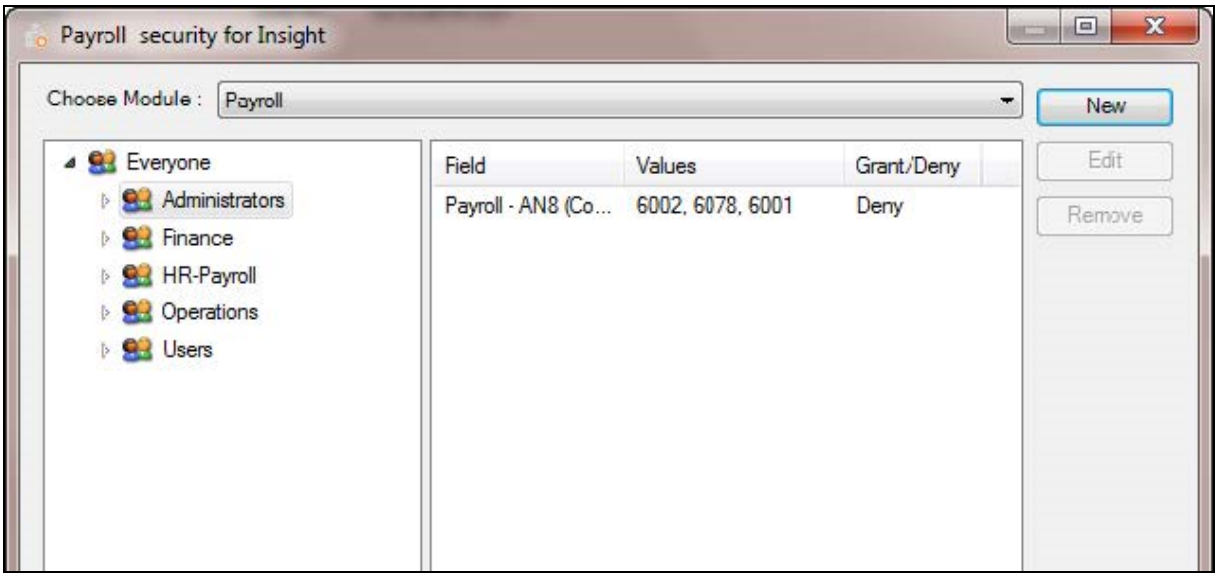
Employee Name	Employee Number	Hours Worked	Gross Pay	Net Pay
Abbott, Dominique	6002	780.01	14,249.86	10,702.61
Aiken, Gwen	6078	40.00	520.00	394.11
Allen, Ray	6001	1,040.00	18,750.14	10,017.76
Anderson, Jeanette	8014	2,280.00	39,780.00	24,486.27
Ato, Connie	6832	80.00	1,471.12	1,146.76
Beck, Jeremy	4803	416.00	9,097.52	7,056.04
Breton, Josephine	4801	447.00	6,742.50	5,394.63
Brown, Harvey J.	8447	368.00	7,104.00	3,890.28
Carmichael, Bradley P.	5056	200.00	4,327.00	3,149.35
Chamberlain, Carol M.	7564	520.00	8,000.20	5,596.86
CPA Bennett, Jody	8446	128.00	2,072.00	1,443.76
Dobson,Jane	9200	520.00	13,937.54	9,085.26
Ebby, Chester	5127	520.00	6,249.87	4,945.24
Edwards, Angela	8012	2,200.48	41,410.00	23,513.23
Ellis, Jody A.	2479	432.00	6,156.00	4,402.42
Escalante, George	2428	168.00	2,326.80	1,676.52
Flanagan, Seamus	6080	400.00	7,384.60	5,385.11
Fraser, Carol	4802	497.00	9,027.00	7,096.91
Fuentes, Jason	7550	136.00	3,604.00	2,561.21
Guererra, Joe	4804	376.00	4,762.50	3,619.39
Ingram,Paul	2111	520.00	5,562.46	4,228.56

In Administrator, we will apply security to the Administrator Group as shown below. This will affect all users within this group. We selected the Payroll Module at the top of the dialog, then selected the

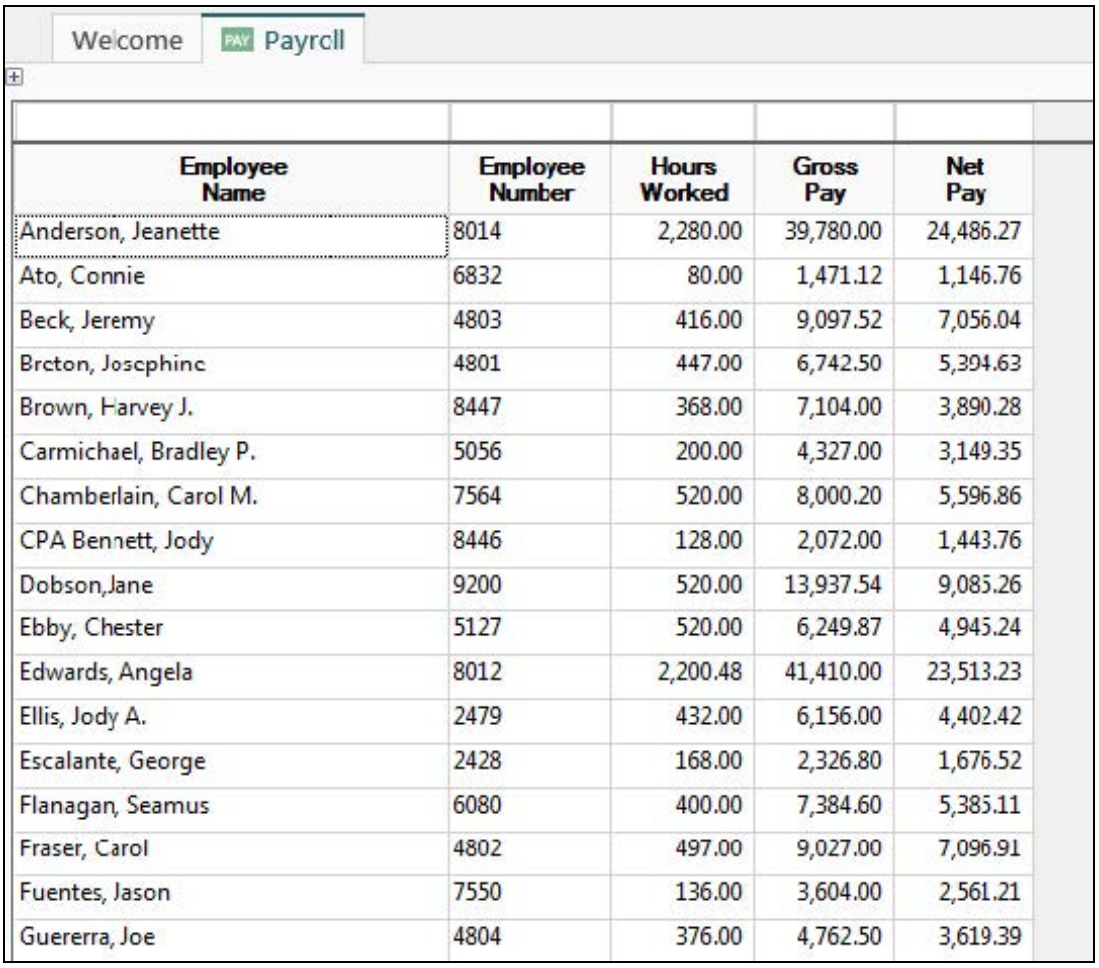
Administrator group. In the new security entry, we denied access to the AN8 field for values 6002, 6078 and 6001.



After clicking **OK**, you see the security entry for the Administrator group:



After closing and re-opening the inquiry, you see that the inquiry results no longer contain the Employee Numbers 6002, 6078 and 6001. This is because we denied the user visibility to these employees by using the Deny option to those specific field values:

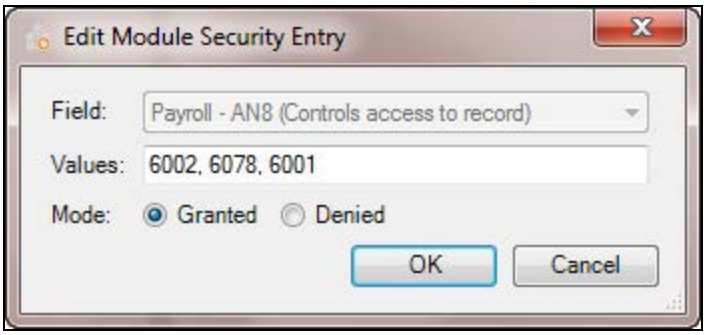


Welcome | Payroll

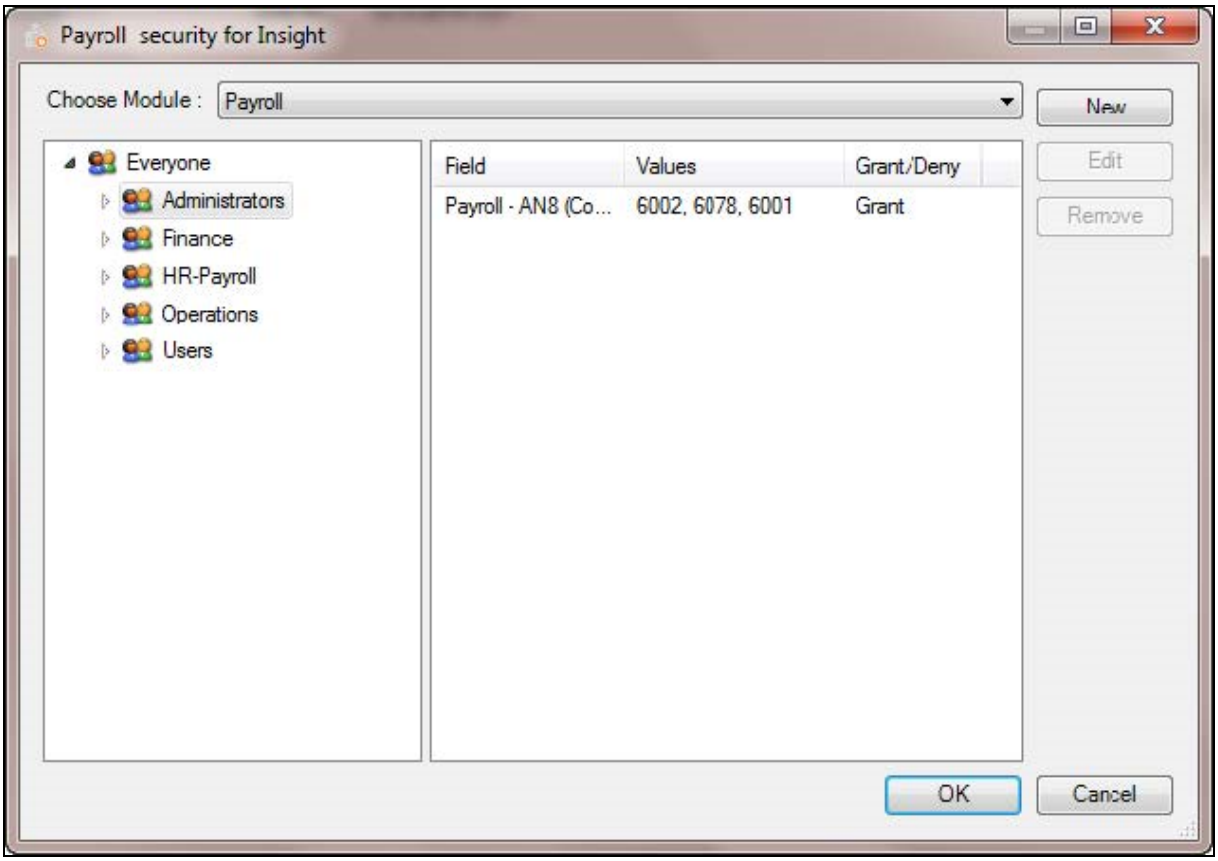
Employee Name	Employee Number	Hours Worked	Gross Pay	Net Pay
Anderson, Jeanette	8014	2,280.00	39,780.00	24,486.27
Ato, Connie	6832	80.00	1,471.12	1,146.76
Beck, Jeremy	4803	416.00	9,097.52	7,056.04
Brcton, Joscphinc	4801	447.00	6,742.50	5,394.63
Brown, Harvey J.	8447	368.00	7,104.00	3,890.28
Carmichael, Bradley P.	5056	200.00	4,327.00	3,149.35
Chamberlain, Carol M.	7564	520.00	8,000.20	5,596.86
CPA Bennett, Jody	8446	128.00	2,072.00	1,443.76
Dobson,Jane	9200	520.00	13,937.54	9,085.26
Ebby, Chester	5127	520.00	6,249.87	4,945.24
Edwards, Angela	8012	2,200.48	41,410.00	23,513.23
Ellis, Jody A.	2479	432.00	6,156.00	4,402.42
Escalante, George	2428	168.00	2,326.80	1,676.52
Flanagan, Seamus	6080	400.00	7,384.60	5,385.11
Fraser, Carol	4802	497.00	9,027.00	7,096.91
Fuentes, Jason	7550	136.00	3,604.00	2,561.21
Guererra, Joe	4804	376.00	4,762.50	3,619.39

Example 2: Granting specific values

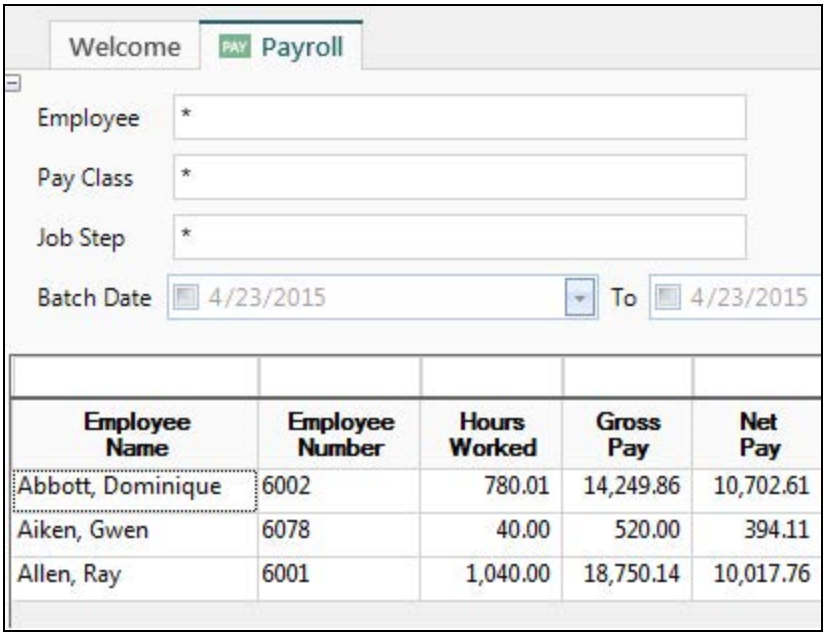
In the next example we can see the result of using the Granted mode against specific criteria. In Administrator, change your previously entered security condition and click Edit. Change the security entry to Granted, as shown below:



Click **OK** to see the changes referenced in the dialog:

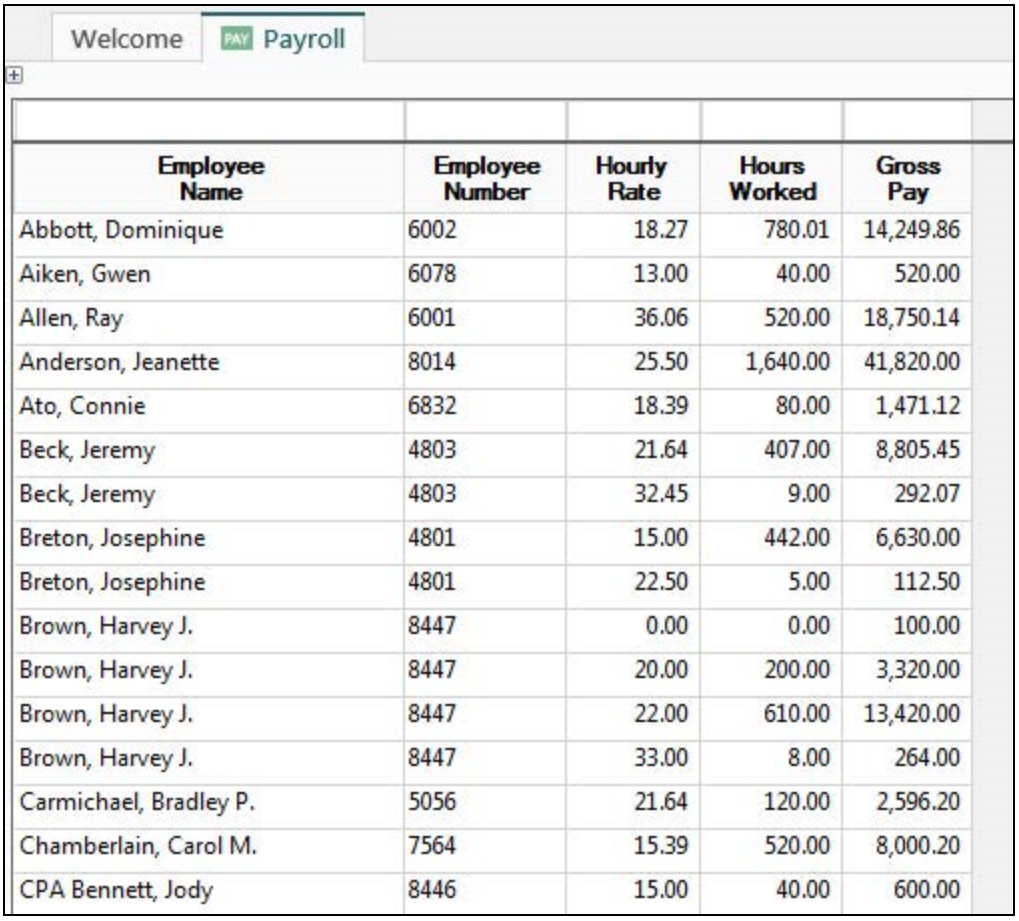


After closing and re-opening the inquiry, you see that the results have now been amended so we can see only the field values that were specified using the **Granted** option:



Example 3: Suppress label columns

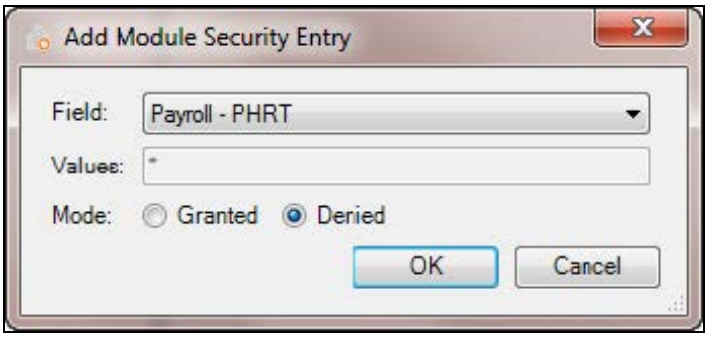
Some fields can be set to suppress the display of sensitive information from a user. In this example we will suppress the display of Hourly Rate, a label column found with the Payroll History Template. Before any security is applied, the inquiry looks like this:



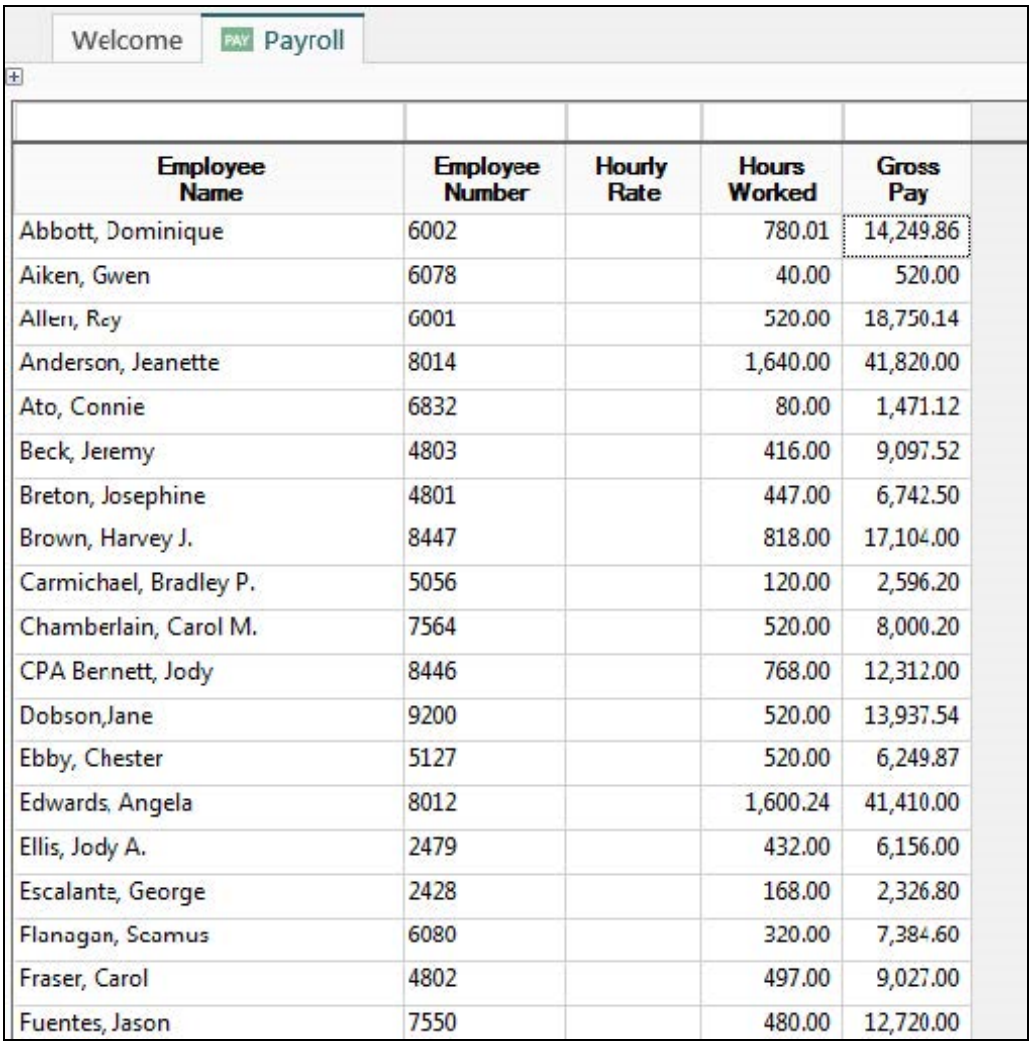
Employee Name	Employee Number	Hourly Rate	Hours Worked	Gross Pay
Abbott, Dominique	6002	18.27	780.01	14,249.86
Aiken, Gwen	6078	13.00	40.00	520.00
Allen, Ray	6001	36.06	520.00	18,750.14
Anderson, Jeanette	8014	25.50	1,640.00	41,820.00
Ato, Connie	6832	18.39	80.00	1,471.12
Beck, Jeremy	4803	21.64	407.00	8,805.45
Beck, Jeremy	4803	32.45	9.00	292.07
Breton, Josephine	4801	15.00	442.00	6,630.00
Breton, Josephine	4801	22.50	5.00	112.50
Brown, Harvey J.	8447	0.00	0.00	100.00
Brown, Harvey J.	8447	20.00	200.00	3,320.00
Brown, Harvey J.	8447	22.00	610.00	13,420.00
Brown, Harvey J.	8447	33.00	8.00	264.00
Carmichael, Bradley P.	5056	21.64	120.00	2,596.20
Chamberlain, Carol M.	7564	15.39	520.00	8,000.20
CPA Bennett, Jody	8446	15.00	40.00	600.00

In Administrator, add a new security entry on the Payroll - PHRT field. The PHRT field cannot be specified as in the previous examples, so the **Values** field is grayed out to prevent data entry. Instead, the **Values** section of the dialog is populated with a '*' (a select all) to indicate that all data returned will be affected.

For this example we will apply a **Denied** mode, as shown below:



Once the Module Security is set, the associated user will see that the Hourly Rate (PHRT) is now suppressed as shown below:


Welcome | Payroll

Employee Name	Employee Number	Hourly Rate	Hours Worked	Gross Pay
Abbott, Dominique	6002		780.01	14,249.86
Aiken, Gwen	6078		40.00	520.00
Allen, Roy	6001		520.00	18,750.14
Anderson, Jeanette	8014		1,640.00	41,820.00
Ato, Connie	6832		80.00	1,471.12
Beck, Jeremy	4803		416.00	9,097.52
Breton, Josephine	4801		447.00	6,742.50
Brown, Harvey J.	8447		818.00	17,104.00
Carmichael, Bradley P.	5056		120.00	2,596.20
Chamberlain, Carol M.	7564		520.00	8,000.20
CPA Bernett, Jody	8446		768.00	12,312.00
Dobson,Jane	9200		520.00	13,937.54
Ebby, Chester	5127		520.00	6,249.87
Edwards, Angela	8012		1,600.24	41,410.00
Ellis, Jody A.	2479		432.00	6,156.00
Escalante, George	2428		168.00	2,326.80
Flanagan, Seamus	6080		320.00	7,384.60
Fraser, Carol	4802		497.00	9,027.00
Fuentes, Jason	7550		480.00	12,720.00

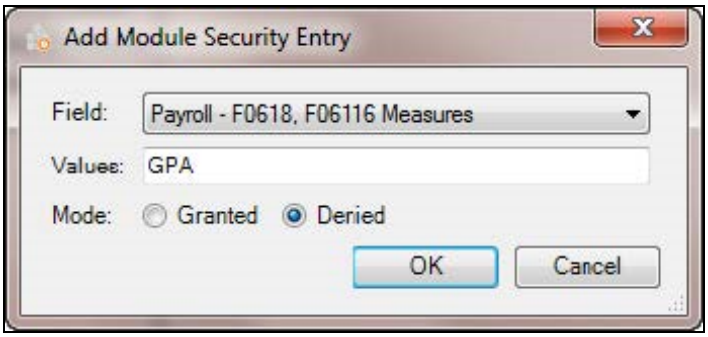
Example 4: Suppressing value columns

Module Security also provides a way of suppressing the display of value columns. As with previous examples, you need to select the correct field from the drop-down list within the Module Security dialog. (The below example illustrates one value column being affected. However by entering an asterisk (*) in the value section of the **Add Module Security Entry** dialog, you can select all value columns, allowing you to grant or deny all values in all columns.) It is important to know that if you suppress all the value columns in your inquiry, no data will be returned in the result set. To see records, you must enable the Zero Balances feature in Hubble.

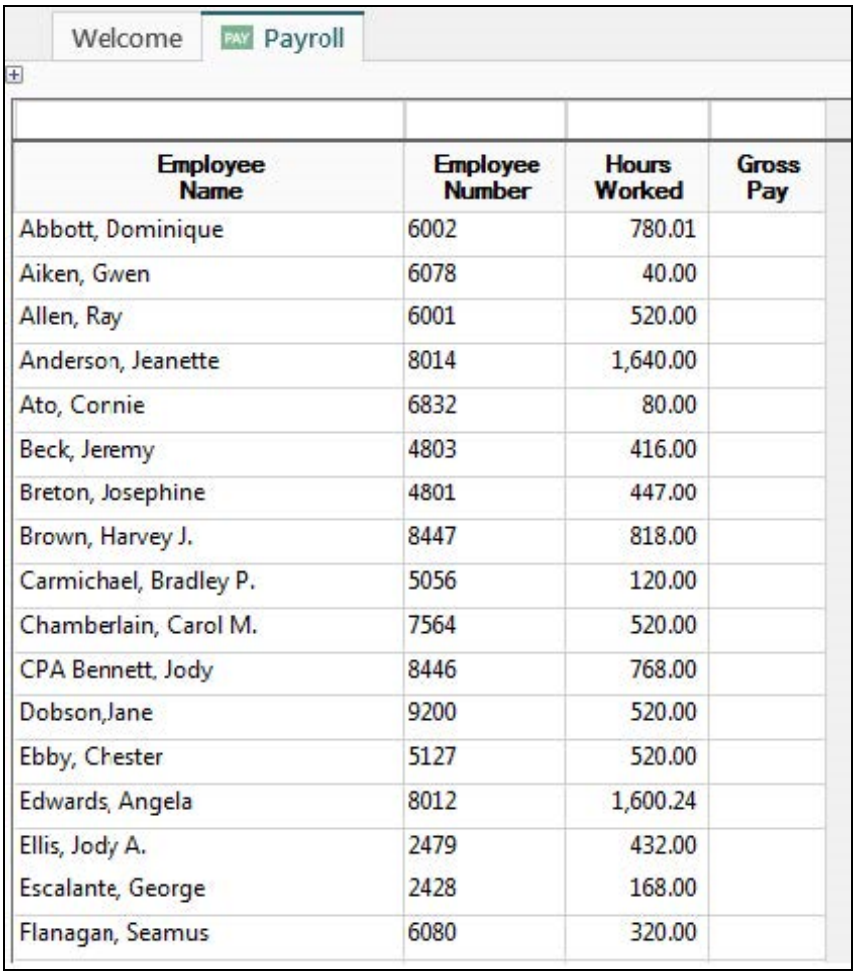
In this example, we are going to restrict the Administrator group from viewing the Gross Pay value column (GPA). In the **Add Module Security Entry** dialog:

- **Field**: Payroll – F0618, F06116 Measures. [The inquiry is based off the Payroll History Template, which contains data from the Employment Transaction History (F0618) and Employee Transaction Detail File (F06116) tables. This is why we have chosen the field that is in both the F0618 and F06116 tables.]
- **Values**: GPA (Again, we only are suppressing values in this column, so this is the only one that needs to be specified here. To select all columns, you would enter an asterisk (*).

- **Mode**: Denied (setting used for suppressing data in the specified value column).



As a result of the Module Security setting, the Gross Pay column, although specified in the filter, will no longer be displayed to users in the Administrator Group as shown below:



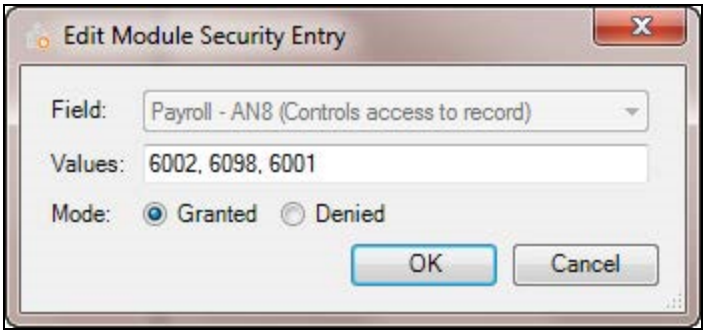
Employee Name	Employee Number	Hours Worked	Gross Pay
Abbott, Dominique	6002	780.01	
Aiken, Gwen	6078	40.00	
Allen, Ray	6001	520.00	
Anderson, Jeanette	8014	1,640.00	
Ato, Cornie	6832	80.00	
Beck, Jeremy	4803	416.00	
Breton, Josephine	4801	447.00	
Brown, Harvey J.	8447	818.00	
Carmichael, Bradley P.	5056	120.00	
Chamberlain, Carol M.	7564	520.00	
CPA Bennett, Jody	8446	768.00	
Dobson,Jane	9200	520.00	
Ebby, Chester	5127	520.00	
Edwards, Angela	8012	1,600.24	
Ellis, Jody A.	2479	432.00	
Escalante, George	2428	168.00	
Flanagan, Seamus	6080	320.00	

Example 5: Combinations of security

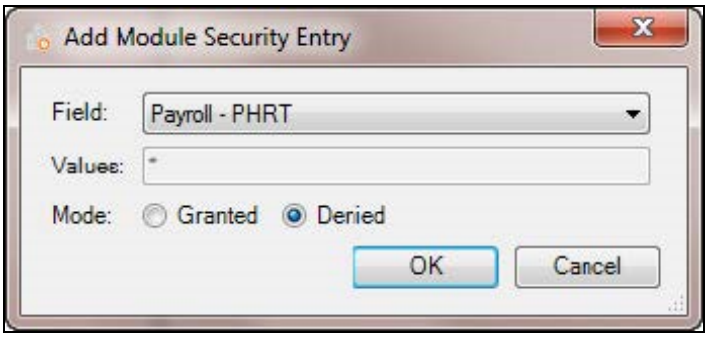
In the previous examples we have used single selections to Grant or Deny access to certain values; however it is also possible to use multiple selections.

The following example demonstrates how you may wish to grant access to a user for specific employees, but deny the user the ability to view payroll information such as Hourly Rate.

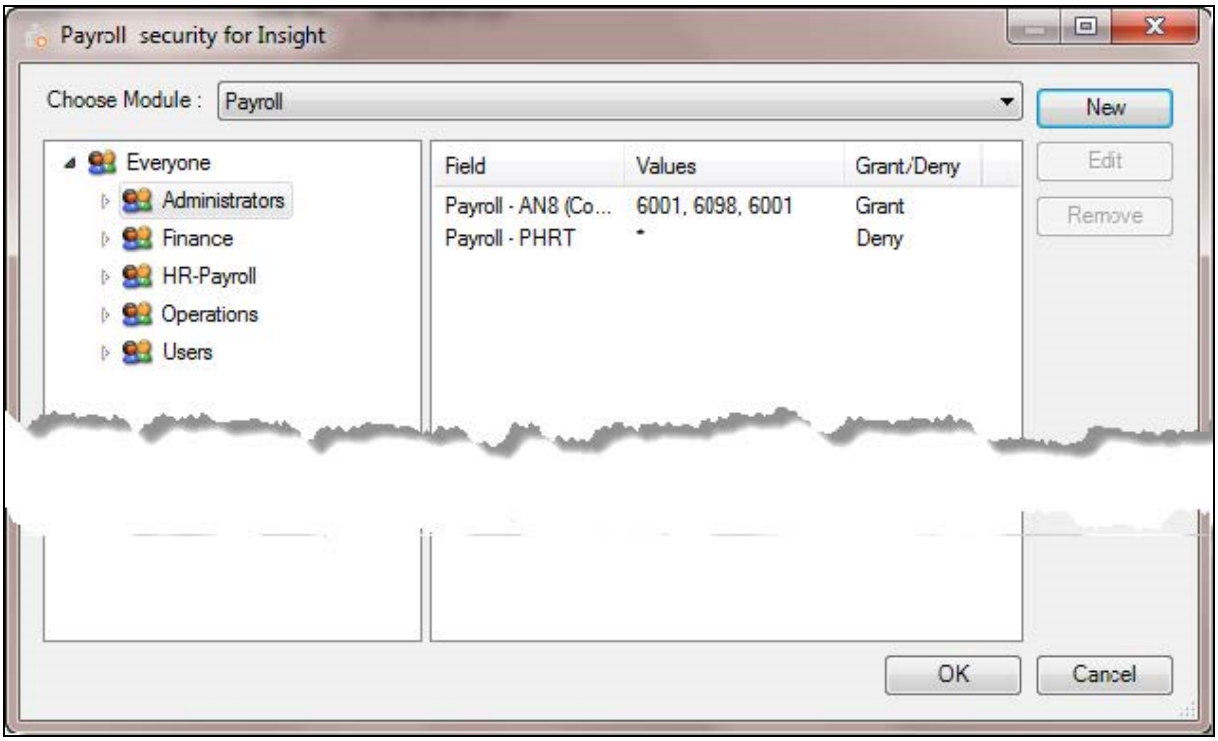
For the first condition, we will repeat the condition established in the 2nd example, granting specific values:



For the second condition, we will repeat the condition established in the 3rd example, suppressing label columns:

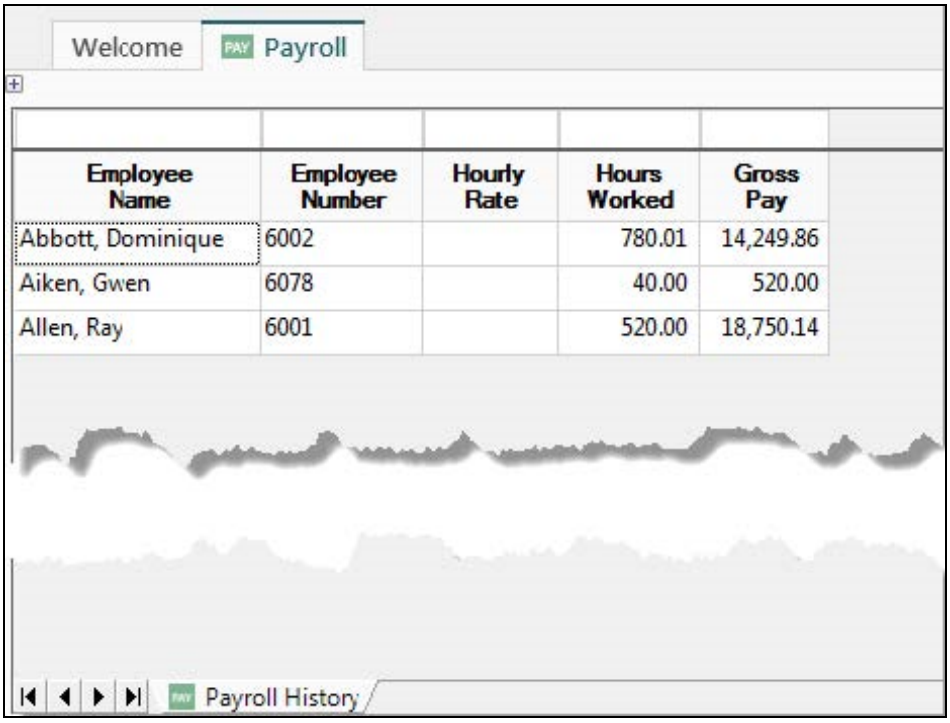


The **Module Security** dialog will then display both conditions:



As shown below, the user has been limited to the three employee's records via **Granted** mode and the hourly rate has been affected by the **Denied** mode.

The combination of security conditions allows for detailed and complicated authorities to be handled in a reasonably straightforward manner.



Inheritance And Priority

Module Security is designed to work with large hierarchical organizational structures by allowing users and groups to inherit security conditions from their respective parent groups. The underlying security engine will combine all the levels for one particular **Field**. However a condition established with a **Deny** mode will take precedence over a **Granted** mode.

Security Inheritance on a two-level system

The table below shows how security condition priorities would be applied when security is set at the Group and User levels.

GROUP LEVEL SECURITY	USER LEVEL SECURITY	RESULT
Grant 1000	Grant 2000	User can see 1000 and 2000 only
Deny 1000	Deny 2000	User can see everything except 1000 and 2000
Deny 1000	Grant 1000	Denies everything; denying a specific field and setting takes precedence

GROUP LEVEL SECURITY	USER LEVEL SECURITY	RESULT
Grant 1000:2000	Deny 1500	User can see 1000:1499 and 1501:2000

GROUP LEVEL SECURITY	USER LEVEL SECURITY	RESULT
Grant 1000	Deny *	Will deny all
Deny 1000	Grant *	Will allow all

Security Inheritance on a three-level system

The table below shows examples of how priorities would be applied when security is set on a three level system:

Everyone Level

Group Level

User Level

EVERYONE LEVEL SECURITY	GROUP LEVEL SECURITY	USER LEVEL SECURITY	RESULT
Deny *	Grant 1000:5000	Grant 7000	User can view records for employees 1000:5000 and 7000
Deny *	Grant 1000:5000	Deny 3000	User can view records for employees 1000:5000 but not 3000
Deny *	Deny 1000:5000	Grant 7000	User can view records for employee 7000 only
Deny *	Deny 1000:5000	Deny 7000	User cannot see any employee records
Deny 3000	Grant 1000:5000	Grant 7000	User can view records for employees 1000:5000 and 7000 except for 3000

EVERYONE LEVEL SECURITY	GROUP LEVEL SECURITY	USER LEVEL SECURITY	RESULT
Deny 3000	Grant 1000:5000	Deny 4000	User can view records for employees 1000:5000 except for 3000 and 4000
Grant *	Grant 1000:5000	Grant 7000	User can view records for all employees
Grant *	Grant 1000:5000	Deny 7000	User can view records for all employees except 7000

EVERYONE LEVEL SECURITY	GROUP LEVEL SECURITY	USER LEVEL SECURITY	RESULT
Grant *	Deny 1000:5000	Grant 3000	User can view all records for employees except 1000:2999 and 3001:5000
Grant *	Deny 1000:5000	Deny 7000	User can view records for all employees except 1000:5000 and 7000

Incorporate JD Edwards Security

JD Edwards EnterpriseOne Security

Hubble incorporates the JD Edwards EnterpriseOne security as described below.

JDE E1 Environment Login Security

In the Hubble profile that connects to the JDE production data, there is a JDE environment that is associated. For example, a production profile could have the JPD920 environment associated. When a user logs into Hubble and selects the production profile, the user will only complete the logon if one of his/her active roles (individual role selected or *ALL role selected at logon) has access to the JPD920 environment.

JDE E1 Row Security

Hubble appropriately applies row security as inclusive or exclusive based on the JDE system definition.

Hubble follows the EnterpriseOne user, role, *Public hierarchy to apply row security. This means that if row security is found at the user level, only this row security is applied. If nothing is found at the user level, it goes to the role level and applies that security if it is found. If nothing is found at the user level or at the role level, row security at the *Public level is applied if it is set up. Hubble also incorporates role conflict resolution when multiple roles associated to the user have row security defined.

Hubble follows the same EnterpriseOne table, then *ALL hierarchy. In other words, if row security is found at the specific table level, then this row security is applied. If nothing is found at the specific table level, row security at the *All table level is applied if it is found.

Hubble also restricts table access when inclusive row security is defined and the table has View, Add, Change and Delete set to no.

JDE Inclusive Row Security

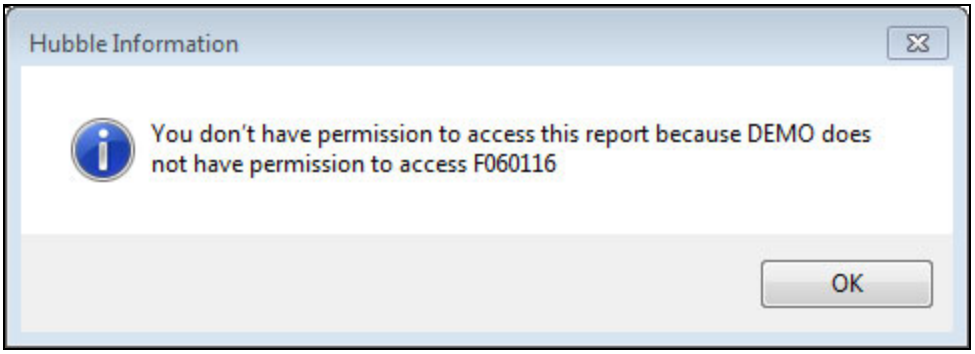
The JDE row security functionality allows JDE sites to setup Inclusive row security, where a role cannot view a table.

Example of JDE Inclusive Row Security:

ROLE	TABLE	COLUMN	RANGE	VIEW	ADD	CHANGE
*Public	F06116	AN8	*BLANKS-99999999	N	N	N
ABC	F06116	AN8	*BLANKS-99999999	Y	Y	Y

- STEPHEN is part of ABC role.
- DEBBIE is part of XYZ role.
- STEPHEN can View, Add, Change F06116.YTAN8 between 0-99999999.
- DEBBIE cannot access F06116 at all because of the *PUBLIC against the F06116 with View, Add, Change, Delete all set to N.

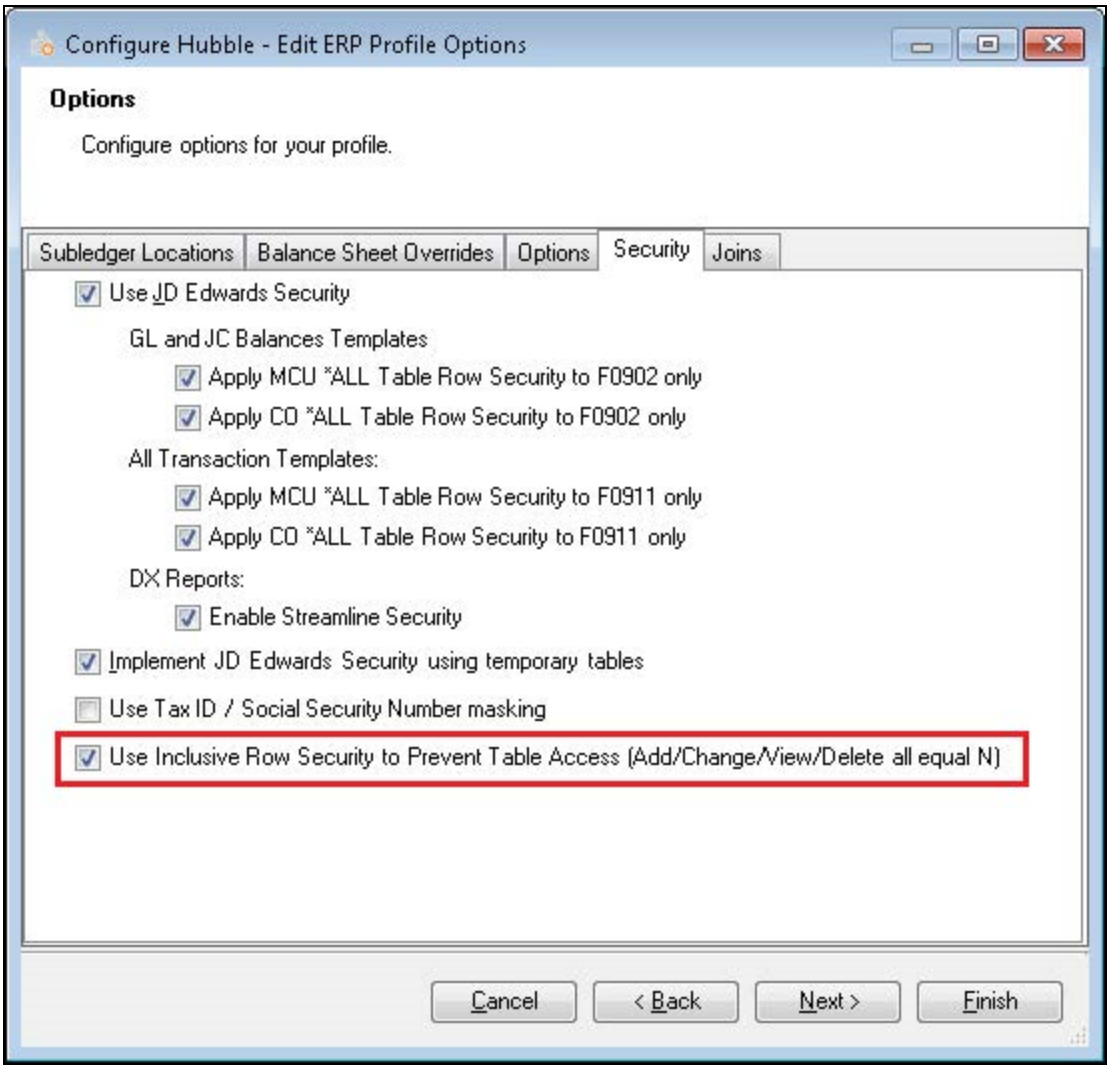
If the HR Employee Detail table where F06116 is the fact table is opened by a user without permission, they will receive this message:



If the restricted table is optional, then the template can still be opened but will be displayed in gray and cannot be selected to be used in the report.

A report that has a column in use from a restricted table would result in an error if a restricted user tries to open it.

This feature is disabled or enabled via a security Profile Option (it is enabled by default).



JDE E1 Column Security

Hubble applies column security established for JDE tables and *ALL Table. Hubble will not be able to incorporate column security created for a JDE application or for a JDE form because it is not possible to cross reference between JDE applications or forms to tables. Hubble applies column security at the appropriate user, role, *Public hierarchy and at the appropriate specific table, *ALL table hierarchy.

JDE E1 Address Book Data Privacy Security

Hubble applies address book data privacy security to restrict users from viewing address book information that is determined as personal data. Hubble applies address book data privacy security at the appropriate user, role, *Public hierarchy.

When data is being masked in Hubble, the columns still display on the report but the data is masked. The data displays as ********** in the column if it is an alpha column, and 0 if the column is a numeric column.

There is not anything that you need to do in order to set up the Address Book data privacy feature in Hubble. As long as this is set up in JD Edwards E1 in P01138, the same setup is honored in Hubble. (In JD Edwards E1, you must activate Personal Data Security as well as set up exactly what data you want to mask and which users or roles would see the masked data).

JD Edwards World Security

Hubble incorporates the JD Edwards World security as described below.

JDE World Environment Login Security

In the Hubble profile that connects to JDE production data, there is a JDE environment that is associated. For example, a production profile could have the JDWP environment associated. When a user logs into Hubble and selects the production profile, the user will only complete the logon if his/her user or group has access to the JDWP environment.

JDE World Business Unit Security

Hubble applies business unit security against tables with a business unit column and applies it with an inclusive approach.

Hubble follows the same World user, group, *Public hierarchy to apply business unit security. This means that if row security is found at the user level, then only this row security is applied. If nothing is found at the user level, it applies row security at the group level if it is set up. If nothing is found at the user level or at the group level, it applies row security at the *Public level if it is found.

Hubble follows the same World specific table, *ALL table hierarchy. So if business unit security is found at the specific table level, only this row security is applied. If nothing is found at the specific table level, business unit security is applied at the *All table level if it is set up.

Incorporate Oracle EBS Security

Hubble incorporates Oracle EBS security as described below.

General Ledger Security

Functional Security

Functional security is controlled through roles (responsibilities). GL module licenses are only assigned to users who require them.

Data Access Set Security

Data Access Sets secure access to ledgers, ledger sets, and portions of ledgers by using primary balancing segment values. All ledgers in the same data access set must use the same chart of accounts and accounting calendar.

The ERP data regarding which roles can access a Data Access Set to generate SQL Join conditions on specific tables is used. In some tables, the field containing this data is called SET_OF_BOOKS_ID, a

legacy from version 11i of EBS. The list of tables for which these conditions are generated is maintained in the source code of the Hubble application.

Segment Value Security

Segment value security rules are set up against 'value sets' to control access to parent or detail segment values.

In practice:

- **Oracle**: Securing a value set denies access to all values by default. Create conditions and assign them to specific data roles to control access to your value set values.
  Hubble: SQL based on the conditions is generated, provided this SQL is compatible with the report code.
- **Oracle**: Restrict data entry, online inquiry, and reporting to specific values by using segment value security rules.
  Hubble: SQL conditions based on the specific values is generated.

Chart Of Accounts Security

Oracle allows the enabling of security for a Chart of Accounts. This denies access to all users except as permitted by Segment Value Security.

Default Ledger Selector

In many Hubble templates a filter on the Ledger Id is included, and a Selector to set the filter value equal to the default ledger is generated. This is not exactly security, as it allows the users to change or remove the filter value, but it is helpful, especially where a user only works on a single ledger.

Ledger security also applies in Visual Assists, as the user will not be able to put a ledger they should not see into a filter.

HR Business Group Security

In HR and Payroll there is security on the links between roles and business groups. It is expected that the associated rules be set up by the customer.

HR And Payroll Security

There is a second layer of security for HR and Payroll. The permitted Persons, Organization Units, Positions, Assignments, Payrolls can be returned as lists from Oracle EBS functions. These lists are then stored in temporary tables and joined to the report to restrict access.

Even when running on Actian Vector, Hubble requires a connection back to the Oracle source database in order to provide this security. This is set up in the profile as the Security Connection and must be to the APPS user.

Additional Features

Time Out Option

Hubble applications do not have a time out option, but the database server can usually be configured to drop connections after a period of inactivity. Hubble will then offer to reconnect, however it does not demand a user password when doing so.

Journals And Journal Receivers

Background

Journaling is an AS/400 integrated database feature which keeps track of changes made to physical files (e.g. record created, deletion, modification; file open and close). this information can be used for audit purposes or to undo/redo changes made.

Any journal receiver which is out of use can be deleted manually immediately or automatically by the system. For detailed information on the subject of Journal Management beyond what is provided below, please refer to IBM's website:

http://www-01.ibm.com/support/knowledgecenter/ssw_ibm_i_71/rzaki/rzakiconcepts.htm

Usage in Hubble

Hubble uses journals and their associated journal receivers for transaction support when updating the Object Repository tables.

Journal and journal receiver creation happens automatically when creating a SQL collection. When executing 'CREATE COLLECTION' via STRSQL, among other objects the system creates QSQJRN (the journal) and QSQJRN0001 (the journal receiver). The journal provides a hook into the physical file activity. In order to record activity, the journal uses a journal receiver which is created using CRTJRNRCV. Conceptually, the journal can be seen as a notebook and the receiver as a page within it. Like a page in a notebook, a receiver can become filled up; when this is the case, the journal can be configured to log a message and have an administrator create a new receiver and attach it, or the system can just create a new receiver automatically using the full one as a template

Deleting Journals

If journaling is used for auditing purposes, then the administrator would back up detached (full) receivers to tape and then delete them. In case the journals are only used to support transactions (as is the case with the object repository), the detached receivers can simply be deleted.

To turn on automatic receiver deletion, run the following command (assuming that the collection is called HUBBLE): CHGJRN JRN(OSTORE/QSQJRN) DLTRCV(*YES). This will only delete the journal receivers for the HUBBLE library.

You can remove the existing Journal Receivers that are not being used. This is done by the library so it won't affect other processes or jobs outside of those in the Hubble library. The system will not allow you to remove Journal Receivers that are being used currently.

Remove DWTEMP Files

On Oracle databases, there are times when the DWTEMP tables are not deleted from the database. This can happen whenever Hubble is closed before an inquiry is closed with the Close Inquiry button or if the software experiences a database time out.

Oracle database administrators can use the following unsupported example to create a script that will clean out DWTEMP tables that are at least 1 day old. Please provide the below script to your database administrator for their review to confirm the script meets your company policies and needs.

```
DECLARE
sqlstmt    VARCHAR2(255);
CURSOR    dropcursor IS
SELECT 'DROP TABLE ' || owner || '.' || object_name || ' CASCADE
CONSTRAINTS'
FROM all_objects
WHERE object_name LIKE 'DWTEMP%' AND object_type = 'TABLE' AND created <
SYSDATE - 1;
BEGIN
OPEN dropcursor;
FETCH dropcursor INTO sqlstmt; LOOP
EXIT WHEN dropcursor%NOTFOUND; EXECUTE IMMEDIATE sqlstmt;
--    dbms_output.put_line ( sqlstmt );
FETCH dropcursor INTO sqlstmt; END LOOP;
CLOSE dropcursor; EXCEPTION
WHEN OTHERS THEN
dbms_output.put_line ( 'SQL error while executing ' || sqlstmt || ' / SQL
Error ; ' || SQLERRM);
END;
/
```

Unable To Log In: Possible Reasons

There are a number of possible reasons as to why you may not be able to log in to the application. Be sure to check the following items:

- Ensure that the username and password are entered correctly.
- If the connection is to a JD Edwards World configuration, the username and password will be the user's normal JD Edwards username and password.
- If the connection is to a JD Edwards EnterpriseOne configuration, the username will be their normal JD Edwards username and their password is that which is set in Administrator in the user's profile.
- If the connection is to EBS, the username is their normal EBS username and their password is that which is set in Administrator in the user's profile.
- Check that the username exists in the Hubble Object Repository and that the user has Read permissions to the Data Source Connection and Profile being used.

Error that my user is not defined in the F0093 library - This error is saying that your user group or role is not associated with this environment it is associated with in the JD Edwards F0093 table.

The specific error is: **User '<username>' is not defined in the [<database>].[<table_prefix>].[F0093] library**.

A Hubble Administrator can confirm this by using the following SQL to see if the user exists.

```
SELECT LLUSER,LLLL
 FROM<TABLE_PREFIX>.F0093
 WHERE LLLL = '<ENVIRONMENT>'
AND LLUSER IN ('<USERNAME>','<USERSGROUPOR_ROLE>')
```

Where:

- <TABLE_PREFIX> is the table prefix
- <ENVIRONMENT> is the environment
- <USERNAME> is the JD Edwards username
- <USERSGROUPOR_ROLE> is the user's group or role

If the user has access to that environment, at least one row will be returned. If the user does not have access to that environment, no results will be returned.

For this example we will be using database OPENWORLD2007, table prefix DBO, environment DEMO900, user JASON and groups/roles SUPPORT and SUPPORT1.


```
USE OPENWORLD2007
SELECT LLUSER,LLLL
FROMDBO.F0093
WHERE LLLL = 'DEMO900'
AND LLUSER IN ('JASON','SUPPORT','SUPPORT1')
```

Running the SQL against the database returns zero rows.

Selecting all columns and returning all results reveals that groups/roles SUPPORT and SUPPORT1 only have access to environment DEMO810NT.

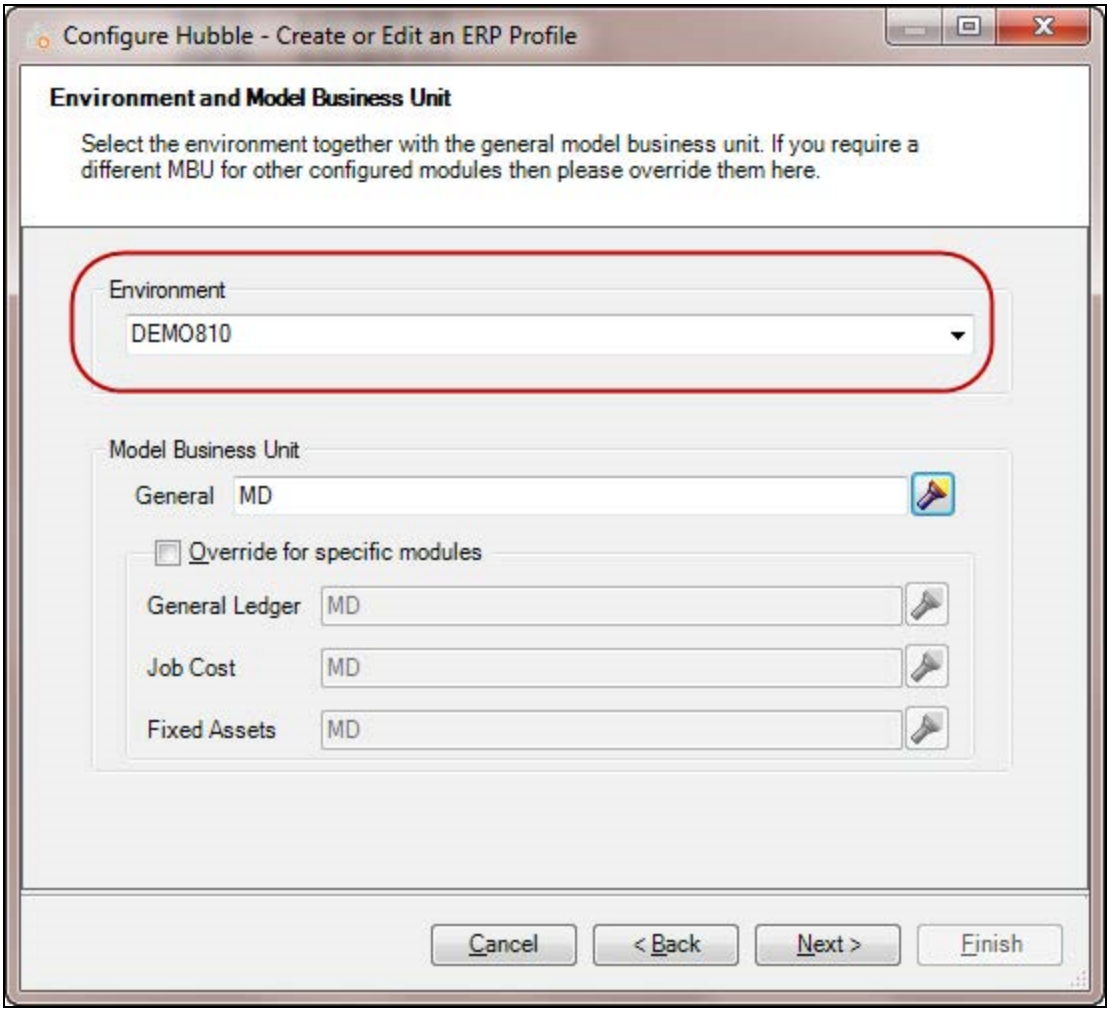
LLUSER	LLLL	LLSEQ	LLMNI
Accountirg	DEMO81C	1	
ANNETTE	DEMO81C	1	
APPLEAD	DEMO81C	2	
CNCADMIN	DEMO81C	2	
DEBBIE	DEMO81C	2	
DEMO	DEMO81C	10	
DEMO	DEMO01C400	20	
DEMO	DEMO81CHP	30	
DEMO	DEMO81CNT	50	
DEMO	DEMO81CRS6	40	
DEMO	DEMO81CSUN	60	
DEMOE	DEMO81C	10	
PRODUSER	DEMO81C	1	
PURCHASING	DEMO81C	1	
ROBERT	DEMO81C	4	
SALES	DEMO81C	2	
SUPPORT	DEMO81CNT	1	
SUPPORT1	DEMO81CNT	1	
NULL	*NULL*	*NULL*	*NULL*

To resolve this issue, the user or user's group/role will need to be granted access to the environment from within JD Edwards.

In Administrator, view the profile being used to log into the Hubble application to verify which JD Edwards environment your user ID is being validated against. To do this, follow these steps:

1. Log into the repository if you are not logged in already.
2. Expand the **Data Sources** node in the left panel.
3. Select **Profiles** and in the right panel.
4. Right-click on the specific profile being used to log into the application.
5. Select **Edit**.
6. Click **Next** in the Profile Wizard until you get to the **Environment and Model Business Unit** screen.
7. The environment defined here is that which is being used in JD Edwards to validate the user

signing in:


Configure Hubble - Create or Edit an ERP Profile
Environment and Model Business Unit
Select the environment together with the general model business unit. If you require a different MBU for other configured modules then please override them here.
Environment
DEMO810
Model Business Unit
General
MD
Override for specific modules
General Ledger
MD
Job Cost
MD
Fixed Assets
MD
Cancel
< Back
Next >
Finish