TOC

Logi Symphony 24

Manage Symphony 24 Users, Licenses, Tenants

Quick Start Reference - Manage Symphony Users, Licenses, Tenants

Managing Symphony covers multiple areas:

Using Symphony

- Product Overview
- Log On To Symphony
- Edit Your Profile And Change Your Password
- Using The Status Bar
- Using Dockable Windows
- Rename An Item

Managing Users

- Manage Users In Symphony
- Symphony User Personas
- Supplied Users And User Groups
- Add New Users
- Advanced User Management
- Modify Users
- Application Privileges

- View Active Logon Sessions
- Logon History
- Use Custom Attributes to Filter Data by User
- Using a Security Hierarchy to Filter Data by User
- Using a Security Hierarchy to Filter SSAS Data by User
- Using Custom Data and Custom Attributes to Filter SSAS Data

Groups

- Symphony User Groups
- Add and Remove Members of a Group
- Advanced Group Management
- Manage User Groups in Visual Data Discovery

Multi-Tenancy

- Multi-Tenancy In Symphony
- Create A New Tenant
- Create And Add Additional Tenant Admin Users
- Create Tenant Projects
- Define Access To Data Discovery Connectors

- Add And Edit Tenant Users
- Disable, Enable, And Remove Tenants

Licensing

- Manage Licenses
- About Symphony Licenses
- Cumulative Licensing
- License Types
- Multiple Servers
- Core Counts
- License Seat Modes
- Elasticity - Hours And Seats
- Configure Elasticity
- Seat Usage For Symphony Licenses
- Floating And Concurrent Logon Sessions
- SaaS And Multi-Tenancy License Assignment

Single Sign On

- Symphony Single Sign On
- Create And Use Logon And Session Tokens For Symphony

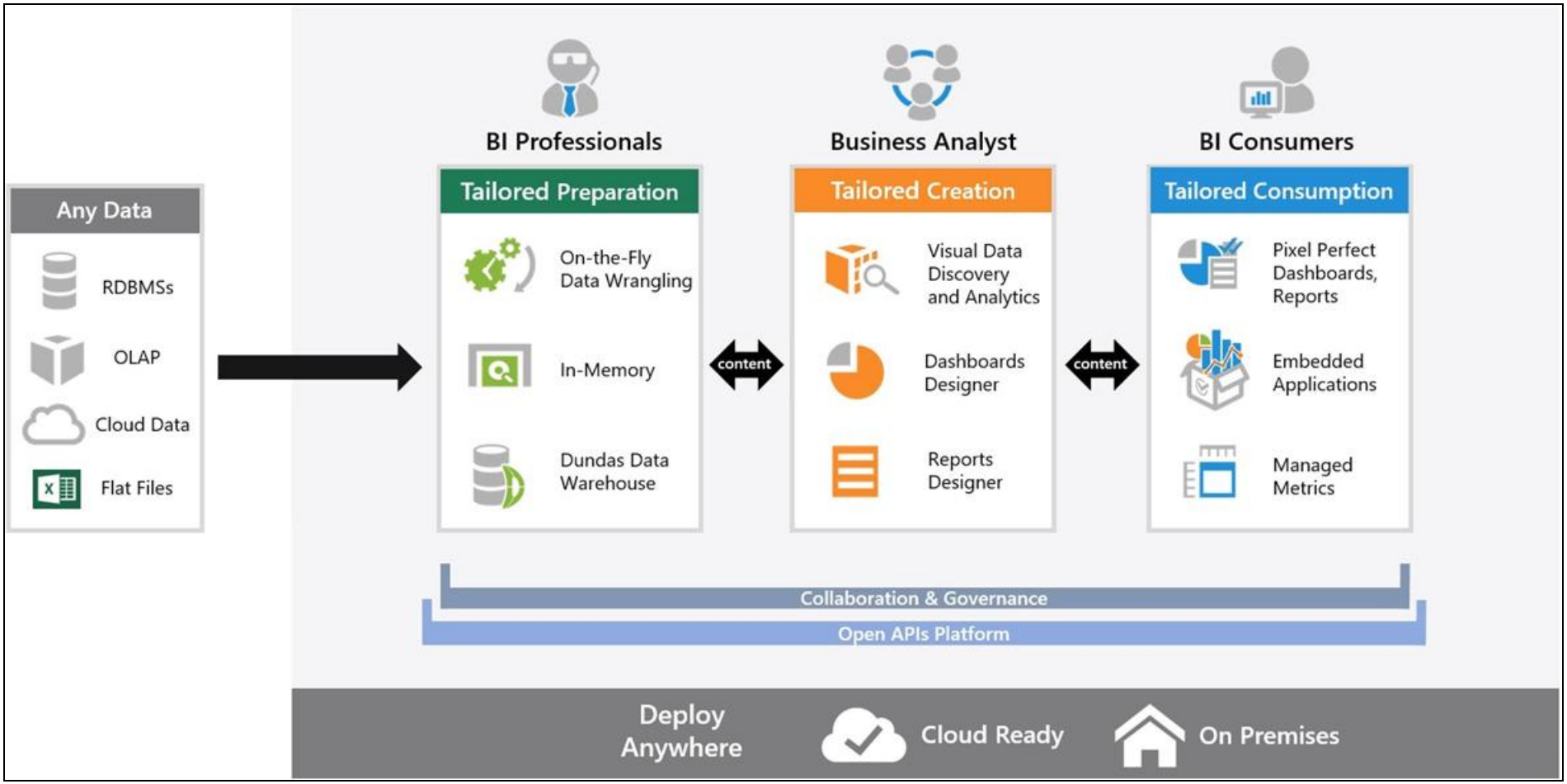
Configuration and Administration

- Application Logs
- Application Privileges
- Configuration Best Practices
- Configuration Settings
- Configuring Notifications and Other Scheduling Features
- Customize Branding for Each Tenant
- Dedicated Warehouse Databases for Tenants
- Enabling Active Directory Authentication From Multiple Forests
- Enabling Federated Authentication
- Advanced Group Management
- Health Check
- How To Enable Anonymous Log On
- How to Recycle the Application Pool

Product Overview

This applies to: *Managed Dashboards, Managed Reports*

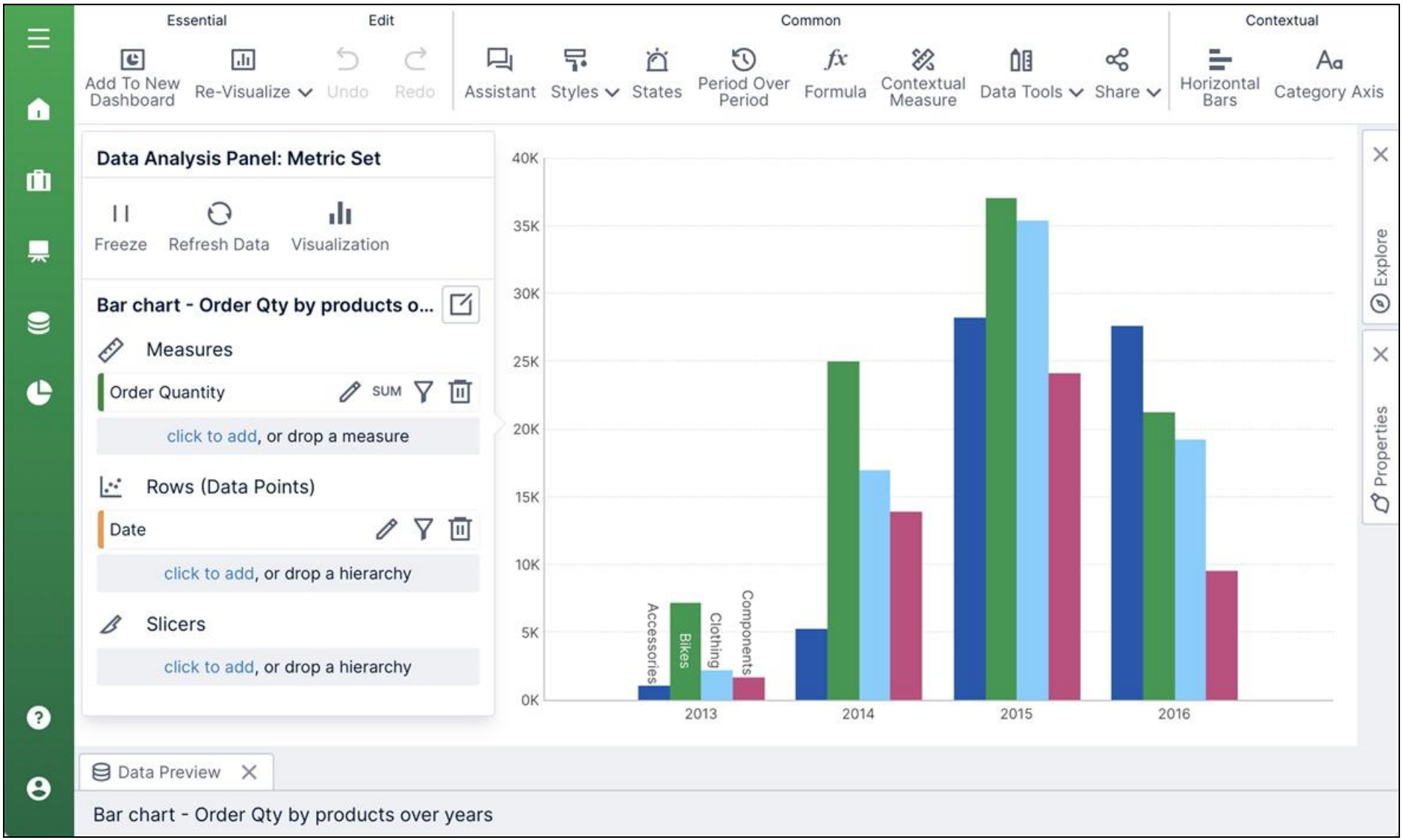
Symphony is a state-of-the-art embeddable business intelligence platform for data exploration, visual analytics, and creating & sharing dashboards, reports, and more. You can deploy it as the central data portal for your organization, or integrate it into an existing website as part of a custom or embedded BI solution. Symphony is flexible enough to adapt to your needs and to every type of user.



Key Benefits and Features

Self-Serve Business Intelligence

Symphony gives you the ability to perform data exploration and analysis, run ad hoc queries, and create your own dashboards and reports, all without having to involve your organization's technical or IT staff. Using the interactive screens in Symphony, you can easily explore available data sources, use intuitive operations to visualize your data, and arrange it in dashboard, multi-page report, scorecard, and small multiple views. Apply formulas using a familiar toolbar interface, access other analysis options with a single click, or ask the Assistant for help. Smart defaults and automatic data preparation are used throughout Symphony to provide a streamlined workflow, which means there are a lot fewer steps needed to progress from your data to desired visuals.



Fully Open APIs

Symphony itself was built on a completely open API platform designed for extensibility, integration, and embedding. Every capability you see in the user interface from administration through to analysis and views can be embedded, and is powered by public .NET, REST, and JavaScript APIs, which you have access to as well. You can insert your own custom extensions into virtually any part of the Symphony workflow using the same plug-in architecture used for built-in components,

including data providers, transforms, formulas, visualizations, export providers, and much more. Tailor to your needs using custom CSS and JavaScript, the familiar syntax of in calculations and advanced formulas, or the built-in JavaScript editor with pop-up help and suggestions.

HTML5, Mobile & Touch

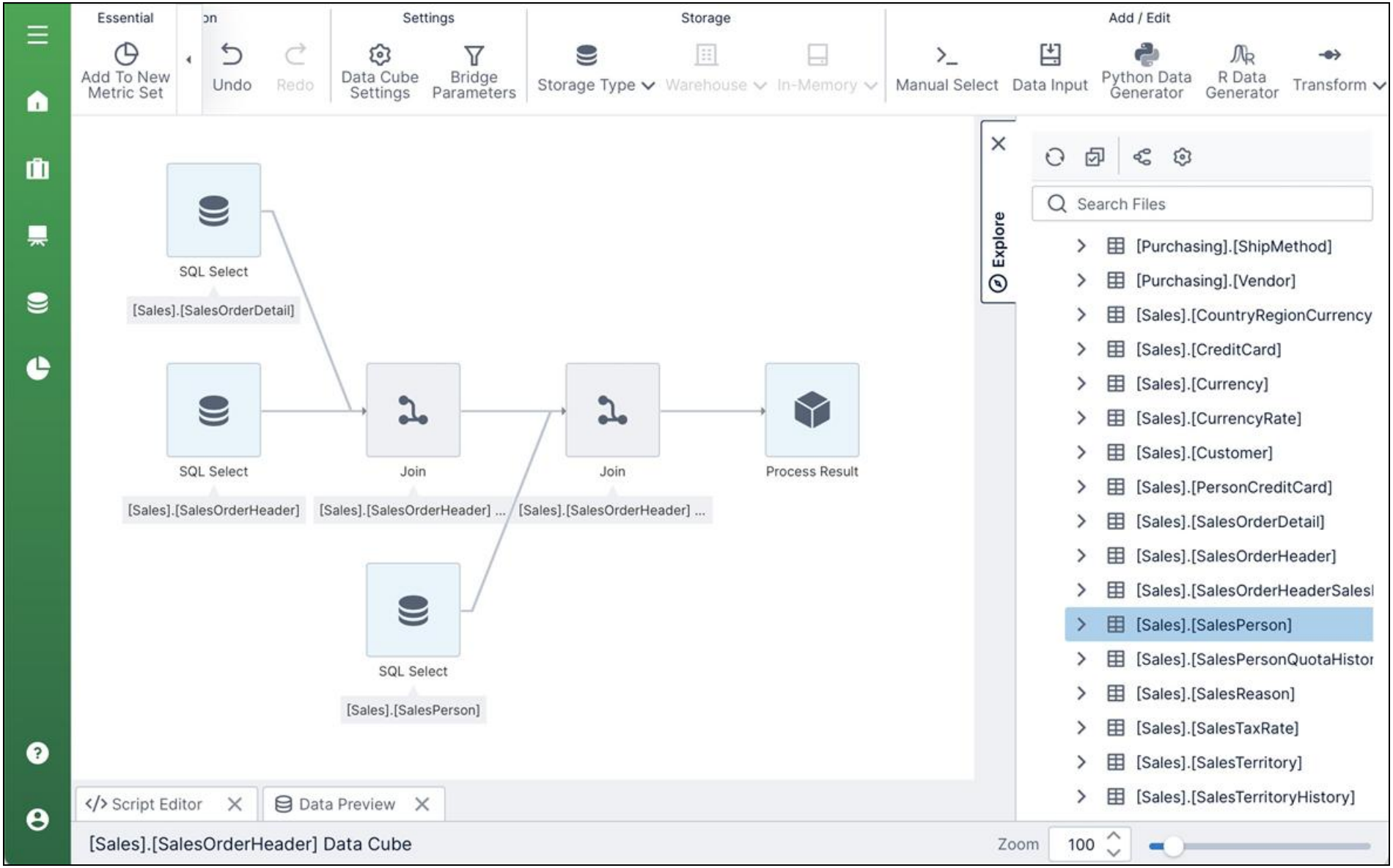
The client-side of the Symphony platform is based entirely on the latest web standards including HTML5, JavaScript, and CSS. There is no requirement for browser plug-ins, or for users to install software. This means Symphony works and looks the same on a desktop as it does on a mobile device such as a tablet or smartphone. The user interface of Symphony fully supports touch-based gestures so you can analyze data or design dashboards and reports directly on an iPad, or administer Symphony from your phone. All you need is a standards-compliant browser for your device.

Data Visualizations

Symphony provides a wide array of data visualization types you can use to analyze and view your data, including a complete chart library, maps, tables, gauges, relationship diagrams and more. Our visualizations are highly interactive and responsive, with intuitive animated transitions, and with performance and support for ad hoc analysis in mind. We've programmed our visualizations with styles and behavior that automatically conform to established best practices in data visualization, and smart visualizations can make choices and recommendations for you as you work with your data, including one-click advanced analytics. Each visualization is rich with features and customization options for optimal gaining and sharing of insights.

ETL Layer & In-Memory Analytics

Extract-Transform-Load (ETL) capability is built directly into Symphony via our data cube layer. A wide variety of transforms are available for you to add and connect together to perform data cleansing, integrate data from different sources, access machine learning and other advanced analytics with R or Python, and any other data preparation you may need. Data cubes can also store data input through a spreadsheet-like interface or through custom forms on dashboards. The output of a data cube is a reusable data model you can prepare with predefined formatting and metadata and share with others. Connect to your data live, store it as needed in our internal data warehouse for improved performance, or build it as an in-memory model to enable even faster analytical query results.



Administration & Configuration

Symphony provides a flexible data security model, which includes complete built-in support for optional multi-tenant / SaaS deployment. You can use whatever form of authentication you need for seamless integration with your own applications or systems, with a variety of standard protocols ready to use. For scalability,

load balancing is supported through the use of application and data processing server groups, and containerization and Kubernetes support for scaling on cloud or server cluster deployments. Authorized users can access administrative tasks with one click from Symphony's menu, using intuitive interfaces to manage the complete set of configuration settings, logs, licensing, user account management, and other application functions, without additional tools.

Log on to Symphony

This applies to: *Managed Dashboards, Managed Reports*

Since Symphony is web-based, all you need is a web browser to get started. Just navigate to the Symphony website address and log in with your account information.

Depending on how Symphony has been installed or hosted, the URL could look like any of the following:

- https://servername/
- http://servername:8000/
- https://servername.example.com/

If you're logged onto a Windows server computer where Symphony was installed, you can also launch the Symphony instance from the Start menu.

Symphony Login Screen

When you navigate to the URL for Symphony, you should see the login screen.

Enter your Symphony **Login Name** and **Password** if you have them, and then click the **Log in** button.

If you have just installed Symphony yourself, the default logon name is **admin** and the password is the one that you specified during the installation procedure.

You can also register for a new account as shown below, or contact your Symphony administrator directly to obtain a login name and password if you prefer.

Log on Using Windows or Another Provider

Different login options may appear if your Symphony instance was configured to use another identity provider.

In this case, click the corresponding button instead, such as **Log in with Windows** for Windows authentication.

If you are using Windows authentication, an alternative is to specify your domain-qualified Windows user name in the Logon Name field. Depending on the Windows user name format indicated by your Symphony administrator, you may use either the default NT4 format *(DOMAIN\UserName)* or the User Principal Name *(UserName@Domain.com)*.

Register For a New User Account

If you don't have a Symphony user account, you can register for one by clicking the **Register** button. You'll be able to log in after your Symphony administrator approves the request.

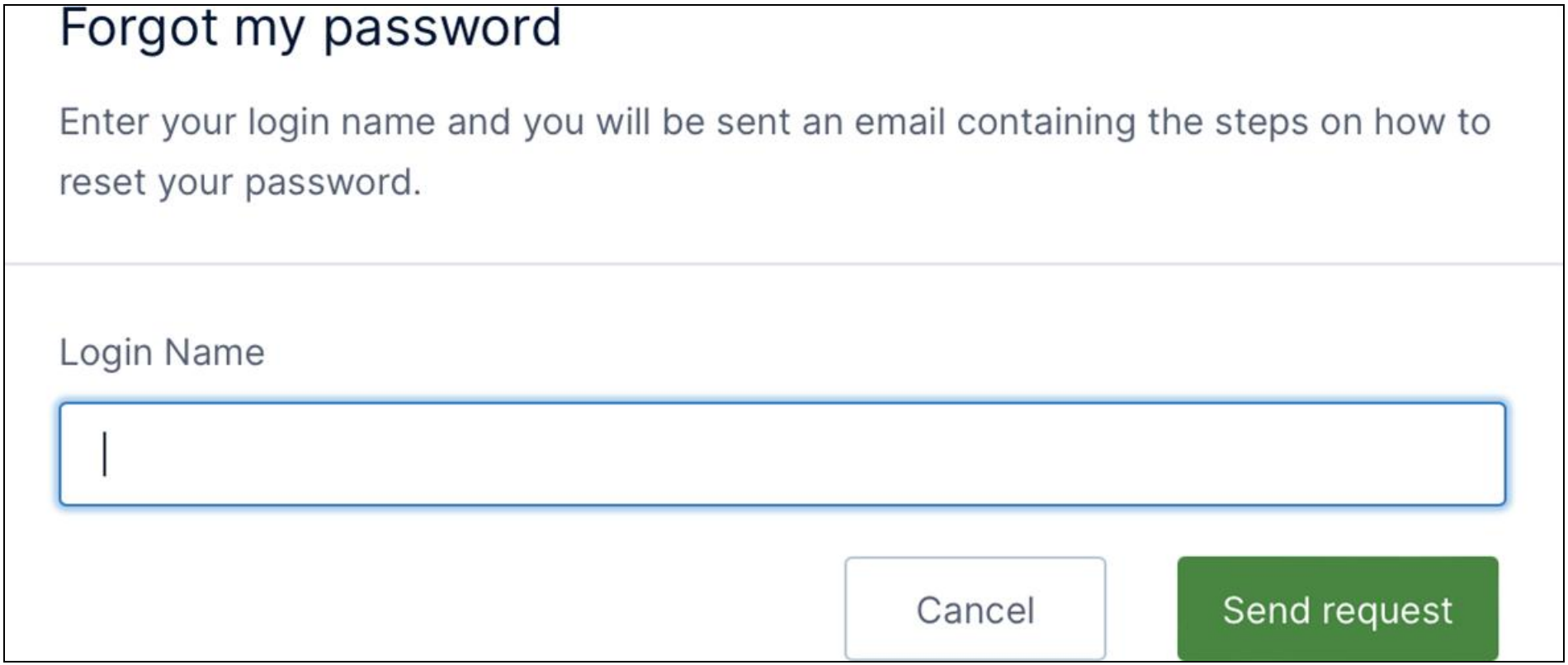
Under *Register new account*, enter the following information:

- your email address
- an login name, which you will use to log on with (can be the same as your email address)
- a display name (visible to other users)
- an optional message for the administrator to read when seeing your request

Reset Your Password

If you have forgotten your password, click **Forgot password**.

Enter your **Account Name** and then click the button below to send your request. You'll receive an email with instructions for resetting your password.



For more information, see

- Home Page
- How to Reset the Admin Password

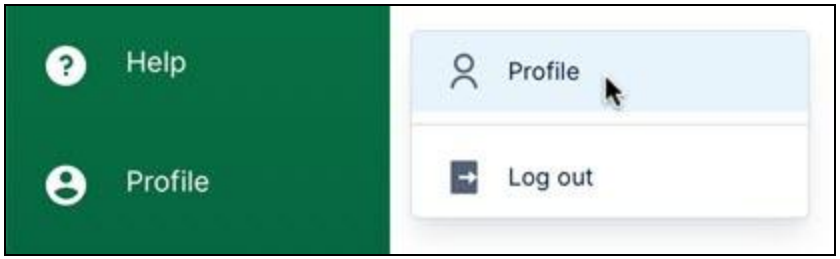
Edit Your Profile and Change Your Password

This applies to: *Managed Dashboards, Managed Reports*

My Profile lets you view your user account details, choose what you see when you log on, change your password and more.

From the main menu, select **Profile**. This opens a menu of account-related items – select **Profile** again to open the full profile dialog and:

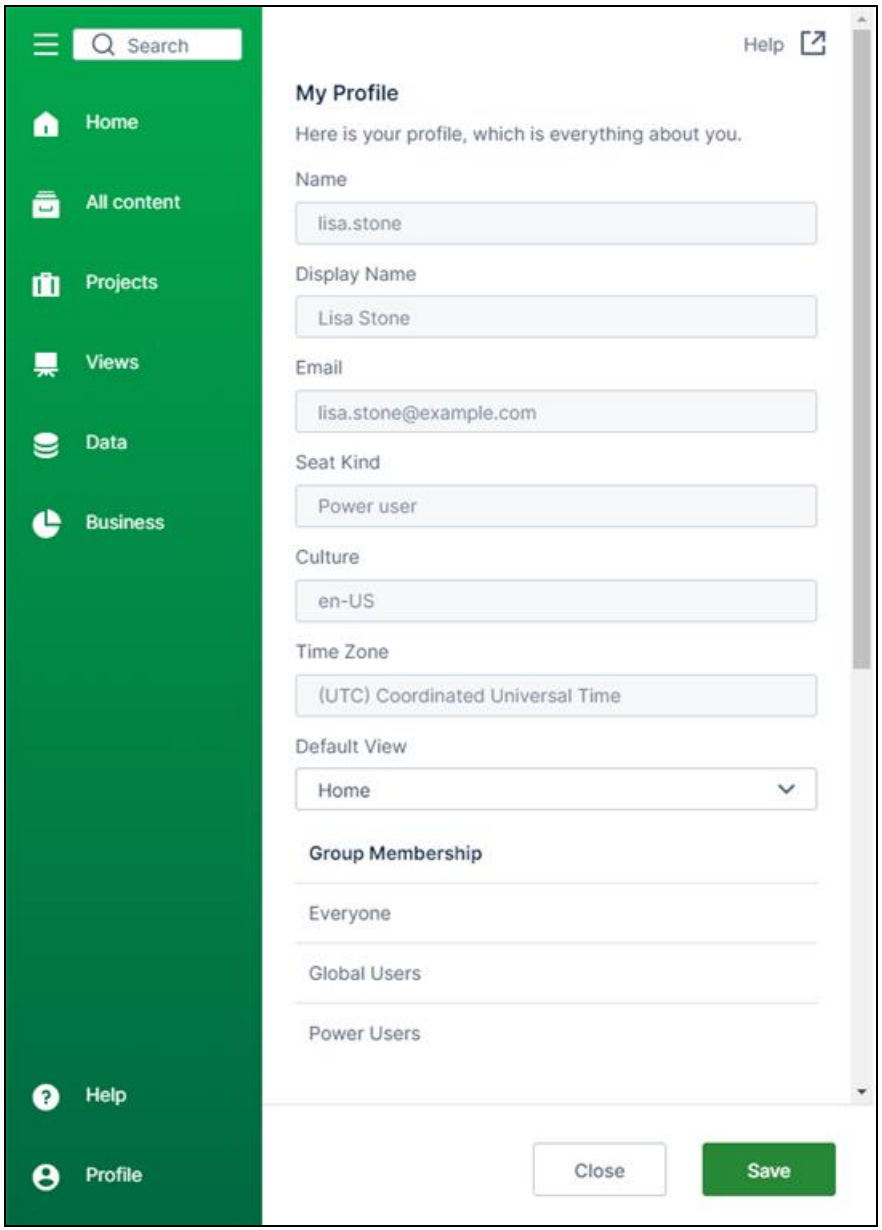
- View information about your user account.
- Set up a default view such as a favorite dashboard to appear each time you log in.
- Turn touch events on or off.
- See a list of recently deleted files and recover them.
- View and manage any notifications you've created.
- Find your export history and download exported files.
- View a list of data cubes you have access to and their storage job status.
- Create and manage custom tokens to use when filtering data.



View User Information

The *My Profile* dialog shows you the following read-only items of information related to your user account:

- Name – This is your username (i.e., the name you use to log in).
- Display Name – Usually your real name which shows up in different places in the user interface.
- Email – The email address associated with your user account.
- Seat Kind – The type of license seat assigned to your user account:
  - *Standard user* – You can create views such as dashboards, reports, scorecards, and slideshows.
  - *Power user* – You can create data connectors, hierarchies, time dimensions, metric sets, and views.
  - *Developer* – You can do everything a power user can do, plus create data cubes and cube perspectives.
- Culture – The name of the culture (e.g., en-US) associated with your user account, if any.
- Time Zone – The time zone for your user account.
- Group Membership – A list of groups that you belong to.

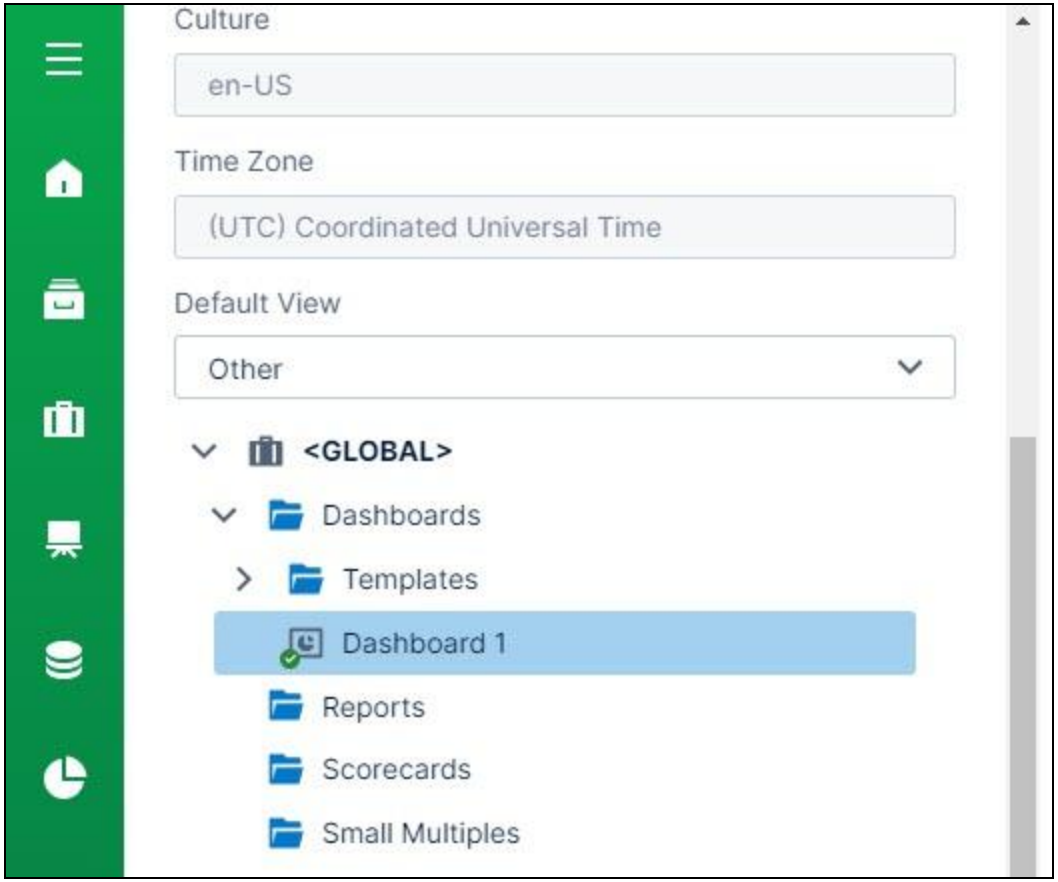


Contact your administrator if you want to change any of these details.

Set the Default View

The **Default View** option lets you decide what to show after you log in. When set to *Home*, this shows the default home screen.

Alternatively, set this to *Other* and select a specific dashboard, report, or other view to display instead. (Switch projects if necessary before opening your profile dialog.)



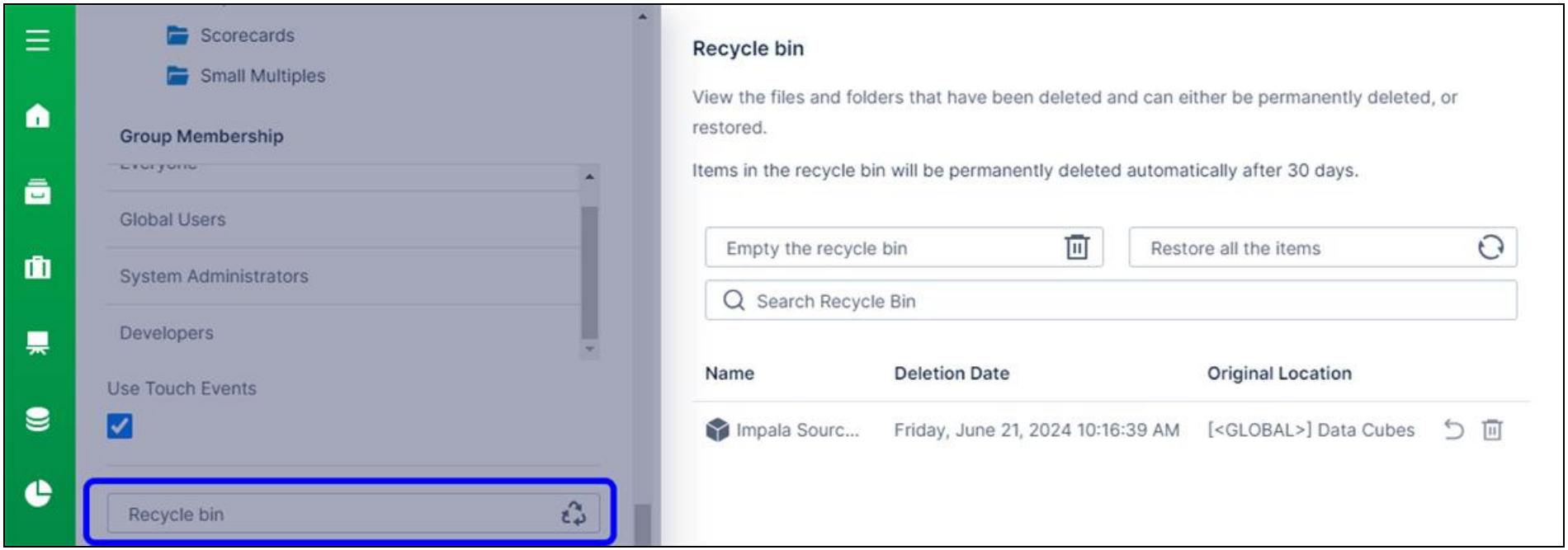
Use Touch Events

The **Use Touch Events** checkbox allows you to force touchscreen interactions on or off.

For example, you can enable this option if you have a device that supports both touch and mouse/trackpad interactions such as a touchscreen laptop. Otherwise, your input device is normally detected automatically and should work without you changing this setting.

Recycle Bin

If you deleted an item by accident, or changed your mind, click *Recycle bin* to find the list of recently-deleted files and folders. You can either restore or permanently delete each item using the icons along the right.

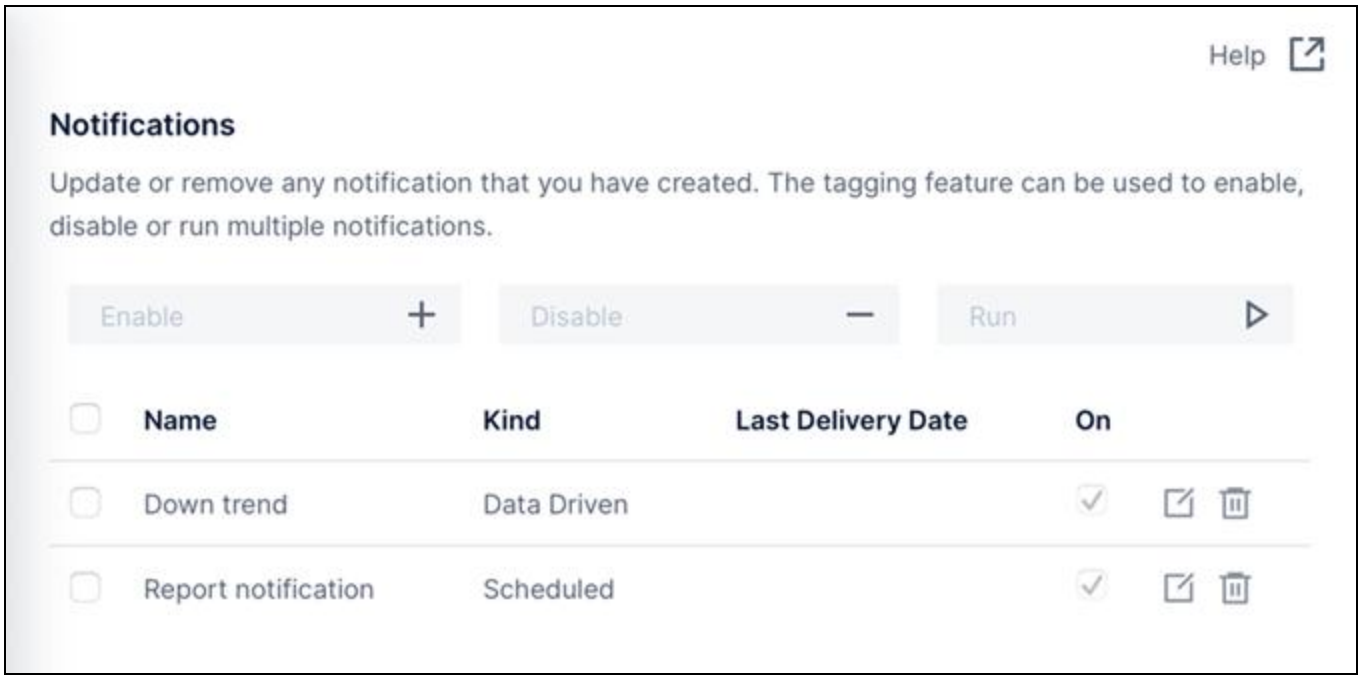


Recycled items will be permanently deleted automatically after a set amount of time, which is configurable by your administrator.

Manage Notifications

Notifications offer a way to send emails or other alerts on a periodic schedule or if data meets certain conditions, and deliver an image or data export from the dashboard, report, or other view it was created from.

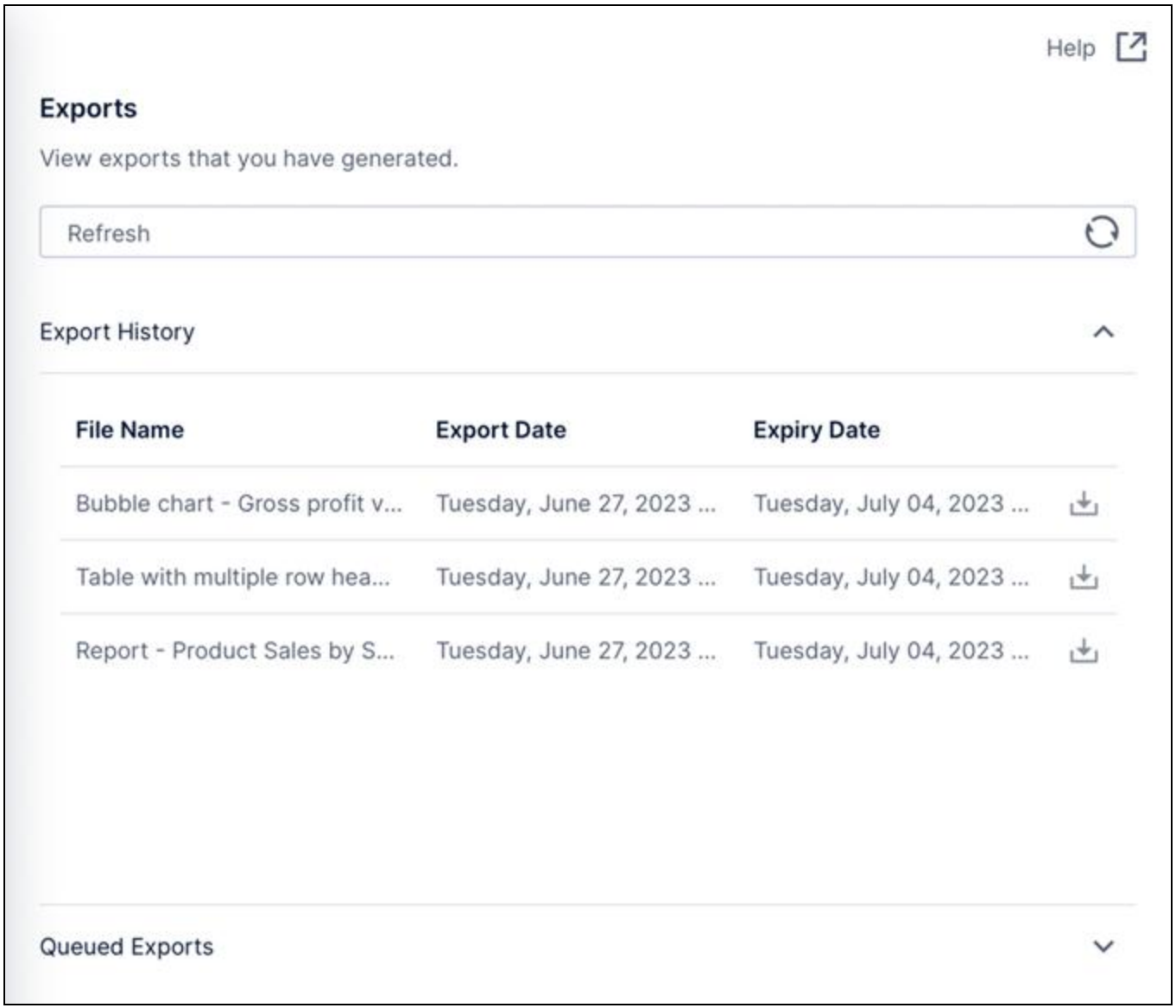
Click **Notifications** to view a list of notifications you've created, with options to enable/disable, run, edit, and delete them.



Manage Exports

Click **Exports** to view the list of files you exported from a dashboard, report, or other view.

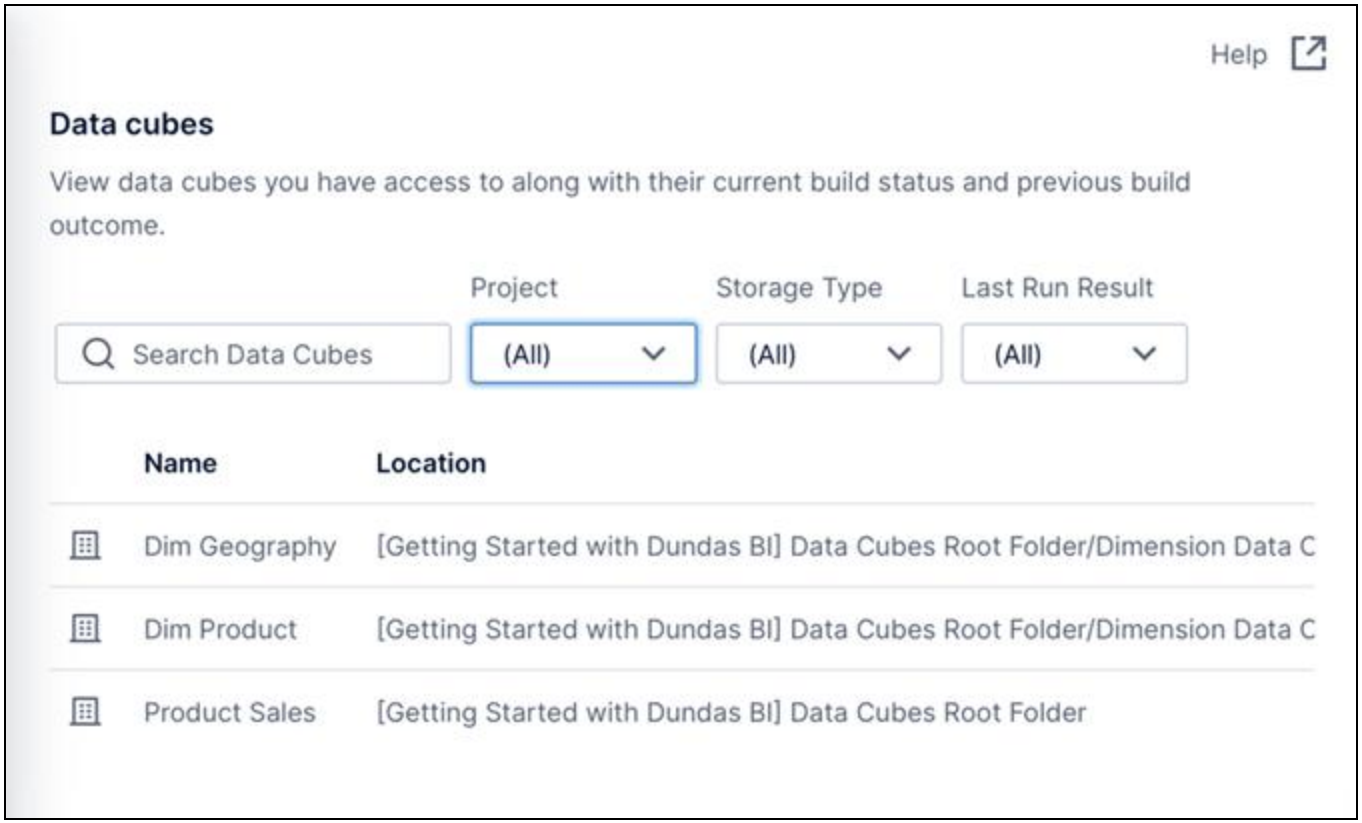
Click the download icon next to an export in the **Export History** section to download the file, or expand the **Queued Exports** section to monitor or cancel any longer-running exports currently in progress.



Data Cube Status

You can view details about data cubes you have access to, including their build status for data cubes using warehouse or in- memory storage options (as indicated by their icons).

Click Data cubes from your profile. You can view and filter data cubes by project, storage type, and build status, with each storage job's *Schedule, Job Status, Last Run Date,* and *Last Run Result* listed.

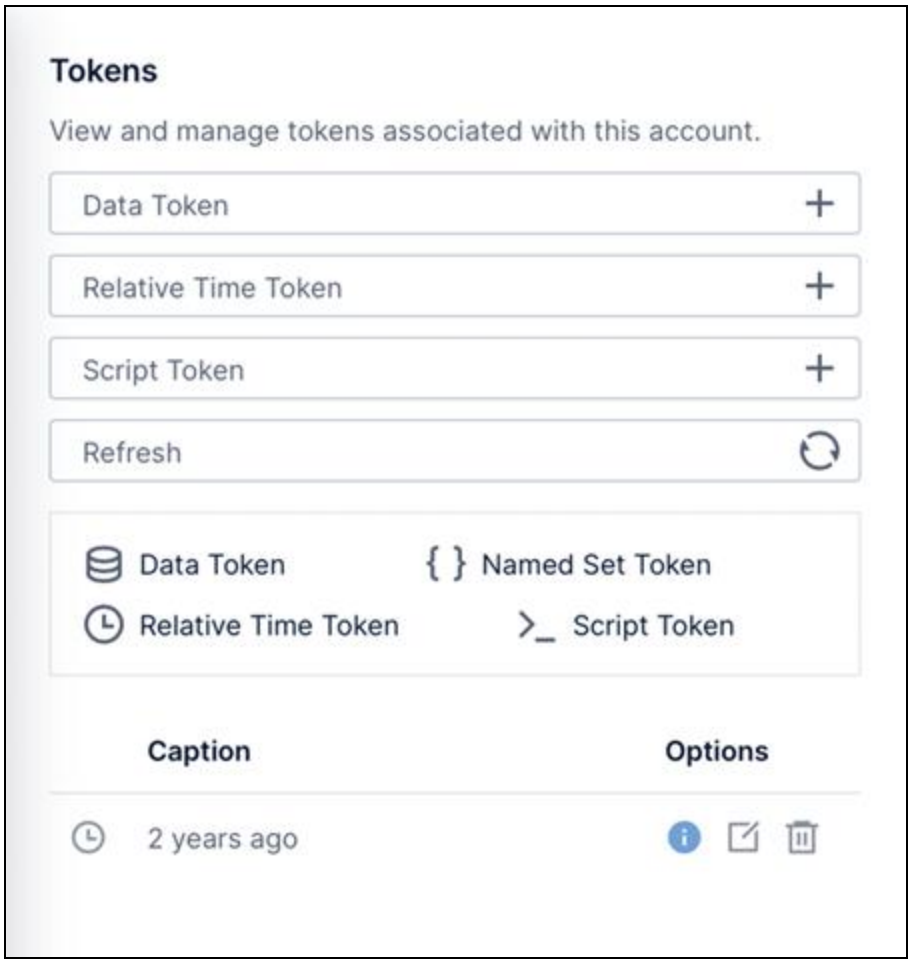


You can also right-click a data cube and choose **References**. This is a shortcut to the same *References* dialog available from the file properties, allowing you see data cubes and other files that refer to or are referenced by this data cube.

Manage Tokens

Filters provide a menu of tokens you can choose for more options besides specific data source values, such as tokens that change over time like *Year to date*. You can create your own to choose from when filtering data in addition to the built-in tokens.

Click **Tokens** in your profile to manage the custom tokens associated with your account and to create some types of custom tokens.



Clear Personalization

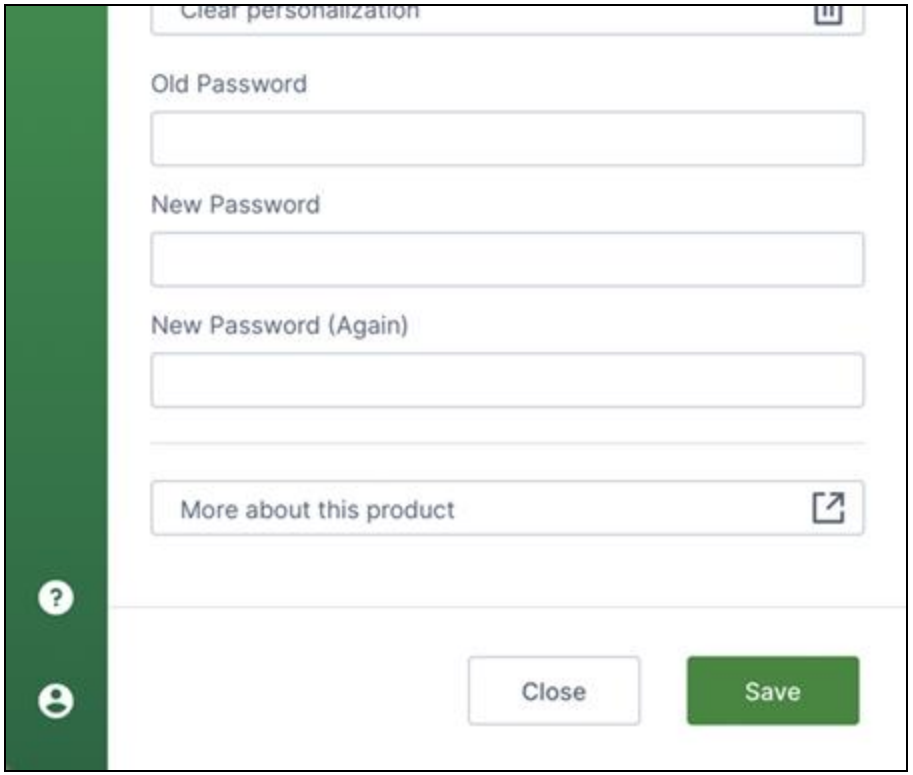
When enabled, personalization automatically saves customizations you make when with a dashboard, report, or other view open, such as filtering and sorting when viewing one that's checked in, or the arrangement of dockable windows when editing.

Click **Clear personalization** to clear these customizations and reset these options to their initial settings.

Change Your Password

To change your password, scroll down toward the bottom of the *My Profile* dialog and click **Change password**.

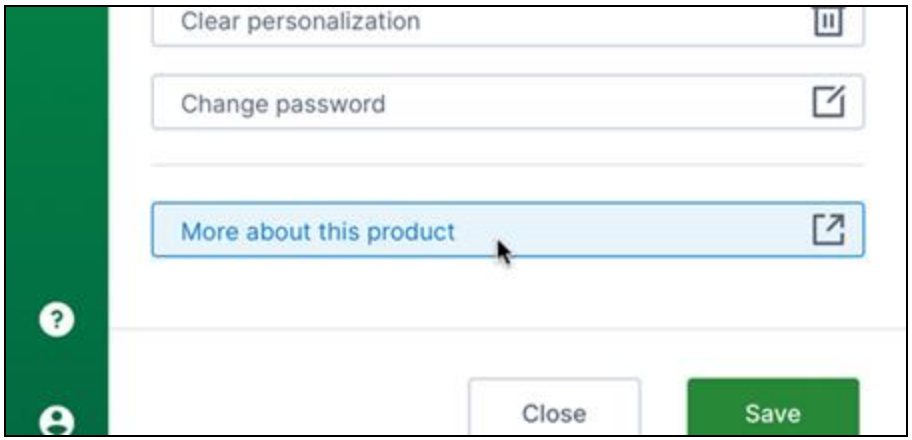
Enter your old password, enter your new password twice, and then click the save button at the bottom-right of the dialog.



Product Version and Other Information

Scroll all the way down and click **More about this product** to view information about the software instance that you are using in a new browser window or tab.

Administrator users see more detailed information.



For more information, see:

- Home Page
- Dashboard Editing Export Options
- Symphony Notifications (Alerts)
- Using Personalization
- Creating Custom Tokens

Using the Status Bar

This applies to: *Managed Dashboards, Managed Reports*

The status bar normally appears at the bottom of the screen, and contains several key features. The status bar is also known as a taskbar.

Elements of the Status Bar

After opening any file that you work with full screen like a dashboard or metric set, the status bar normally appears and contains some or all of these common elements.

The figure below illustrates the different parts of the status bar as seen when editing a dashboard:

Note: Hover over or long-tap part of the taskbar for to see details about it in a tooltip popup.

Name of the Item

The name of the file you currently have open (e.g., metric set or dashboard) is displayed on the left side of the status bar. Double-click the name in the status bar to rename it.

To find out which project and folder contains the current item, you can hover over (or long-tap) the name to view its full location in a tooltip popup.

Status Message

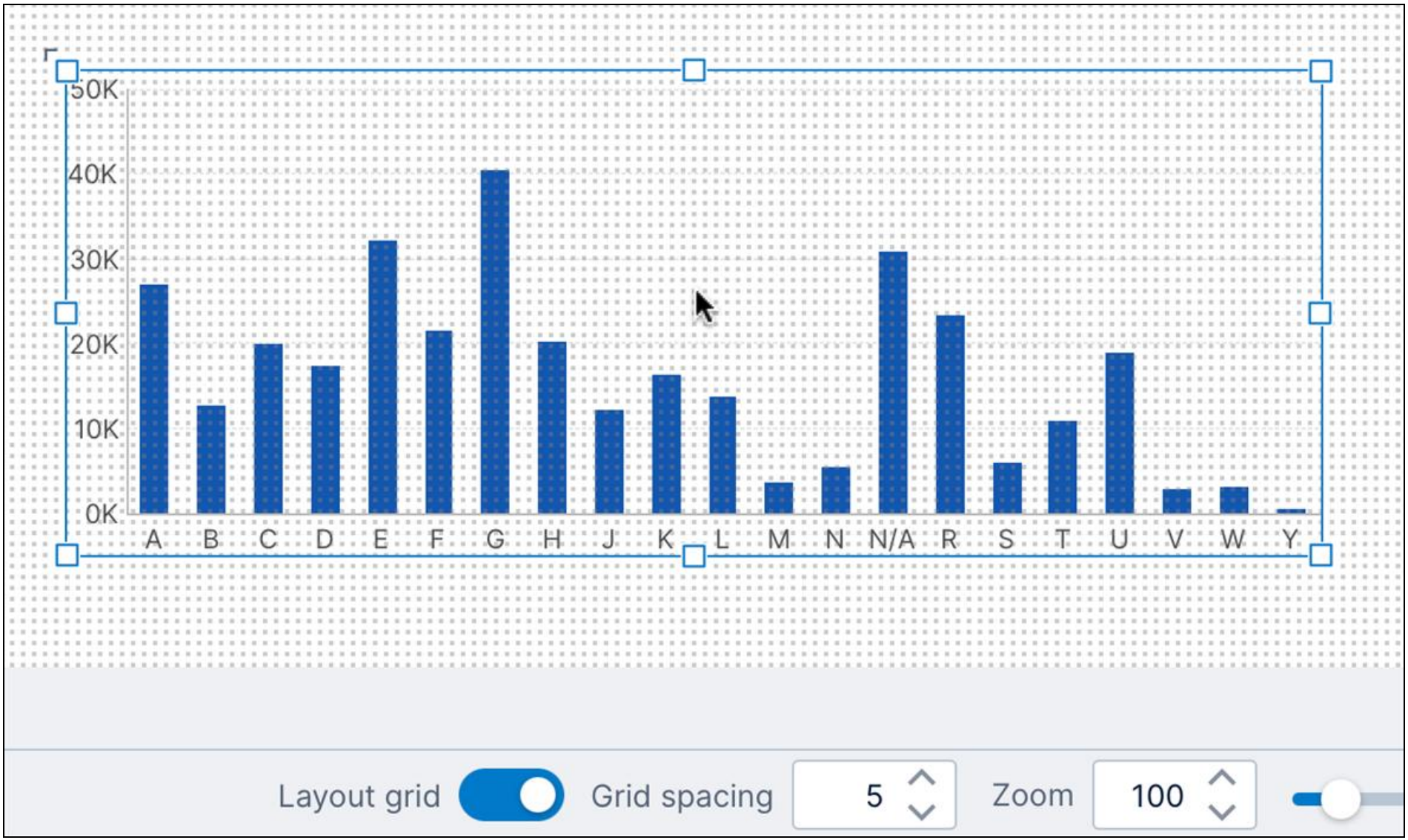
Beside the name of the item is a section for status messages. For example, if you make any changes to the file you're working on, you'll see a Saved message appear in the status bar when your progress is automatically saved.

Snap to Grid

When editing a view with a canvas, such as a dashboard or report, the snap grid options are available.

If the snap to grid option is enabled in the status bar, you'll see the grid of dots while you drag components around on the canvas. Positionally, components will always be lined up with the grid dots when snap to grid is enabled, which makes it easy for you to align and leave consistent spacing between components.

The default spacing between grid dots is *10* pixels. You can increase or decrease this from the status bar.



Note: If you turn off the snap to grid option, the component being dragged will still be snapped against other components on the canvas. If you don't want this behavior, press Alt while dragging your component.

Zoom Level

Screens such as dashboards, reports, and data cubes allow you to zoom in or out.

The canvas zoom level is normally 100 percent but may be set up to scale automatically to fit your screen. A higher value for the zoom level means you are *zoomed in* (everything appears larger). To change the zoom level, type in a new zoom percent value, use the up/down controls, or move the zoom slider.

You can reset the zoom level back to its initial level by double-clicking the zoom slider or by using the **Reset Zoom** button.

Note: You can also use keyboard shortcuts to zoom in or out, or use pinch-to-zoom or double-tap gestures on touch devices.

View Panel

When zooming and scrolling is available on the screen, a *view panel* popup appears when moving the mouse over the zoom level controls on the right side of the status bar.

This indicates what part of the entire canvas is currently visible using a blue rectangle. Dragging this rectangle is an easy way to quickly pan across your dashboard, and an alternative to using scrollbars to access the parts of your dashboard that are scrolled out of view.

Data Summary

When selecting rows or columns in a table visualization, or data points in a chart, some basic statistics of that data will appear in the status bar.

When editing a dashboard or other view, you can either open Data Preview and select data in its table, or switch to **View** in the toolbar to select data in visualizations.

See Metric set analysis tools for more details on displaying a data summary.

Using Dockable Windows

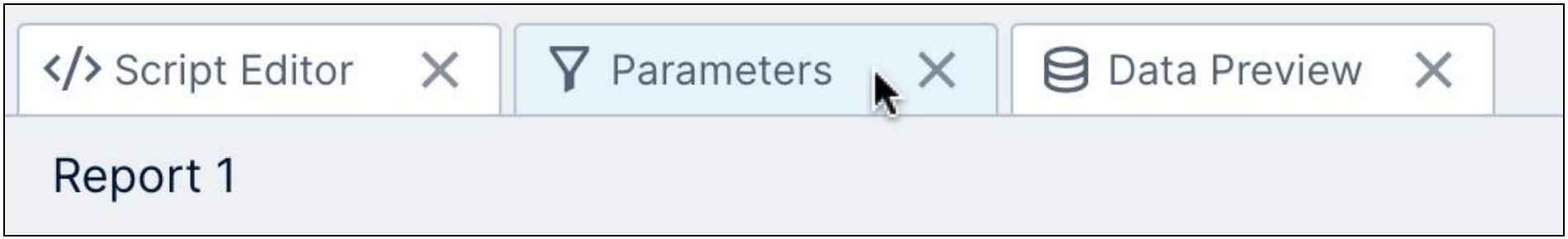
This applies to: *Managed Dashboards, Managed Reports*

A set of tabbed windows (or panels) are docked along the bottom and right sides of most editor screens, such as the Explore window.

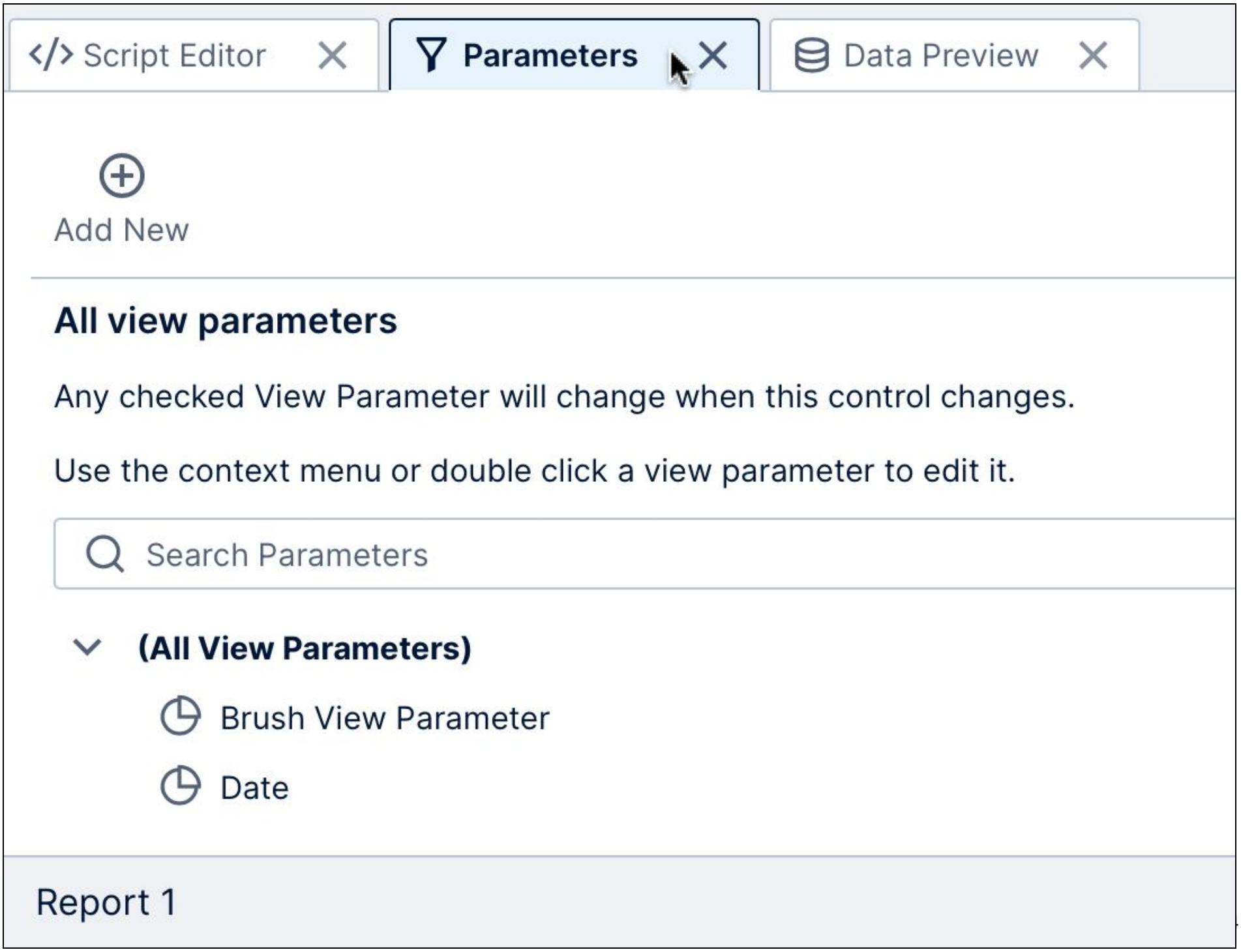
Simply click on one of these tabs to open or switch to it. For other tips, see below.

Expand and Collapse

When all the windows along one side of the screen are collapsed, click on a tab to open or expand that window, making it the active tab.

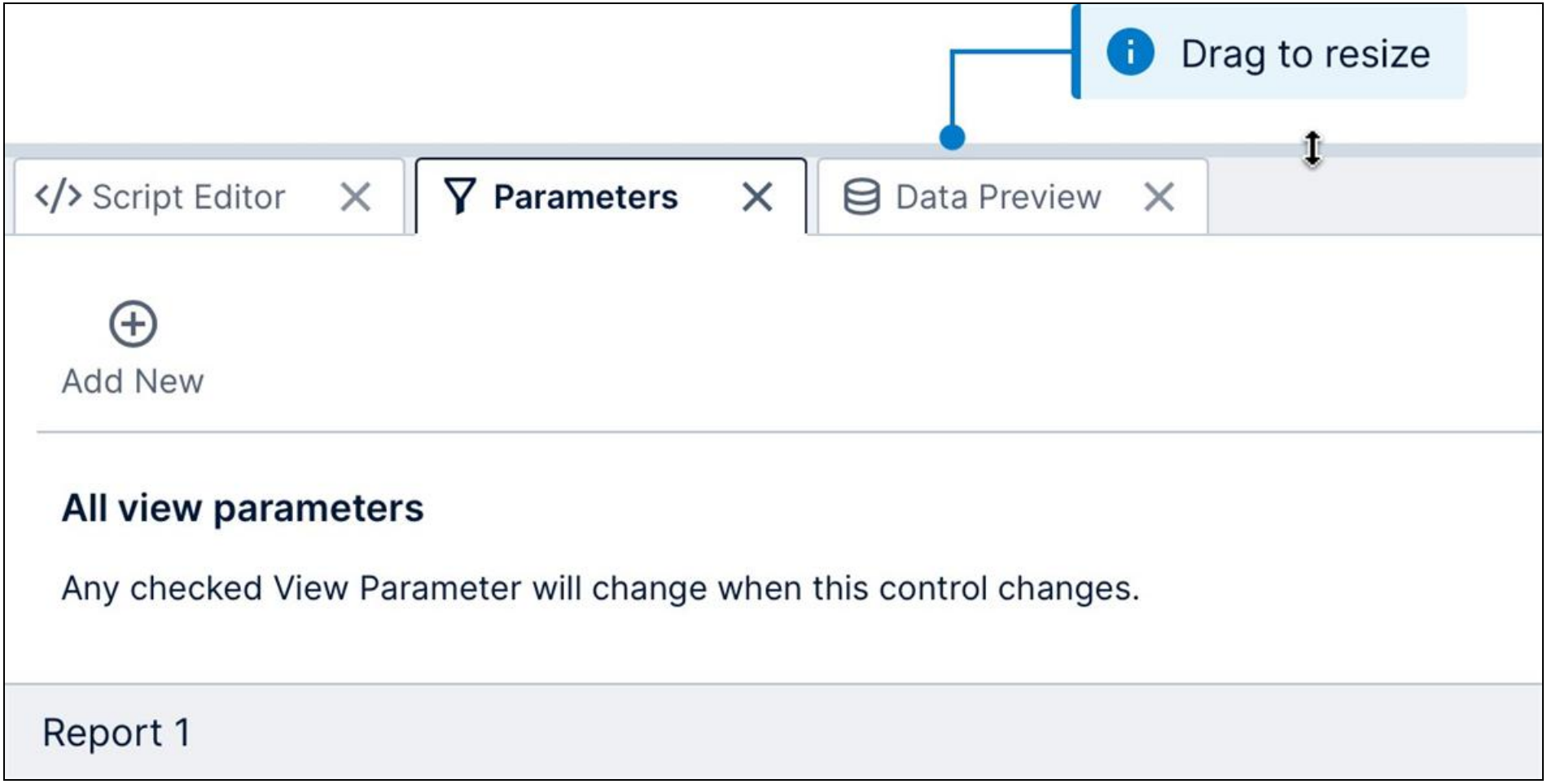


To collapse the window that is currently open and free up space on that side of the screen, click on the active tab.


Script Editor
Parameters
Data Preview
Add New
All view parameters
Any checked View Parameter will change when this control changes.
Use the context menu or double click a view parameter to edit it.
Search Parameters
(All View Parameters)
Brush View Parameter
Date
Report 1

Resize a Window

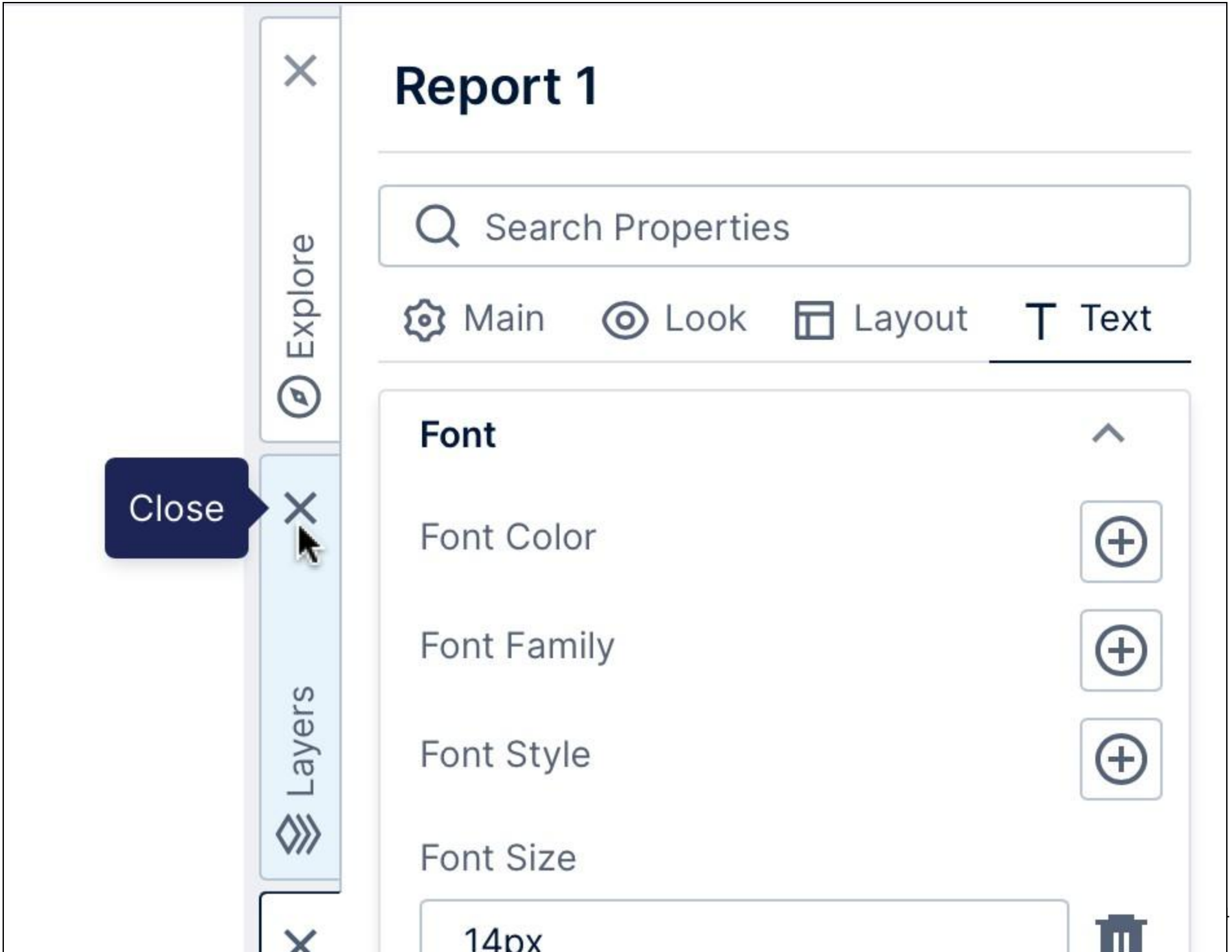
Resize an expanded window by clicking and dragging its inside edge.



Closed or Minimized Windows

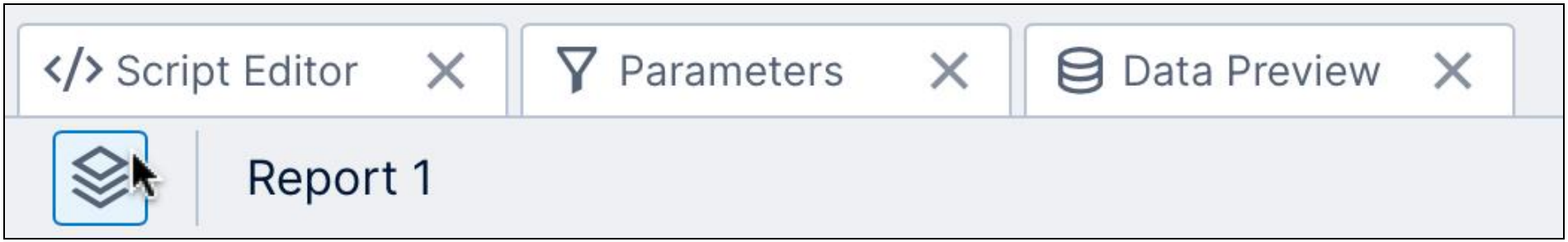
Each window can also be closed (or minimized), moving it from the side of the screen to a small icon in the status bar.

To do this, click the **Close** button on the window tab.


Report 1
Search Properties
Main
Look
Layout
Text
Font
Font Color
Font Family
Font Style
Font Size
14px
Explore
Layers
Close

Windows may close themselves automatically if you switch to a small screen such as a smartphone, or resize your browser window very small.

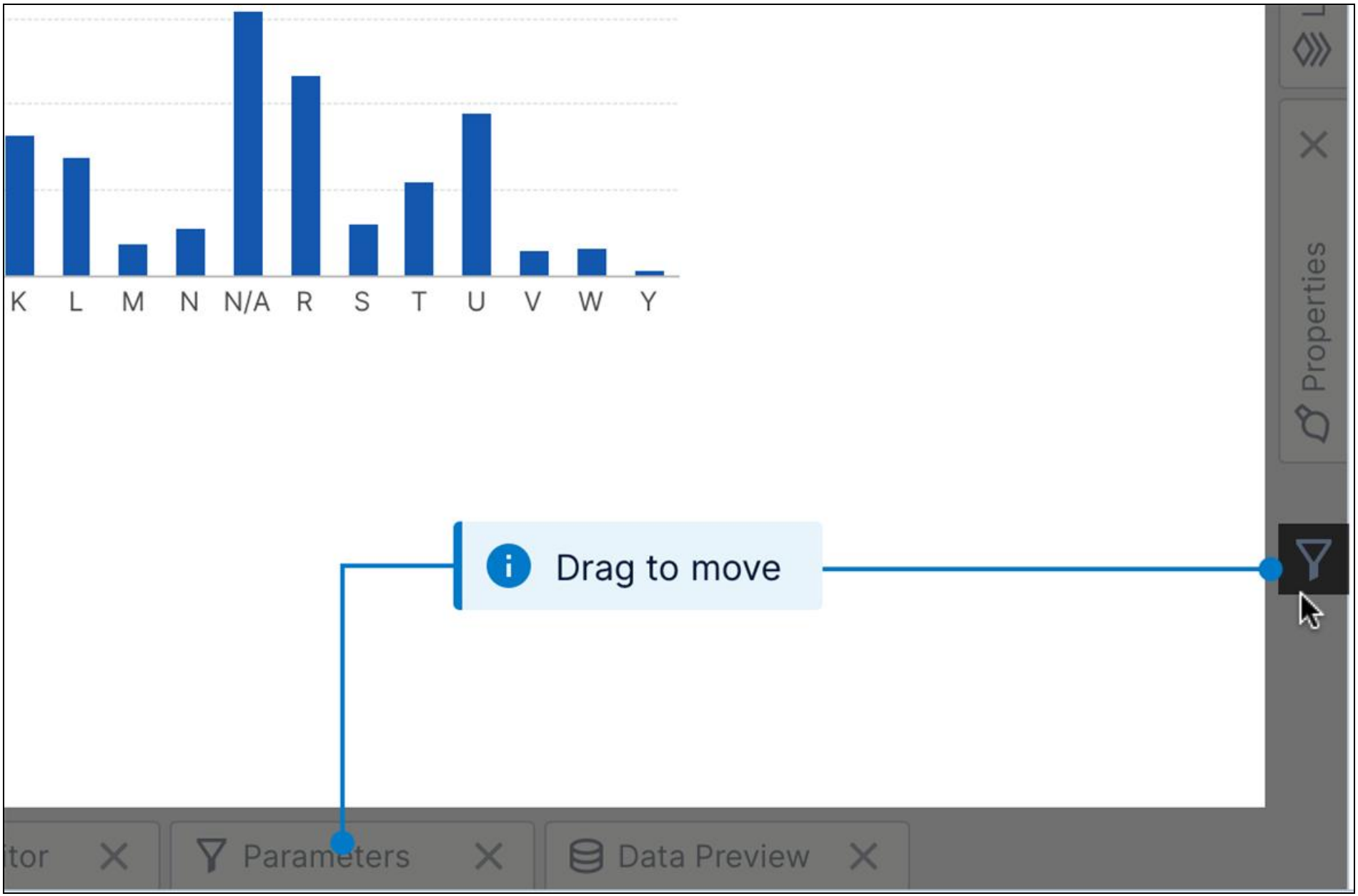
To reopen or restore a closed window, go to the left edge of the status bar at the bottom of the screen and click the window's icon.



You can hover over or long-tap the icon to view its description in a tooltip popup if you don't recognize its icon.

Change the Docked Location

You can reposition any docked window from the right side of the screen to the bottom side or vice versa by dragging its tab. For example, drag the **Parameters** window and dock it on the right instead of the bottom.



A window may move itself automatically to another side of the screen if the window is too small to fit all of the tabs currently positioned there, but you can drag it back again once there is room.

Rename an Item

This applies to: *Managed Dashboards, Managed Reports*

You can rename items such as dashboards, metric sets, and data cubes from the status bar when it's open, or you can use the Explore window or another file explorer.

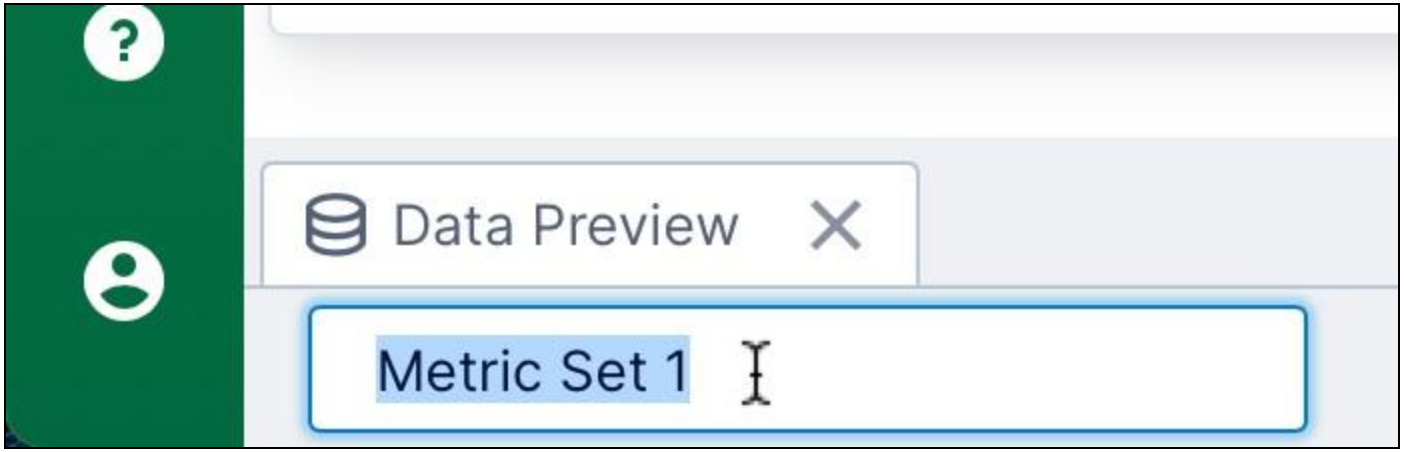
Rename From the Status Bar

When you have an item open, its name appears in the status bar at the bottom of the screen.

Note: Hover over or long-tap the name to also see its location, including what project contains it.

Double-click the name of your item to modify it.

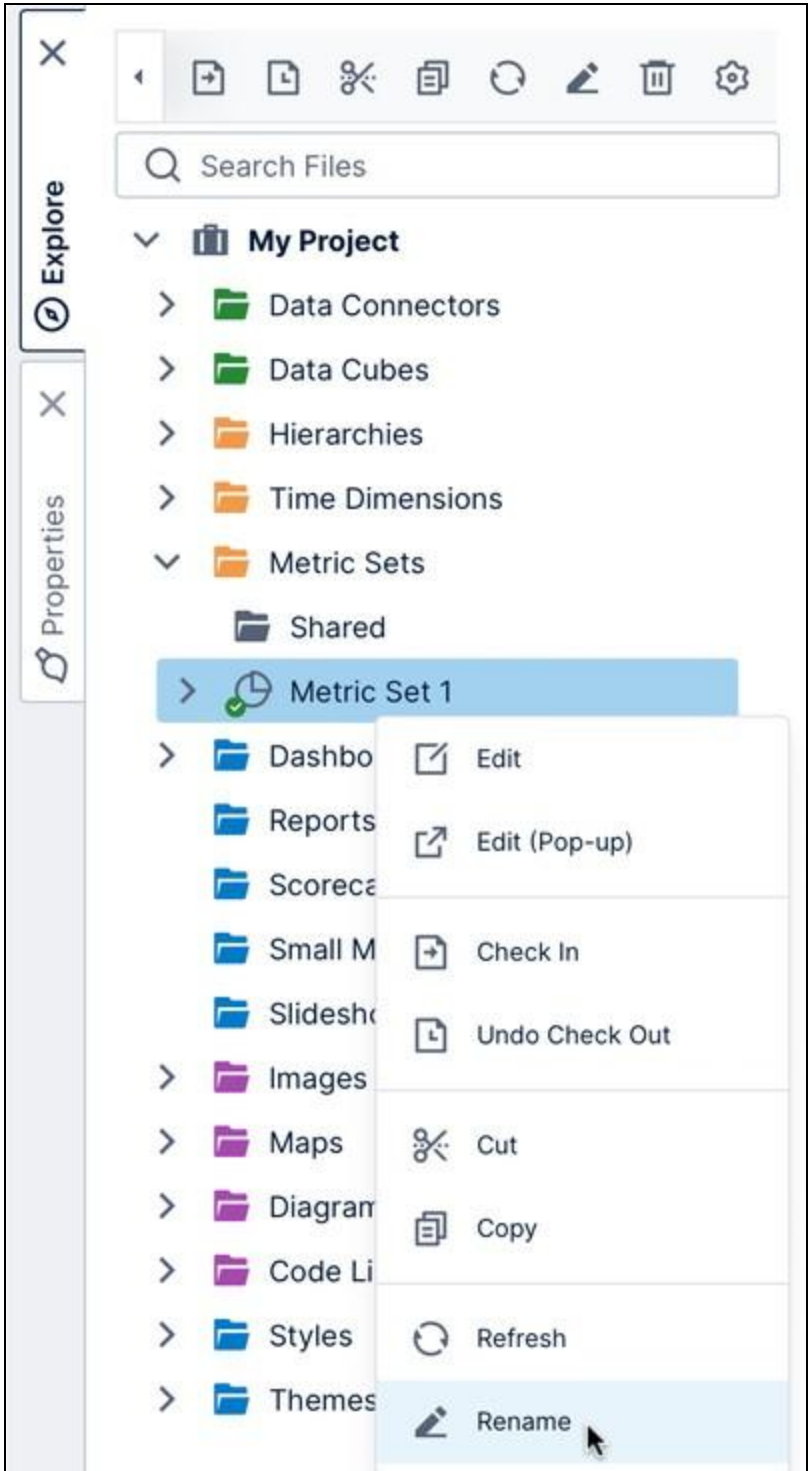
Make your changes and then type the enter/return key or click somewhere else.



Rename From a File Explorer

You can use any file explorer to rename an item, such as the Explore window or in an *Open* dialog. This works even when you have a different item open.

Right-click or long-tap the item, and then **choose** Rename from the menu.


Explore
Properties
Search Files
My Project
Data Connectors
Data Cubes
Hierarchies
Time Dimensions
Metric Sets
Shared
Metric Set 1
Dashbo
Reports
Scoreca
Small M
Slidesh
Images
Maps
Diagram
Code Li
Styles
Themes
Edit
Edit (Pop-up)
Check In
Undo Check Out
Cut
Copy
Refresh
Rename

Rename Using the Properties Dialog

You can also rename an item from its file Properties dialog in the same situations as above:

1. Right-click or long-tap the item, and then choose **Properties** from the menu.
2. In the Properties dialog, change the **Name** and then click to save at the bottom of the dialog.

For more information, see:

- Home Page
- How to Reset the Admin Password
- File and Folder Properties

Symphony User Personas

Symphony user personas are designed to allow you to give your users the flexibility they need to perform the day to day and occasional tasks needed to manage your data and environment. The primary user personas are users who perform frequent tasks in Symphony. Other user personas provide more back end support for your environment, such as installation, upgrades, and security tasks.

Data Author

As a Data Author, you create the environment your users access and interact with. Using the content user interface, you can create and update connections, create sources, data cubes, and data connectors, define groups, set data level security and object level permissions. You'll also create dashboards, reports and visuals for other users.

Content Author

As a Content Author, you can manage the information your users access and interact with. Using the content user interface, you'll create dashboards, reports, and visuals for other users. As needed, you'll also define object level permissions for users in your environment and self service users in embedded environments.

In embedded Symphony environments, you'll have access to Symphony content you embed in your app and the Symphony self service user interface. Here you'll create sources, data cubes, data connectors, and perform data transformation (ETL) to enable other self service users. As needed, you can schedule and share content you have created or can access to users at your level or to Consumer users, including visuals, dashboards, and dashboard reports.

Self Service User

In embedded Symphony environments, you'll have access to Symphony content you embed in your app and the Symphony self service user interface. Here you'll create visuals, dashboards, and reports as needed. Schedule and share content you have created to users at your level or to Consumer users.

Consumer

As a consumer, you can view all dashboards shared with you. Schedule dashboards, visuals, and reports for other consumers. Other users may send you email notifications, reports for review, and share dashboards and visuals.

Administrator

As an Administrator user, you install and upgrade Symphony, configure the environment, and manage apps and access to your instances and embedded resources.

- Environment: Install, Configure, Deploy, and Upgrade Symphony, and monitor system health
- Users: Enable system users, user access, and their connection through identity providers
- Manage Applications: Configure security access, identity provider access, database access, object migration, application health

Note: Some specialized tasks, such as connector management and multi-tenancy management, are performed by system administrators. See Supplied Users and User Groups.

Additionally, you'll customize and define the environments available to your users.

	Stand Alone	Embedded (Self Service)
Develop and update the parent application	Contains managed reports	Contains the embedded self service workflow
Customize the UI - Define themes, languages, features render	For managed reports	For embedded components
Authentication	Single sign on support for the your application with embedded Symphony	Single sign on support for your application and embedded Symphony content using trusted access
Develop Interactivity	Embed Manage Report communication in the parent application	N/A
Embed components	Manage Report communication and a view only Manage Report	Data Authoring and Self Service components, including Visual Builder, Dashboard Builder, and Object management lists

Administrator (Symphony SaaS)

In Symphony SaaS environments, administrators:

- Manage apps and access to your instances and embedded resources
- Add, edit, and remove users and user groups
- Administer access to data and content, such as data sources, dashboards, visualizations, and more

For more information, see Manage Users in Symphony.

Manage Users in Symphony

Symphony provides the management controls necessary to create users and manage user access of Symphony. Authorization for users to use product features and functions is controlled by the privileges, permissions, and attributes that are assigned to users, groups, and tenants.

When using SAML single sign-on protocol, users and groups may be automatically provisioned in Symphony (account level synchronization). For more information, see Symphony Supported Authentication Tools.

To add a new user quickly and easily, see Add New Users.

Edit an Existing User

You can quickly and easily edit a user as an admin by selecting **Users** from the main menu on the Symphony home page. More advanced changes can be made in the Managed Dashboards module, or the Data Discovery module.

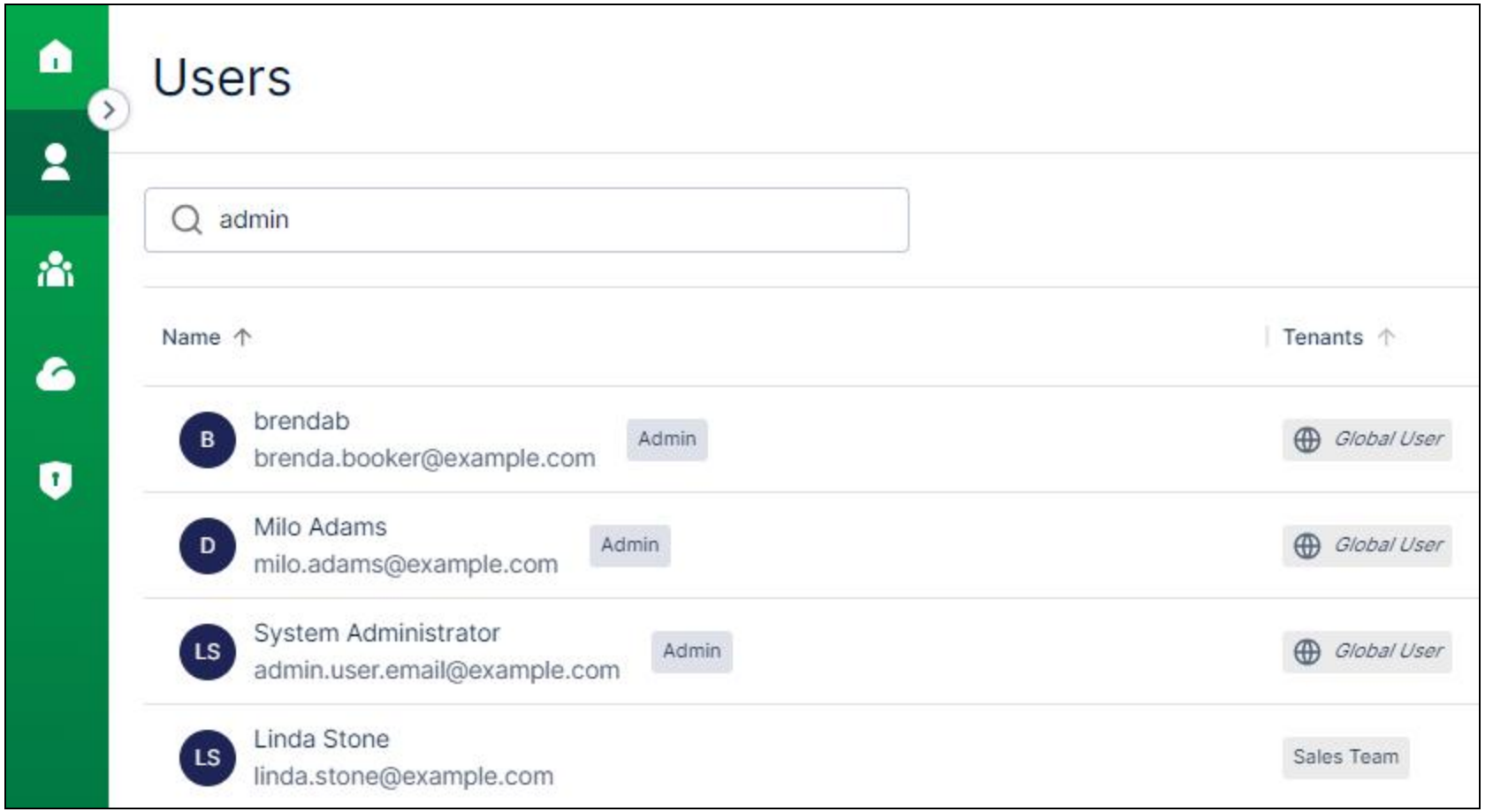
Edit basic user information as a tenant admin

1. Log in as a tenant admin.
2. Verify you're in the appropriate tenant (if you are the administrator for multiple tenants) by selecting **My Tenants** from the main menu.
3. Select **Users** from the main menu. The Users work area opens.

i. System admins are listed with an **Admin** tag in the Name column on the main **Users** landing page.

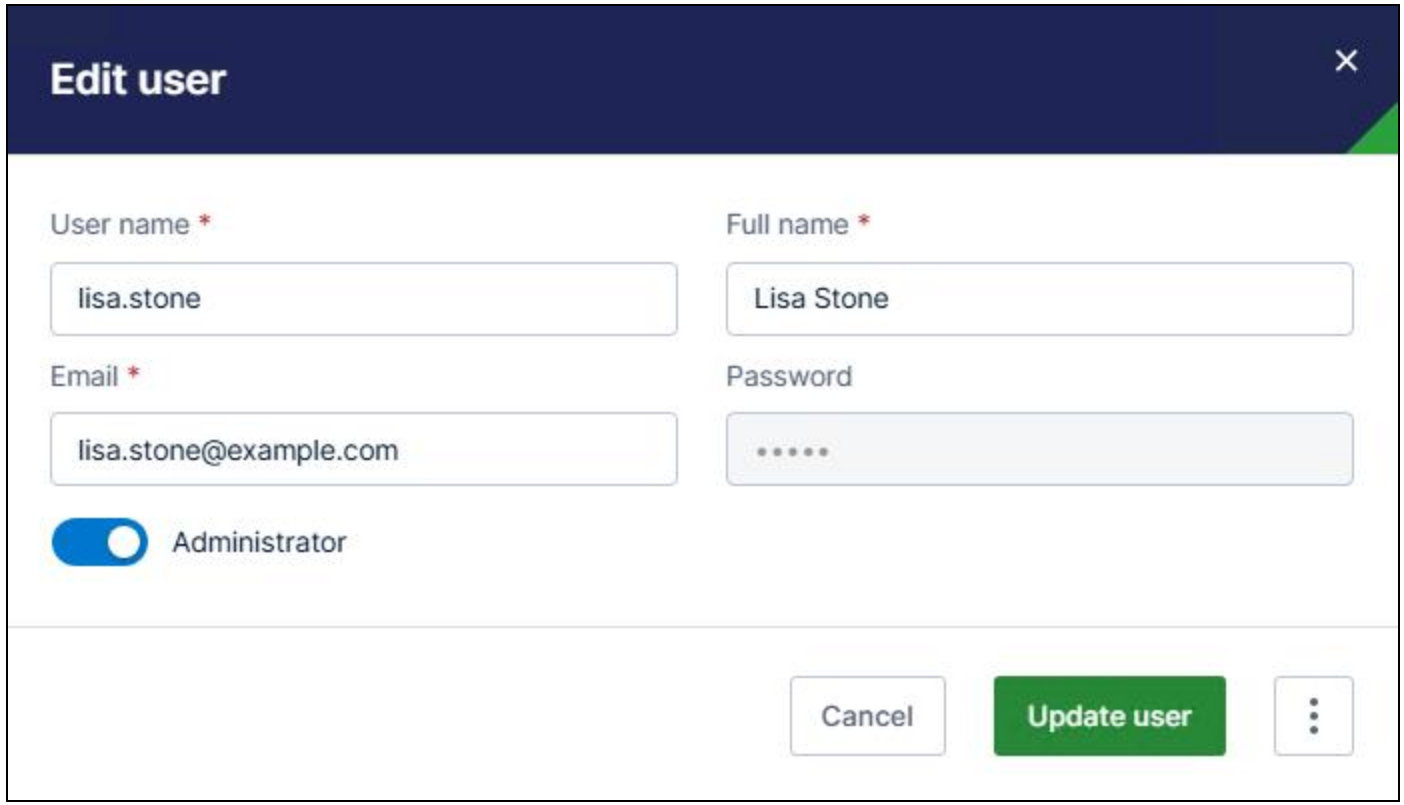
i. Only Global Users can be system admins, and show a **Global User** tag in the Tenants column.

ii. Search for all admins by entering **Admin** in the search box.



4. Scroll to find an existing user, or use the Search field to find a user.

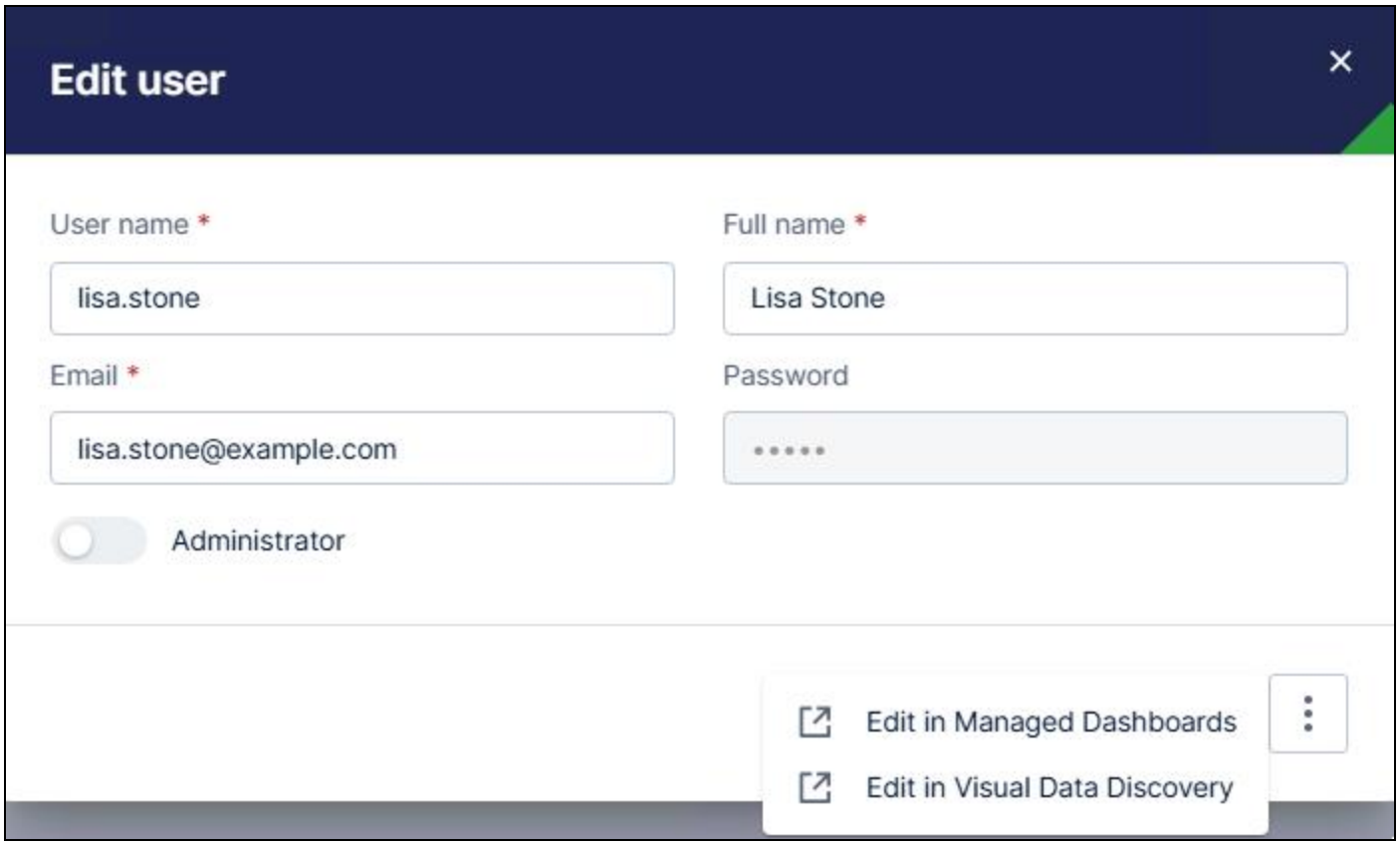
5. Select **Edit user** from the **Actions** menu for the user you want to update. An Edit user pop up dialog opens.



6. Update the **User name**, **Full name**, and **Email** as needed. Optionally, enable or disable **Administrator**.

7. Select **Update user** to save your changes.

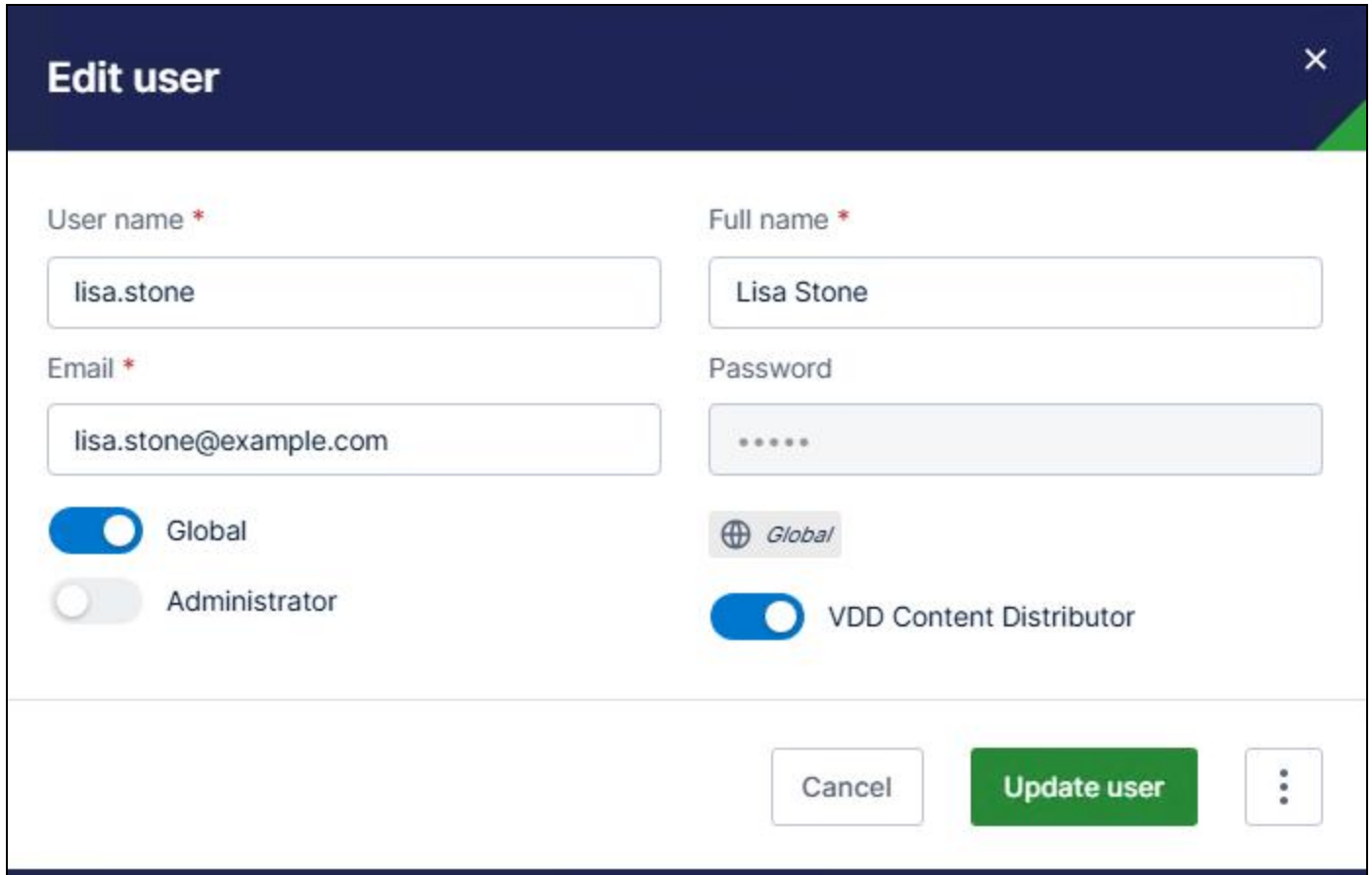
If you need to make other changes to this user, select the action menu, then select a module to edit the user information in that module. Make appropriate changes in Managed Dashboards or in Visual Data Discovery.

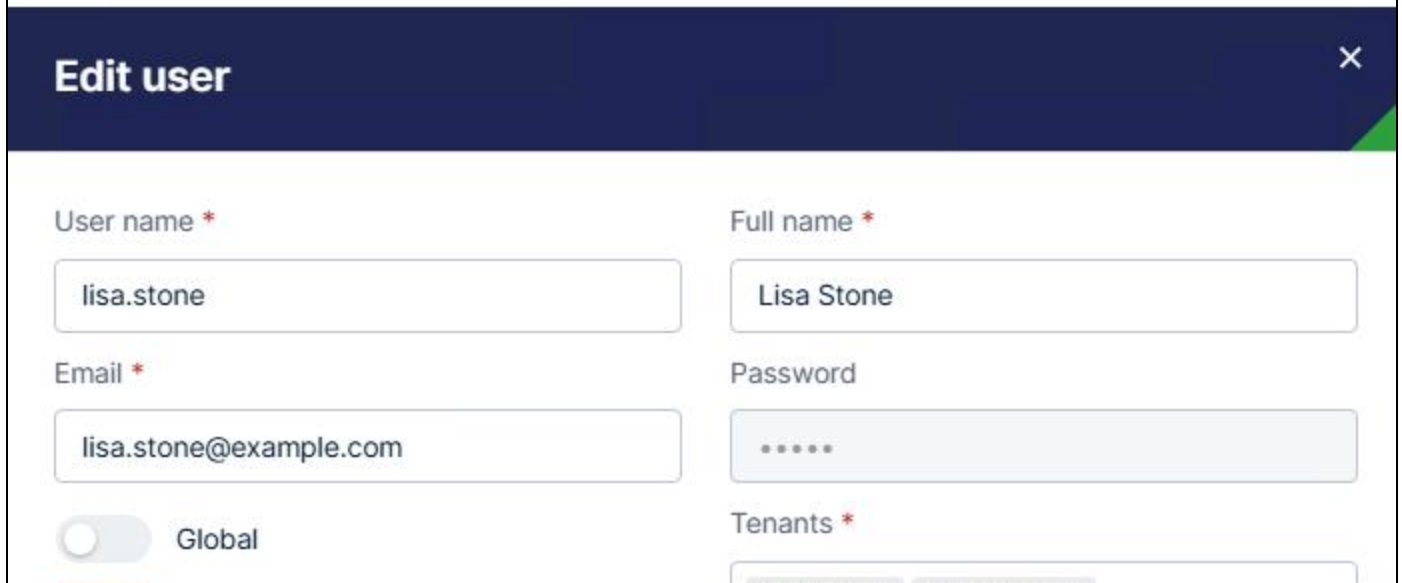


Edit basic user information as a system administrator

1. Log in as a system administrator.
2. Select **Users** from the main menu. The Users work area opens.
3. Scroll to find an existing user, or use the Search field to find a user.

4. Select **Edit user** from the **Actions** menu for the user you want to update. An Edit user pop up dialog opens


Edit user
User name *
lisa.stone
Full name *
Lisa Stone
Email *
lisa.stone@example.com
Password
Global
Global
Administrator
VDD Content Distributor
Cancel
Update user


Edit user
User name *
lisa.stone
Full name *
Lisa Stone
Email *
lisa.stone@example.com
Password
Global
Tenants *

5. Make any changes needed to editable fields, then select **Update user** to save your changes.

If you need to make other changes to this user, select the action menu, then select a module to edit the user information in that module. Make appropriate changes in Managed Dashboards or in Visual Data Discovery.

Perform advanced user tasks in Managed Dashboards

Most advanced user tasks are performed in the Managed Dashboards module.

1. Log in as a system admin or tenant admin. If you are logged in as a tenant admin, verify you're in or switch to the appropriate tenant.
2. Select **Users** from the main menu. The Users work area opens.
3. Scroll to find an existing user, or use the Search field to find a user.
4. Select **Edit user** from the **Actions** menu for the user you want to update. An Edit user pop up dialog opens
5. Select the actions menu button, then **Edit in Managed Dashboards**.
6. A list of users opens. Search for the user, or scroll to find the user you want to edit.
7. Select a user, then **Edit** from the **Contextual** menu, then make and **Save** your user changes.

Perform advanced user tasks in Visual Data Discovery

Some advanced user tasks are accomplished in the Visual Data Discovery module.

1. Log in as a system admin or tenant admin. If you are logged in as a tenant admin, verify you're in or switch to the appropriate tenant.
2. Select **Users** from the main menu. The Users work area opens.
3. Scroll to find an existing user, or use the Search field to find a user.
4. Select **Edit user** from the **Actions** menu for the user you want to update. An Edit user pop up dialog opens.
5. Select the actions menu button, then **Edit in Visual Data Discovery**.
6. A list of users opens. Search for the user, or scroll to find the user you want to edit.
7. Select a user, then make and **Save** your user changes.

See the following topics:

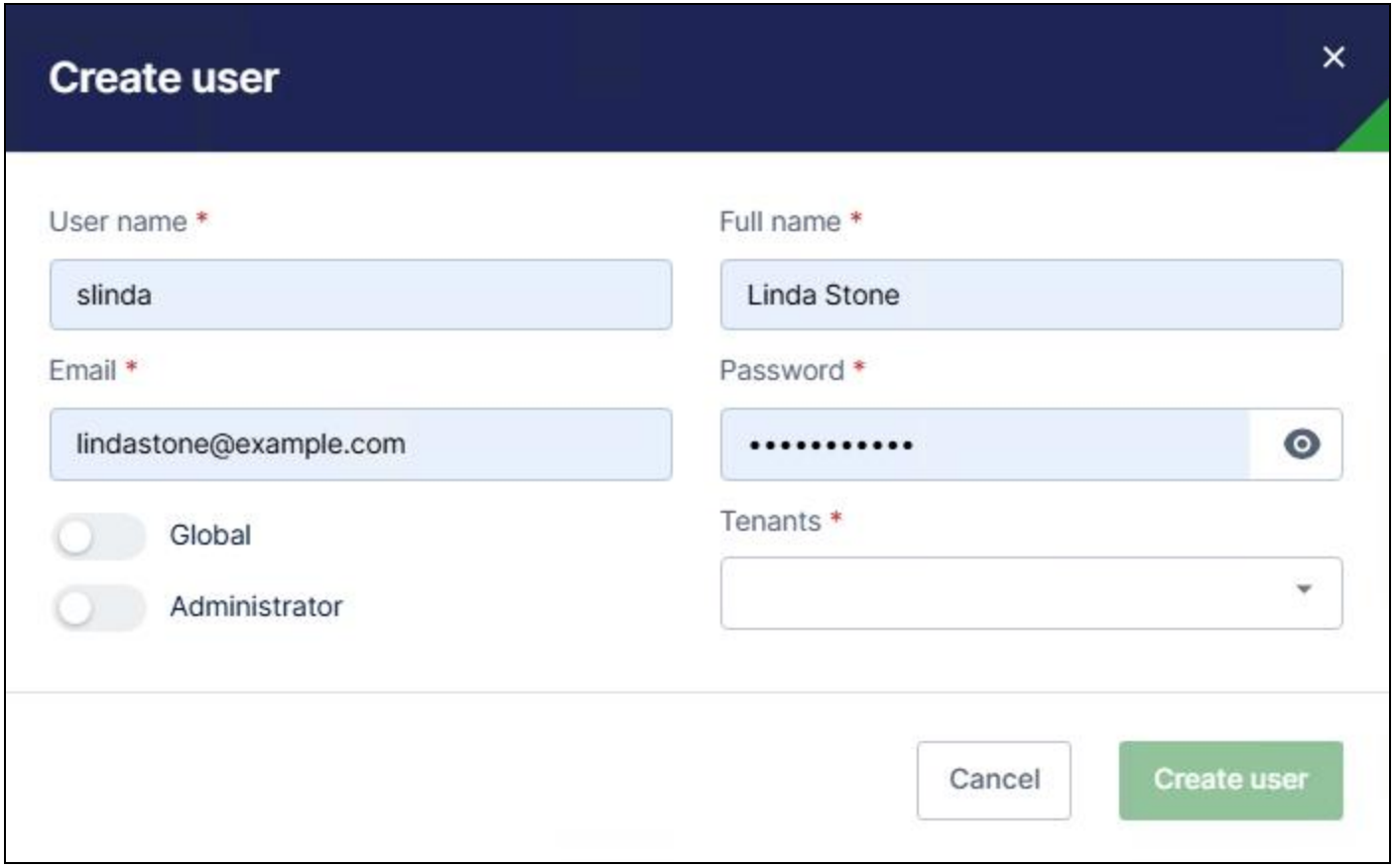
- Add New Users
- Advanced User Management
- Symphony User Personas
- Supplied Users And User Groups
- Modify Users
- Assign and Remove Users in Tenants

Add New Users

As an admin user or user with appropriate permissions, you can quickly and easily add new users to your Symphony environment.

Add a new user as a system administrator

1. Log in to Symphony as a system administrator.
2. Select **Users** from the main menu. The Users work area opens.
3. Select **Create**. A Create user pop up dialog opens.



4. Supply values for the **User name**, **Full name**, **Email**, and **Password**.

   Important: You must select a tenant for a user or add them as a Global User to finish creating the user account.

5. Assign the user to one or more **Tenants**, or enable the **Global User** toggle to make them a global user.

i. If you enable the toggle **Global**, the user has access to all global content and Visual Data Discovery content outside of individual tenants. Optionally, enable **VDD Content Distributor** to allow this user to import and share content to users and tenants.

ii. If you leave the toggle **Global** disabled, you must add the user to at least one tenant.

6. Optionally, enable the toggle **Administrator** to make them an administrator. All administrator users have the same ability to import and share content as members of the Content Distributors group.

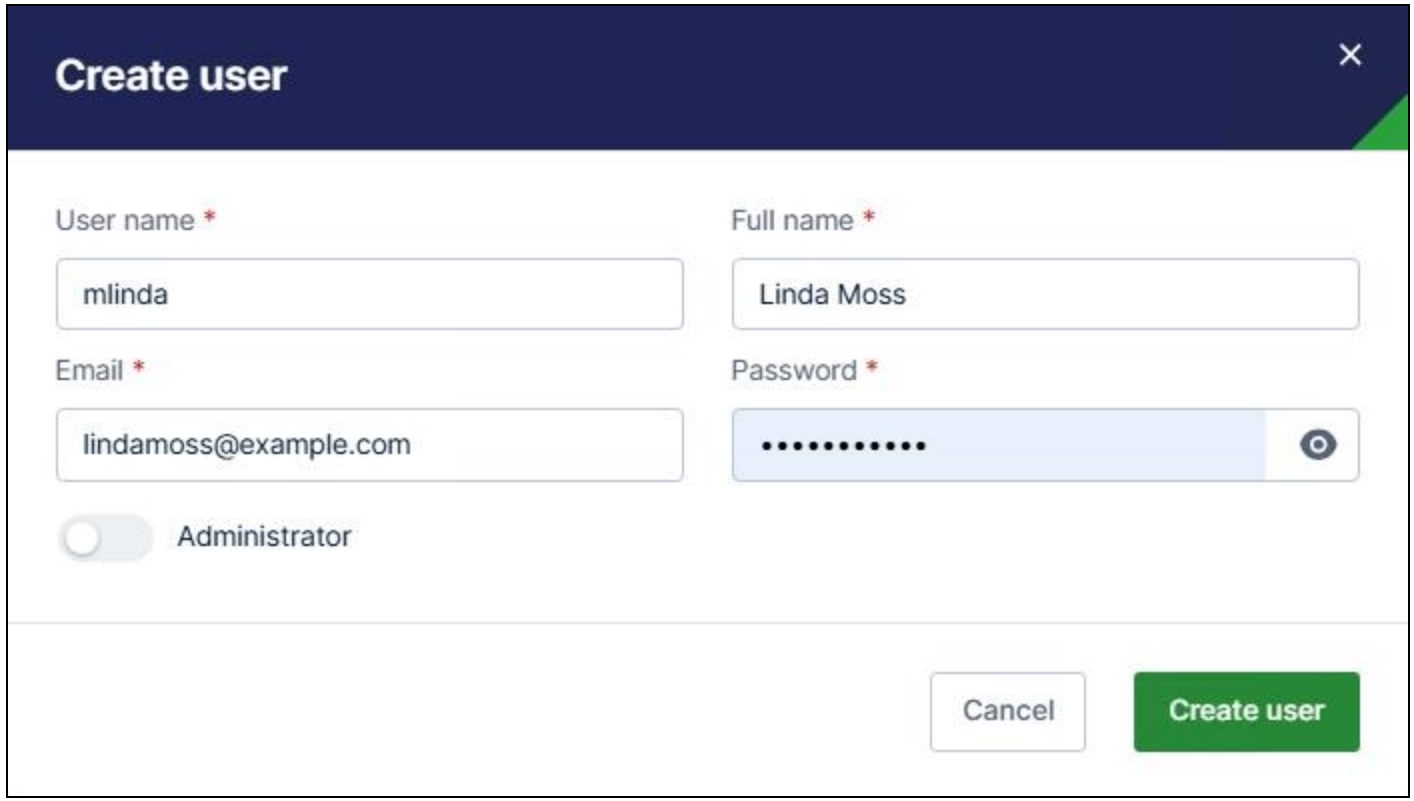
i. If this is a **Global**user , the new user is a System Administrator.

ii. If this is a member of one or more **Tenants**, the new user is a tenant administrator for those tenants.

7. Select **Create user** to create the new user. A success message appears, and you are returned to the User work area.

Create a new user as a tenant administrator

1. Log in to Symphony as a tenant admin.
2. Verify you're in the appropriate tenant (if you are the administrator for multiple tenants) by selecting **My Tenants** from the main menu.
3. Select **Users** from the main menu. The Users work area opens.
4. Select **Create**. A Create user pop up dialog opens.



5. Supply values for the **User name**, **Full name**, **Email**, and **Password**.
6. Optionally, enable the toggle **Administrator** to make them an administrator of the tenant you're working in and adding them to.
7. Select **Create user** to create the new user. A success message appears, and you are returned to the User work area.

Advanced User Management

Symphony provides the account management controls necessary to create users and manage user access of your software environment. Authorization for users to use product features and functions is controlled by the groups to which the users are assigned.

Users are created and generally managed by administrators.

System administrators:

- Create new users and new administrator users in existing tenants.
- Manage user accounts by:
  - Updating and maintaining general information, such as user names, seat types, and enabling or disabling a user.
  - Adding users to groups in Visual Data Discovery and groups in Managed Dashboards.
  - Setting options, including culture-language options, active projects, and account limitations linked to passwords and log on logging.
  - Adjusting options that include defining Application Privileges, and Custom Attributes.
  - Troubleshooting and confirming the user experience is as you've designed by impersonating a user.

Tenant administrators can perform many of the same user tasks as system administrators for users within the tenants they administer.

Manage User Information and Privileges - Managed Dashboards

When you create a user, it's populated with the basic information provided at account creation time: Symphony populates it with seat information, default culture and timezone information, and more. You can update this information or disable a user by editing these settings in the Managed Dashboards module.

Access and update user account information in Managed Dashboards

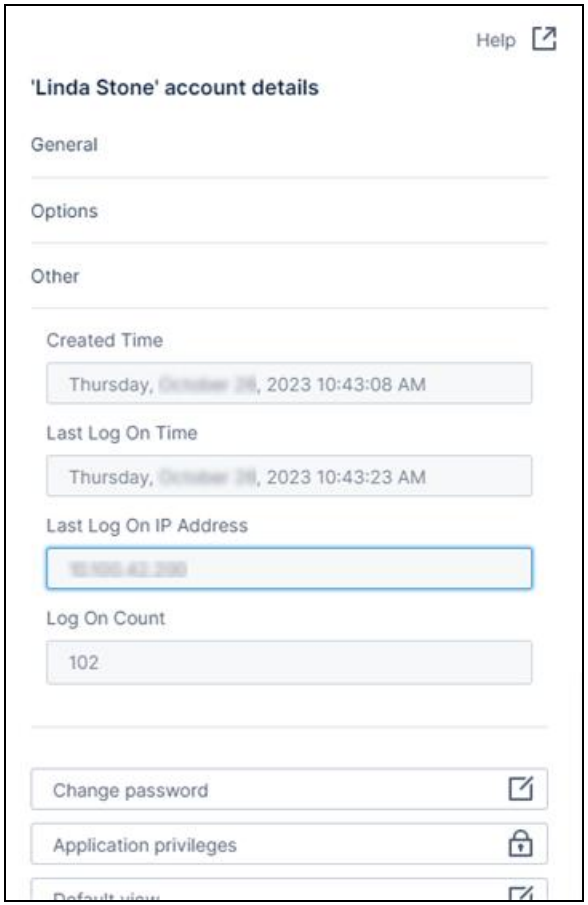
1. Log in as a system admin or tenant admin. If you are logged in as a tenant admin, verify you're in or switch to the appropriate tenant.
2. Select **Users** from the main menu. The Users work area opens.
3. Scroll to find an existing user, or use the Search field to find a user.
4. Select **Edit user** from the **Actions** menu for the user you want to update. An Edit user pop up dialog opens
5. Select the actions menu button, then **Edit in Managed Dashboards**.

6. A list of users opens. Search for the user, or scroll to find the user you want to edit.

7. Select a user, then **Edit** from the **Contextual** menu, then make and **Save** your user changes.

The account details work area includes sections you can expand to edit:

- General
- Options
- Other



The account details options you can view and update are listed in the table below:

Account Details Section	Field	Description
General	ID	This user's account ID (a GUID value). You can search for users by their ID in the user Accounts work area.
	Account Type	If applicable, select an account type. The default is Local user.
	Tenant	The Tenant for this user account. Not editable here.
	Name	The login name for this user. Editable.
	Seat Type	Select a Seat Type from the available options.
	Seat Mode	Indicates the seat mode for this account. This may be reserved or floating.
	Email Address	The email address associated with this user account. Editable.
	Display Name	The user's display name. Editable.
	Enabled	Indicates the user account is enabled if checked, disabled if blank. Editable.
	Notes	An editable text field; add notes about this user here.
Options	Culture	Enter a language code (such as en-US) for this user. If blank, defaults to Symphony's defined culture.
	Time Zone	This user's time zone. Select a UTC option, or leave at Default.
	Logon Session Idle Timeout	Define this user's idle timeout. Format as `dd.hh:mm:ss` or `hh:mm:ss`.
	Explicit Password Expiry Date	If defined, overrides the **Days Before Password Expire** setting. if **Password Never Expires** is enabled, this value is ignored.
	Account Expiry Date	Define the date this account expires.
	Allowed IP Addresses	Define the IP address or range of addresses this user must use to connect to your environment.
	Active Project	The user's active project. Select the edit icon to change their active project.
	Can Change Password	Enable to allow this user to change their own password.
	Password Never Expires	Enable to override any environment or user account password expiration dates.
	Track Log On History	Enable to track this user's log on history.

Account Details Section	Field	Description
Other	Created Time	The date and time this user account was created. Not editable.
	Last Log On Time	The last date and time this user account connected to your environment. Not editable.
	Last Log On IP Address	The last IP address this user account used to connect to your environment. Not editable.
	Log On Count	The number of times this user account connected to your environment. Not editable.
	Change password	Select to manually change this user's password.
	admin	Select to update this user's application privileges. See Application Privileges.
	Default view	Select to change this user's default view. Defining this overrides their group default view. See Application Privileges.
	Active logon sessions	Select to view the user's current logged on sessions.
	Custom attributes	Select to define the users' custom attributes. See Custom attributes.
	Effective custom attributes	Select to view the effective custom attributes for this user.
	Tokens	Select to view and manage tokens associated with this user.
	Member of	Select to view and edit the groups this user is a member of.
	<User Name>'s recycle bin	Select to view the files and folders this user has deleted and can be restored.
	<User Name>'s notifications	Select to update or remove this user's notifications.
	<User Name>'s project	Select to view and manage this user's project, project files, and content.
	Impersonate <User Name>	Select to impersonate this user and verify their user experience. Any changes you make as the user will persist.

Perform advanced user tasks in Visual Data Discovery

1. Log in as a system admin or tenant admin. If you are logged in as a tenant admin, verify you're in or switch to the appropriate tenant.
2. Select **Users** from the main menu. The Users work area opens.
3. Scroll to find an existing user, or use the Search field to find a user.
4. Select **Edit user** from the **Actions** menu for the user you want to update. An Edit user pop up dialog opens.
5. Select the actions menu button, then **Edit in Visual Data Discovery**.
6. A list of users opens. Search for the user, or scroll to find the user you want to edit.
7. Select a user, then make and **Save** your user changes.

For more information about advanced user tasks you can peform in Visual Data Discovery, see Modify Users.

See the following topics:

- Manage Users in Symphony
- Add New Users
- Symphony User Personas
- Supplied Users and User Groups
- Modify Users
- Assign and Remove Users in Tenants

Multi-Tenancy in Symphony

Multi-tenancy allows administrators to easily create and manage tenants. Each tenant has its own complete set of administrators, users, and groups.

One use of a multi-tenant instance is for a SaaS solution provider who wants to enhance their software BI and analytics capabilities by integrating Symphony content. Additionally, you can deploy a multi-tenant instance to deploy a client-facing portal, or to support a large internal deployment that requires complete isolation between different departments or lines of business.

Symphony tenants are specially designed to be completely isolated from other tenants in a single Symphony instance where:

- Each tenant can have its own content
- Content can be shared with all tenants using optional data security based on who is logged on
- You can design an environment where a combination of both approaches is used

Important: You must have the appropriate licensing from insightsoftware to see this option.

There are several steps you'll take to deploy multi-tenancy in your environment. Create the tenants, define an admin user for the tenant, create tenant projects, set up access to data connectors, and create users within the tenant.

For more information, see:

- Create a New Tenant
- Create Tenant Projects
- *New*Define Tenant Access to the <GLOBAL> Project
- Connect to Data and View it on a Dashboard
- Create and Add Additional Tenant Admin Users
- Add and Edit Tenant Users
- Disable, Enable, And Remove Tenants

Create a New Tenant

When you create a new tenant in Symphony, you're creating an isolated work area for specific clients, departments, or lines of business. You'll create a tenant, assign an administrative user, create a project for the tenant, and define a data connector.

When you create a tenant in Symphony, you're creating a work area for specific clients, departments, or lines of business. You'll create a tenant, assign an administrative user, create one or more projects for the tenant, and define their data connectors.

Important: You must have the appropriate licensing from insightsoftware to see this option.

If you create an environment that includes multiple tenants, they can access items in the <GLOBAL> project of Managed Dashboards and Reports unless you specifically exclude their access to this content. As needed, you can designate items to be shared across multiple tenants using security privileges.

Create a Tenant in Symphony

1. Log in as the supplied admin user or a system administrator.
2. Select **Tenants** from the main menu. The Tenant work area opens.
3. Select **Create** to create a new tenant. The Create tenant work area opens.
4. Add a **Tenant name**.

   Note: By default, the tenant is enabled by default. If you're not ready to enable this tenant, disable by sliding the **Enabled** toggle to the left.

5. Select **Create tenant** to complete the initial tenant creation.

   A message is returned indicating the tenant is successfully created, and is added to the list of tenants in the Tenants work area.

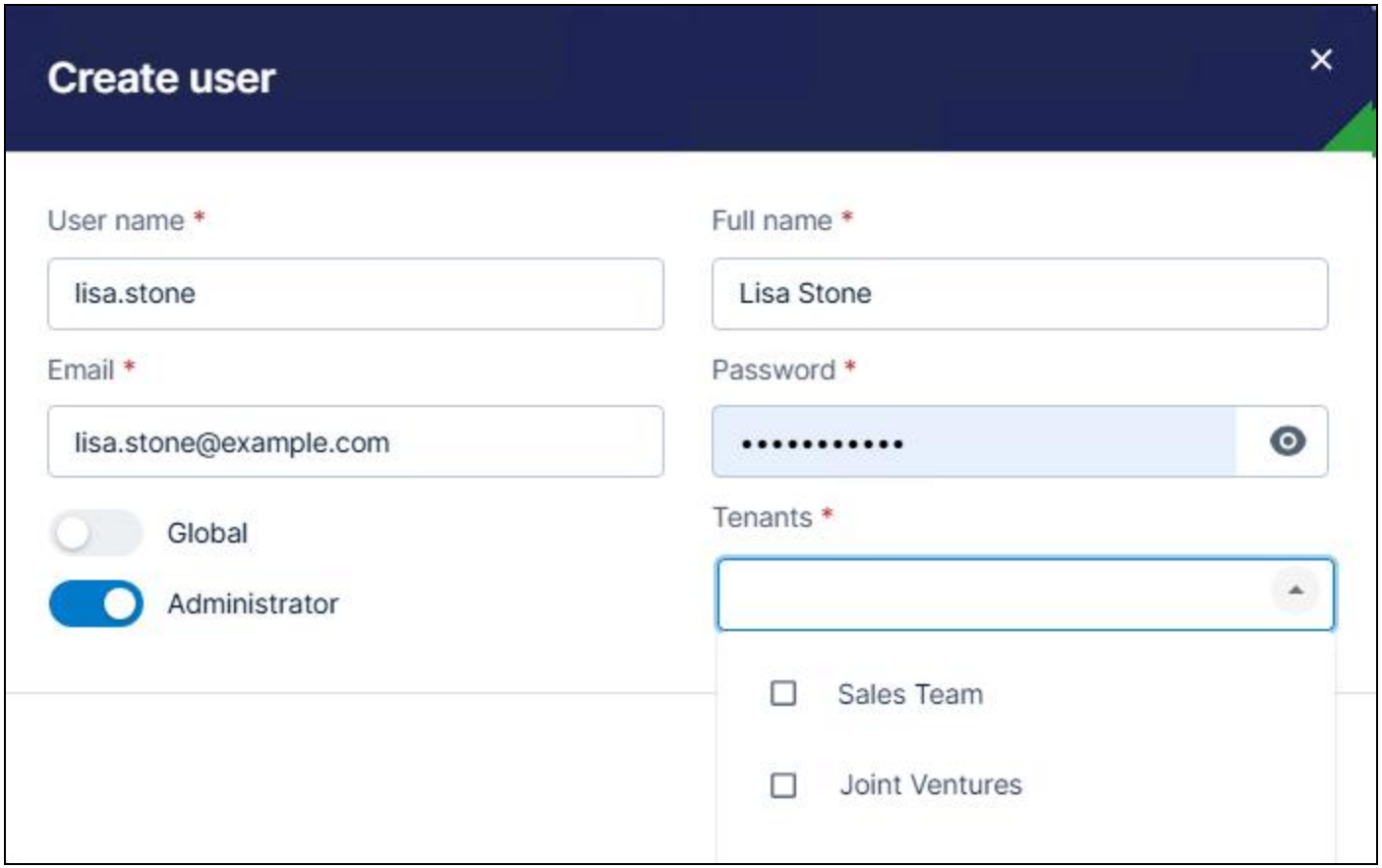
Next, create or add a tenant admin for your new tenant.

Create a New Tenant Admin

After you've created your tenant, add or create at least one admin user for the new tenant.

1. Log in as the supplied admin user or other system administrator.
2. Select **Users** from the main menu on the Symphony home page. The Users work area opens.

3. Select **Create**. A **Create user** pop up window opens.

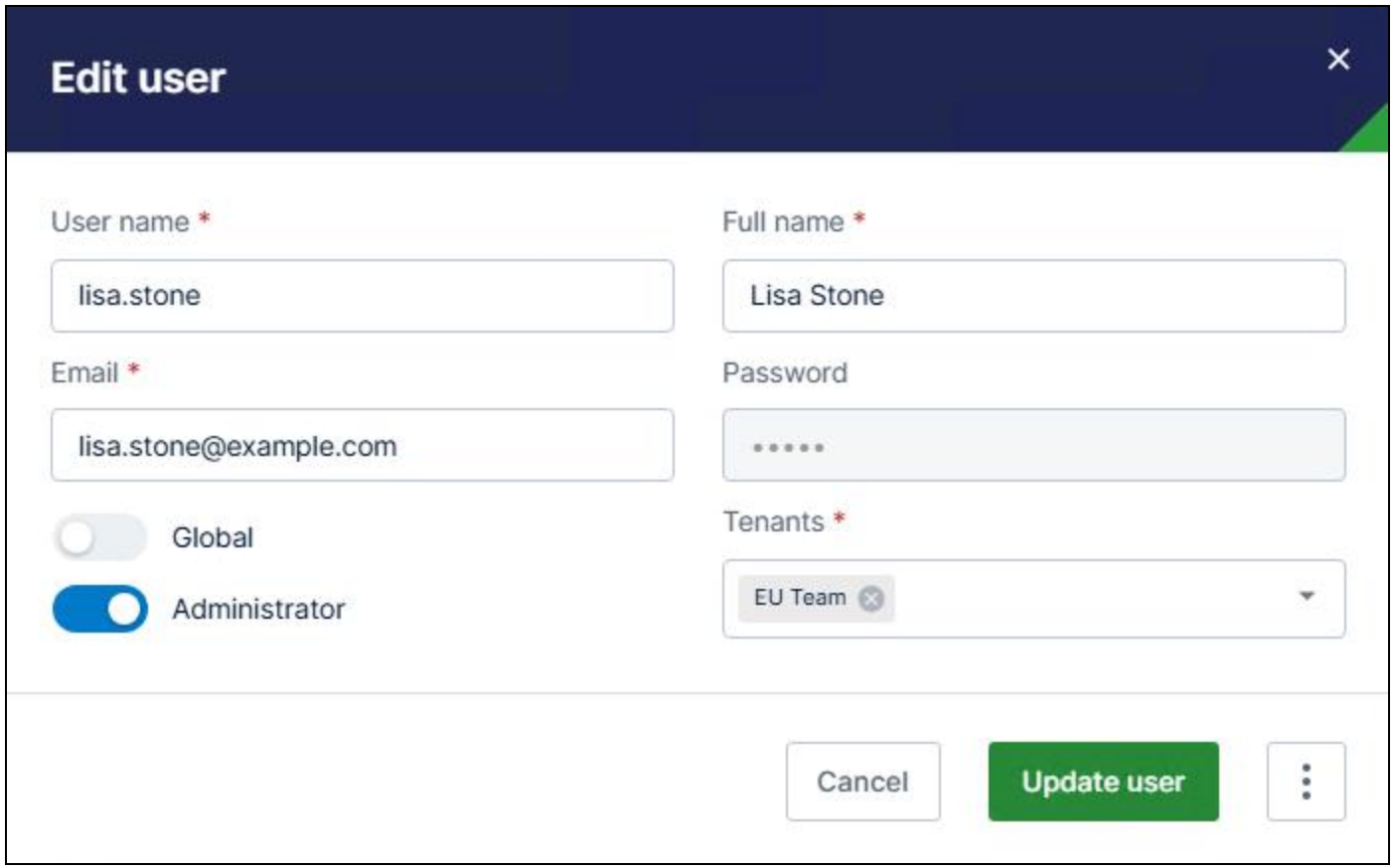


4. Supply values for the **User name**, **Full name**, **Email**, and **Password**. Select your new **Tenant** from the drop-down list.
5. Enable **Administrator** to make this user an admin of this tenant.
6. Select **Create user**. A success message is displayed, and the tenant admin is added to the tenant.

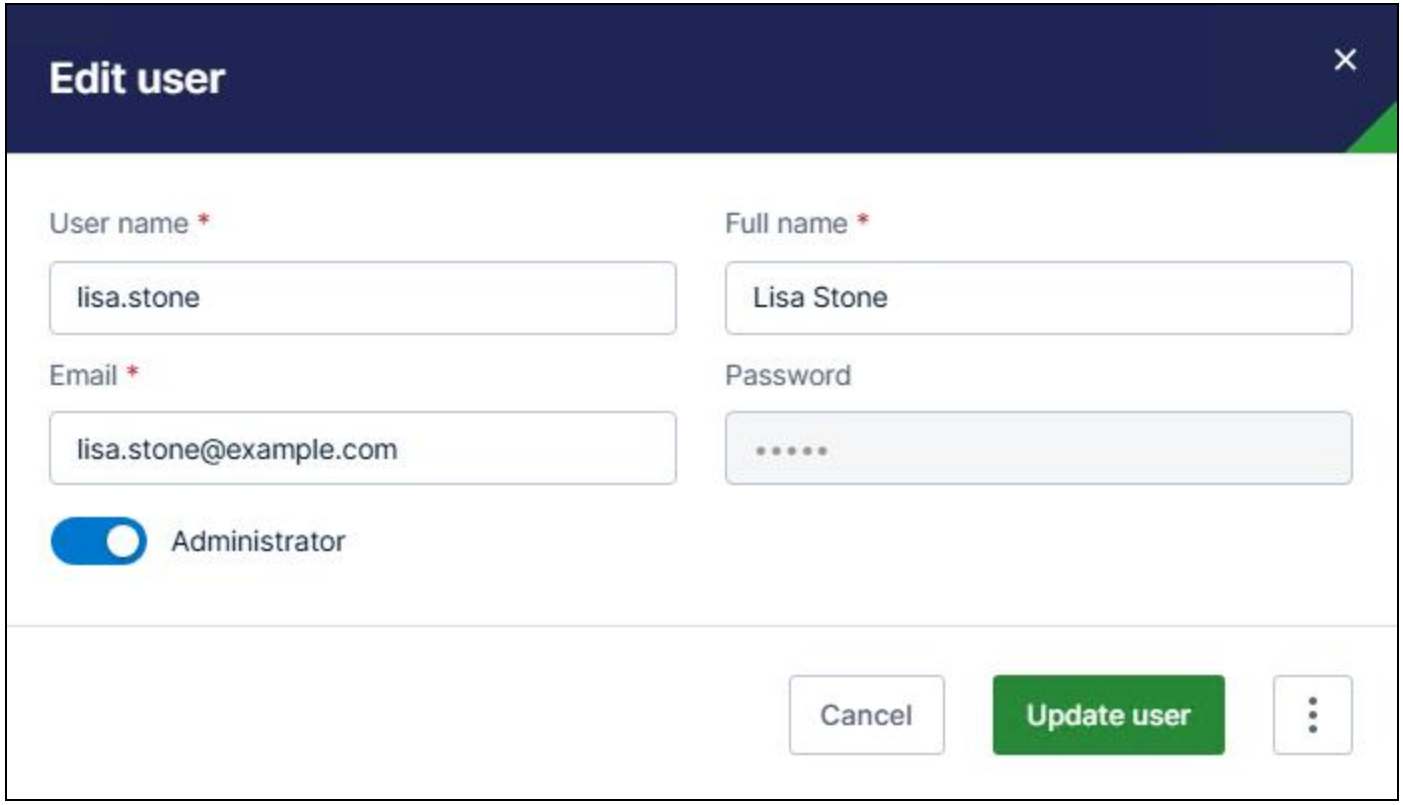
Make an Existing User a Tenant Admin

1. Log in as a system admin or tenant admin. If you are logged in as a tenant admin, verify you're in or switch to the appropriate tenant.
2. Select **Users** from the main menu. The Users work area opens.
3. Scroll to find an existing user, or use the Search field to find a user.
4. Select **Edit user** from the **Actions** menu for the user you want to update. An Edit user pop up dialog opens.
5. Enable the toggle **Administrator** to make this user an admin for the tenants listed in **Tenants**.

i. If you are a system admin, you can add or remove tenants here. The user becomes a tenant admin for all listed tenants.



ii. If you are a tenant admin, the user becomes a tenant admin for the tenant you are working in.



6. Select **Update user** to save your changes.

If you need to make other changes to this user, select the action menu, then select a module to edit the user information in that module. Make appropriate changes in Managed Dashboards or in Visual Data Discovery.

- Create Tenant Projects
- Connect to Data and View it on a Dashboard
- Create and Add Additional Tenant Admin Users

- Add and Edit Tenant Users
- Disable, Enable, and Remove Tenants

Disable, Enable, and Remove Tenants

You can temporarily disable or completely remove (delete) tenants as needed to manage your environment.

Disable a Tenant

If you want to remove access to a tenant without removing all users and content, disable the tenant for as long as needed.

When you disable a tenant, users who are members only in this tenant can no longer access content they've created there and see a message that the tenant has been disabled.

Disable a tenant

1. Log in as a system administrator.
2. Select **Tenants** from the main menu. The Tenant work area opens.
3. Scroll through the list of tenants or search for the tenant by name.
4. When you find your tenant, select the **Actions** menu, and choose **Edit tenant**. The **Edit tenant** work area opens.
5. Slide the Enabled toggle to the left (disable).
6. Select **Update tenant** to disable the tenant.

   A message is returned indicating the tenant is updated. To view disabled tenants, enable the toggle **Show disabled** in the Tenants work area.

Enable a Tenant

Disabled tenants can be enabled in your software environment when you're ready to allow users to create and work with their content.

Enable a tenant

1. Log in as the supplied admin user (System Administrator).
2. Select **Tenants** from the main menu. The Tenant work area opens.
3. Enable the toggle **Show disabled** in the Tenants work area. Scroll through the list of tenants or search for the tenant by name.
4. When you find your tenant, select the **Actions** menu, and choose **Edit tenant**. The **Edit tenant** work area opens.

5. Slide the Enabled toggle to the right (enable).
6. Select **Update tenant** to enable the tenant.

   A message is returned indicating the tenant is updated. Users can now log in to the tenant and work with their content.

Remove a Tenant

If you remove (delete) a tenant, all content created for that tenant is deleted.

- If a user is associated only with that tenant, the user is deleted as well.
- If a user associated with multiple tenants, their user remains in your environment, and can still access their other tenant work areas.

Remove a tenant

1. Log in as the supplied admin user or a system administrator.
2. Select **Tenants** from the main menu. The Tenant work area opens.
3. Enable the toggle **Show disabled** in the Tenants work area if needed. Scroll through the list of tenants or search for the tenant by name.
4. When you find your tenant, select the **Actions** menu, and choose **Remove tenant**. The **Remove tenant** confirmation dialog opens.
5. Select **Remove** to remove the tenant and any resources.

   A message is returned indicating the tenant is removed.

Create and Add Additional Tenant Admin Users

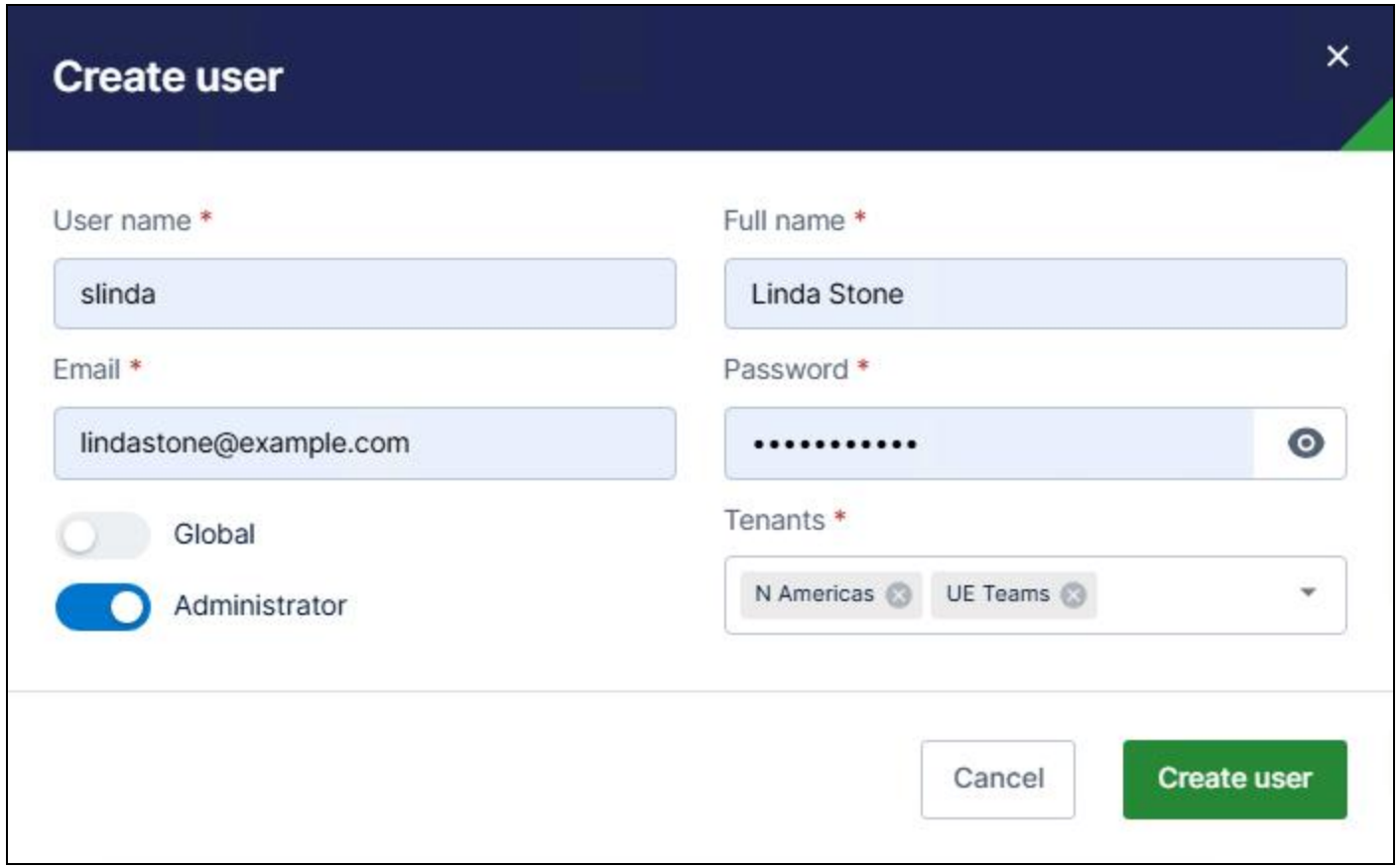
When you create a new tenant in Symphony, you're creating an isolated work area for specific clients, departments, or lines of business. After creating the tenant, you'll need to define one or more Admin users to manage the tenant resources. After a system administrator creates the first admin user for the tenant, they can create additional users as tenant admins, or add existing users to the Administrators group.

Create Admin Users for a Tenant

Create the first tenant admin for an existing tenant to allow them to manage tenant users and resources.

Create a new user to be a tenant admin for one or more tenants

1. Log in to Symphony as a system administrator.
2. Select **Users** from the main menu. The Users work area opens.
3. Select **Create**. A Create user pop up dialog opens.



4. Supply values for the **User name**, **Full name**, **Email**, and **Password**.

   Important: You must select at least one tenant to create the user as an admin in a tenant.

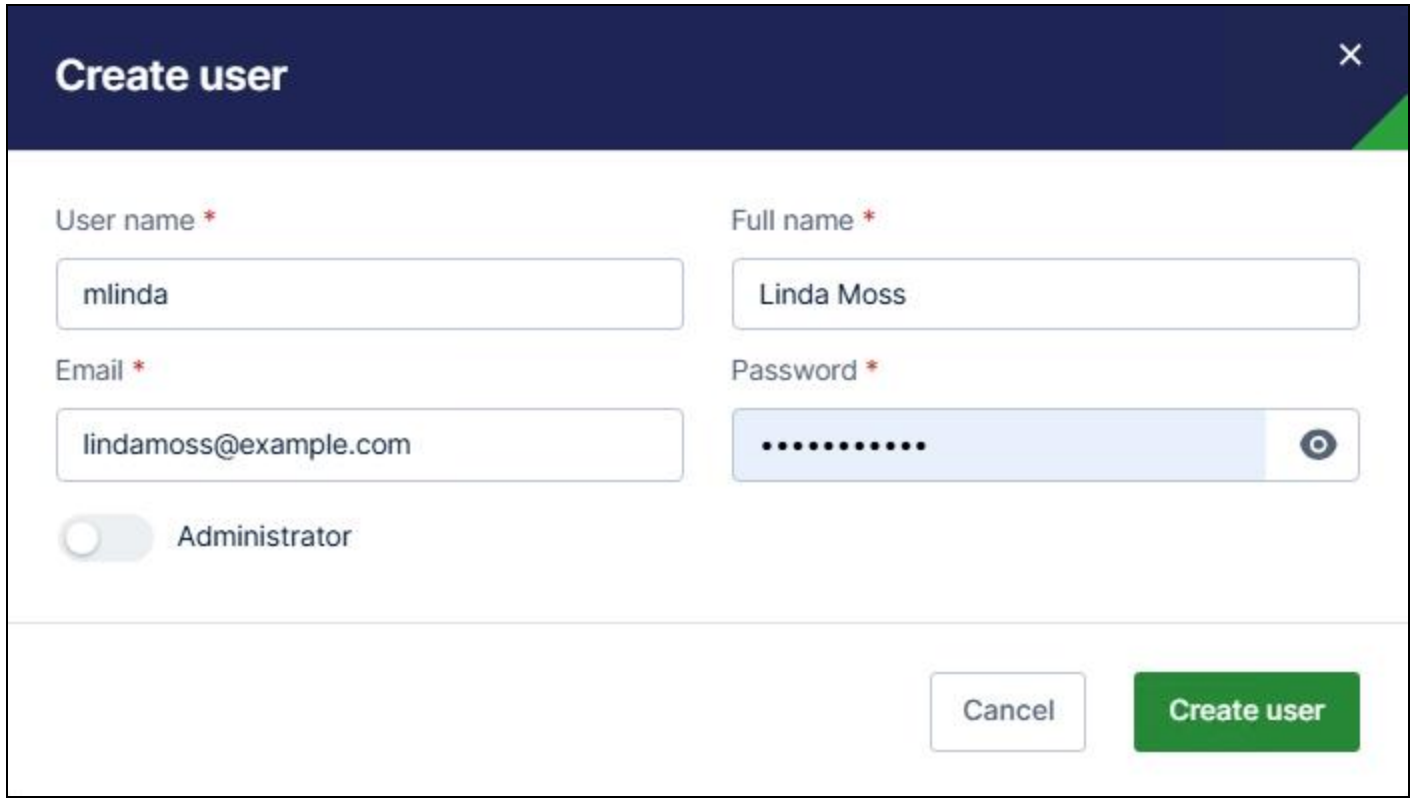
5. Assign the user to one or more **Tenants**, or enable the **Global** user toggle to make them a global user.

6. Enable the toggle **Administrator** to make them a tenant administrator.

7. Select **Create user** to create the new user as a tenant admin for the selected tenants. A success message appears, and you are returned to the User work area.

Create a new user as a tenant administrator

1. Log in to Symphony as a tenant admin.
2. Verify you're in the appropriate tenant (if you are the administrator for multiple tenants) by selecting **My Tenants** from the main menu.
3. Select **Users** from the main menu. The Users work area opens.
4. Select **Create**. A Create user pop up dialog opens.



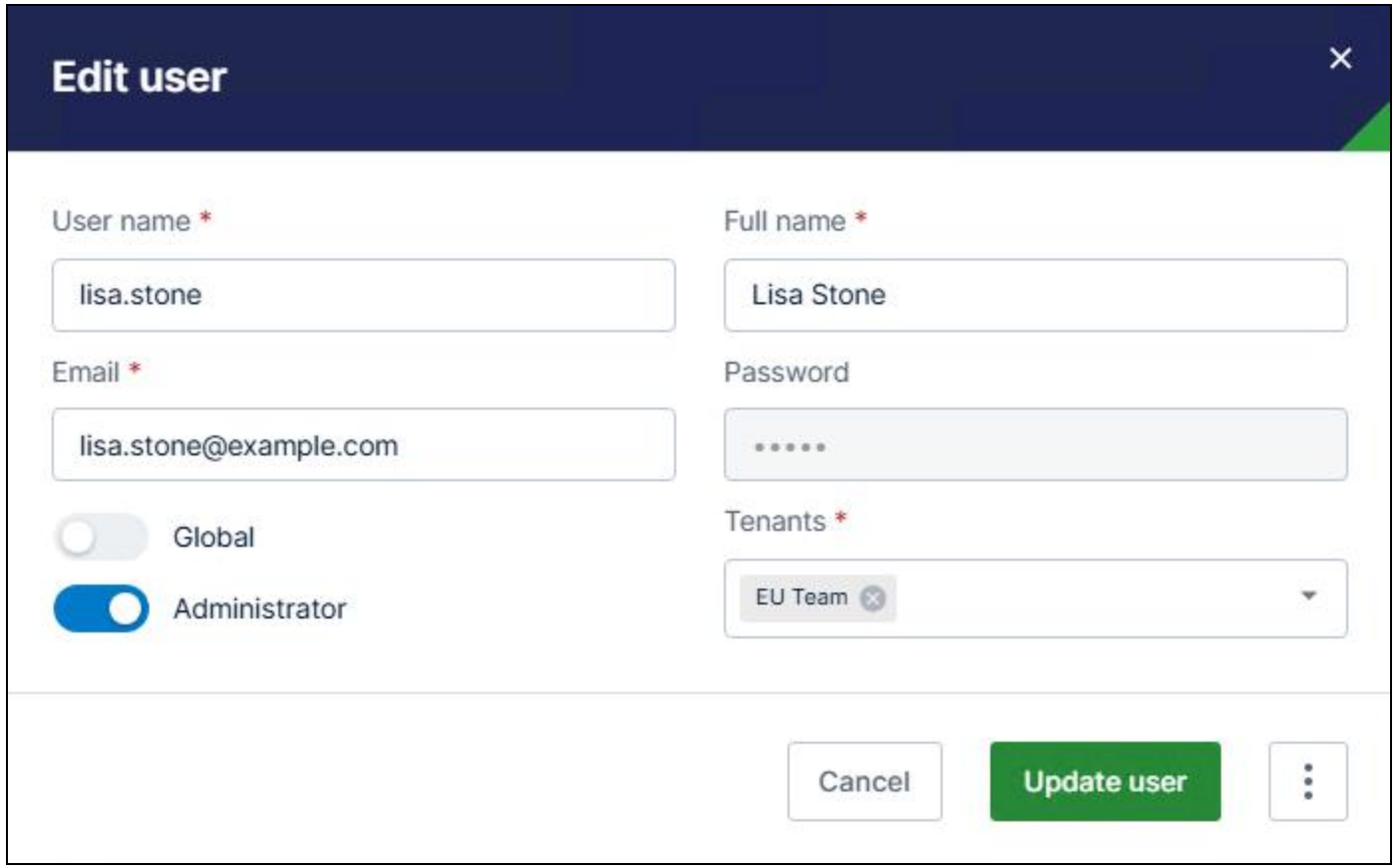
5. Supply values for the **User name**, **Full name**, **Email**, and **Password**.
6. Optionally, enable the toggle **Administrator** to make them an administrator of the tenant you're working in and adding them to.
7. Select **Create user** to create the new user. A success message appears, and you are returned to the User work area.

Add Existing Users as Additional Admins for a Tenant

Add additional administrative users for a tenant either as the tenant admin or as a system admin user.

Add or remove existing users as tenant admins for your tenant as a system admin

1. Log in as a system admin user.
2. Select **Users** from the main menu. The Users work area opens.
3. Scroll to find an existing user, or use the Search field to find a user.
4. Select **Edit user** from the **Actions** menu for the user you want to update. An Edit user pop up dialog opens.

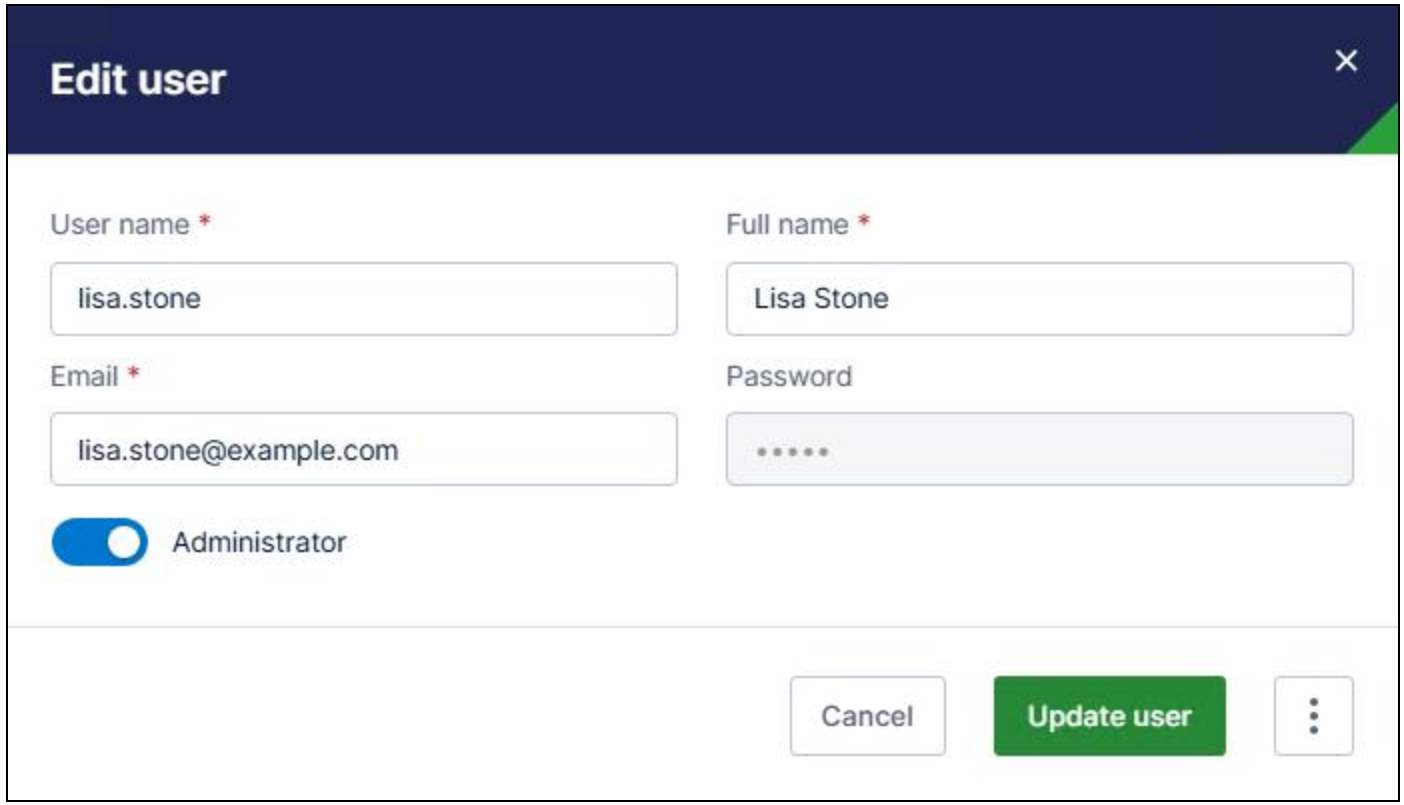


5. Select to enable **Administrator** to add this user as a tenant admin to all listed tenants. Disable this toggle to remove them as a tenant admin. Optionally, add or remove tenants for this user.
6. Select **Update user**. A success message is displayed, and the admin user is added to Symphony for your selected tenant.

Add or remove existing users as tenant admins for your tenant as a tenant admin

1. Log in as a tenant admin.
2. Verify you're in the appropriate tenant (if you are the administrator for multiple tenants) by selecting **My Tenants** from the main menu.
3. Select **Users** from the main menu. The Users work area opens.

4. Scroll to find an existing user, or use the Search field to find a user.
5. Select **Edit user** from the **Actions** menu for the user you want to update. An Edit user pop up dialog opens.



6. Select to enable **Administrator** to add this user as a tenant admin to the tenant you are working in. Disable this toggle to remove them as a tenant admin.
7. Select **Update user**. A success message is displayed, and the admin user is added to Symphony for your selected tenant.

For more information, see:

- Create Tenant Projects
- Define Access to Data Discovery Connectors

- Add and Edit Tenant Users

Create Tenant Projects

When you create a new tenant in Symphony, you're creating an work area for specific clients, departments, or lines of business. Content you work with in Symphony that uses Managed Dashboards or Reports content are organized inside of projects you can use to structure your content as needed.

When you create a tenant, Symphony generates several projects for your users to work in:

- **My Project** - A personal project, unique to each user. Everyone can use their My Project work area to create dashboards for prototyping or quick analysis.
- **<GLOBAL>** - A global project, shared across all users inside and outside of your tenants in your environment. Use this project to store any items common to your other projects for reuse. If you prefer to remove access to the <GLOBAL> project from tenant users, see Remove access to the GLOBAL project for all tenants.
- ***<tenant name>*** - A tenant-based project, shared across all users inside of your tenant. Use this project to store any items common to your other tenant projects for reuse.

If you have the appropriate permissions, you can add more projects for your use, or as a tenant administrator for all tenant members to use.

As a system administrator or tenant administrator, you can create new projects for tenants in your environment in addition to the default project for each tenant created automatically when you created .

For more information, see:

- Add And Edit Tenant Users

Create Additional Projects for A Tenant

1. Log in as a system admin and open the Managed Dashboards work area. Your main dashboards work area opens.
2. Select **Projects** from the main menu. The Projects work area opens.
3. Select **Create new project**. A **Create a new project** window opens.
4. Give the project a name, then select the appropriate **Tenant** name from the list of tenants.

   Note: If you do not select a tenant, it is made available to all global users.
5. Optionally select (check) **Set As Active Project**.

6. Change the **Initial Project Privileges** to **Custom**. You can adjust the specific settings after the project is created.

7. Select **Save** to create this project. Symphony returns a success message, and a Security work area opens.

Define the Security Settings for This Project

1. After you create a new project, the **Security** work area opens so you can define the privileges for users of this project.

   > **Note:** If you navigate away from this area, select the Project in the Project work area, **Edit** it, then scroll down in the Properties modal to select **Security** and reopen this work area.

2. Set the Security options as follows with the group **Everyone** selected:

Field	Set To
Delete	Not Set
Execute	Allow
Full Control	Not Set
List Folder Contents	Allow
Modify Folder	Allow
Read	Allow
Write	Allow

3. Select Save to save your custom security settings. Symphony returns a success message, and you are returned to the Projects work area.

Create a New Project for Multiple Tenants

1. Log in as a tenant admin of multiple tenants. If you are an admin for only one tenant, only the tenant you are an admin for can use this Project.

2. Select **Projects** from the main menu. The Projects work area opens.

3. Select **Create new project**. A **Create a new project** modal opens.

4. Give the project a name, then select (check) **Set As Active Project**.

5. Change the **Initial Project Privileges** to **Custom**. You can adjust the specific settings after the project is created.

6. Select **Save** to create this project for all of your tenants. Symphony returns a success message, and a Security work area opens.

Define the Security Settings for This Project

1. After you create a new project, the **Security** work area opens so you can define the privileges for users of this project.

   > **Note:** If you navigate away from this area, select the Project in the Project work area, **Edit** it, then scroll down in the Properties modal to select **Security** and reopen this work area.

2. Set the Security options as follows with the group **Everyone** selected:

Field	Set To
Delete	Not Set
Execute	Allow
Full Control	Not Set
List Folder Contents	Allow
Modify Folder	Allow
Read	Allow
Write	Allow

3. Select Save to save your custom security settings. Symphony returns a success message, and you are returned to the Projects work area.

Next, you'll add any needed Data Discovery connectors for your users or tenants users. See Connect to Data and View it on a Dashboard.

For more information, see:

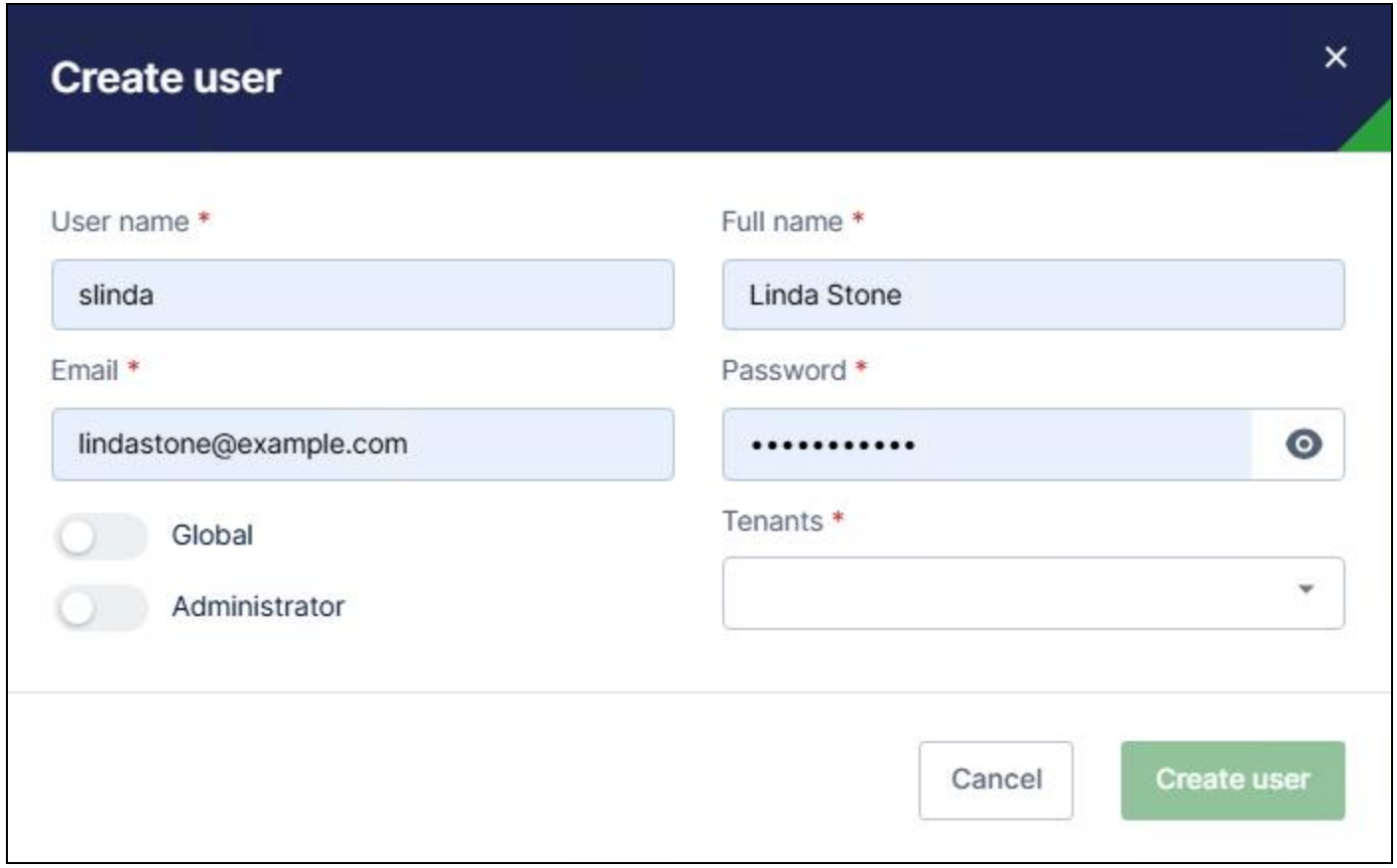
- Add And Edit Tenant Users

Add and Edit Tenant Users

Once your tenant environment is set up, tenant admin users can create your users and other tenant admins.

Add a new user to a tenant

1. Log in as a system admin or tenant admin. If you are logged in as a tenant admin, verify you're in or switch to the appropriate tenant.
2. Select **Users** from the main menu. The Users work area opens.
3. Select **Create**. A Create user pop up dialog opens.



4. Supply values for the **User name**, **Full name**, **Email**, and **Password**.

i. If you are a tenant admin, this user is automatically assigned to this tenant as a member of the admin group.

ii. If you are a system admin, select the appropriate **Tenant** or tenants from the drop-down list.

5. Leave **Administrator** disabled.

6. Select **Create user** to create the new user. A success message appears, and you are returned to the User work area.

> **Note:** You may not see a user you've created or added until after they log in for the first time.

To update, edit, or make other changes to existing users, see Edit an Existing User.

Symphony User Groups

Symphony provides the management controls necessary to create and manage groups in Symphony. Authorization for users to use product features and functions is controlled by the privileges, permissions, and attributes that are assigned to users, groups, and tenants.

Note: When using SAML single sign-on protocol, users and groups may be automatically provisioned in Symphony (account level synchronization). For more information, see Symphony Supported Authentication Tools.

Users can belong to multiple groups. You can also have groups inside of groups.

Note: In general, groups and group membership is primarily managed in Symphony, using the Symphony interface and integrated tools from the Managed module (even if you are only using Visual Data Discovery). Some tasks can be performed, if needed, in the Visual Data Discovery module.

Default Symphony groups include:

Managed Dashboards Module

- **Everyone** - All users are members.
- **Global Users** - System administrators and users you select belong to this group and can access all global content, including content in Visual Data Discovery. Users can see all content as their privileges permit if there are no tenants with separate content in your environment.
- **Developers** - Membership depends on the seat type of a user.
- **Power Users** - Membership depends on the seat type of a user.
- **Standard Users** - Membership depends on the seat type of a user.
- **System Administrators** - Includes users who are system administrators.
- **Tenant Administrators** (***tenant name***) - Includes users who are admins for a tenant. This group is created by Symphony.
- **Tenant Members** (***tenant name***) - Includes users who are members of a tenant. This group is created by Symphony.

Visual Data Discovery Module

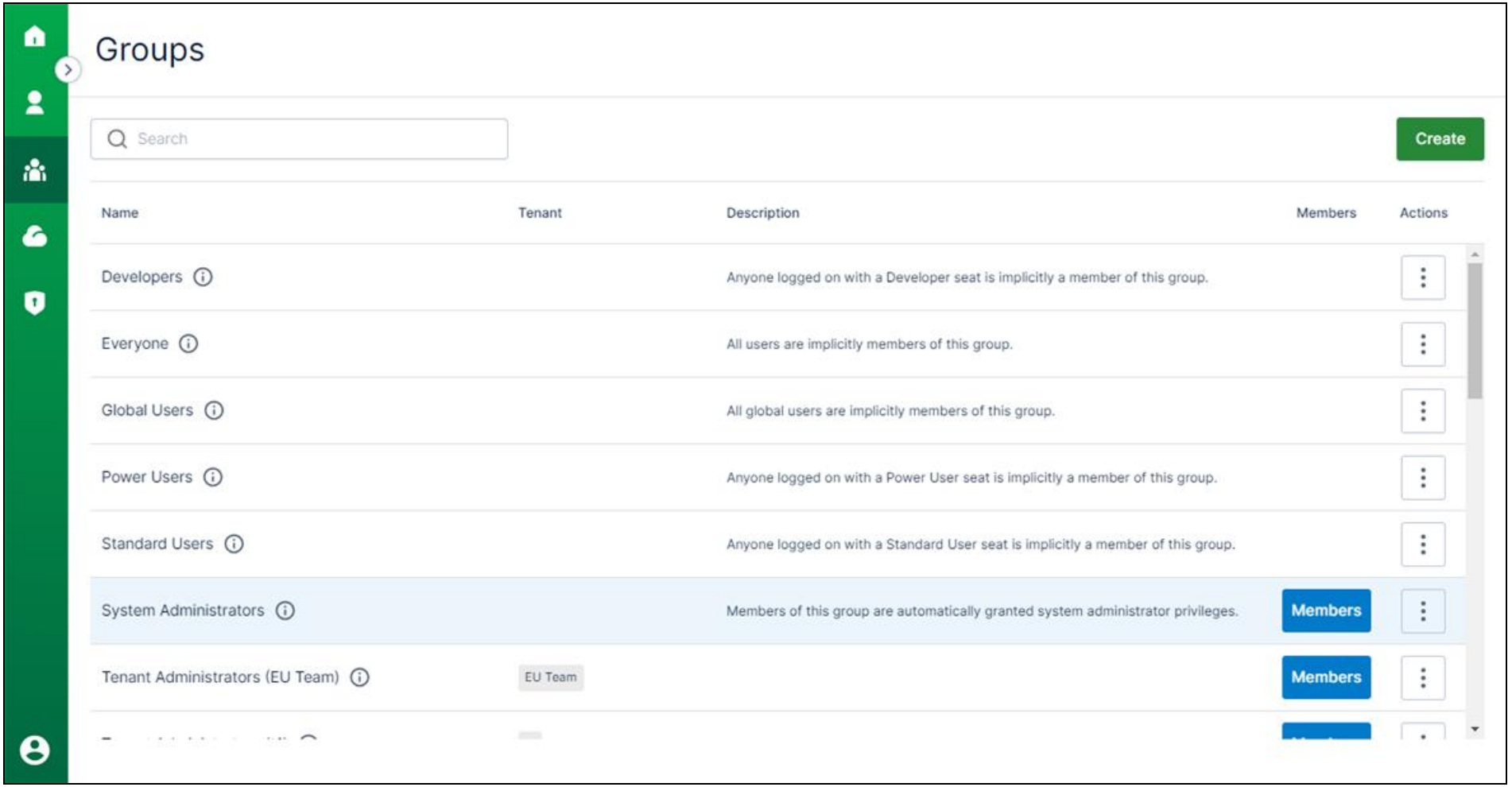
- **Administrators** - All system admins belong to this group. If you are in a tenant, this group contains your tenant admins only.
- **Content Distributors** - All system admins belong to this group. Add non-admin members to this group as needed by editing the user to enable the **VDD Content Distributor** toggle. This allows them to import and export content across tenants for Visual Data Discovery resources.
- **Supervisors** - All system admins belong to this group in all environments. Add non-admin members to this group if needed. This allows them to perform a subset of administrator level tasks in your environment.

Use the Symphony Groups Work Area

Create, manage, and update user group basics as needed all in one place in the Symphony interface.

If you find you need to make more detailed changes to group privileges, you can navigate to the appropriate module from this central location. View a list of groups, add new groups, and add or remove members of a group as needed.

System administrators can use this work area to view and manage group membership and basics for all tenant groups; search for a specific tenant's groups by searching by the tenant name.



For more information, see:

- Create And Edit Symphony Groups
- Advanced Group Management
- Manage User Groups in Visual Data Discovery

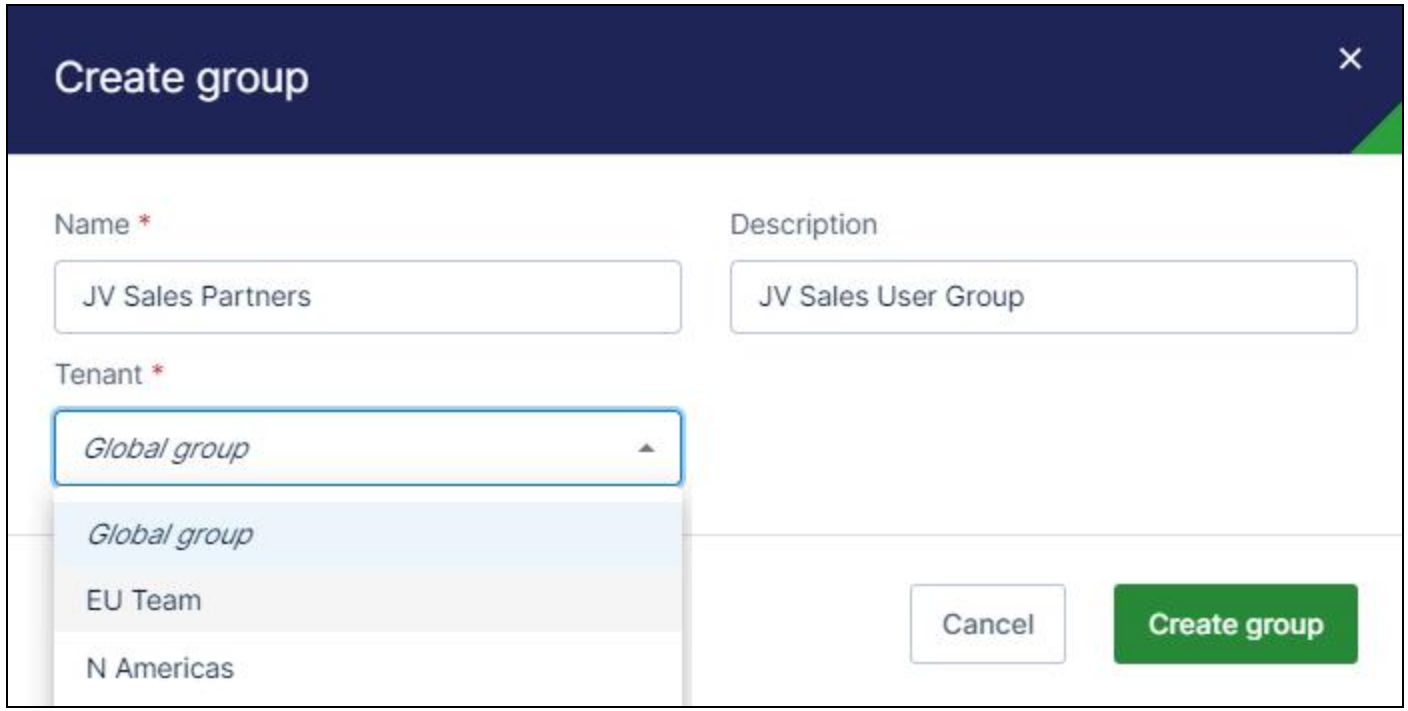
Create And Edit Symphony Groups

Create and edit users all in one place, the Groups work area. Accessible from the Groups option in the main menu, managed your groups and membership quickly and easily.

Create New Groups

Create new user groups to accommodate your organization's needs. Use these groups to assign them specific privileges, or grant them access to specific resources.

1. Log in as a system admin or tenant admin. If you are logged in as a tenant admin, verify you're in or switch to the appropriate tenant.
2. From the main menu, select **Groups**. The Groups work area opens.
3. Select **Create**. A Create group pop up dialog opens.



4. Enter the group **Name** and **Description**. These are required fields.

5. If you are a system administrator, select the tenant you want this group to be created in, or Global group to make it available to all global users.

   If you're a tenant administrator, this field is not shown. The group is created in the tenant you are working in.

6. Select **Create group** when you've entered all required data. A success message appears, and you are returned to the Groups work area.

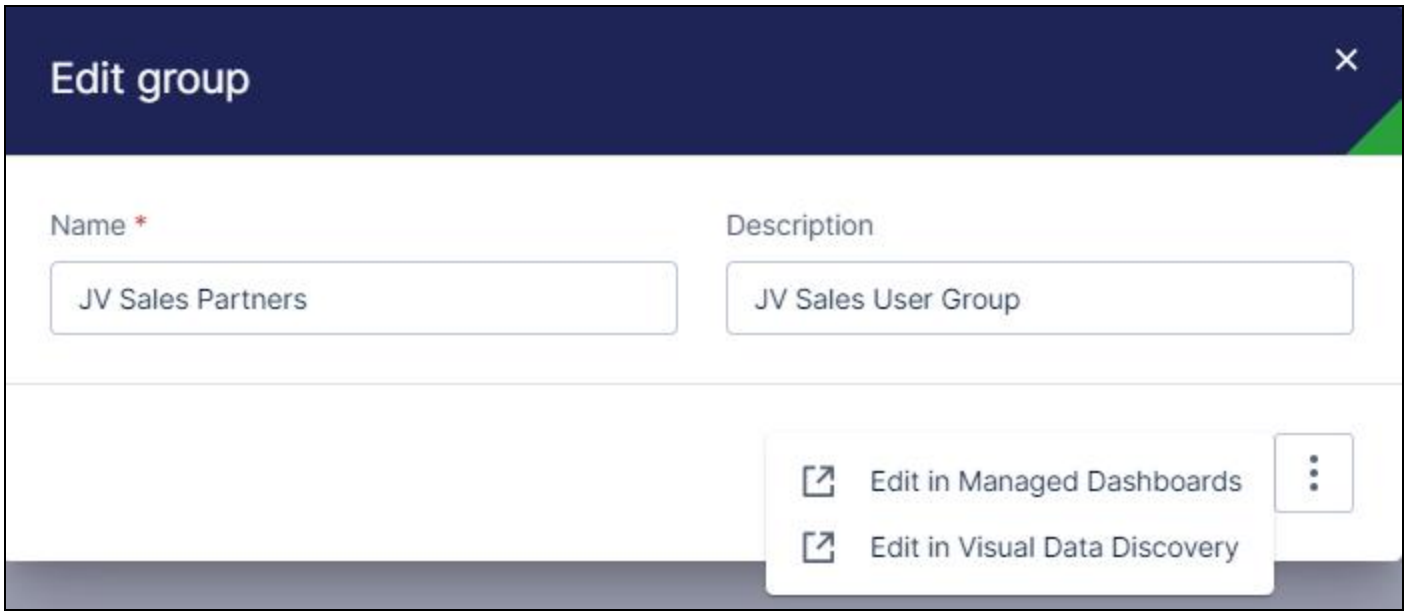
Edit Existing Groups

You can quickly and easily edit a groups as an admin by selecting **Groups** from the main menu on the Symphonyhome page. More advanced changes can be made in the Managed Dashboards module, or the Data Discovery module.

Edit basic group information as a tenant admin

1. Log in as a tenant admin.
2. Verify you're in the appropriate tenant (if you are the administrator for multiple tenants) by selecting **My Tenants** from the main menu.
3. Select **Groups** from the main menu. The Groups work area opens.
4. Scroll to find an existing group, or use the Search field to find a group.
5. Select **Edit group** from the **Actions** menu for the group you want to update. An Edit group pop up dialog opens.
6. Update the group **Name** and **Description** as needed.
7. Select **Update group** to save your changes.

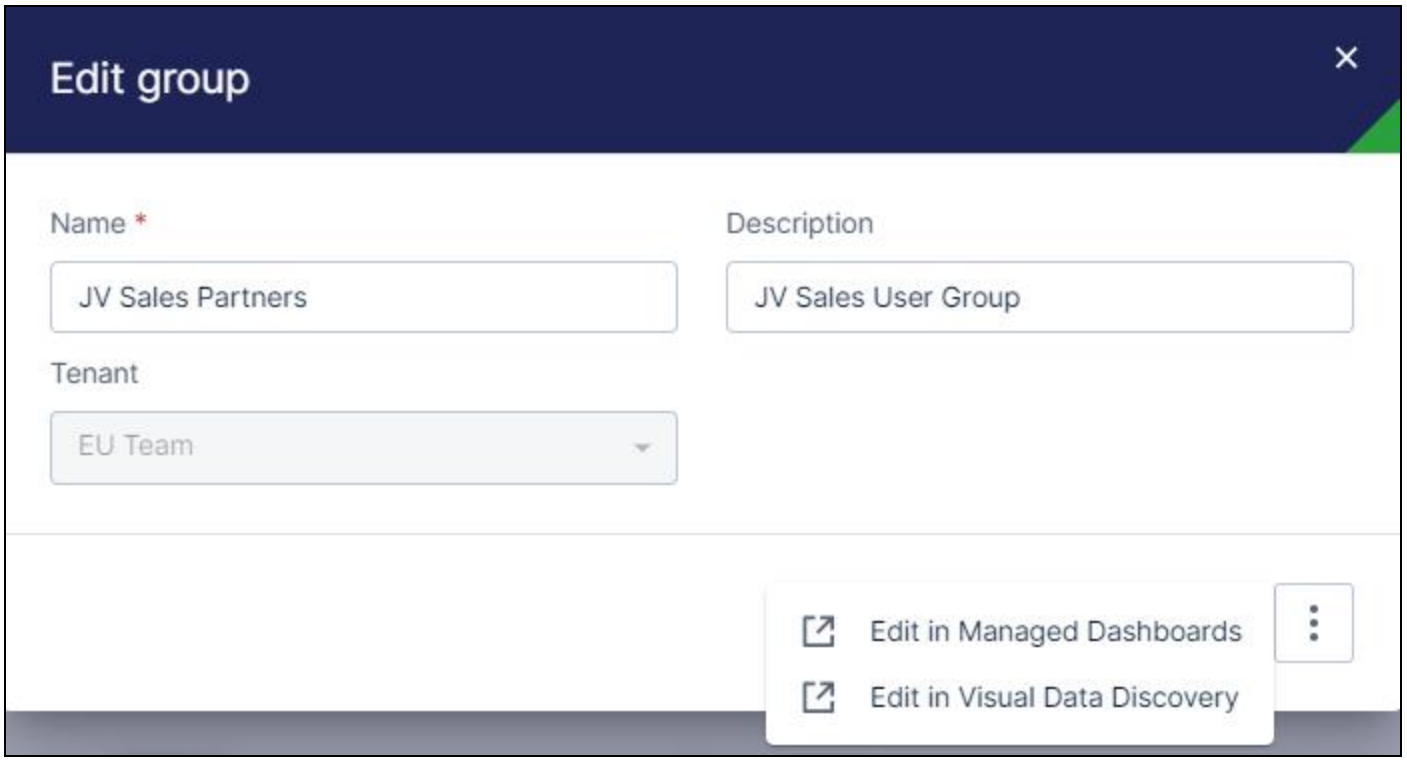
If you need to make other changes to this group, select the action menu in the Edit group pop up, then select a module to edit the group information in that module. Make appropriate changes in Managed Dashboards or in Visual Data Discovery.



Edit basic group information as a system administrator

1. Log in as a system administrator.
2. Select **Groups** from the main menu. The Groups work area opens.
3. Scroll to find an existing group, or use the Search field to find a group.
4. Select **Edit group** from the **Actions** menu for the group you want to update. An Edit group pop up dialog opens.
5. Update the group **Name** and **Description** as needed. The tenant cannot be changed here.
6. Select **Update group** to save your changes.

If you need to make other changes to this user, select the action menu, then select a module to edit the user information in that module. Make appropriate changes in Managed Dashboards or in Visual Data Discovery.



Perform advanced group tasks in Managed Dashboards

Most advanced group tasks are performed in the Managed Dashboards module.

1. Log in as a system admin or tenant admin. If you are logged in as a tenant admin, verify you're in or switch to the appropriate tenant.
2. Select **Groups** from the main menu. The Groups work area opens. Scroll to find an existing groups, or use the Search field to find a group.
3. Select **Edit group** from the **Actions** menu for the group you want to update. An Edit group pop up dialog opens
4. Select the actions menu button, then **Edit in Managed Dashboards**.
5. A list of groups opens. Search for the group, or scroll to find the group you want to edit.
6. Select a group, then **Edit** from the **Contextual** menu, then make and **Save** your group changes.

   See Advanced Group Management to learn more about the changes you can make to your groups in this module.

Perform advanced group tasks in Visual Data Discovery

Some advanced group tasks are accomplished in the Visual Data Discovery module.

1. Log in as a system admin or tenant admin. If you are logged in as a tenant admin, verify you're in or switch to the appropriate tenant.
2. Select **Groups** from the main menu. The Groups work area opens. Scroll to find an existing group, or use the Search field to find a group.
3. Select **Edit group** from the **Actions** menu for the group you want to update. An Edit group pop up dialog opens.
4. Select the actions menu button, then **Edit in Visual Data Discovery**.
5. A work area for users and groups opens. Select the Groups tab, then search for the group, or scroll to find the group you want to edit.
6. Select a group, then make and **Save** your group changes.

   See Manage User Groups in Visual Data Discovery to learn more about the changes you can make to your groups in this module.

See the following topics:

- Add and Remove Members of a Group
- Advanced Group Management
- Manage User Groups in Visual Data Discovery
- Add New Users
- Advanced User Management
- Symphony User Personas
- Supplied Users And User Groups
- Modify Users
- Assign And Remove Users In Tenants

Add and Remove Members of a Group

You can add, and remove users from a group, and groups from a group when you are logged in as a system administrator or tenant administrator.

1. Log in as a system or tenant administrator.

   If you are logged in as a tenant admin, verify you're in or switch to the appropriate tenant. See Switch Tenants.

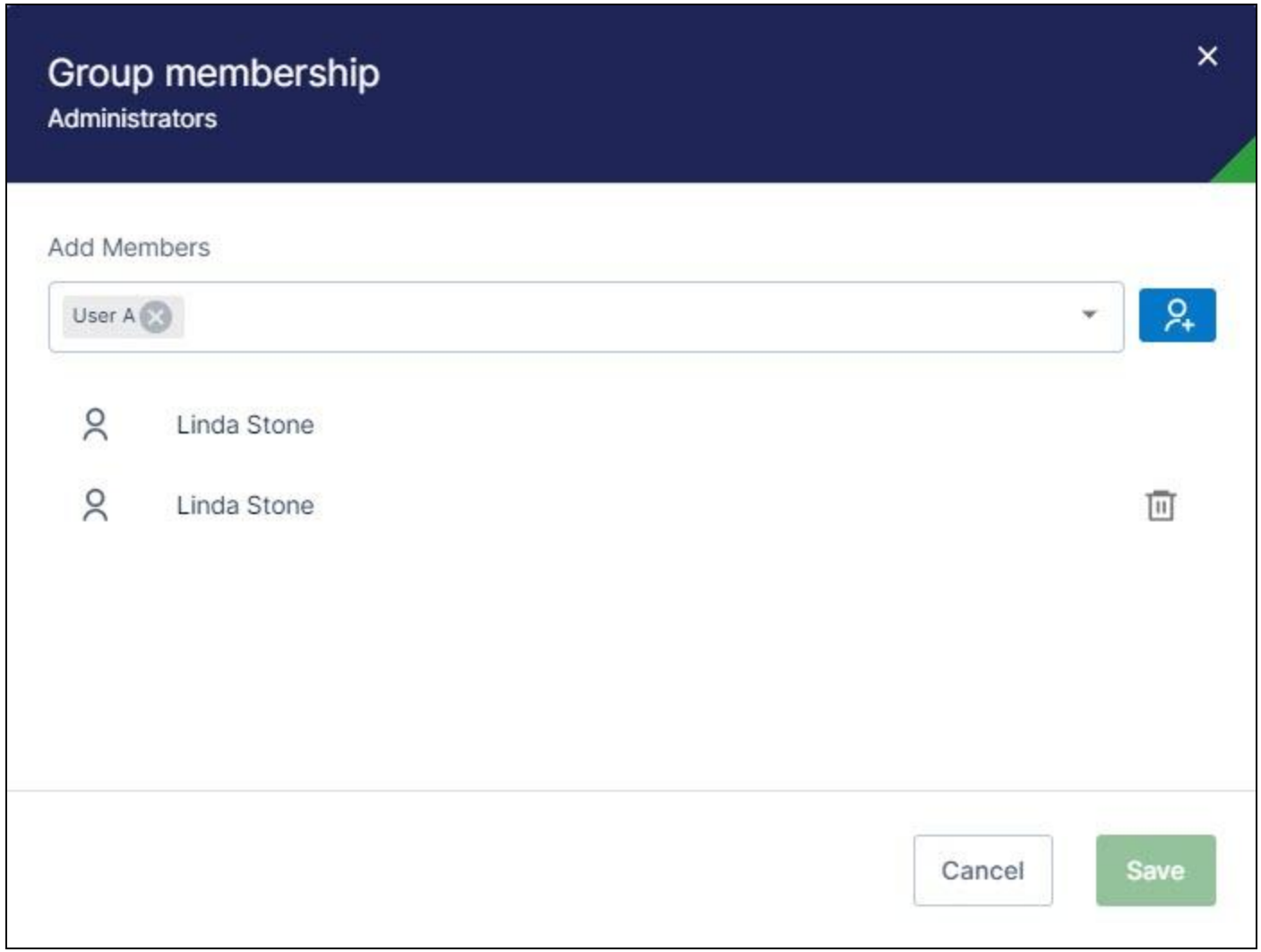
2. From the main menu, select **Groups**. The Groups work area opens, listing the groups you can manage.

3. Select the **Members** button for the group. The Group membership work area opens.

   Note: You can remove members from the group on this screen by selecting the remove icon next to a name.

4. In the **Add Members** field, scroll and select from the available users and groups listed, or enter a few characters to search for specific users or groups.

5. Confirm the names of the new members, then select the add members icon ()to add the listed users and groups to the group.



6. After making your changes, select **Save**. The selected user(s) and group(s) are added or removed and an update confirmation is displayed.

Request and Apply a New License Key

Visual Data Discovery Module

This applies to: *Visual Data Discovery*

> **Note:** Use the DevNet License Manager to obtain license keys. These are provided to the person in your organization we term the License POC (Point of Contact). If you don't know who your License POC is, please reach out to your Account Manager.

> **Note:** When a Symphony standard or trial license expires, only system administrators can log in (to update the license). Regular users are shown a message that the license has expired.

Manage your license keys in one of three ways:

- Manage License Keys In The UI
- Manage License Keys Using The Licensing API
- Manage License Keys Using Configuration Properties Or Environment Variables

Manage License Keys in the UI

This applies to: *Visual Data Discovery*

Apply a new license key:

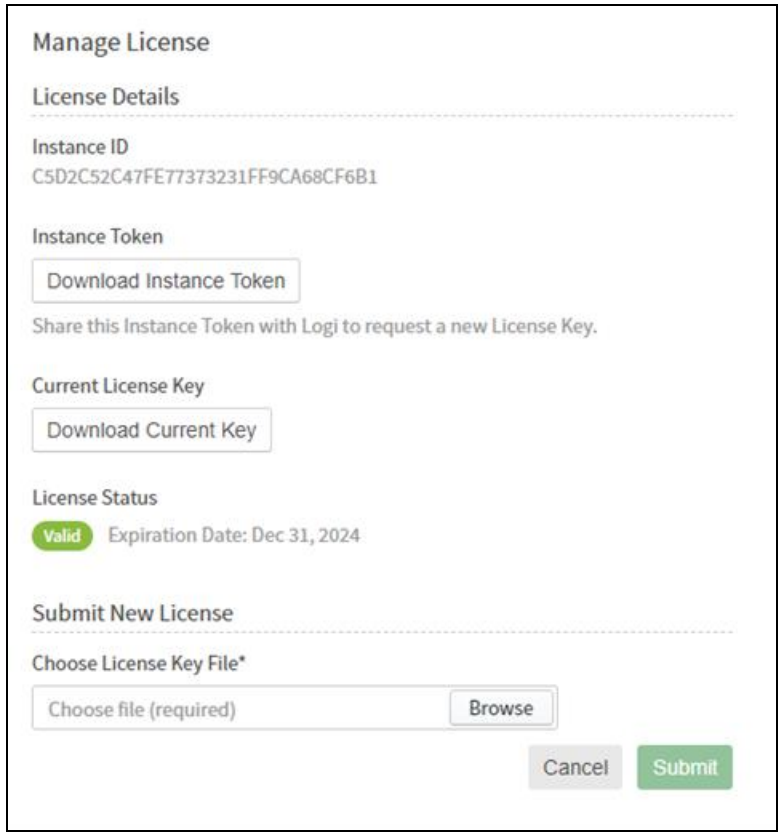
1. In the environment for which you need a new license key, log in as a system administrator.

   > **Note:** To log in after a trial license has expired, navigate to `https://your-symphony-instance/discovery/login` to log in as a system administrator and access the Visual Data Discovery UI.

2. Select **Licenses** from the main menu to open a Licenses work area for all modules.

3. Select **License details** from the **Actions** menu for the license you want to apply an update for. A **Licenses** the Manage License work area appears for this license.

   Alternatively, select **Tools > License** from the main menu in Visual Data Discovery. The Manage License work area appears.



This work area shows your current data discovery instance ID and its current expiration date.

> **Note:** If you select **Download Current Key**, your current license key is downloaded in a `license.key` file.

4. Select **Download Instance Token**. A `.tok` file is downloaded to your computer.
5. Log into DevNet and visit the License Management page to create a license file. You do this by assigning one of your license keys to a specific instance of Symphony data discovery, by uploading the `.tok` file from the previous step. DevNet generates a license.key file, and downloads the file to your machine.
6. Browse to find the license key you just downloaded. Then, select **Submit**. Symphony data discovery applies the new license to your instance.

Manage License Keys Using the Licensing API

This applies to: *Visual Data Discovery*

Endpoint	Method	Description
`/api/license`	GET	Returns license information for the instance.
	POST	Updates license information for the instance

API documentation is provided with your Symphony installation at this link: *`<symphony-URL>/discovery/swagger-ui.html`*.

If a problem occurs, contact your sales or technical support representative.

Manage License Keys Using Configuration Properties or Environment Variables

This applies to: *Visual Data Discovery*

Add your license keys and installation id to `zoomdata.properties`. Format the variables as shown below:

```
zoomdata.license.key=<value>
zoomdata.installation.id=<value>
```

Important: License information provided via configuration properties or environment variables have a higher priority than keys stored in the database previously provided via API or user interface. If you attempt to change the keys using the API in an environment where licensing information from configuration properties or environment variables are in use, Symphony data discovery returns a failure message. Update the license key in the configuration files instead.

Licenses in Managed Dashboards and Reports Module

This applies to: *Managed Dashboards, Managed Reports*

Once you've applied a valid retail license, the evaluation watermark is removed the next time you log in.

Add a new license key (Licenses work area)

1. Select **Licenses** from the main menu. A Licenses work area for all modules opens.
2. Select **License details** from the **Actions** menu. A **Licenses** a work area specific to the module you selected, showing the licenses in your environment.

3. Select **Add New** to add a new license. An **Add License** work area opens.
4. Add the license information in one of the following ways:

i. Drag and drop the license file from your computer or networked location

ii. Select **Choose File** to select a file from your computer or networked location

iii. Copy and paste the license text into the field provided

5. **Save** your license. The license list is updated with the new entry.
6. Log out, then log back in to view the license update, and if applicable, the removal of the evaluation watermark.

View Licenses

View your licenses (Licenses work area)

1. Select **Licenses** from the main menu. A Licenses work area for all modules opens, showing license module name, status, expiration date, and days remaining in the current licensing period.
2. Use the filters to limit the licenses shown by selecting a module, or view all licenses by selecting **All**.
3. To see more information about a specific license, select **License details** from the **Actions** menu.

   A **Licenses** a work area specific to the licensed module opens, showing the licenses in your environment.
4. Take any actions needed for the licenses, or navigate away when you're done viewing the licenses.

Manage Licenses

Use Symphony licenses to incorporate one or more modules into your Symphony environment. This article discusses licensing for the Managed Dashboards and Managed Reports modules and the Visual Data Discovery module.

Managed Dashboards and Managed Reports Modules

This applies to: *Managed Dashboards, Managed Reports*

Important: If you are running Managed Dashboards and Reports along with Visual Data Discovery, you will need a license for each module.

Select **Licenses** from the main menu to open a Licenses work area for all modules. Here you can see overview details about all licenses, or filter only the license types by module you want to see.

Select **License details** from the **Actions** menu to open a work area specific to that module's licenses to manage as needed.

Important: If your licenses have expired or there are other issues with your licenses, system administrator users can still log on. They are restricted to Viewer privileges, but can correct the licensing issue.

Add a License

Note: Obtain your license file or text from your Symphony account manager.

Add a new license key (Licenses work area)

1. Select **Licenses** from the main menu. A Licenses work area for all modules opens.
2. Select **License details** from the **Actions** menu. A **Licenses** a work area specific to the module you selected, showing the licenses in your environment.
3. Select **Add New** to add a new license. An **Add License** work area opens.
4. Add the license information in one of the following ways:

i. Drag and drop the license file from your computer or networked location

ii. Select **Choose File** to select a file from your computer or networked location

iii. Copy and paste the license text into the field provided

5. **Save** your license. The license list is updated with the new entry.
6. Log out, then log back in to view the license update, and if applicable, the removal of the evaluation watermark.

View Your Licenses

You can view your license information in the Licensing work area. Select any license in the list, then select **Details** for more information on the license.

View your licenses (Licenses work area)

1. Select **Licenses** from the main menu. A Licenses work area for all modules opens, showing license module name, status, expiration date, and days remaining in the current licensing period.
2. Use the filters to limit the licenses shown by selecting a module, or view all licenses by selecting **All**.
3. To see more information about a specific license, select **License details** from the **Actions** menu.

   A **Licenses** a work area specific to the licensed module opens, showing the licenses in your environment.
4. Take any actions needed for the licenses, or navigate away when you're done viewing the licenses.

Visual Data Discovery Module

This applies to: *Visual Data Discovery*

Important: If you are upgrading to Symphony, Visual Data Discovery module from Composer, you will need add a license for Logi Symphony as well.

Note: Use the DevNet License Manager to obtain license keys. These are provided to the person in your organization we term the License POC (Point of Contact). If you don't know who your License POC is, please reach out to your Account Manager.

Note: When a Symphony standard or trial license expires, only system administrators can log in (to update the license). Regular users are shown a message that the license has expired.

Manage your license keys in one of three ways:

- Manage License Keys In The UI
- Manage License Keys Using The Licensing API
- Manage License Keys Using Configuration Properties Or Environment Variables

For more information, see Request and Apply a New License Key.

About Symphony Licenses

Use Symphony licenses to incorporate one or more modules into your Symphony environment. This article discusses licensing for the Managed Dashboards and Managed Reports modules and the Visual Data Discovery module.

Managed Dashboards and Managed Reports

This applies to: *Managed Dashboards, Managed Reports*

Managed Dashboards and Managed Reports licenses grant your organization a number of license seats. These licenses license your use of the software, and enables users to log on and use your environment.

Optional features such as SaaS / Multi-Tenancy require licenses as well. Licensed additional features only appear in your software application if enabled through use of a license.

The following articles describe the types of licenses, seats, and how to manage and administer them.

- Manage Licenses
- Cumulative Licensing
- Multiple Servers
- License Types
- Core Counts
- License Seat Modes
- Seat Types
- Elasticity - Hours and Seats
- Configure Elasticity
- Seat Usage for Symphony Licenses

- Floating and Concurrent Logon Sessions
- SaaS and Multi-Tenancy License Assignment

Note: You may need to add a new license if you are upgrading an instance between major versions of Symphony.

Note: Obtain your license file or text from your Symphony account manager.

Important: If your licenses have expired or there are other issues with your licenses, system administrator users can still log on. They are restricted to Viewer privileges, but can correct the licensing issue.

Visual Data Discovery Module

This applies to: *Visual Data Discovery*

Note: Use the DevNet License Manager to obtain license keys. These are provided to the person in your organization we term the License POC (Point of Contact). If you don't know who your License POC is, please reach out to your Account Manager.

Note: When a Symphony standard or trial license expires, only system administrators can log in (to update the license). Regular users are shown a message that the license has expired.

Manage your license keys in one of three ways:

- Manage License Keys In The UI
- Manage License Keys Using The Licensing API
- Manage License Keys Using Configuration Properties Or Environment Variables

For more information, see Request and Apply a New License Key.

Cumulative Licensing

This applies to: *Managed Dashboards, Managed Reports*

Symphony licenses are cumulative. For example, if your organization needs 5 more license seats, you can obtain a license from insightsoftware that adds 5 more users on top of what you already have.

In other cases, a license may replace or invalidate a prior license: adding a retail license on top of the evaluation license that is included with the Symphony installer invalidates the evaluation license.

Where Can I Find My License Information?

This applies to: *Managed Dashboards, Managed Reports*

To view the applied licenses, select **Licenses** from the main menu. A Licenses work area for all modules opens. This includes overview information about licenses for all modules, which you can filter to view only the license types by module. This work area also includes an **Actions** menu you can select to view **License** details about a specific license.

License Types

This applies to: *Managed Dashboards, Managed Reports*

A number of license types are available in your software environment. Depending on the environment you connect to, you may not see all of these license types listed below.

License Type	Description
Evaluation	■ Included with Symphony installer ■ Time-limit of 25 days ■ Watermark appears on UI screens
Retail	■ Designed for productionSymphony instances ■ Invalidates evaluation license ■ Removes watermark from UI screens
Development	■ Designed for development, test, or staging Symphony instances
OEM Retail	■ For ISVs and their clients
Development	■ For ISVs and their clients
Development	■ Used in Symphony training courses/sessions

Multiple Servers

This applies to: *Managed Dashboards, Managed Reports*

Symphony supports multi-server deployment out-of-the-box for load balancing purposes or for failover support. In these scenarios, multiple servers have Symphony installed but they each point to (or share) the same Symphony Application Database.

For licensing purposes, the entire ecosystem of servers and software referencing a single Symphony Application Database is considered one 'instance', and licensing is tied to the instance of the application database. There may be a limit on the number of servers permitted to connect to the application database as indicated in the license.

Core Counts

This applies to: *Managed Dashboards, Managed Reports*

A Symphony license may specify a set number of allowed CPU cores. The core counting method is indicated in the license:

- Per-server – the sum of CPU cores present on the server running the application.
- Per-instance – the sum of CPU cores used by each of the servers running the application (for a load-balancing environment).

If there are more CPU cores available than indicated in the license, Symphony will only use the allowed number of cores.

Note: When running Symphony on a physical machine, physical CPU cores are counted. When running Symphony on a virtual machine, the logical (virtual) CPU cores are counted.

Important: Symphony is limited to a maximum of 64 cores per operating system process.

License Seat Modes

This applies to: *Managed Dashboards, Managed Reports*

A license seat allows users to log on to Symphony. Two license seat modes may be available to support your organization's specific needs: Reserved (Named) Seats and Floating Seats.

Reserved Seats (also known as Named Seats)

- Allows users to log on regardless of who else may be using the application.
- Ideal for users who need use the application frequently or for long periods of time.
- Seat types: Reserved Standard User, Reserved Power User, Developer.
- Symphony Developers always use a reserved seat.

Floating Seats (also known as Concurrent Seats)

- Floating license seats make it possible to support a large number of Symphony users.
- The key is that the floating users cannot be using the application all at the same time.
- The number of floating users logged on simultaneously cannot exceed a certain limit as determined by Symphony licensing.
- Seat types: Floating Standard User, Floating Power User.

To better understand the concept of floating seats, think of chairs at a table. If all of the chairs are taken, people standing will have to wait until someone gets out of a chair before they can sit down.

Note: Accounts set as an API account do not consume a seat, but can only be used for making API calls without using the UI or making a data retrieval call.

For information on managing seat usage, see Seat Usage for Symphony Licenses.

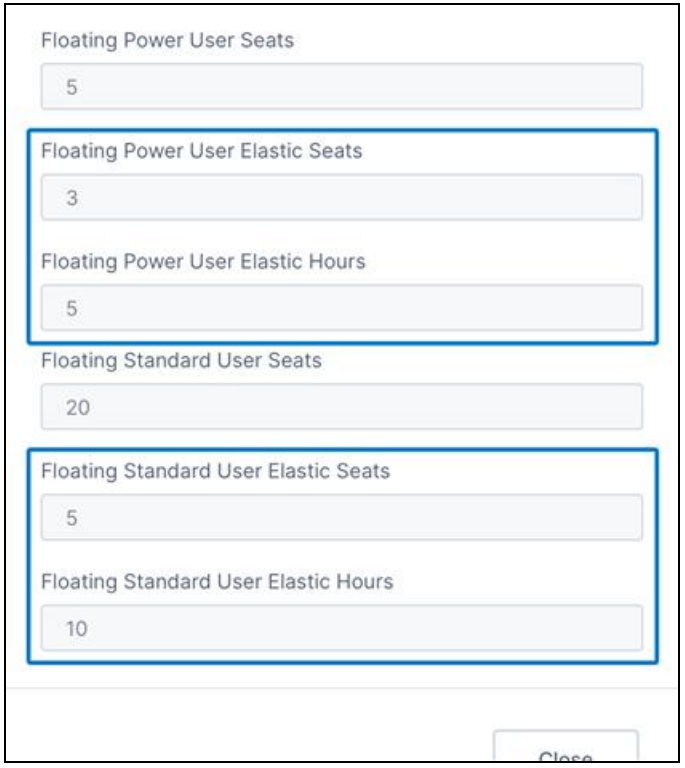
Elasticity - Hours and Seats

This applies to: *Managed Dashboards, Managed Reports*

Elasticity is a built-in feature of the licensing system that allows a user to temporarily exceed the floating license limits. This feature allows a user to log on and continue working while giving Symphony system administrator notice and an opportunity to review the organization's need for more license seats.

A retail license typically includes a fixed number of **elastic hours** for standard users and power users. For example, standard users may be permitted to exceed the license limits by logging on for up to 5 hours (in total for all standard users combined) per calendar quarter. Note that unused elastic hours are not carried over from one quarter to the next.

Besides elastic hours, there is also the concept of **elastic seats**. These represent the number of concurrent users that are permitted to log on and consume elastic hours when all floating seats are occupied. Two license fields, F**loating Power User Elastic Seats** and **Floating Standard User Elastic Seats** represent the maximum number of concurrent users that can be logged on and using elastic seats for power users and standard users, respectively.



See Configure Elasticity for information on managing the elasticity of the seats available to your organization.

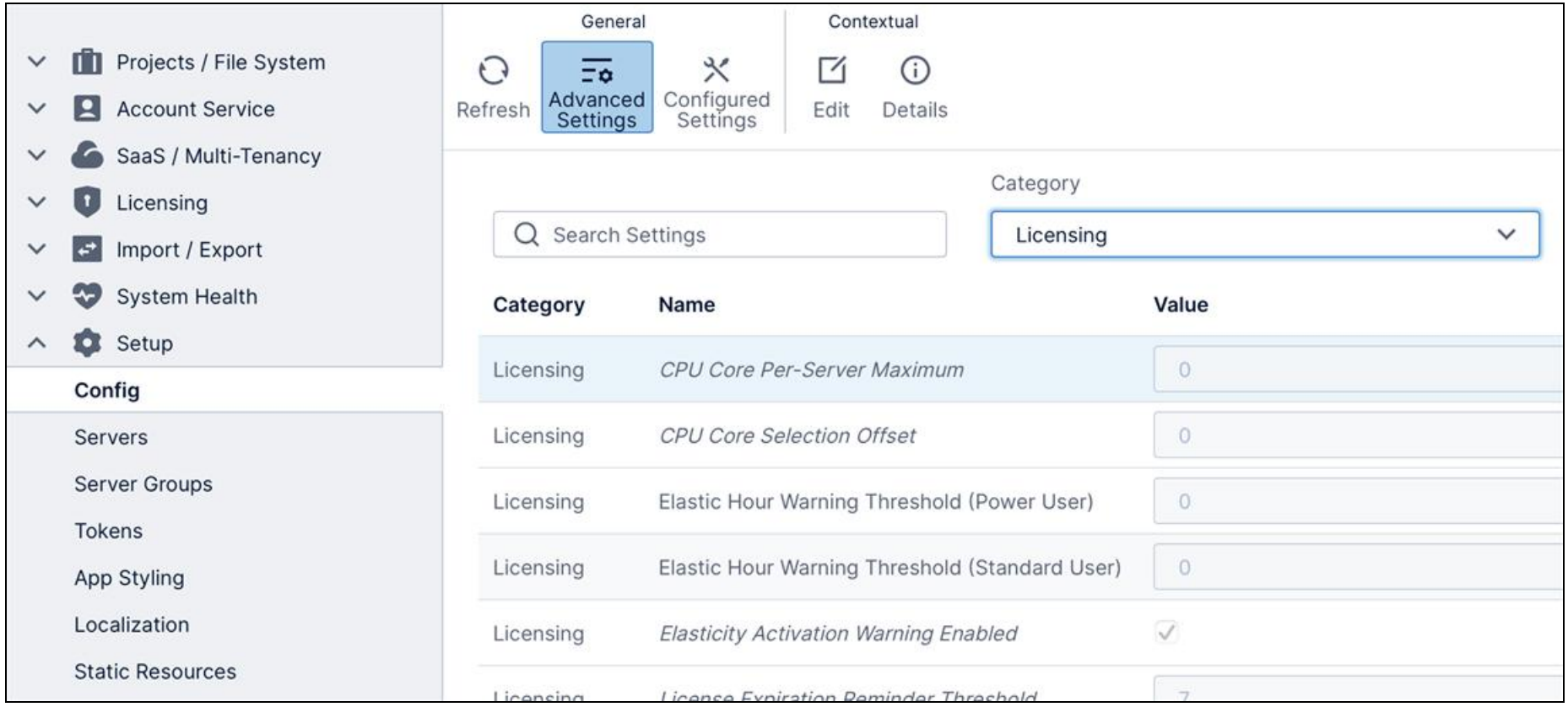
Configure Elasticity

This applies to: *Managed Dashboards, Managed Reports*

There are a few configuration settings related to license elasticity. Use the Setup work area to configure warnings for elasticity use.

Enable elasticity related warnings

1. Connect to Symphony as an administrative user.
2. In the Administration interface, select and expand the **Setup** work area, then selecting **Config**. The configuration work area opens.
3. Select Licensing in the **Category** drop-down, then select **Advanced Settings** in the toolbar. Licensing information and elasticity options open.



4. Enable one or more elasticity options, as needed.

i. The **Elasticity Activation Warning Enabled** setting determines whether an email will be sent to the system administrator or maintainer the first time a user starts using an elastic seat in any given elasticity period. The email will be sent a maximum of one time per calendar quarter. Email settings must be configured to send this notification.

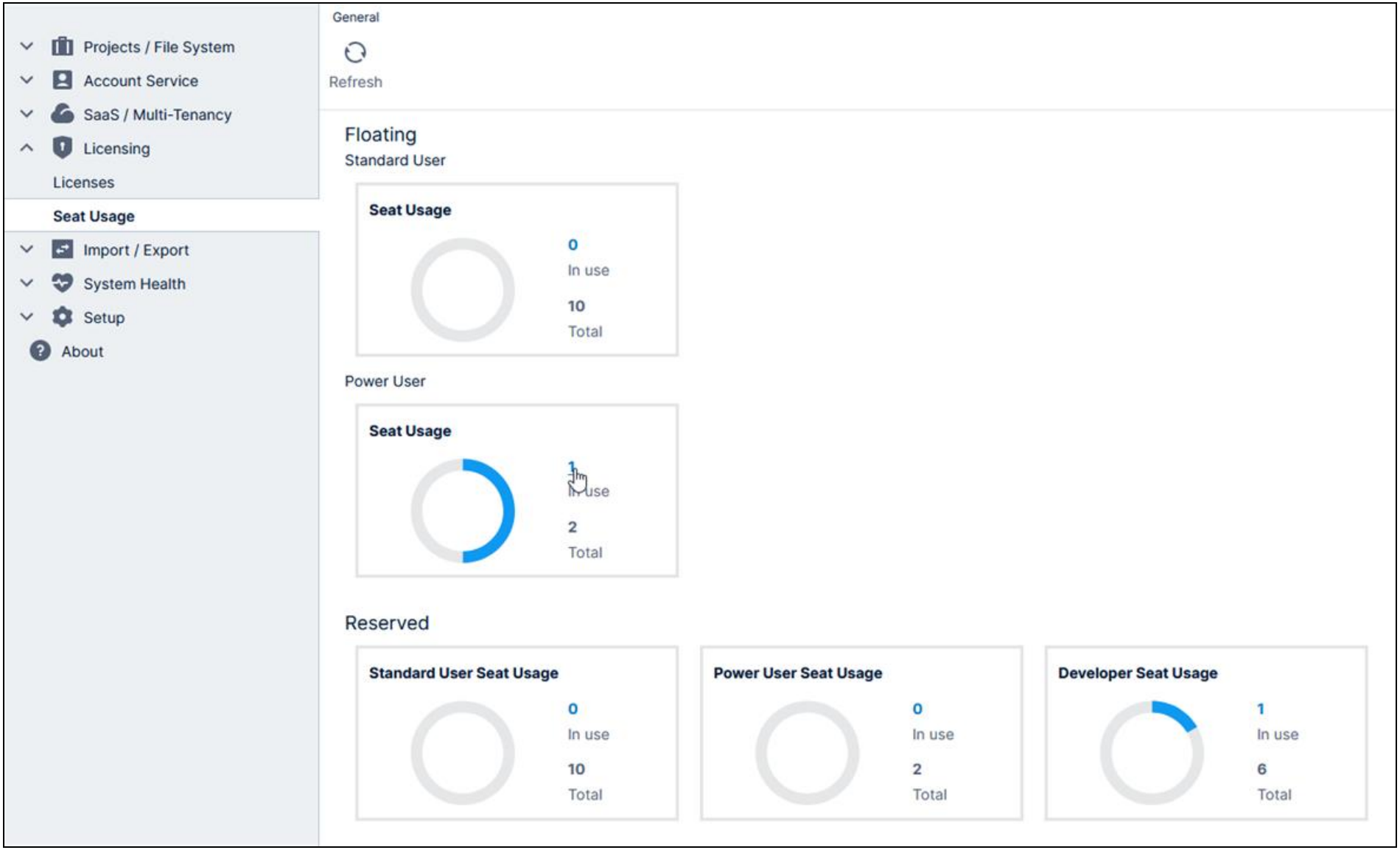
ii. The **Elastic Hour Warning Threshold** settings are used to send an email to the system administrator or maintainer when a specific number of elastic hours are remaining. By default, this is set to zero hours, and the email will be sent when the hours have been exhausted. No warning email is sent if the threshold is set to **-1**.

Manage your license and seat usage remotely using the Administration interface.

Seat Usage for Symphony Licenses

This applies to: *Managed Dashboards, Managed Reports*

The Seat Usage page displays the number and distribution of seats that are currently in use for this Symphony instance as a series of charts.



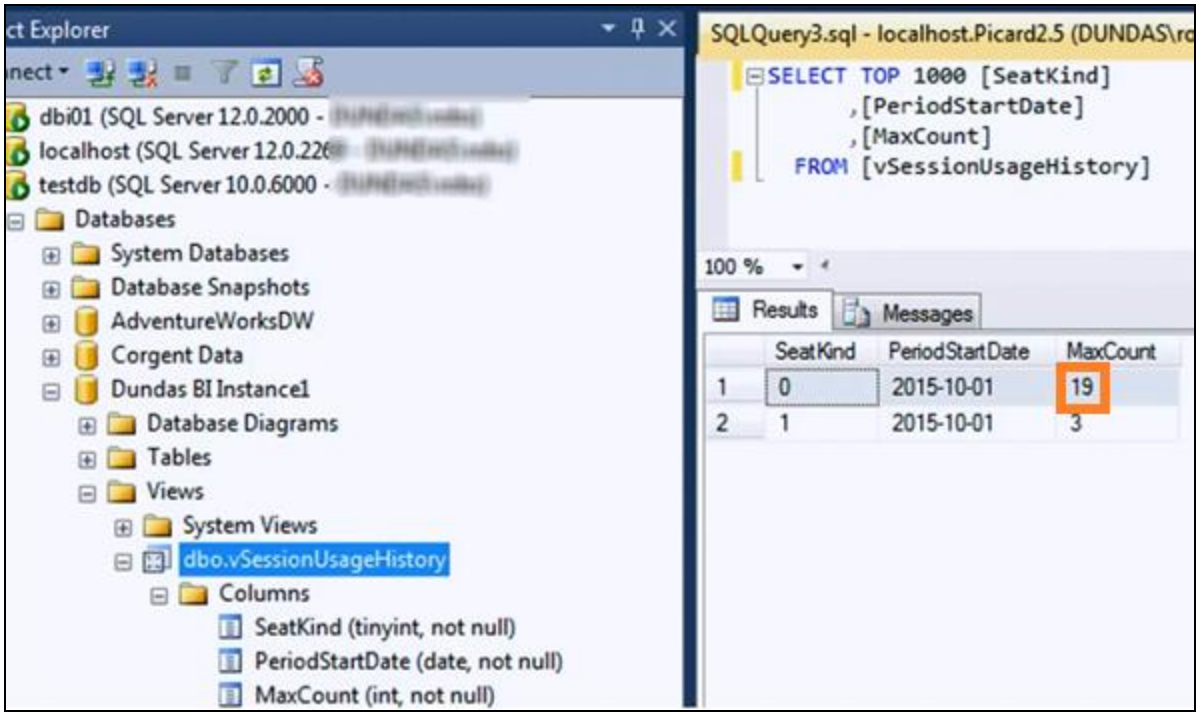
Select a hyperlinked number of in-use seats to see more details. You will be taken to the Active Logons page for floating seats because these seats are taken up by active sessions, versus the page for reserved seats.

Floating and Concurrent Logon Sessions

This applies to: *Managed Dashboards, Managed Reports*

The maximum number of floating (concurrent) logon sessions reached in a given calendar month for each floating seat type (e.g., standard or power user) is recorded in a database view named **vSessionUsageHistory** in the Symphony Application Database. You can use this information to monitor how close your organization is to reaching your floating license limits.

For example, in the figure below, the maximum number of floating logon sessions (for standard users or SeatKind = 0) reached in October 2015 was 19.



The values for the **SeatKind** column are defined in the LicenseSeatKind enumeration.

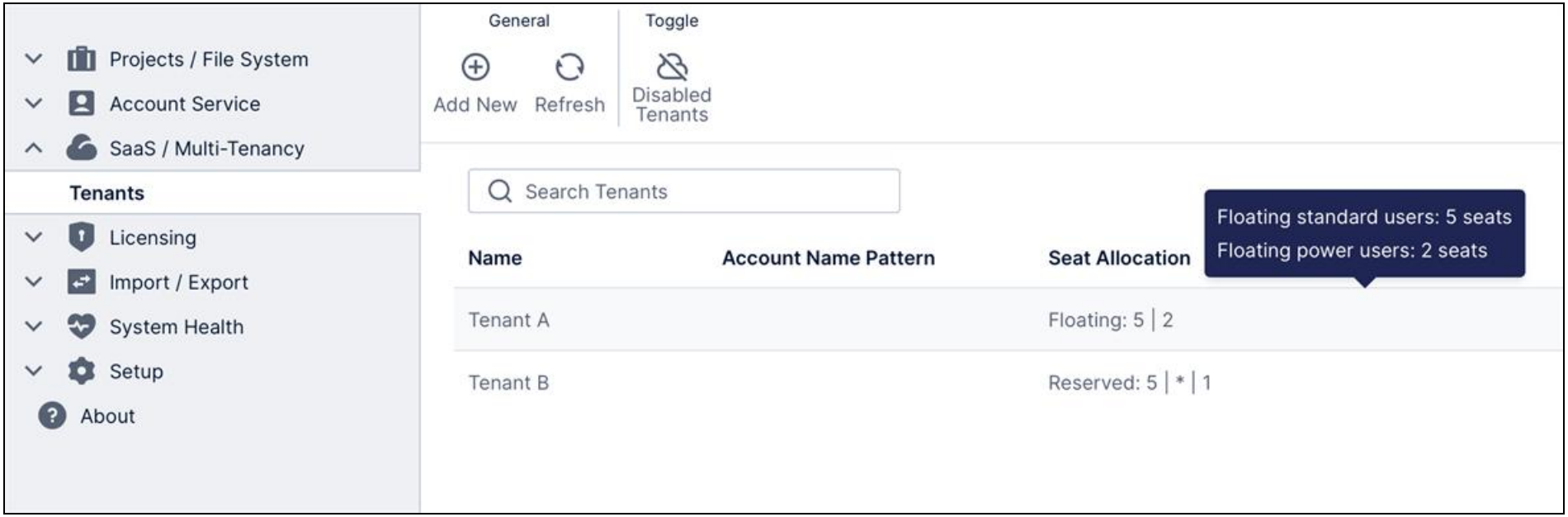
SaaS and Multi-Tenancy License Assignment

This applies to: *Managed Dashboards, Managed Reports*

Symphony provides built-in support for SaaS (software-as-a-service) and multi-tenant scenarios. This feature allows a single instance to serve multiple independent tenants.

Note: This feature is an option you enable through appropriate licensing.

Under the **SaaS/Multi-tenancy** section of Administration, the **Tenants** page allows system administrators to create and set up multiple tenants that are completely isolated from each other. System administrators can also assign seats and elastic hours on a per-tenant basis.



The list of tenants includes a **Seat Allocation** column you can use to quickly view how your licensed seats have been allocated between tenants. More details are listed in a tooltip popup when you hover or long-press the appropriate field.

If **Seat Allocation** is blank, the tenant draws from your overall, or global pool of available seats.

Edit a tenant's Seat Allocation settings to change the allocation.

Each tenant can be assigned their own tenant administrators. Tenant administrators can add and manage users, groups, and projects within their own tenant without having to involve the system administrators.

Note: For tenant administrators, the Seat Usage screen is accessible from the Account Service section.

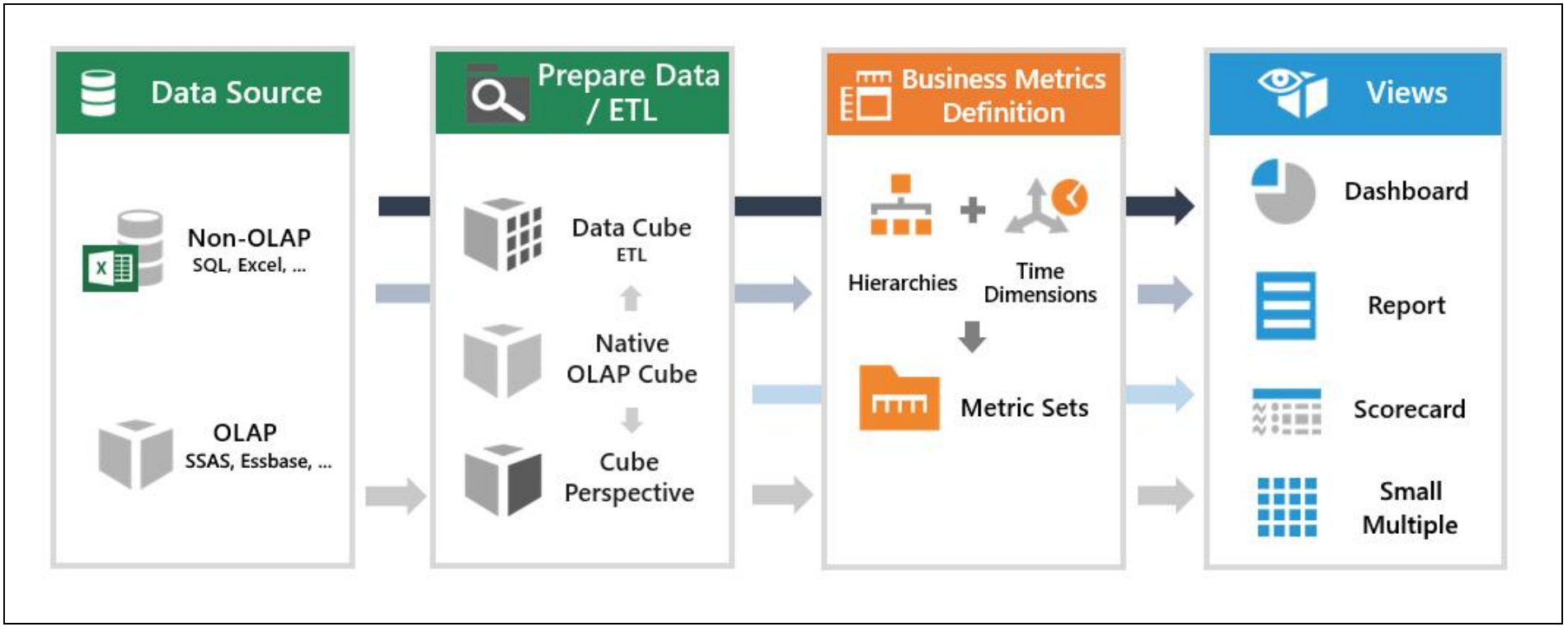
See multi-tenancy for more details on administering tenants.

The Managed Dashboards Data Model

This article outlines the overall data model and how the different types of files you can create work together.

The Data Model

The following diagram shows the main elements of the data model and how data flows in the system. Although the pathways are a bit different if you're working with relational data versus OLAP data, everything is ultimately modeled though cubes and visualized through metric sets.



The data flow is flexible, as indicated by the background arrows in the figure above and described below. You don't need to create every element in the data flow, and can drag and drop a spreadsheet or database table directly onto a dashboard, for example. It is also modular, giving you the opportunity to reuse and collaborate on any part of the workflow.

Related video: Data Flow

Data Connectors

- A data connector holds the information necessary to connect to a data source.
- The connection information required is different depending on the type of data provider that you select.
- For example, to connect to SQL Server, you generally need to choose an authentication method, specify a server instance, and indicate the database you want.
- Once you've created a data connector, you can go to the Explore window to access native data structures such as tables, views, stored procedures, functions, or OLAP cubes.
- For example, you can drag columns from native tables under your data connector and visualize it right away on your dashboard. Behind the scenes, items such as metric sets are auto-generated for you in order to have a complete data flow like the one in the diagram.

Data Cubes (ETL)

- A data cube is a multidimensional model of your data that consists of measures, hierarchies, and metadata such as formatting.
- Works primarily with non-OLAP sources such as relational databases, letting you view your data as a cube without having to use an OLAP system like Analysis Services.
- You can set up an ETL process when editing a data cube by choosing from our wide range of transforms and connecting them together to perform tasks such as data cleansing and combining data.
- The MDX Select transform lets you use an OLAP data source as input for selecting a tabular set of data to join with other data.
- Performance can be improved by using the optional storage types: warehouse to store the cube's output, or in-memory for faster analytics.
- There is always a cube behind a visualization and its metric set, so a data cube may be auto-generated for you if you drag data directly from a data connector so that you can start to work with it immediately.

Hierarchies and Time Dimensions

- Hierarchies (also called 'dimensions') are used for grouping data into rows and columns, and setting up drill downs.
- Hierarchies can have multiple levels, allowing you to easily drill up/down, expand upper-level items, or change levels.
- You can optionally define a hierarchy and its available settings ahead of time, or you can just use a plain column of data such as text or date values as a hierarchy directly.
- A time dimension is a container for one or more date and time hierarchies that are based on the same calendar system, which you can use with any column of date values to group and explore by levels such as Year and Month.
- Each project has a built-in time dimension ready to use, which you can modify if needed (e.g., to add levels such as Hour if your data includes times of day).
- New time dimensions can also be created, optionally based on other calendar types such as your company's fiscal calendar.

Metric Sets

- A metric set selects a set of data from a data source or cube to display, and performs analytic tasks on it such as grouping, sorting, filtering, and formula calculations.
- To define a metric set, you add measures (numerical data), assign hierarchies to its Rows, Columns, and Slicers axes, and change their settings.
- In this way, a metric set is like selecting data in a 'pivot table', a query against an OLAP database, or other applications that use dimensions and measures.
- Metric sets also handle other things specific to the data you're selecting, including states, missing data rules, and formatting. These settings will apply regardless of which visualization you choose to use to display the metric set, and a single metric set can be reused multiple times and visualized in different ways.
- A metric set may be auto-generated for you. For example, you can drag and drop data directly onto a dashboard without first creating a metric set from the main menu.

Views

- Dashboards, reports, scorecards, and small multiples are all different types of 'views', which display data by combining multiple visualizations connected to metric sets.
- Dashboards are the easiest type of view to create, allowing you to simply place content where you want it, usually for display on a screen.
- Reports lay out content into multiple pages with scrolling, ideal for saving to PDF and for printing. (Reports meant for displaying on your screen without much scrolling can usually be created using a dashboard.)
- Reports, scorecards and small multiples have a lot in common: they give you an easy but structured way to create complex views involving repeated visualizations, just by using drag-and-drop operations.
- You can also add one view inside another: for example, a scorecard view can be dragged onto a dashboard and combined with other content, or you can create a dashboard combining several smaller dashboards together into a personalized view of data.
- Slideshows can display the views you select in sequence as a presentation, on automatic rotation, or combined into a single exported file such as PDF or PowerPoint.

OLAP Sources

In the case of OLAP data sources, there is no need for another data cube because OLAP cubes are already multidimensional data sources that can be used directly. For example, if you have a data connector hooked up to a Microsoft SQL Server Analysis Services (SSAS) database, you can go to the Explore window and see the database's cubes under the data connector, and the measures and dimensions under each cube. Drag any measure or dimension onto a metric set or dashboard canvas, and the metric set will be based directly on the OLAP cube.

Cube Perspective

A cube perspective lets you define a subset of a native OLAP cube. This is an optional item you can create in order to limit the measures and dimensions available to users when creating corresponding metric sets, dashboards, reports, etc.

For more information, see:

- Video: Data Flow
- Seat Types

Seat Types

This applies to: *Managed Dashboards, Managed Reports*

Each user in Symphony is assigned a seat type, which determines which areas of Symphony they can access if not restricted by other privileges. See Symphony Managed Dashboard and Managed Report Security.

- **Standard Users** and above (all users) can create and interact with views such as dashboards, reports, and slideshows to combine visualizations together, filter, drill down, etc.
- **Power Users** and above can create and edit metric sets to access data sources or cubes directly and choose which columns or dimensions to view and analyze, joining data sources together if needed.
- **Developers** can create and edit data cubes and access the full set of data transformation, querying, and scripting options.

Standard users can interact with metric sets created by other users but not directly with any data sources or data cubes. Similarly, power users can use data cubes created by developers but cannot see or change how the data cube was set up for them.

Administrators can assign seat types to individual users, or to groups of users that use floating seats.

Feature Security

This applies to: *Managed Dashboards, Managed Reports*

Application privileges control which users have access to specific capabilities and functionality. For example, users can be prevented from making measure value corrections that will be seen by other users, or writing manual queries that modify data sources. You can also customize the options shown in the UI such as filtering or sharing/exporting. See the article on application privileges for the full list.

Application privileges can be set up by administrators on user accounts or groups of users, or they can be disabled on views or visualizations along with other options such as Re-Visualize menu items for anyone viewing that dashboard, report, or other view.

Data Security

This applies to: *Managed Dashboards, Managed Reports*

Symphony Managed Dashboards and Managed Reports support user-based filtering of data or row-level security using attributes that describe each logged-in user and can be used to filter the data they see. You can create your own custom attributes and assign values to user accounts or groups of users to use for filtering against a particular column, for example returning only data where the Region is North America for the appropriate users.

- Set up a security hierarchy based on custom attributes to completely hide non-applicable values from users, including in filters, while allowing for the option to use data cube storage options.
- You can also configure a transform in a data cube to filter the data according to an attribute such as account name or a custom attribute.
- Some data sources may already have row-level security set up. If you use impersonated Windows credentials or roles impersonation when creating the data connector, or if each user creates their own data connector with their own credentials, each user will see data according to the existing rules.

When creating a data connector or data cube for other users to use, you can also determine which tables, columns, or cubes are included, for table-level and column-level security. Select data structures to include under a data connector, or columns to include in a data cube's select transform or process result. When connecting to an OLAP database, cube perspectives define a subset of measures and dimensions to be provided when using them. The security privileges described in the previous section can be used to provide access to only the appropriate files to each user. DundasScript used for example in a data cube's calculated element can check the current session and the user's attributes or custom attributes to determine whether or which values should be displayed depending on the user.

Metric sets have options to make use of measures for formulas or states, for example, but hide their values completely from users visualizing the result or exporting the data. If users should be able to visualize but not export data, you can also prevent export of metric sets or only certain measures or hierarchies.

Organizational Security

This applies to: *Managed Dashboards, Managed Reports*

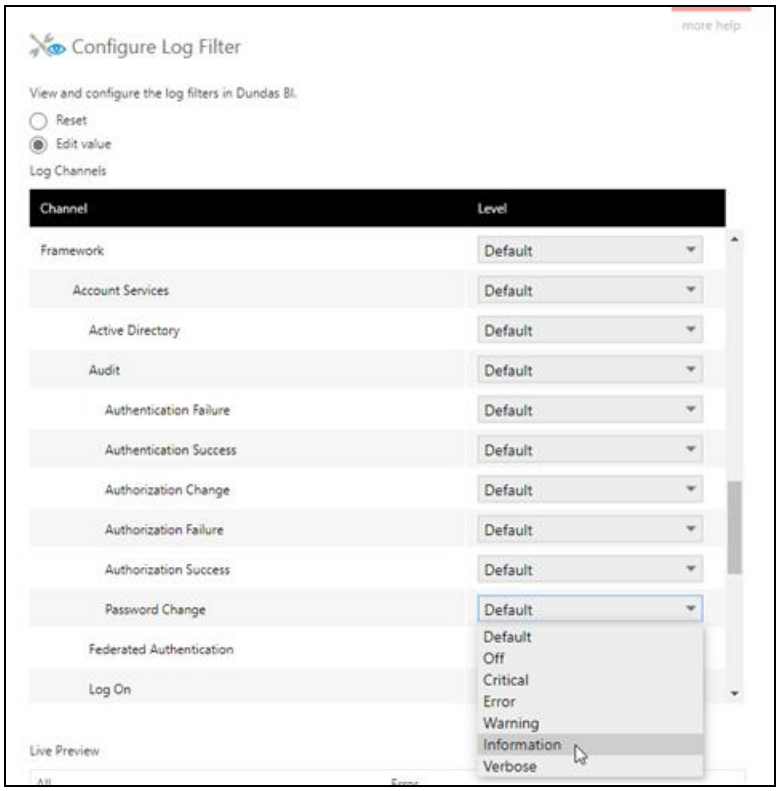
Your organization's infrastructure and security practices are supported by various features, such as authentication, auditing, usage tracking, data privacy, and multi-tenancy.

Authentication

Rather than requiring setup of separate accounts and credentials, Symphony supports built-in integration with a variety of identity providers you may already be using at your organization and single sign-on so that users don't need to sign in separately to use Symphony.

Auditing

Symphony provides fine-grained logging options that can be used to keep track of authentication, authorization, and other events in the application logs. Entries are determined by the Log Filter in the configuration settings.



Usage Tracking

Your instance of Symphony can locally record usage data. Record such things as which users are viewing specific dashboards and reports, and for what length of time. Review this data using the Usage Tracking Dashboard sample available from the Deployment application, or analyze the data on your own.

Data Privacy

Since Symphony is installed on your own IT infrastructure, Symphony does not have access to any of your data. The amount and type of data that you wish to expose to your users is entirely within your control.

Multi-Tenancy

If you are providing Symphony to different customers or departments, or another scenario requiring isolation between different groups of users,Symphony has built-in dedicated support for separate tenants. Each tenant can operate as if it was its own application with separate licensing, administrators, users, and groups,

where tenant users will never know about the existence of other tenants. Tenant users can be allowed to create and manage their own content while allowing you to also share content across all tenants.

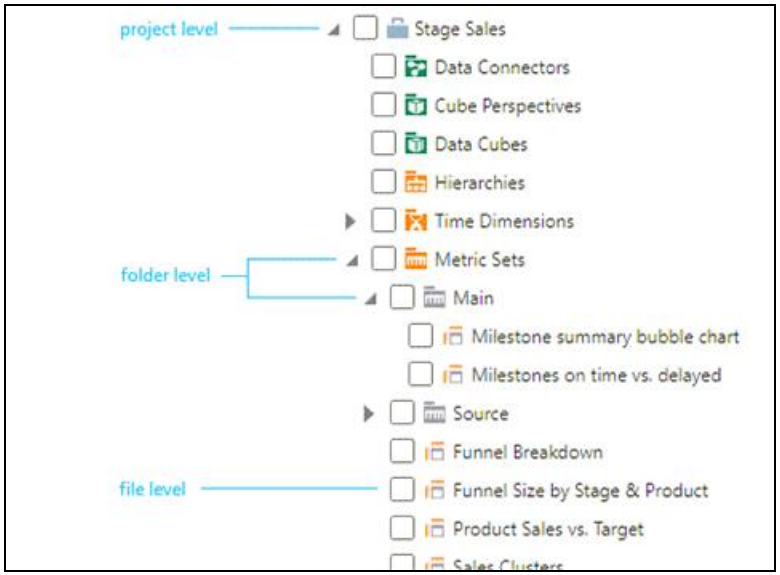
For details on tenant management and options in Symphony, see Multi-Tenancy in Symphony.

Content Security

This applies to: *Managed Dashboards, Managed Reports*

Each piece of content created in Symphony Managed Dashboards and Reports is saved as a file, including data connectors, data cubes, and dashboards. Each file is located in a project that is set up for personal use, collaboration in teams, or for sharing.

Security privileges can be set up on projects, folders, or individual files to customize which user accounts or groups can access them and their level of access. For example, on each item, you can decide who can read (e.g., view), write (e.g., edit), list folder contents, or delete a file. Grouping files into folders allows you to set up security privileges on all contained files together.



Any user can customize the security privileges on an item if they are assigned the Full Control privilege on it themselves, for example if they created the file. For a full list of security privileges and how to set them, see the article on file and folder properties.

Symphony Single Sign On

This applies to: *Managed Dashboards, Managed Reports*

Single sign-on (SSO) allows users to log in once on their workstation, and gain access to multiple systems without being prompted to log in again. This article provides guidelines and summarizes how to use SSO within the Symphony application.

There are multiple ways to accomplish single sign-on:

- Federated authentication: see Enabling Federated Authentication.
  - Federated authentication behaves as Single Sign On (SSO), enabling the user to access multiple services without the need for further authentication.
  - Authentication is possible using SAML 2.0, OpenID Connect (OIDC), Azure Active Directory/Microsoft Identity, JWT, and other protocols.
  - Automatic logon with federated authentication can be accomplished by setting the custom logon page configuration setting to the authentication URL: `https://yourinstance/AuthBridge/Auth/ExternalAuth`

- Anonymous logon: see How To Enable Anonymous Log On.
  - Use to provide access to some or all Symphony Managed content without any users needing to take any action to log on.
  - This is ideal for implementation of a public dashboard/reporting site or kiosk.
  - Users are automatically logged onto a specific account specified in the application configuration settings **Anonymous User Name** and **Anonymous Password**.

- Embedding Symphony content: see Create And Use Logon And Session Tokens For Symphony.
  - Your application can use optionally use Symphony's API to create one-time tokens to log in users automatically and securely.
  - Create and pass a one time **logon token** to create a session for a specified user and log them on.
  - Log on through the API and create a session for the user, optionally setting up session properties such as custom attributes, and create a one-time **session token** the user can use to access that session.
  - Use server-side code to create these one-time time-limited tokens and pass them to your client application's JavaScript or HTML.

    Note: You can also use the federated authentication feature to authenticate using JSON Web Tokens (JWTs). These are different from Symphony logon and session tokens.

Create and Use Logon and Session Tokens for Symphony

This applies to: *Managed Dashboards, Managed Reports*

When you embed Symphony in another application, you can Symphony's API as an alternative to other SSO login options to create one-time tokens to log in users automatically and securely. Use server-side code to create one-time time-limited tokens, then pass them to your client application's JavaScript or HTML.

You can create:

- A one time **logon token** to create a session for a specified user and log them on.
- Log on through the API and create a session for the user, optionally setting up session properties such as custom attributes, and create a one-time **session token** the user can use to access that session and to confirm ahead of time that the logon is successful.

For example, your server-side code can create these one-time, time-limited tokens and pass them to your client application's JavaScript or HTML.

> **Note:** You can also use the federated authentication feature to authenticate using JSON Web Tokens (JWTs). These are different from Symphony logon and session tokens.

Create Tokens

Create logon tokens through the .NET API using GetLogonToken(LogOnParameters) or through the REST API using POST /LogOn/Token. Specify the `EffectiveAccountName` in the options when calling with administrator account privileges to log on a different, specified user account. For more information and a working example, see POST /LogOn/Token.

For session tokens, first log on the desired user using ILogonService in .NET or POST /LogOn using the REST API. Similar to when creating logon tokens, you can specify the `EffectiveAccountName` when calling with administrator account privileges. In Symphony 24.4 and later, you can also specify `CustomAttributes` to apply or `AccountProperties` for creating or updating accounts. Otherwise, use the session ID you obtain as a result of logging on, you can use ISessionService methods or a REST method such as POST /Session/CustomAttributes to customize the session, then create a session token using ILogonService.GetSessionToken or POST /Logon/GetSessionToken.

Use Tokens

To make use of a one-time logon or session token, you can:

- Pass it as `logonTokenId` or `sessionToken` in the Symphony URL's query string parameters (for example, `https://symphony.example.com/managed/?logonTokenId=<token>`), or set the respective option when using the embed library. This will automatically log the user on.

- Use the token in your own API calls to obtain a `session ID` to pass in subsequent calls when performing actions on the user's behalf. To use a logon token to access the REST API, for example, call POST /LogOn specifying the LogOnToken option instead of credentials to get the session ID, then pass it in Authorization request headers (for example, `Authorization: Bearer <session ID>`) to other REST API methods. To exchange a one-time session token for a session ID instead, call POST /LogOn/ExecuteSessionToken.

For a sample web application that uses server-side code to get a logon token and use it to embed Symphony, see the Symphony viewer integration sample.

Application Logs

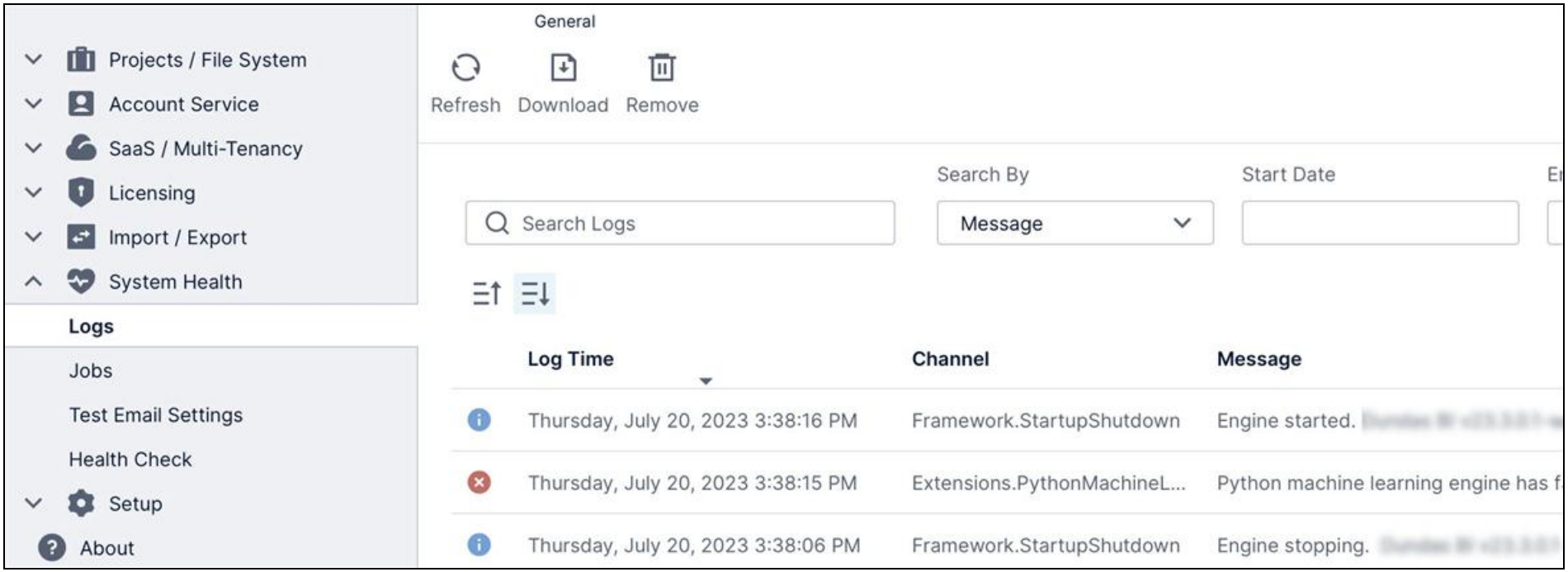
This applies to: *Managed Dashboards, Managed Reports*

The application log in Symphony can help you troubleshoot operational warnings or errors and diagnose performance issues.

View the Application Log

To view the application log in Symphony, expand the **System Health** category along the left side of the administration interface, and then click **Logs**.

The application log entries are displayed in a table on the right.



To search for log entries, use the **Search** box and choose one of the following attributes of a log entry in the **Search By** drop-down:

- Level - This is the severity level of the log entry (Critical, Error, Warning, or Information).
- Channel - Identifies a specific area of the Symphony application that is the source of the log entry (e.g., Framework.Licensing).

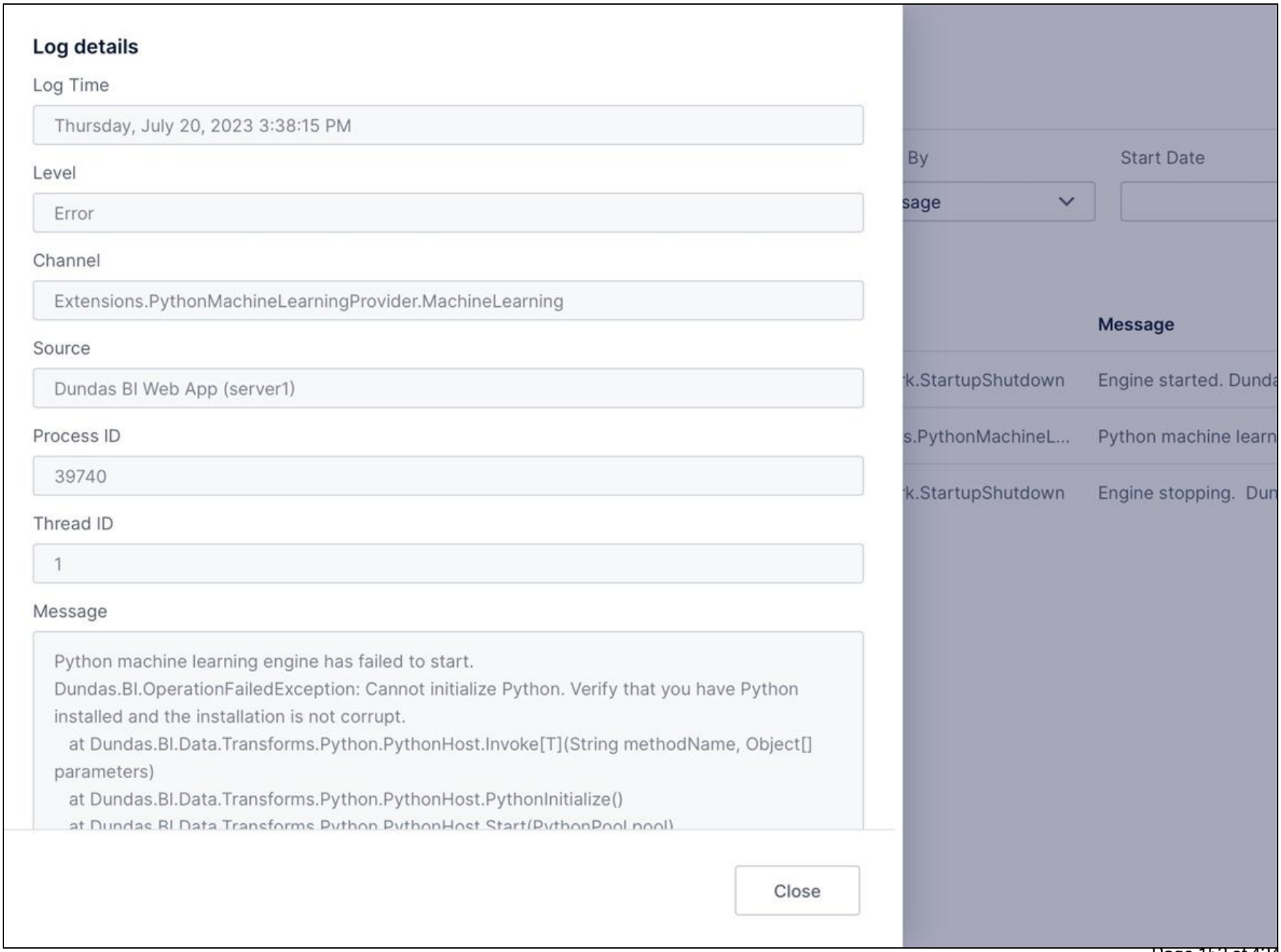
- Message - This is the description for the log entry.
- Account ID - View logs for a specific account ID.

Or, sort the log entries by Level, Channel, or Log Time using the **Order By** drop-down, and use the buttons after it to switch between ascending and descending order.

The *Log Filter* configuration setting determines what events are logged by the system – see Configuration settings for more details. You can change what log entries appear if you don't see the ones you expect or if you need more information while diagnosing a problem.

View Log Details

Click to select an entry in the log table and click **Details** in the toolbar to see more details of the entry in the dialog that opens. You can also double-click an entry instead.


Log details
Log Time
Thursday, July 20, 2023 3:38:15 PM
Level
Error
Channel
Extensions.PythonMachineLearningProvider.MachineLearning
Source
Dundas BI Web App (server1)
Process ID
39740
Thread ID
1
Message
Python machine learning engine has failed to start.
Dundas.BI.OperationFailedException: Cannot initialize Python. Verify that you have Python installed and the installation is not corrupt.
at Dundas.BI.Data.Transforms.Python.PythonHost.Invoke[T](String methodName, Object[] parameters)
at Dundas.BI.Data.Transforms.Python.PythonHost.PythonInitialize()
Close
By
Start Date
Message
k.StartupShutdown
Engine started. Dunda
s.PythonMachineL...
Python machine learn
k.StartupShutdown
Engine stopping. Dun

Remove Old Log Entries

By default, log entries are deleted automatically based on the *Log Entry Maximum Age* configuration setting. This is set to 30 days initially which means once a log entry becomes older than 30 days, it is removed.

If you want to manually delete log entries yourself, you can do so from the Logs screen by clicking **Remove** on the toolbar.

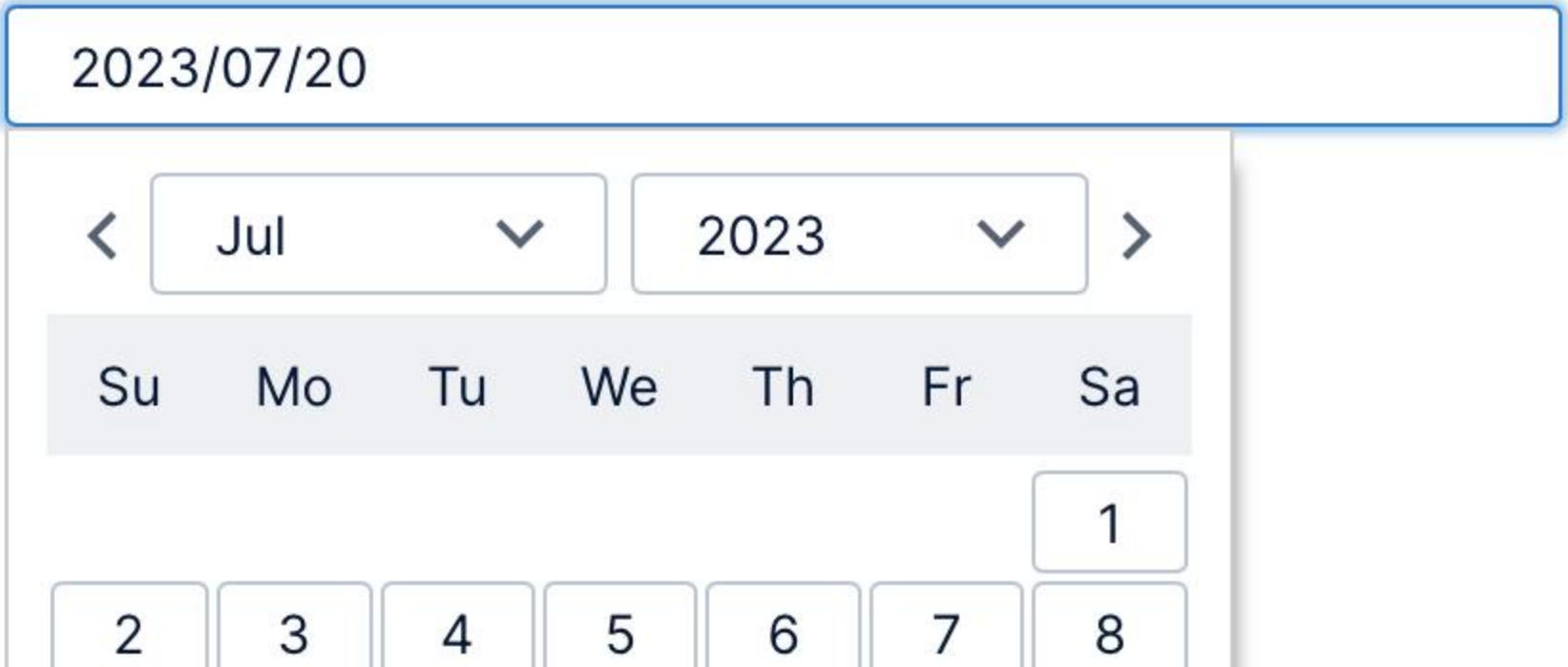
In the dialog that appears, click inside the text box, and then use the calendar to select a date. All log entries older than this date will be removed. Click to **Save** to perform the removal.

Remove logs

Remove all log entries that occur before the specified date. Log entries are automatically removed based on the 'Log Entry Maximum Age' setting.

Data is removed independently of any filters configured in the main screen.

Remove before



Download Logs

Click the **Download** icon on the toolbar to download a .CSV file containing all of the logs in the application based on the applied filters.

This file can be viewed in Excel, for example. You may need to resize or select some cells in order to view the entire message or the date of an entry.

Note: The exported file follows the Excel cell limit of 32,767 characters and an entry is included listing the time zone of the entry log times.

For more information, see:

- Configuration Settings
- Monitoring System Health

Application Privileges

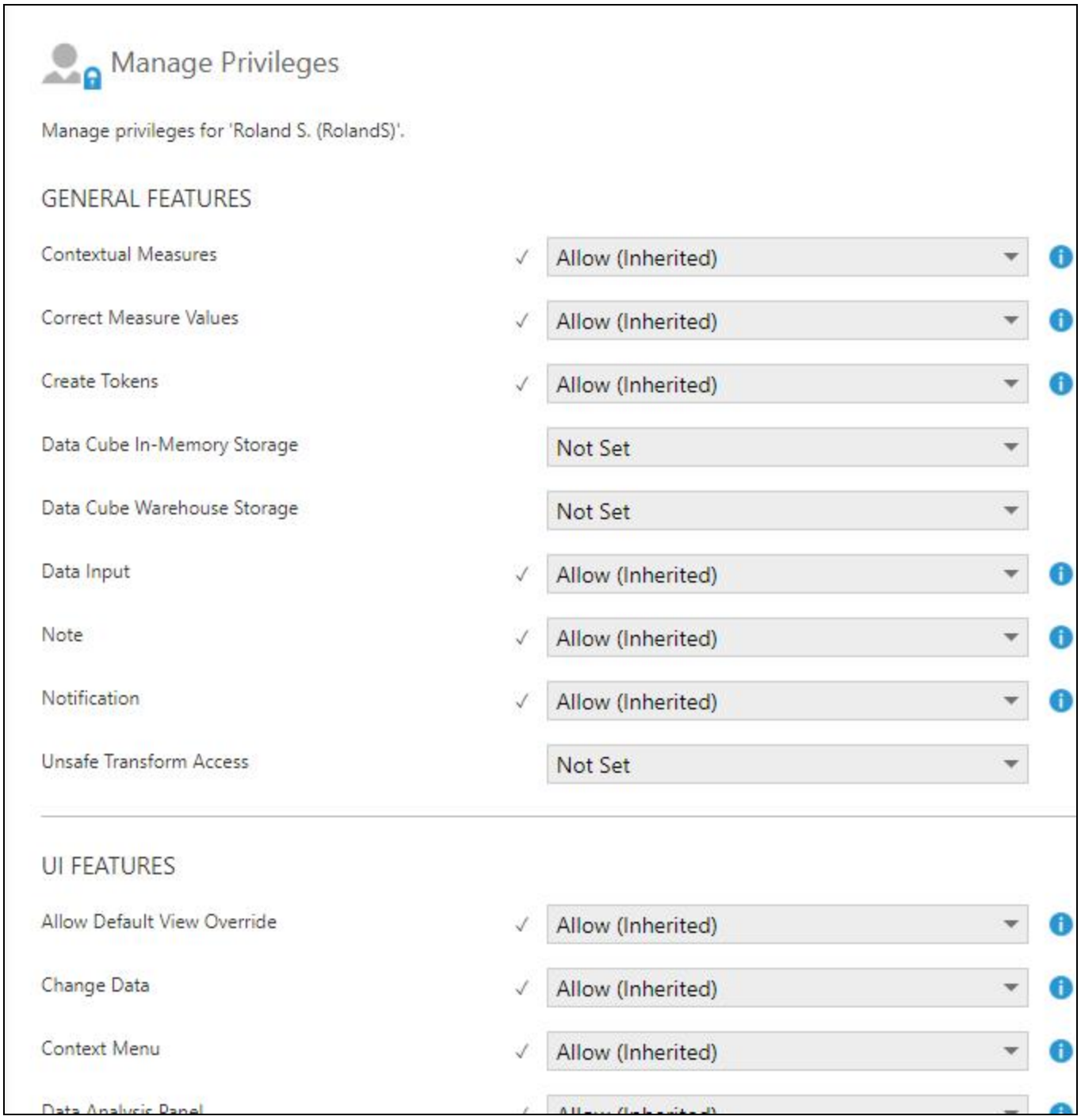
This applies to: *Managed Dashboards, Managed Reports*

Application privileges control whether a user has access to certain application functionality, such as using the toolbar or context menu while working with dashboards and other views, or entering public measure value corrections.

Symphony administrators can *allow* or *deny* application privileges when creating or editing a user or group by clicking the **admin** button. Denying a privilege means the user either is prevented from using certain functionality, or can no longer access user interface elements such as toolbars, menus, or toolbar & menu items.

Note: Many of these privileges can also be disabled for all non- administrator users on views such as dashboards or their visualizations.

A *deny* assignment set for an account or one of its groups always takes precedence and cannot be overridden by assigning *allow* without removing the *deny* assignment. The account or one of its groups must also have *allow* assigned for a privilege for it to be granted. Note that system administrators have all privileges and are not effectively denied any privilege.


Manage Privileges
Manage privileges for 'Roland S. (RolandS)'.
GENERAL FEATURES
Contextual Measures
Allow (Inherited)
Correct Measure Values
Allow (Inherited)
Create Tokens
Allow (Inherited)
Data Cube In-Memory Storage
Not Set
Data Cube Warehouse Storage
Not Set
Data Input
Allow (Inherited)
Note
Allow (Inherited)
Notification
Allow (Inherited)
Unsafe Transform Access
Not Set
UI FEATURES
Allow Default View Override
Allow (Inherited)
Change Data
Allow (Inherited)
Context Menu
Allow (Inherited)

When editing an existing account or group, many privileges are often *inherited* from a group that contains it, and a blue information icon appears on the right that you can click to find out where it is inherited from. You can also access a description of each privilege by clicking this icon, or by hovering the mouse over or long-tapping the name of the privilegeList of Privileges

List of Features - General Features

Privilege	Description
Contextual Measures	Allows the user to define contextual measures as well as enter data for these measures.
Correct Measure Values	Allows the user to enter public measure value corrections.
Create Tokens	Provides the ability to create account-specific parameter tokens.
Data Cube In-Memory Storage	Allows the user to configure a data cube for in-memory storage.
Data Cube Warehouse Storage	Allows the user to configure a data cube for warehouse storage.
Data Input	Allows the user to define warehouse tables and enter data for these structures.
Note	Allows the user to add notes to data.
Notification	Allows the user to create and manage notifications associated with their account.
Specify Notification Recipients	Allows the user to add or remove recipients when creating or editing a notification.
Unsafe Transform Access	Allow the user to create data cubes using manual SQL, MDX, or Python, which may be unsafe.

List of Features - UI Features

Privilege	Description
Allow Default View Override	Allows the user to override the default view indicated by administrators.
Change Data	Allows the user to see the context menu options that change the data that's displayed. These include Drill Down, Drill Up and Change Level. This option is for views (dashboards, reports, slideshows, etc.).
Context Menu	Allows the user to see the context menu (right-click or long-tap).
Data Analysis Panel	Provides access to the Data Analysis Panel.
Data Preview	Show the Data Preview dockable window for views such as dashboards and reports, which includes performance statistics.
Edit	Show the Edit option in the toolbar and context menus (including the Explore window).
Edit Copy for Analysis	Show the Edit Copy for Analysis option in the toolbar and context menus.
Full Screen	Show the options for entering & exiting Full Screen mode for views such as dashboards and reports.
Maximize	Show the options to Maximize or Restore Down a visualization to/from full screen in a dashboard.

Privilege	Description
Modify Data	Show the Modify Data options including period over period, states, and formulas for a selected data visualization when editing views such as dashboards and reports.
Natural Language Input	Allows the user to see the Assistant option in metric sets for typing natural language queries to display and analyze data, if the plug-in is installed.
Quick Access Properties Panel	Allows the user to see the Quick Access Properties panel when editing views (dashboards, reports) and metric sets.
Re-Visualize	Show the Re-Visualize option in the toolbar and context menu for a selected data visualization.
Set Up Interactions	Show the Set Up Interactions option in the toolbar and context menu for a selected data visualization.
Share	Show the Share option in the toolbar and context menu.
Sorting and Filtering	Show the Sort and Filter options on visualizations (does not affect metric set sorting and filtering options if the user can edit them).
Store User UI Customizations	Allows the application to automatically save the UI customizations for the user, such as the locations of dockable windows, or the toolbar settings on the Home page.
Store View Personalization	Allow the saving of personalized settings such as the state of filters while viewing dashboards and other views.
Toolbar	Show the toolbar for dashboards and other views. Does not apply to other toolbars such as for a full-screen metric set.

Example - Grant the Share Privilege To All Users

This example assigns privileges to the *Everyone* group so that they take effect for all users at once. The same concept applies when assigning privileges to other groups for the members of those groups.

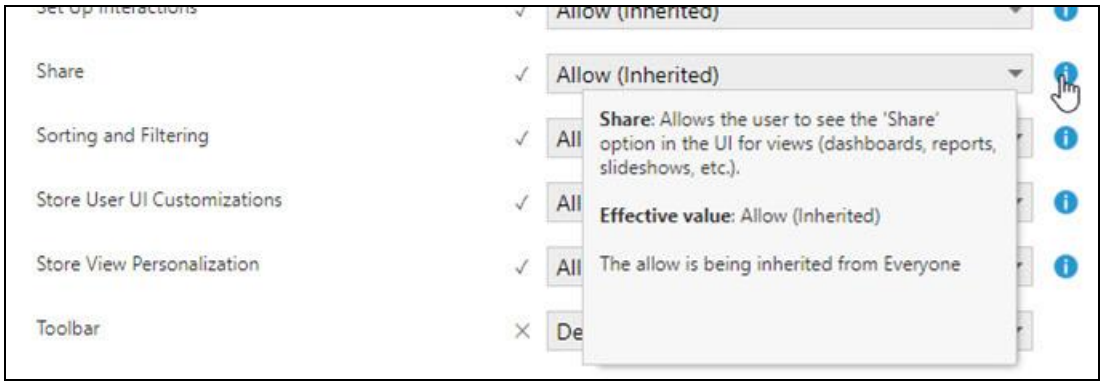
Note: The Everyone group implicitly contains all users of the system. Its membership cannot be changed, however you can still assign privileges and custom attributes to this group. All privileges allowed or denied on this group are inherited by all accounts or groups belonging to this group.

Go to the administration area, expand the **Account Service** category along the left, then select **Groups**.

Select the *Everyone* group for this example, and click **Edit** in the toolbar (or double-click the group as a shortcut).

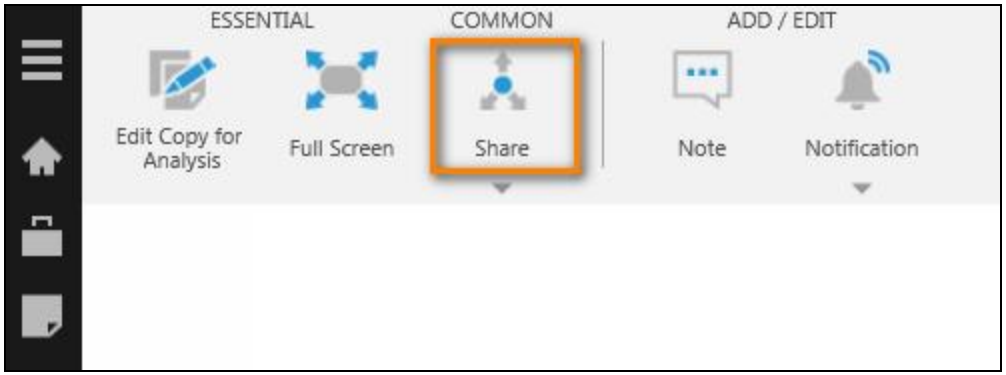
In the *Group Details* dialog, click **admin** and set the **Share** privilege drop-down to *Allow*.

After submitting the dialogs, click to go the **Accounts** page on the left, edit an account, and click **admin** to see that members of the group you just changed have the *Share* privilege allowed.

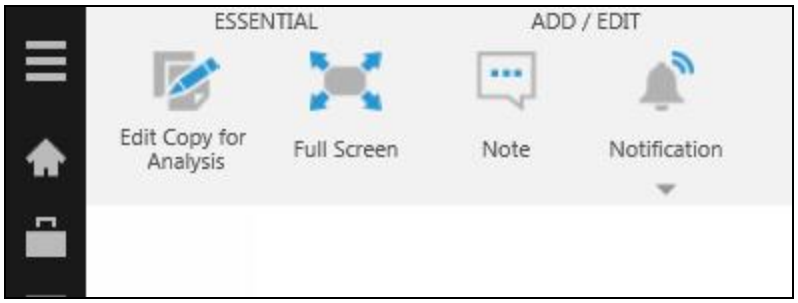


Click the information icon on the right for a description of where the privilege is inherited from and to confirm the effective privilege assignment.

The privilege in this example ensures the Share option appears in the toolbar when the affected users view a dashboard or other view:



If this privilege is denied, the option does not appear:



For more information, see:

- Configuration Best Practices
- Configuring Notifications and Other Scheduling Features
- How To Enable Anonymous Log On
- Set Up a Custom Logon URL
- Setting a Default Theme
- Turn Off Automatic Saving For Views
- Set a Configuration Value From the Command Line
- Override Config Settings Using an XML File
- Create Custom Application Configuration Settings
- Script Library: Application Configuration Service

Configuration Best Practices

This applies to: *Managed Dashboards, Managed Reports*

Symphony allows you to configure and secure the application using many options to meet your own needs. The following are recommended configuration best practices and settings.

Deployment

- When installing Symphony, configure the website to use HTTPS using an SSL certificate, or deploy to a virtual directory on an existing HTTPS website. Ensure the website's bindings remain configured to allow only HTTPS connections in your web server (IIS or Nginx).
- If the website is public-facing and accessible from the Internet, use a firewall with denial-of-service attack prevention features.

Best Practices

- Either set the **Maintainer Email Address** configuration setting or set the **Email Address** on the built-in *System Administrator* account to an address that will be monitored by someone who maintains Symphony in case of issues.
- Uncheck **Enabled** to disable the built-in *System Administrator* account so that the names of the enabled administrator accounts are not well-known.
- Edit the *Everyone* group to remove any application privileges not needed by all of your users. You can create new groups or configure individual accounts for granting application privileges instead.

Security Configuration

It is recommended to review the following security-related configuration settings and configure them as needed:

Setting	Review
Always Use Custom Home Page	For public-facing installations where users shouldn't see the built-in home screen
Allowed Admin IP Addresses	Always
Trusted Proxy IP Addresses	If a reverse proxy and/or load balancer is used
Log On Modes	Always
Registration Enabled	If using local accounts - consider disabling
Authentication.Excessive Logon Failure	If using local accounts

Setting	Review
Protection category	
Authentication.Password Policy category	If using local accounts
Allow External File-Based Data Sources	Always
Allowed Data Providers	If desired
Allowed Export Providers	If desired
Allowed Delivery Providers	Disable the *File* provider if untrusted users can set up notifications
Allow Custom Email Recipients	Always
Email Address Domain Whitelist	If *Allow Custom Email Recipients* is enabled
Maximum Resource Size	To prevent uploading very large files/resources in a denial-of-service attack attempt
Session Inactivity Timeout	Always
Lock Session To IP Address	Always
Setting	Review
Federated Authentication Debug Screen Allowed	If using federated authentication
SMTP Enable SSL	Always
Hide Error Stack Traces	Always - should be enabled for production environments
Signing Certificate	If using federated authentication with the SAML2 protocol
Allowed Embedding Origins	Set to *self*; or when embedding, to your domains that run or embed Symphony

Some settings such as password policies and allowed IP addresses can also be configured for users and groups.

Other Configuration Settings

Also consider reviewing the following configuration settings that are not security-related but can help ensure the smooth operation of the application:

- *Job Failure Email Policy* - consider enabling emails sent to the *Application Maintainer* (or *System Administrator*)
- *Creator Metadata Text / Company Metadata Text* - used to populate metadata fields in exported documents such as Excel
- *License Expiration Reminder Threshold*
- *Performance Statistics Maximum Age* - consider setting to 0 to improve server performance when performance tracking is not needed

Run the Symphony health check to identify other potential issues or suggestions.

For more information, see:

- Symphony Managed Dashboard and Managed Report Security
- Configuration Settings
- Configuring Notifications and Other Scheduling Features
- Health Check
- Create Custom Application Configuration Settings
- Advanced Group Management

Configuration Settings

This applies to: *Managed Dashboards, Managed Reports*

You can view and modify configuration settings in Symphony through the administration interface.

Note: For the full list of all configuration settings, view them within Symphony where you can filter and search through them.

Symphony allows you to secure the application using many configuration options to meet your own needs, such as:

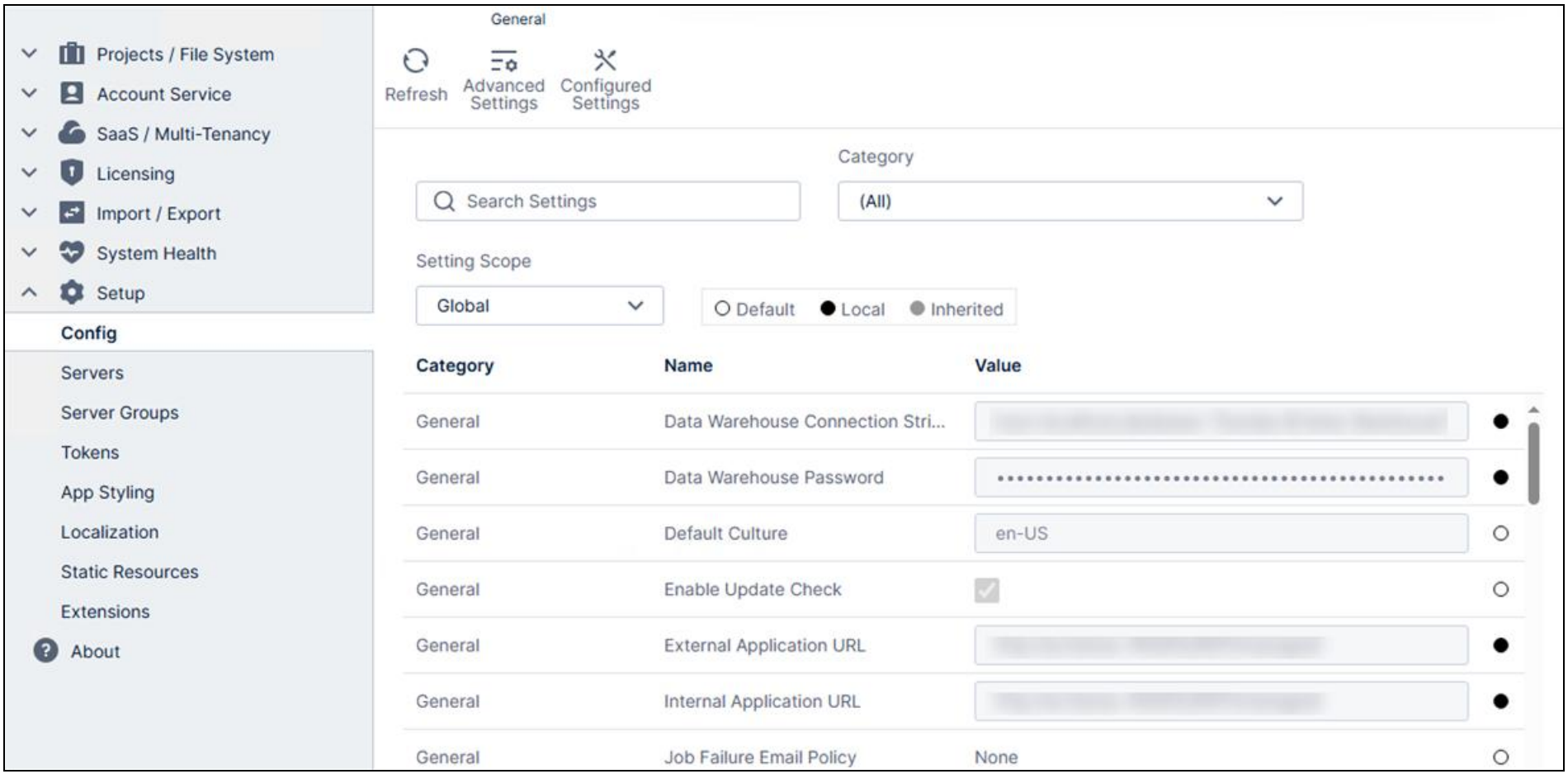
- **IP locks**: Administrators can limit access to admin accounts to a range of IP addresses, limit IP addresses/ranges for other accounts and groups, and lock each logon session to its specific IP address.
- **Excessive logon failure protection & password policies**: When accounts and credentials are managed within Symphony, use built-in safeguards against attacks.
- **Email whitelists**: Prevent users from sharing potentially sensitive content from the application by e-mailing outside of your organization or to non-SymphonyI users.
- **Limit data sources**: Administrators can limit the data providers that other users can connect to on their own, for example allowing only Excel and flat files and adding trusted connections to databases or prepared data cube models for them to use.

Our configuration best practices guide provides a full list of recommended security configuration settings.

View or Modify Configuration Settings

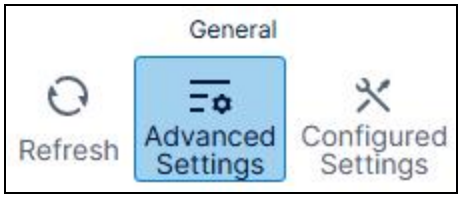
To view or modify configuration settings in Symphony, go to the Administration area.

Expand the **Setup** section along the left and click **Config**. The configuration settings are displayed in a table.



Advanced Settings

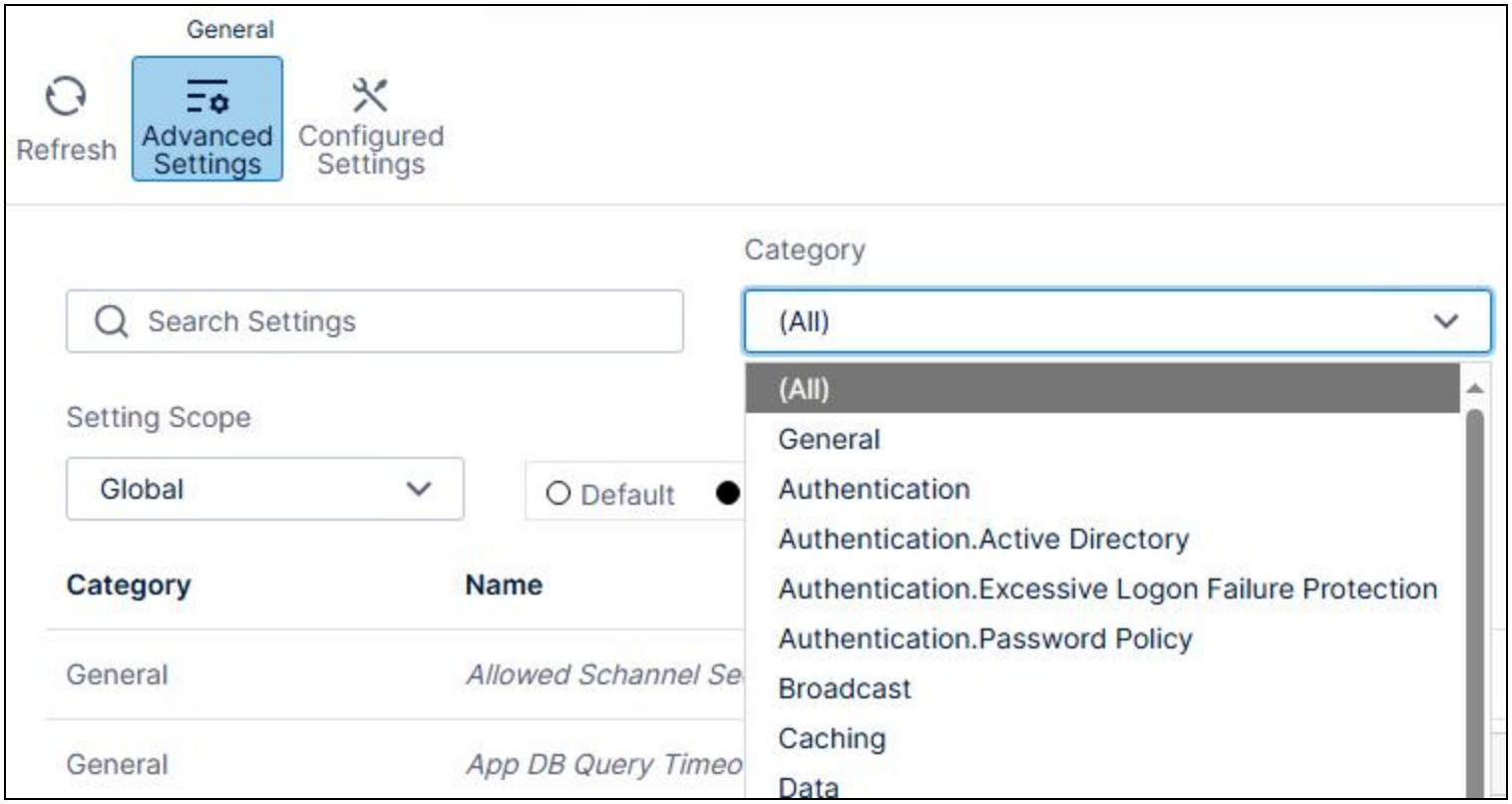
By default, advanced settings (such as *App DB Query Timeout*) are hidden. To see the complete list of settings, click the **Advanced Settings** icon on the toolbar. Advanced settings are displayed in italics.



Filter by Category or Search for Settings

Use the **Search** box or the **Category** drop-down to easily find the setting(s) you need.

For example, if you want to see only email-related settings, set the **Category** drop-down to *Email*. The table of settings will be filtered accordingly.



To filter the list to include only settings that have been previously set or changed, click **Configured Settings** in the toolbar next to the advanced option.

Setting Scope

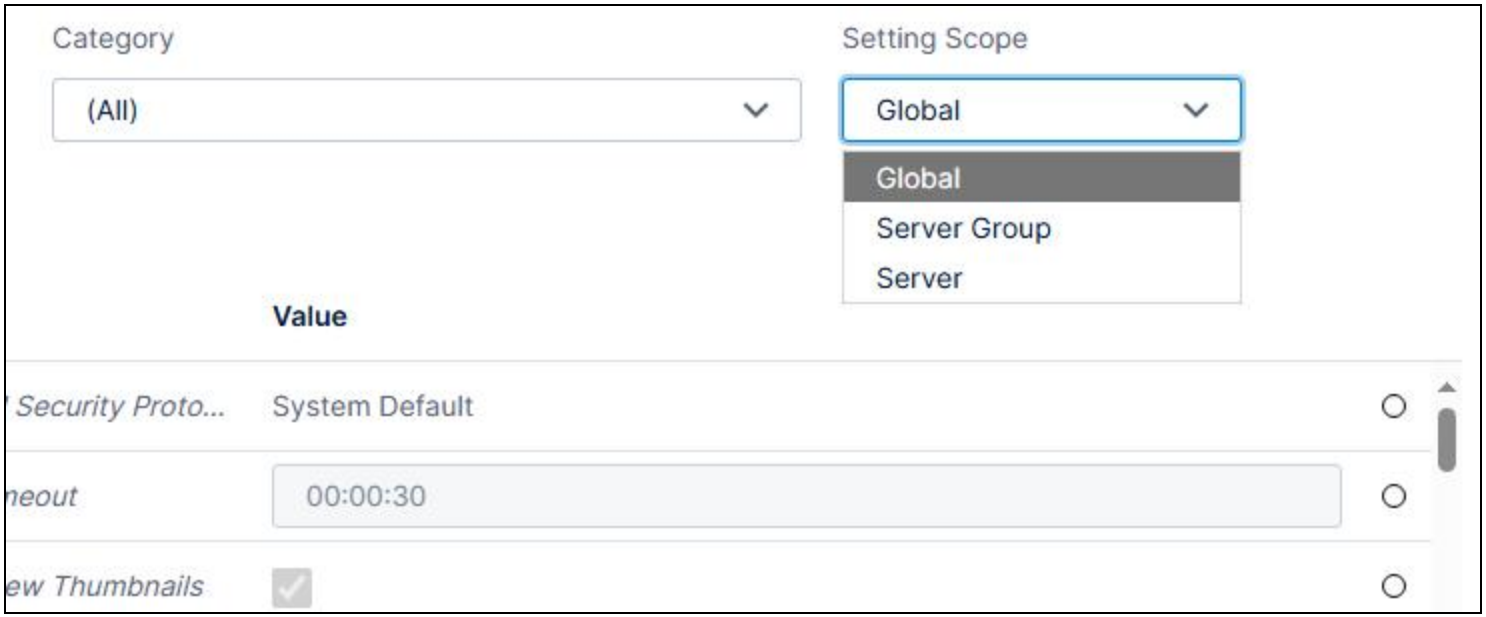
For scalability, Symphony supports using multiple servers (i.e., a server farm) for handling application and data processing.

When your installed Symphony instance has server groups set up, you can override each configuration setting on different levels such as globally, across a server group, or per-server. The override system works as follows:

- A configuration setting may have a built-in default value.
- A *Global* value for a configuration setting will override the corresponding default value.
- A *Server group* value for a configuration setting will override the corresponding global value.
- A *Server* value for a configuration setting will override the corresponding server group value.

Use the **Setting Scope** drop-down if applicable to view or modify the configuration setting values at the Global, Server Group, or Server levels.

If you don't provide a setting value at a certain level, it will just inherit the setting value from the next priority level. For example, if you're at the *Global* scope and you don't specify the value for the *Default Culture* setting, it will inherit the default value of *en-US*.

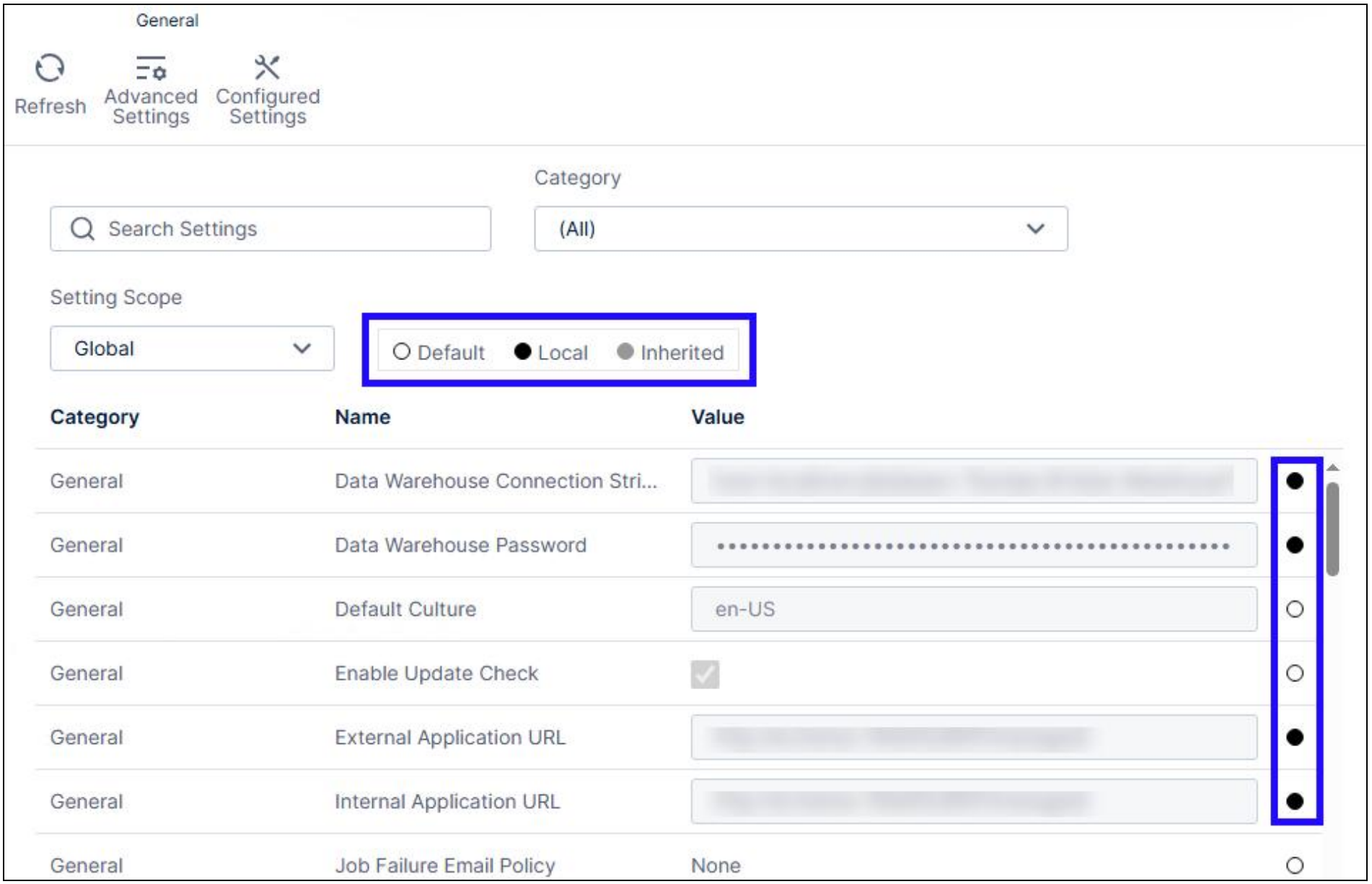


Note: When you don't have multiple servers, you can just use the *Global* setting scope.

Source For a Configuration Setting

Beside each configuration setting is a symbol that helps you quickly identify which settings have been customized:

- Default (empty) - The setting value is the default, built-in value.
- Local (filled) - The setting value is set directly in the current setting scope.
- Inherited (shaded) - The setting value is inherited from another scope (where applicable).

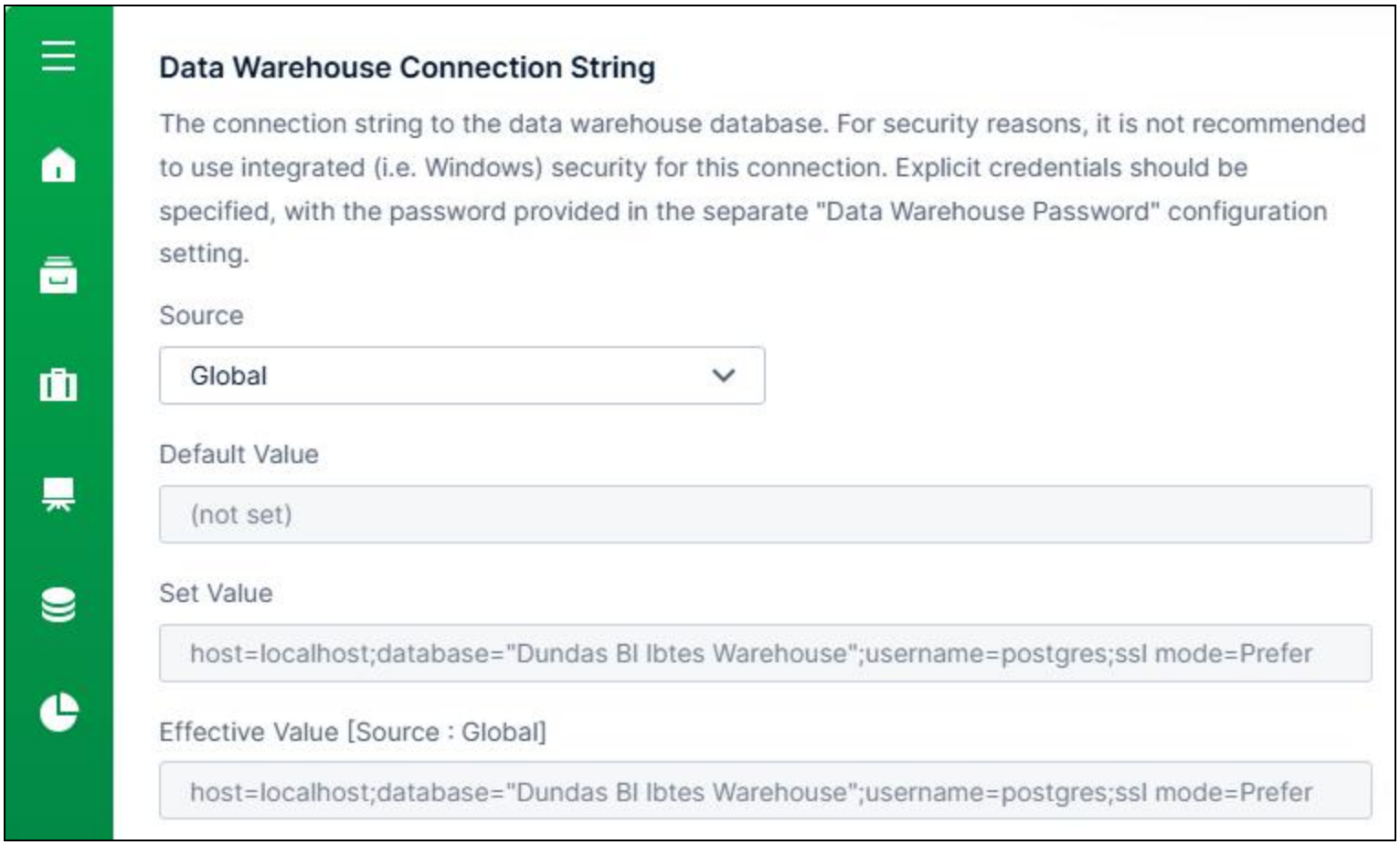

General
Refresh
Advanced Settings
Configured Settings
Category
Search Settings
(All)
Setting Scope
Global
Default
Local
Inherited
Category
Name
Value
General
Data Warehouse Connection Stri...
General
Data Warehouse Password
General
Default Culture
en-US
General
Enable Update Check
General
External Application URL
General
Internal Application URL
General
Job Failure Email Policy
None

View the Details For a Configuration Setting

Select a configuration setting and then click the **Details** icon on the toolbar.

The following details are displayed for that setting:

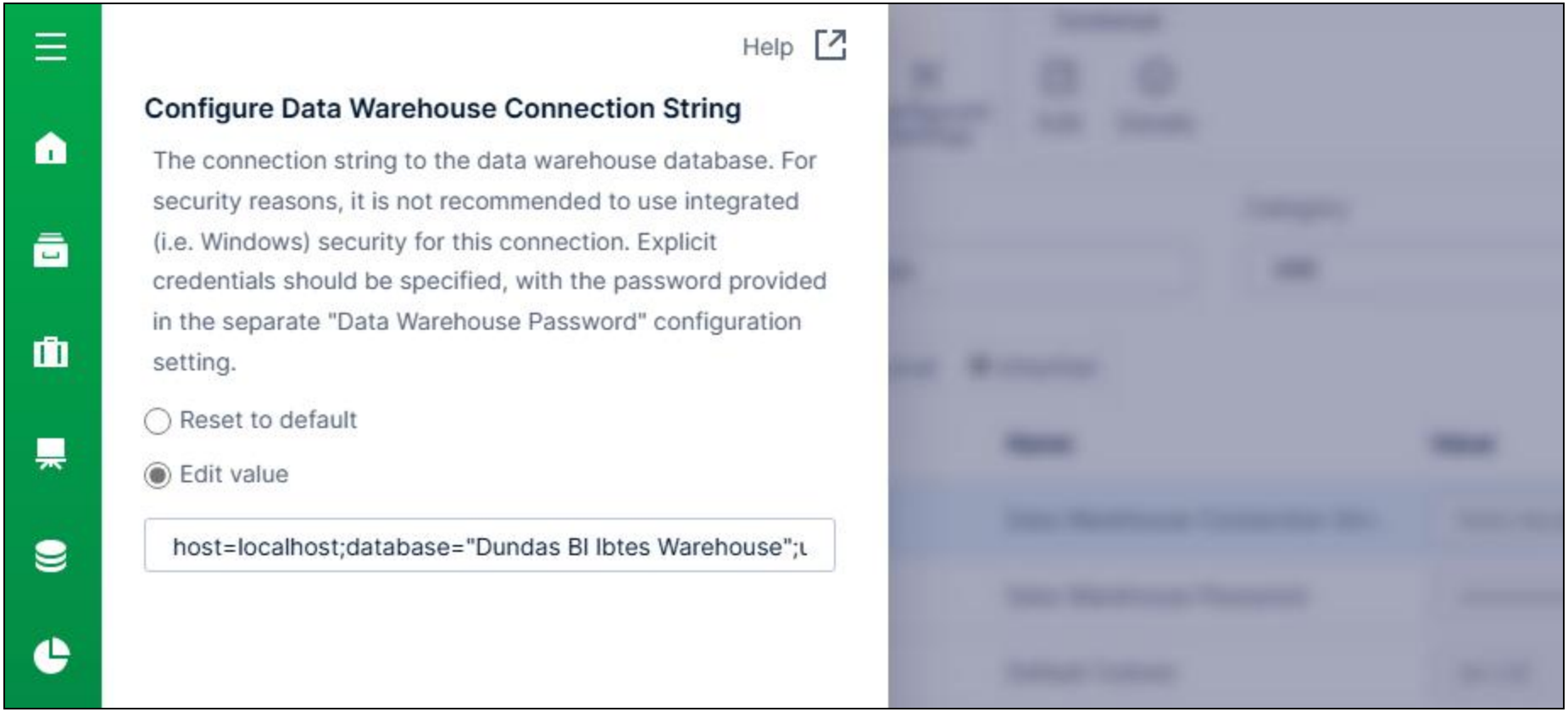
- A description of the setting.
- The default value of the setting (if any).
- Whether the setting is set in the current scope or not, and its value if it is set.
- The effective value of the setting and its source.



Modify a Configuration Setting

To edit/modify a configuration setting, make sure you are in the proper setting scope if applicable, select the setting and then click the **Edit** icon on the toolbar.

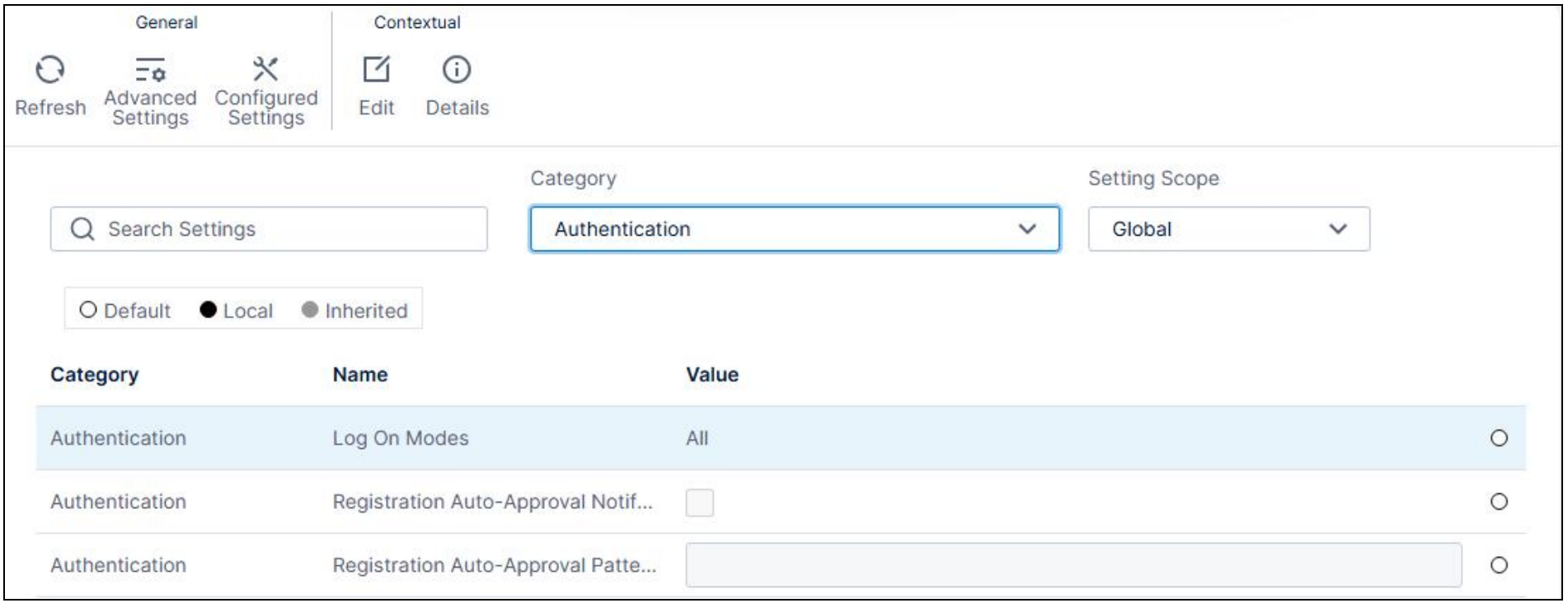
A dialog appears on the left, allowing you to set a value or reset it back to default. The actual options in the dialog will be different depending on the configuration setting.



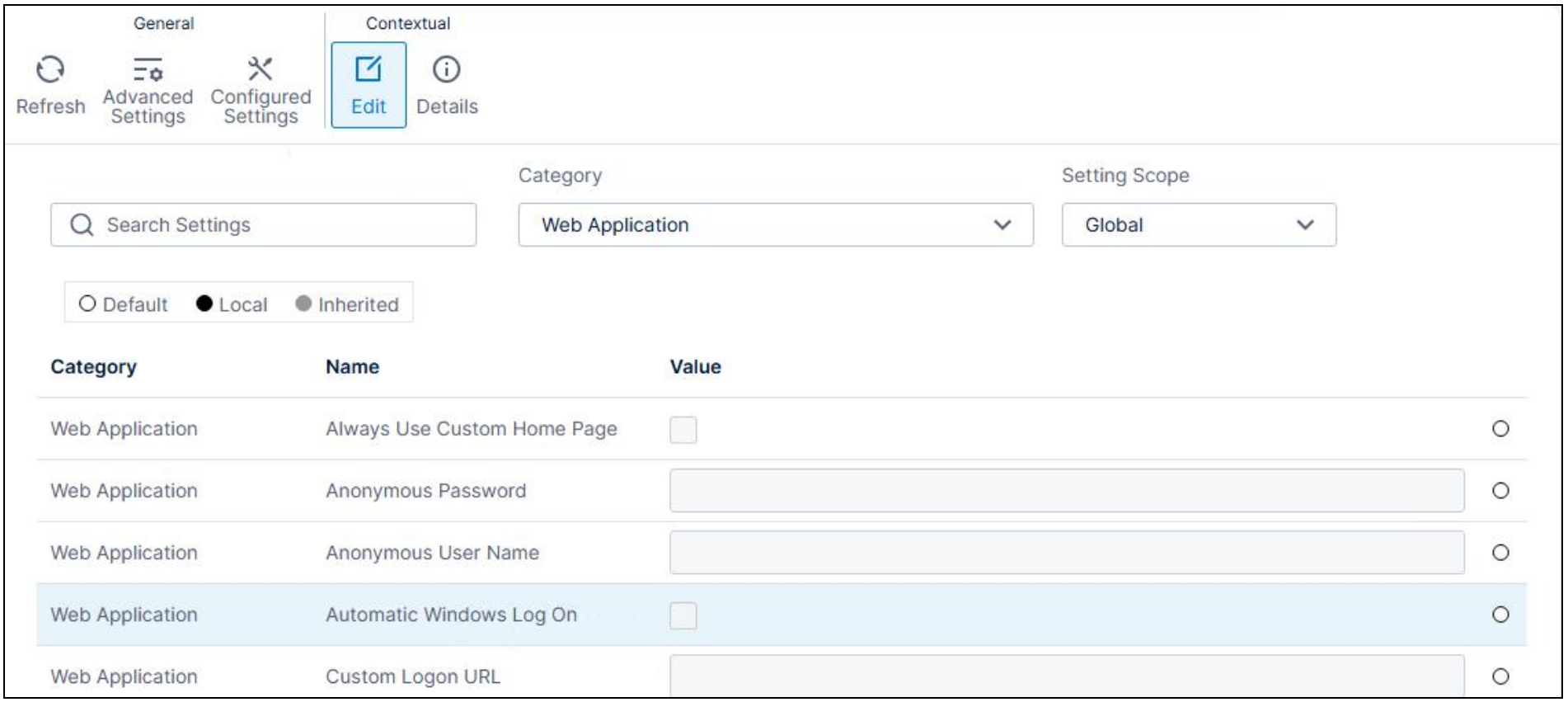
Example Settings - Automatic Windows Log On

Automatic Windows Log On is one available method of Single Sign On (SSO) when logging on with Windows credentials. By default, this setting is turned off in the Symphony configuration settings.

Before enabling this option, first ensure that the *Log On Modes* configuration setting is set to *All* or *Windows*.



Then enable the *Automatic Windows Log On* configuration setting.



Note that Windows authentication must be enabled in IIS as well. For more details, see this Microsoft article: Configure Windows Authentication (IIS 7).

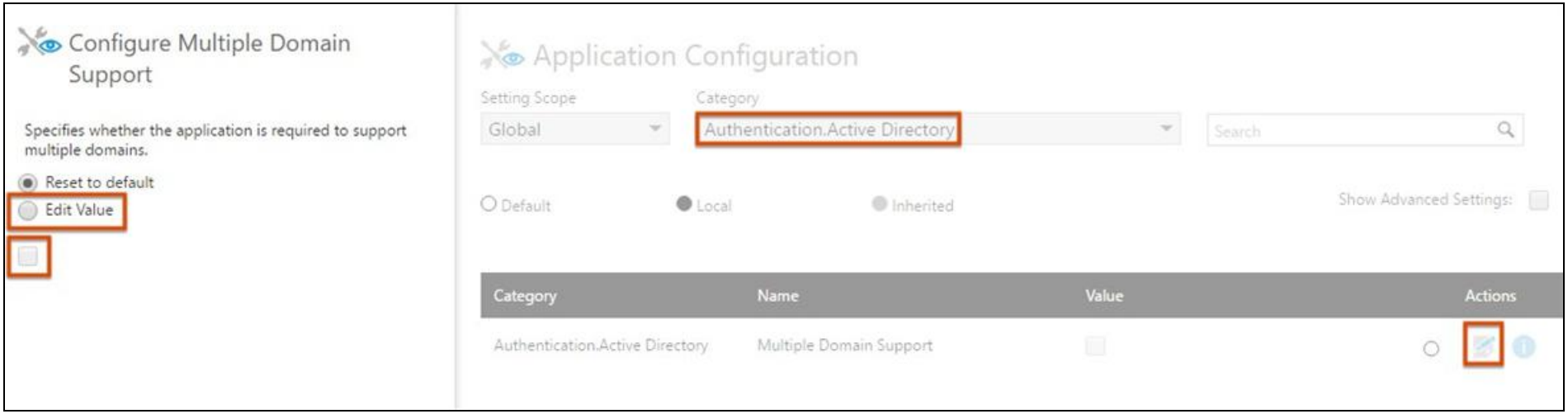
Once enabled, automatic logon will occur for all URLs that do not require explicit authentication. For example, navigating to *http://yourinstance/* will take you directly to the home screen, whereas *http://yourinstance/LogOn/* will still show the Log On screen.

Example Settings - Multiple Domain Support

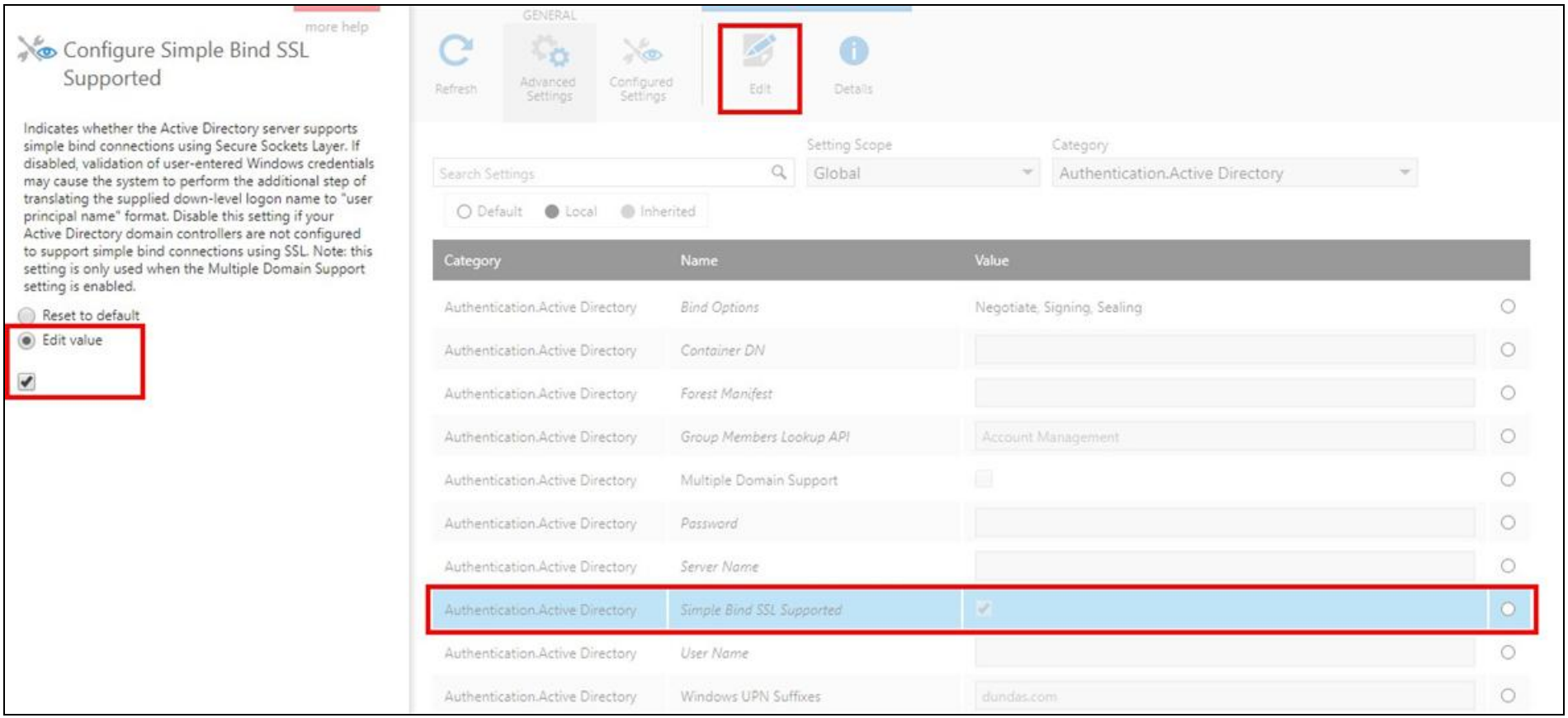
This setting enables Symphony to work with multiple Active Directory domains. Activating the *Multiple Domain Support* setting lets you set up cross domain authentication by adding Windows accounts and Windows groups from another domain.

Note: Built-in Local Groups are not available for Windows Group accounts, regardless of the domain being used.

Under **Category**, select *Authentication.Active Directory*, select the *Multiple Domain Support* setting and then click **Edit** on the toolbar. On the edit settings dialog click **Edit Value** and select the checkbox.



If your Active Directory domain controllers are not configured to support simple bind connections using Secure Sockets Layer (SSL), you have to disable the *Simple Bind SSL Supported* setting. This setting is an advanced setting.



Example Settings - Default Home Page (Relative Path)

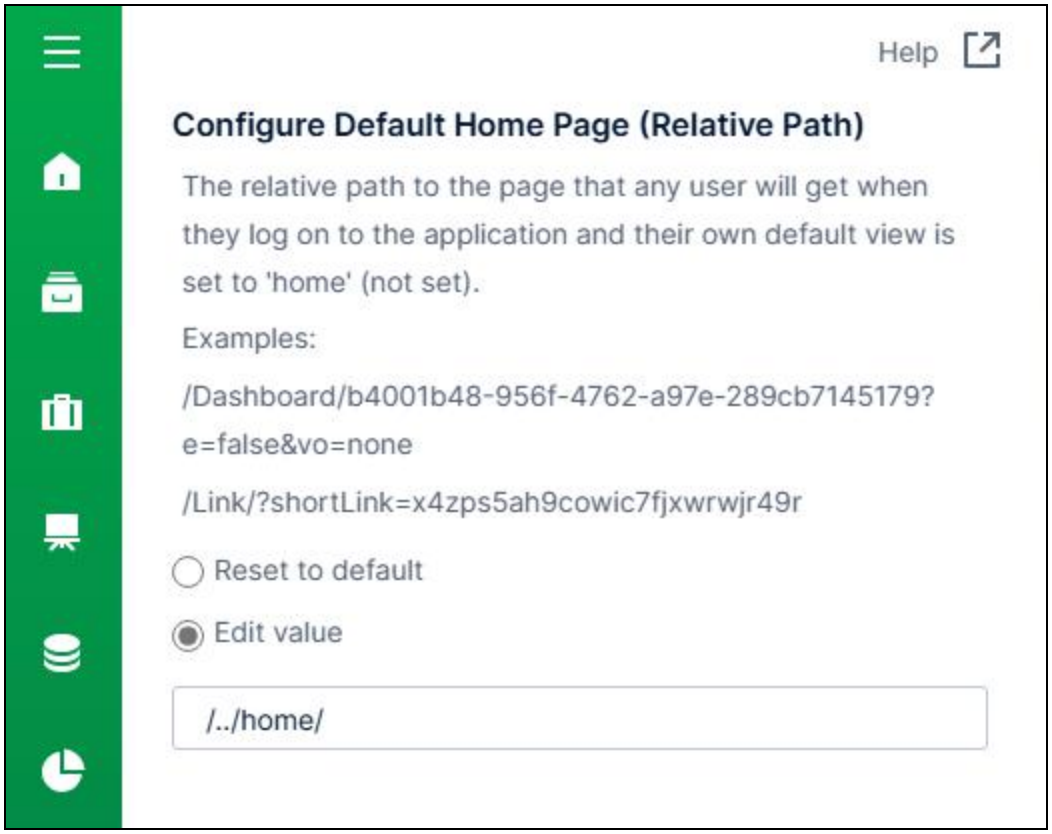
This configuration setting lets you set the page that appears when a user logs on to Symphony. It applies to all users application-wide as long as their Default View is set to Home (i.e., the user has not set a specific default view).

The setting value must be a relative URL like the one you get when you open a dashboard:

```
/Dashboard/abd7c93f-c9a6-4ecd-b7cf-7206d1977eae?e=false&vo=none
```

Or, it can be a relative URL like the one you get when you use the share link option:

```
/Link/?shortLink=yt1sca4pw9ir7ryke9ymew54th
```

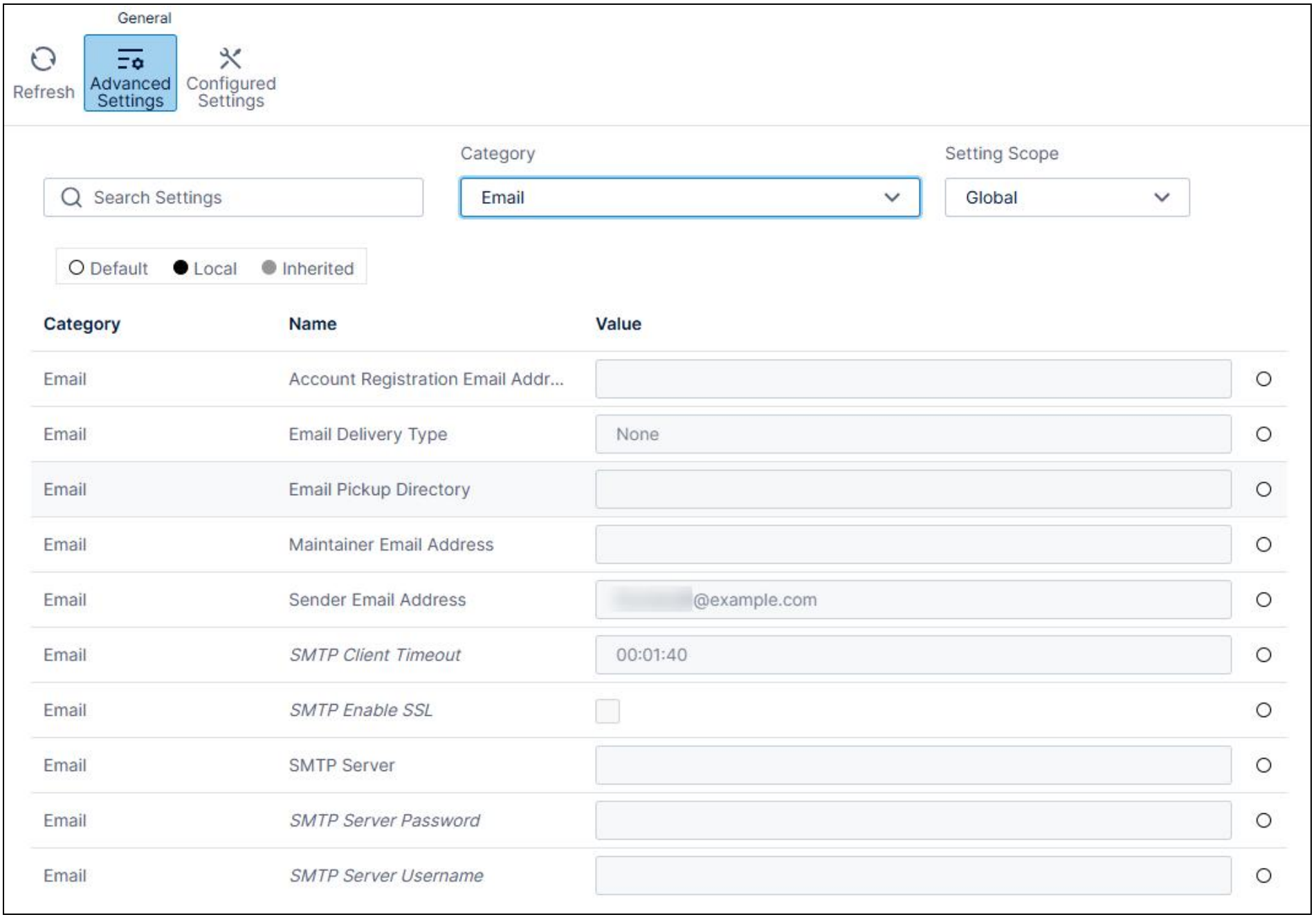


You can also configure the related setting *Always Use Custom Home Page* to also direct users to the customized home page when they navigate back there after logging in.

Example Settings - Email Settings

For installed versions of Symphony, email settings must be configured for certain features to work, including notifications and password reset from the logon screen. You may have configured these already when deploying.

Set the **Category** drop-down to Email to filter to the available email settings. Note that the **Advanced Settings** toggle is necessary to see some settings.

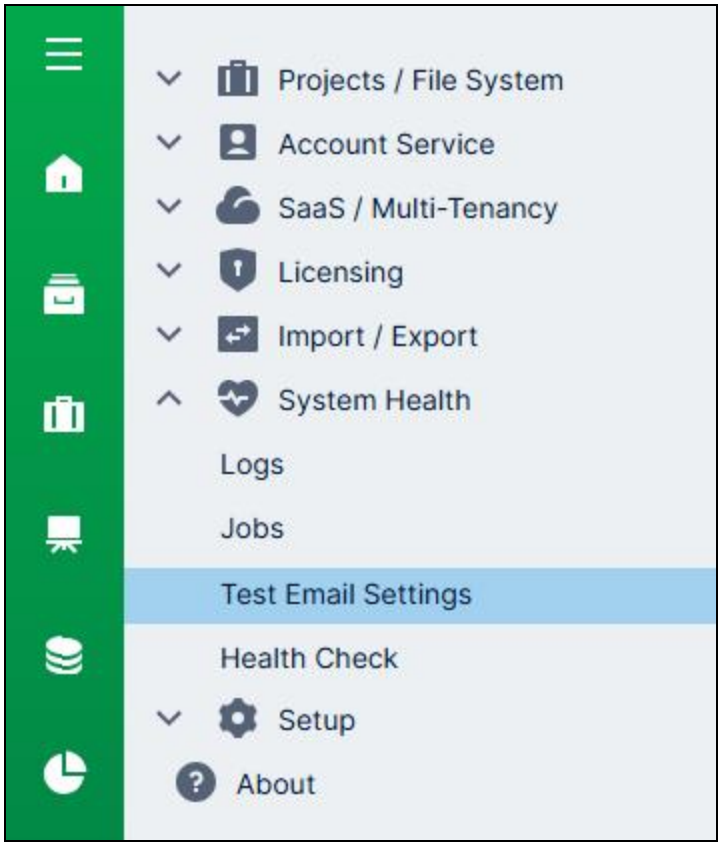

General
Refresh
Advanced Settings
Configured Settings
Search Settings
Category
Email
Setting Scope
Global
Default
Local
Inherited
Category
Name
Value
Email
Account Registration Email Addr...
Email
Email Delivery Type
None
Email
Email Pickup Directory
Email
Maintainer Email Address
Email
Sender Email Address
@example.com
Email
SMTP Client Timeout
00:01:40
Email
SMTP Enable SSL
Email
SMTP Server
Email
SMTP Server Password
Email
SMTP Server Username

The following table describes the various settings needed to enable sending emails. Symphony supports sending email via an SMTP server, or you can have the email messages delivered as files to a network share folder.

Setting	Description	Values / Example
Account Registration Email Address	The email address to which the account registration notifications are sent. If not specified, the system maintainer email address is used.	registration@example.com
Email Delivery Type	The email delivery type to be used by the application: ■ SMTP: Use this in conjunction with the SMTP settings to send actual emails. ■ Drop Folder: Store email messages as files in a pickup directory. These will be *.eml files which you can sort by date. ■ Test: Simulates a working email service, but doesn't actually attempt to send anything. This option lets you test features such as scheduled notifications that require email, without having to worry that emails are being sent. ■ None: If you try to use features requiring email (such as account registration), it will result in an error.	■ None (default) ■ SMTP ■ Drop Folder ■ Test
Email Pickup Directory	Email pickup directory location (applies when the email delivery type is Drop Folder). For example, set this to a network share folder.	\\server1\share
Maintainer Email Address	The maintainer email address for Symphony. Used to send system notifications. If not specified, the default admin account email address is used.	maintainer@example.com
Sender Email Address	The sender of the email messages sent by the email service.	sender@example.com
SMTP Client Timeout	The amount of time after which an SMTP operation fails. Formats include dd.hh:mm:ss or hh:mm:ss.	00:01:40
SMTP Enable SSL	If enabled, SSL will be used when connecting to the SMTP server.	true/false (default)
SMTP Server	The SMTP server (applies when the email delivery type is SMTP). An optional port may be specified here as well (e.g. "smtp.example.com:25").	smtp.example.com
SMTP Server Password	The password for SMTP server authentication.	Leave empty if authentication is not required.
SMTP Server Username	The username for SMTP server authentication.	Leave empty if authentication is not required.

There are a couple of ways to test the email settings after you've set them.

The first way is to expand the **System Health** administration section and click **Test Email Settings**. You'll be asked to enter an email address to receive a test email.

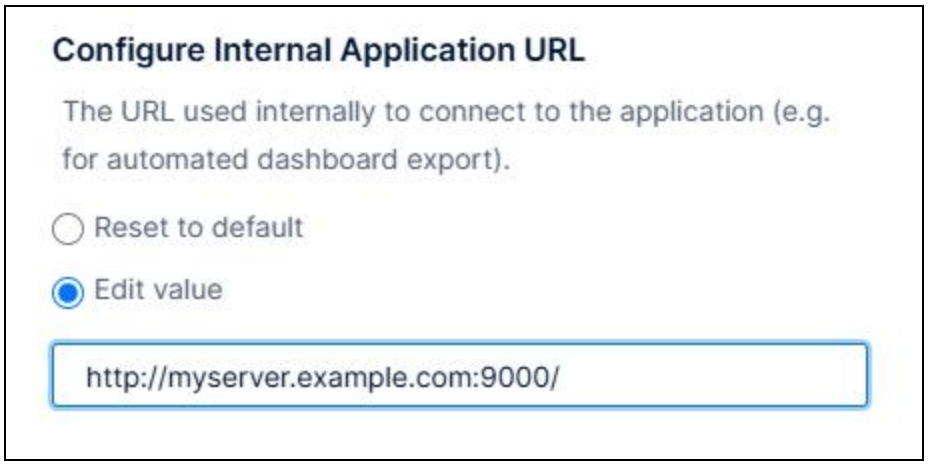


A second way to test is to create a note-based notification and then add a note to a data point in a visualization. Next, check your inbox or drop folder for the notification message. If you don't see the message, view the application logs for any email-related errors (e.g., search for "Email"). If you get errors when using the Drop Folder delivery type, it may be due to permissions on the network share folder.

It is also recommended to set the *Maintainer Email Address* setting in case of issues such as license expiry or job failure. (If unset, the built-in *System Administrator* account's email address will be sent these messages.)

Example Settings - Internal Application URL

The *Internal Application URL* setting (if applicable) must be configured properly for scheduling-related features such as scheduled notifications to work properly. This URL is used by the Symphony Scheduler Service.

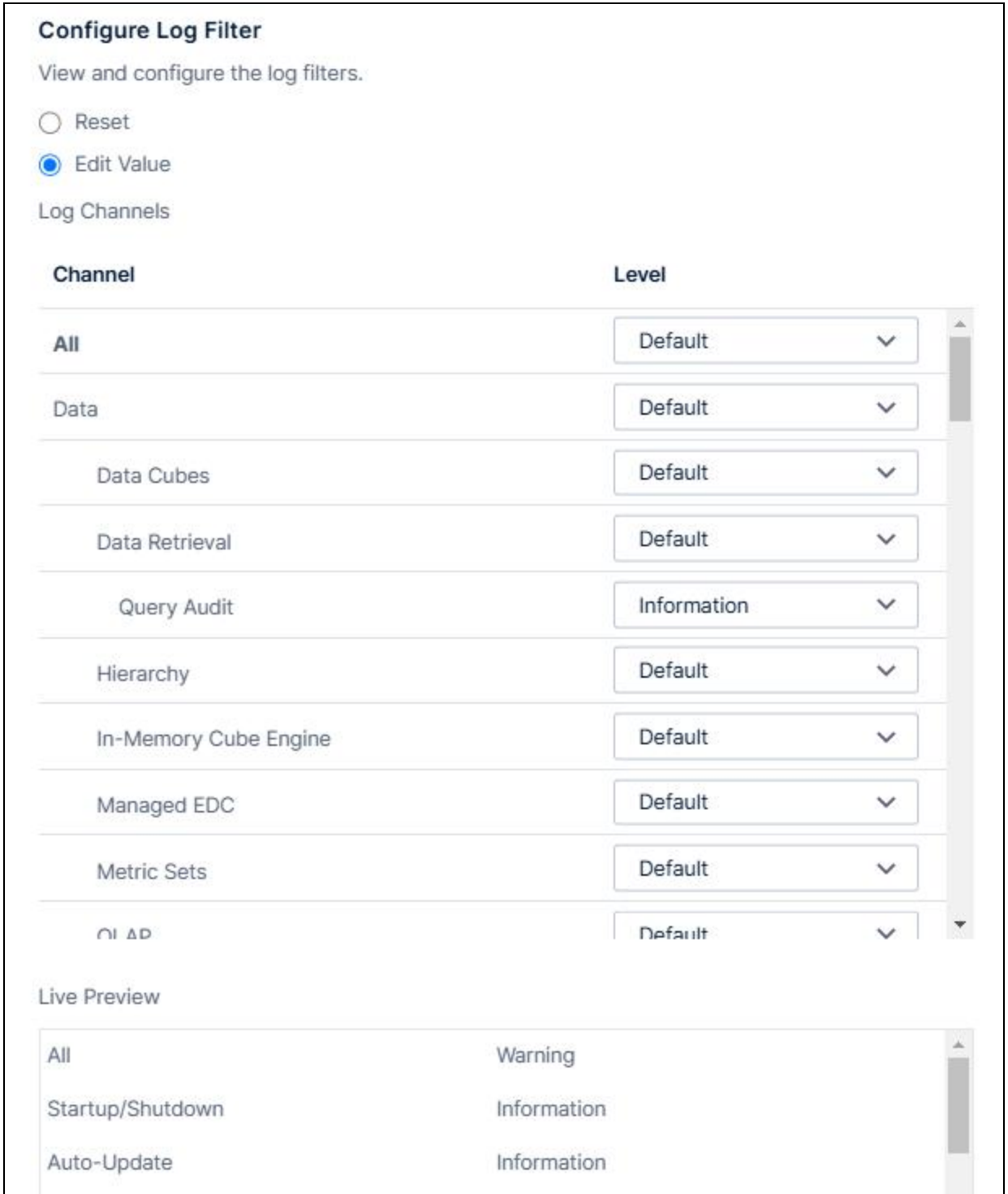


Example Settings - Log Filter

The *Log Filter* configuration setting lets you control the filtering of messages in the application logs. For each log channel (application area), you can independently set the level of logging you want (such as log only Critical messages or do Verbose logging). Use the scrollbar to see all of the available log channels.

If you change the level for a channel, you'll see it listed in the *Live Preview* section.

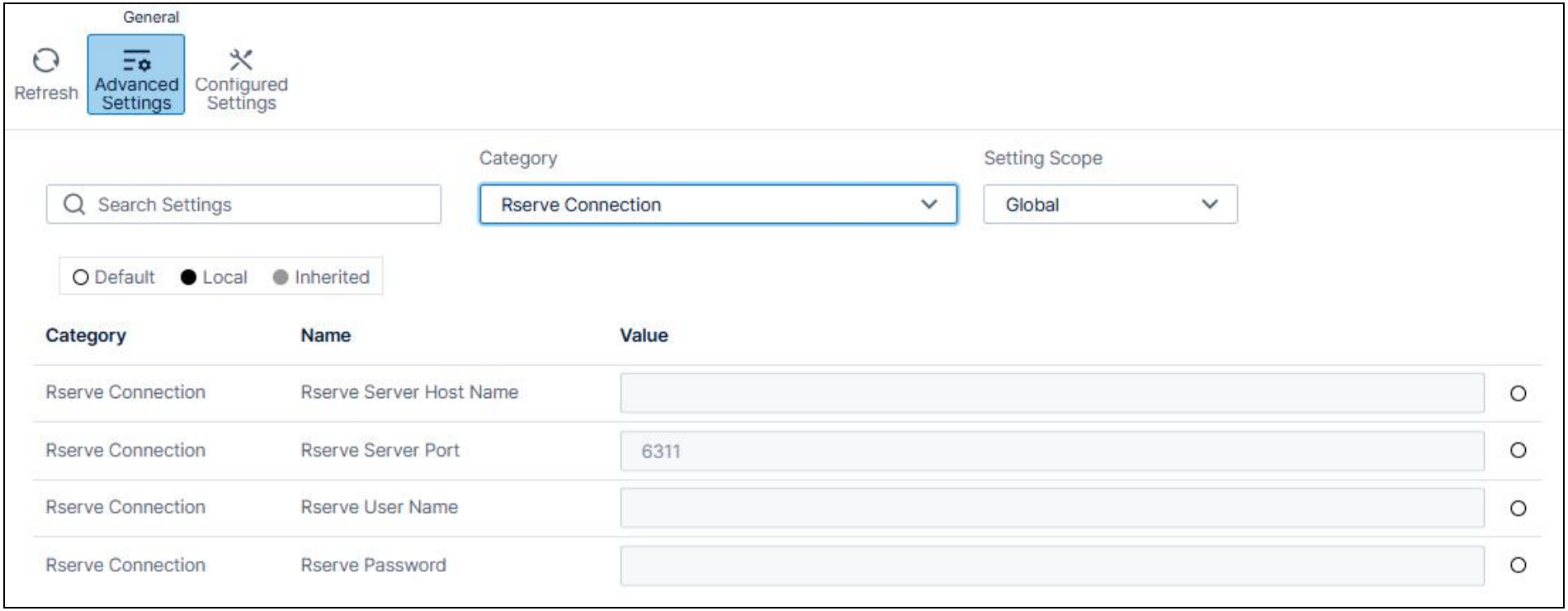
For example, if you set *Query Audit* to an Information level, every query sent to the database for data retrieval will be included in the log.


Configure Log Filter
View and configure the log filters.
Reset
Edit Value
Log Channels
Channel
Level
All
Default
Data
Default
Data Cubes
Default
Data Retrieval
Default
Query Audit
Information
Hierarchy
Default
In-Memory Cube Engine
Default
Managed EDC
Default
Metric Sets
Default
Default
Live Preview
All
Warning
Startup/Shutdown
Information
Auto-Update
Information

Example Settings - Rserve Connection

The *Rserve Connection* settings let you specify the details for connecting to an external R server. This is required in order to use the R language transforms such as R Data Generator.

If you have installed Rserve for Windows on your Symphony server for testing purposes, then the default Rserve Connection settings should suffice.



Additional Export Command Line Arguments

The exporting application in Symphony relies on the Chrome Embedded Framework (CEF), which sometimes requires additional arguments. The *Additional Export Command Line Arguments* setting lets you specify any extra command line arguments required for the exporting application.

The following table describes the various CEF arguments supported in Symphony.

Argument	Description
--proxy=address:port	Specifies the proxy server to use (e.g. --proxy=192.168.1.42:8080).
--proxy-type= [http|socks5|none]	Specifies the type of the proxy server. The default server type is set to http.
--proxy-auth	Specifies the authentication information for the proxy server (e.g. --proxy-auth=username:password).

For more information, see:

- Configuration Best Practices
- Configuring Notifications and Other Scheduling Features
- How To Enable Anonymous Log On
- Set Up a Custom Logon URL
- Setting a Default Theme
- Turn Off Automatic Saving For Views

- Set a Configuration Value From the Command Line
- Override Config Settings Using an XML File
- Create Custom Application Configuration Settings
- Script Library: Application Configuration Service

Configuring Notifications and Other Scheduling Features

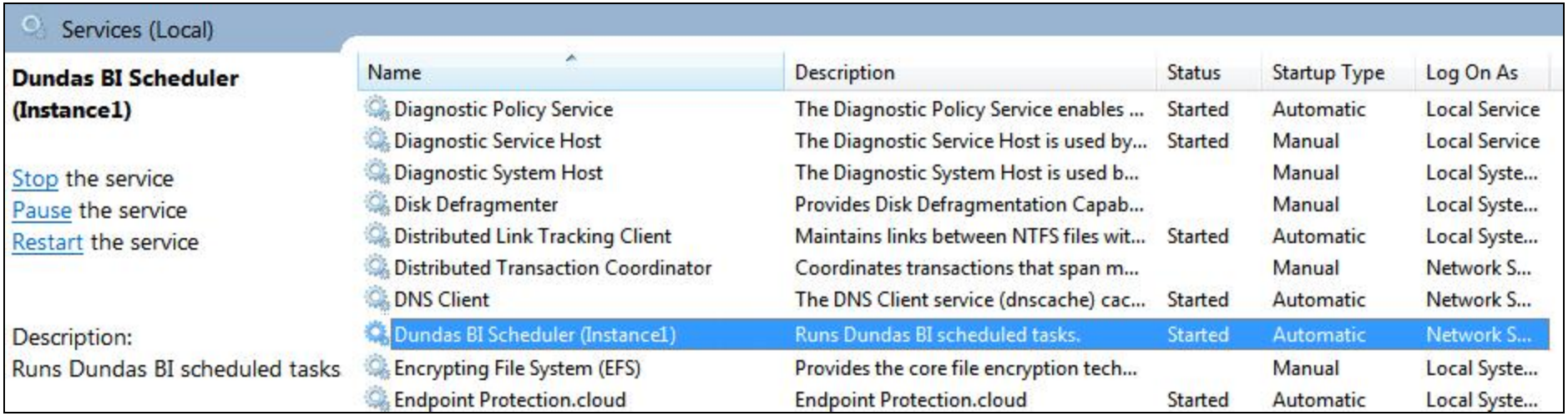
This applies to: *Managed Dashboards, Managed Reports*

The Symphony Scheduler service needs to be running and various configuration settings must be applied for notifications and other scheduling-related features in Symphony to work.

Symphony Scheduler Service

For any scheduled task in Symphony to work (e.g., notifications, scheduled data cube storage), the Symphony Scheduler service needs to be running on the server where Symphony was installed. There is a health check you can run from Symphony's administration area named *DBI0040 : Scheduler Service Status* that can confirm whether this is running and can connect.

The Symphony Scheduler service is typically installed along with the application. To verify that the service is running on Windows, open **Services** from the Start menu under *Windows Administrative* Tools, or go to this tab in the Windows Task Manager.



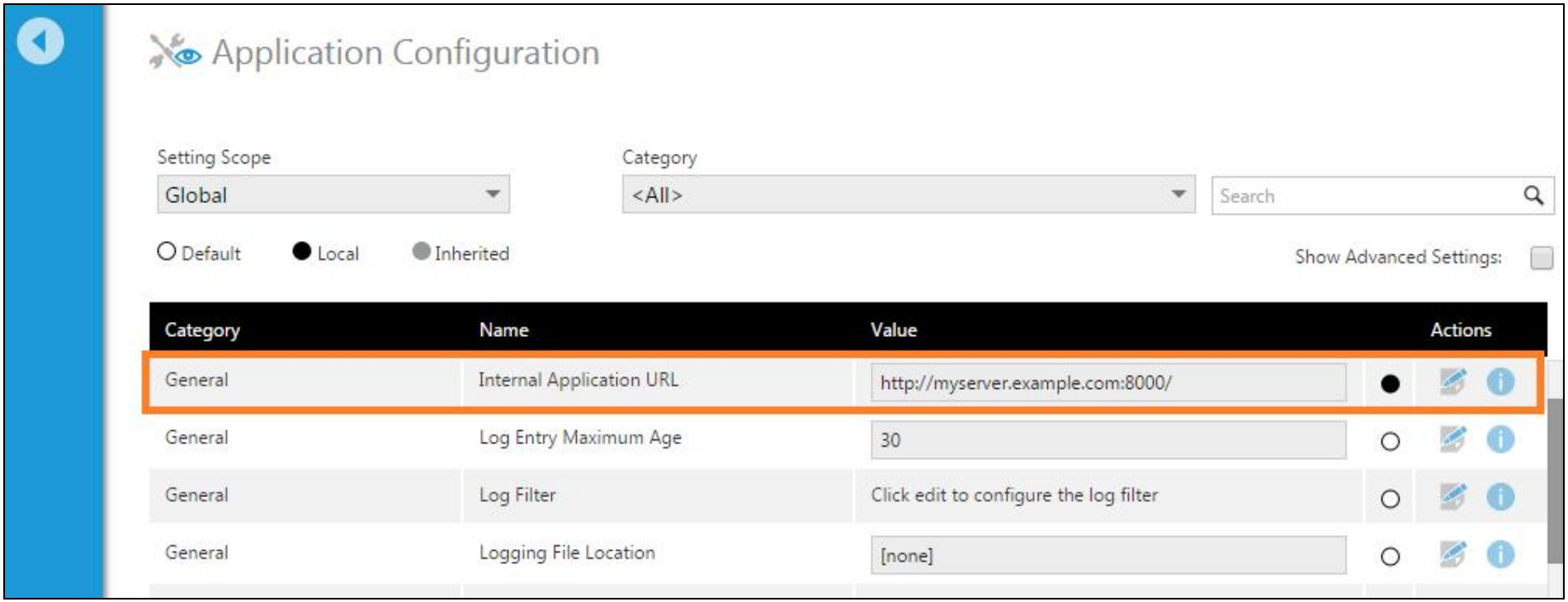
If you have changed the permissions for the database login used to connect to Symphony's application and warehouse databases since installation, ensure this login still has access to read and write to these databases.

Symphony Configuration Settings

The following configuration settings should be set correctly. To access them, go to Administration in the main menu, expand **Setup**, and click **Config**.

Internal Application URL

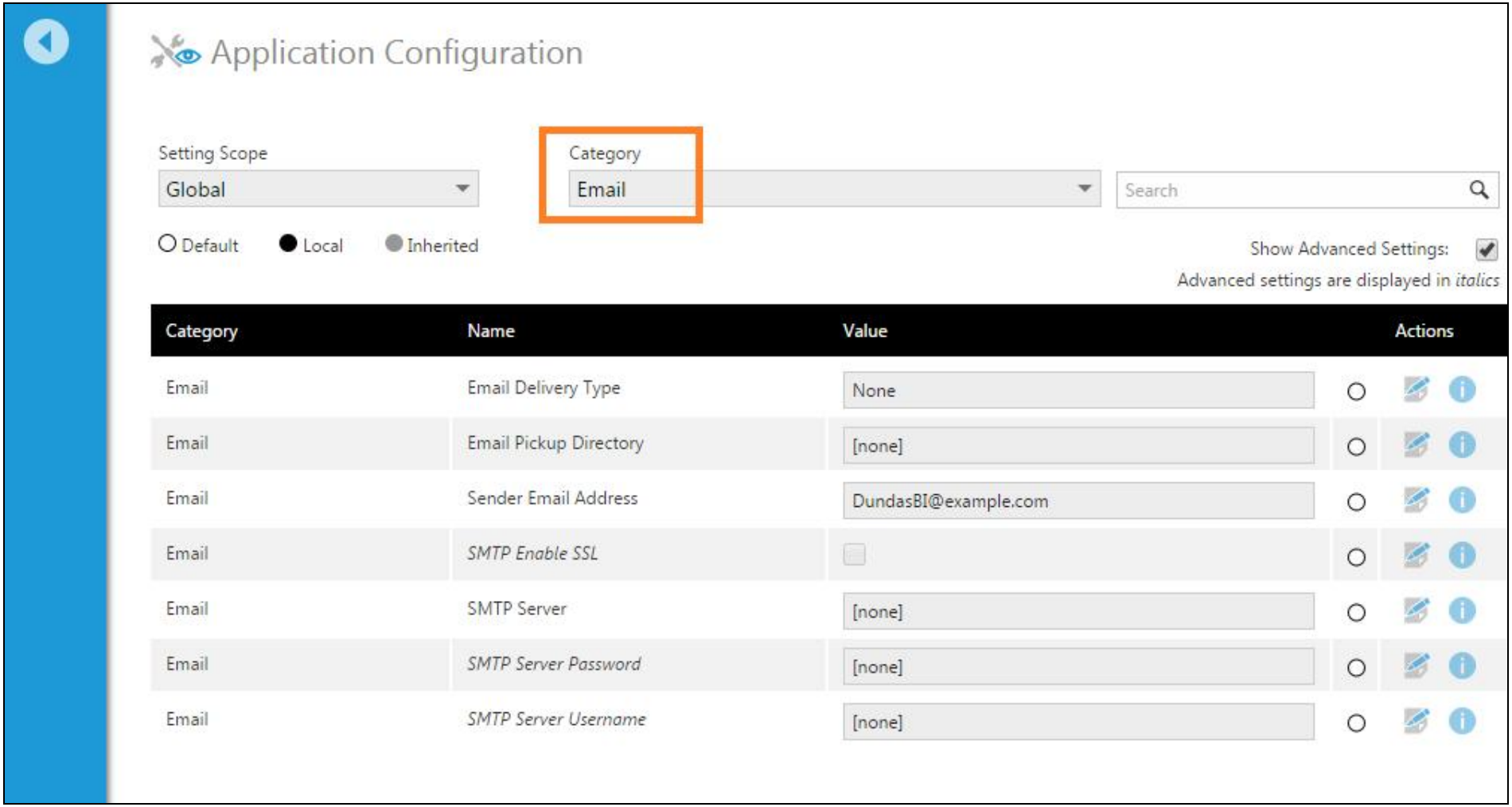
The *Internal Application URL* setting should be correct for scheduling-related features such as scheduled notifications to work properly. This URL is used by the Symphony Scheduler service.



There is a dedicated health check named *DBI0045: Internal Application URL Status* that can confirm this setting is correct.

Email Settings

Email settings must be configured for certain features to work, including notifications and password reset from the Log on screen.



These are described in detail in the configuration settings article. You can test email settings from the System Health section.

Notification Content Security

You may also want to consider how your users should be able to share content through notifications:

- If the *Allow Custom Email Recipients* configuration settings is enabled, users can add email addresses as recipients that may not be users of Symphony. See configuration best practices.

- The *Specify Notification Recipients* application privilege determines which users can add other users as recipients to a notification. Users with this ability may add another user as a recipient of exported content from a view that they wouldn't otherwise be able to access.

- If enabled, the *Enforce Recipient Account Exports* configuration settings always exports content using each recipient's account separately, ensuring that they can each only receive the content and data that they have access to through security privileges and data security.

For more information, see:

- Notification Options
- Troubleshooting notifications
- Data Cube Data Storage Options
- Configuration Settings
- Configuration Best Practices
- Application Privileges
- Symphony Managed Dashboard and Managed Report Security

Customize Branding for Each Tenant

This applies to: *Managed Dashboards, Managed Reports*

Multi-tenancy enables you to use a single instance of Symphony to serve multiple tenants (where each tenant is one of your clients) whose users are isolated from other tenants and see only the appropriate content and data.

This article shows you how to apply further customization to multi-tenant instances at the application level and at the dashboard level so that users belonging to different tenants see different branding elements, such as logos and color schemes, or other customizations.

Note: If you are also providing different URLs for each tenant to access Symphony, you can also set up External Application URI Overrides.

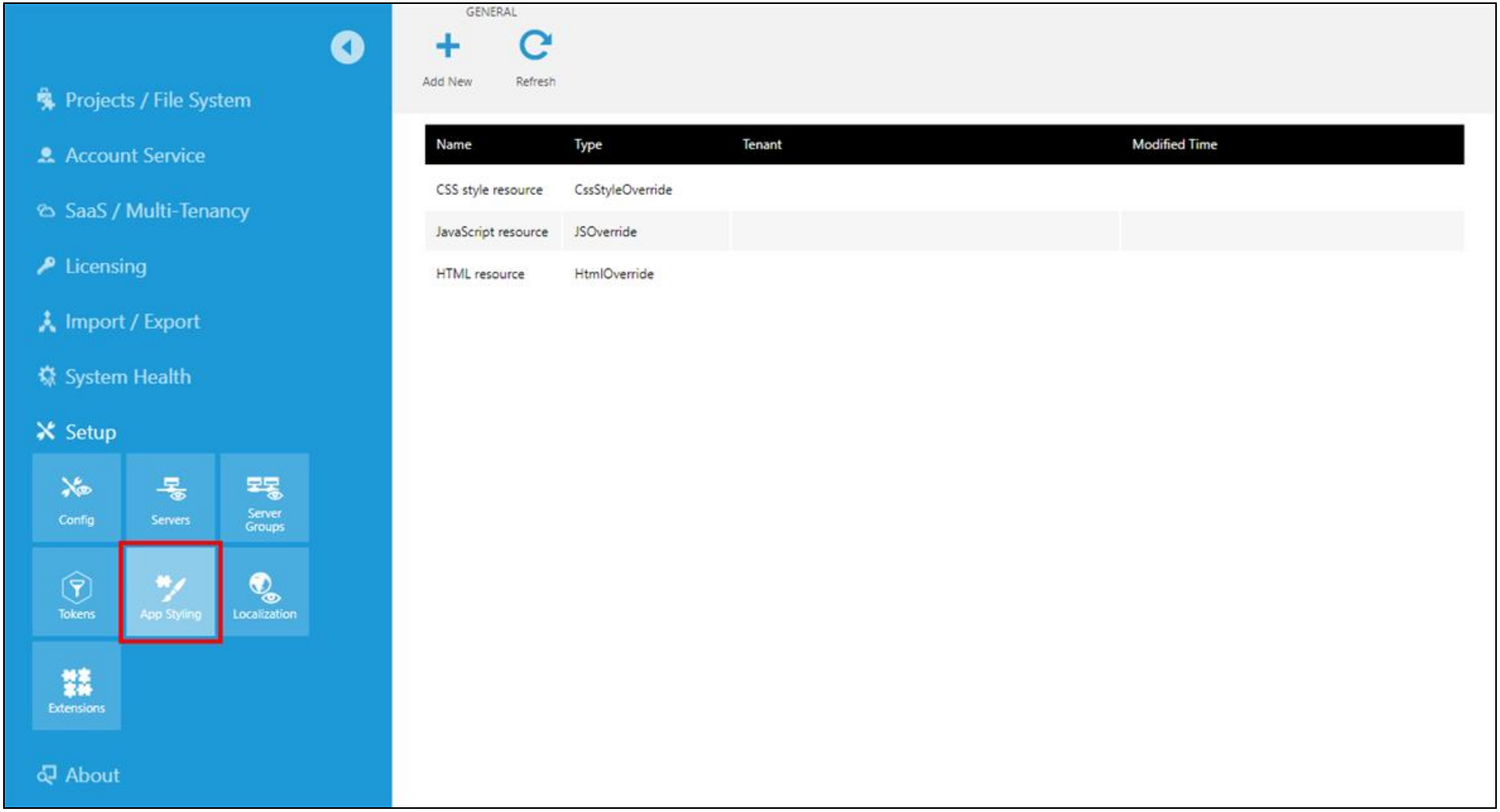
Application Styling Resources

System administrators can add custom CSS styles, JavaScript, and HTML by editing the application styling resources through the Administration interface, as shown in the article on white labeling.

In the case of tenant-specific resources, you can follow the same steps except to add separate styling for each tenant.

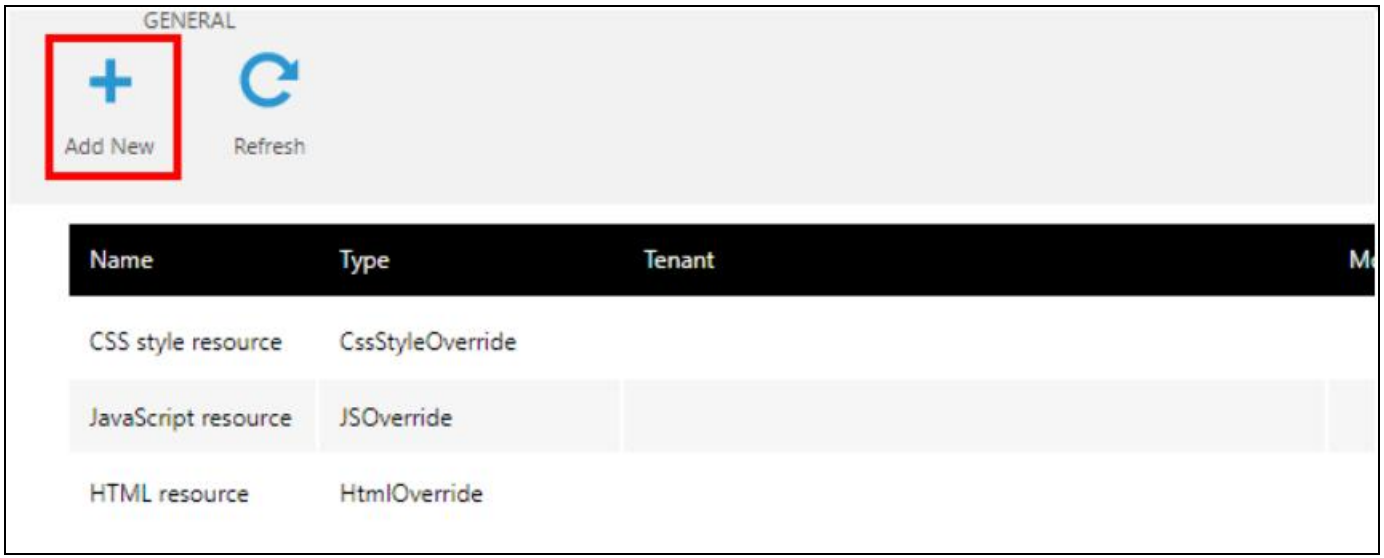
Adding Tenant Resources

Access Administration from the main menu, expand **Setup** and then click **App Styling**.

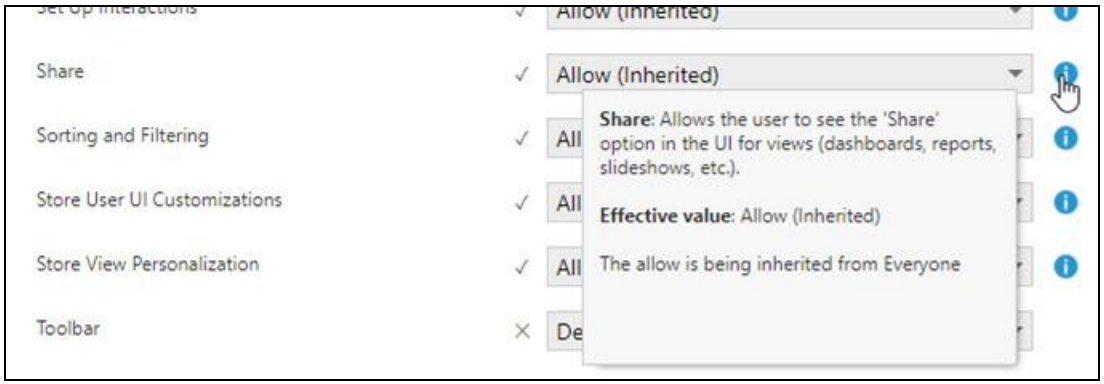


A list of application styling resources is displayed on the right.

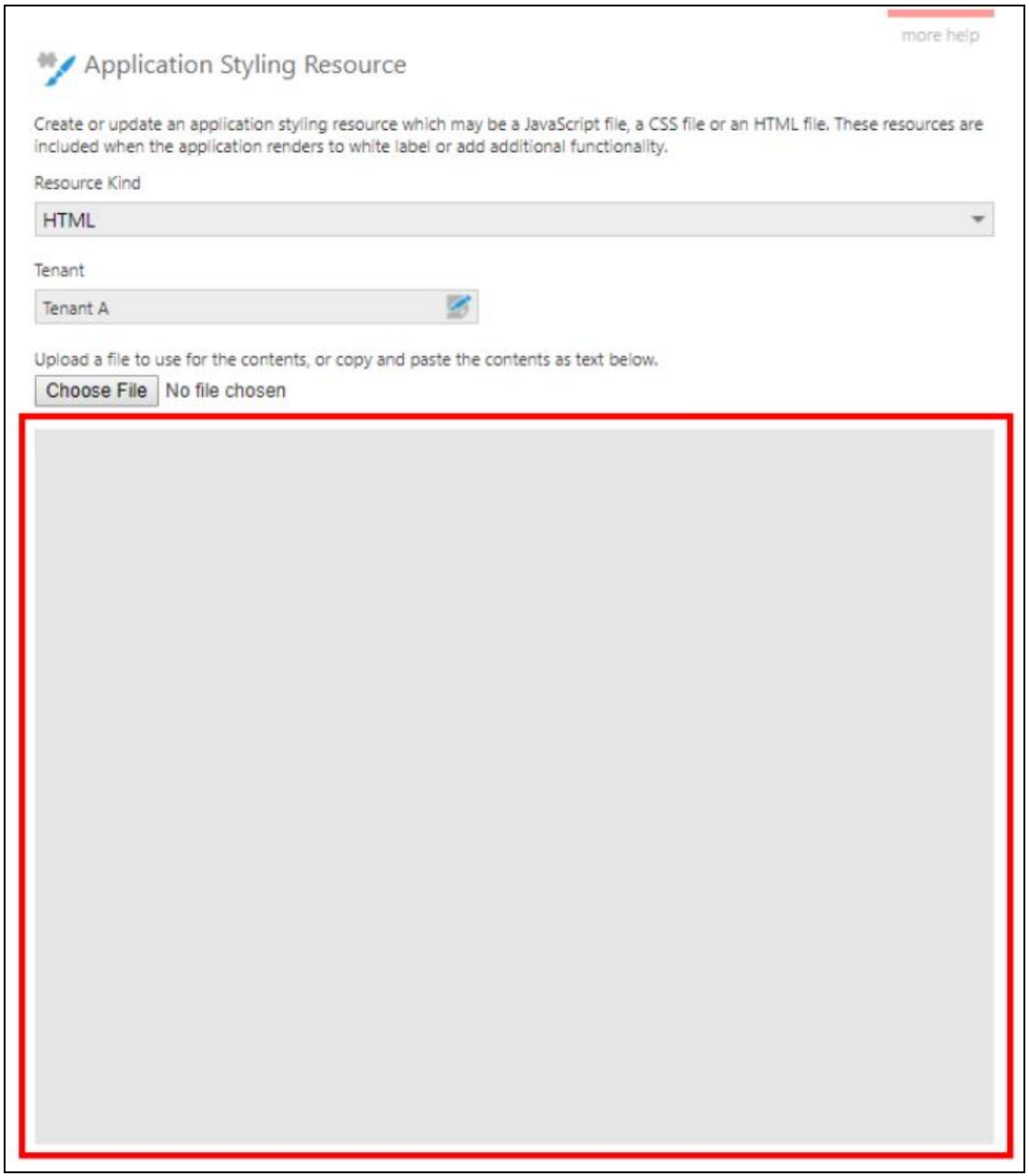
On an instance with multiple tenants, you can click **Add New** in the toolbar to add a new resource that is specific to a tenant.



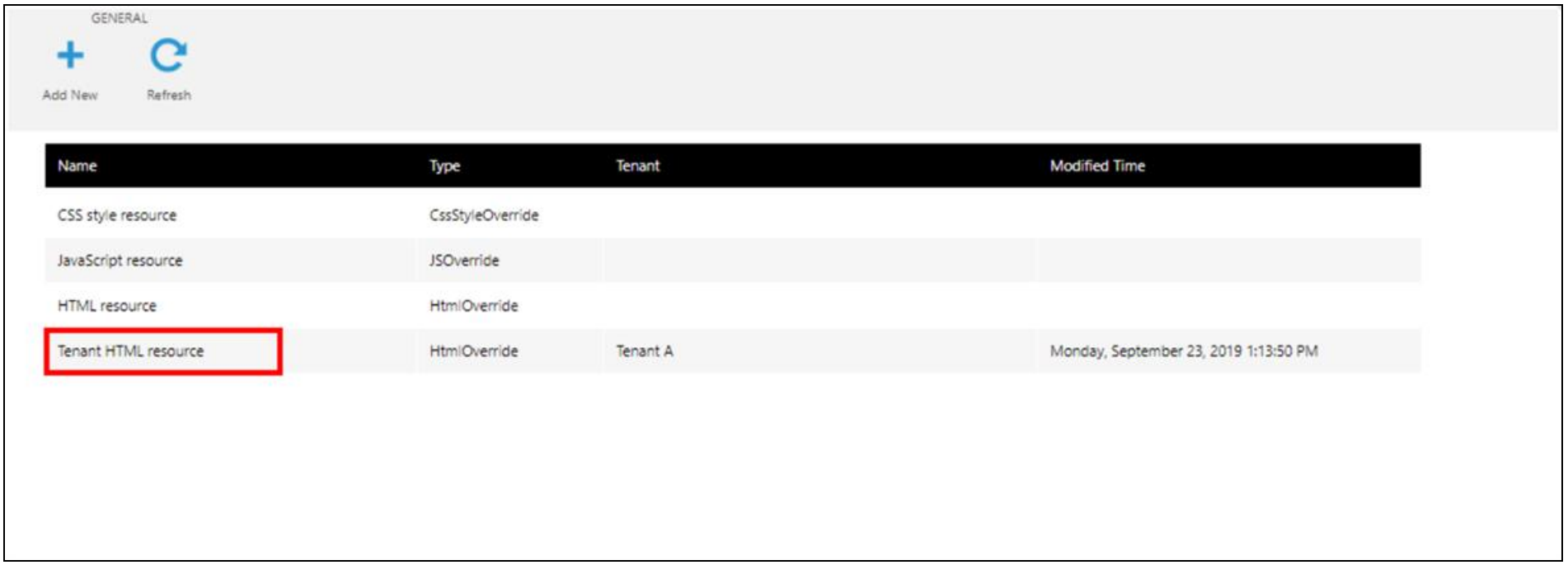
In the *Application Styling Resource* dialog, choose the **Resource Kind** and then select the **Tenant**.



Click **Choose File** to select an existing file containing the content, or enter or paste the styling content directly into the dialog.



Click **Submit**. A separate tenant resource is now listed, which is now applied the next time one of the tenant's users loads a page in Symphony.



Branding the Log On Screen

Styling resources pertaining to the log on page are applied by passing in the corresponding tenant ID via query string when navigating there. For example:

```
http://dbi.example.com:8000/LogOn/?tenantId=bcfad362-12c3-458b-b072-9ea0e4110c4e
```

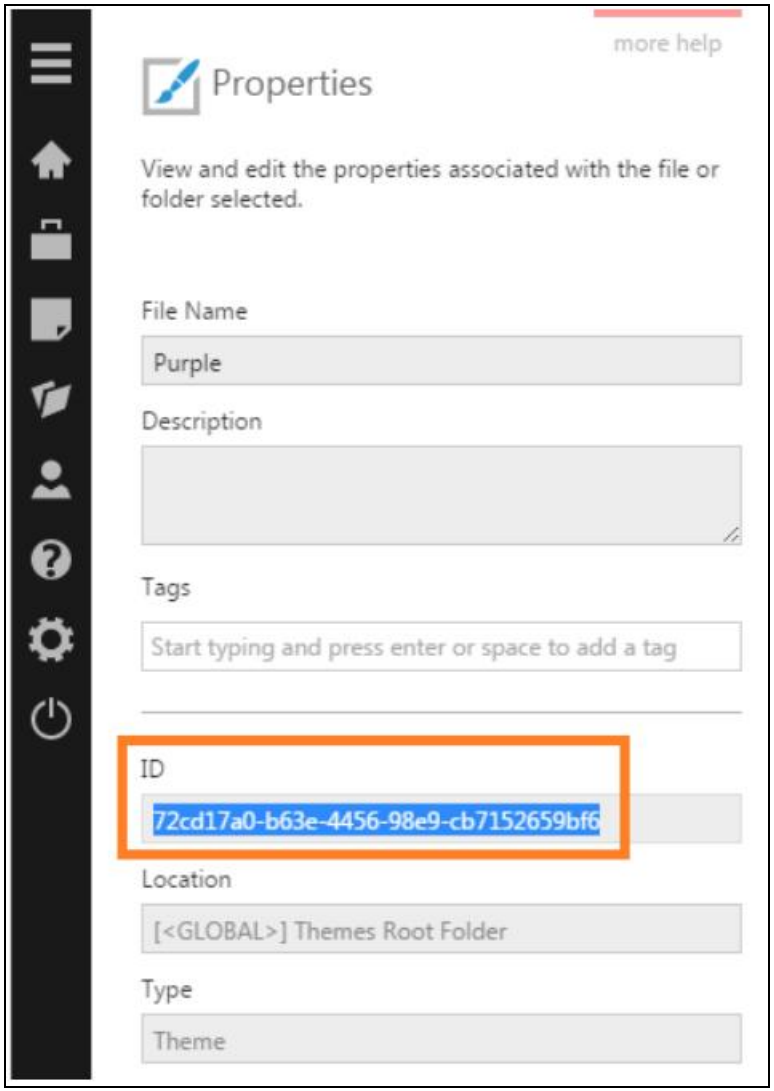
Testing the Styling

To test your tenant-specific resources beyond the log on screen, log on to Symphony with a user account that belongs to the tenant (i.e., the Tenant field is set for this user account). The scripts, styles, and HTML associated with this tenant will be applied.

Apply Dashboard Theme Per Tenant

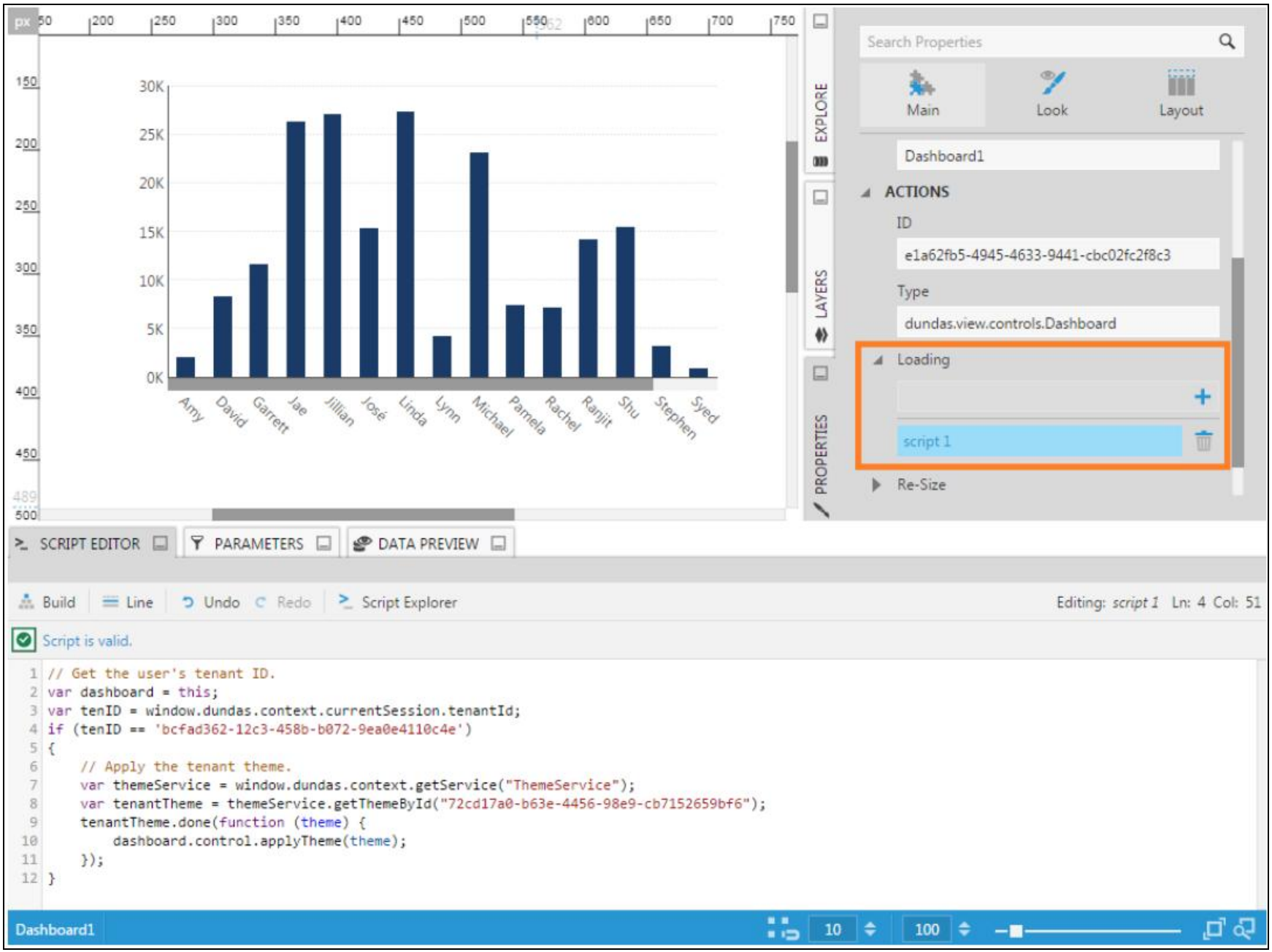
When you want to customize the styling of dashboards that are reused between different tenants, an alternative to using the application styling resources described above is to define tenant-specific styles and themes within Symphony. A simple script can then be used in the **Loading** action of the shared dashboard to load the appropriate theme.

To use this method, first record the ID of the theme file from its Properties dialog.



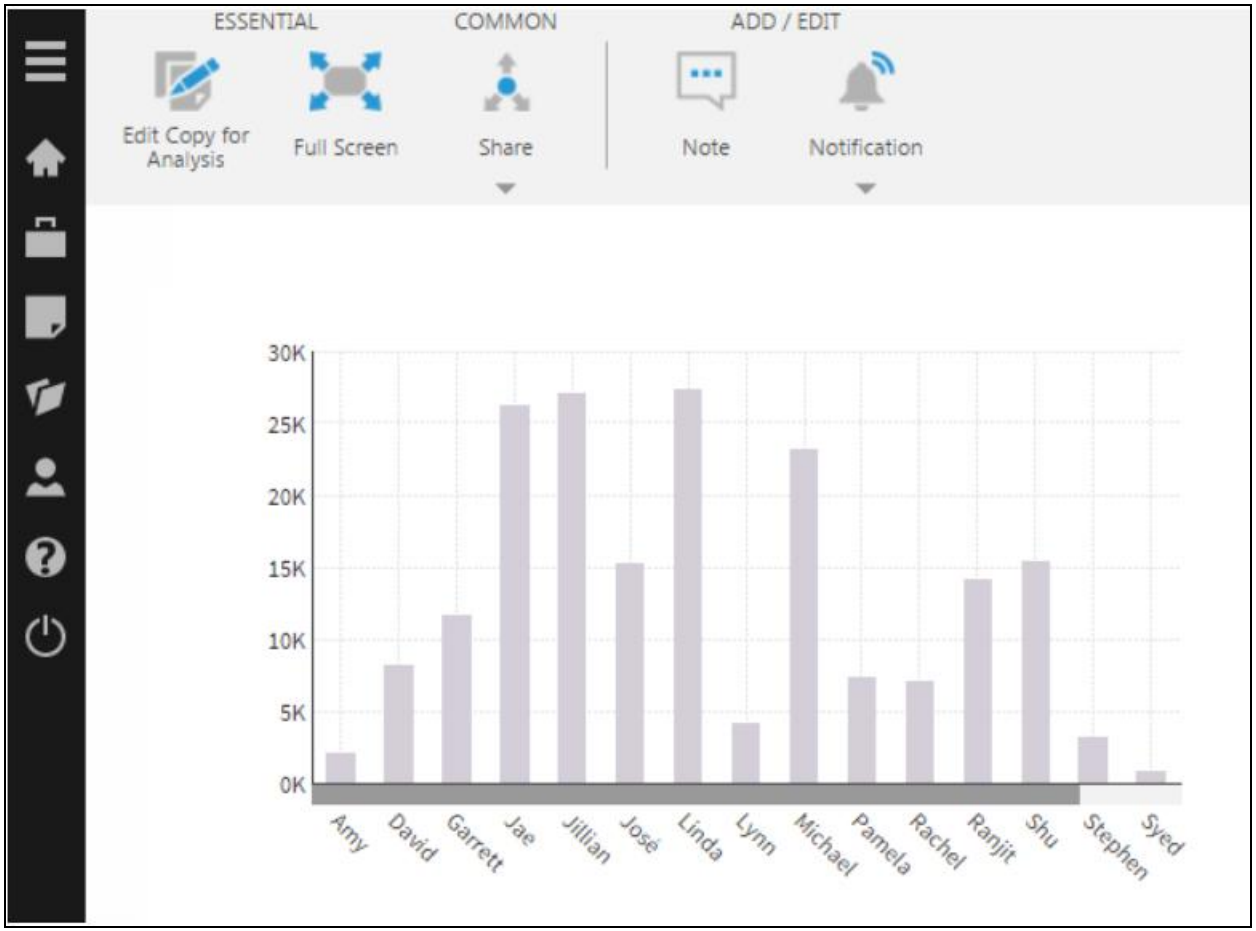
Next, go to the **Properties** window when editing the dashboard and add a **Loading** script action. In the **Script Editor**, you can use code like the following:

```
// Get the user's tenant ID.
var dashboard = this;
var tenID = window.dundas.context.currentSession.tenantId;
if (tenID == 'bcfad362-12c3-458b-b072-9ea0e4110c4e')
{
       // Apply the tenant theme.
       var themeService = window.dundas.context.getService("ThemeService");
       var tenantTheme = themeService.getThemeById("72cd17a0-b63e-4456-98e9-cb7152659bf6");
       tenantTheme.done(function (theme) {
              dashboard.control.applyTheme(theme);
       });
}
```


30K
25K
20K
15K
10K
5K
0K
Amy
David
Garrett
Jae
Jillian
José
Linda
Lynn
Michael
Pamela
Rachel
Ranjit
Shu
Stephen
Syed
EXPLORE
LAYERS
PROPERTIES
Search Properties
Main
Look
Layout
Dashboard1
ACTIONS
ID
e1a62fb5-4945-4633-9441-cbc02fc2f8c3
Type
dundas.view.controls.Dashboard
Loading
script 1
Re-Size
SCRIPT EDITOR
PARAMETERS
DATA PREVIEW
Build
Line
Undo
Redo
Script Explorer
Editing: script 1 Ln: 4 Col: 51
Script is valid.
// Get the user's tenant ID.
var dashboard = this;
var tenID = window.dundas.context.currentSession.tenantId;
if (tenID == 'bcfad362-12c3-458b-b072-9ea0e4110c4e')
{
// Apply the tenant theme.
var themeService = window.dundas.context.getService("ThemeService");
var tenantTheme = themeService.getThemeById("72cd17a0-b63e-4456-98e9-cb7152659bf6");
tenantTheme.done(function (theme) {
dashboard.control.applyTheme(theme);
});
}
Dashboard1
10
100

To test the dashboard, check it in, log off and log back on as a user that belongs to the tenant, then view the dashboard.

For the example script above, the Purple theme should be automatically applied.



For more information, see:

- White Labeling the Application
- Localization and Multi-Language Support
- Setting a Default Theme

Dedicated Warehouse Databases for Tenants

This applies to: *Managed Dashboards, Managed Reports*

Tenants can have their own dedicated warehouse databases. This allows for better security control and also helps isolate the load on the warehouse databases between tenants, when compared to a shared warehouse database.

This article provides the necessary steps to:

- Create a dedicated tenant warehouse database and migrate tenant data from the global warehouse database.
- Remove a dedicated tenant warehouse database and migrate tenant data back to the global warehouse database.

Note: The tasks detailed in this article are advanced and it is recommended that they be performed by users familiar with using .NET or REST APIs and the command line interface.

Create a Dedicated Tenant Warehouse Database

Creating a dedicated warehouse database and migrating tenant data from the global warehouse database to the tenant warehouse database involves the following steps.

Disable the Tenant

Admin users can select **Tenants** from the main menu to open the Tenants work area. Find your tenant, select **Edit tenant** in the **Actions** menu, and slide the **Enable tenant** toggle to the left.

For more information, see Disable, Enable, and Remove Tenants.

Set the Configuration Value From the Command Line

Set the *AllowTenantWarehouses* configuration setting value to **True** using the command line. Using the command prompt, enter the following:

```
dt setConfigValue /settingId:cde27d97-d493-475d-aba2-783b4a200237 /value:True
```

See Set a Configuration Value From the Command Line.

Add the Tenant Warehouse Override Using the API

You must add a tenant warehouse override using either the .NET API or the REST API.

Note: More than one *TenantWarehouseOverride* can be created for a tenant, each one corresponding to a different *scope* (similar to configuration settings). This flexibility would be required if you have a server farm in which different servers need to use different connection strings for the same physical database. The overrides here represent a different means of accessing the same database, rather than accessing different databases. In most cases this flexibility is not required, and the warehouse override should be applied only at the *Global* scope.

The following example demonstrates how to add a tenant warehouse database override using the .NET API:

```
// get tenant
var mtSvc = Engine.Current.GetService<IMultiTenancyService>();
Tenant tenant = mtSvc.GetTenant(/*pass tenant ID here*/);

// create tenant warehouse override
TenantWarehouseOverride whOverride = new TenantWarehouseOverride()
{
       Scope = AppSettingScope.Global, // desired scope
       ScopeTarget = null, // desired scope target
       ConnectionString = tenantWHConnStr, // connection string to the future tenant warehouse DB
};
tenant.SetWarehouseOverride(whOverride);
mtSvc.SaveTenant(tenant);
```

The following example demonstrates how to add a tenant warehouse database override using the REST API from JavaScript, where a *sessionId* has already been obtained via logging on:

```
var warehouseOverrideData = {
       connectionString: "[connectionString]",
       password: "[password]",
       scope: "[scope]",
       scopeTarget: "[scopeTarget]"
};

var jqXHR = $.ajax({
       url: "/api/tenant/SetWarehouseOverride?id=[tenantId]",
       type: "POST",
       contentType: "application/json",
       headers: { "Authorization": "Bearer " + sessionId" }
       dataType: "json",
       data: JSON.stringify(warehouseOverrideData)
});
```

Migrate Tenant Data Using the Command Line

The dt command line tool is used as shown below to migrate the tenant data. You can choose either to create the tenant warehouse database manually using your database administration tools and then run the *migrateTenantData* command to migrate tenant data to the warehouse database, or you can just run the *migrateTenantData* command on the command line to both create the warehouse database and migrate tenant data to it.

Ensure that the connection string used here has the same server and database as the connection string used for the tenant warehouse override and its credentials need to have the appropriate privileges to create and/or instantiate the database and migrate data from your global warehouse to it.

```
dt migrateTenantData /tenantId:[tenant ID] /direction:toTenantWh /tenantWhCs:[connection string to the tenant warehouse DB]
```

Enable the Tenant

Admin users can select **Tenants** from the main menu to open the Tenants work area. Select **Show disabled** to display disabled tenants. Find your tenant, select **Edit tenant** in the **Actions** menu, and slide the **Enable tenant** toggle to the right.

For more information, see Disable, Enable, and Remove Tenants.

Remove a Dedicated Tenant Warehouse Database

Removing a tenant database and migrating the tenant data back to the global warehouse database involves the following steps.

Disable the tenant

Before removing a dedicated tenant warehouse database you must disable the tenant.

Remove the tenant warehouse override using the API

You can remove a tenant warehouse override using either the .NET API or the REST API. The examples below follow from the ones earlier that added overrides.

In .NET:

```
// get tenant
var mtSvc = Engine.Current.GetService<IMultiTenancyService>();
Tenant tenant = mtSvc.GetTenant(/*pass tenant ID here*/);

// remove tenant warehouse override
tenant.RemoveWarehouseOverride(AppSettingScope.Global, null);
mtSvc.SaveTenant(tenant);
```

Using REST:

```
var warehouseOverrideRemoveData = {
       scope: "[scope]",
       scopeTarget: "[scopeTarget]"
};
var jqXHR = $.ajax({
       url: "/api/tenant/RemoveWarehouseOverride?id=[tenantId]",
       type: "POST",
       contentType: "application/json",
       headers: { "Authorization": "Bearer " + sessionId" }
       dataType: "json",
       data: JSON.stringify(warehouseOverrideRemoveData)
});
```

Migrate Tenant Data Back to the Global Warehouse DB Using the Command Line

Use the dt command below to migrate tenant data back to the global warehouse database.

Ensure that the connection string used here has the same server and database as the connection string that was used when setting up the tenant warehouse override. The credentials must also have the appropriate privileges to migrate data from your tenant warehouse to the global warehouse, and to remove the the tenant warehouse database if you use the *dropTenantWh* argument.

```
dt migrateTenantData /tenantId:[tenant ID] /direction:toGlobalWh /tenantWhCs:[connection string to the tenant warehouse DB]
```

Enable the Tenant

Re-enable the tenant as described above.

Important Notes

- Tenant warehouse overrides are not transferred by export/import. If they are required, they should be created independently in each instance.
  - If both source and target instances have tenant warehouse databases, tenant data will be transferred from the source tenant warehouse database to the target tenant warehouse database.
  - If only the source instance has tenant warehouse database, the tenant data will be transferred from the source tenant warehouse database to the target global warehouse database.

  - If only the target instance has tenant warehouse database, tenant data will be transferred from the global warehouse database to the target tenant warehouse database.

- It is recommended to include the tenant name or ID into the name of your tenant warehouse database for maintenance purposes.

- The tenant ID is stored in the *GlobalProperty* table of the tenant warehouse database, under the *TenantId* property name. This ID is also used to validate the migration processes.

- Processes such as upgrade or health checks that are applicable to the global warehouse database, will be applied to all existing tenant warehouse databases. Note that even though the process mimics the transactional behavior, integrity across multiple warehouse databases is not guaranteed. For example, the upgrade can succeed for the global warehouse database but could fail for tenant warehouse databases.

- The *TenantWarehouseOverride* is active only if a matching scope and scope target is stored in the configuration settings. When tenant data is processed, the app tries to find *TenantWarehouseOverride* matching the effective application scope and scope target. If not found, the application tries to use the *TenantWarehouseOverride* created *for AppSettingScope.Global*, and if that is not available, the global warehouse database will be used.

For more information, see:

- Using the dt Command Line Tool
- Set a Configuration Value From the Command Line
- Multi-Tenancy in Symphony
- Manage Licenses
- Getting started with the .NET API
- REST API Reference

Enabling Active Directory Authentication From Multiple Forests

This applies to: *Managed Dashboards, Managed Reports*

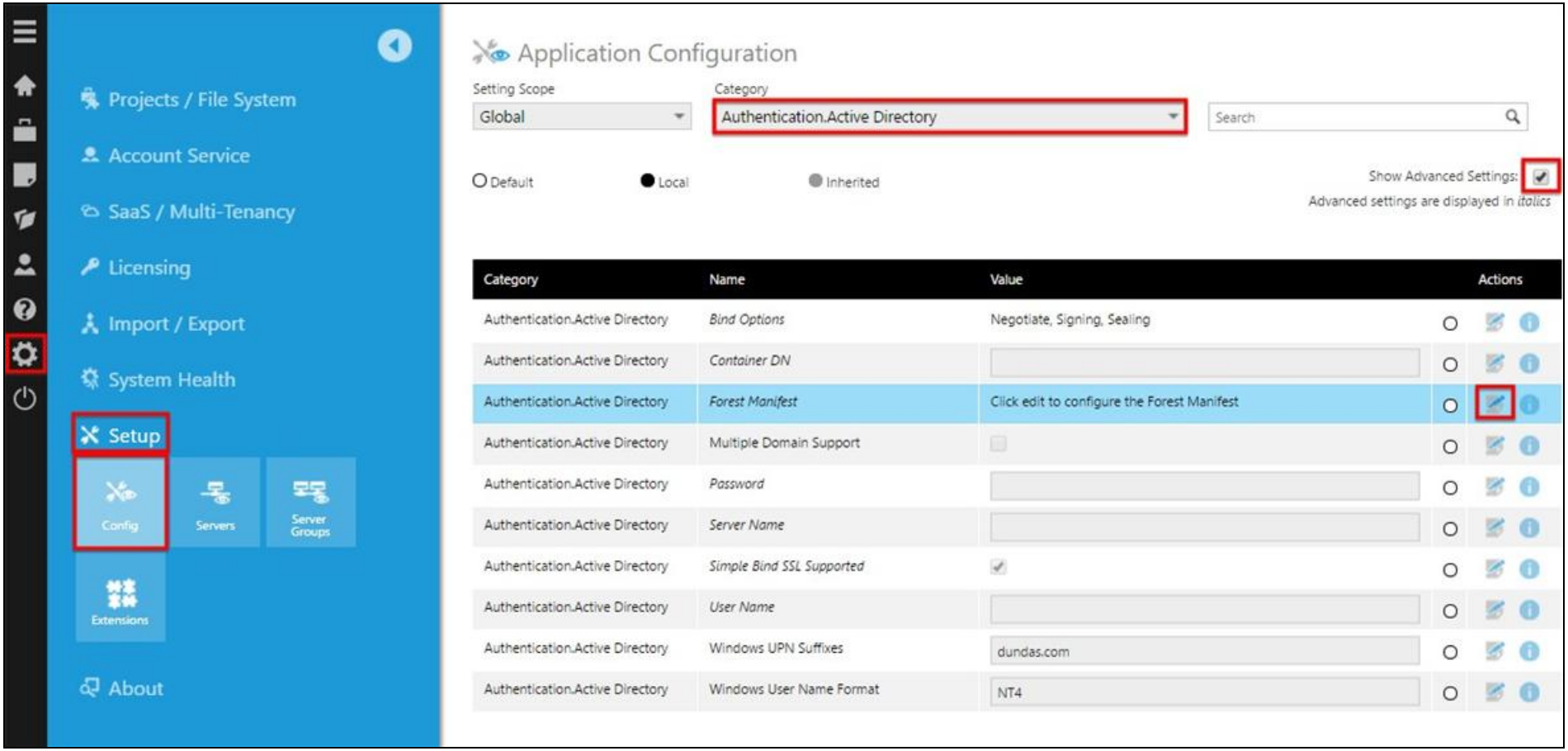
Active Directory or Windows authentication in Symphony can be set up according to other configuration settings or by using a *Forest Manifest*. The manifest is a JSON array that defines and configures one or more Active Directory domains.

Note: When using the *Forest Manifest* configuration setting, Symphony will ignore the other Active Directory configuration settings.

Forest Manifest

To create the manifest, open the **Admin** section of Symphony, then select **Setup** and **Config**.

Change the **Category** to *Authentication.Active Directory* and choose the option to display advanced settings, then select and edit *Forest Manifest*.



Manifest Properties

The manifest is configured in the form of a JSON array containing the following properties of any desired Active Directory forests:

- **ForestName** (optional). Specifies the name of the forest. This property must be unique across all the forests in the manifest. If not specified, the name of the forest associated with the server's domain will be used.

- **Domains**. A case-insensitive list of domain names that map to the forest.

- **ServerName** (optional). Specifies the name of the domain or domain controller to which Active Directory queries will be directed for this forest. If not specified, the name of the forest will be used,
- **UserName** (optional). The name of the user to use when querying Active Directory. If not specified, explicit credentials will not be used when querying.
- Password (optional). The password of the user to use when querying Active Directory. If not specified, an explicit password will not be used when querying.
- **BindOptions** (optional). Specifies options that are used when binding to the Active Directory server. If not specified, the default value will be used *(Negotiate, Signing, Sealing)*. For a full list of options, see the Microsoft ContextOptions Enumeration.
- **ContainerDN** (optional). Specifies the distinguished name (DN) of the container to use when binding to Active Directory. If not specified, no container will be specified in the connection.
- **SimpleBindOverSslSupported** (optional). A Boolean value indicating whether the Active Directory server supports simple bind connections using Secure Sockets Layer (SSL). If disabled, the validation of user-entered Windows credentials may cause the system to perform the additional step of translating the supplied down-level logon name to User Principal Name (UPN) format. If not specified, the default value will be used *(True)*.

Note: If you are receiving an error stating *The application encountered a problem trying to validate your Windows credentials with the underlying error The LDAP server is unavailable*, it may be due to a connection protocol issue. You can resolve this issue by setting SimpleBindOverSslSupported to *False*.

Example

Paste or type the JSON array into the text field. The following example configures two forests in the most basic way, the first of which specifies the forest associated with the server's domain:

```
[
        {
                "ForestName": "example.com",
                "Domains": [ "example", "example.com" ],
        },
        {
                "ForestName": "rootdomain.local",
                "Domains": [ "rootdomain", "rootdomain.local", "sample.sample" ],
        }
]
```

For more information, see:

- Configuration Settings
- Symphony Single Sign On
- Administration home page

Enabling Federated Authentication

Federated authentication enables your users to log on to Symphony by authenticating using a third-party identity provider. For example, redirect users to an Okta login screen instead of the standard Symphony log on. Your users authenticate using relevant credentials, then are redirected back to Symphony along with their user information.

Once authenticated through the identity provider, federated authentication behaves as Single Sign On (SSO).Users can access multiple services without the need for further authentication.

Setting up federated authentication Symphony requires two things:

1. A **Federated Authentication Manifest** – a JSON array containing all of the properties required for the federated authentication.
2. A **Federated Authentication Bridge** – a web application in the Symphony infrastructure.

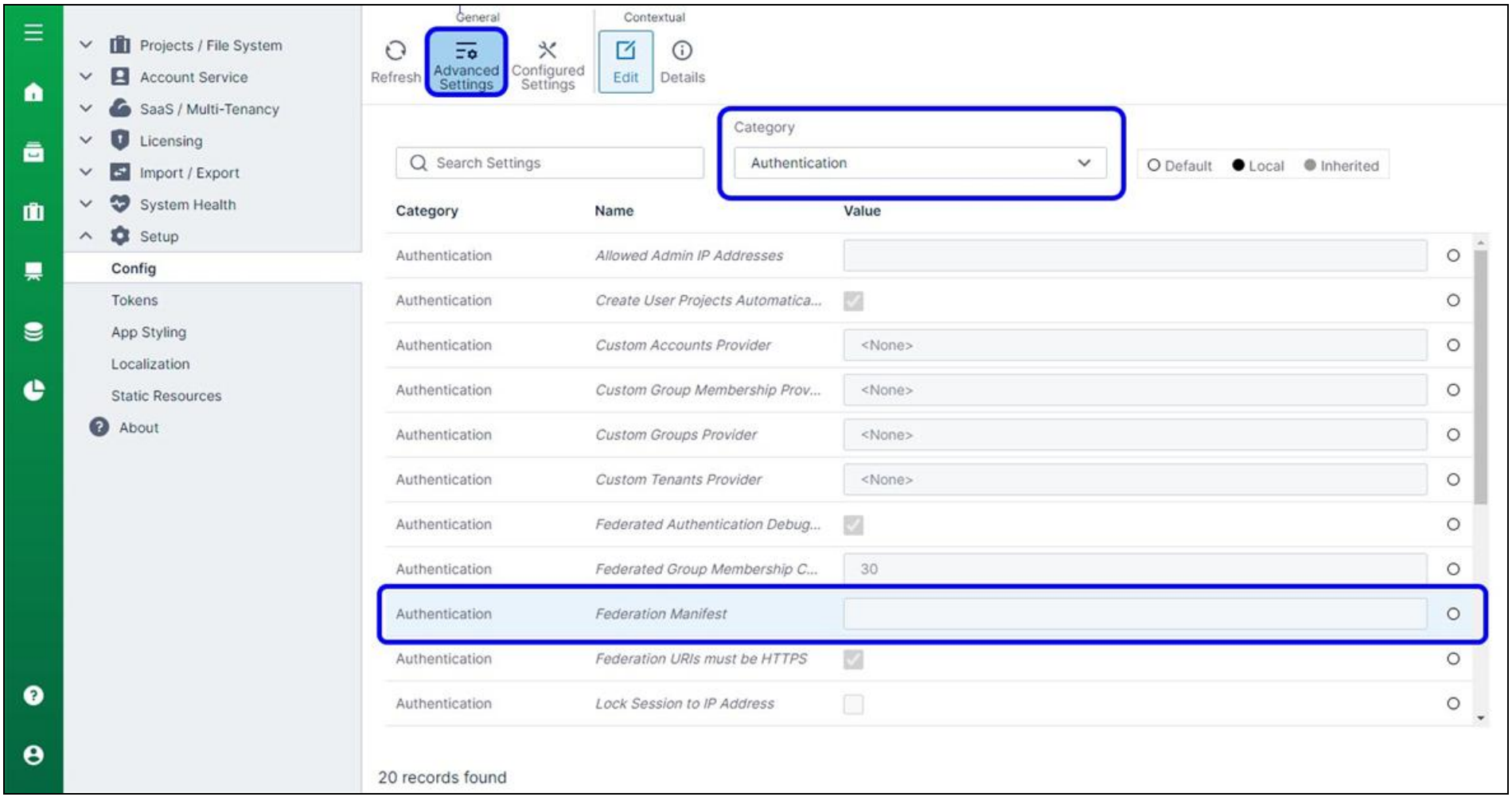
Once federated authentication is set up, External User accounts may be created automatically or an administrator may create External User accounts and External Group accounts, which can be logged on only through federated authentication. See Advanced User Management.

Federated Authentication Manifest

The authentication manifest defines and configures one or more Federated Authentication Providers, which are external applications you are entrusting with authenticating on behalf of Symphony.

To create the manifest:

1. Navigate to the Administration area of Symphony from the main menu in Managed Dashboards and Managed Reports (**Profile** > **Administration**).
2. Expand the **Setup** section, then select **Config** to edit Symphony's configuration settings.
3. Change the **Category** to **Authentication**, ensure **Advanced Settings** is selected on the toolbar.
4. Select the **Federation Manifest** setting and then select **Edit** on the toolbar.



The manifest is configured in the form of a JSON array containing the following properties for each authentication provider you wish to configure:

- **Id (optional)**. An arbitrary string used to identify the provider (referred to elsewhere on this page as `providerId`). May be omitted if the manifest only contains one provider. Must be unique when specifying multiple authentication providers in the manifest. Note: for compatibility reasons, the value should only contain characters which can be used in a URL without being escaped.

- **Caption (optional)**. Specifies the text that should be displayed on the Logon page button for this authentication provider, or set to "-" (a dash) if it should not be shown. If not set, the caption will default to the provider ID.

- **ProtocolId**. Specifies the ID of the protocol to be used by the authentication provider. Symphony supports the following protocols, or see the sections below for details:
  - Saml2
  - OpenIdConnect
  - GoogleOAuth2
  - MicrosoftIdentity
  - Facebook
  - Jwt
- **Properties**. A JSON object containing protocol-specific information, such as a metadata URL, client ID, and client secret. See the protocol-specific section for details on the properties that may be specified here.
- **ClaimTypes (optional)**. A JSON object providing a mapping between claim types and specific kinds of information required by Symphony (see the **Claim type mappings** section below). The minimum required mapping is that one claim corresponds to `AccountName`. Specifying explicit claim type mappings is not required if the default mappings are already correct.
- **CustomAttributeClaimTypeMapping (optional)**. A JSON object providing a mapping of custom attribute IDs to claim types. When a user authenticates, the value of each specified custom attribute on their logon session will be populated with the data from the corresponding claim.
- **AccountAutoCreationMode (optional)**. Specifies how Symphony should behave when a user successfully authenticates. The value may be one of the following:
  - **None**. An external user account should never be automatically created. Only users with pre-existing accounts in Symphony should be able to log on.
  - **Group (default)**. If the claim contains a group name corresponding to an External Group account, a virtual user account should be created for the user.
  - **Open**. A non-virtual user account should be created for any user that successfully authenticates. The created External User account will default to authenticate only via the used identity provider, which can be modified later.
- **AccountAutoCreationSeatMode (optional)**. Specifies the account auto-creation seat mode. If not specified, the default value will take effect. The value may be one of the following, subject to the availability of licensed Standard User seats:
  - **Floating (default)**. An external user account will be automatically created with a floating seat.
  - **Reserved**. An external user account will be automatically created with a reserved seat.

- **AccountNamePrefix (optional)**. A prefix that is prepended to the account names extracted from the claims.
- **AllowMissingTenantClaim (optional)**. A value indicating whether the application will allow authentication when there is a tenant name or ID mapping, but no corresponding claim was returned with that information. The value may be either `true` or `false`. The default value is `false`.
- **EnableFederatedLogout (optional)**. If set to **true**, logs out of the identity provider when the user actively logs out through the UI or navigates to the path `/LogOn/LogOff` under the Symphony instance. SAML 2.0 requires a signing certificate to be configured for this option – for details, see the note in the SAML 2.0 section.

Minimal example:

```
[
	{
		"ProtocolId": "SAML2",
		"Properties":
		{
			"idpMetadataLocation": "https://identityprovider.example.com/FederationMetadata.xml",
		},
	},
]
```

Extended example:

```
[
	{
		"Id": "ADFS-Saml2",
		"ProtocolId": "SAML2",
		"Caption": "Windows Active Directory Logon",
		"AccountAutoCreationMode": "Open",
		"Properties":
		{
			"idpMetadataLocation": "https://identityprovider.example.com/FederationMetadata.xml",
			"clientSecret": "skljdsf978dsf74A-cjmr7B6",
		},
		"ClaimTypes":
		{
			"AccountName": "http://schemas.xmlsoap.org/ws/2005/05/identity/claims/name",
			"DisplayName": "displayName",
		},
		"CustomAttributeClaimTypeMapping":
```

```
                {
                        "9f984590-01c6-4b3f-a892-03c10d405823": "http://schemas.xmlsoap.org/ws/2005/05/identity/claims/postalcode",
                        "38e91753-09fd-4f91-87bb-b2fa8510d61b": "http://schemas.xmlsoap.org/ws/2005/05/identity/claims/country",
                },
        },
        {
                "Id": "Google",
                "ProtocolId": "GoogleOAuth2",
                "AccountAutoCreationMode": "Open",
                "AccountNamePrefix": "GoogleAccount_",
                "Properties":
                {
                        "clientId": "01234567890-abcdefghijklmnopqrstuvwxyz012345.apps.googleusercontent.com",
                        "clientSecret": "skljdsf978dsf74A-cjmr7B6",
                },
        },
]
```

Configure Federation Manifest

The configuration manifest for federated authentication. Value is a JSON array containing the properties of any desired federated authentication providers.

○ Reset to default

◉ Edit value

```
[
    {
        "ProtocolId": "SAML2",
        "Properties":
        {
            "idpMetadataLocation": "https://identityprovider.example.com/Federatio
        },
    },
]
```

Important: Any URLs specified in the manifest (or read from the identity provider's metadata) must use the HTTPS protocol. If the HTTP protocol is required, disable the `Federation URIs Must Be HTTPS` configuration setting.

Claim Type Mappings

The default claim type mappings in Symphony are as follows:

Item	Claim Type
AccountName	http://schemas.xmlsoap.org/ws/2005/05/identity/claims/nameidentifier
DisplayName	http://schemas.xmlsoap.org/ws/2005/05/identity/claims/name
Email	http://schemas.xmlsoap.org/ws/2005/05/identity/claims/emailaddress
Culture	http://schemas.xmlsoap.org/ws/2005/05/identity/claims/locality
GroupName	http://schemas.microsoft.com/ws/2008/06/identity/claims/role

These default mappings may be overridden by information built-in to the authentication protocol, and further by the authentication provider using the **ClaimTypes** property in the federation manifest. See the corresponding protocol-specific section below for information on which claim type mappings are overridden by that protocol (if any).

When using multi-tenancy, additional claim types can optionally be specified in a provider's **ClaimTypes** property, in order to allow automatically-created accounts to be associated with a particular tenant:

- **TenantId** - The GUID of the tenant.
- **TenantName** - The name of the tenant.

If both a tenant ID and a tenant name are included in the claims, the ID takes precedence. If neither are included, but a claim type mapping has been set up for the tenant ID and/or name, then an error will occur when attempting to automatically create the account (unless the **AllowMissingTenantClaim** property has been specified with a value of `True`.)

Important: If a mapping for the tenant ID and/or name has been specified, a corresponding claim *must* be included in the response by the identity provider. This is done for security reasons to reduce the likelihood of an account incorrectly not being associated with a tenant due to misconfiguration of the identity provider's claim rules.

Authentication Protocols

This section lists the federated authentication protocols supported by Symphony. Note that SAML 2.0 and OpenID Connect are standards adopted by various identity providers.

SAML 2.0

Protocol ID: SAML2

Properties:

- **idpMetadataLocation**. The URL of the identity provider's metadata document.
- **spEntityId (optional)**. This is the service provider ID, which Symphony will use to identify itself to the identity provider. If the value is not specified, it will default to the `Federation Bridge URL`. Note: if a value is specified for this property, it must be a well-formed URI.
- **requestSigningBehavior (optional)**. The preferred behavior for signing requests. The values may be `Always`, `Never`, or `IfIdpWantAuthnRequestsSigned` (outgoing requests will be signed only if the identity provider metadata specifies that this is required). If the value is not specified, it will default to `IfIdpWantAuthnRequestsSigned`.
- **minIncomingSigningAlgorithm (optional)**. The minimal security hash algorithm (SHA) acceptable in the signature. To allow SHA1, the value should be `http://www.w3.org/2000/09/xmldsig#rsa-sha1`. If the value is not specified, it will default to SHA2.

Important: If the identity provider metadata specifies that authentication requests must be signed, signing will be performed using the certificate specified in the applicable configuration settings (**Signing Certificate** on Windows-based installations or **Signing Certificate Path** on Linux-based installations).

Note: Symphony does not support unsolicited IdP-initiated SAML responses; the SP-initiated flow must be used.

OpenID Connect

Protocol ID: `OpenIdConnect`

Properties:

- **metadataAddress (optional)**. The URL of the identity provider's metadata document.
- **authority (optional)**. The authority to use when making OpenID Connect calls. This is required if the metadata location is not specified.
- **clientId**. The `client_id` parameter used in the protocol.

- **clientSecret (optional)**. The secret key provided by the identity provider used to redeem an authorization code for an access token. Not required in many cases.

- **scope (optional)**. The value of the scope parameter in the OpenID Connect flow. If not specified, defaults to **openid profile**.

Redirect URI

If required by your identity provider, the redirect URL for Symphony should be in one of the following formats.

Linux installations and all installations :

```
{Base URL}/managed/AuthBridge/signin-oidc/{providerId}
```

Or on Windows:

```
{Base URL}/managed/AuthBridge/
```

For example, if you have set up a provider in the federated authentication manifest with "`Id`": "`MyProvider`", the URI may be something like `https://symphony.example.com/managed/AuthBridge/signin-oidc/MyProvider`.

Microsoft Identity (Office 365 and Azure Active Directory)

Protocol ID: `MicrosoftIdentity`

To configure federated authentication using Azure Active Directory, perform the following steps in the Azure Portal (https://portal.azure.com):

1. Create a new App Registration for Symphony. The redirect URI should be set in the format `{Base URL}/managed/AuthBridge/signin-oidc/{providerId}`. For more details, set this according to the Redirect URI section above for OpenID Connect.

2. Use the **Manage** > **Certificates** & secrets blade to create a new client secret for the App Registration. Use this as the value of the `clientSecret` property in the federation manifest.

3. In the **Manage** > **Authentication** blade, enable the **ID** tokens option under the **Implicit Grant** section, and save your changes.

4. Use the **Manage** > **API Permissions** blade to grant basic permissions to Symphony. The following delegated permissions will need to be granted under **Microsoft Graph**:

   a. `User.Read` (Sign in and read user profile)

   b. `Directory.AccessAsUser.All` (Access directory as the signed in user)

5. Once the above permissions have been added, select **Grant admin consent** , then **Yes** on the confirmation popup.

6. Edit the Manifest of the App Registration, and change the value of the `groupMembershipClaims` property to "`SecurityGroup`".

Properties:

- **tenantId**. The tenant GUID (Directory ID) for the Azure subscription associated with your Azure Active Directory instance.
- **clientId**. The application ID from the App Registration in the Azure Portal.
- **clientSecret**. The secret key generated in the Azure Portal.
- **domain (optional)**. The explicit name of the domain to use for authentication.
- **instance (optional)**. The URL of the instance to authenticate against. If not specified, defaults to `https://login.microsoftonline.com/`.
- **metadataAddress (optional)**. The URL of the identity provider's metadata document.
- **authority (optional)**. Typically something like `https://login.microsoftonline.com/<TENANT_GUID>`.

Overridden claim type mappings:

Item	Claim Type
AccountName	preferred_username
DisplayName	name
Email	preferred_username
GroupId	groups

Google OAuth 2.0

Protocol ID: `GoogleOAuth2`

Use the Google Developer Console to create a new OAuth 2.0 client ID and register the Symphony Authentication Bridge web application. Specify `Web application` as the application type. An authorized redirect URI must be specified in the following format:

```
{Base URL}/managed/AuthBridge/signin-google/{providerId}
```

For example, if you have set up a Google provider in the federated authentication manifest, and the ID of the provider is `MyGoogleProvider`, the URI may be something like `https://symphony.example.com/managed/AuthBridge/signin-google/MyGoogleProvider`.

Properties:

- **clientId**. The client ID provided when setting up the OAuth 2.0 credentials in the Google API Manager.
- **clientSecret**. The Google-assigned client secret.

Overridden claim type mapping:

Item	Claim Type
AccountName	http://schemas.xmlsoap.org/ws/2005/05/identity/claims/emailaddress

Facebook

Protocol ID: `Facebook`

The Facebook Developer Portal has to be used to register the Symphony Authentication Bridge web application. An authorized redirect URI must be specified for the `Web` platform in the following format:

```
{Base URL}/managed/AuthBridge/signin-facebook/{providerId}
```

For example, if you've set up a Facebook provider in the federated authentication manifest, and the ID of the provider is `MyFacebookProvider`, the URI may be something like `https://symphony.example.com/managed/AuthBridge/signin-facebook/MyFacebookProvider`.

The Symphony account name for this provider is in the format `Facebook_<nameid>`, where `nameid` corresponds to the ID of the Facebook account.

Properties:

- **appId**. The application ID provided when setting up the application in the Facebook Developer Portal.
- **AppSecret**. The Facebook-assigned client secret.

Overridden claim type mapping:

Item	Claim Type
AccountName	http://schemas.dundas.com/dbi/2016/11/claims/prefixednameid

JWT (JSON Web Tokens)

Protocol ID: `Jwt`

When you use the JWT protocol, your web application triggers an authentication process instead of redirecting users to another URL to authenticate. The authentication process makes the following **POST** request to Symphony's federated authentication bridge application:

```
{Base URL}/managed/AuthBridge/Jwt-{ProviderId}/ProcessJwt
```

- **URI Parameters**: You can include the optional query string parameters listed in the configuration section below.
- **Body**: Your JWT created including sub (username) and other claims should be provided in the body of the request, either using URL encoding (application/x-www-form-urlencoded) with the key *jwt*, or with the JWT as the entire body. For example, a form with an action attribute set to the request URL, and containing a hidden input with name set to *jwt* and value containing the JWT string, will make this request.
- **Response**: Upon successful authentication, a Symphony session will be created, the JWT will no longer be referenced, and the user will be redirected to the Symphony application as a logged-in user or to your specified return URL.

Properties:

- **signingKey**. The secret key used to sign the JWT.
- **issuer (optional)**. If specified, the application will ensure that the issuer included in the JWT matches the value specified here.
- **validateAudience (optional)**. If true, the audience property of the JWT is both required and verified. The default value is true. To disable, set to *false*. The audience value of the JWT is expected to be equal to the AuthBridge URL: `{Base URL}/managed/AuthBridge/`.

  Important: The supported signing algorithms are HMAC and RSA. RSA support requires Symphony 24.2 and later.

Groups

When a user logs on using federated authentication, the list of groups they are associated with is read from the collection of *GroupName* claims. For each External Group Account set up with a name that name exactly matches one of the groups from the claims, the user's logon session identifies a membership in that group.

For example, an administrator creates an External Group Account named Group 1. When a user logs on using federated authentication, the list of claims returned by the identity provider contains two claims corresponding to the `http://schemas.microsoft.com/ws/2008/06/identity/claims/role` claim type (the default claim type mapping for *GroupName*); *Group 1* and *Group 2*. Because an External Group Account named *Group 1* exists in your environment, the user is a member of that group for the duration of their logon session. There is no External Group Account named *Group 2*, so that claim is ignored.

Because it's possible to use multiple identity providers, Symphony offers the ability to restrict automatic group assignment to one or more specific providers, using the *Federated Authentication Providers* property of the External Group Account.

Federated Authentication Bridge

Federated authentication is accomplished through a series of redirections, primarily handled by the **Federated Authentication Bridge** (FAB) web application included in the Symphony infrastructure. This web application is an optional module installed as a subpath (e.g., virtual directory) named *AuthBridge* under the primary web application (BIWebsite).

Installation

The Authentication Bridge (*authbridge*) can be configured in your Kubernetes environment.

Configuration

When a user wants to log on using a specific authentication provider, you need to construct an Authentication URL that goes to the FAB in the following format:

```
{Base URL}/managed/AuthBridge/Auth/ExternalAuth?providerId={providerId}&returnUrl={return URL}
```

Where:

- `{Base URL}` is the base URL of the Symphony Managed Dashboard web application.
- `{providerId}` is the ID of the federated authentication provider specified in the manifest. If only one federated authentication provider has been defined, this can be omitted.

The following optional elements may be added to the query string of the Authentication URL:

- `{return URL}` – A relative URL to where the user should be redirected once authorization succeeds. The URL is relative to `{Base URL}`. If not specified, the user will be redirected to the home screen.
- `debug` – If specified with a value of `true`, an intermediate screen will be shown before the final redirection, containing information about the authentication operation (the claims sent from the identity provider, the property values extracted from those claims, and the result of attempting to create a logon session corresponding to the user).
- `deleteOtherSessions` – Specified with a value of `true` or `false`. If enabled, and the logon cannot succeed because the required seat is not available, the least-used session preventing the logon from succeeding will be terminated. If not specified, the `Delete Other Sessions On Log On` configuration setting determines the behavior.

- `explicitCultureName` - The culture to associate with the logon session (for example, `explicitCultureName=en-CA`). If not specified, the culture associated with the account or the default culture for the application will be used.

- `rememberMe` - If not specified or specified with a value of `true`, the session cookie corresponding to the user's logon session will be created with a long-term expiry. If specified with a value of `false`, the session cookie may be forgotten when the user's browser is closed.

Important: To avoid exposing potentially-sensitive claims data, disable the ability to set debug to `true` in production environments. Use the `Federated Authentication Debug Screen Allowed` configuration setting.

Automatic Log on Using Federated Authentication

Automatic log on using federated authentication can be achieved by pointing the `Custom Logon URL` configuration setting to the authentication URL. The return URL placeholder will be automatically set by the application.

For example:

```
https://symphony.example.com/managed/AuthBridge/Auth/ExternalAuth
```

Service Provider Metadata

SAML 2.0

When using the SAML 2.0 protocol, Service Provider (also known as Relying Party) metadata is available using a URL constructed as follows:

```
{Base URL}/managed/AuthBridge/Auth/FederationMetadata/{providerId}
```

For example:

```
https://symphony.example.com/managed/AuthBridge/Auth/FederationMetadata/MySamlProvider
```

If there is only one federated authentication provider specified in the manifest, the provider ID may be omitted.

Other Protocols

If the identity provider requires a URL to identify the Symphony application (may be referred to as "sign-on URL", "home page URL", "relying party URL", "SP entity ID" etc.), provide the URL to the Federated Authentication Bridge.

For example:

```
https://symphony.example.com/managed/AuthBridge/
```

Identity Provider-Specific Information

This section contains information to help in setting up federated authentication with Symphony for specific identity providers.

Okta SAML 2.0

To integrate with Okta, create a SAML 2.0 application integration including the following steps. For the sake of the example, we will assume that your Symphony installation is accessible via `https://symphony.example.com`.

1. Create a new SAML 2.0 Application in Okta.
2. In the **App visibility** section, check the boxes so that the application is not displayed to users (i.e., a chiclet will not be shown to users). The application being set up here will not work as a clickable chicklet, so it's best to prevent it from being displayed.
3. In the **Single sign on URL** field, enter a temporary URL, such as `http://www.example.com`. This will be updated later.
4. In the **Audience URI (SP Entity ID)** field, enter the URL to the Federated Authentication Bridge, such as `https://symphony.example.com/managed/AuthBridge/`.
5. On the next page, find the link to **Identity Provider metadata** and copy the URL. It will be something like `https://example.okta.com/app/asdfsadfiuoh00h7/sso/saml/metadata`. You may be able to find this from the Actions menu of the records in the **SAML Signing Certificates** section of the **Sign On** tab.
6. In Symphony, create an entry for your Okta provider in the `Federation Manifest` configuration setting. Use the URL from the previous step as the value for the `idpMetadataLocation` property.
7. To obtain the correct Single Sign On URL to use in Okta, you will need to examine the Service Provider metadata from Symphony. See above for instructions on how to do this. Once you have the XML, extract the value of the ACS URL for the `HTTP-POST` binding. It will be something like `https://symphony.example.com/managed/AuthBridge/AuthServices-Saml2-MyProvider/Acs`.
8. In Okta, go back and edit your SAML 2.0 application. Update the **Single sign on URL** to the value you extracted in the previous step.

Once the above steps are completed, federated authentication should be working correctly with your Okta application. You should see a new button on the Logon page that will initiate the authentication flow. However, pay attention to the following additional considerations:

- If you want to bypass the Logon page and have your users automatically get signed in, you will still need to set the `Custom Logon URL` configuration setting in Symphony (see above).
- If you want your users to be able to access your installation from an Okta chiclet, you will need to set up a new Bookmark Application in Okta, which will redirect your users to the base URL of your Symphony installation (e.g., `https://symphony.example.com/`).

Troubleshooting

If federated authentication does not succeed, the following tips may be useful for troubleshooting:

- Check the application log. Often this will contain details corresponding to a failed federated authentication attempt.
- Take advantage of the **debug** option in the query string of the authentication URL, in order to see detailed information about the authentication operation. For example: `https://symphony.example.com/AuthBridge/Auth/ExternalAuth?providerId=MyProvider&debug=true`.
- Check any logs on the identity provider.
- Check the Console and Network tabs of the browser's Developer Tools window for errors which could be related to the federated authentication operation.

Diagnostics

It's also possible to access application diagnostics for the federated authentication bridge web application similar to those you can access from the About page for the main Symphony web application to view various details about the running process.

First, find and copy your **Logon Session ID** when you are logged on as an administrator from the About page.

Next, navigate to the following URL, filling in the missing `sessionId` portion:

```
https://symphony.example.com/managed/AuthBridge/Home/DiagnosticsFile?mode=view&sessionId=<sessionId>
```

To download the diagnostics as a file rather than viewing them in the browser, remove the portion *mode=view&* of the URL.

For more information, see:

- Symphony Single Sign On
- Configuration Settings

- Add New Users

Advanced Group Management

This applies to: *Managed Dashboards, Managed Reports*

Use the Groups work area to perform many of the basic tasks needed to create and edit groups. This versatile work area is also useful for listing Symphony user groups, adding and removing members to and from a group. If needed, use this page to navigate to a module to perform more tasks specific to that module.

Groups Work Area Tasks

View a list of groups in Symphony

1. Navigate to the Groups work area by selecting the **Groups** option in the main menu.
2. A list of all Symphony groups is shown.

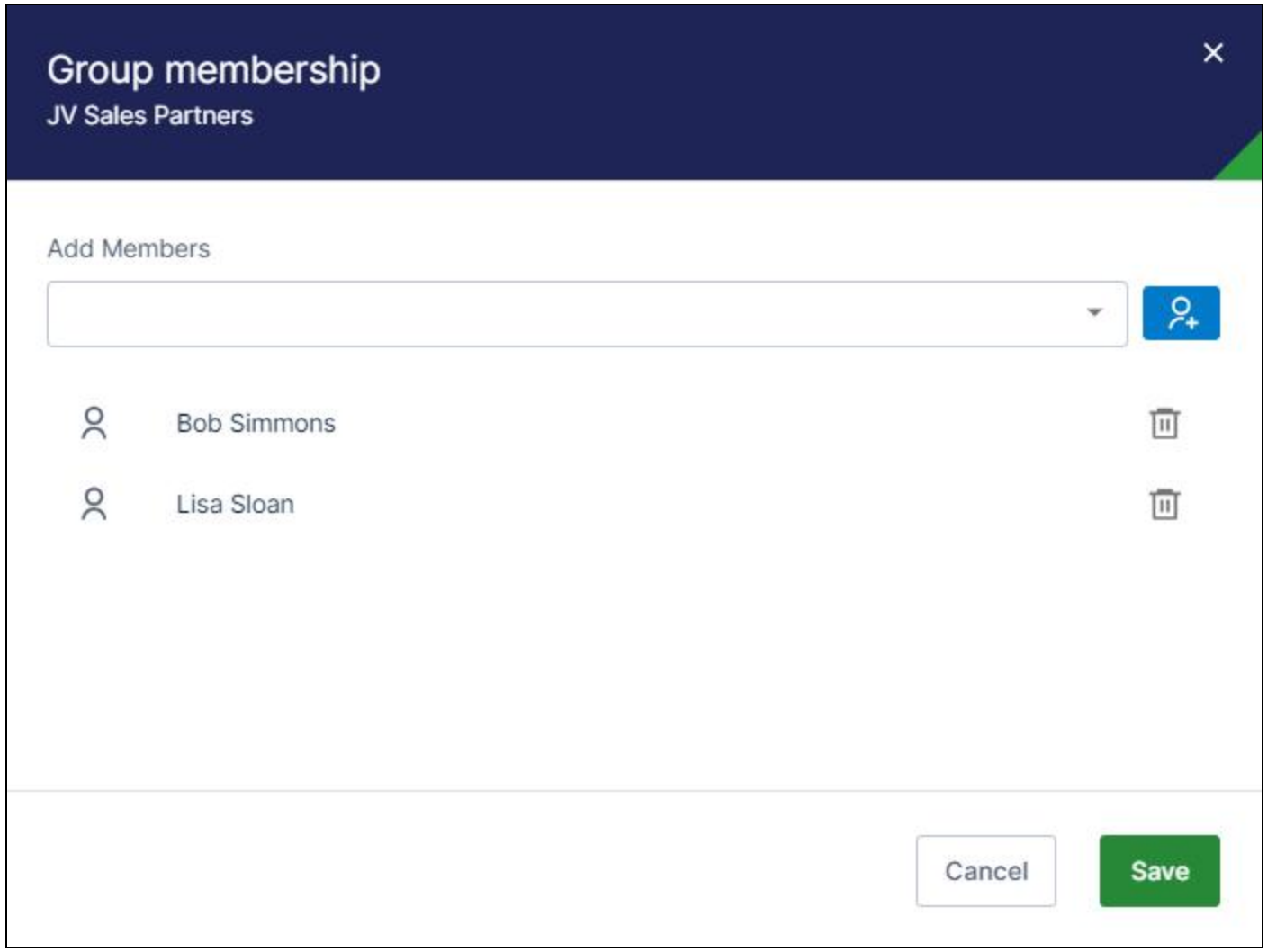
i. If you're a system admin, all groups are listed, except for two specific Visual Data Discovery groups, Content Distributors and Supervisors.

ii. If you're a tenant admin, all groups in the tenant you are working in are listed.

3. Add, edit, or manage group membership in this work area, then select another menu option to navigate away from this work area.

View members of and add members to a group

1. Log in as a system admin or tenant admin. If you are logged in as a tenant admin, verify you're in or switch to the appropriate tenant.
2. From the main menu, select **Groups**. The Groups work area opens.
3. Scroll to find an existing group, or use the Search field to find a group.
4. Select Members. A Group membership work area opens, listing the current group members.

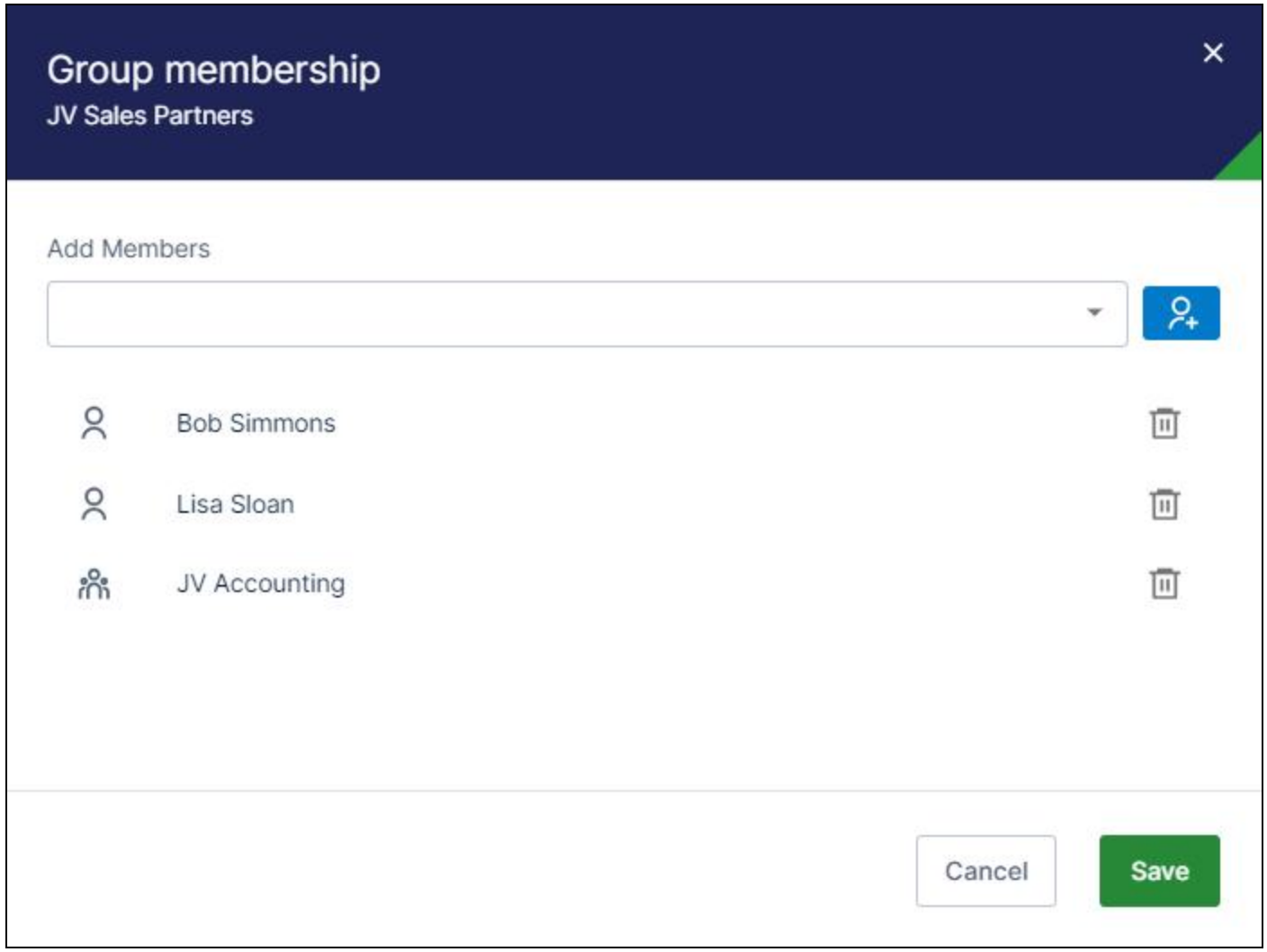


5. Select eligible users from the **Add Members** drop down, then select the add members icon () to make them members of this group.
6. **Save** your changes. A success message appears, and you are returned to the Groups work area.

Note: Select the delete icon next to any group member to remove them from the group, then **Save** your changes.

Add a group to a group

1. Log in as a system admin or tenant admin. If you are logged in as a tenant admin, verify you're in or switch to the appropriate tenant.
2. From the main menu, select **Groups**. The Groups work area opens.
3. Scroll to find an existing group, or use the Search field to find a group.
4. Select Members. A Group membership work area opens, listing the current group members.



5. Select eligible groups from the **Add Members** drop down, then select the add members icon ( ) to make the group a member of this group.
6. **Save** your changes. A success message appears, and you are returned to the Groups work area.

Note: Select the delete icon next to any group to remove them from the group, then **Save** your changes.

Edit in Managed Dashboards

Some infrequent tasks are managed by administrators directly in the Managed dashboards module. Navigate to the appropriate work area from the Groups page.

Advanced Group Settings

If you need to define settings specific to a group, you can do so by editing the group in Managed dashboards. These tasks may include:

- **Allowed IP Addresses** - An IP address or range that the group members must log on from.
- **Culture** - The default culture for this group. Must be a valid IETF language tag such as en or *en-US*.
- **Time Zone** – The default time zone for this group.
- **Minimum Floating Seat Privilege** - This seat type or higher will be assigned to all group members that use floating seats (see the Seat Mode setting in Accounts) even if their own Seat Type is set lower. Choose between *Standard user* or *Power user* license seat types, since *Developer seats* are always reserved.
- **Application Privileges** - Allow or deny access to specific functionality or UI elements.
- **Default View** - Select a default view for all the members of the group. This setting will override the regular homepage, but can still be overridden by individual default view settings.
- **ID** - View the group ID in the group details pane. You can search for the group in administrative work areas by this ID.
- **Custom Attributes** - assign custom attributes to a group.

Define advanced group settings and permissions

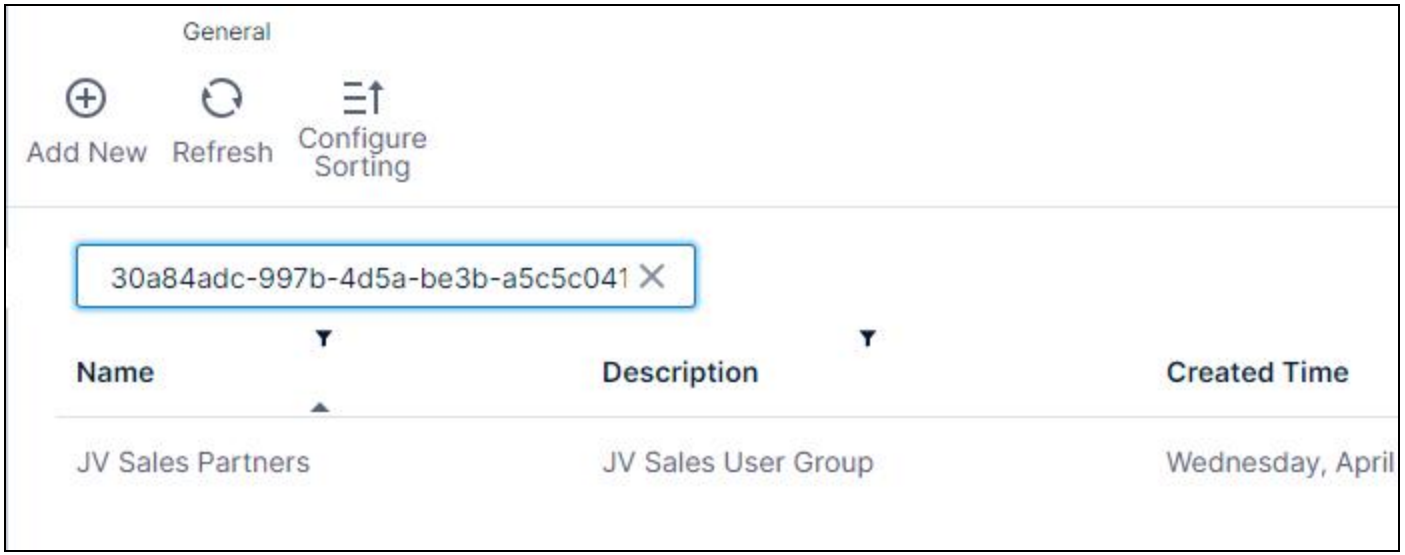
1. Log in as a system admin or tenant admin. If you are logged in as a tenant admin, verify you're in or switch to the appropriate tenant.
2. Select **Groups** from the main menu. The Groups work area opens. Scroll to find an existing groups, or use the Search field to find a group.
3. Select **Edit group** from the **Actions** menu for the group you want to update. An Edit group pop up dialog opens
4. Select the actions menu button, then **Edit in Managed Dashboards**.
5. A list of groups opens. Search for the group, or scroll to find the group you want to edit.

6. Select a group, then **Edit** from the **Contextual** menu. The group details work area for this group opens.

7. Make changes to the available fields in this group, then select **Save** to save your group changes.

Search for a group by ID

Every group has an ID (a GUID value). If you only know the ID of a specific group, you can quickly search for the corresponding group in the *admin* screen by pasting the ID in the *Search* box.



Health Check

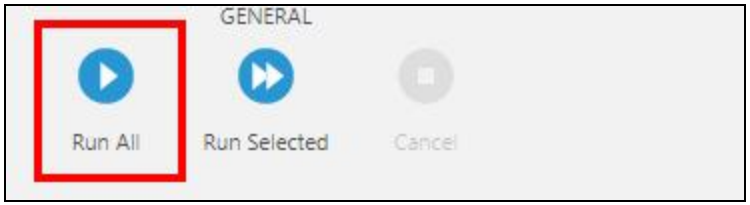
This applies to: *Managed Dashboards, Managed Reports*

Administrators can run health checks to identify any potential issues with their Symphony instance, and apply fixes when available.

Under the **System Health** category in Administration, click on **Health Check**.

Admin Options

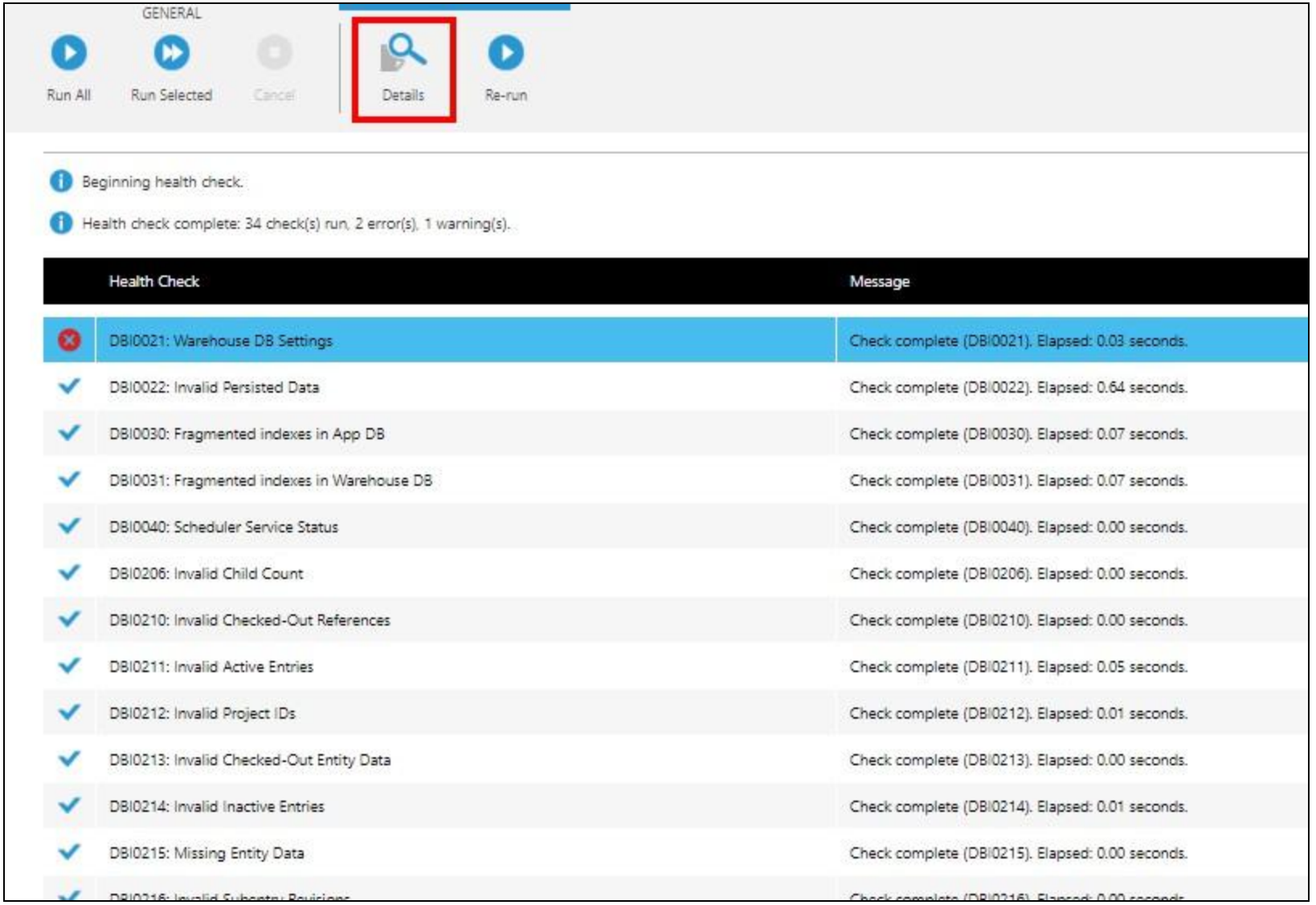
Click **Run All** on the toolbar to run all standard health checks that can apply in general to your instance.



To choose specific health checks or to choose from the complete list of those available, click **Run Selected** instead.

Fixing Issues

After running the health checks, view the result, which will display an icon to the left if any potential problems were found. Select the health check and then click the **Details** icon on the toolbar to get more information:



The details dialog will give you more information on the error/issue:

If an automatic fix is available, you can click the **Apply fix** button.

List of Available Health Checks

ID	Name	Description
DBI0010	Application DB Connectivity	Ensures that the application can connect to the application database.
DBI0011	Warehouse DB Connectivity	Ensures that the application can connect to the warehouse database.
DBI0012	App DB Schema	Ensures that the tables in the application database are valid according to the expected schema.
DBI0020	Application DB Settings	Ensures that various settings related to the application database are correct.
DBI0021	Warehouse DB Settings	Ensures that various settings related to the warehouse database are correct.
DBI0022	Invalid Persisted Data	Identifies data persisted to a database which is in an invalid format.
DBI0030	Fragmented Indexes in Application DB	Detects overly fragmented indexes in the application database.
DBI0031	Fragmented Indexes in Warehouse DB	Detects overly fragmented indexes in the warehouse database.
DBI0040	Scheduler Service Status	Checks whether the Scheduler service is running and can connect to the Symphony web application.

ID	Name	Description
DBI0045	Internal Application URL Status	Checks whether the internal application URL set in the configuration settings is accessible.
DBI0060	Application Folders Write Permission	Checks that the web server identity has Write access to application folders.
DBI0206	Invalid Child Count	Finds the system entries with invalid values in the ChildCount column.
DBI0210	Invalid Checked-Out References	Finds references from checked-out entries where the corresponding entity is not actually checked-out.
DBI0211	Invalid Active Entries	Finds transient subentries which are no longer referenced by the latest revision of their parent entity, and marks them as inactive.
DBI0212	Invalid Project IDs	Finds entries whose project ID does not match the ID of the project under which the entry resides.
DBI0213	Invalid Checked-Out Entity Data	Finds checked-out data for entities which are not actually checked-out.
DBI0214	Invalid Inactive Entries	Finds inactive subentries which should be active.
DBI0215	Missing Entity Data	Finds entities which are missing their underlying data.
DBI0216	Invalid Subentry Revisions	Finds subentries whose current revision doesn't match that of their corresponding primary entry.
DBI0217	Orphaned References	Finds references from entity revisions which do not exist.
DBI0218	Incorrect Privilege Assignee Kind	Finds privilege assignments where the Everyone group has the incorrect assignee kind.
DBI0219	Missing Referenced Entities	Finds references to non-existing entities.
DBI0220	Duplicate Tenant Project Folders	Finds tenants with more than a single Tenant Project Folder.
DBI0221	Circular References	Finds entities which directly or indirectly reference themselves.
DBI0222	Orphaned Tenant Overrides	Finds tenant overrides corresponding to items which do not exist.
DBI0223	Invalid Project Temp Folder Privileges	Finds project-level temporary folders which don't have correct privilege assignments.
DBI0224	Invalid Project Privilege Inheritance	Finds projects which incorrectly inherit privileges.
DBI0225	Invalid User Project Tenants	Finds user projects and project items which have tenants different from the account's tenant.
DBI0300	Orphaned Account, Group and Tenant Data	Finds data corresponding to accounts, groups, and tenants which no longer exist.
DBI0305	License Seat Usage	Detects when more seats are being used than what is permitted by the licenses.
DBI0310	Empty User Projects	Finds and removes empty non-developer user projects.
DBI0315	Orphaned Notification Jobs	Finds and removes notification jobs without related notifications.
DBI0400	Log Filter Settings	Warns if the current log filter setting may be overly verbose.

ID	Name	Description
DBI2000	Unused Warehouse Tables	Finds warehouse tables that are not in use.
DBI2010	Invalid Default Time Dimensions	Finds projects whose specified default time dimension couldn't be found in the system.
DBI2015	Transient and Inactive Native Structures	Finds native structures (tables, views, etc.) which are incorrectly marked as transient or inactive.
DBI2020	Duplicate Storage Jobs	Finds native structures or data cubes which have more than one active associated warehouse or in-memory storage job.
DBI2025	Third-Party Drivers for Data Connectors	Ensures that third-party drivers are installed for all data connectors.
DBI2030	Notifications with Invalid Metric Set References	Finds notifications referencing metric sets which no longer exist or metric sets to which the associated account is no longer authorized. This check will remove the request if the referenced metric set no longer exists and will remove the entire notification if all metric sets no longer exist. Metric set privileges will not be modified.
DBI2031	Single-Use Notifications That Didn't Get Deleted	Finds and deletes notifications that were created internally for a single use but weren't deleted, for example because of an error or shutdown.
DBI2035	Missing Warehouse Tables	Finds data cubes that are missing their warehoused data.
DBI2050	Synchronize Account Services Objects with Visual Data Discovery	Synchronizes tenants, groups and users between Managed Dashboards and Reports and Visual Data Discovery.
**DBI2040	Duplicate Relationships (omitted by default)	Finds duplicate relationship data.

** Indicates that the health check is omitted by default when using the **Run All** health checks option.

Scheduled Health Checks

In Symphony, there is a built-in *Health* checks maintenance job that you can enable and schedule.

The configuration settings in the *Health Check* category let you set up which issues to check for, the level of severity that should trigger an email to the configured *Maintainer Email* address (in the *Email* category), and whether to apply fixes automatically when possible.

For more information, see:

- Monitoring System Health
- Manage Users in Symphony
- Advanced Group Management
- Perform a Health Check Using the Command Line

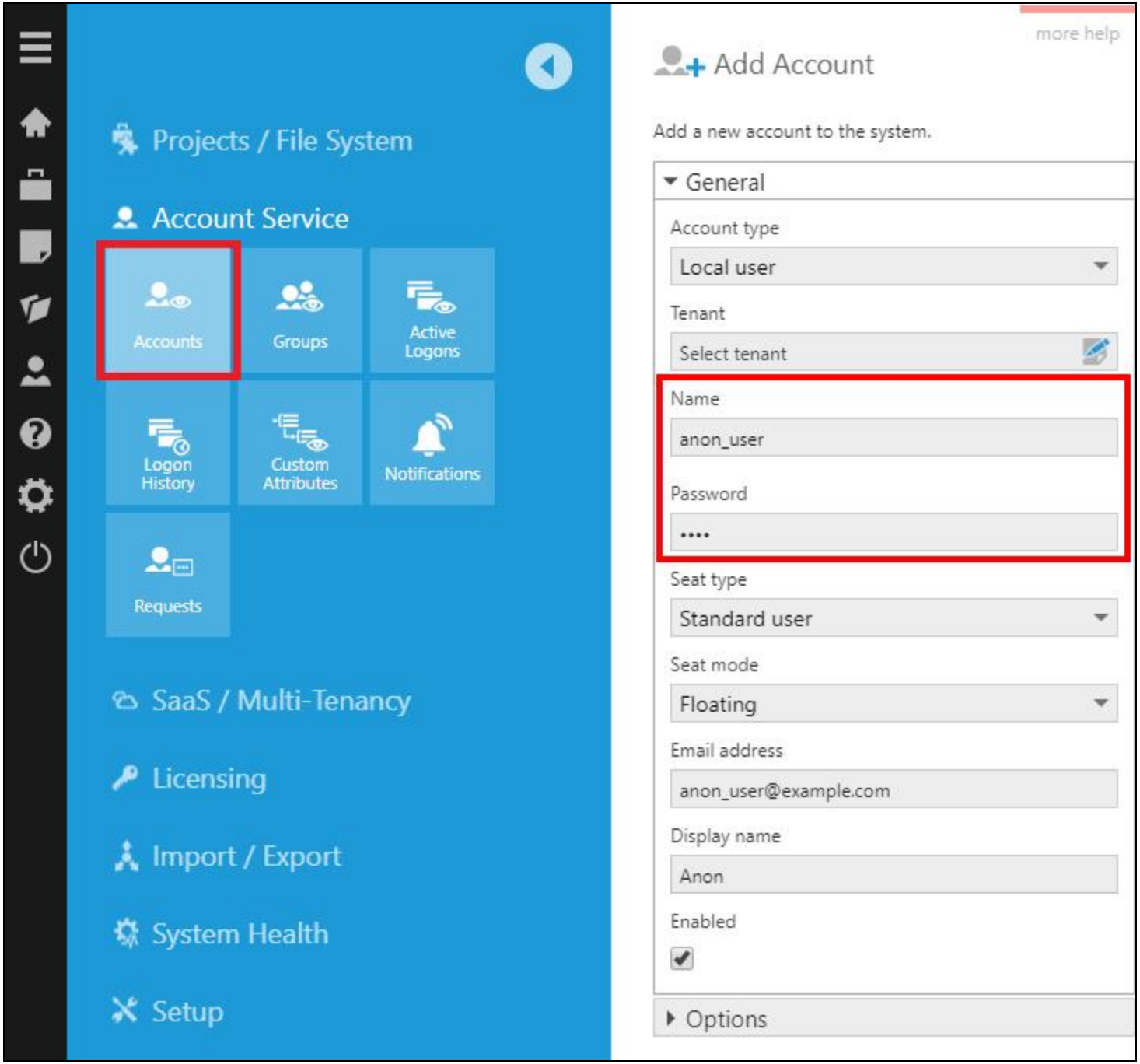
How To Enable Anonymous Log On

This applies to: *Managed Dashboards, Managed Reports*

This article shows you how to set up Symphony for anonymous log on to facilitate implementation of a public dashboard/reporting site or kiosk.

Create an Anonymous User

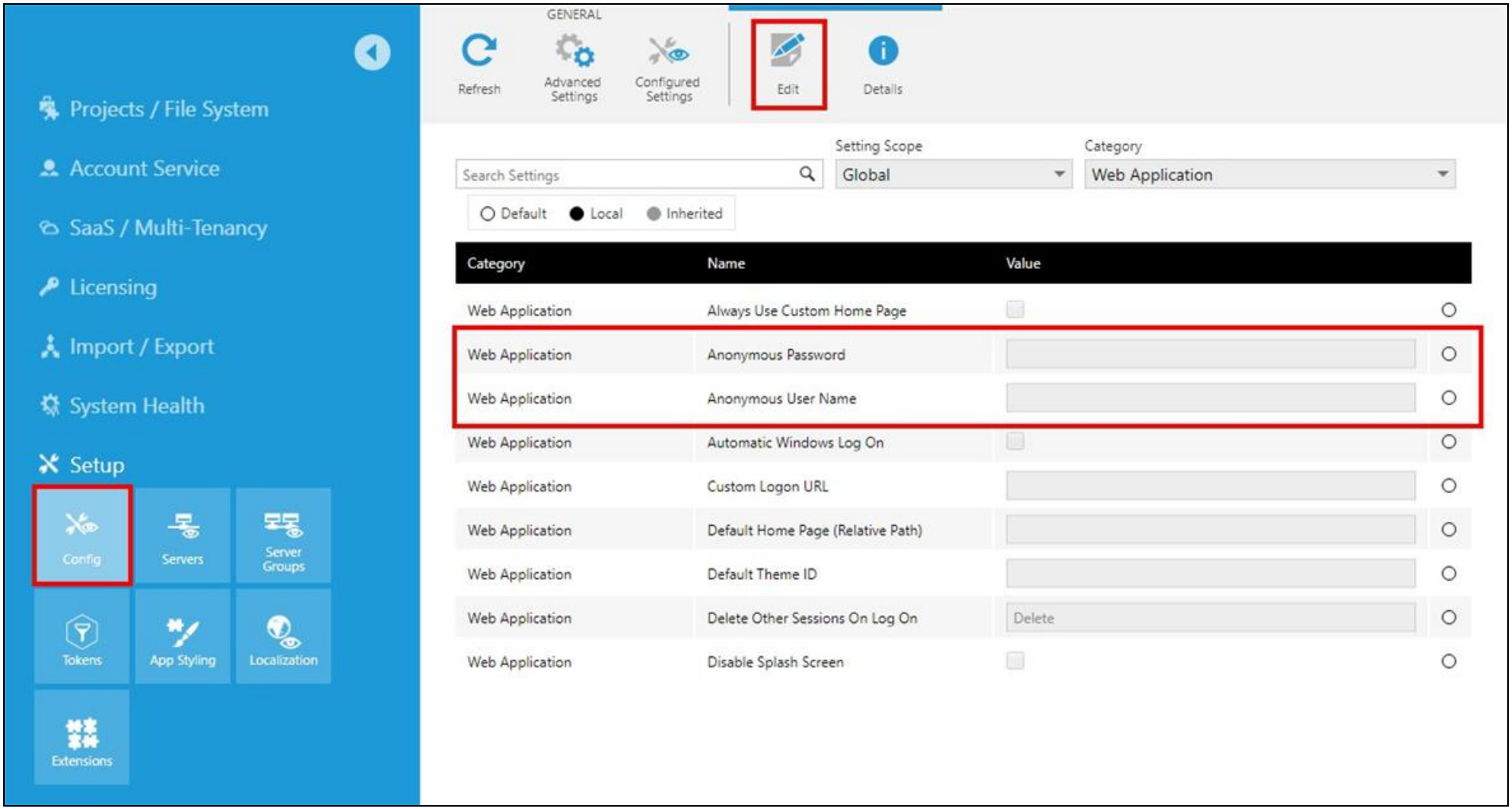
Log on to Symphony as an administrator, then create a new user to be used specifically for anonymous log on. Take note of the account name and password.


Projects / File System
Account Service
Accounts
Groups
Active Logons
Logon History
Custom Attributes
Notifications
Requests
SaaS / Multi-Tenancy
Licensing
Import / Export
System Health
Setup
more help
Add Account
Add a new account to the system.
General
Account type
Local user
Tenant
Select tenant
Name
anon_user
Password
••••
Seat type
Standard user
Seat mode
Floating
Email address
anon_user@example.com
Display name
Anon
Enabled
Options

Modify Configuration Settings

In the Administration area, expand the **Setup** section and click **Config**.

In the configuration settings that are listed, set the **Category** to *Web Application*.



Edit the following configuration settings:

- Anonymous User Name - Set this to the account name that you created in the previous step
- Anonymous Password - Set this to the password of the anonymous user account

Anonymous log on will be enabled automatically once both settings are configured.

Test Anonymous Log On

When anonymous log on is enabled, a user navigating to your Symphony website (e.g., `http://symphony.example.com:8000/`) will be automatically logged on. They will see the home screen, for example, instead of seeing the Log On screen.

An administrator may still need to log on to Symphony for admin purposes. In this case, simply navigate to the LogOn page directly to see the normal Log On screen. For example, navigate to `http://symphony.example.com:8000/LogOn/` and log on as usual.

When a user is logged on anonymously and the session expires, the page will be reloaded and they will be logged back on automatically.

When a non-anonymous user is logged on and the session expires, the user will be returned to the Log On screen and a *Session has expired* message will be shown.

For more information, see:

- Configuration Settings
- Log Into the ComposerSymphony UI

How to Recycle the Application Pool

This applies to: *Managed Dashboards, Managed Reports*

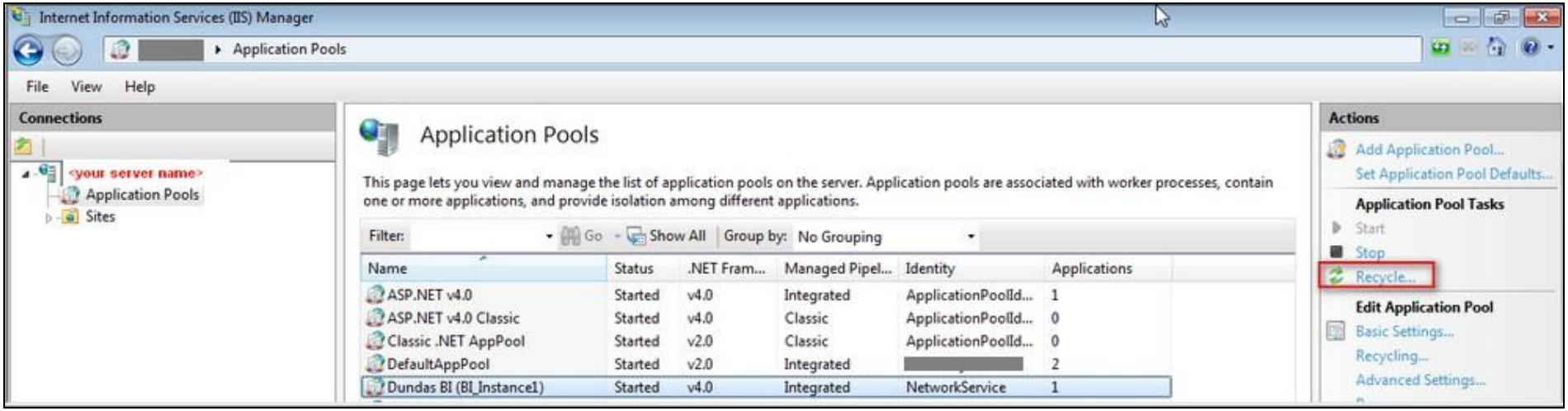
This article shows you how to recycle the Symphony application pool in the IIS web server when installed on Windows. After performing certain installation and/or configuration tasks, it is necessary to recycle the application pool in order for the changes to take effect, or for Symphony to work properly. These include:

- Configuring the configuration file.
- Configuring the Oracle data connector's `tnsnames.ora` file.
- Restoring the Symphony application database from a SQL Server database backup - this is necessary in order to clear any old cryptography keys which may be stored in memory.

Recycle the Application Pool

Though using *iisreset* is also possible, the best way to restart the Symphony website is to recycle the application pool so that other applications running on the server are not affected. To do this:

1. Open the IIS Manager. You can do this in the start menu by typing to search for *IIS*, or typing to run *inetmgr*.
2. In the IIS management console, select **Application Pools** under your server name.
3. Select your Symphony application pool.
4. Under Actions on the right, click **Recycle...**



For more information, see Symphony Managed Dashboards and Reports Config File.

How to Reset the Admin Password

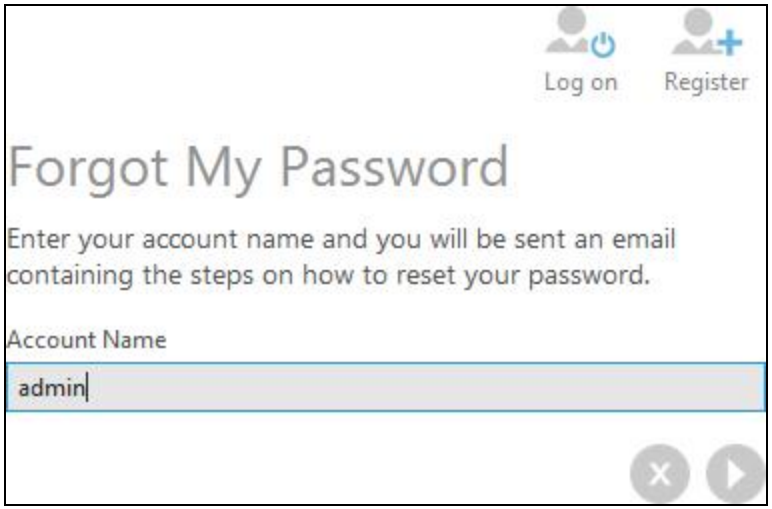
This applies to: *Managed Dashboards, Managed Reports*

This article shows a couple of ways to reset the Symphony administrator password.

Use the Forgot Password Link

Go to the Symphony Log On screen and click the **Forgot Password** link.

Under *Forgot My Password*, type admin as your **Account Name** and click **Submit**.



The admin user will receive a Reset Password email containing a link for changing the password.

Note: For installations of Symphony, the email settings need to be configured correctly for this option to work.

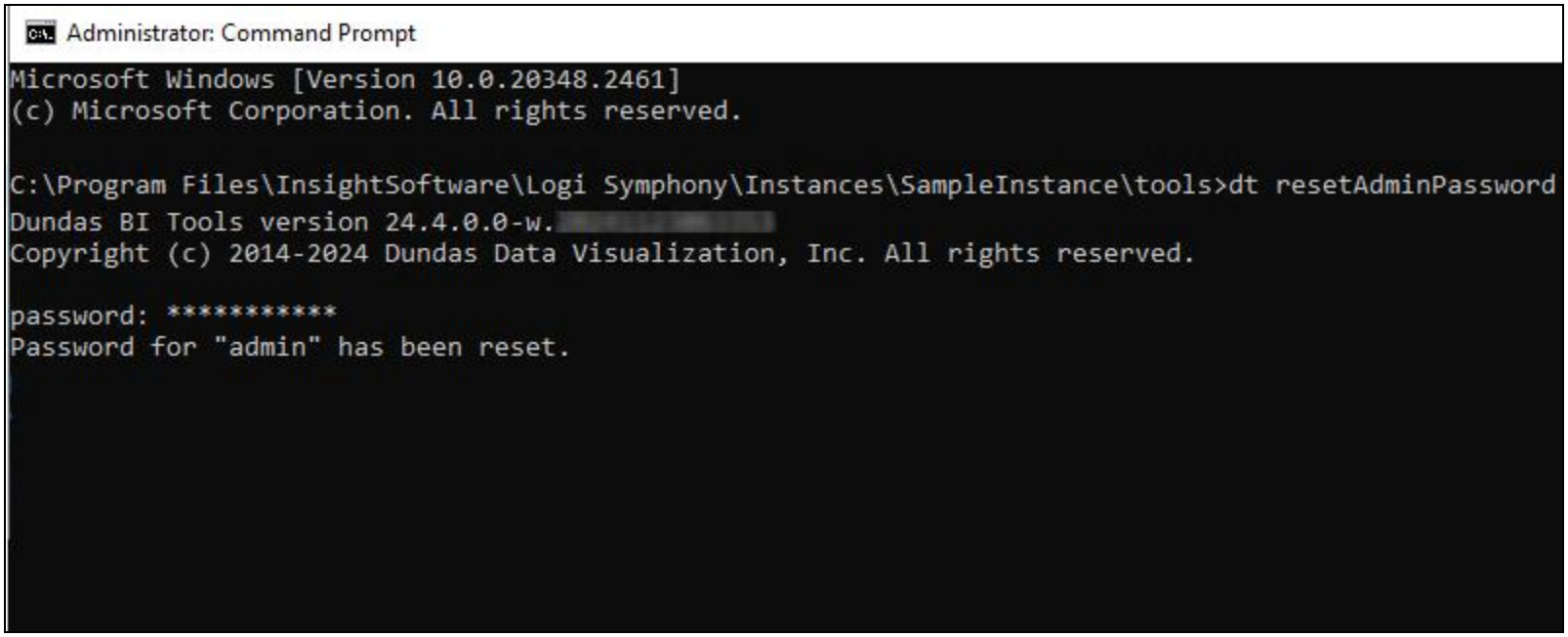
Use the dt Command Line Tool

If Symphony was installed, log on to its server computer and use a command prompt or terminal to navigate to the *tools* folder containing the *dt* tool. For details, see Using the dt Command Line Tool.

Use the *resetAdminPassword* command. For example:

```
dt resetAdminPassword
```

When prompted, enter a new password and press Enter:



Note: As an alternative, you can provide the password as an argument in the initial command. For example: *dt resetAdminPassword /password:1234*.

For more information, see:

- Log Into the ComposerSymphony UI
- Configuration Settings
- Using the dt Command Line Tool

Import and Export a Project

This applies to: *Managed Dashboards, Managed Reports*

This article shows you how to use the export and import options available to administrators for Symphony projects, their files such as data cubes and dashboards, and other files and objects.

Various items can all be exported from a Symphony instance and stored in an *export* file (or **DBIE** file). This export file can then be imported back into the same or another instance of Symphony.

For example, you can use this functionality to migrate a project from a development or staging instance of Symphony to a production instance. Importing content that already exists overwrites it with the version contained in the export file.

> **Important:** Export/DBIE files are compressed but not encrypted. These files may contain credentials from data connector connection strings. If you require encryption you must use a third-party tool for this.

Export or Import

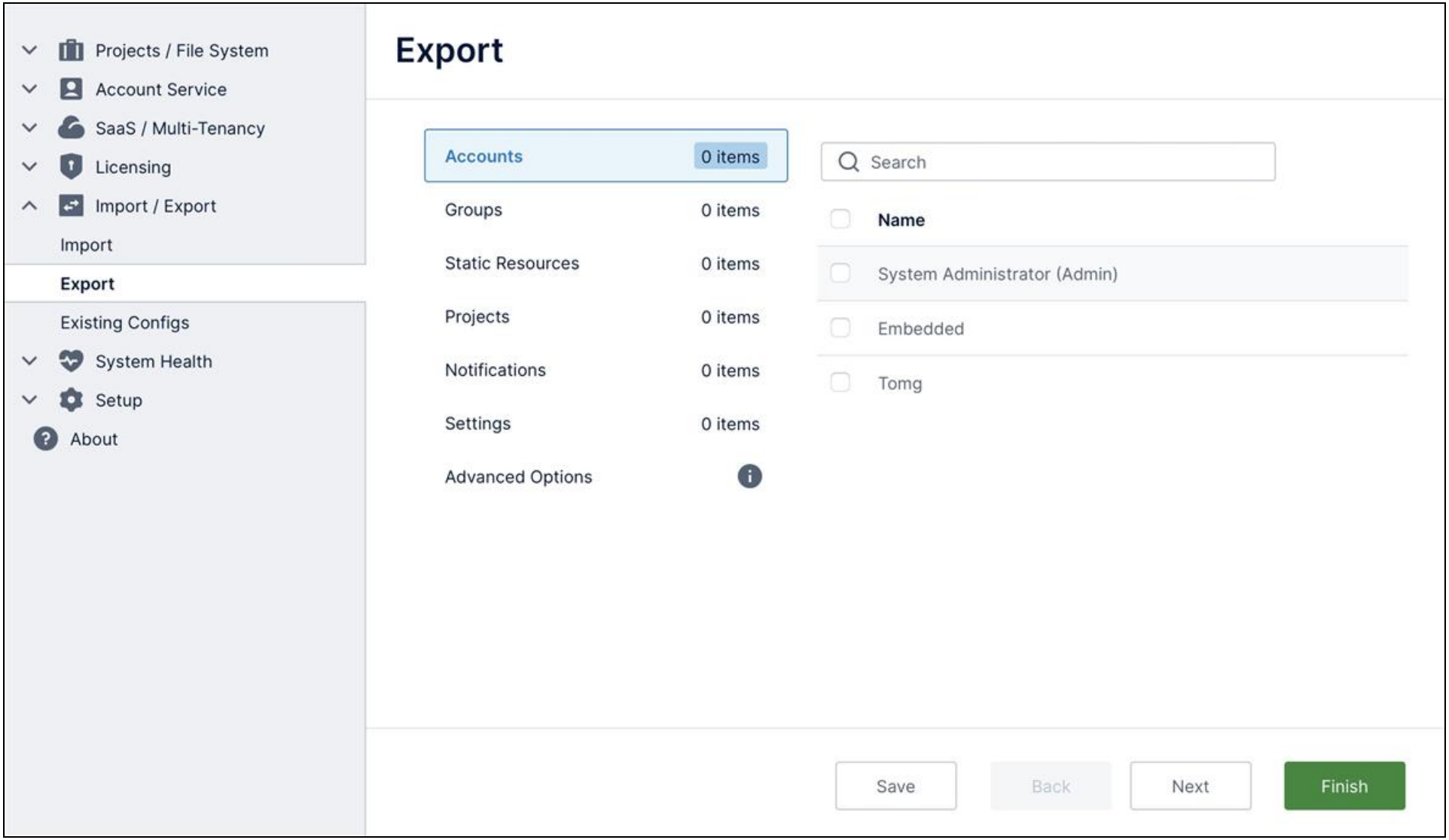
In the administration area, expand **Import / Export** along the left, and then click either **Export** or **Import**.

If you are importing an existing DBIE file, click **Choose File** to browse to it, or you can drag and drop the file.

Next, step through each type of item:

- *Tenants* – Available only on multi-tenant instances.
- *Accounts* – Users & groups.
- *Groups* – Groups.
- *Static Resources* – Custom files used when white labeling or customizing the application.
- *Projects* – Projects and the files contained in its folders, including data connectors, dashboards, styles & themes, etc.
- *Notifications* – Notifications created by a user for a view (this account and view must exist when importing).

- *Settings* – Application configuration settings that you want to save, load, or migrate.
- *Advanced Options* – Export or import additional kinds of items, or access important options related to the items you selected.



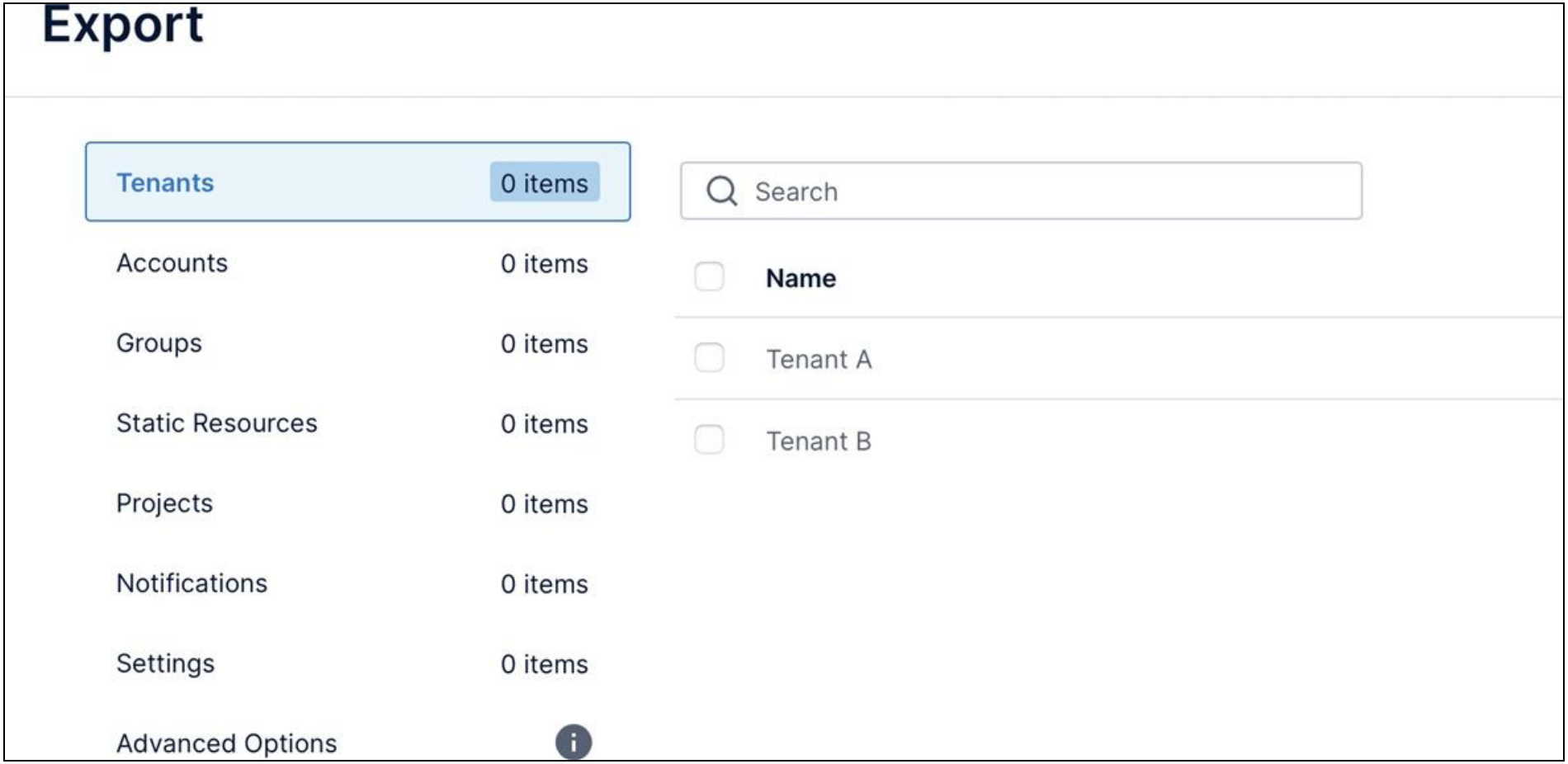
Some steps are detailed further in the following sections.

Each step is optional and you can click **Next** without selecting items if you aren't interested in them. When importing, some options will not be available if they weren't included when exporting.

Selecting Tenant Items

The *Tenants* step is only available on instances containing tenants, or if the export file contains tenants when importing.

Select tenants in this step to export or import the tenants themselves, or to be able to include accounts, groups, projects, files, and other items that belong to these tenants in later steps.



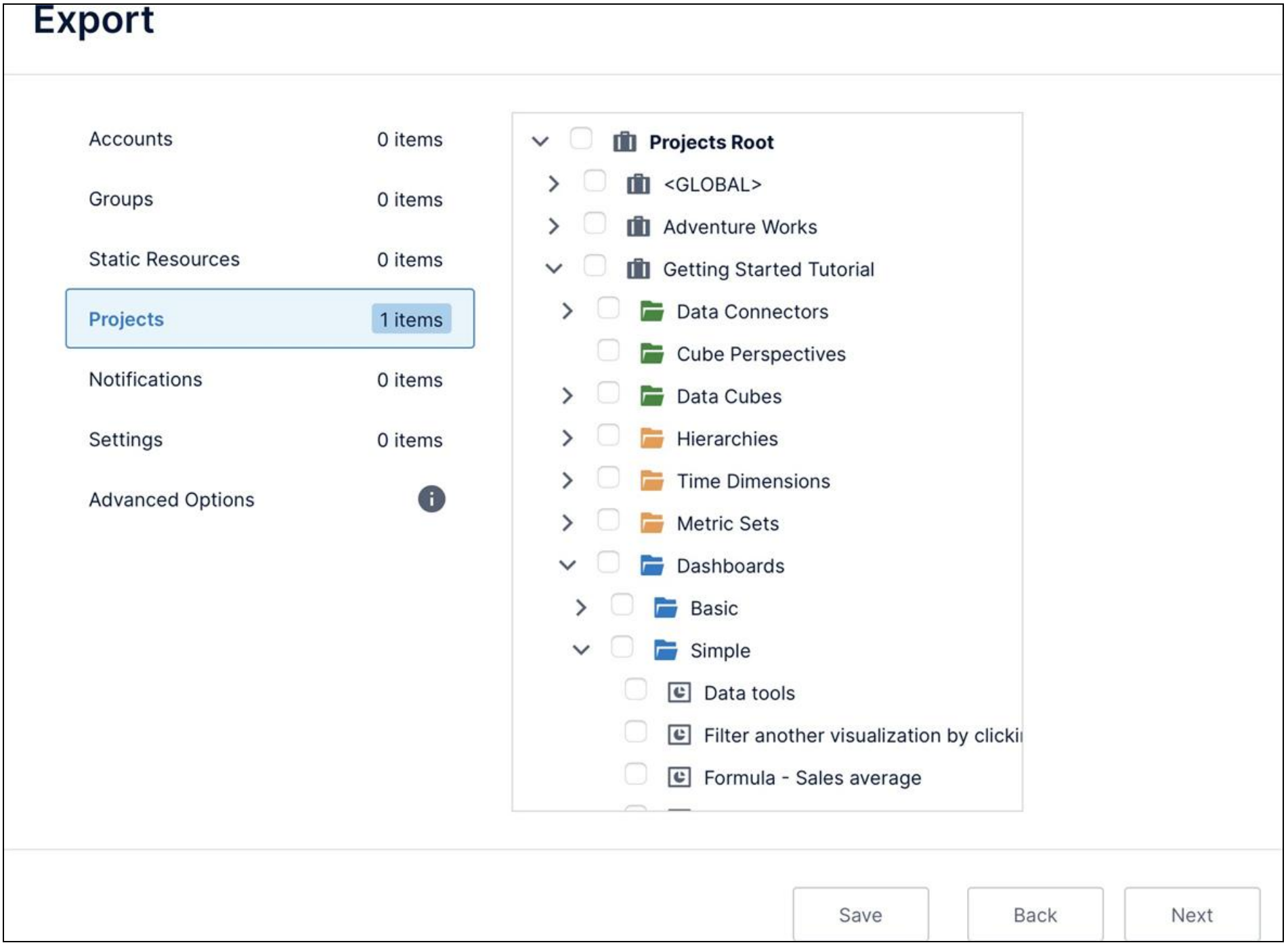
In the steps that follow, tenant items may be identified separately, or you may need to select the tenant from a drop-down before being able to select its items.

You can also use the advanced option *All Tenants* when exporting to be able to use other options such as *All Accounts* for items like tenants.

Selecting Projects and Files

Exporting and importing is often used to save or transfer projects or some of their files.

In the *Projects* step, you can click to expand each item and use the check boxes to select entire projects, or only specific folders or files within them, such as specific data connectors, dashboards and reports, etc.


Export
Accounts 0 items
Groups 0 items
Static Resources 0 items
Projects 1 items
Notifications 0 items
Settings 0 items
Advanced Options
Projects Root
<GLOBAL>
Adventure Works
Getting Started Tutorial
Data Connectors
Cube Perspectives
Data Cubes
Hierarchies
Time Dimensions
Metric Sets
Dashboards
Basic
Simple
Data tools
Filter another visualization by clicki
Formula - Sales average
Save
Back
Next

Note: Files need to be checked in to export them unless the advanced option *Checked Out Versions* is enabled.

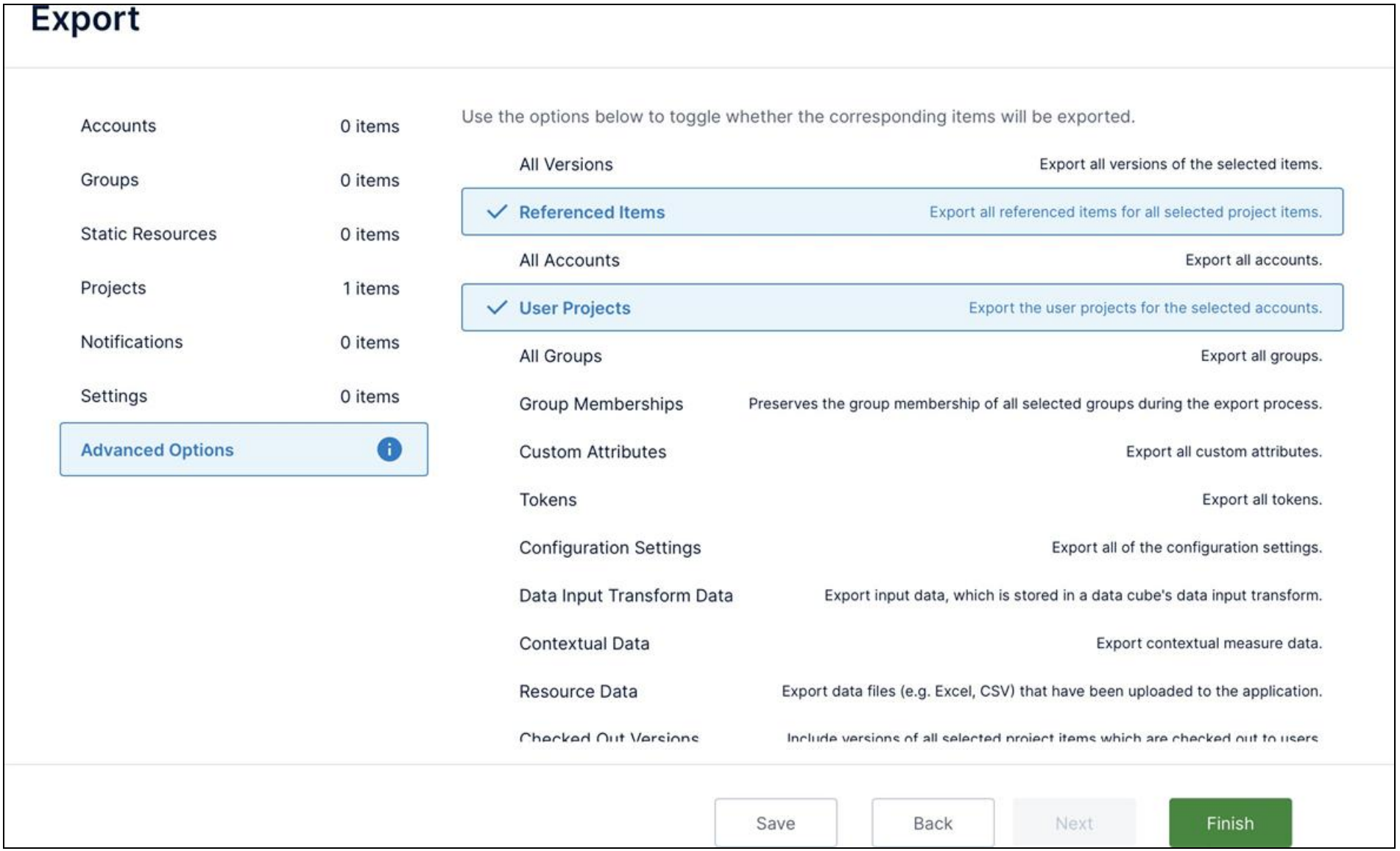
When selecting specific items, any other items they rely on will automatically be included by default, such as metric sets, data cubes, and data connectors, according to the advanced option to include *Referenced Items* that is enabled. When importing, these referenced files must be included in the export file or already exist to be able to import the files that depend on them.

Personal projects (named 'My Project') belonging to users are not listed in this step. To export these projects, select their *Accounts* instead, and ensure the advanced option is enabled to *Include User Projects*.

When importing, your Symphony instance may already contain some of the same content as the DBIE file if it was exported from there originally or imported earlier. In these cases, items will be replaced by the version in the DBIE file. (Different content that was created with the same name and location is *not* replaced because it will have a different ID. The imported content may instead be renamed to avoid confusion.)

Set Advanced Options

In this last step before exporting or importing begins, there are several advanced options that can be toggled on or off. It is possible to click **Finish** before you get to this step if you know you want to use the existing selections.



Some important advanced options are described below.

All Versions

Select *All Versions* if you want to include the entire revision history of each file, including the ability to rollback to previous revisions, otherwise only the latest checked-in revision will be included.

Note: When using this option and importing a data connector that already exists, the existing data connector's settings will be overwritten.

Referenced Items

Leave the *Referenced Items* option enabled to automatically include all referenced items that the files you selected from projects depend on. This includes items such as custom attributes and tokens that are referenced by selected data cubes or metric sets, even when not explicitly selecting to include any other items. Referenced items do not include input data or data resources such as uploaded Excel files, as described in the next section.

Important: You may not be able to import or use files later if referenced files are missing, and they may not function correctly without other referenced items such as tokens. You can leave out referenced items when exporting if they will already exist when importing.

Data, Corrections, and Notes

The following advanced options involve data and user input that may be considered sensitive or to be handled with caution, and are not included by default when exporting or importing:

- *Data Connector Settings* – (Import only) Connection settings in data connectors. The *All Versions* option will have the same effect. For tenant overrides, deselect this option to prevent overwriting existing overrides.
- *Data Input Transform Data* – Data stored in a data cube's Data Input transform, whether entered directly into the transform or as a data source for a metric set, or input through data input interactions on a dashboard or other view.
- *Contextual Data* – Data entered into a contextual measure in a metric set.
- *Resource Data* – Uploaded Excel, CSV, or other data files used for a data connector.
- *User Input Entries* – Notes added to data from selected or existing data cubes, and measure corrections (data annotations) for selected or existing metric sets.

It can be important to include this data when exporting, however you should use caution when importing as existing data will be overwritten for associated files that already existed in that Symphony instance.

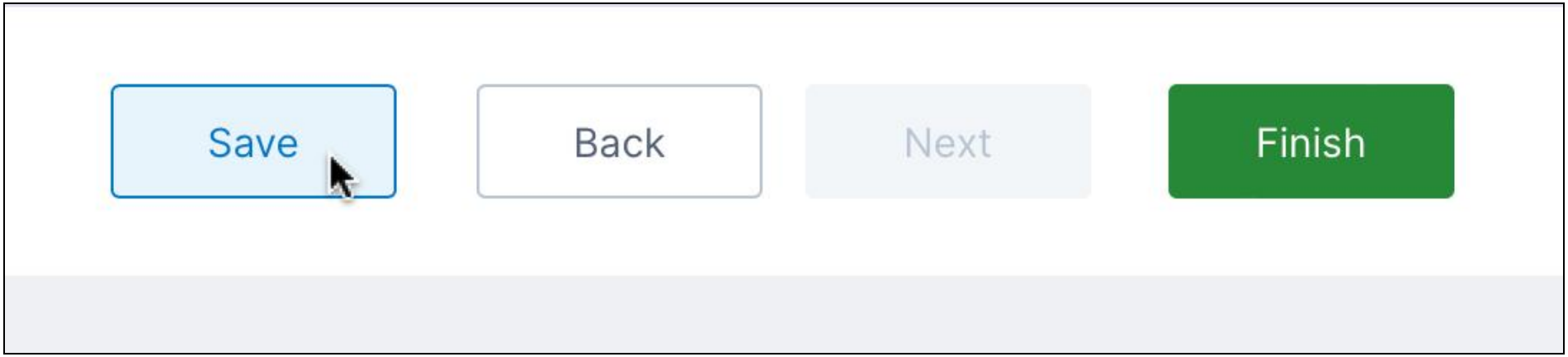
Publish Histories

If you use the Publish feature for publishing files from one project to another in a single Symphony instance, a relationship is created between the corresponding files to help when re-publishing the same content again later.

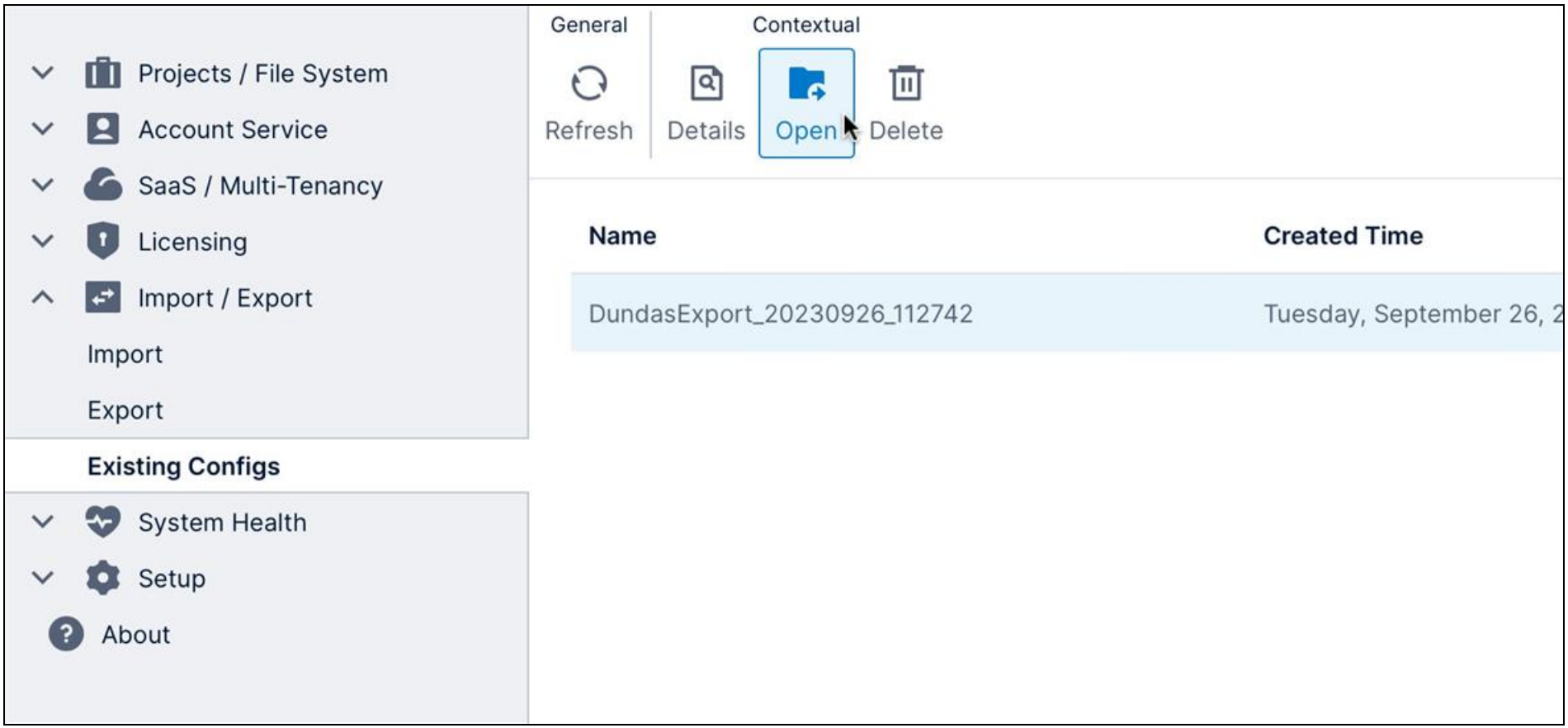
You can select to include the *Publish Histories* of selected project items to maintain these relationships when publishing again in the future.

Save Configuration

When exporting, you can click **Save** at the bottom if you want to reuse your selections again later to perform the exact same export. For example, you might export the same items on a regular basis from here or using the dt command line tool.



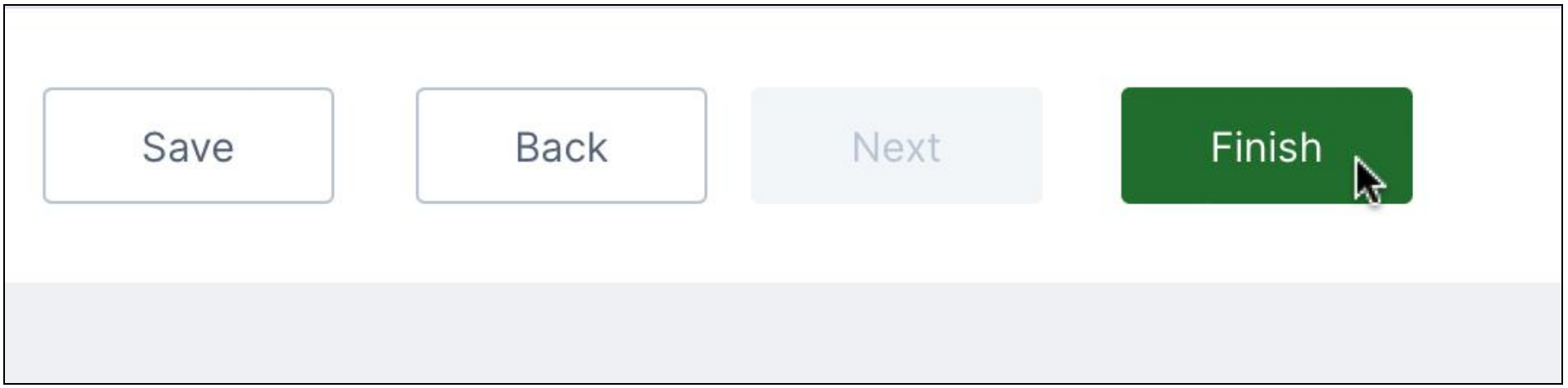
To see and use your saved export configurations, click **Existing Configs** under the *Import / Export* category.



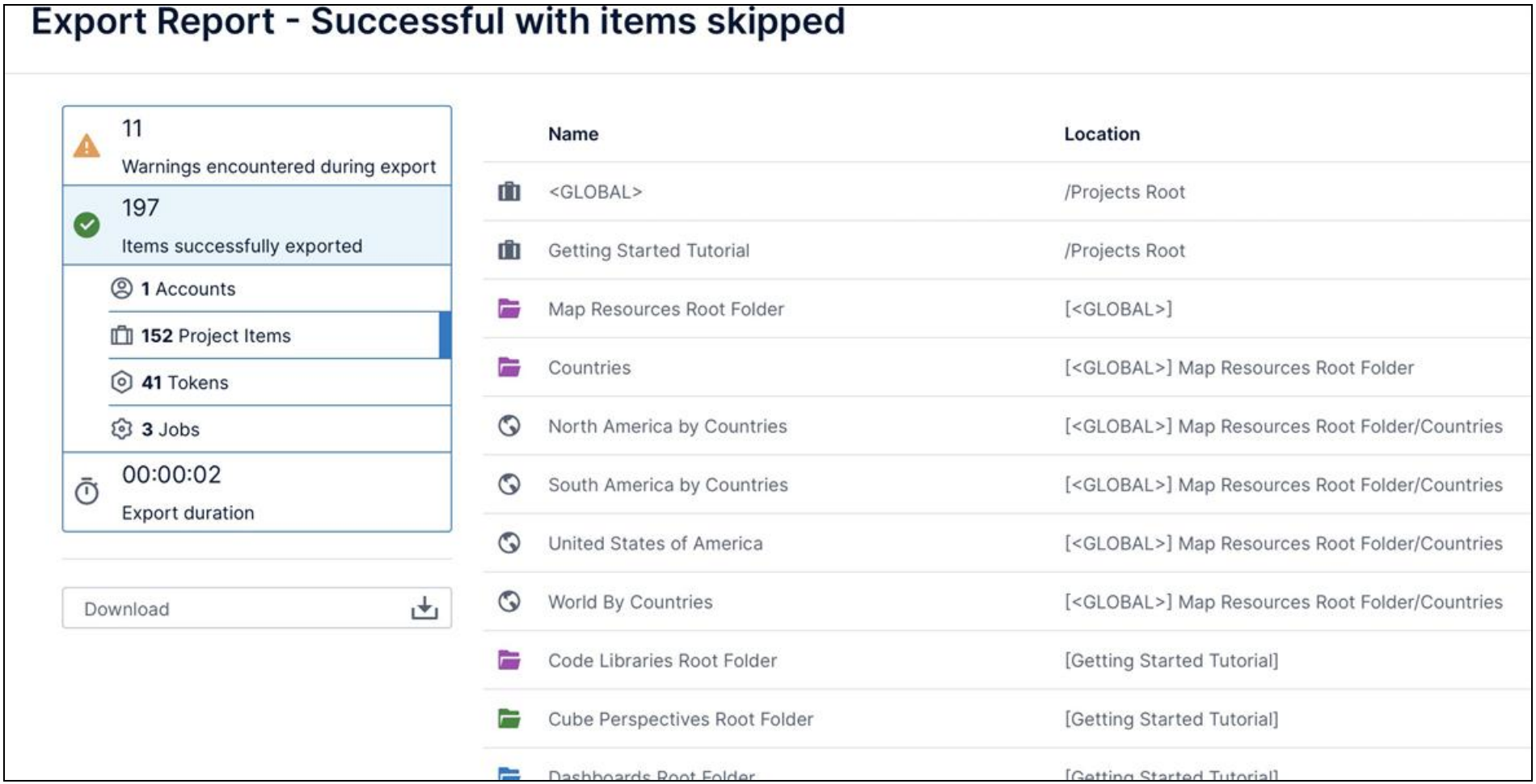
To use an export configuration, select it and click **Open** in the toolbar.

Finish

Begin the export or import procedure by clicking **Finish** after reviewing all of the options, or at any point if you know all desired options are selected.



A report is displayed when the procedure completes.



Note: Importing a data cube that uses warehouse or in-memory storage will include its storage jobs and schedules, but the jobs will not automatically run immediately. You will need to build the cube's storage or wait until the job runs according to its schedule.

The report details all of the items that were exported or imported along with any errors or warnings that you should review.

Click to navigate through each section on the left to list its items in the table to the right. You can click on a row in the table to see more details in a dialog.

Download the Export File

When you are exporting and the process was successful, the export file will normally be downloaded automatically, otherwise you can click the **Download** button. The file will be named *Export_<Date>_<Time>.dbie* to include the date and time of the export.

For more information, see:

- Check In, Check Out and Auto Saving
- Manage Projects and the File System
- Working With Projects

Localization and Multi-Language Support

This applies to: *Managed Dashboards, Managed Reports*

Symphony provides support for multiple languages through the use of XML localization (translation) files on the server that determine all user interface text, and through culture-sensitive formatting of numbers and dates.

Text that appears in the various user interface screens, dialogs, and toolbars can be customized by editing the localization XML files and replacing whatever text you require, or by using overrides, which can help with application branding. Currently, Symphony does not ship with alternative language translations, but this can be accomplished by third parties or your own organization.

For information about localizing tokens including the system-defined attribute and relative time tokens see Managing tokens. Text displayed within dashboards and other views can be localized using code libraries.

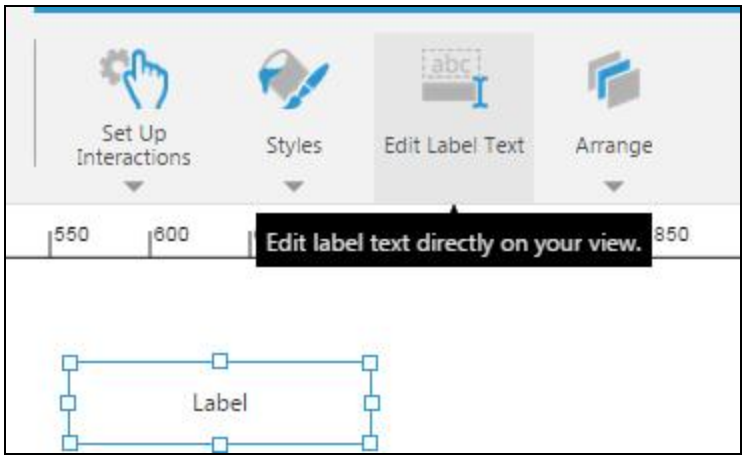
Right-to-Left Support

Symphony lets you use right-to-left languages such as Arabic and Hebrew when entering text for display purposes in the dashboard designer.

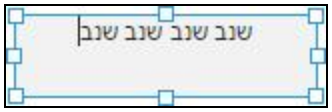
As an example, create a new dashboard in Symphony and add a **Label** component to the canvas.

Go to your Windows Language bar and change the input language to one that flows right-to-left (e.g., Hebrew).

Select the label component and click **Edit Label Text** from the toolbar (or the right-click menu).



Press CTRL+SHIFT on the right side of your keyboard. This will ensure the cursor position is correct for right-to-left text entry. You can now begin typing the label text in a right-to-left manner.



Similarly, when entering text in the **Properties** window for a data visualization control (e.g., **Title** property for a chart axis), press CTRL+SHIFT and then begin typing right-to-left text.

Culture Settings

A locale or culture is a collection of settings that defines a user's language, country and preferences for viewing specific kinds of information in a user interface, such as numbers, dates, times, and currency. Numbers and dates will automatically display according to each user's current culture without any other configuration.

A culture is represented in Symphony as a **culture name**, typically consisting of two parts:

1. A lowercase *culture code* associated with a language.
2. An uppercase *subculture code* associated with a country or region.

Below are some examples of culture names:

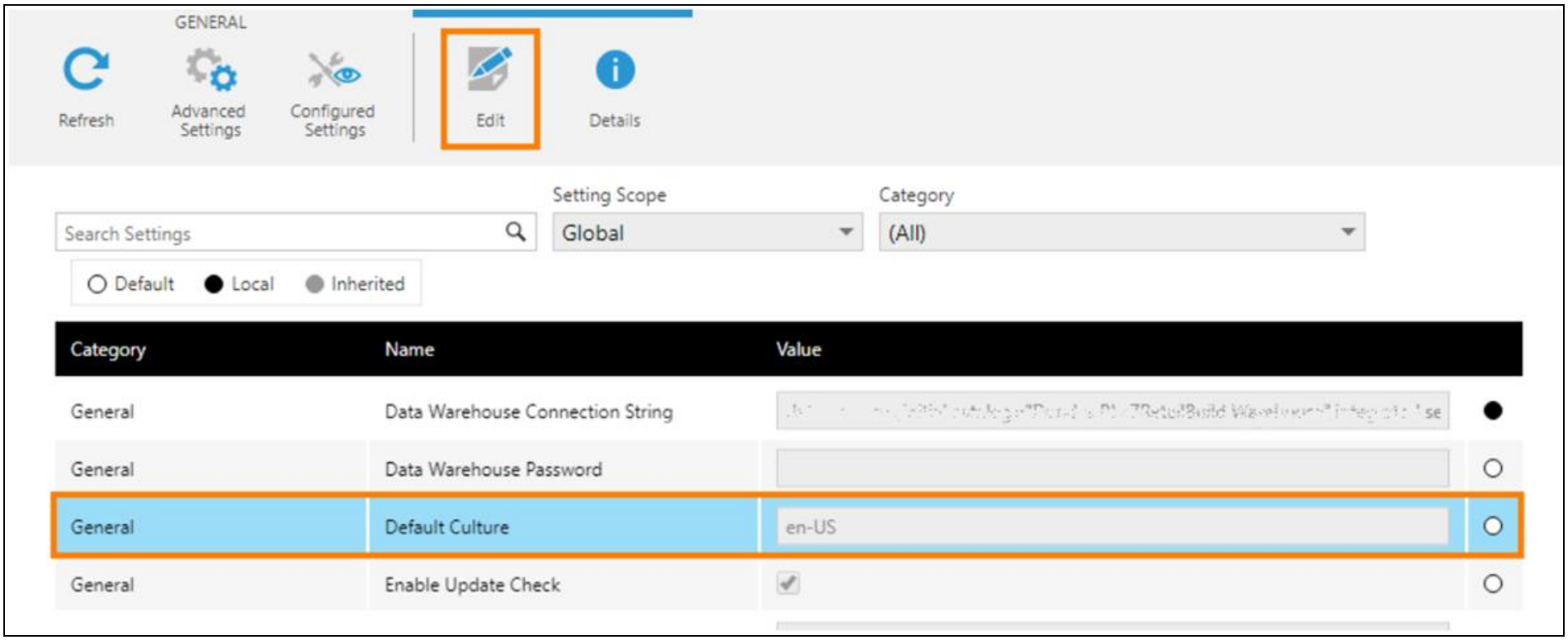
Culture Name	Language (Country/Region)
en-US	English (United States)
en-CA	English (Canada)
fr-FR	French (France)
fr-CA	French (Canada)
de-DE	German (Germany)

An extensive list of culture names (or 'language tags') is available here and can apply to Symphony whether its server is running on Windows or Linux.

Default Culture

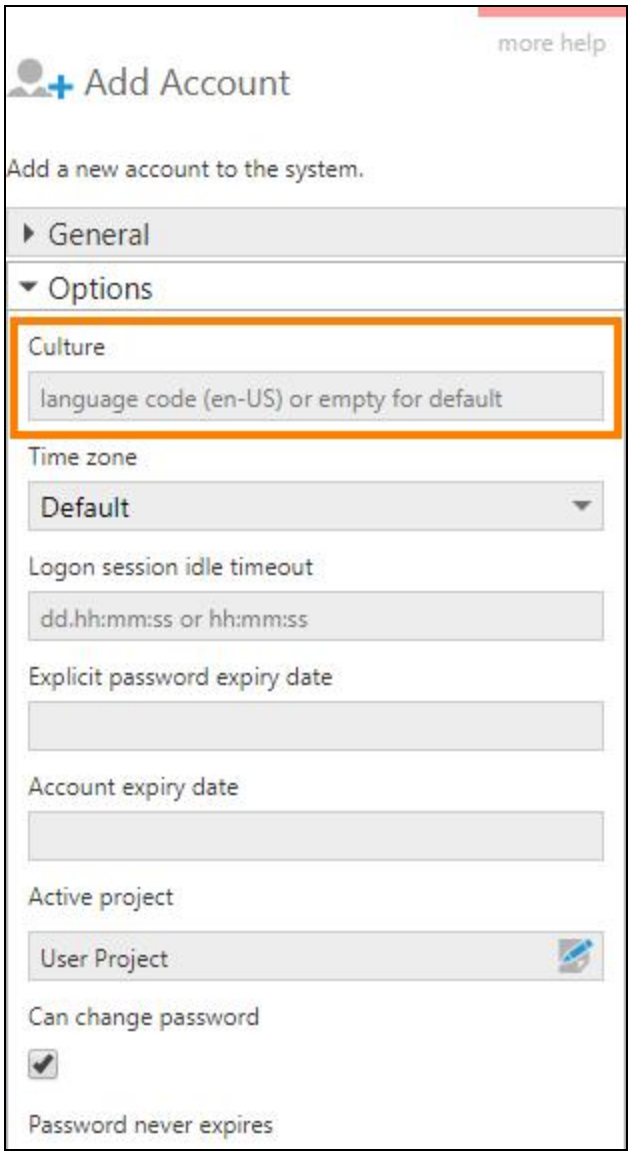
The Symphony application is installed with a *default culture* using the culture settings of the server, but this can be changed by an administrator via a configuration setting.

To change the default culture for Symphony, click **Admin** from the main menu, expand **Setup**, and then click **Config**. In the Configuration settings, select the *Default Culture setting* and click **Edit** in the toolbar.



User Account and Group Culture

A culture setting can also be applied directly to a user or group by an administrator to assign them different cultures. This setting takes precedence over the application's default culture for each user.



Session Culture

The culture can also be set for a user just for their current logon session. This culture takes precedence over their account and server culture settings described above.

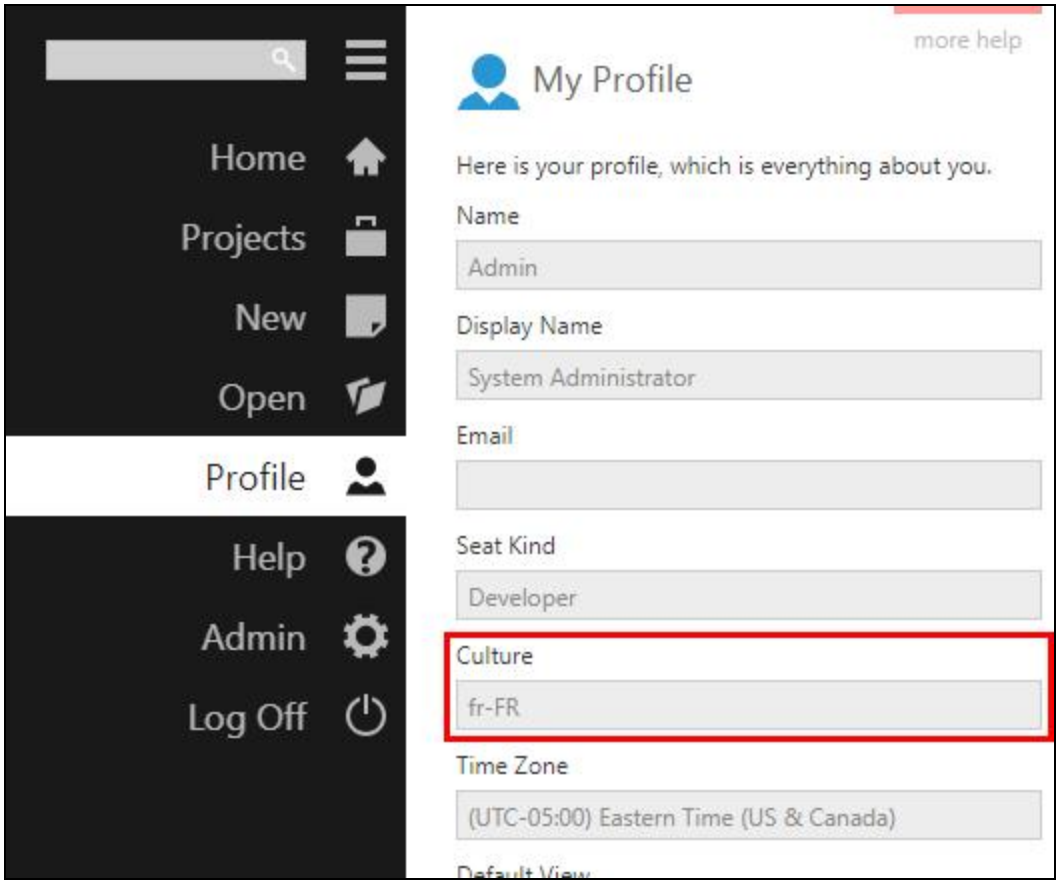
The session's culture can be automatically determined by the language settings from the user's browser if the *Enable Accept-Language Header Culture* application configuration setting is enabled.

It is also possible to specify directly the culture you want to use for your logon session by navigating to the Symphony Log On screen with the **cultureName** query string parameter.

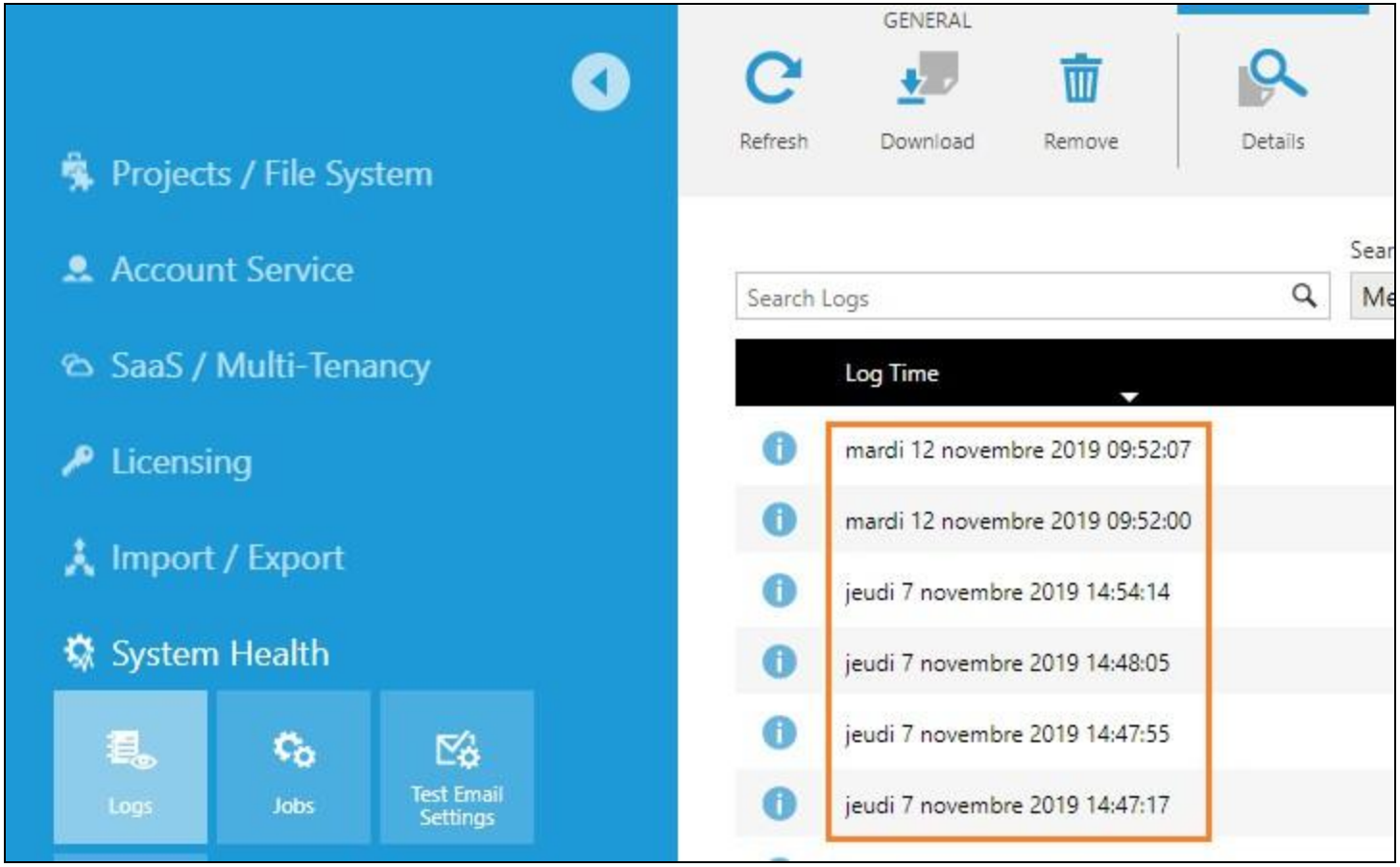
Here is an example URL for specifying a French (France) culture:

```
http://myserver:8000/LogOn?cultureName=fr-FR
```

After logging on, you can confirm the culture associated with your logon session by clicking on **Profile** in the left menu, and finding the **Culture** field.



Various places in the application will display numbers and dates formatted accordingly as well.



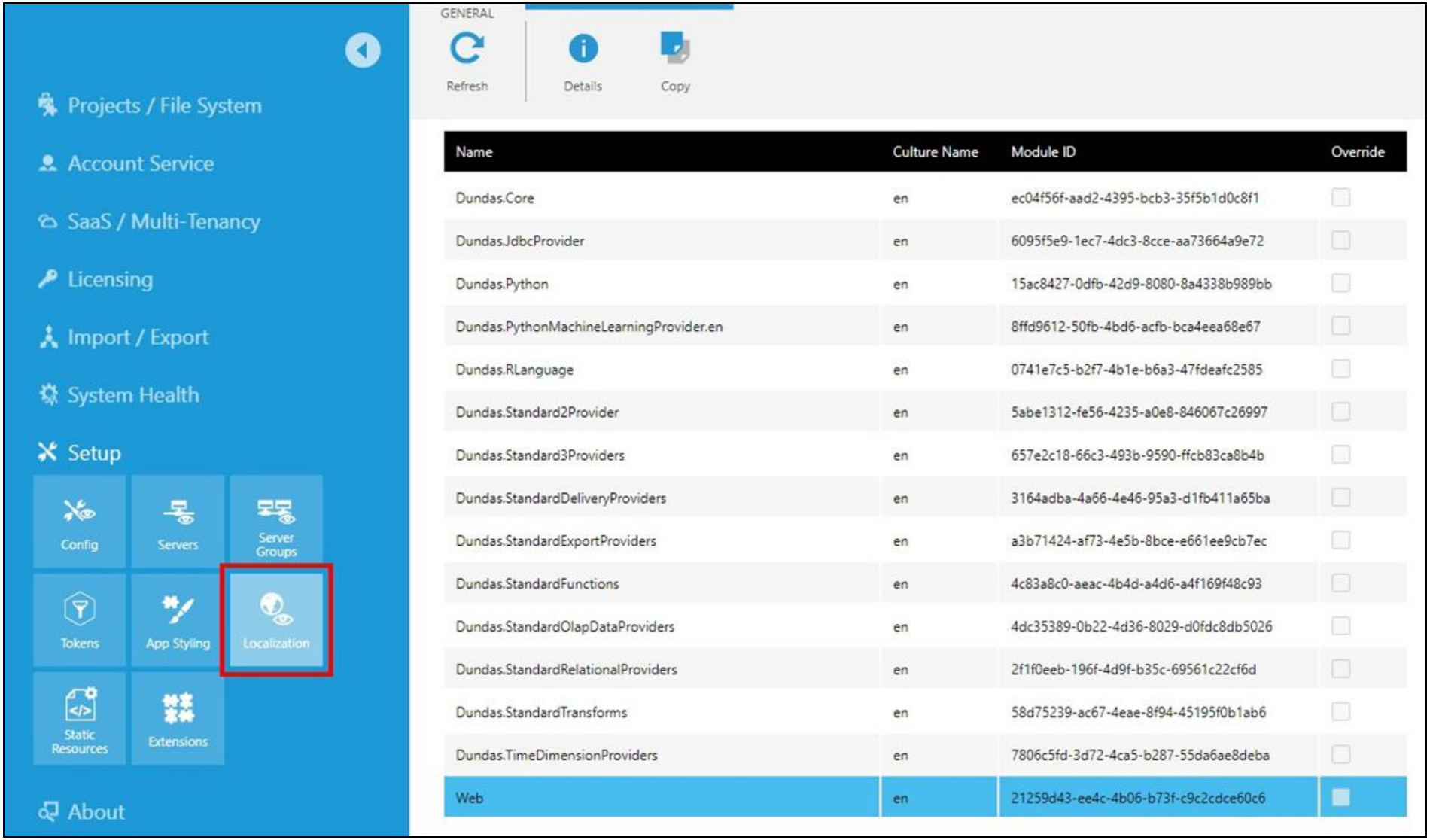
The culture for a user's logon session is determined from these settings (in order from highest to lowest priority):

1. The culture as specified via the cultureName query string parameter.
2. The culture specified in the browser's language settings (Accept-Language header) if enabled in the config settings.
3. The culture assigned to the user's account.
4. The culture assigned to a group that contains the user.
5. The default culture as specified in the application configuration.

Localizing for a Specific Culture

Most text displayed in Symphony (other than numbers, dates, and data from data sources) comes from localizations. To change this text for different cultures and languages, additional localizations are needed providing the translated text for each required language and/or country.

Localization files are stored in Symphony and managed through Symphony's administration interface from the **Localization** page, found by expanding the **Setup** category.



The Web.xml file, for example, contains most of the localization strings pertaining directly to the user interface of Symphony (for a specific language). You can download a copy of one of the built-in localizations by double-clicking it or by selecting it and clicking **Details** in the toolbar, then clicking **Download localization**.

XML File Format

A language localization file is an XML document with the following basic structure:

```
<?xml version="1.0" encoding="utf-8"?>
<localization>
  <group>
    <string></string>
    ... more strings ...
    ... more groups ...
  </group>
  ... more groups ...
</localization>
```

Element: localization

The **localization** element specifies the culture of the localization file. Only one localization element is permitted per localization file.

Example:

```
<localization xmlns="http://dundas.com/schemas/BI/localization.xsd"
              culture="en"
              moduleId="EC04F56F-AAD2-4395-BCB3-35F5B1D0C8F1">
    ... one or more groups ...
</localization>
```

Element: group

The **group** element is used to group related translation strings. Groups can be nested within another group. Example:

```
<group name="LogOnView">
    ... one or more strings ...
    <group name="PasswordReset" tags="client">
    ...
    </group>
</group>
```

Element: string

The **string** element is used to specify the translated text for a string that appears in the application's user interface. The **key** attribute uniquely identifies the string and must not be changed. The actual translated text appears between the start and end tags of the string element.

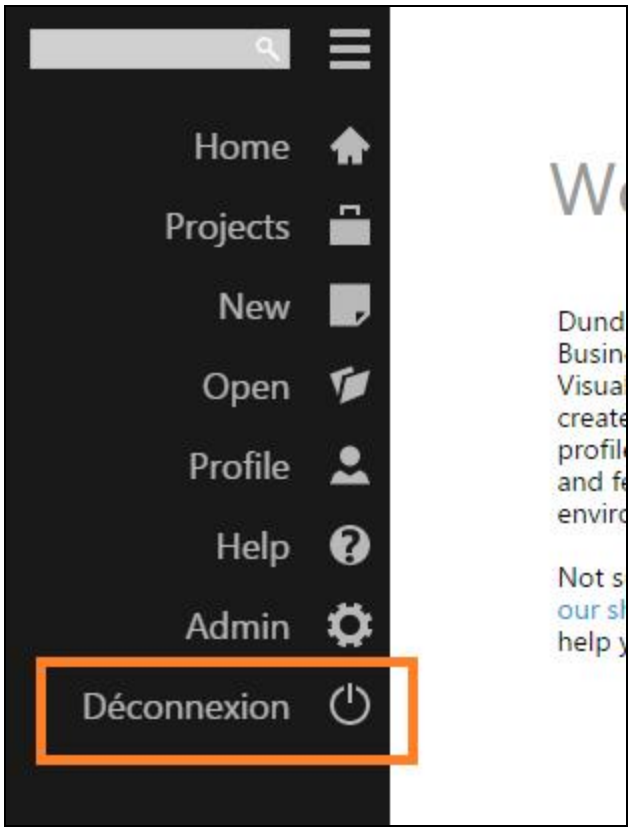
Example:

```
<string key="GS_LogOn_Title">Log on to Symphony</string>
```

Example: Localizing for French

This example shows how to add support for the *French (France)* culture, localizing the text of the Log Off button in the main menu as an example.

1. From the main menu, click **Admin**, expand **Setup** and then click **Localization**.
2. Select the **Web** override file from the list of files and then click **Details** on the toolbar.
3. Click **Download localization** to save the localization file as an XML file.
4. In the localization file, change the values of the string elements to your target language. As an example, change the string with key *GS_MainMenu_LogOff from Log Off to Déconnexion*. (To complete the localization for another language, any remaining strings should also be localized, or they can be removed.)
5. Select the localization *Web* in the list and then click **Copy** on the toolbar.
6. Set the *Target Culture* to *fr-FR* and click **Submit**.
7. From the list of localizations, select the *fr-FR* culture version of the Web localization and then click **Details** on the toolbar.
8. Click **Choose File** and select the localization file saved and edited earlier, or you can paste the contents, then submit the dialog.
9. You may need to recycle the application pool for the changes to take effect.
10. Navigate to *< website>/LogOn?cultureName=fr-FR* and log on.
11. Expand the main menu to see the localized text for the Log Off button.



Override Mechanism

For the purposes of branding or white labeling, you typically want to modify a few localization strings (e.g., related to product name) instead of adding support for a whole new language. In this case, you can use the override mechanism to replace a subset of localization strings for an existing culture.

See White labeling the application for an example of customizing Symphony text using overrides.

For more information, see:

- White Labeling the Application
- Managing Tokens

- Using Code Libraries
- Configuration Settings

Logon History

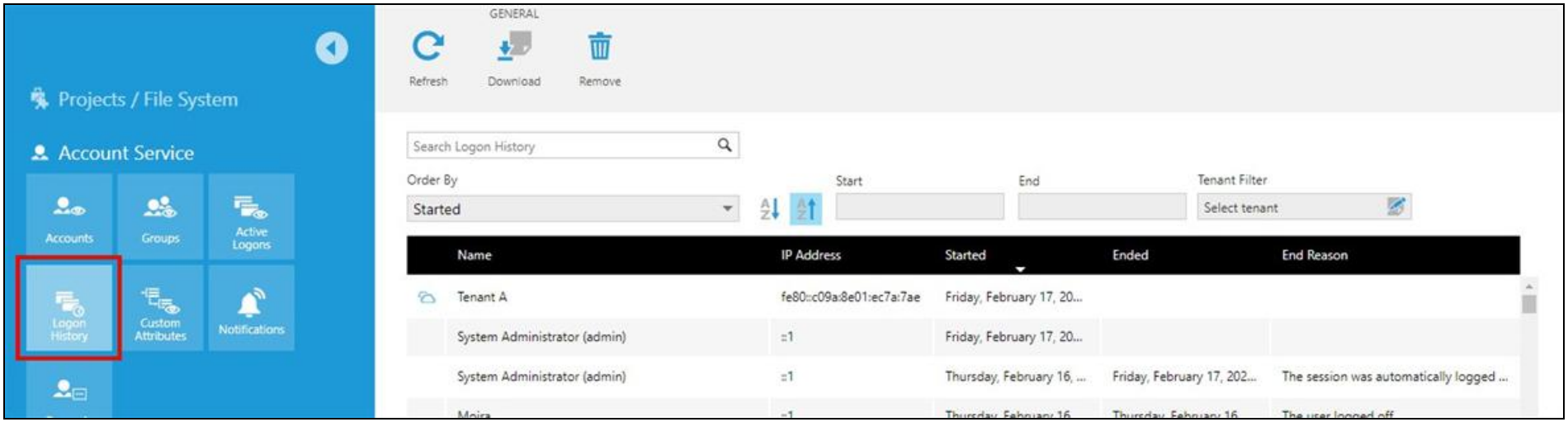
This applies to: *Managed Dashboards, Managed Reports*

This article shows you how to view the logon history in Symphony.

View the List of Logons

To view the entire logon history, expand the **Account Service** section in the Admin screen and click **Logon History**.

For each logon record, you can see the corresponding account name, IP address, start time, end time, and end reason, and you can filter and sort the records. Any impersonated sessions will appear with a distinct icon.



To view the list filtered to a particular user, you can open their Account Details as described below and click **Log on history**. If you have an account ID (GUID), session ID, or IP address, you can enter these into the search box.

Actions for a Logon

After clicking to select a record or right-clicking it, additional actions are available in the toolbar or context menu:

- Choose **Details** to view additional information such as the session ID, seat type, and seat mode.

- Click Account Details to open the same *Account Details* dialog for that user.

- For an active session (with no end time), choose **Logon Session Details** to open the same *Logon Session Details* dialog that is accessible from the Active Logons page, containing various session and account details.

Download Logon History

Click **Download** in the toolbar to download a CSV file containing all of the logon history records displayed for your current filter settings.

This file can be viewed in Excel or a similar app. You may need to resize columns or select cells in order to view its entire contents.

For more information, see:

- Advanced User Management
- Use the Administration Homepage
- View Active Logon Sessions

Manage Projects and the File System

This applies to: *Managed Dashboards, Managed Reports*

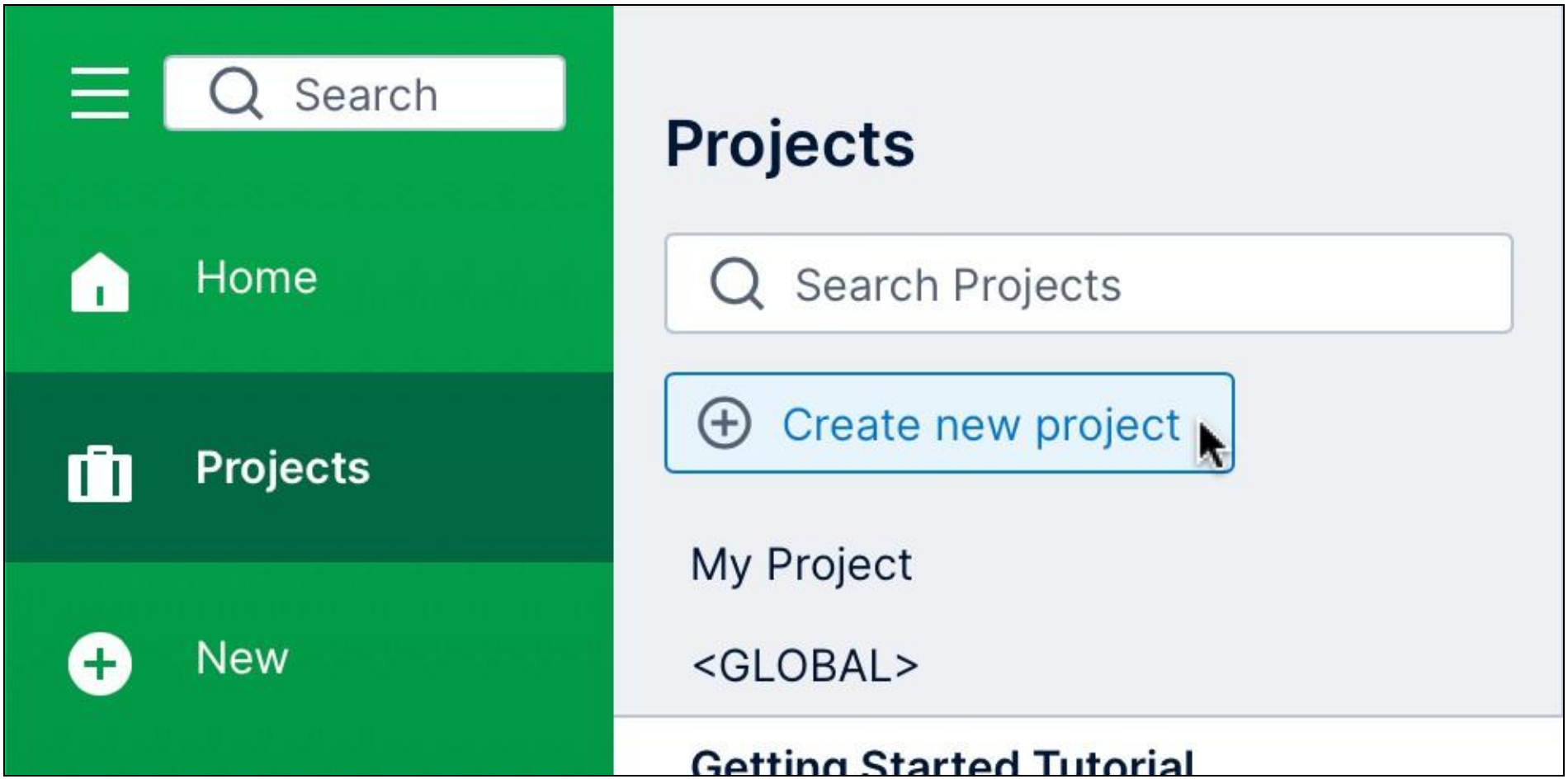
This article shows you how to manage projects and their files as an administrator in Symphony, including data cubes and their storage.

All of your work items in Symphony, such as data cubes and dashboards, are treated as files within the file system. A project lets you organize related files and collaborate with other users who have access to the same project. See Working with projects.

Add a New Project

Administrators can add new projects from the main menu.

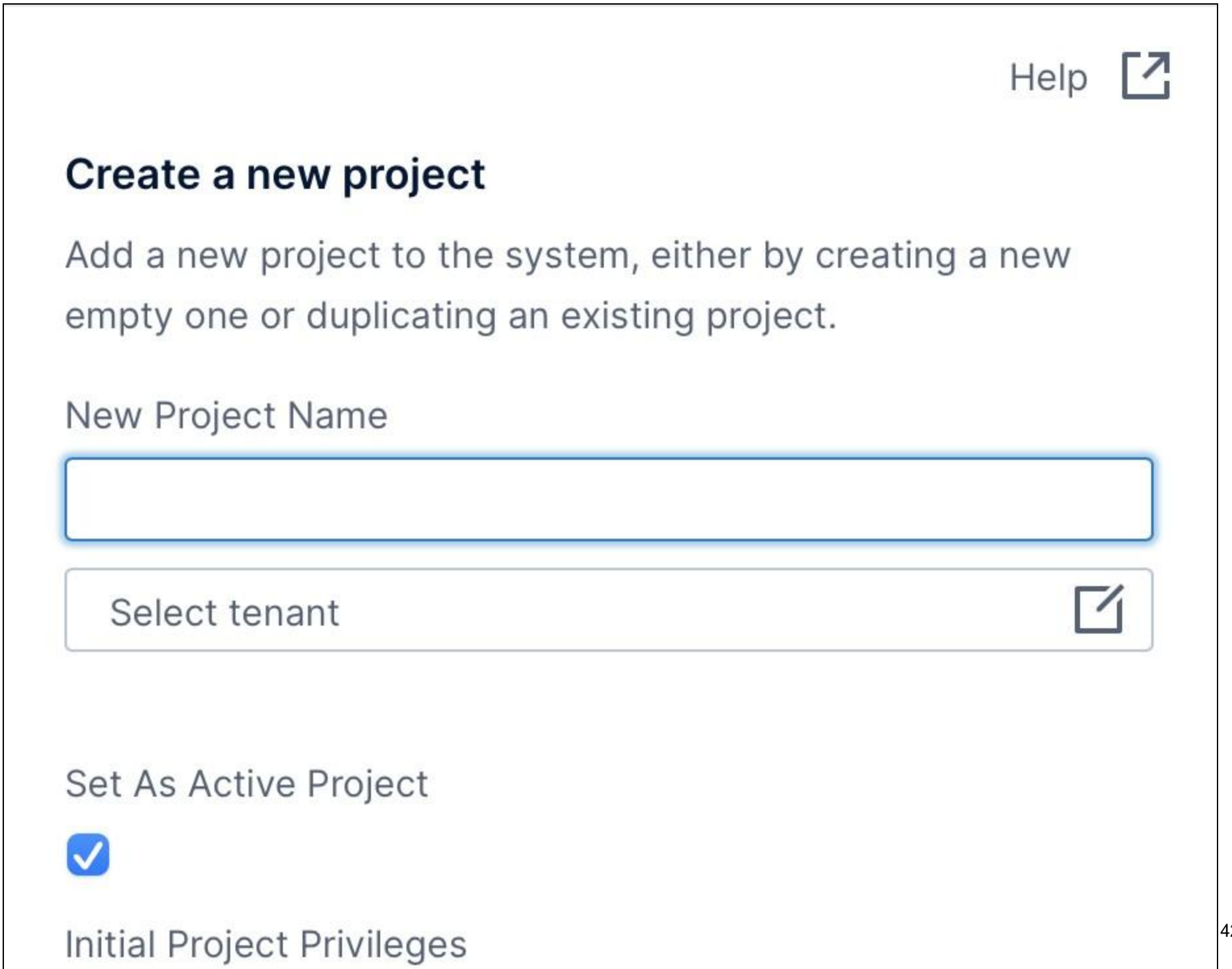
Create a new project at any time by clicking **Projects**, and then click **Create new project** or **Add New...** in the list of projects that appears.



You can also add a new project from the toolbar of the Projects page in Administration, shown in the next section.

In the *Create a New Project* dialog, type a name for the new project and set the **Initial Project Privileges**:

- *Private* – After the project is created, only the creator will have access to it.
- *Public* – After the project is created, the Everyone group will have *Read* access to it.
- *Custom* – After the project is created, the project's *Security* dialog will open.


Help
Create a new project
Add a new project to the system, either by creating a new empty one or duplicating an existing project.
New Project Name
Select tenant
Set As Active Project
Initial Project Privileges

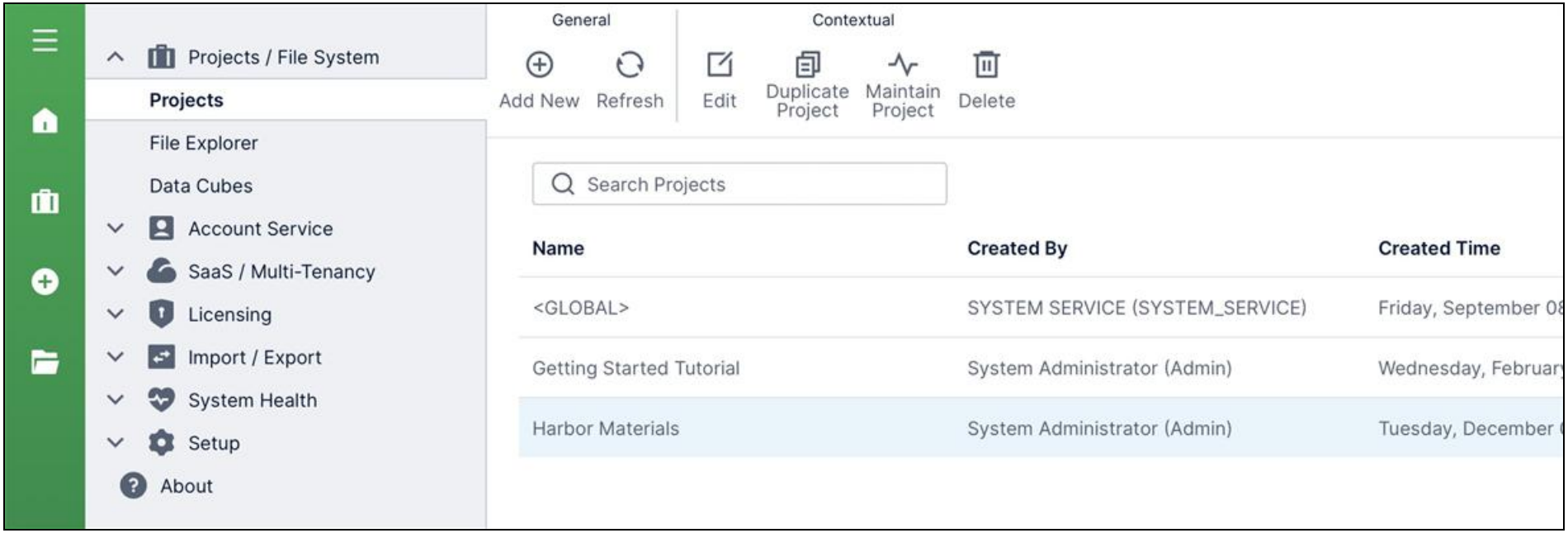
If you're using multi-tenancy and have existing tenants, you can choose a tenant to be associated with the new project. Projects not assigned to a tenant can be accessed by all tenants with access according to the project's security privileges.

Select the **Active Project** option if you also want the new project to be set as the active/current project once it's created, otherwise you and other users with access can select it from the main menu.

Manage Projects

You can manage existing projects from the Administration area, which administrator users can access from the main menu.

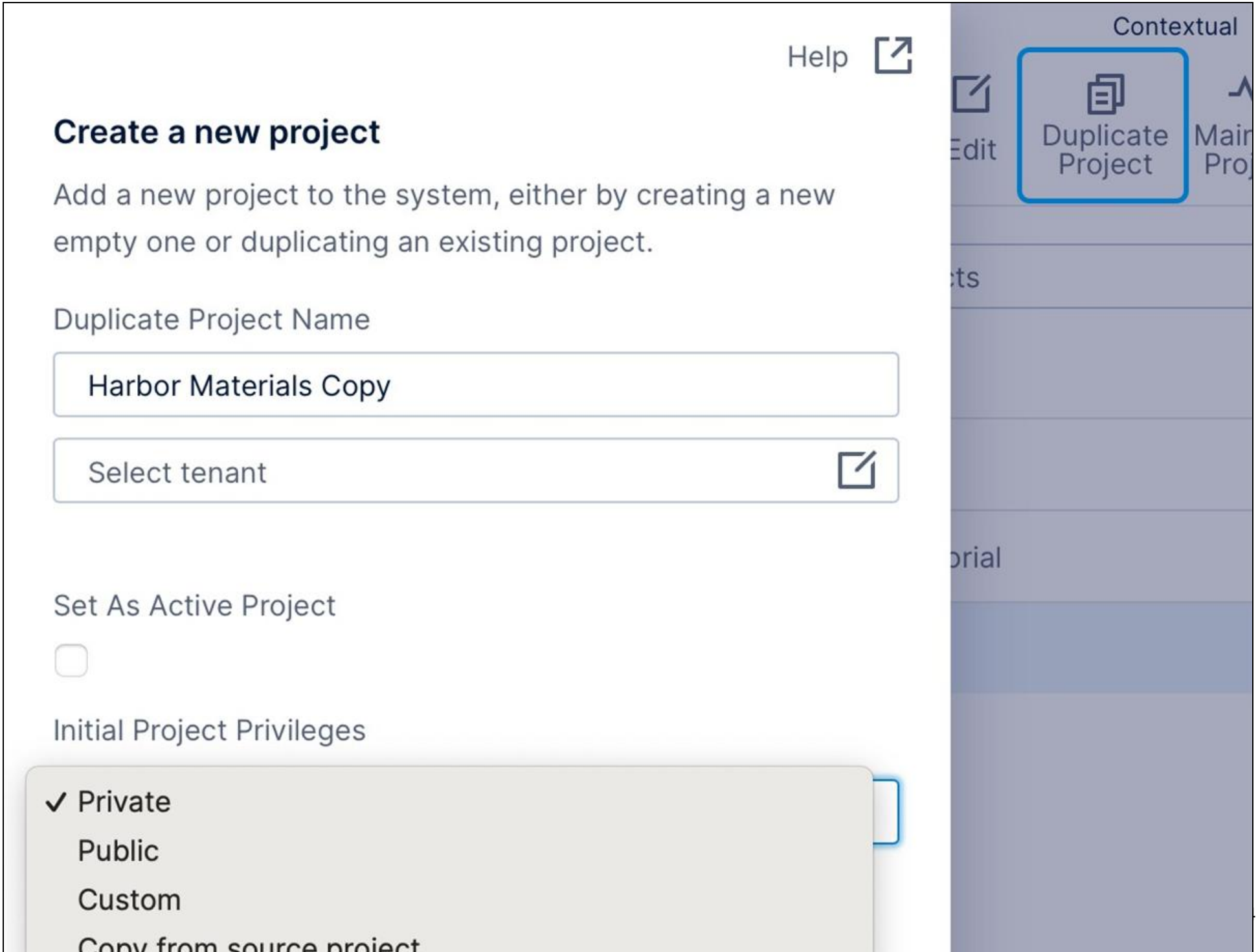
Under the **Projects / File System** section on the left, click on **Projects**.



Click to select a project and choose from the options shown in the toolbar:

- To view or modify the settings for a project in the list, including its name, tooltip description, and security privileges, click **Edit** in the toolbar to open the Properties dialog.
- Make a copy of an existing project by clicking **Duplicate Project** in the toolbar. You'll be asked to enter a new name for the copy and the **Initial Project Privileges**. The privileges drop-down provides the same options as for Add a New Project, except that you can also choose *Copy from source project* to

continue using the same security privileges in the new duplicate project.


Help
Create a new project
Add a new project to the system, either by creating a new empty one or duplicating an existing project.
Duplicate Project Name
Harbor Materials Copy
Select tenant
Set As Active Project
Initial Project Privileges
Private
Public
Custom
Copy from source project
Contextual
Edit
Duplicate Project

- Click **Maintain Project** in the toolbar to view, edit, and delete unused entities in the project.
- To delete a project, click **Delete** in the toolbar and then confirm the operation. Note that the built-in *<GLOBAL>* project cannot be deleted.

> **Note:** You can also publish content from one project to another rather than duplicating it.

Administrators can also access several of these options whenever right-clicking a project in any file explorer throughout the application, including in *Open* dialogs and the Explore window.

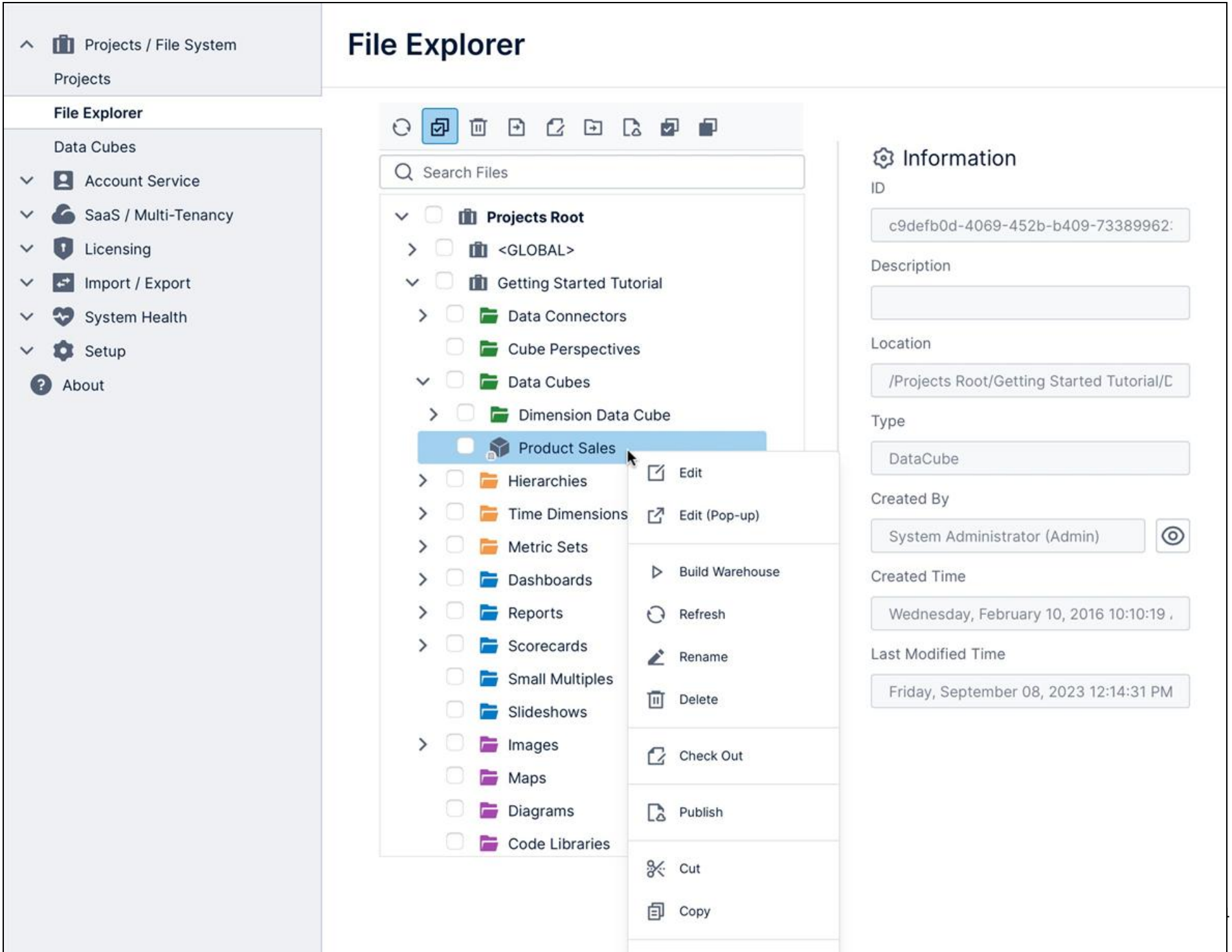
User Projects

The list of projects in the *Projects* screen does not include each user's personal project (named 'My Project'). To access another user's personal project, edit the user, scroll down, and click the button for their project.

> **Note:** To prevent a user project from being automatically created for each user when they first log on, change the **Create User Projects Automatically** configuration setting.

Using the File Explorer

Under **Projects / File System**, the **File Explorer** option lets administrators navigate Symphony projects and manage the files and folders they contain. It provides administrators the same options as the Explore window but shows all projects at once.


Projects / File System
Projects
File Explorer
Data Cubes
Account Service
SaaS / Multi-Tenancy
Licensing
Import / Export
System Health
Setup
About
File Explorer
Search Files
Projects Root
<GLOBAL>
Getting Started Tutorial
Data Connectors
Cube Perspectives
Data Cubes
Dimension Data Cube
Product Sales
Hierarchies
Time Dimensions
Metric Sets
Dashboards
Reports
Scorecards
Small Multiples
Slideshows
Images
Maps
Diagrams
Code Libraries
Edit
Edit (Pop-up)
Build Warehouse
Refresh
Rename
Delete
Check Out
Publish
Cut
Copy
Information
ID
c9defb0d-4069-452b-b409-73389962
Description
Location
/Projects Root/Getting Started Tutorial/D
Type
DataCube
Created By
System Administrator (Admin)
Created Time
Wednesday, February 10, 2016 10:10:19
Last Modified Time
Friday, September 08, 2023 12:14:31 PM

You can use either the File Explorer or the Explore window to:

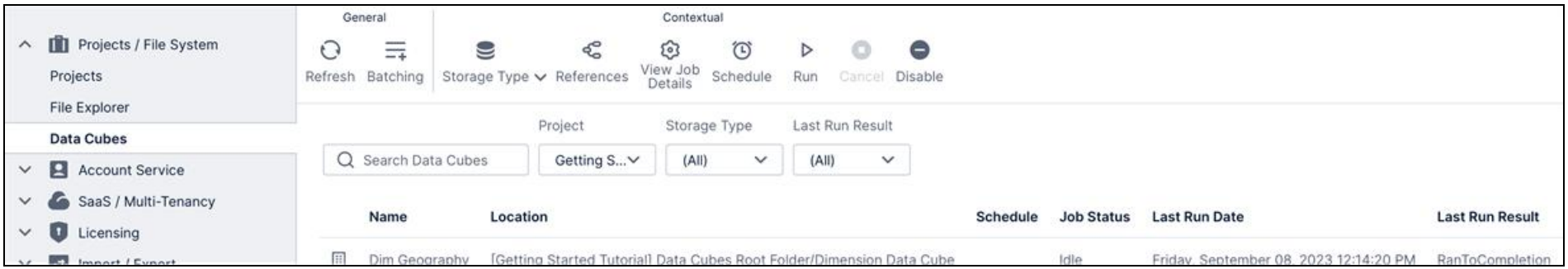
- Right-click on an individual file or folder to edit or publish, manage check out status, cut/copy/paste between folders, create new folders, or view or edit properties such as security privileges.
- Use the checkboxes next to the files to select files and perform a batch operation on them, choosing options from the toolbar similar to the right- click operations.
- When you click on a file, some quick details are displayed to the right similar to the properties. You can toggle off the checkboxes from the toolbar if you want to click to select files only to view these details.
- Search for files by typing in search terms or by entering the file ID (e.g., if provided in an error message).

Depending on their security privileges, non-administrator users can also perform most of these operations from their Explore window within their current project.

Administrators have a **Transfer Check Out** option when another user has a file checked out. If that user is unavailable, for example, you can transfer their changes to your account and either check in or undo their changes and allow someone else to check out the file.

Manage Data Cubes

Under **Projects / File System**, click **Data Cubes** to manage data cubes and especially their storage options and build status.



Data cubes are listed by name and filtered by the **Projects** drop-down, which you can use to switch between projects or to view all of them at once. You can also view and filter by the storage job status for data cubes using warehouse or in-memory storage (as indicated by their icons).

Click to select a data cube to choose from options in the toolbar:

- You can quickly change the cube's **Storage Type**. For warehouse or in-memory storage, you'll be given the option to automatically build other cubes that it references directly via Data Cube transforms.

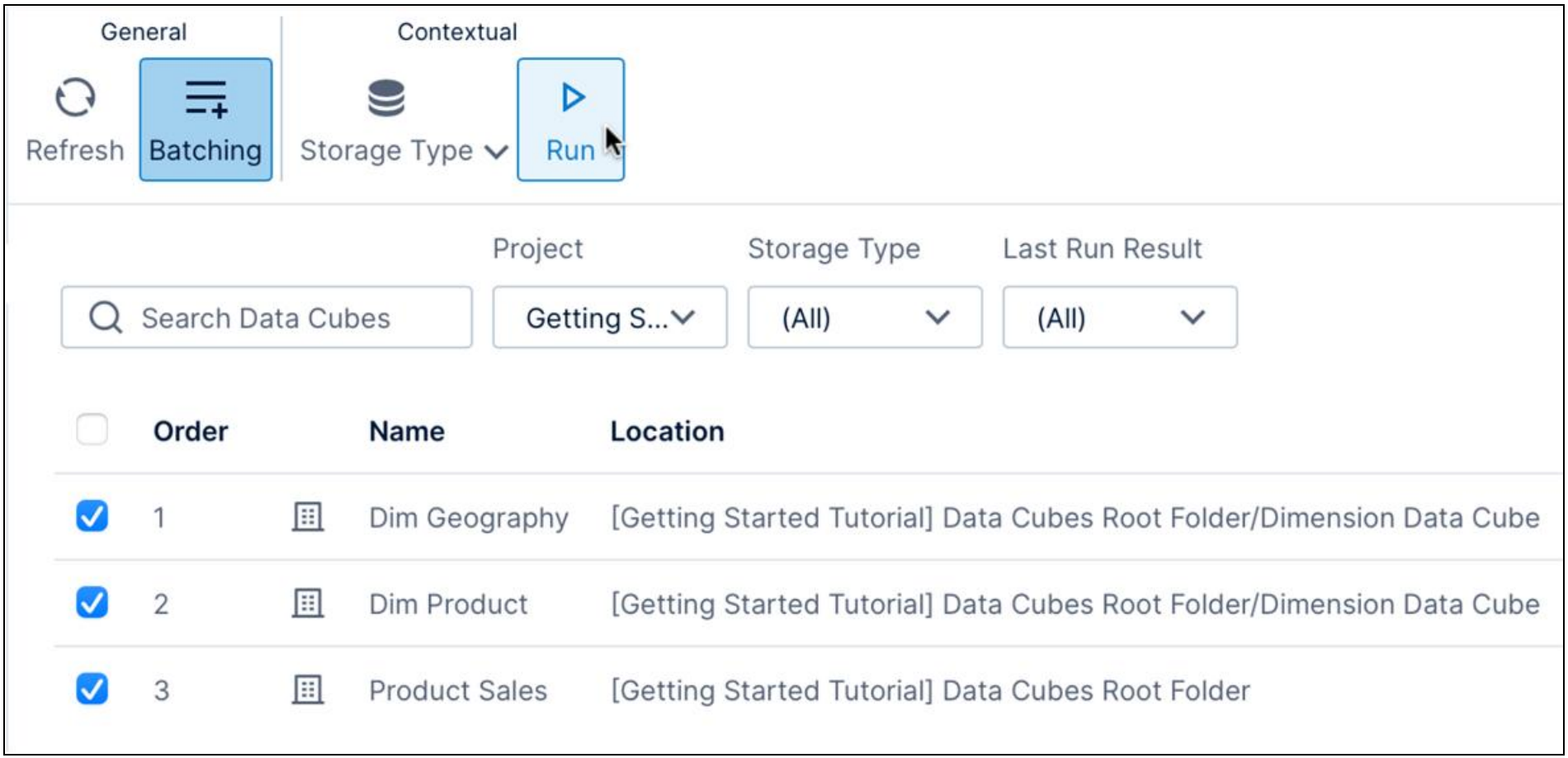
- Access the data cube's **References**, especially to find data cubes that reference each other or are dependencies, either directly or indirectly. This is the same dialog you can access from each file's Properties.

- For data cubes using a storage option, you can schedule, run, cancel, or disable its storage job, or navigate to its full job details page.

If you are managing a multi-tenant instance, the **Tenant Filter** field will be available on this screen. Set it to manage data cubes created by a tenant's users, or to view and edit optional separate schedules for each tenant for a data cube based on tenant overrides rather than use a single shared schedule.

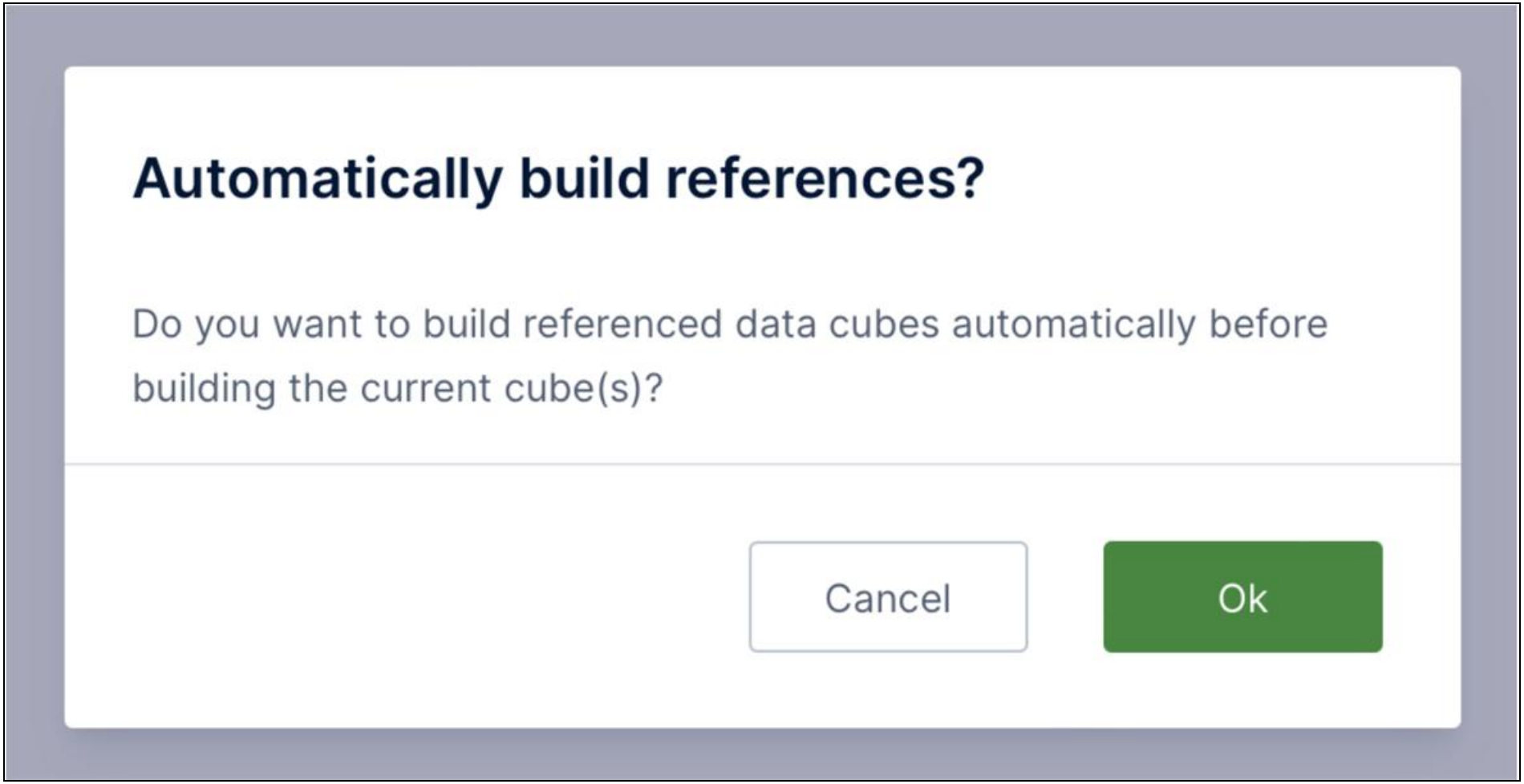
Batching

When you have multiple data cubes that you want to build all at once, click **Batching** in the toolbar to be able to select multiple data cubes using checkboxes along the left.



If you have a particular order in mind for which data cubes should build first, click the individual checkboxes to select them in that order, and their sequence will then be indicated in the *Order* column. You can build the selected cubes immediately by clicking **Run** in the toolbar.

You can also set up scheduled builds for the selected cubes, optionally including references. With one or more cubes selected, click **Storage Type** and choose from **Warehouse** or **In-Memory** storage. The *Schedule Rule* dialog will appear just like it does for individual data cubes, but in this case applies to multiple. After submitting this dialog, you will be given the option to automatically build directly-referenced data cubes at the same time.



Setting up a batched storage job like this creates a new *sequence* type job that builds storage for multiple cubes at once. Now when you view the schedule and build status for these cubes, or navigate to their job details, it will be for this sequence storage job.

Note: Sequence jobs are not maintained when copying or publishing the data cubes, and will need to be recreated for the copies.

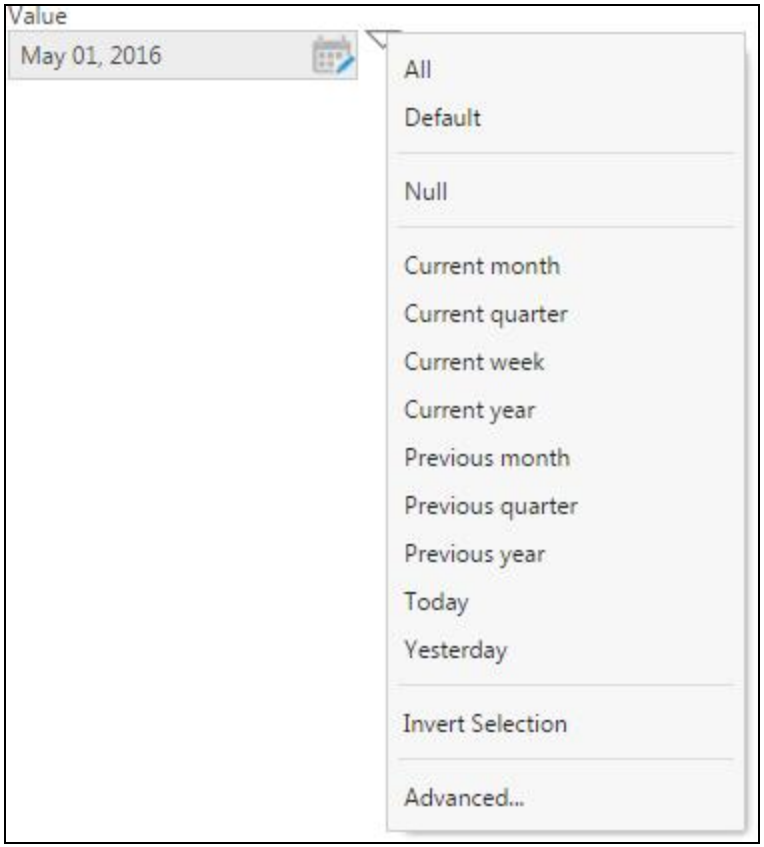
For more information, see:

- Use the Administration Homepage
- Working With Projects
- File and folder properties
- Check In, Check Out and Auto Saving
- Home Page
- Data Cube Data Storage Options
- Monitoring System Health
- Multi-Tenancy in Symphony

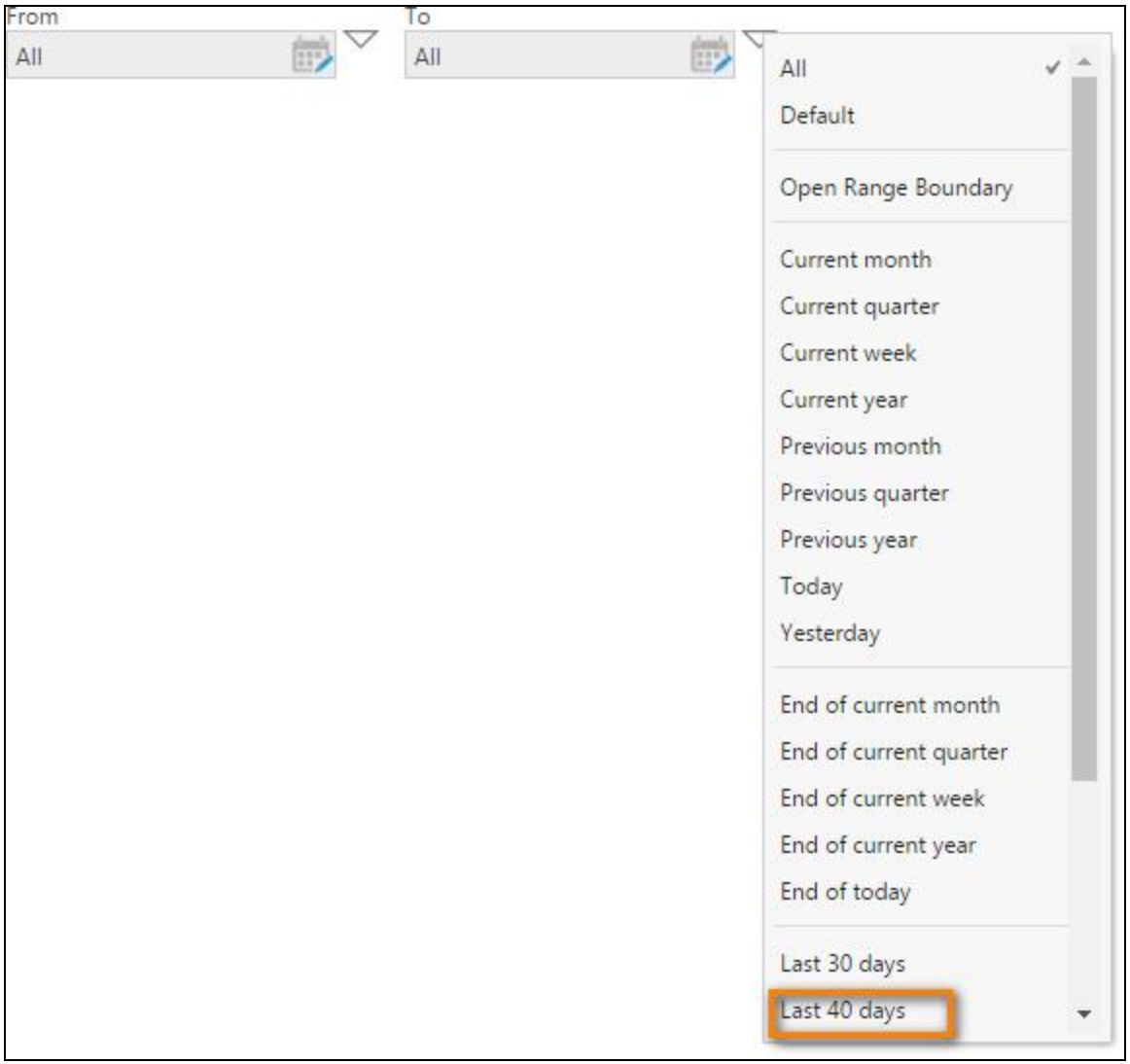
Managing Tokens

This applies to: *Managed Dashboards, Managed Reports*

Tokens are used in Symphony to provide options for setting filters besides choosing specific data source values. Most filters provide a token menu containing options such as *All* or *Null*. For time dimension filters, additional tokens let you select relative date values such as *Today, Current week*, or *Year to date*.



All user types can create custom tokens for themselves, but Symphony administrators and Tenant administrators with the *Create Token* privilege can manage all tokens, including tokens built into Symphony, or create new tokens for other users to use.



Token Types

Token Category	Description	Example
Attribute	Based on the user logged in	Current Account Name, Current Culture Name

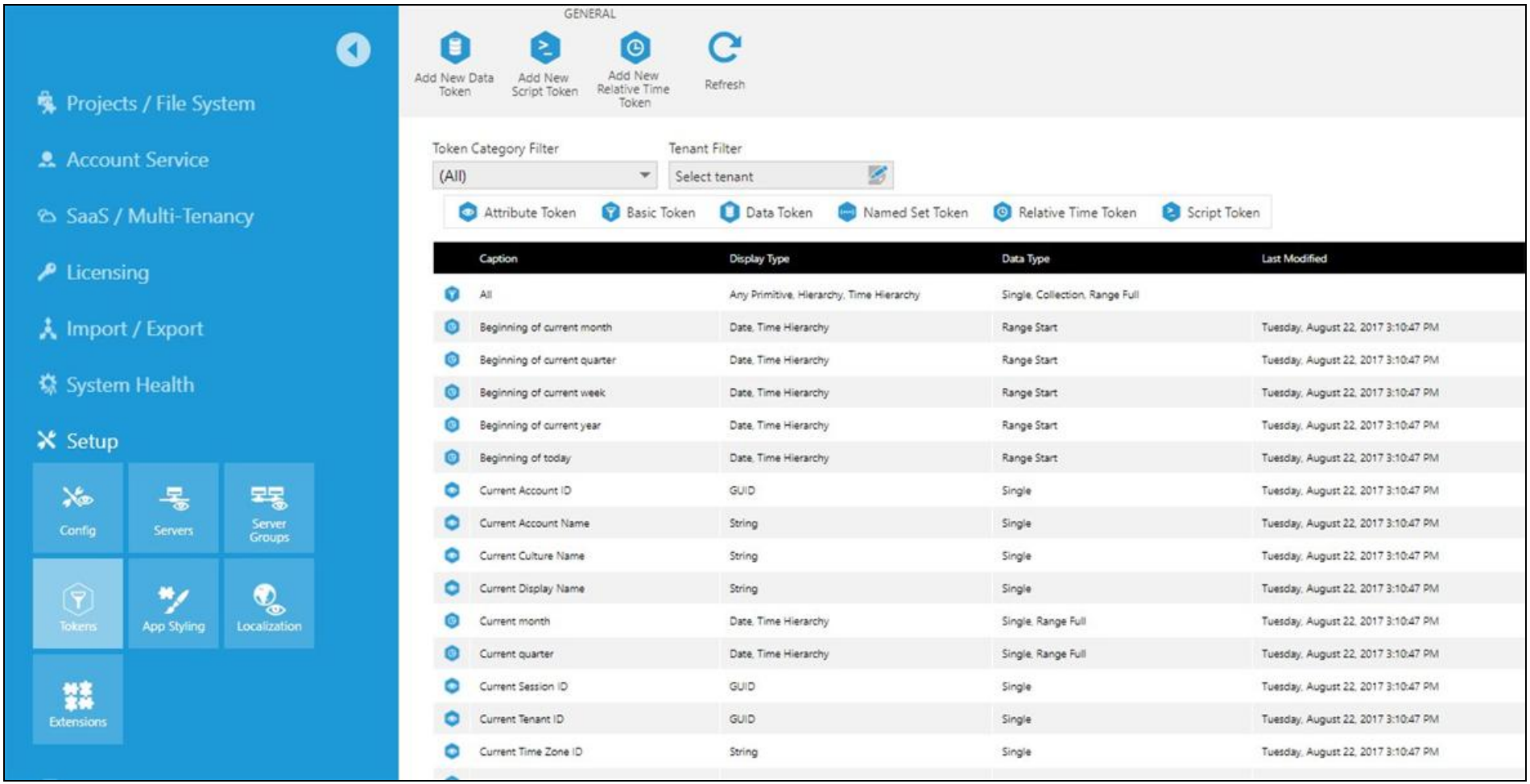
Token Category	Description	Example
Basic	Basic tokens	All, Default, Null
Data	Defined by querying an element of the data cube	First day, Largest order
Named Set	Defined on a specific dimension hierarchy	USA, Canada, Paris
Relative Time	Time based parameter token definition	Current Week, Last 30 days, Beginning of Today
Script	Defined using DundasScript, allowing unlimited flexibility	return TimeZoneInfo.ConvertTimeFromUtc(DateTime.UtcNow, currentSession.TimeZone);

You can create custom Named Set, Data, Relative Time, or Script tokens, while Attribute and Basic tokens are defined by the system but have options that can be set. There are also custom attributes you can define that can appear in token menus.

Note: Attribute tokens and custom attributes are listed in token menus only when editing data cubes.

Creating and Managing Tokens

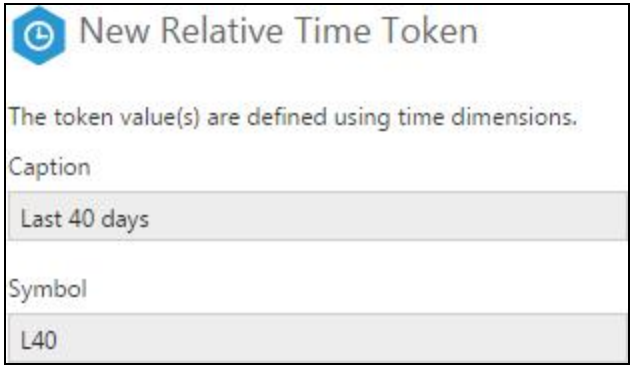
To create and manage tokens as an administrator, expand the **Setup** section in Administration, then click **Tokens**.



Creating tokens as an administrator is the same as for other users except that you can create script and relative time tokens from this screen. You can also create and manage tokens for other users of the system and promote user defined tokens to global tokens.

Administrators can access additional options for tokens:

- **Symbol**: Optionally set a symbol to use when including this token as part of a URL query string.



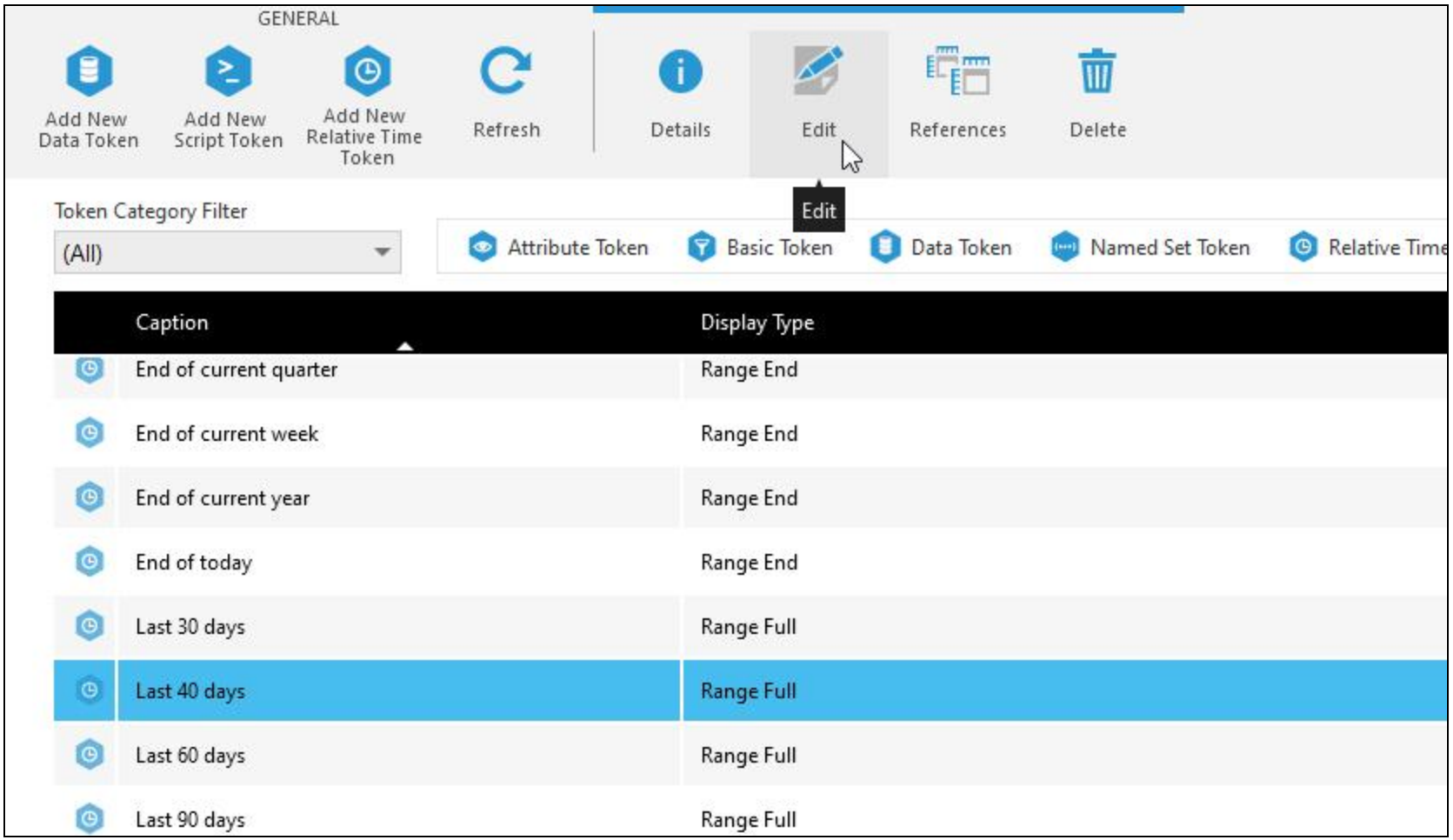
- **Token Association**: When creating a token as an administrator, this will be *Global* by default and available for all users. If you want to have a tenant- specific or account/group-specific token, select the desired token association from the drop-down list, and then choose the tenant or account.

See Creating custom tokens for details on creating each type of token.

Rename or Localize a Token

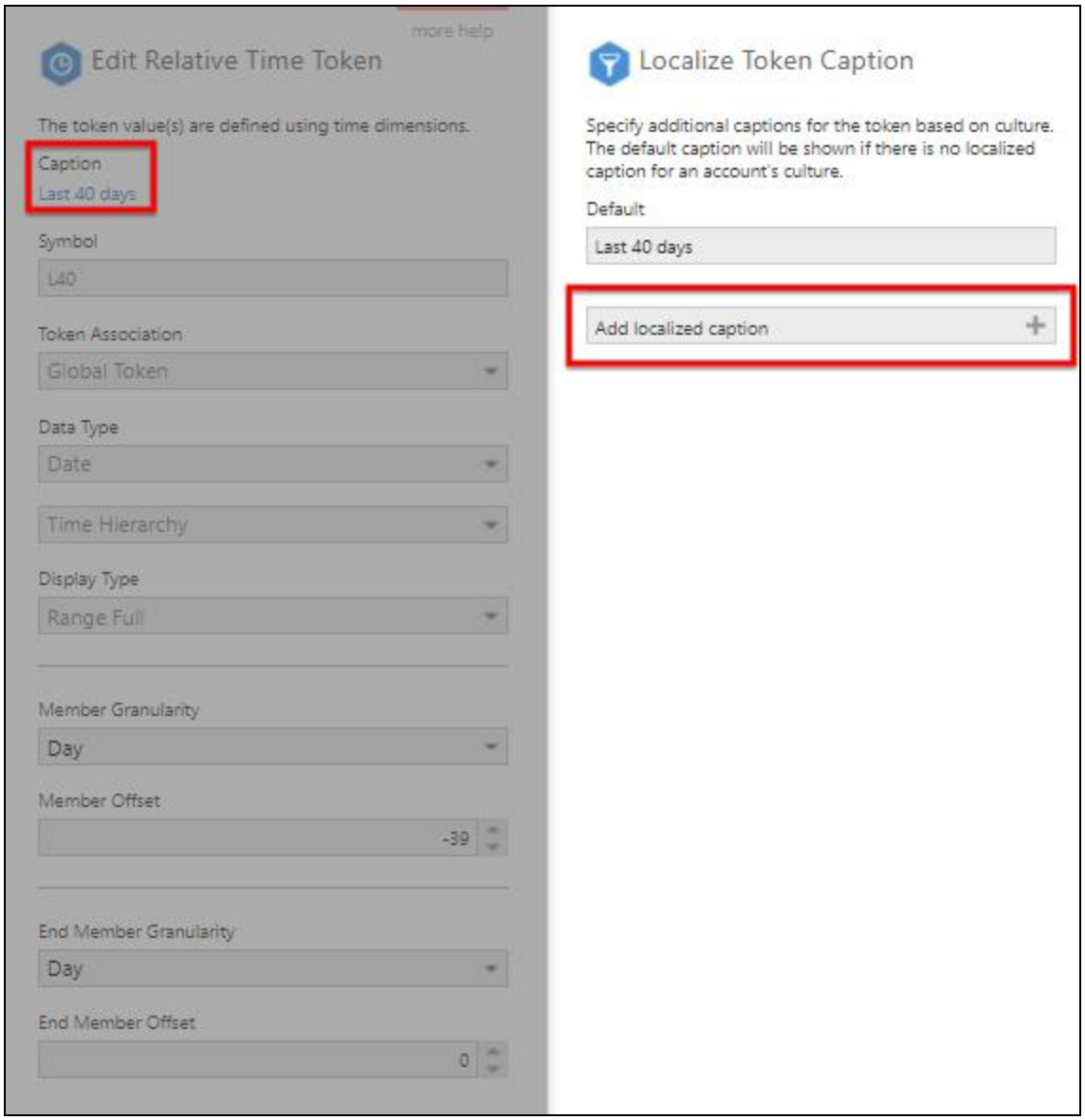
You can specify different captions for a token to be displayed depending on the language/culture of the user who is logged in. This applies to all types of tokens, including the system-defined attribute and basic tokens.

Locate and select the token from the list in the Tokens setup screen and click the **Edit** button in the toolbar.

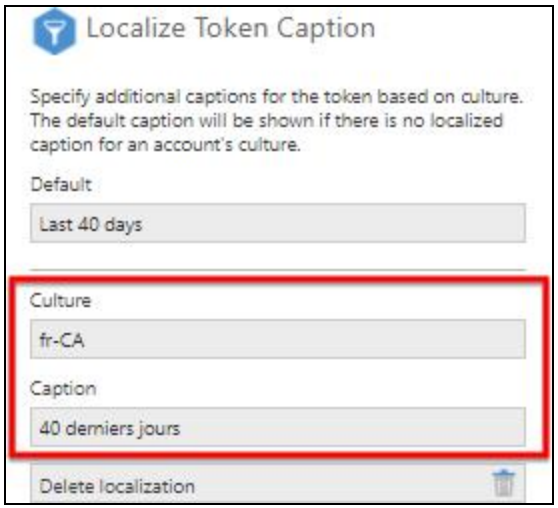


Click the caption link at the top of the edit dialog.

To rename the token for all users, change the text under **Default**; otherwise, click **Add localized caption**.



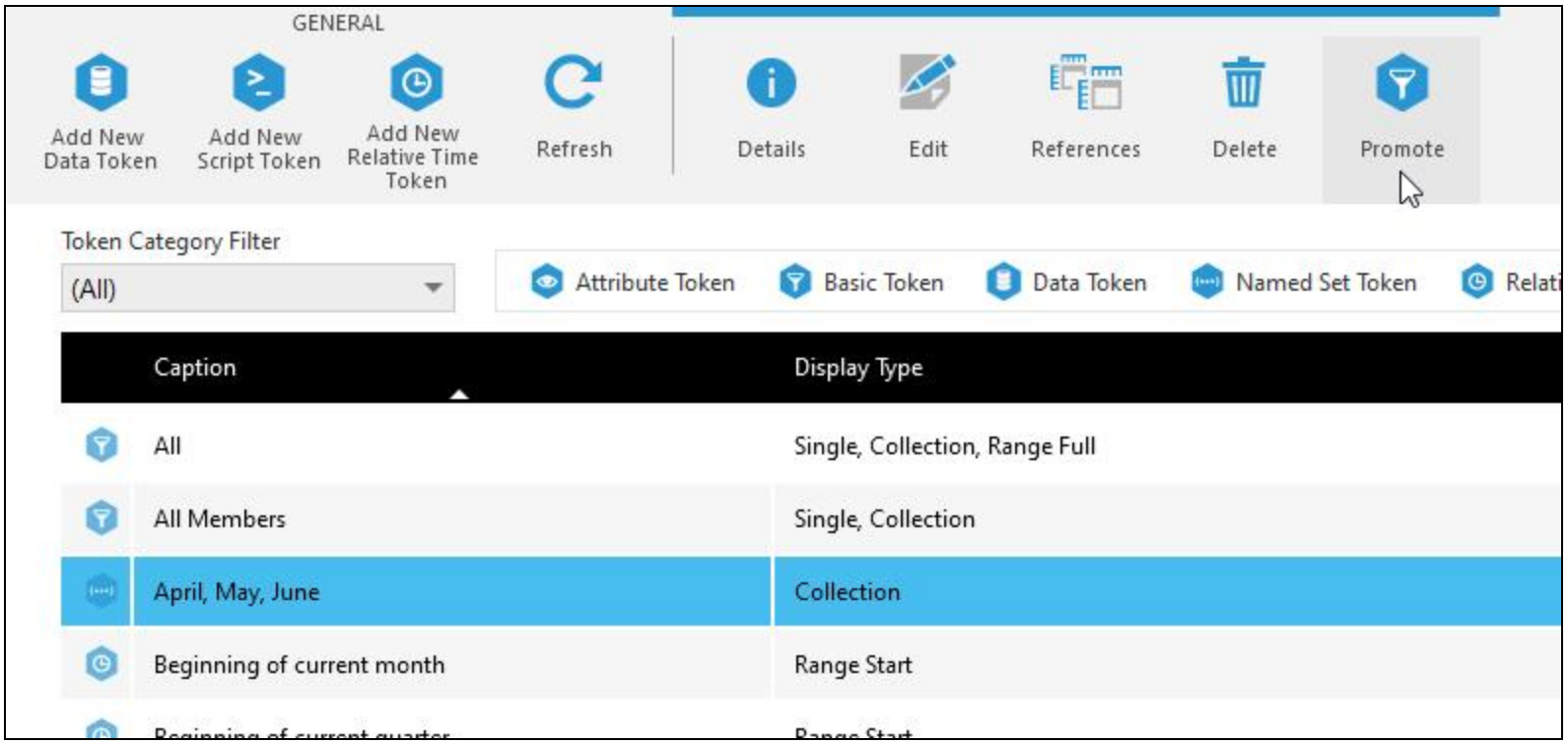
For a localized caption, enter the IETF language tag in the **Culture** field, and fill in the **Caption** field.



Promoting a Custom Token

You can promote a user created custom token to a global token.

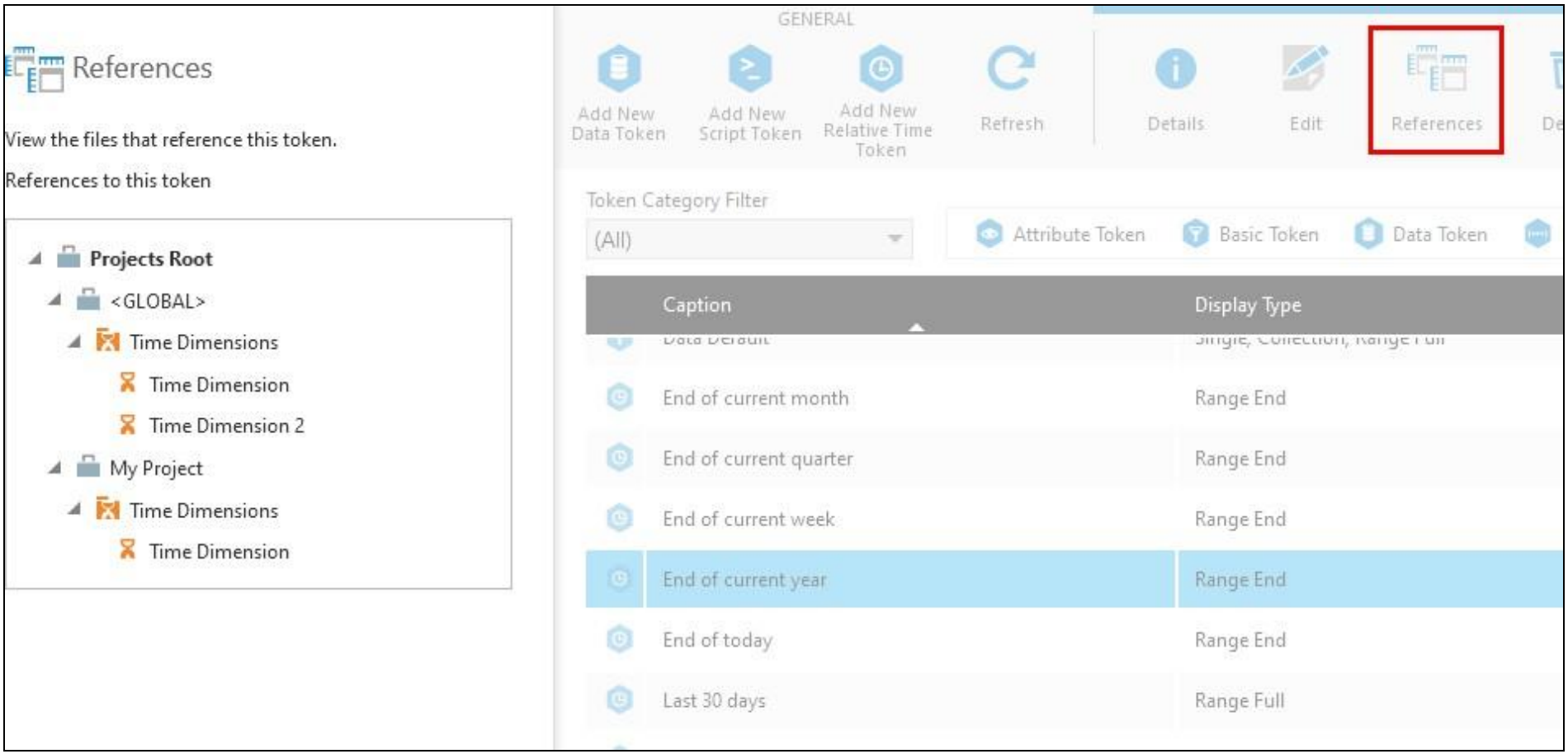
Locate and select the token from the list on the Tokens screen and click the **Promote** button on the toolbar.



Checking References

For all types of tokens other than *Basic*, you can check for any files referencing the token, such as a data cube transform parameter, a metric set's filtering, or a Parameters or filter. This can tell you, for example, whether it's safe to delete the token.

Select a token and choose **References** in the toolbar. The *References* dialog will list files using the token, similar to the dialog you can access from a file's properties.



For custom attribute tokens, if you want to find instead which accounts/groups have values assigned to this custom attribute, you can check the references of the custom attribute directly.

For more information, see:

- Use the Administration Homepage
- Adding Filters
- Creating Custom Tokens

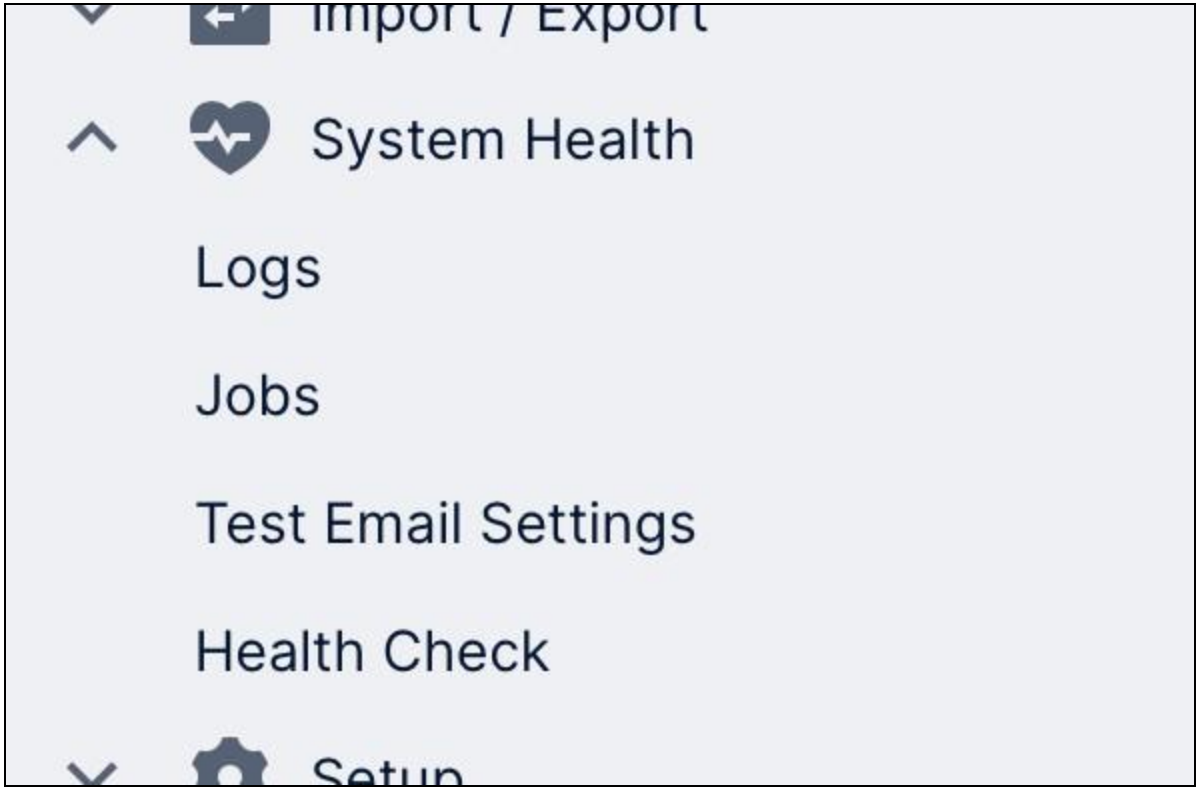
- Manage Users in Symphony
- Multi-Tenancy in Symphony
- Import and Export a Project
- Use Custom Attributes to Filter Data by User
- Using the Filter Transform With Tokens

Monitoring System Health

This applies to: *Managed Dashboards, Managed Reports*

Use the System Health options in the administration interface to:

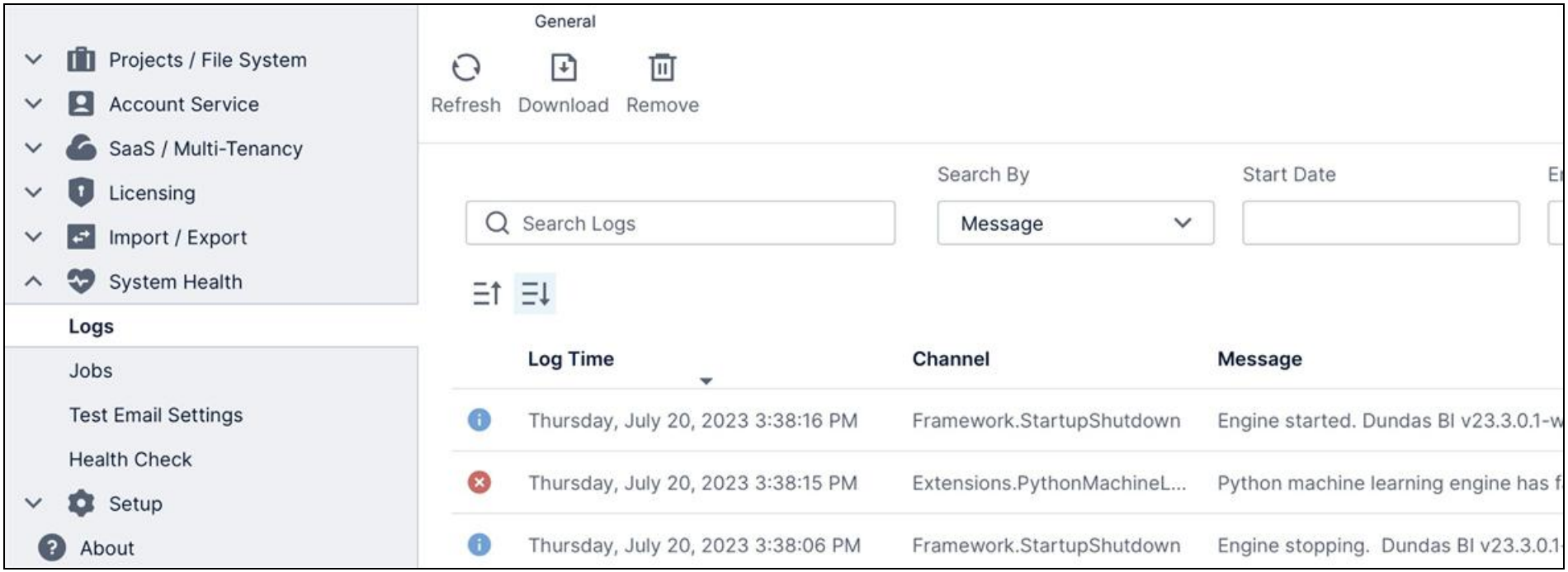
- Examine the application log for any errors or warnings
- Manage running and scheduled jobs as detailed below, including data cube storage and notifications
- Verify email settings by sending a test email
- Run health check and fix identified issues



Viewing Logs

The application log can help you to troubleshoot operational warnings or errors.

See Application Logs for details on accessing the log and configuring log filters.



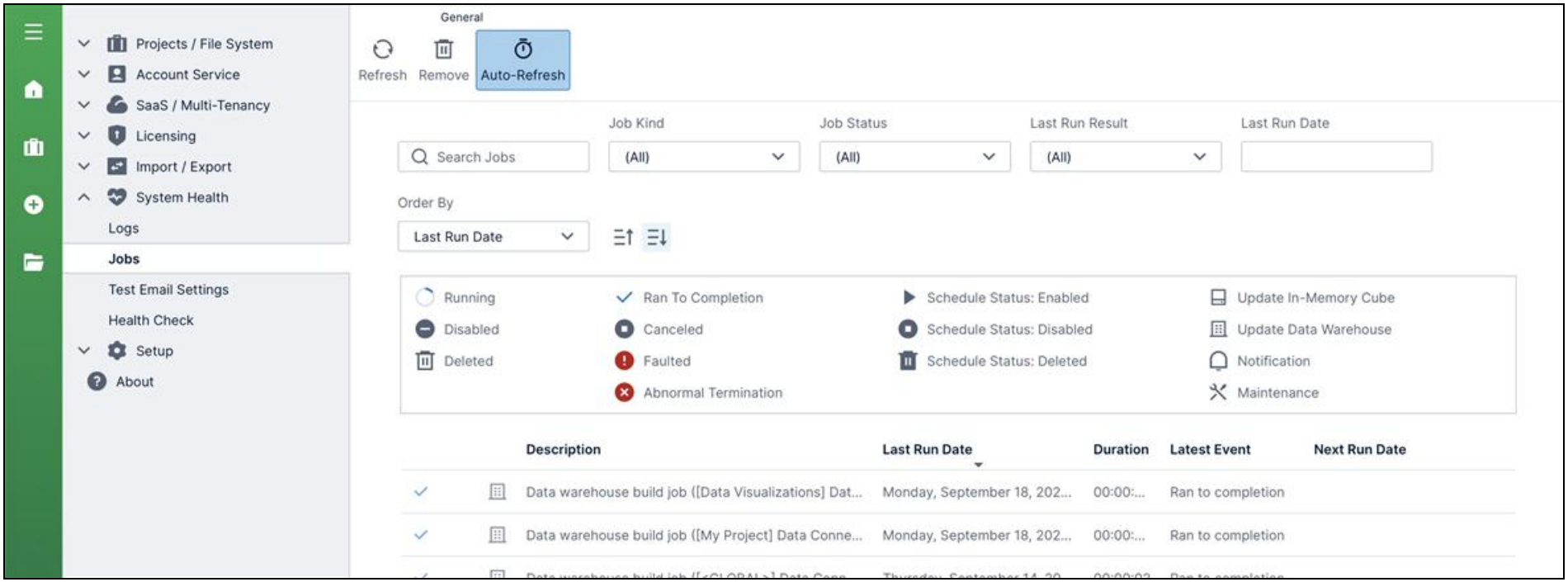
Managing Jobs

View All Jobs

Click to expand **System Health** along the left side of the administration area, then click **Jobs** to monitor the status of past, scheduled, and currently running jobs. The following kinds of jobs can be listed:

- Update In-Memory Cube – Builds in-memory storage for a data cube. May also be a sequence job that builds storage for multiple cubes as a batch.
- Update Data Warehouse – Builds data warehouse storage for a data cube. May also be a sequence job that builds storage for multiple cubes as a batch.
- Notification – Execution of scheduled notifications including data-driven notifications.

- Maintenance – Built-in jobs that can perform regular maintenance, performed by the system service:
  - *System cleanup* – Deletes expired records from the application database (log entries, performance statistics, usage tracking data, etc.). Control the frequency of the cleanup job and the expiry interval of the records in advanced configuration settings, or from the toolbar when viewing the job details.
  - *Rebuild indexes* – Rebuilds the indexes in the application and warehouse databases to avoid index fragmentation. Schedule or disable/enable the job from the toolbar when viewing the job details.
  - *Health checks* – Runs health checks automatically at the scheduled interval, and can automatically fix issues and/or email the configured maintainer email address in case of issues. View the job details to enable and schedule the job, and set it up using the *Health Check* category of configuration settings.



Jobs are listed in a table providing the following information:

- An icon indicating the result of the last job run.
- An icon indicating the status of a job (idle, running, disabled, deleted).
- An icon indicating the kind of job (in-memory, data warehouse, notification, cleanup).

- A description of the job.
- The tenant the job is associated with if applicable.
- The last run date and time.
- The last run duration.
- A description of the latest event.
- The next run date and time.

The legend above explains what each icon means, or you can hover over (or long-tap) an icon in the table to see a descriptive tooltip.

Note: Jobs interrupted by a server shut down will by marked as *Abnormal Termination* by the Cleanup job. Seat Types

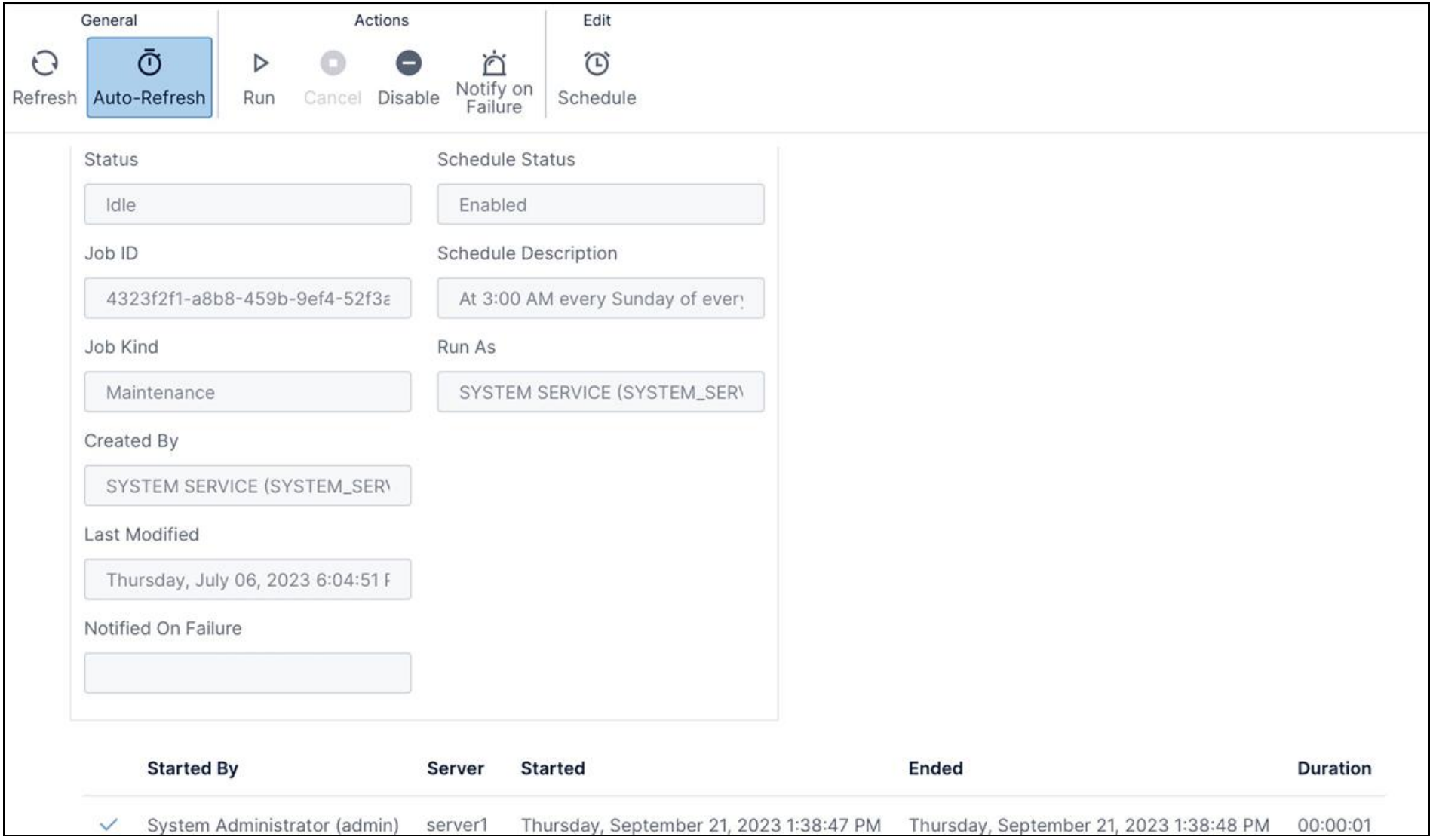
Filter and Sort Jobs

Use the options at the top of this page to help you find certain jobs:

- **Search Jobs** by their description or ID. Descriptions often include project and data cube names, for example.
- Use the drop-downs to filter by **Job Kind** or **Job Status**.
- Click the **Last Run Date** box and use the calendar to choose a specific date for filtering the job entries. For example, you can easily click to show only jobs that ran **Today**.
- Use the **Order By** drop-down to sort the jobs by the last run date or the job creation date. The buttons after this let you switch between ascending or descending order.
- If your instance is using multi-tenancy, click **Select tenant** to choose a tenant and view only the jobs specific to that tenant.

View and Edit Job Details

From the main Jobs page, click to select a job in the list and then click **Details** in the toolbar to access its details including its run history. You can also double-click or right-click to open the details.



In the job details toolbar, you can:

- Manually **Run** the job or **Cancel** it if it's currently running
- **Disable** a job. This button acts as a toggle and is highlighted if the job is disabled.

- When the Job Failure Email Policy is set to notify the *Job Maintainer*, click to **Notify on Failure** a particular user that you choose. This user is then displayed in the corresponding field in the details listed below. If there is a parent job, click **View Parent Job** first and set the job maintainer on it instead.

- Modify the schedule of any scheduled job. If this job is for data cube storage for a specific tenant when using tenant overrides, you can optionally create a schedule for the tenant separate from the main parent job that otherwise runs for all tenants.

- Disable **Auto-Refresh** while viewing this page if you prefer, otherwise the job details will be automatically refreshed every several seconds.

A table lists each time the job has run, including if one is in progress as indicated by an animated icon.

There are additional details about each time a job has run, which you can view by selecting a job run from the list and clicking **Details** in the toolbar.

Maintenance Job Run Details

Refresh

Job Run ID	Server
94	server1
Job ID	Started
4323f2f1-a8b8-459b-9ef4-52f3a79143(	Thursday, September 21, 2023 1:38:47 P
Run As	Ended
SYSTEM SERVICE	Thursday, September 21, 2023 1:38:48 P
Started By	Duration
System Administrator	00:00:01
	Result
	Ran To Completion

Job Run Events

Started Canceled Faulted Message Ran To Completion

A dialog opens with job run details, including a list of events that have occurred while running the job. The list of events may include details about its progress, or an error message if there was a failure.

Click the **View** icon for an event to view the entire message or to copy it. Click the **Close** button at the bottom of the dialogs to return to the job details. To return to the list of all jobs, go back using your browser or click **Jobs** again in the sidebar to the left.

Clear Old Job Data

By default, the data associated with a job is cleared automatically based on the *Job Data Maximum Age* configuration setting. This is set to 30 days initially, which means job data is cleared once it becomes older than 30 days.

If you want to manually clear job data yourself, you can do so from the main Jobs screen by clicking **Remove** in the toolbar.

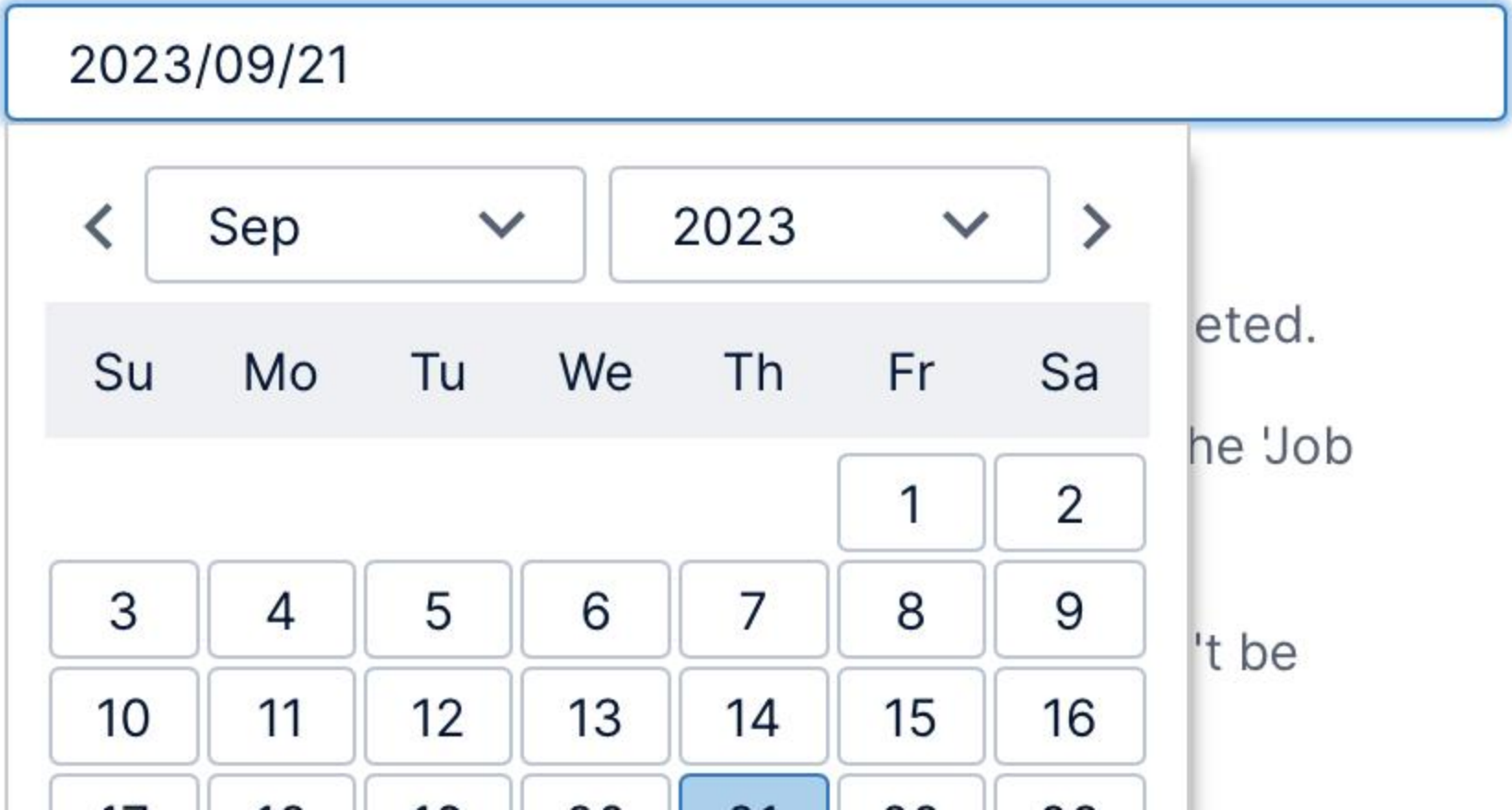
In the *Remove Job Data* dialog, click the box under **Remove before**, and then use the calendar to select a date. All job data older than this date will be cleared. Click **Submit** to clear the data.

Remove job data

Removes old job data that occurs before the specified date.

Data is removed independently of any filters configured in the main screen.

Remove before



eted.

he 'Job

't be

Configure Job Failure Emails

Users can be notified by email when a job fails by setting up the *Job Failure Email Policy* in the application configuration settings. This can be set to notify any combination of:

- The Application Maintainer (this is either the built-in *System Administrator* user, or the address from the *Maintainer Email Address* configuration setting if set).
- The creator of the job (for data cube storage, this may be the user that created the data cube or first set up its storage – to confirm, you can view a job's details).
- The runner of the job when run manually, otherwise the creator of the job can be notified instead when scheduled.
- A designated job maintainer, which can be set for each job from its details page in administration, by developer users when editing a data cube using storage, or when any user sets up a notification that runs on a schedule.

There is also an advanced setting *Job Failure Email Throttle Period* that can prevent multiple emails from being sent within the specified period.

Automatically Retry Jobs

You can set up your application instance so that failed jobs are automatically retried up to the specified total number of attempts. For example, a data cube storage job might have failed only due to an intermittent database connection issue and could be successful if attempted again.

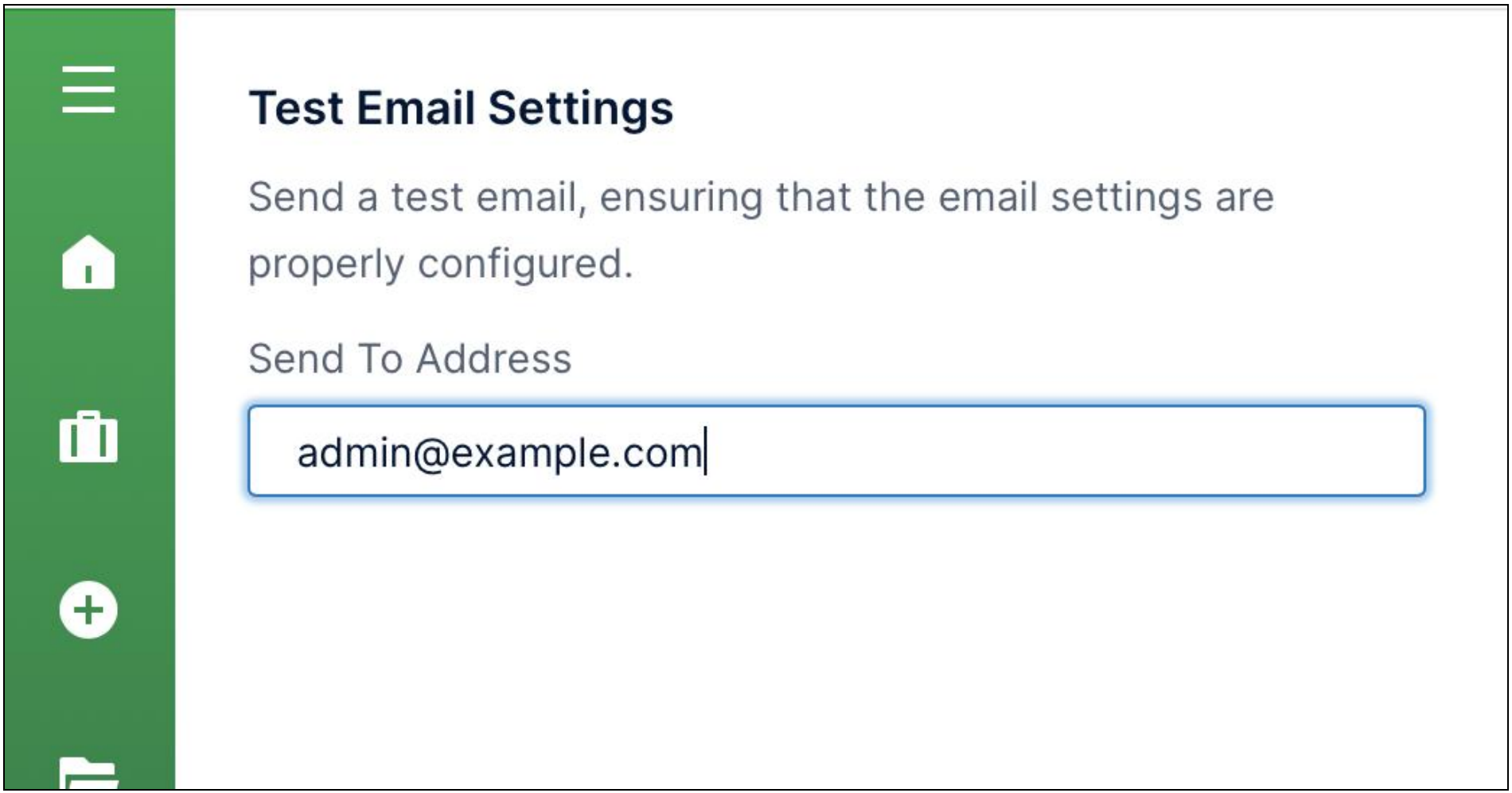
In configuration settings, set the *Job Execution Attempts Count*. A job failure email will only be sent if all attempts failed.

Testing Email Settings

Email settings must be configured properly in order for certain features such as notifications to work properly.

To check your email settings, expand the System Health options and click **Test Email Settings**.

Type an email address to receive a test email and then click **Submit**.



Check the appropriate inbox for the test email which will have the subject line: *Symphony test email*.

Health Check

Your application instance can automatically check itself for potential issues, and provide you with details and the option to fix issues automatically.

For details, see Health Check. To schedule health checks to run themselves automatically and fix or report on issues, see the details above about this built-in maintenance job.

For more information, see:

- Application Logs
- Configuration Settings
- Notification Options
- Data Cube Data Storage Options
- Health Check

Override Config Settings Using an XML File

This applies to: *Managed Dashboards, Managed Reports*

This article shows you how to override configuration settings in Symphony using an XML file.

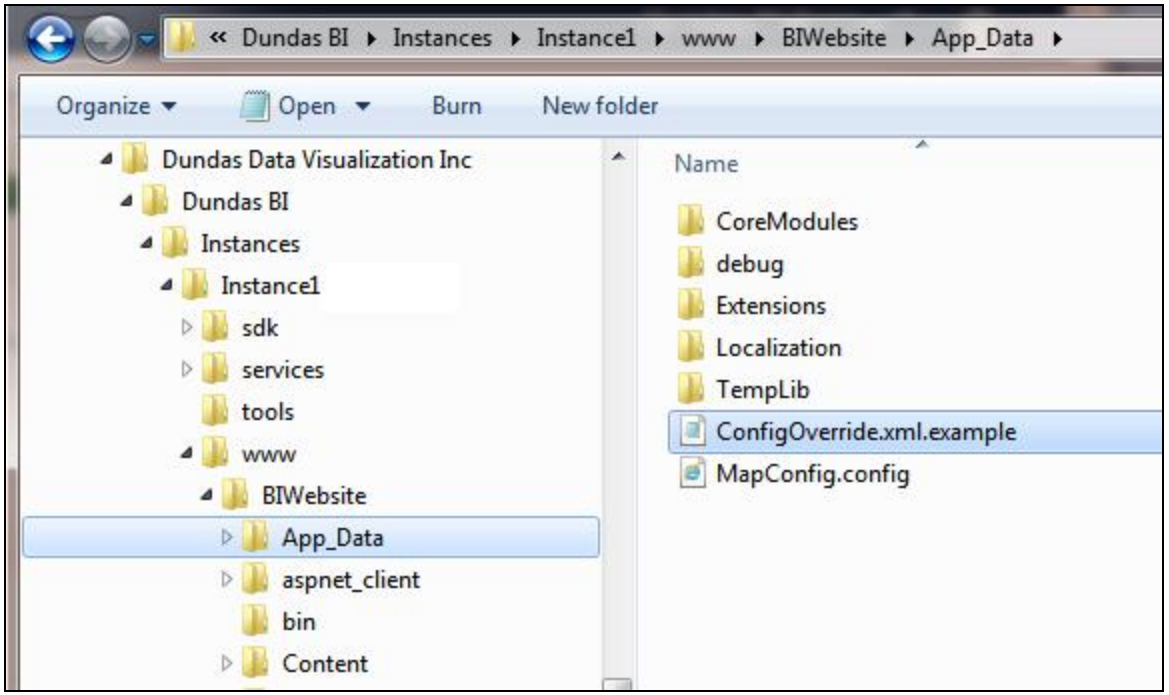
This is a failsafe option in case the application won't start due to some invalid configuration settings.

In most cases though, it is recommended to use the dt.exe command line tool instead if you need to change a configuration setting outside of the Symphony administration user interface.

ConfigOverride.xml

To override configuration settings, create a *ConfigOverride.xml* file and place it in the *www\BIWebsite\App_Data* folder of your Symphony instance.

In a default installation of Symphony, there is a sample file you can start off with named *ConfigOverride.xml.example*. Just rename this file to *ConfigOverride.xml* by removing the *.example* extension. Then edit the file and make changes to one or more settings. Note that you may need to adjust the security permissions on the file in order to save changes to it.



Example contents of XML file for changing the Internal Application URL config setting:

```
<Config>
	<Module Id="EC04F56F-AAD2-4395-BCB3-35F5B1D0C8F1" Name="Core">
		<Setting Name="InternalApplicationUri">http://localhost:50300/</Setting>
	</Module>
</Config>
```

Here's another example which changes the Default Culture config setting:

```
<Config>
	<Module Id="EC04F56F-AAD2-4395-BCB3-35F5B1D0C8F1" Name="Core">
		<Setting Name="DefaultCulture">fr-FR</Setting>
	</Module>
	<Module Id="21259d43-ee4c-4b06-b73f-c9c2cdce60c6" Name="Web">
	</Module>
</Config>
```

The name for a particular configuration setting is not always the same as its display name in the Admin UI. To be sure you've got the right name in the XML file, look for the configuration setting in the .NET API documentation: CoreConfigSettingsIds Class.

Once you've completed changes to the config file, restart the Symphony website/app pool.

Note: An empty, self-closing setting tag (for example, *<Settng Name="DefaultCulture" />*) will cause the application to use the default value for the setting.

For more information, see:

- Configuration Settings
- Set a Configuration Value From the Command Line

Perform a Health Check Using the Command Line

This applies to: *Managed Dashboards, Managed Reports*

This article shows you how to perform a health check on the Symphony application from a command line, rather than using the Health Check UI.

Perform a Health Check Using dt

The dt command line tool is a utility included with Symphony which can be used to perform various administration and configuration tasks.

The **healthCheck** command checks the Symphony application and its databases for any errors or inconsistencies. The output from dt is color-coded to indicate the severity of items found. There is also an option to fix any errors that are detected.

View the Help Page for healthCheck

On the server where Symphony is installed, open a command prompt or terminal and navigate to the tools folder. For details, see Using the dt Command Line Tool.

Type *dt help healthCheck* (or *./dt.sh help healthCheck* on Linux) to get the help page for this command.

> **Note:** The /fixErrors option doesn't mean that the error or warning will always be fixed. For example, you may need to install a Microsoft hotfix manually to resolve an error, or investigate why a data connector can't connect to a data source.

The available checks you can run (or ignore) are listed in the Health Check article.

Run the Health Check

Here is an example of running all health checks:

```
C:\Program Files\Dundas Data Visualization Inc\Dundas BI\Instances\Instance1\tools>dt.exe healthCheck

Dundas BI Tools version 5.0.0.1
Copyright (c) 2017 Dundas Data Visualization Inc. All rights reserved.

[2016-02-19 16:01:32.521] [Info] [Framework.StartupShutdown] 0: Engine started
[2016-02-19 16:01:32.848] Beginning health check.
[2016-02-19 16:01:33.694] Running check: DBI0010:Check Application DB Connectivity
-> Ensures that the application can connect to the Application Database.
[2016-02-19 16:01:33.696] Successfully connected to the Application database. [2016-02-19 16:01:33.697] Check complete
(DBI0010).
[2016-02-19 16:01:33.702] Running check: DBI0011:Check Warehouse DB Connectivity
```

```
-> Ensures that the application can connect to the Warehouse Database.
[2016-02-19 16:01:33.711] Successfully connected to the Warehouse database. [2016-02-19 16:01:33.711] Check complete
(DBI0011).
[2016-02-19 16:01:33.712] Running check: DBI0020:Check App DB Settings
-> Ensures that various settings related to the application database are correct.
[2016-02-19 16:01:33.716] [Err] For security reasons, it is strongly recommended that SQL Server authentication be used
(instead of Inte grated Security) for connections to the Application database.
[2016-02-19 16:01:34.006] ALLOW_SNAPSHOT_ISOLATION enabled.
[2016-02-19 16:01:34.007] READ_COMMITTED_SNAPSHOT detected.
[2016-02-19 16:01:34.007] Case-sensitive collation detected.
[2016-02-19 16:01:34.008] Check complete (DBI0020).
[2016-02-19 16:01:34.009] Running check: DBI0021:Check Warehouse DB Settings
-> Ensures that various settings related to the warehouse database are correct.
[2016-02-19 16:01:34.010] [Err] For security reasons, it is strongly recommended that SQL Server authentication be used
(instead of Inte grated Security) for connections to the Warehouse database.
[2016-02-19 16:01:34.040] ALLOW_SNAPSHOT_ISOLATION enabled.
[2016-02-19 16:01:34.040] READ_COMMITTED_SNAPSHOT detected.
[2016-02-19 16:01:34.041] Case-sensitive collation detected.
[2016-02-19 16:01:34.042] Check complete (DBI0021).
[2016-02-19 16:01:34.045] Running check: DBI0100:Check for ADSI Hotfix 2683913
-> Ensure that the hotfix for Microsoft KB 2683913 is installed, to prevent random exceptions from being thrown when
calling Active Direct ory functionality
[2016-02-19 16:01:34.793] [Err] A hotfix from Microsoft is required in order to ensure that calling Active Directory
functionality does n't result in unexpected random errors. You can download the hotfix from:
https://support.microsoft.com/en-us/kb/2683913.
[2016-02-19 16:01:34.795] Check complete (DBI0100).
[2016-02-19 16:01:34.796] Running check: DBI0210:Invalid Checked-Out References
-> Finds references from checked-out entities where the corresponding entity is not actually checked-out. [2016-02-19
16:01:34.820] Check complete (DBI0210).
[2016-02-19 16:01:34.821] Running check: DBI0211:Mark Inactive Entries
-> Finds transient subentries which are no longer referenced by the latest revision of their parent entity, and marks them
as inactive. [2016-02-19 16:01:35.228] Check complete (DBI0211).
[2016-02-19 16:01:35.229] Running check: DBI0212:Detect Invalid Project IDs
-> Finds entries whose project ID does not match the ID of the project under which the entry resides. [2016-02-19
16:01:35.771] Check complete (DBI0212).
[2016-02-19 16:01:35.772] Running check: DBI0213:Invalid Checked-Out Entity Data
-> Finds checked-out data for entities which are not actually checked-out. [2016-02-19 16:01:35.791] Check complete
(DBI0213).
[2016-02-19 16:01:35.792] Running check: DBI0214:Fix Invalid Inactive Entries
-> Finds inactive subentries which should not be inactive. [2016-02-19 16:01:35.836] Check complete (DBI0214).
[2016-02-19 16:01:35.837] Running check: DBI0215:Find Entities with Missing Data
-> Locates entities which are missing their underlying data. [2016-02-19 16:01:35.863] Check complete (DBI0215).
[2016-02-19 16:01:35.864] Running check: DBI0216:Invalid Subentry Revisions
-> Finds subentries whose current revision doesn't match that of their corresponding primary entry. [2016-02-19
```

```
16:01:35.876] Check complete (DBI0216).
[2016-02-19 16:01:35.877] Running check: DBI0300:Orphaned Account Data
-> Finds (and optionally deletes) account-related data corresponding to accounts which no longer exist. [2016-02-19
16:01:35.879] Checking File System MRU
[2016-02-19 16:01:35.973] Checking Notifications
[2016-02-19 16:01:35.994] Checking Custom Data Tokens
[2016-02-19 16:01:35.996] Checking Logon Cache
[2016-02-19 16:01:35.997] Checking Logon and Password Tokens [2016-02-19 16:01:35.998] Checking User Data
[2016-02-19 16:01:36.001] Checking Data Source Credentials
[2016-02-19 16:01:36.004] Checking Sessions
[2016-02-19 16:01:36.009] Checking Group Memberships
[2016-02-19 16:01:36.089] Checking User Projects
[2016-02-19 16:01:36.109] Check complete (DBI0300).
[2016-02-19 16:01:36.109] Running check: DBI1000:Check reports and scorecards for upgrade
-> Ensures that reports and scorecards have been properly upgraded from version 1. [2016-02-19 16:01:36.371] Check complete
(DBI1000).
[2016-02-19 16:01:36.371] Running check: DBI2000:Detect Unused Warehouse Tables
-> Finds warehouse tables that are not in use. [2016-02-19 16:01:36.581] No unused tables.
[2016-02-19 16:01:36.583] Check complete (DBI2000).
[2016-02-19 16:01:36.584] Running check: DBI2010:Detect Invalid Default Time Dimensions
-> Finds projects whose specified default time dimension couldn't be found in the system. [2016-02-19 16:01:36.659] Check
complete (DBI2010).
[2016-02-19 16:01:36.659] Health check complete; 16 check(s) run, 3 error(s), 0 warning(s).
[2016-02-19 16:01:36.686] [Info] [Framework.StartupShutdown] 0: Engine stopping C:\Program Files\Dundas Data Visualization
Inc\Dundas BI\Instances\Instance1\tools>
```

For more information, see:

- Using the dt Command Line Tool
- Health Check

Set a Configuration Value From the Command Line

This applies to: *Managed Dashboards, Managed Reports*

This article shows you how to set the value of a configuration setting in the Global scope using the dt command line tool.

You can also use the */reset* argument to reset the setting's values in all scopes and scope targets such as servers.

View the Help Page

On the server where Symphony is installed, open a command prompt or terminal and navigate to the tools folder containing the dt tool. For details, see Using the dt command line tool.

In the command prompt window, *dt help setConfigValue* to get the help page for this command.

```
c:\Program Files\Dundas Data Visualization Inc\Dundas BI\Instances\Instance1\tools>dt help setConfigValue
Dundas BI Tools version 8.0.2.1001-20210416211709
Copyright (c) 2021 Dundas Data Visualization, Inc. All rights reserved.

Sets the global value or resets all scope and target values of a configuration setting.

Syntax:
dt.exe setConfigValue [/appcs:<application database connection string>] [/appStorage:<application database server type>]
                      [/settingId:]<setting identifier> [/value:<new value>] [/reset]

       <application database connection string> - The application database connection string. If not specified, the value will be
taken from the dbi.config file located in the App_Data folder specified in the dt.exe.config file. The argument is
optional.
       <application database server type> - The application database server type. If not specified, the value will be taken from
the dbi.config file located in the App_Data folder specified in the dt.exe.config file. The argument is optional. Valid
values: "SqlServer", "Postgres".
       <setting identifier> - A string identifying the configuration setting. This may be the setting ID (in the case of core or
extension settings), or for other settings, in the format "moduleId:settingName". The argument is mandatory. Specifying the
argument name is optional.
       <new value> - The new value of the setting. Mandatory except when /reset argument is specified. The argument is optional.
       /reset - If specified, resets the setting to the default value in all its scopes and scope targets.

Basic Example:
dt.exe setConfigValue c6e739e5-a58a-49af-be1b-92b1f0fa62a2

Full Example:
dt.exe setConfigValue /appcs:"Data Source=localhost; Initial Catalog=DundasApp; Integrated Security=True"
/appStorage:SqlServer c6e739e5-a58a-49af-be1b-92b1f0fa62a2 /value:"abc" /reset
```

```
c:\Program Files\Dundas Data Visualization Inc\Dundas BI\Instances\Instance1\tools>
```

Get the Setting Identifier

You can specify the setting identifier in two ways:

1. As the ID of the setting.
2. As a string in the form of *moduleID:settingName*.

Setting ID

Each configuration setting has a unique ID (GUID string). For example, the ID of the *Data Warehouse Connection String* setting is *5C42F315-99B5-4AEE- ADDF-3783E0841571*.

You can find the IDs of other Core configuration settings by looking at the remarks of the members from the CoreConfigSettingIds Class.

Module ID

Some settings are loaded via a module and require the module ID to be identified (for example, settings defined in a hosting application such as DBI Web App).

The possible modules are Core, Web, or an extension. You can find the module ID of each extension using the API.

Run dt

At the command prompt, enter the following:

```
dt setConfigValue /appcs:"your connection string" /settingId:ID of config setting /value:"new config value"
```

Example showing how to set the Data Warehouse Connection String setting using dt:

```
dt setConfigValue /appcs:"Data Source=SERVER1\;Initial Catalog='DundasBI_AppDB';Integrated Security=True"
/settingId:5C42F315-99B5-4AEE-AD DF-3783E0841571 /value:"Data Source=SERVER1\;Initial Catalog='DundasBI_WarehouseDB';User
ID=DundasUser;Password=********"
```

For more information, see:

- Configuration Settings
- How to Reset the Admin Password
- Override Config Settings Using an XML File
- .NET API: CoreConfigSettingIds Class
- Using the dt Command Line Tool
- Symphony Managed Dashboards and Reports Config File

Setting a Default Theme

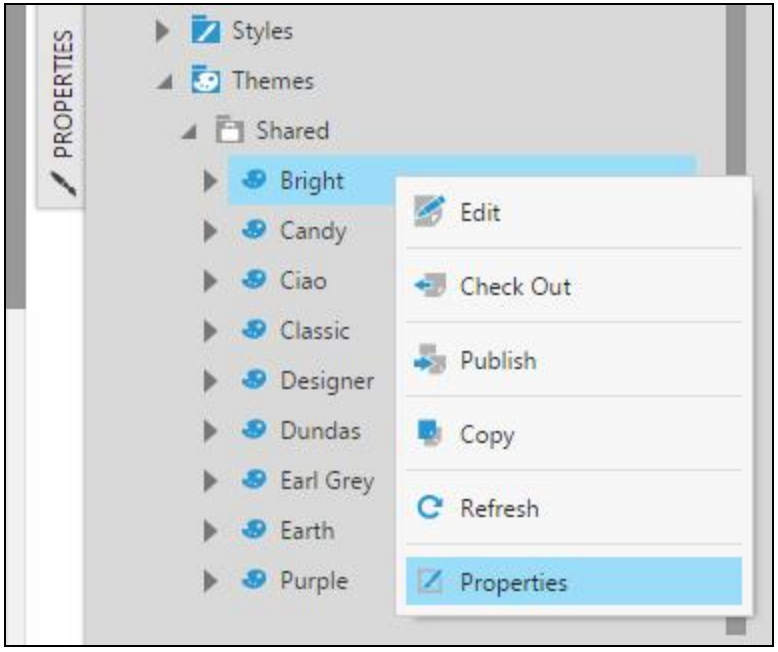
This applies to: *Managed Dashboards, Managed Reports*

Administrators can configure Symphony so that a default theme is applied when first creating visualizations, components, and filters, to customize their default colors and other appearance. This includes when data is first added to a visualization, or when re-visualizing the entire visualization when editing or viewing.

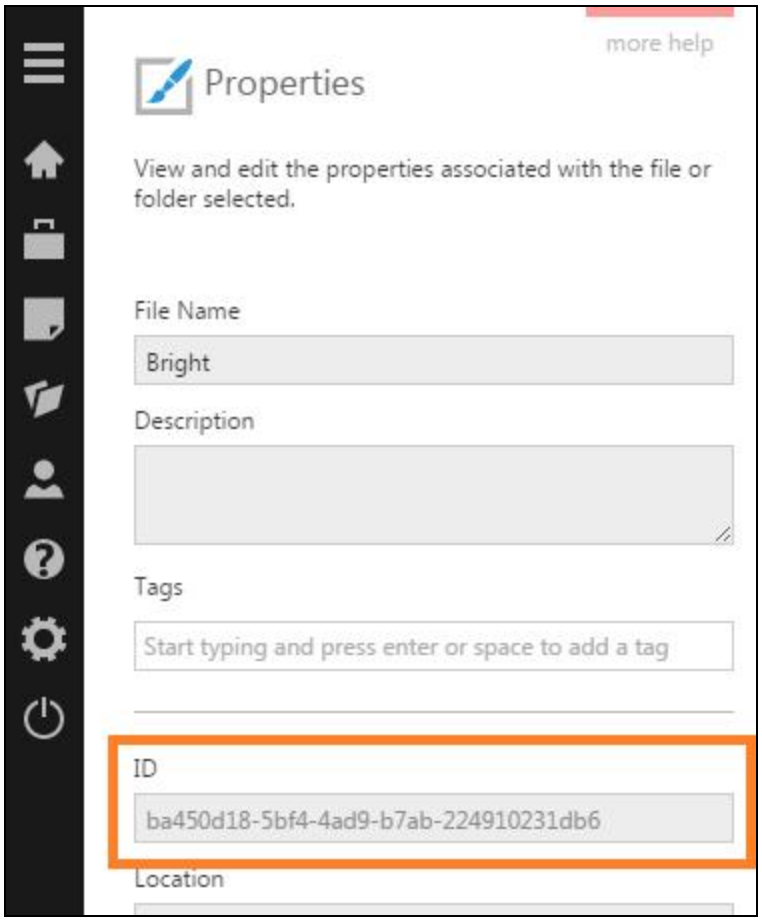
Setting the Default Theme

Get the ID of the Theme

First, right-click the desired theme in **Explore** and select **Properties**.



In the *Properties* dialog for the theme, select the text of the **ID** and copy it (press Ctrl+C) to refer to below.

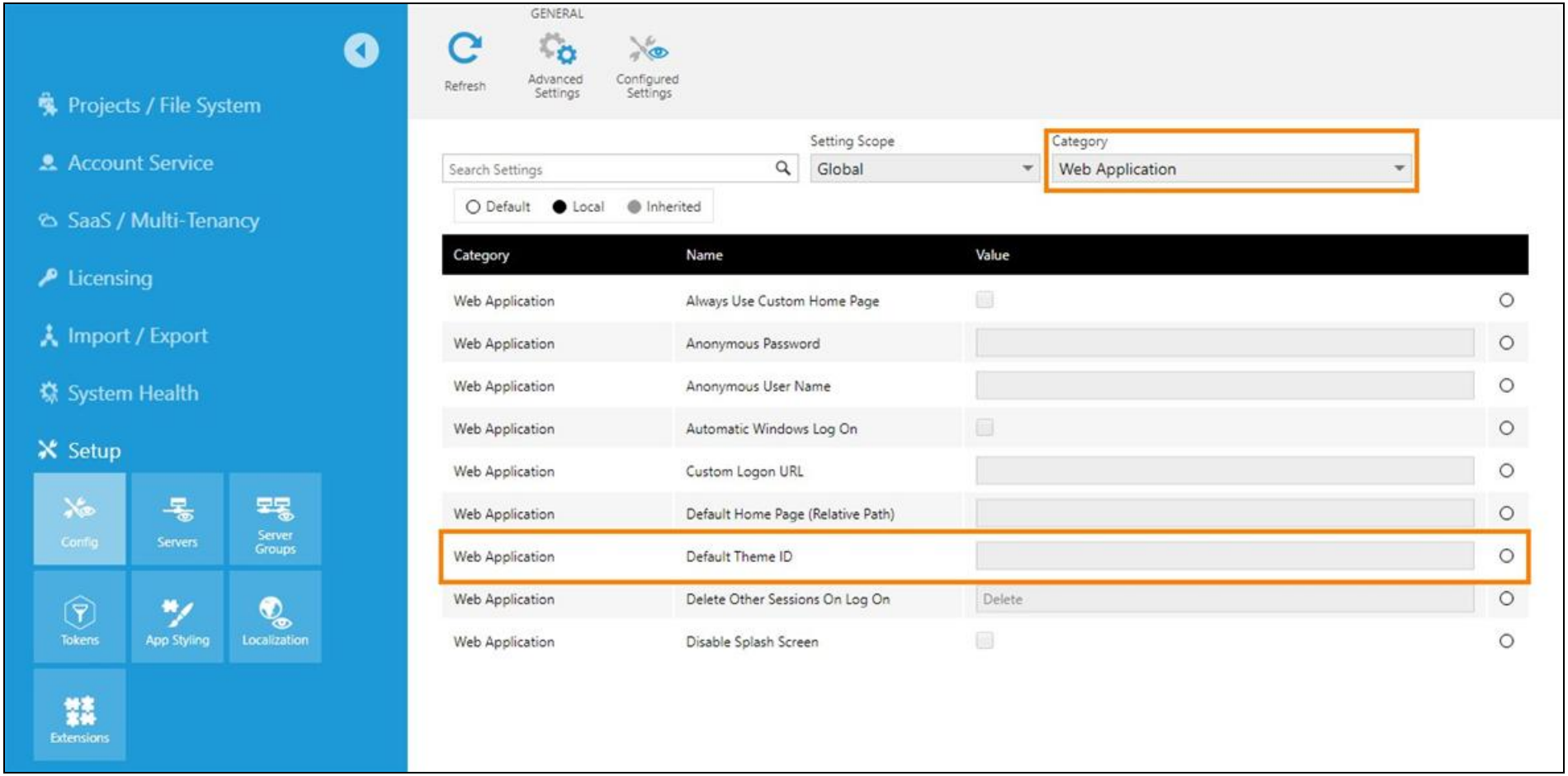


Modify the Config Setting

Access Administration from the main menu (you must be logged on as an administrator). Expand the **Setup** section and click **Config**.

In the *Application Configuration* screen, set **Category** to *Web Application*. Select the *Default Theme ID* setting and click the **Edit** icon.

In the dialog that appears, edit the setting value and paste the ID copied above (press Ctrl+V).



Now whenever a new visualization, component, or filter is added to a dashboard or other view, it will be styled by this theme (if it includes a style that can be applied to that item).

Set Up a Custom Logon URL

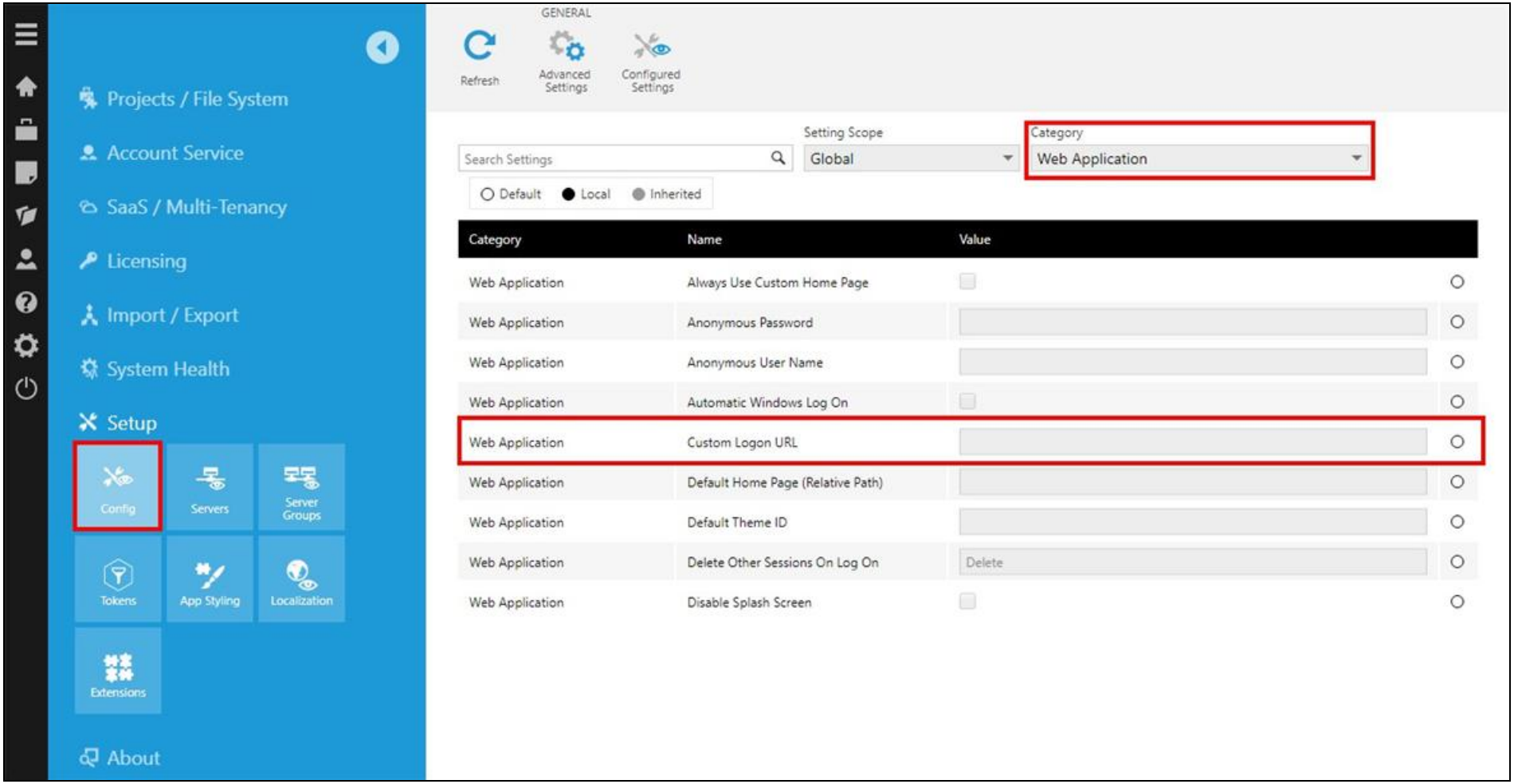
This applies to: *Managed Dashboards, Managed Reports*

The Custom Logon URL configuration setting specifies where the user should be redirected when accessing the logon page. For example, when a user logs out or their logon session times out, you may want to redirect them to a specific location.

Set Up the Configuration Setting

Access Administration from the main menu, click to expand **Setup**, then click **Config**.

Select *Web Application* from the **Category** drop-down select the **Custom Logon URL** setting and then click **Edit** on the toolbar.



Click **Edit value** and provide the target URL.

Click **Submit**.

- The original logon page is still accessible by appending `?doNotForward=true` to the query string (for example, `http://your.instance.com/LogOn?doNotForward=true`).
- The return URL is automatically appended to the query string when redirecting to the custom logon URL. This allows the custom logon page to send the user back to their previous location once they authenticate.
- When working with Multi-Tenancy, the Tenant ID can be appended to the query string (for example, `http://your.instance.com/LogOn?tenantId=092741e1-61a4-4ee8-925a-1e78a90260ad`). Furthermore, when a tenant user is logged on, the Tenant ID is appended to the query string automatically. This means the target page can be set up to redirect or re-brand for the page for each tenant based on the Tenant ID.

For more information, see:

- Configuration Settings
- How To Enable Anonymous Log On

Turn Off Automatic Saving For Views

This applies to: *Managed Dashboards, Managed Reports*

While editing a view (dashboard, report, or scorecard) in Symphony, your changes are automatically saved as needed (e.g., every 10 seconds). The status bar at the bottom of the designer screen displays a *Saved* message whenever Symphony has performed an auto-save operation.

However, there may be scenarios where you want to turn off this feature. For example, you may be building a complex dashboard with a lot elements which can take a second or two to save each time.

This article shows you how to turn off auto-saving for views and enable a **Save** button in **Edit** mode instead.

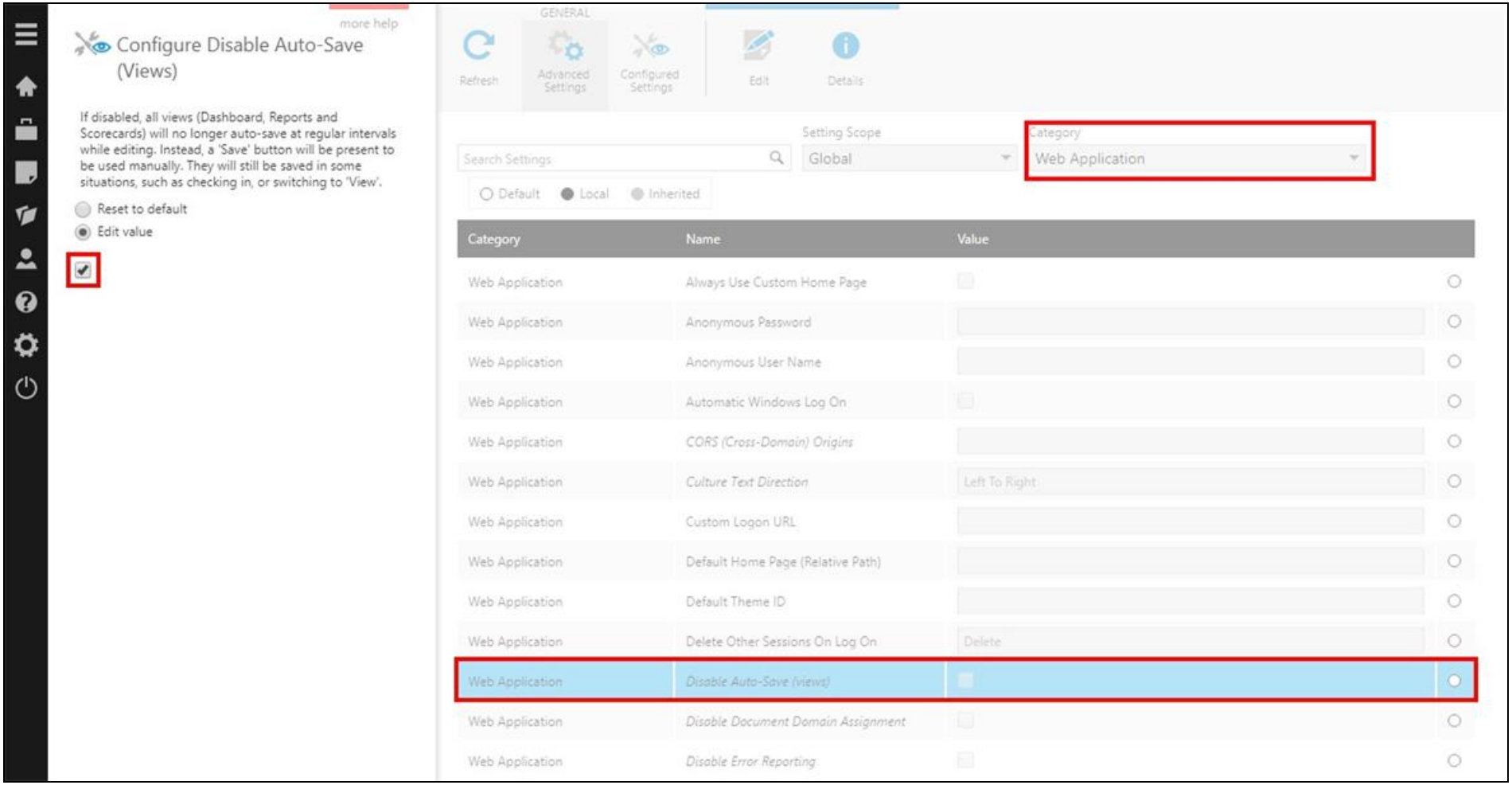
Disable Auto-Save (Views) Config Setting

Log on to Symphony as an administrator and access Administration from the main menu.

Expand the **Setup** section and click **Config**.

In the *Application Configuration* screen, set the **Category** to Web Application. Click the **Advanced Settings** icon on the toolbar to view advanced settings.

Edit the *Disable Auto-Save (Views)* configuration setting and enable it.

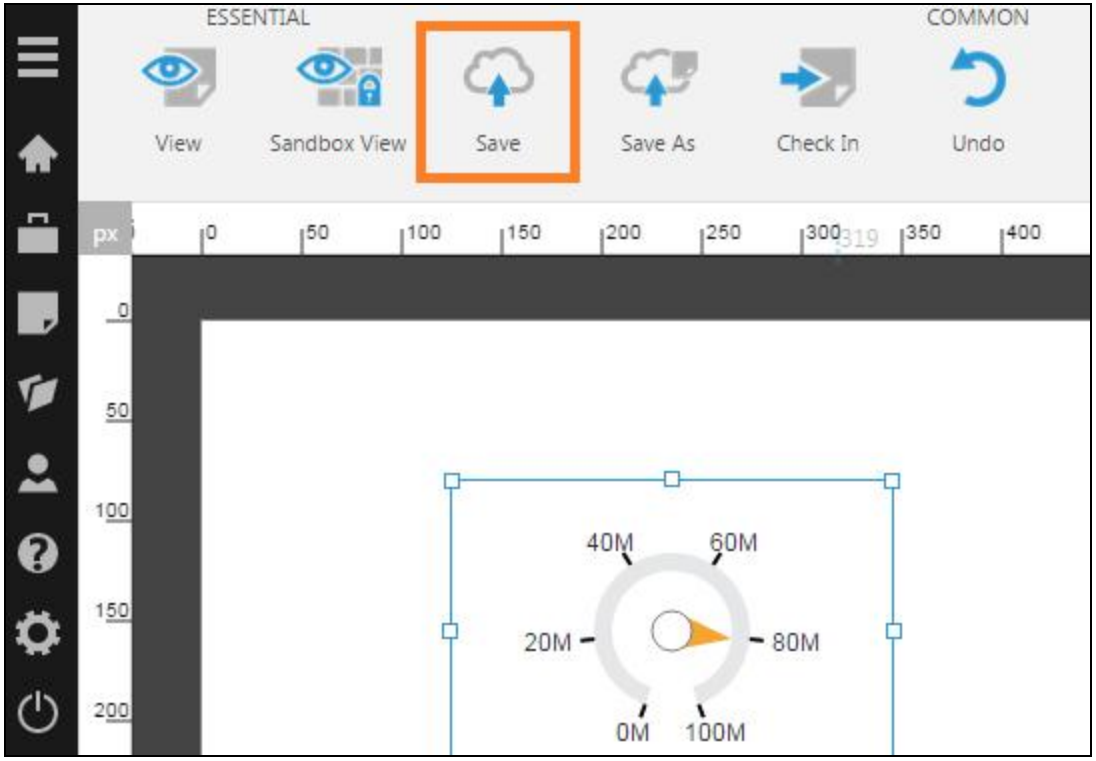


Save Button

Once the configuration setting has been modified, the following will occur while you are editing a dashboard or other type of view:

- A **Save** button appears in the toolbar while you are in Edit mode and the view has been checked out to you for editing.
- Automatic saving of the view no longer occurs except in the following situations:

- Switch from Edit mode to View mode.
- Click Sandbox View.
- Share or export the view.
- Check in the view.
- Enter or leave the Edit Full Screen option under Data Tools.



For more information, see:

- Check In, Check Out and Auto Saving
- Configuration Settings

Usage Tracking

This applies to: *Managed Dashboards, Managed Reports*

When Symphony users view a dashboard, report, or other view, some statistics are recorded in the Symphony application database. A Symphony Developer user with access to the Symphony application database can create a data cube to process these statistics into a more user-friendly format and ultimately display this information in charts, tables, or other visualizations.

The recorded statistics keep track of the view being accessed, the user who is accessing it, and the time and duration of viewing. Based on this data, it is possible to derive additional usage information such as:

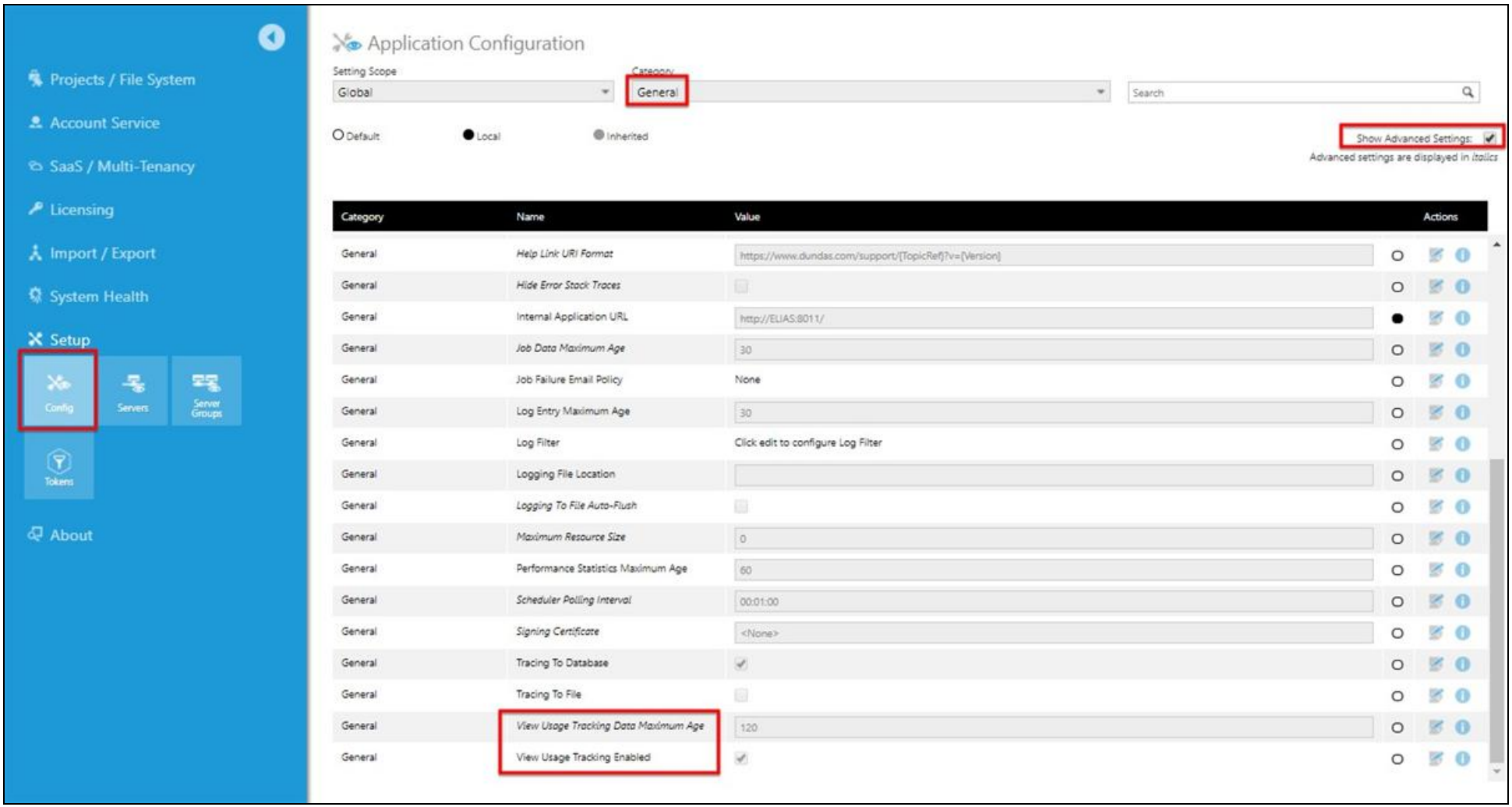
- The number of times it's viewed
- The average time spent viewing
- Time of day usage patterns

Note: Administrators can install and use the Usage Tracking Dashboard sample project, which has a dashboard as well as data cubes ready to use for exploring these kinds of statistics.

Enabling Tracking

Tracking of view usage is enabled by default in a Symphony instance. To view or change the current setting, go to Administration in Symphony and click on Config, click to show the advanced settings, and then scroll down to find:

- View Usage Tracking Data Maximum Age - Tracking data is stored for only the specified number of days
- View Usage Tracking Enabled - This is set to *True* by default

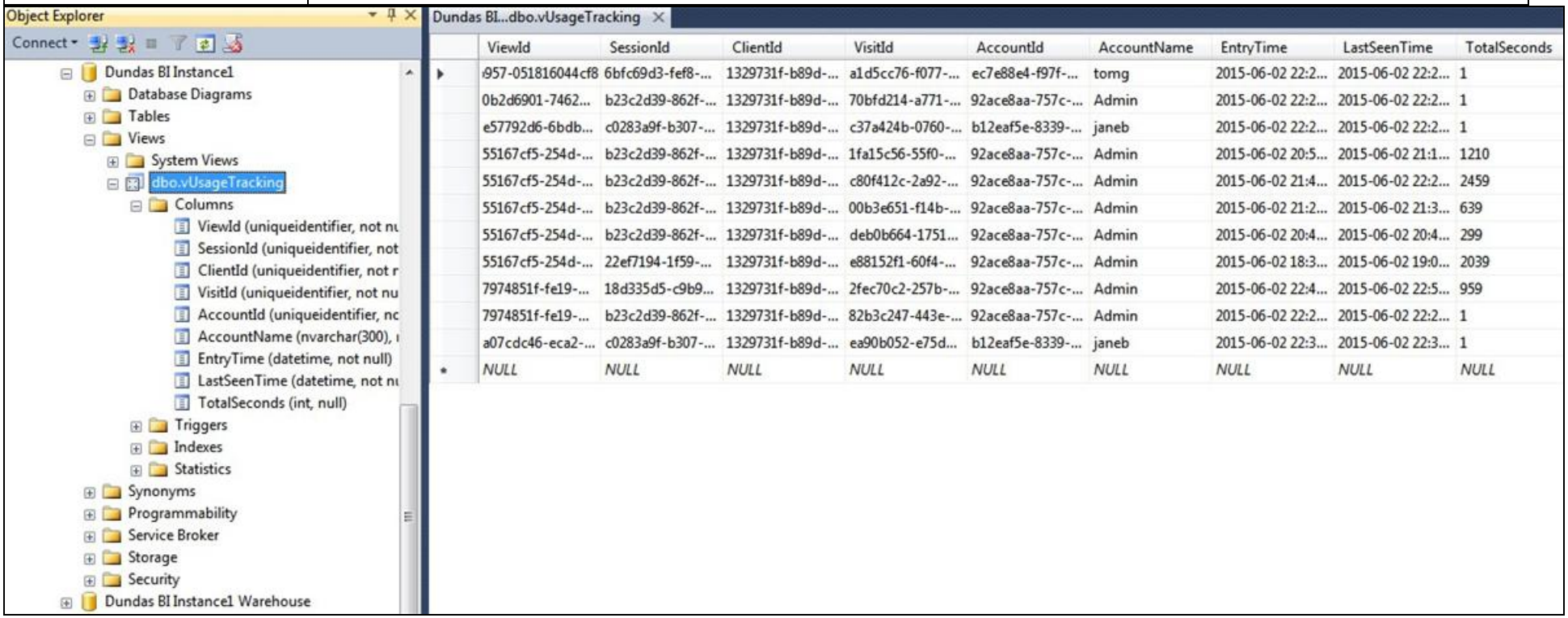


Symphony Application Database UsageTracking

When tracking is enabled, usage statistics are recorded in the Symphony application database.The basic connection details for your application database are displayed on the administration homepage.

For example, if your Symphony instance is named *Instance1*, the corresponding application database will likely be named *Symphony Instance1*. After creating a data connector to your Symphony application database on SQL Server or Postgres, the data connector's *Views* subfolder will contain a view named *vUsageTracking* with the following columns:

Column	Description
ViewId	The ID of the dashboard, report, scorecard, or small multiple being viewed.
SessionId	The ID of the user's logon session.
ClientId	This ID identifies the user's web browser.
VisitId	A unique ID identifying this tracking event.
AccountId	The ID of the user (account) that is viewing.
AccountName	The username of the user (account) that is viewing.
EntryTime	The UTC date and time the viewing began.
LastSeenTime	The UTC date and time the viewing ended.
TotalSeconds	How long the file has been viewed so far (in seconds).



Note: If a user returns to a view more than 5 minutes later than their last seen time but still within the same logon session, a new tracking event (and VisitId) is created.

FileSystemEntry Table

The usage tracking database view gives you the ID of each dashboard, report, and other view file in Symphony that is being accessed. In order to extract more user-friendly information, such as the name of each view, you need to also use the *FileSystemEntry* table in the Symphony application database.Using the FileSystemEntry table, you can look up the names of files in the Explore window based on their IDs. Files such as dashboards, projects, data cubes, and metric sets can all be found in this table. You can determine the ID of any file in the Explore window or Admin File Explorer by right-clicking on the file and opening its properties dialog. Below are some of the columns from the FileSystemEntry table:

Column	Description
Id	The ID of a file such as a dashboard, report, data cube, or metric set.
Name	The name of the file (e.g., dashboard name, report name, data connector name).
ProjectId	The ID of the project containing this file. You can look up the ID in this same table in order to get the name of the project.

Important: This table and others in the Application database are critical to the operation of Symphony. Do not modify these tables.

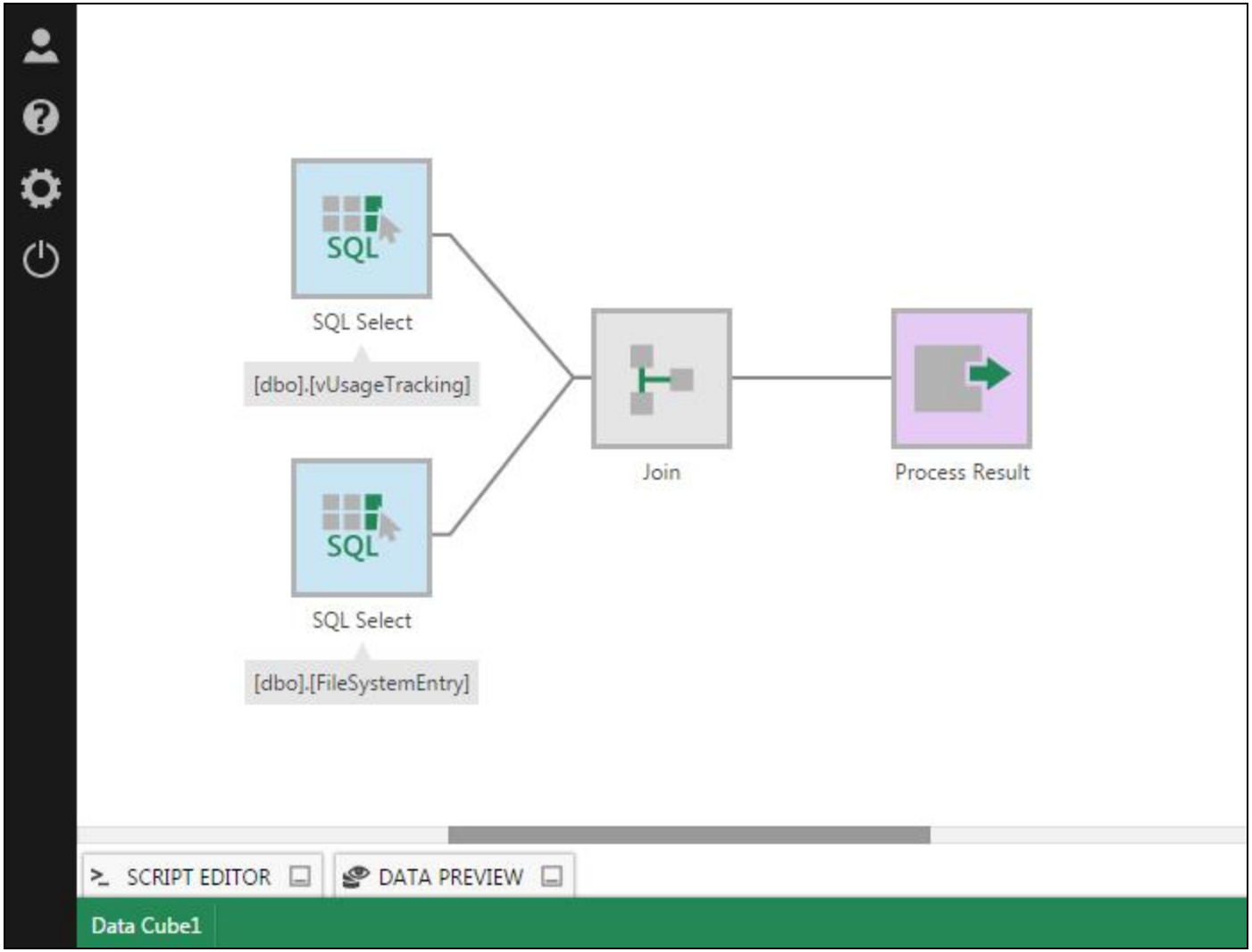
Examples

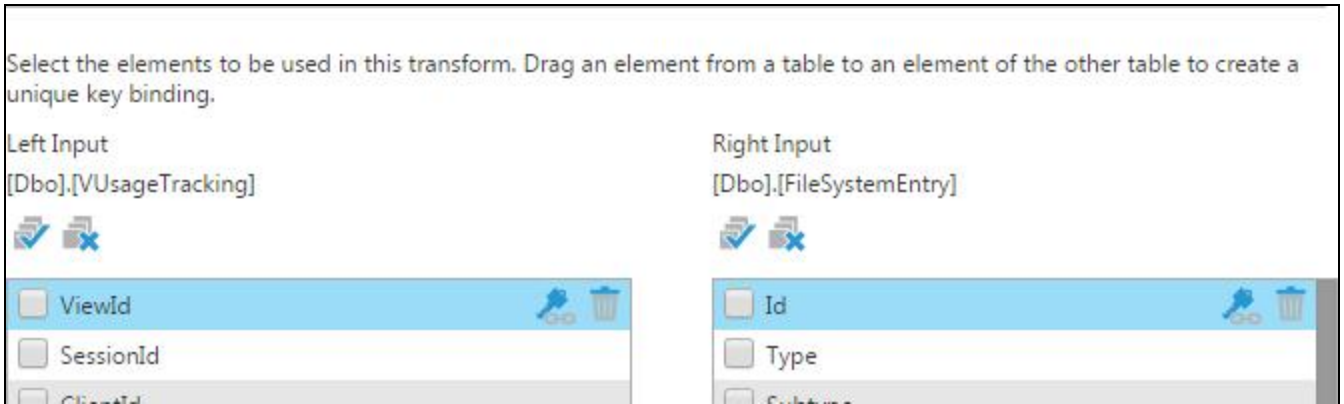
Build a Data Cube to Show Usage Information

The following example shows you how to create a data cube that combines the vUsageTracking data with the FileSystemEntry table in order to show more user-friendly usage information.Here are the detailed steps:

1. Create a new data connector using the SQL Server provider to connect to the Symphony application database.
2. Create a new data cube using the Blank option.
3. Go to the **Explore** window, expand your data connector, and then expand its *Views* folder.
4. Drag *vUsageTracking* to the data cube canvas. It will appear as a SQL Select transform that is connected to a Process Result transform.
5. Select the connection link between the two transforms, click **Insert Common** in the toolbar, and then select to insert a **Join** transform between the two transforms.

6. Drag the *FileSystemEntry* table from the Explore window to the canvas. It will appear as a 2nd SQL Select transform.
7. Click and drag to connect the 2nd SQL Select transform to the join transform, and then double click the Join transform to configure it.
8. In the configuration dialog, drag the *ViewId* element on the left and drop onto the FileSystemEntry table's *Id* element on the right.
9. In the left table, select or uncheck each checkbox to include these columns:
    a. AccountName
    b. EntryTime
    c. LastSeenTime
    d. TotalSeconds
10. In the right table, select these columns:
    a. Name
    b. ProjectId


SQL
SQL Select
[dbo].[vUsageTracking]
SQL
SQL Select
[dbo].[FileSystemEntry]
Join
Process Result
SCRIPT EDITOR
DATA PREVIEW
Data Cube1

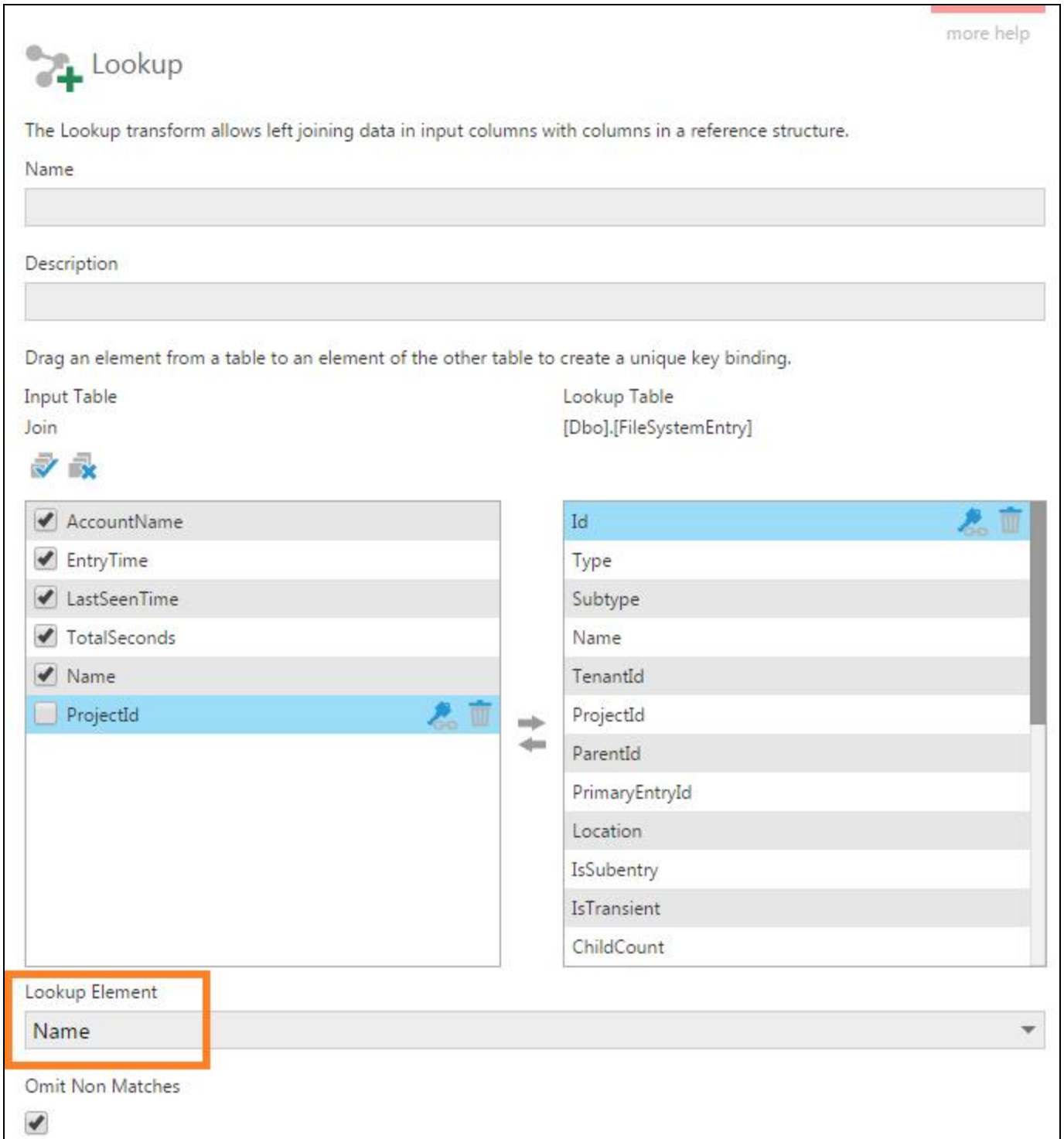

Select the elements to be used in this transform. Drag an element from a table to an element of the other table to create a unique key binding.
Left Input
[Dbo].[VUsageTracking]
ViewId
SessionId
Right Input
[Dbo].[FileSystemEntry]
Id
Type

The next few steps show you how to replace the ProjectId column with the project name:

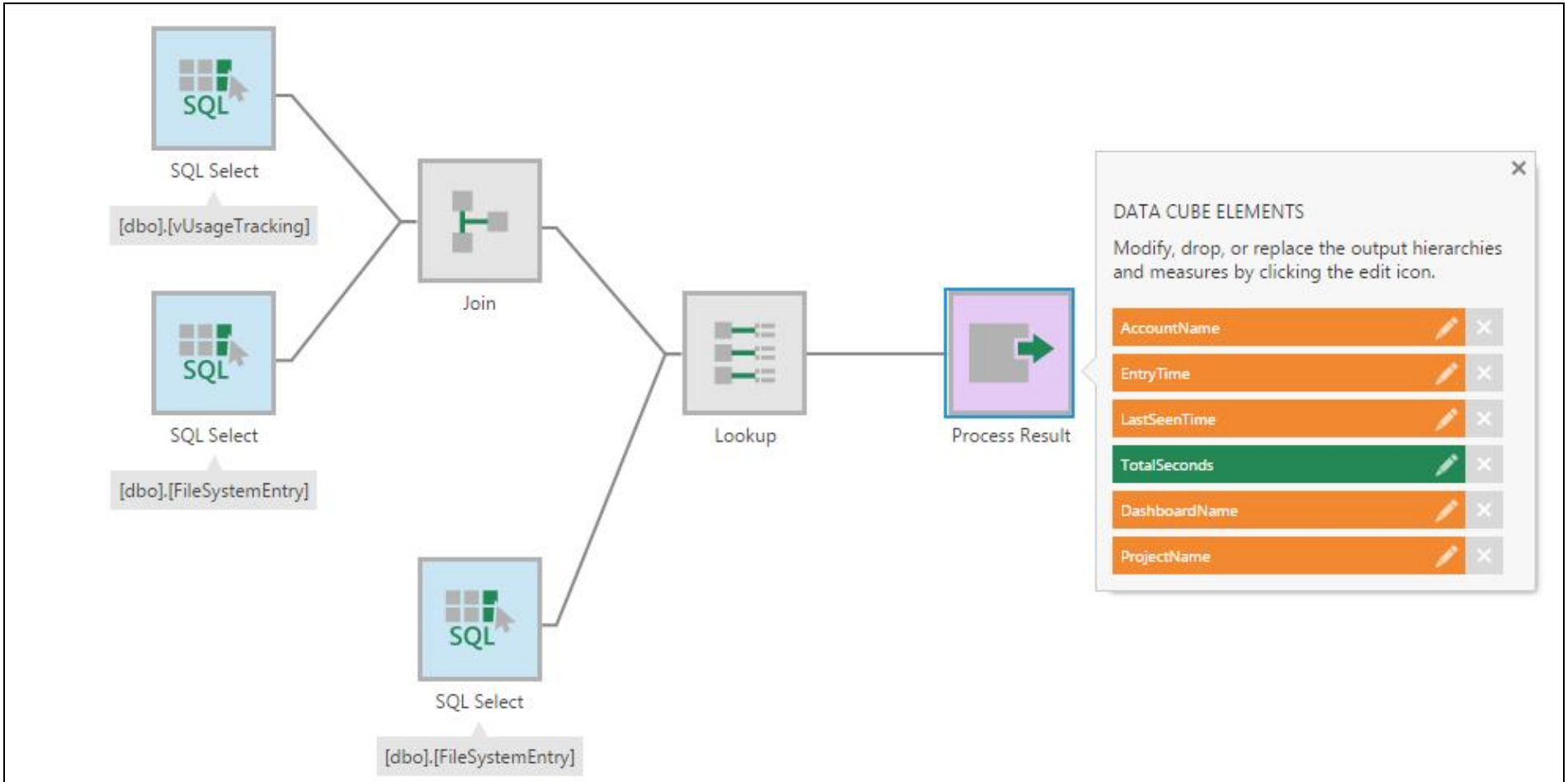
1. Select the last connection link, go to the toolbar, click **Insert Common**, and then select **Lookup**. This will insert a Lookup transform just before the Process Result.

2. Go to the Explore window and drag another FileSystemEntry table to the canvas. It will appear as a SQL Select transform. Click and drag to connect this transform to the Lookup transform.

3. Double-click the Lookup transform to configure it: drag the *ProjectId* element on the left and drop it onto the *Id* on the right. Uncheck the ProjectId element in the left table to exclude it from the output, and set the **Lookup Element** drop-down to Name to output the project name instead. Click to rename the **Output elements** and you'll see two *Name* columns: rename the first one to *ViewName*, and the second one to *ProjectName*.


more help
Lookup
The Lookup transform allows left joining data in input columns with columns in a reference structure.
Name
Description
Drag an element from a table to an element of the other table to create a unique key binding.
Input Table
Join
Lookup Table
[Dbo].[FileSystemEntry]
AccountName
EntryTime
LastSeenTime
TotalSeconds
Name
ProjectId
Id
Type
Subtype
Name
TenantId
ProjectId
ParentId
PrimaryEntryId
Location
IsSubentry
IsTransient
ChildCount
Lookup Element
Name
Omit Non Matches

After submitting the configuration dialog, you can click to open the **Data Preview** to view the resulting data:



SCRIPT EDITOR | DATA PREVIEW

Warnings (0)

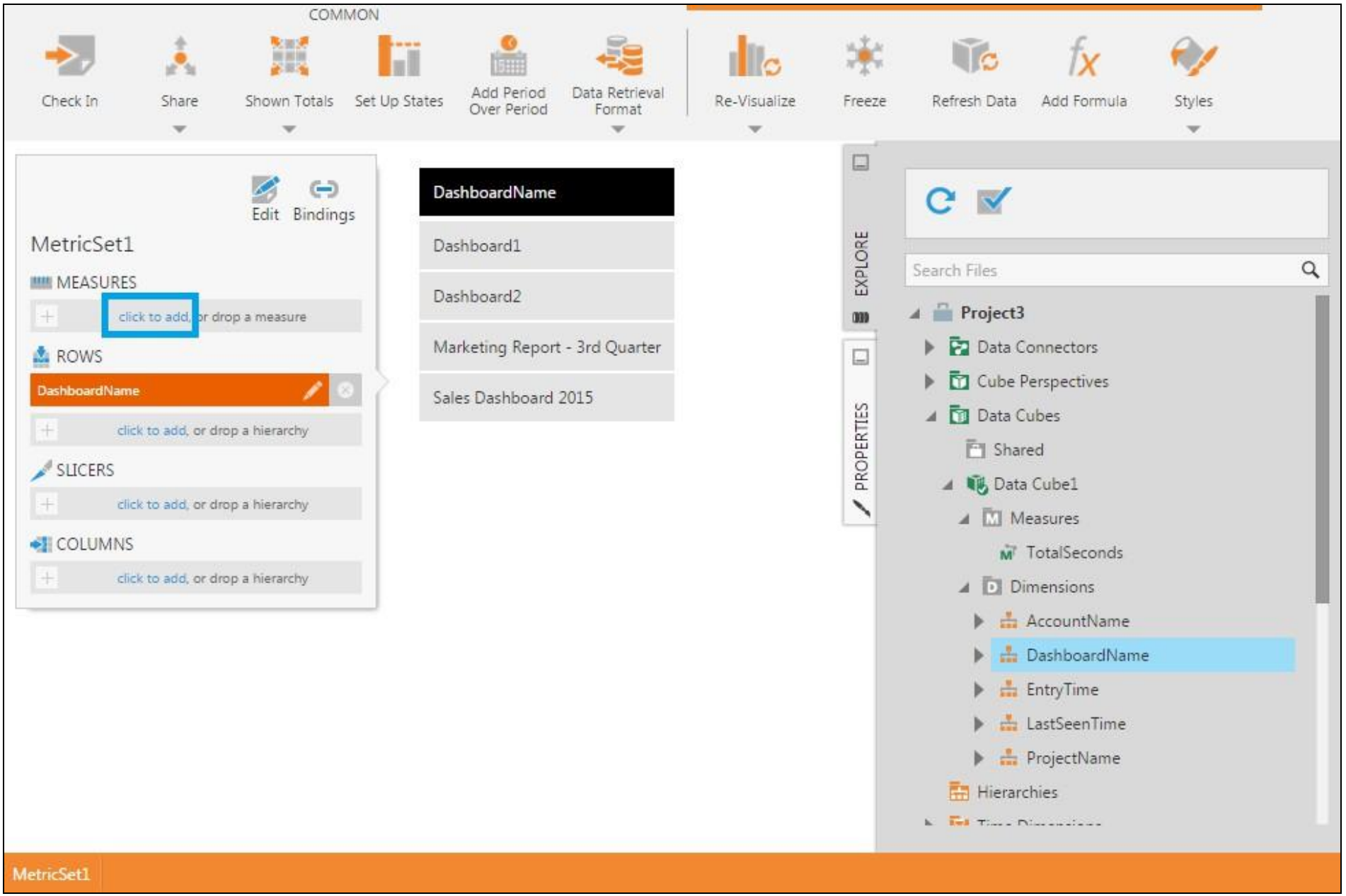
TotalSeconds	AccountName	EntryTime	LastSeenTime	DashboardName	ProjectName
3,119	Admin	09/24/2015 20:01:07	09/24/2015 20:53:05	Dashboard1	Project1
2,580	Admin	09/24/2015 21:16:55	09/24/2015 21:59:55	Dashboard1	Project1

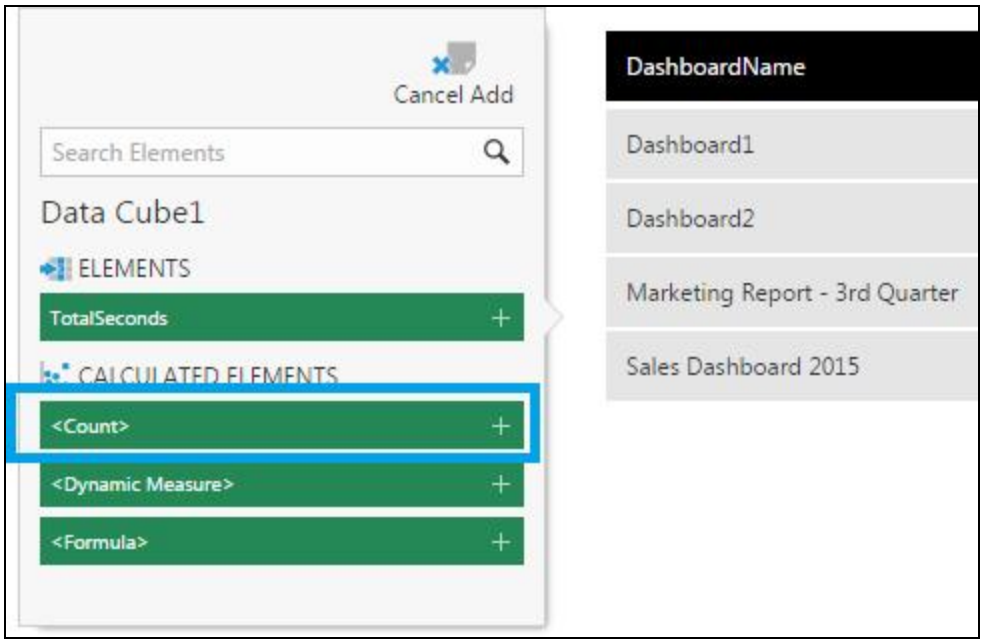
You can now easily display this information in a metric set or dashboard.

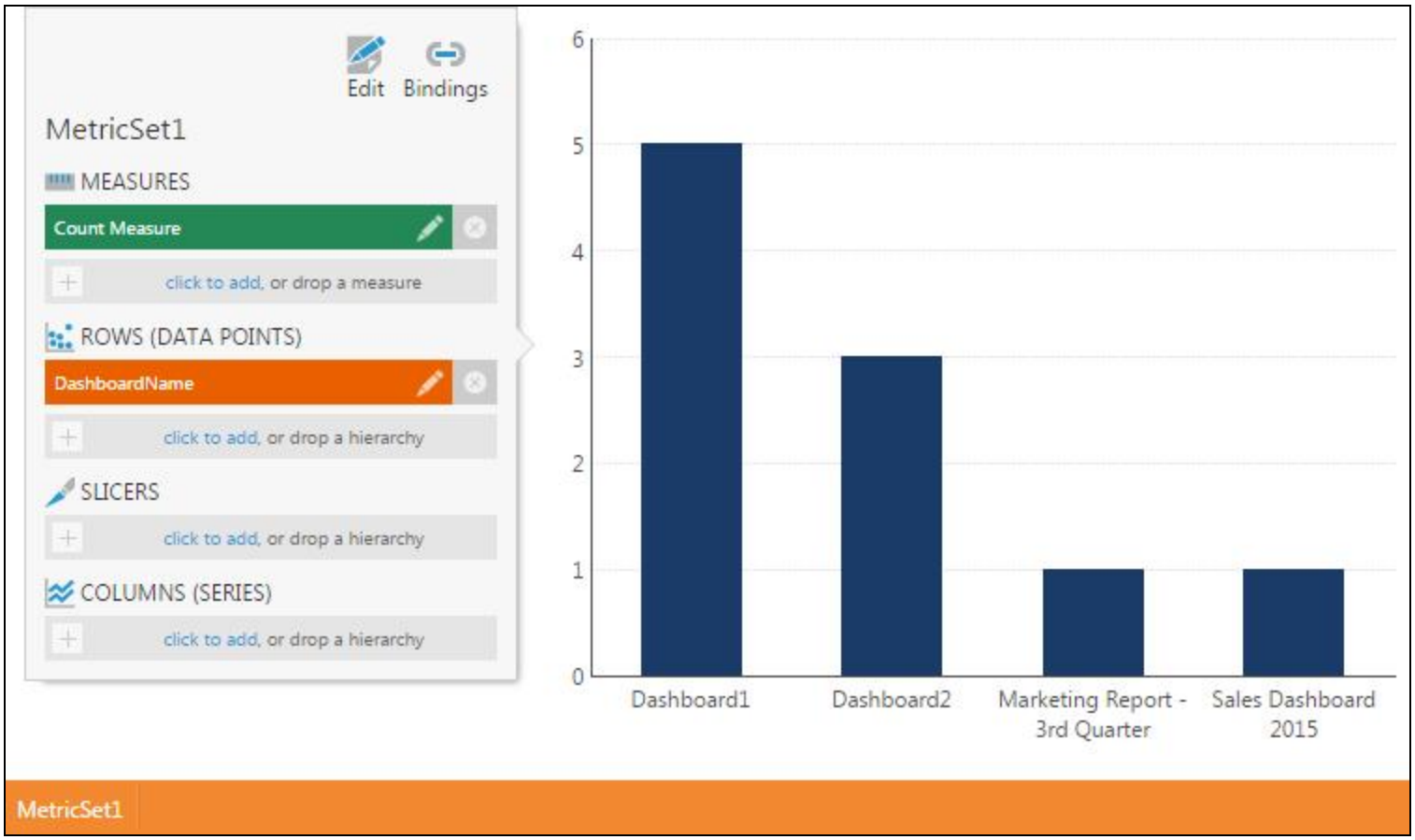
Show how many times each view file has been viewed

Using the data cube created previously, it is easy to set up a chart to display the number of views per dashboard:

1. Create a new metric set from the main menu.
2. Expand the data cube in the Explore window and drag the *ViewName* dimension to the canvas.
3. In the Data Analysis Panel, **click to add** under **Measures**, and choose **<Count>** from the list of elements, located under *Calculated Elements*. This adds a count measure to the metric set.
4. You can click in the toolbar to **Re-visualize** the metric set as a **Bar Chart** if it wasn't visualized this way automatically.


COMMON
Check In
Share
Shown Totals
Set Up States
Add Period Over Period
Data Retrieval Format
Re-Visualize
Freeze
Refresh Data
Add Formula
Styles
Edit
Bindings
MetricSet1
MEASURES
click to add, or drop a measure
ROWS
DashboardName
click to add, or drop a hierarchy
SLICERS
click to add, or drop a hierarchy
COLUMNS
click to add, or drop a hierarchy
DashboardName
Dashboard1
Dashboard2
Marketing Report - 3rd Quarter
Sales Dashboard 2015
EXPLORE
PROPERTIES
Search Files
Project3
Data Connectors
Cube Perspectives
Data Cubes
Shared
Data Cube1
Measures
TotalSeconds
Dimensions
AccountName
DashboardName
EntryTime
LastSeenTime
ProjectName
Hierarchies
MetricSet1


Cancel Add
Search Elements
Data Cube1
ELEMENTS
TotalSeconds
CALCULATED ELEMENTS
<Count>
<Dynamic Measure>
<Formula>
DashboardName
Dashboard1
Dashboard2
Marketing Report - 3rd Quarter
Sales Dashboard 2015



For more information, see:

- Configuration Settings
- Data Cubes
- Connect to Data and View it on a Dashboard
- File and Folder Properties
- Lookup

Using a Security Hierarchy to Filter Data by User

This applies to: *Managed Dashboards, Managed Reports*

This walkthrough shows you how to filter data depending on the user by using a security hierarchy with custom attributes.

Security hierarchies allow you to set up user-dependent filtering, or row-level security, for the data accessed from a data cube. For example, when a user is viewing a dashboard based on a data cube with a security hierarchy, the data that appears can be filtered to correspond to the custom attribute value associated with the user's account.

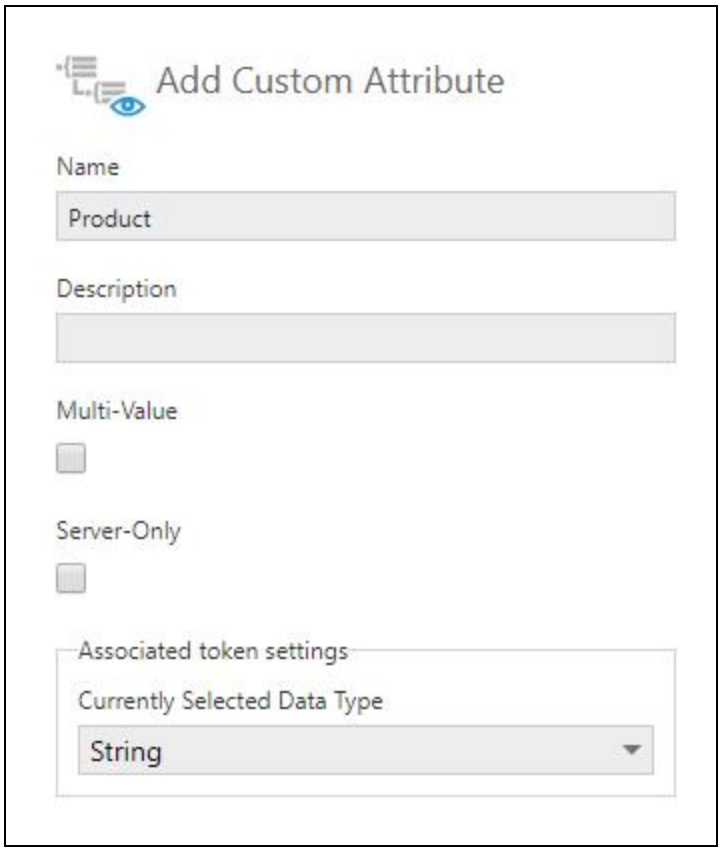
You can also use custom attributes to filter data in a data cube transform's parameter, but setting up a security hierarchy allows for using warehouse or in-memory storage as well as other benefits such as limiting the values shown to users in filters.

> **Note:** Symphony provides built-in support for SaaS (software-as-a- service) and multi-tenant deployment scenarios. If this scenario applies to you, see the article on multi-tenancy.

Example Preparation

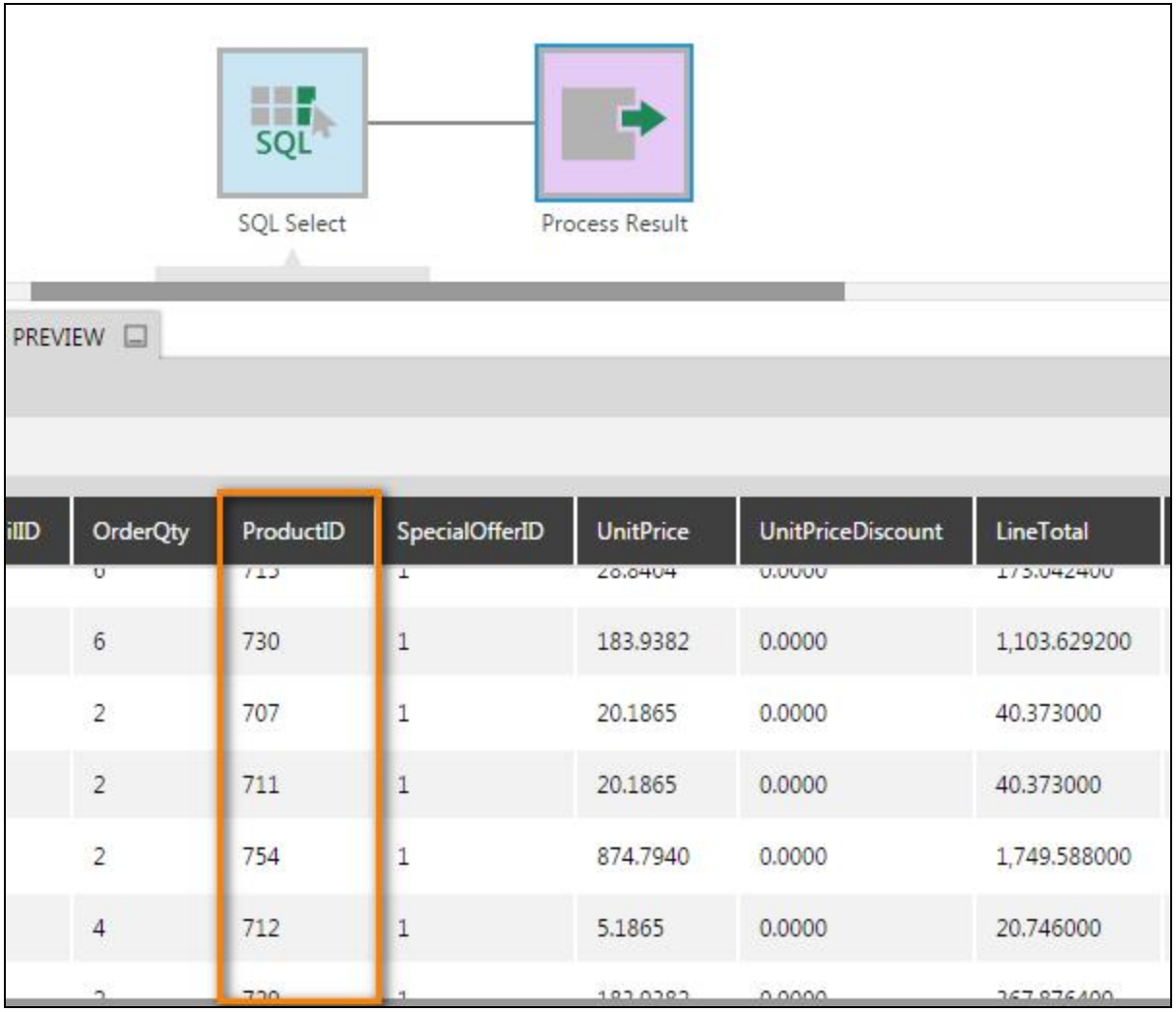
To prepare the example shown in this article, log into Symphony as a member of the *System Administrators* group. First, create a custom attribute that will associate a filter value with each user:

1. Access Administration from the main menu, expand **Account Service** and click **Custom Attributes**.
2. Click to add a new custom attribute and name it *Product* for this example.
3. To be able to select multiple values from a hierarchy to filter by for each user, select **Multi-Value** before submitting the dialog. You can edit a custom attribute later to select this option, but it cannot be changed back if this custom attribute is also used for something besides security hierarchies that requires a single value.



Create a new data cube to use the custom attribute. In this example we choose the **Blank** option for a new data cube, then from an Adventure Works sample database connector in the **Explore** window, we drag the table *[Sales].[SalesOrderDetail]* to the canvas. A SQL Select transform and a Process Result transform appear on the canvas.

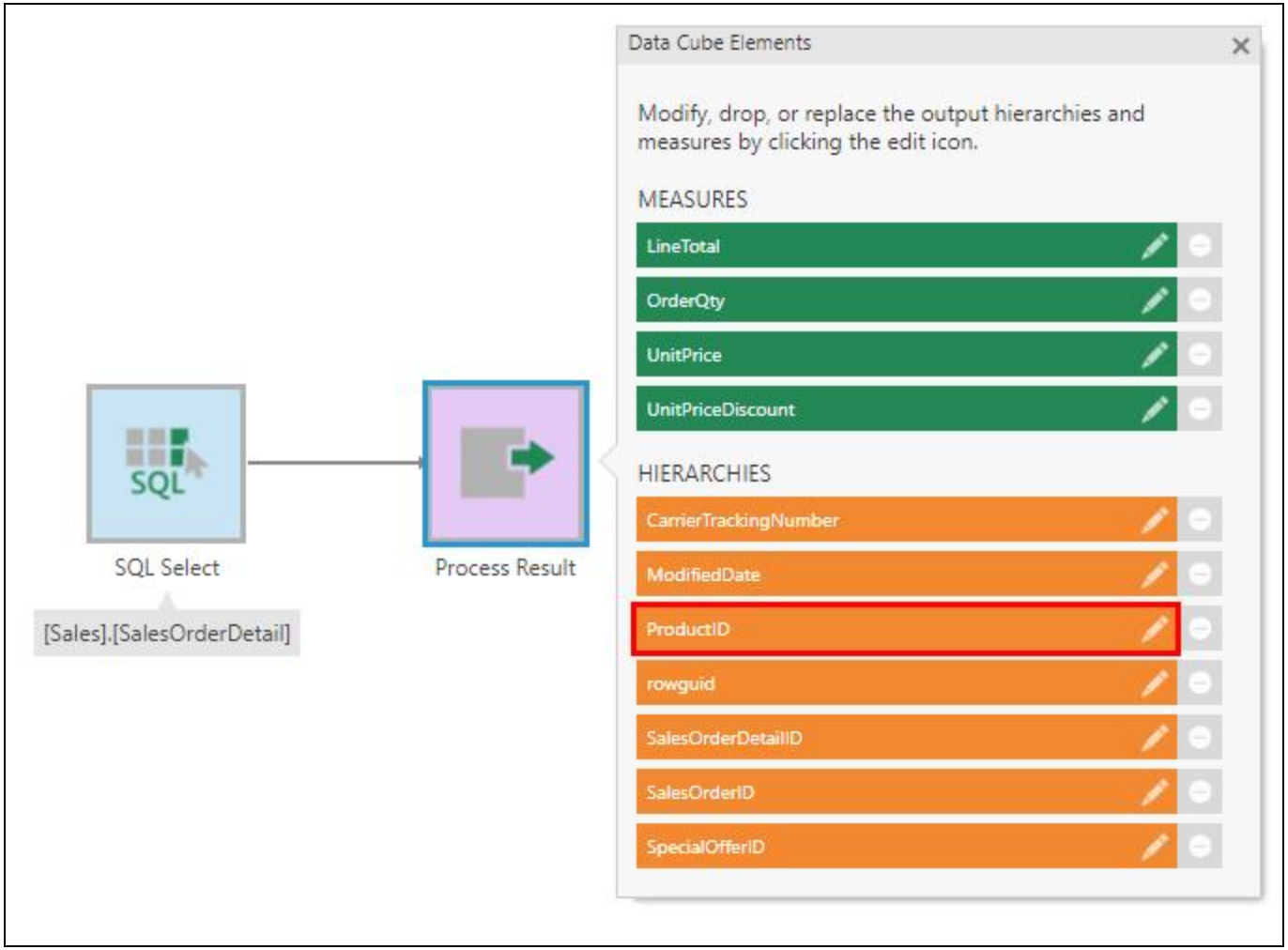
Click the Process Result transform, then open the **Data Preview** window to show the product IDs:



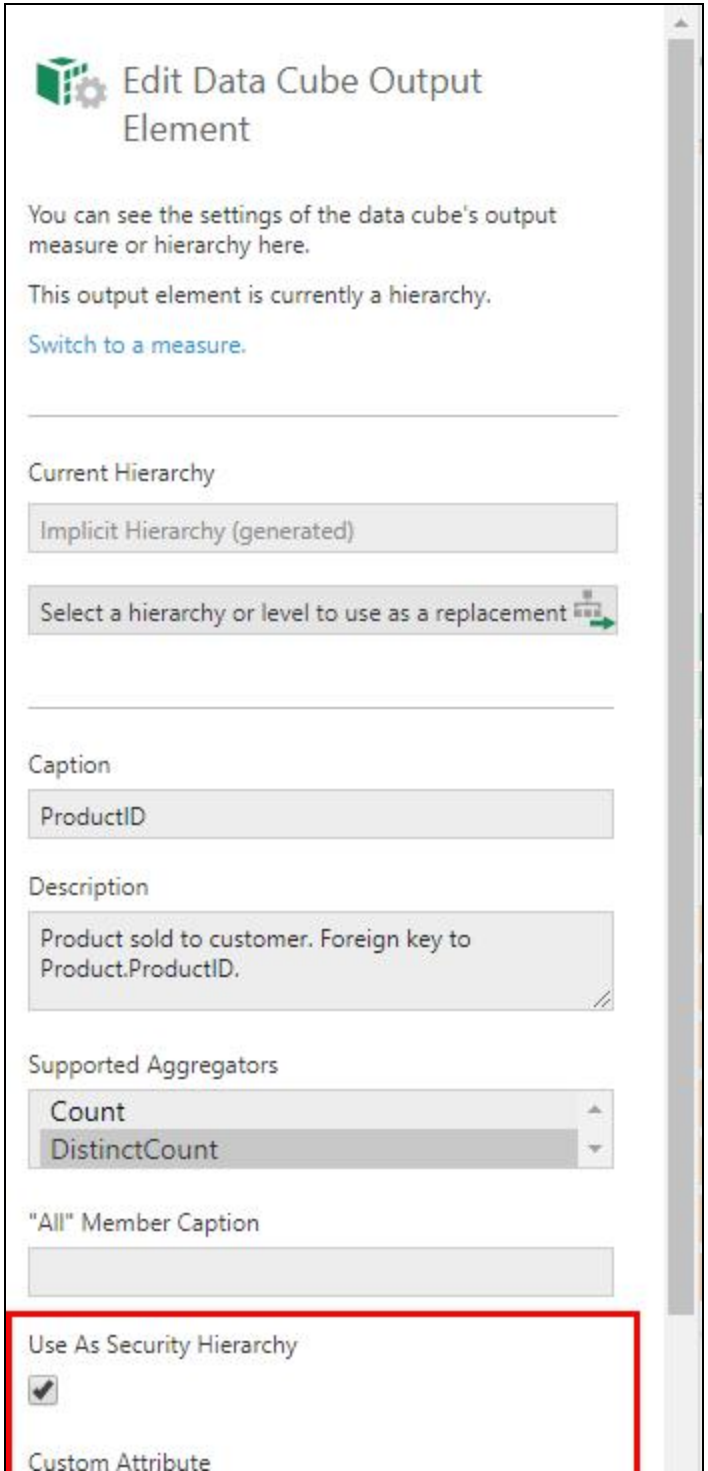
ilID	OrderQty	ProductID	SpecialOfferID	UnitPrice	UnitPriceDiscount	LineTotal
	6	730	1	183.9382	0.0000	1,103.629200
	2	707	1	20.1865	0.0000	40.373000
	2	711	1	20.1865	0.0000	40.373000
	2	754	1	874.7940	0.0000	1,749.588000
	4	712	1	5.1865	0.0000	20.746000

Set the Security Hierarchy

While editing your data cube, select the Process Result transform. In the *Data Cube Elements* popup, click to edit the hierarchy containing values to filter by for each user. For our example, click *ProductID*.

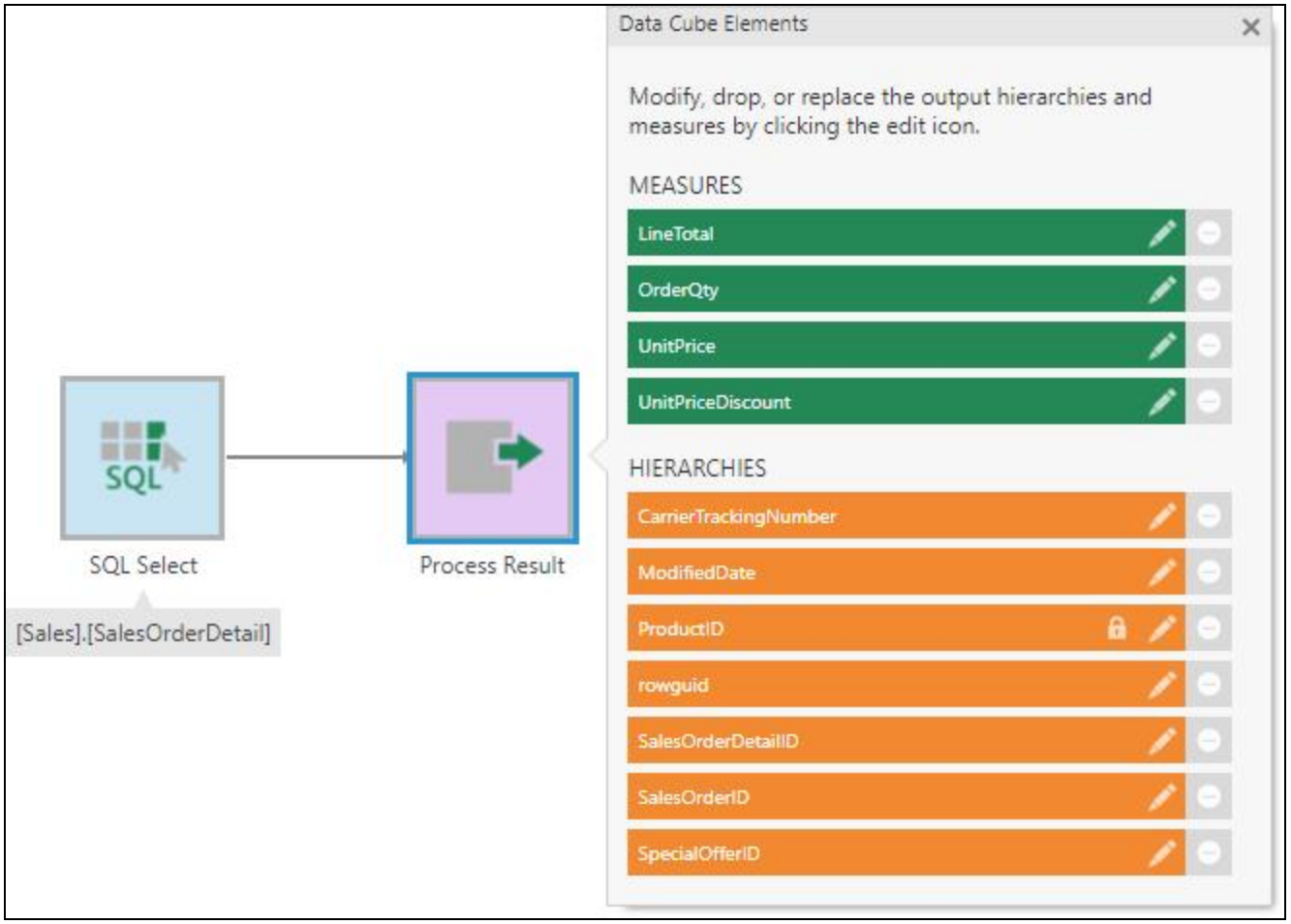


Select the **Security Hierarchy** option, and then select the **Custom Attribute** from the drop-down that will provide a value to filter by for each user (select *Product* for the example above).


Edit Data Cube Output Element
You can see the settings of the data cube's output measure or hierarchy here.
This output element is currently a hierarchy.
Switch to a measure.
Current Hierarchy
Implicit Hierarchy (generated)
Select a hierarchy or level to use as a replacement
Caption
ProductID
Description
Product sold to customer. Foreign key to Product.ProductID.
Supported Aggregators
Count
DistinctCount
"All" Member Caption
Use As Security Hierarchy
Custom Attribute

If this hierarchy should be used to filter the data seen by users but not selected and displayed directly, select the **Hide Hierarchy** option. (Leave this unchecked for now while following this walkthrough.)

Click the submit button at the bottom. The security hierarchy is now configured to filter based on the user's *Product* custom attribute value.

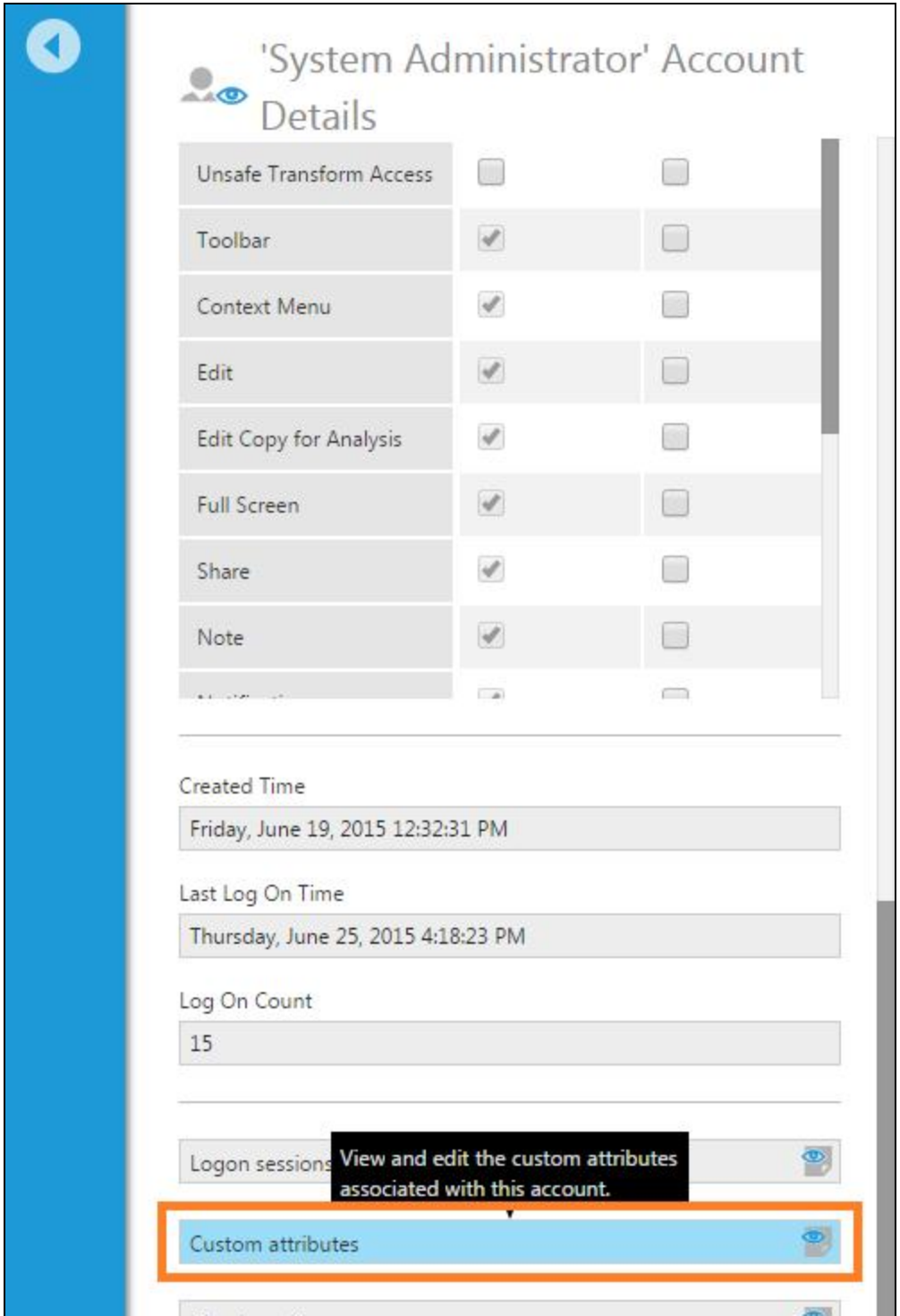


Assign Custom Attribute Values

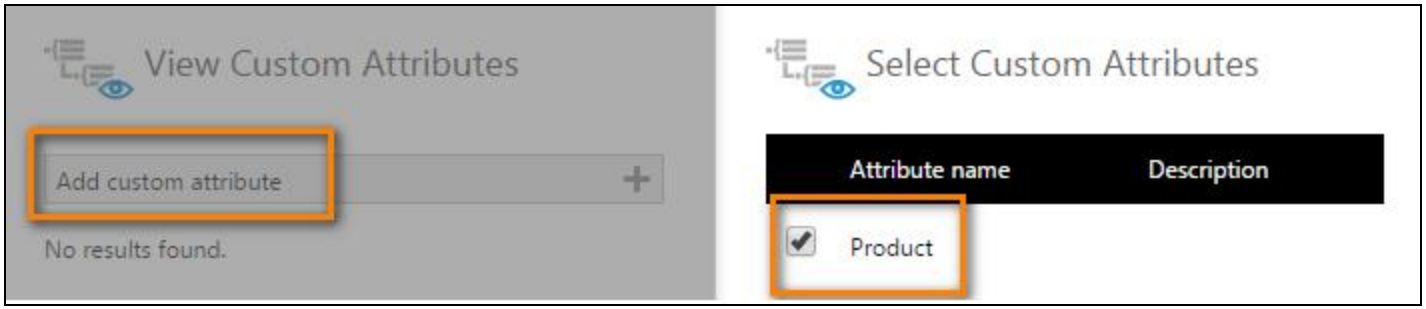
Typically, an administrator will assign the custom attribute value to other users and/or groups. You should assign an appropriate value to each account or group that needs to access this data cube's data.

In the Administration screen, expand **Account Service** and click **Accounts** to see the list of users in the system. (To assign a value to a group of users, click **Groups** instead.)

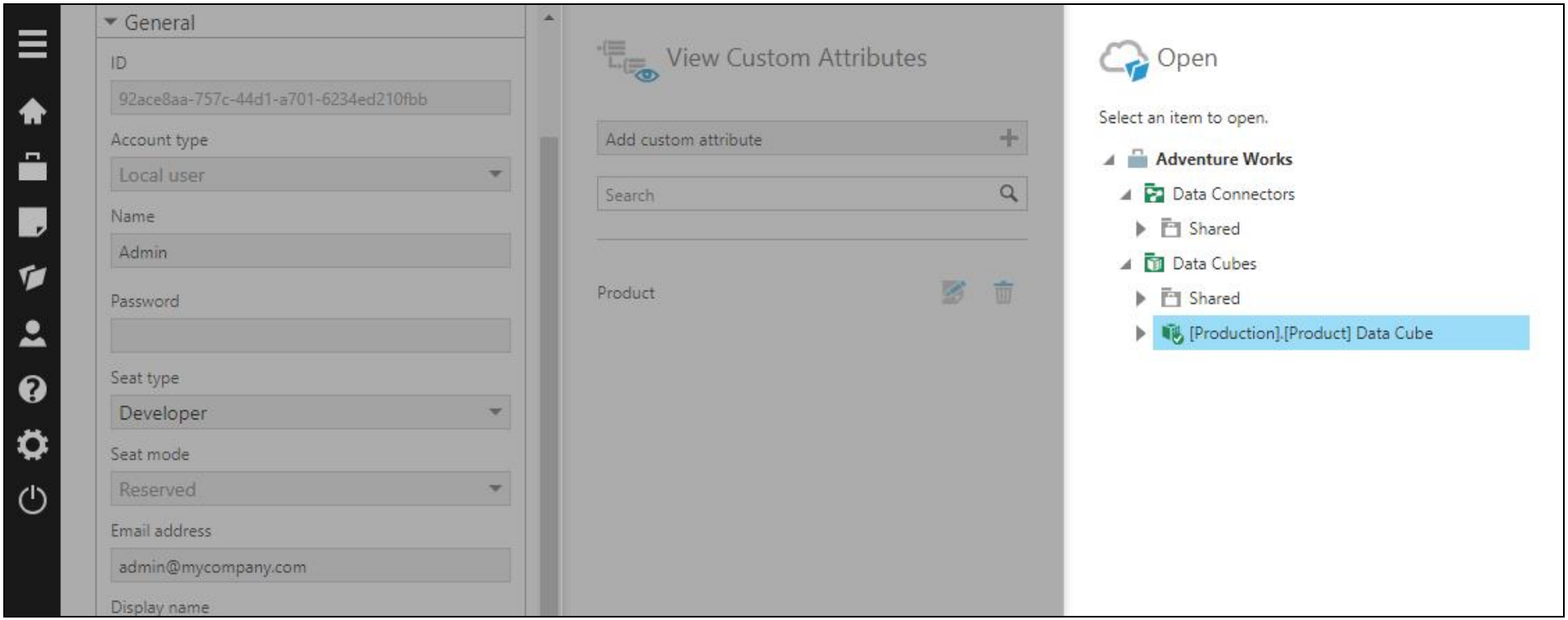
Click the **Edit** button for the user or group. For the purposes of this walkthrough, we will edit *System Administrator* for simplicity. In the *Account Details* dialog, scroll to the bottom and click the **Custom attributes** button.


'System Administrator' Account Details
Unsafe Transform Access
Toolbar
Context Menu
Edit
Edit Copy for Analysis
Full Screen
Share
Note
Created Time
Friday, June 19, 2015 12:32:31 PM
Last Log On Time
Thursday, June 25, 2015 4:18:23 PM
Log On Count
15
Logon sessions
View and edit the custom attributes associated with this account.
Custom attributes

In the *View Custom Attributes* dialog, click **Add custom attribute**. Select the checkbox for the *Product* custom attribute and click the submit button at the bottom.

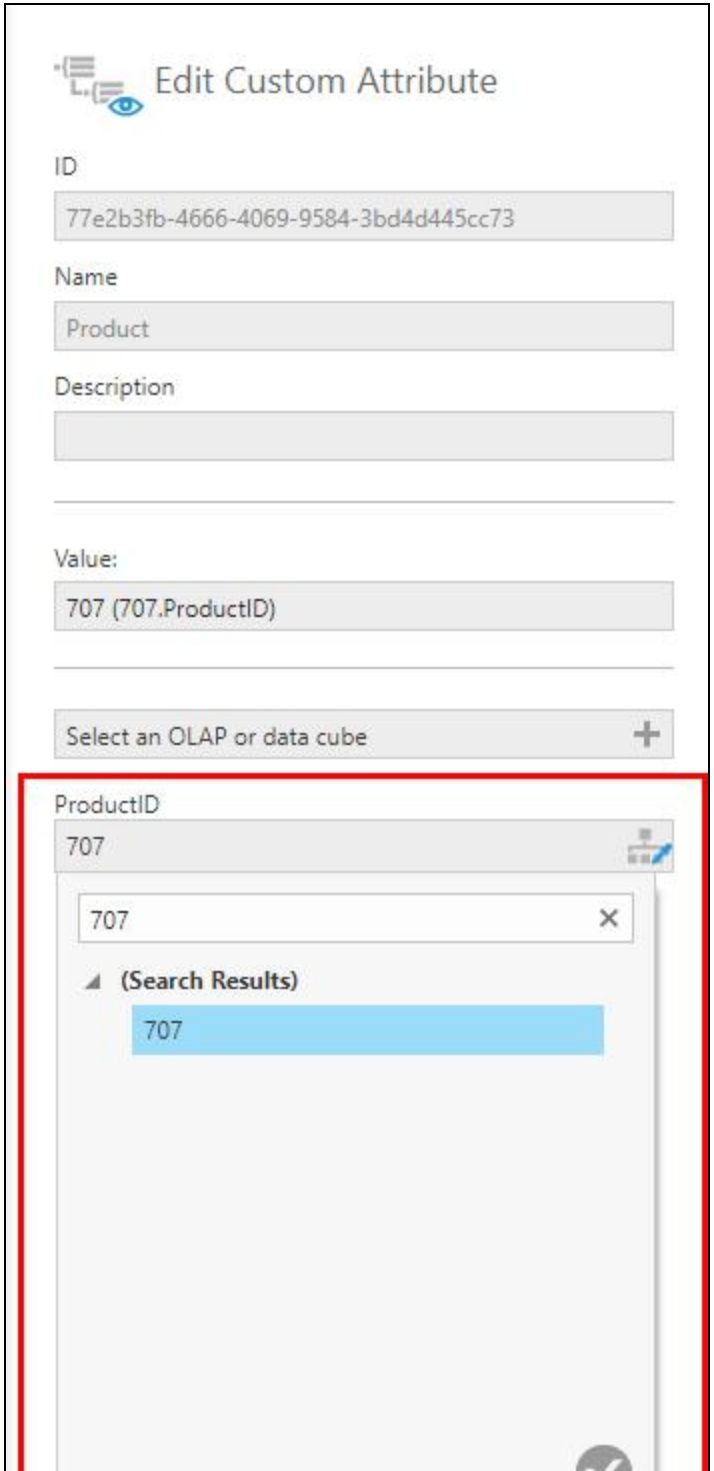


Click the **Edit** button for the new custom attribute. In the *Edit Custom Attribute* dialog, click **Select an OLAP or data cube** and choose the data cube (created above) containing the security hierarchy associated with this custom attribute.



(If the *Open* dialog currently displays the wrong project, close this dialog and use the **Projects** button in main menu at the far left to switch projects before clicking again to select a cube.)

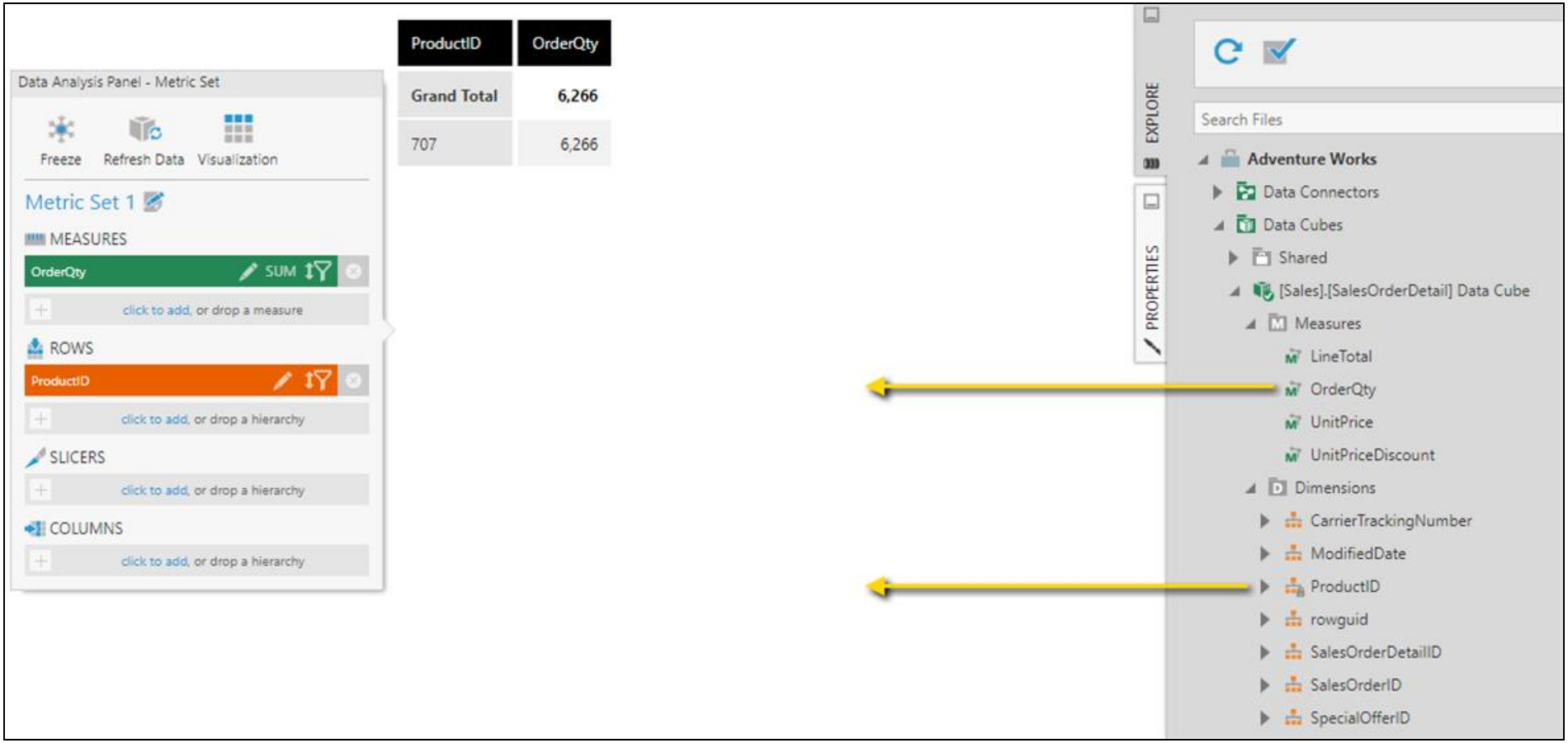
Use the hierarchy value drop-down that now appears for the security hierarchy (for *ProductID* in our example) to browse or search for the value to filter by for this user.


Edit Custom Attribute
ID
77e2b3fb-4666-4069-9584-3bd4d445cc73
Name
Product
Description
Value:
707 (707.ProductID)
Select an OLAP or data cube
ProductID
707
707
(Search Results)
707

If your custom attribute has its **Multi-Value** option selected, each time you choose a hierarchy value it will be added to the list. You can also set the **Value** field to a member unique name, or to the raw keys from the data source for an implicit hierarchy, rather than selecting values from a cube. Submit the dialogs when finished. A popup will inform you that you will need to log off and log back on for the changes to take effect.

Select Data From the Data Cube

After logging in again, create a new metric set from the main menu, then locate the data cube in the **Explore** window.Drag the *OrderQty* measure to the canvas, which will appear as a table visualization. Then drag the *ProductID* dimension onto the area of the table labeled **Row Header**. (A small lock icon identifies ProductID as the security hierarchy in the Explore window.)



Since you're logged on using an account with a value assigned to the security hierarchy's custom attribute, you'll see data filtered by that custom attribute value.

Note: If the option **Hide Hierarchy** is selected for the security hierarchy in the data cube, users cannot select the hierarchy directly to view its data. It will instead filter the other data selected from the cube by the custom attribute value.

For more information, see:

- Use Custom Attributes to Filter Data by User
- Using a Security Hierarchy to Filter SSAS Data by User
- Advanced Group Management
- Advanced User Management
- Data Cubes

Using a Security Hierarchy to Filter SSAS Data by User

This applies to: *Managed Dashboards, Managed Reports*

This walkthrough shows you how to filter data from SQL Server Analysis Services (SSAS) or other OLAP databases differently for each user by using a Symphony security hierarchy with custom attributes.

Security hierarchies are typically used to implement user-dependent filtering or row-level security, similar to using custom data and custom attributes to filter SSAS data and using SSAS roles impersonation. For example, when a user is viewing a dashboard, the data appearing in charts and tables can be filtered so that the user only sees data corresponding to the custom attribute value associated with the user's account.

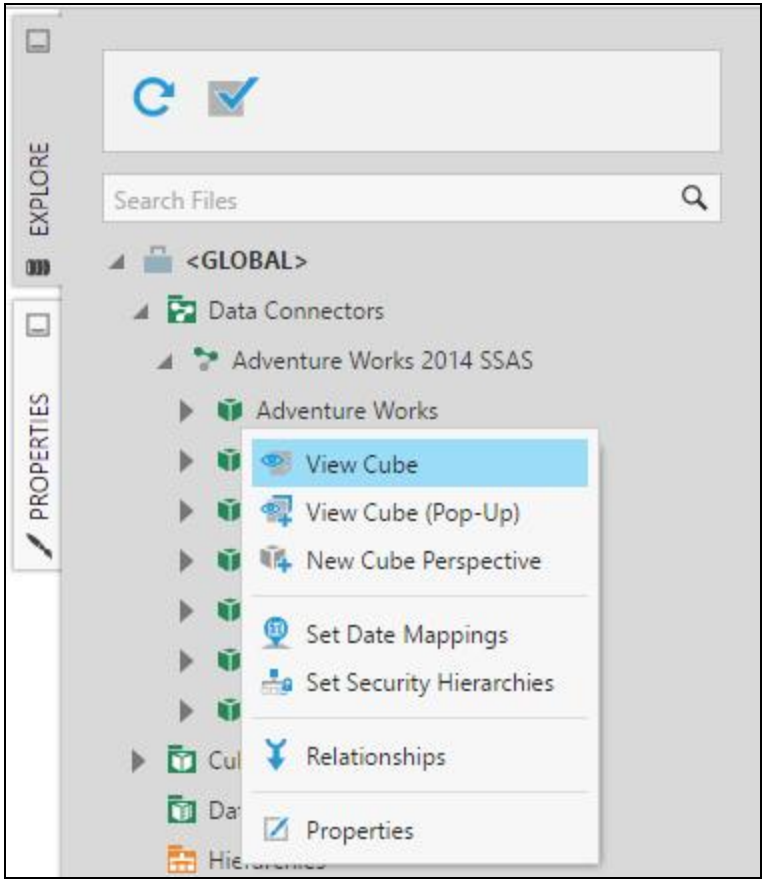
Unlike the other two methods for user-dependent filtering of SSAS data, security hierarchies can be set up within Symphony and do not require additional actions to be taken within the database itself.

Example Preparation

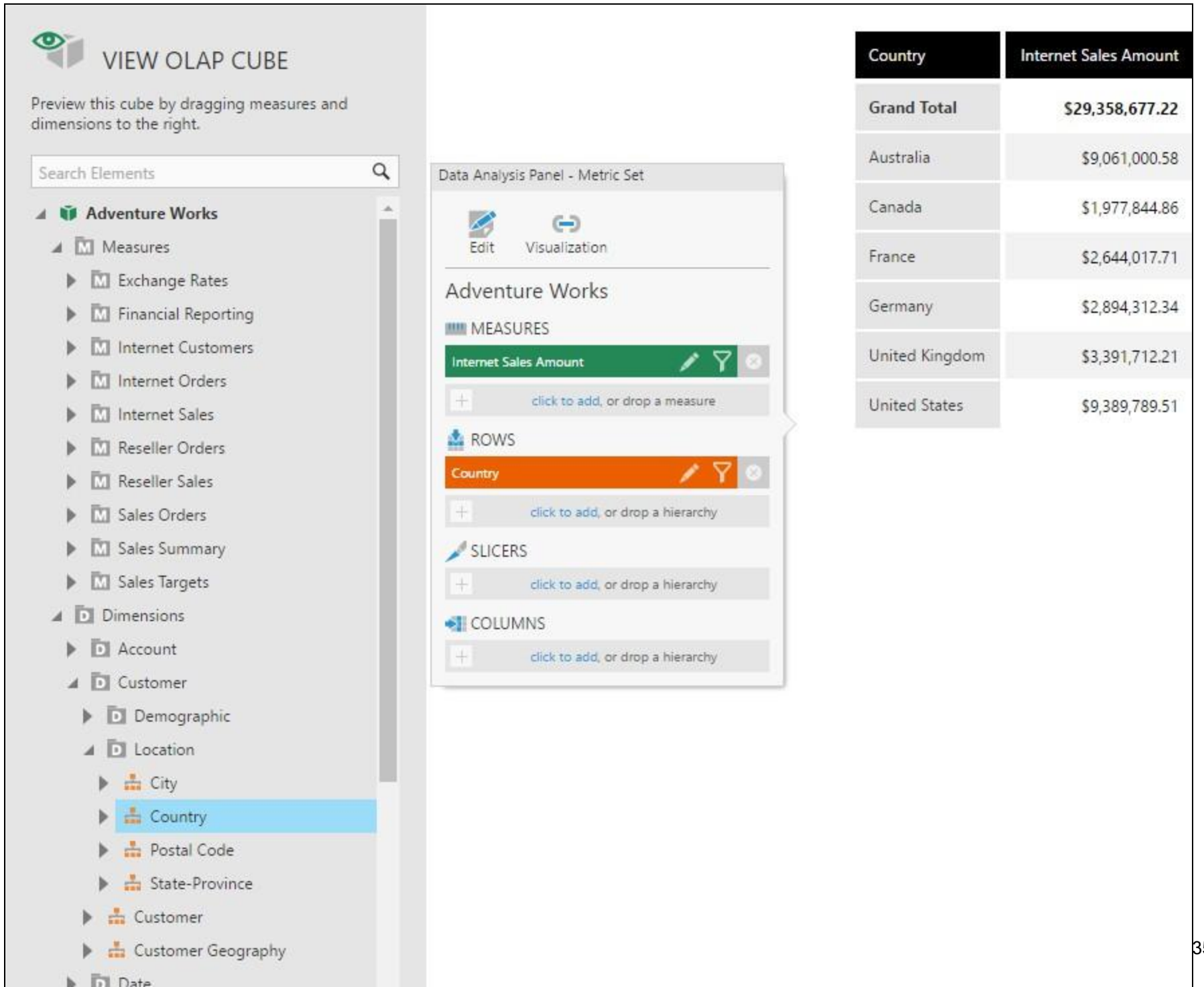
To follow along with this walkthrough, log on as a member of the *System Administrators* group and prepare the following:

1. A data connector to a SQL Server Analysis Services database. The following examples use the Adventure Works DW sample database.
2. A custom attribute. The following examples use a *Country* custom attribute like the one created in Using custom attributes to filter data by user.

To view the data before it's filtered, find the data connector to your OLAP database in the **Explore** window when you have another file open such as a dashboard. Expand the data connector to list its cubes, then right-click one and choose **View Cube**.



In our example shown below, we can expand *Dimensions*, *Customer*, and *Location*, then drag the *Country* hierarchy to **Rows** on the *Data Analysis Panel*, then view the result.

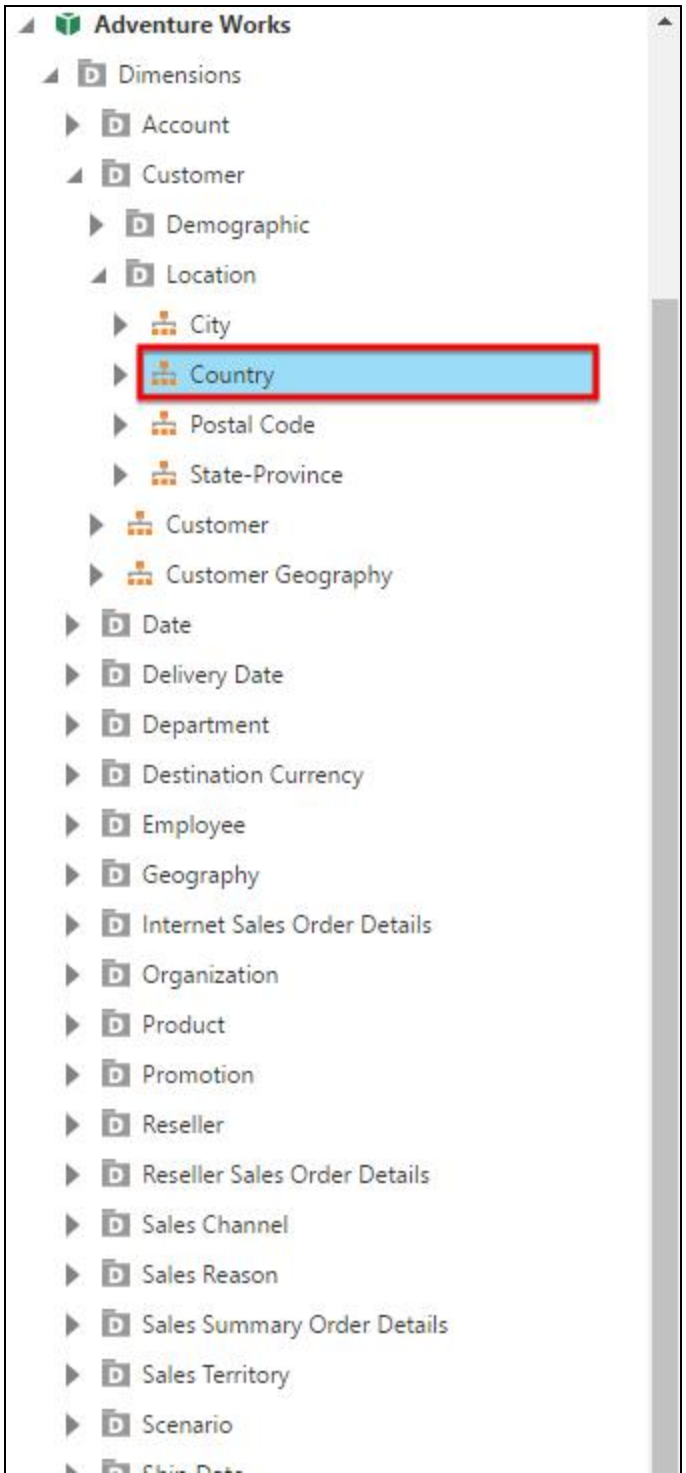

VIEW OLAP CUBE
Preview this cube by dragging measures and dimensions to the right.
Search Elements
Adventure Works
Measures
Exchange Rates
Financial Reporting
Internet Customers
Internet Orders
Internet Sales
Reseller Orders
Reseller Sales
Sales Orders
Sales Summary
Sales Targets
Dimensions
Account
Customer
Demographic
Location
City
Country
Postal Code
State-Province
Customer
Customer Geography
Date
Data Analysis Panel - Metric Set
Edit
Visualization
Adventure Works
MEASURES
Internet Sales Amount
click to add, or drop a measure
ROWS
Country
click to add, or drop a hierarchy
SLICERS
click to add, or drop a hierarchy
COLUMNS
click to add, or drop a hierarchy
Country
Internet Sales Amount
Grand Total
$29,358,677.22
Australia
$9,061,000.58
Canada
$1,977,844.86
France
$2,644,017.71
Germany
$2,894,312.34
United Kingdom
$3,391,712.21
United States
$9,389,789.51

Set the Security Hierarchy

Access the **View Cube** option as described above, then you can choose **Set Security Hierarchies** in the toolbar. (Alternatively, find and expand the data connector in an **Explore** window, right-click one of its cubes, and choose **Set Security Hierarchies**.)

In the *Set Security Hierarchies* dialog, select which hierarchy's values should be filtered differently for each user. In this example, expand *Customer* and *Location*, and select *Country*.

At the bottom of the dialog, choose which **Custom Attribute** will be populated with a value for each user (*Country* in this example).


Adventure Works
Dimensions
Account
Customer
Demographic
Location
City
Country
Postal Code
State-Province
Customer
Customer Geography
Date
Delivery Date
Department
Destination Currency
Employee
Geography
Internet Sales Order Details
Organization
Product
Promotion
Reseller
Reseller Sales Order Details
Sales Channel
Sales Reason
Sales Summary Order Details
Sales Territory
Scenario

The Country hierarchy now has a green checkmark indicating a security hierarchy has been set.

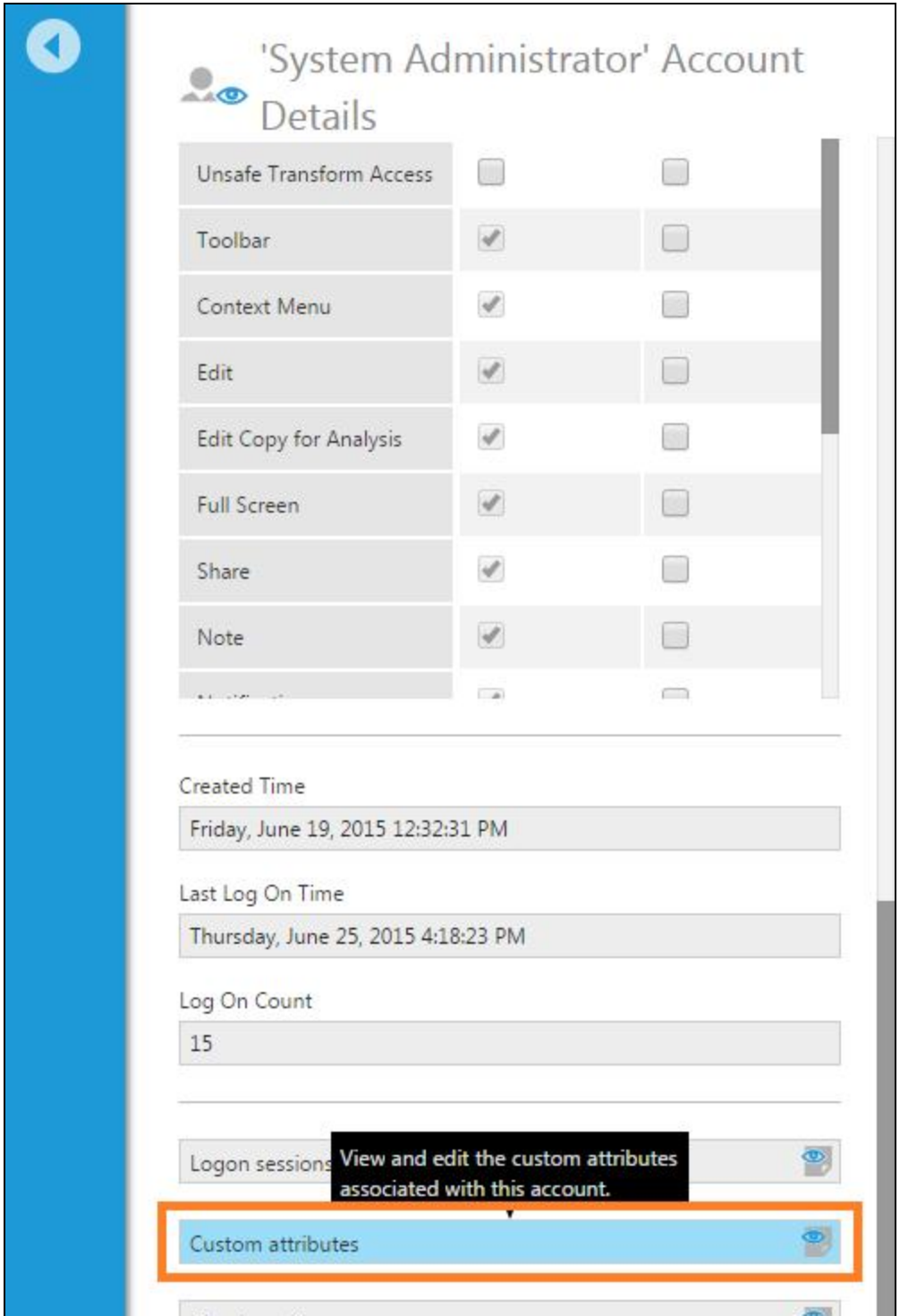
Assign Custom Attribute Values

Typically, an administrator will assign the custom attribute to other users or groups. You should assign an appropriate value to each account or group that needs to access this cube's data.

In the **Admin** screen of Symphony, expand **Account Service** and then click **Accounts** to see a list of users in the system. (To assign a custom attribute value to a group of users, click **Groups** instead.)

Click the **Edit** button for an account or group to assign it a custom attribute value. To simplify this walkthrough, we will edit the *System Administrator* user.

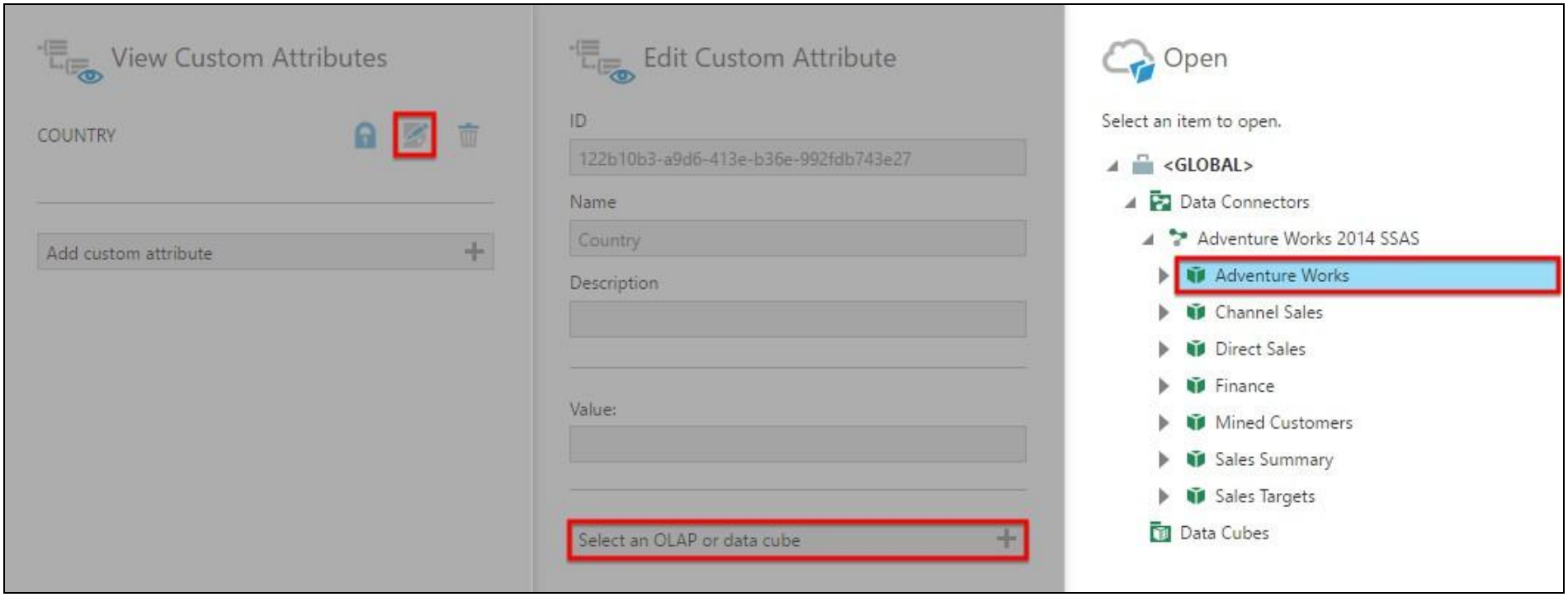
In the *Account Details* dialog, click the **Custom attributes** button.


'System Administrator' Account Details
Unsafe Transform Access
Toolbar
Context Menu
Edit
Edit Copy for Analysis
Full Screen
Share
Note
Created Time
Friday, June 19, 2015 12:32:31 PM
Last Log On Time
Thursday, June 25, 2015 4:18:23 PM
Log On Count
15
Logon sessions
View and edit the custom attributes associated with this account.
Custom attributes

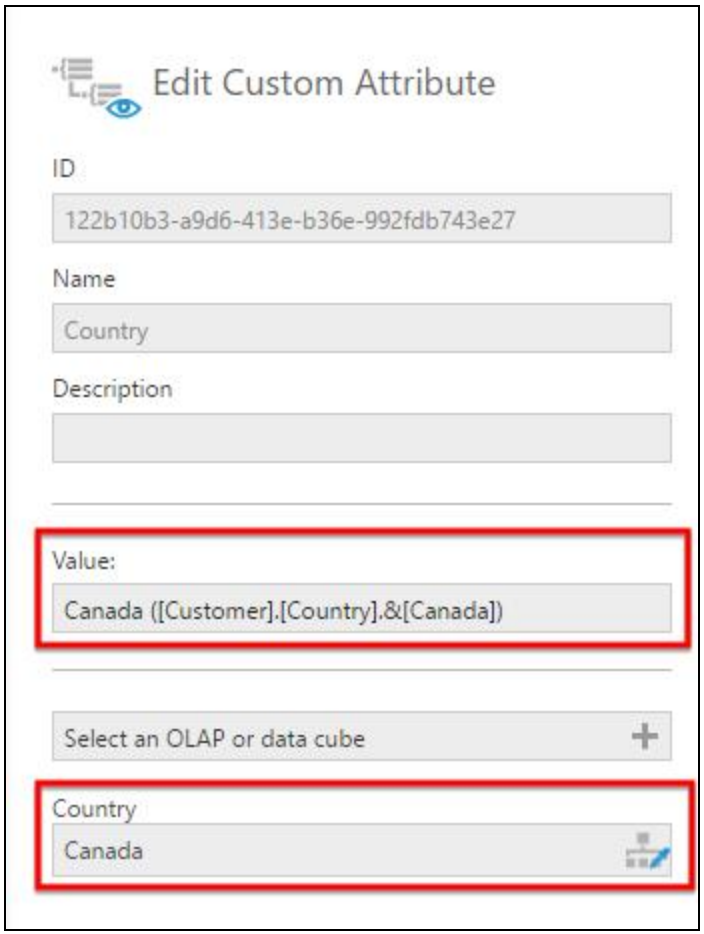
In the *View Custom Attributes* dialog, click **Add custom attribute**.

In the *Select Custom Attributes* dialog, select the checkbox for custom attribute (e.g., *Country*) and click the submit button at the bottom.

Click the **Edit** button for the new custom attribute. In the *Edit Custom Attribute* dialog, click **Select an OLAP or data cube**, select your cube, then click **Submit**.



In the *Edit Custom Attribute* dialog, select a security hierarchy value from the drop-down to populate the Value field above it.



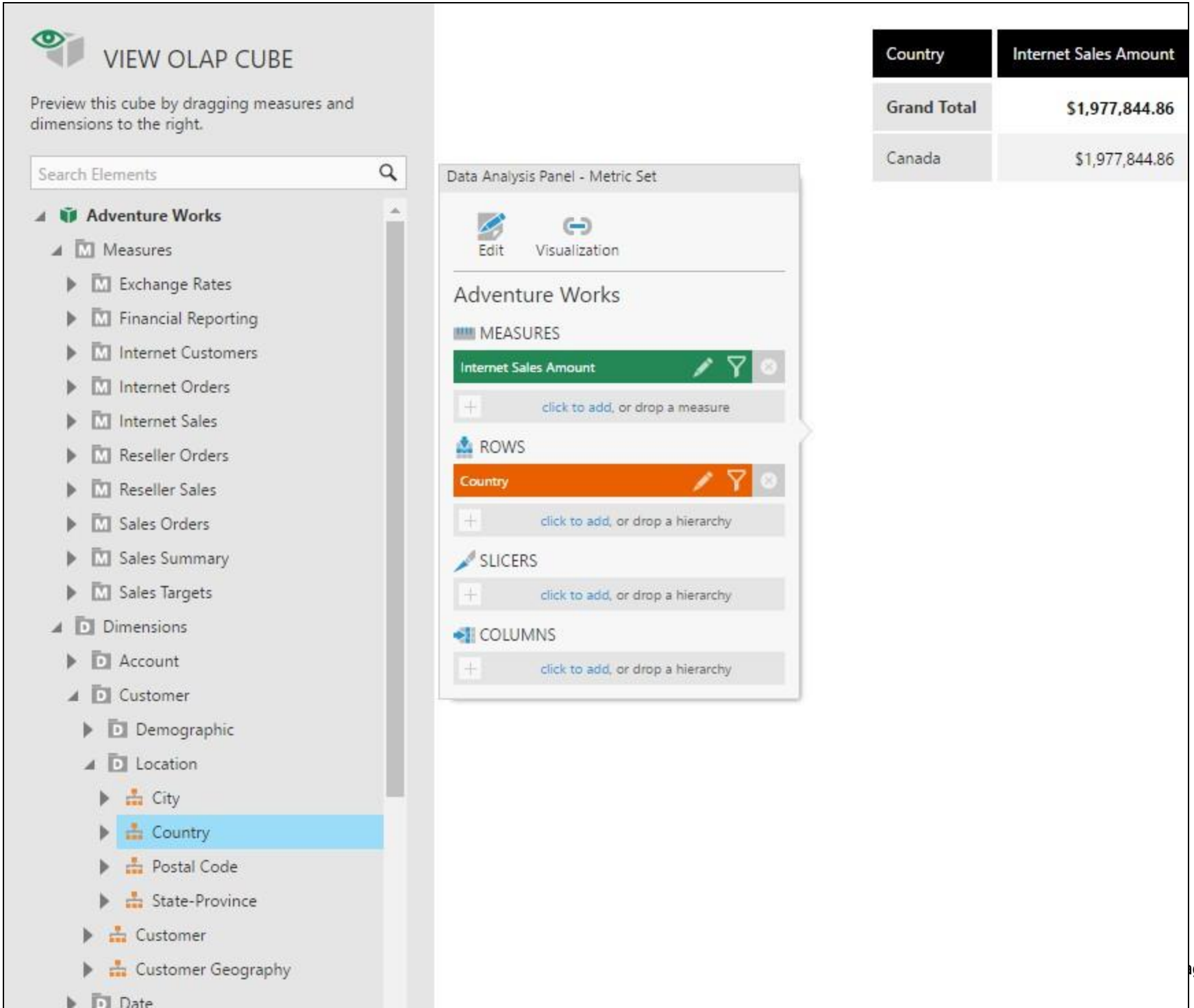
Click **Submit** on both dialogs.

Log off and then log back on for the changes to take effect.

Preview the Metric Set

After logging back on, find and expand the data connector again and choose **View Cube**.

For our example, drag the *Country* hierarchy to **Rows** in the *Data Analysis Panel*. You will see data filtered by the custom attribute value for the current account in the preview.


VIEW OLAP CUBE
Preview this cube by dragging measures and dimensions to the right.
Search Elements
Adventure Works
Measures
Exchange Rates
Financial Reporting
Internet Customers
Internet Orders
Internet Sales
Reseller Orders
Reseller Sales
Sales Orders
Sales Summary
Sales Targets
Dimensions
Account
Customer
Demographic
Location
City
Country
Postal Code
State-Province
Customer
Customer Geography
Date
Data Analysis Panel - Metric Set
Edit
Visualization
Adventure Works
MEASURES
Internet Sales Amount
click to add, or drop a measure
ROWS
Country
click to add, or drop a hierarchy
SLICERS
click to add, or drop a hierarchy
COLUMNS
click to add, or drop a hierarchy
Country
Internet Sales Amount
Grand Total
$1,977,844.86
Canada
$1,977,844.86

For more information, see:

- Use Custom Attributes to Filter Data by User
- Using a Security Hierarchy to Filter SSAS Data by User
- Using a Security Hierarchy to Filter Data by User

Use Custom Attributes to Filter Data by User

This applies to: *Managed Dashboards, Managed Reports*

A *custom attribute* is a custom value assigned to users, groups, or tenants by an administrator. These are similar to several attributes built into Symphony describing each user that you can select as tokens when filtering a data cube, such as *Current Account Name* and *Current Culture Name*.

Filtering by attributes and custom attributes allows you to accomplish user-dependent filtering or row-level security. For example, when a user is viewing a dashboard based on a particular data cube, the data can be automatically filtered so that the user only sees the data corresponding to the custom attribute value associated with their account.

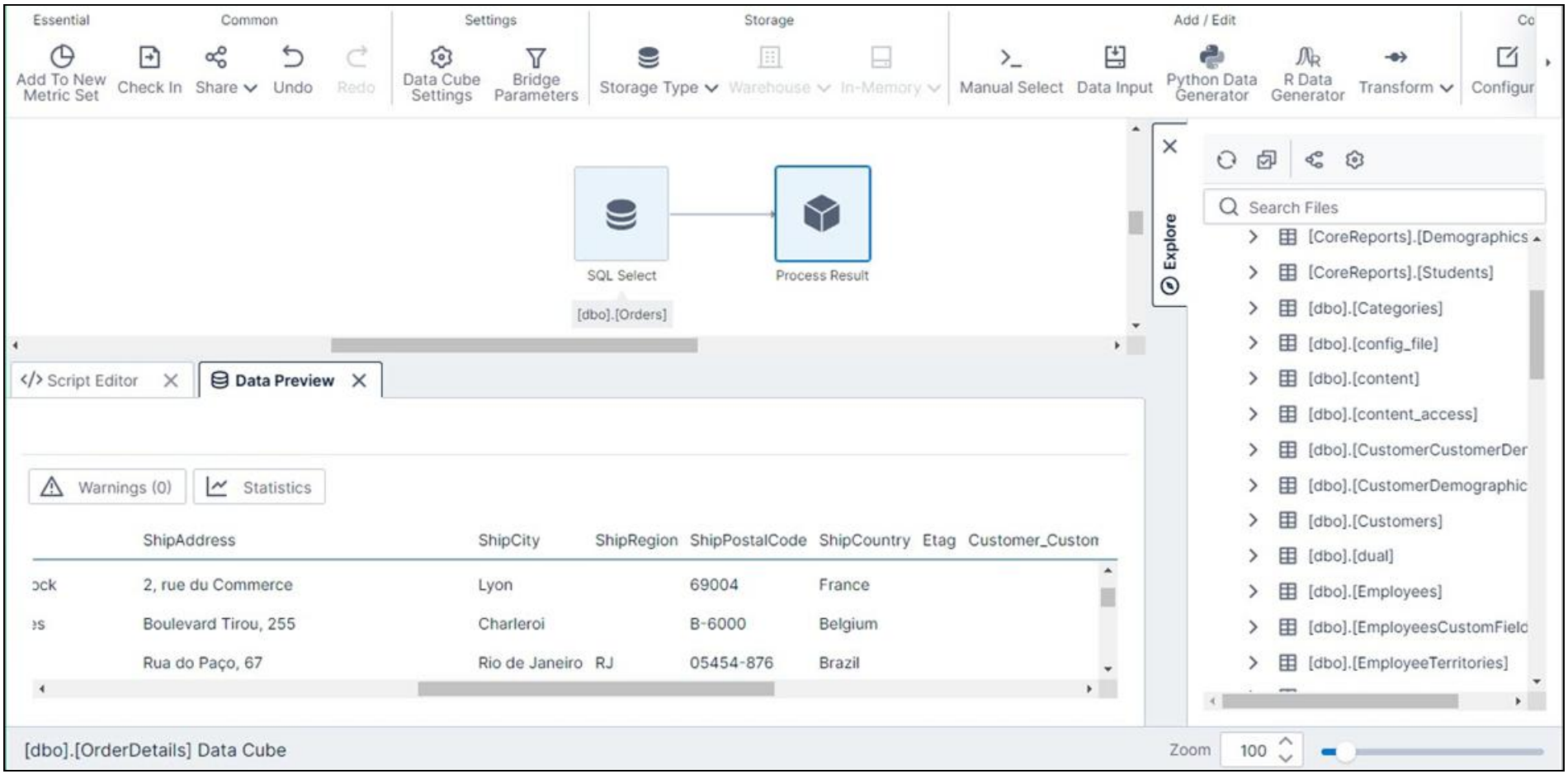
This walkthrough shows you how to set up custom attributes and use them to filter a data cube transform parameter, which is one way to accomplish row-level security.

Note: Use custom attributes with security hierarchies instead of a transform parameter to take advantage of warehouse or in-memory storage and avoid other limitations with lower-level filtering.

Example Preparation

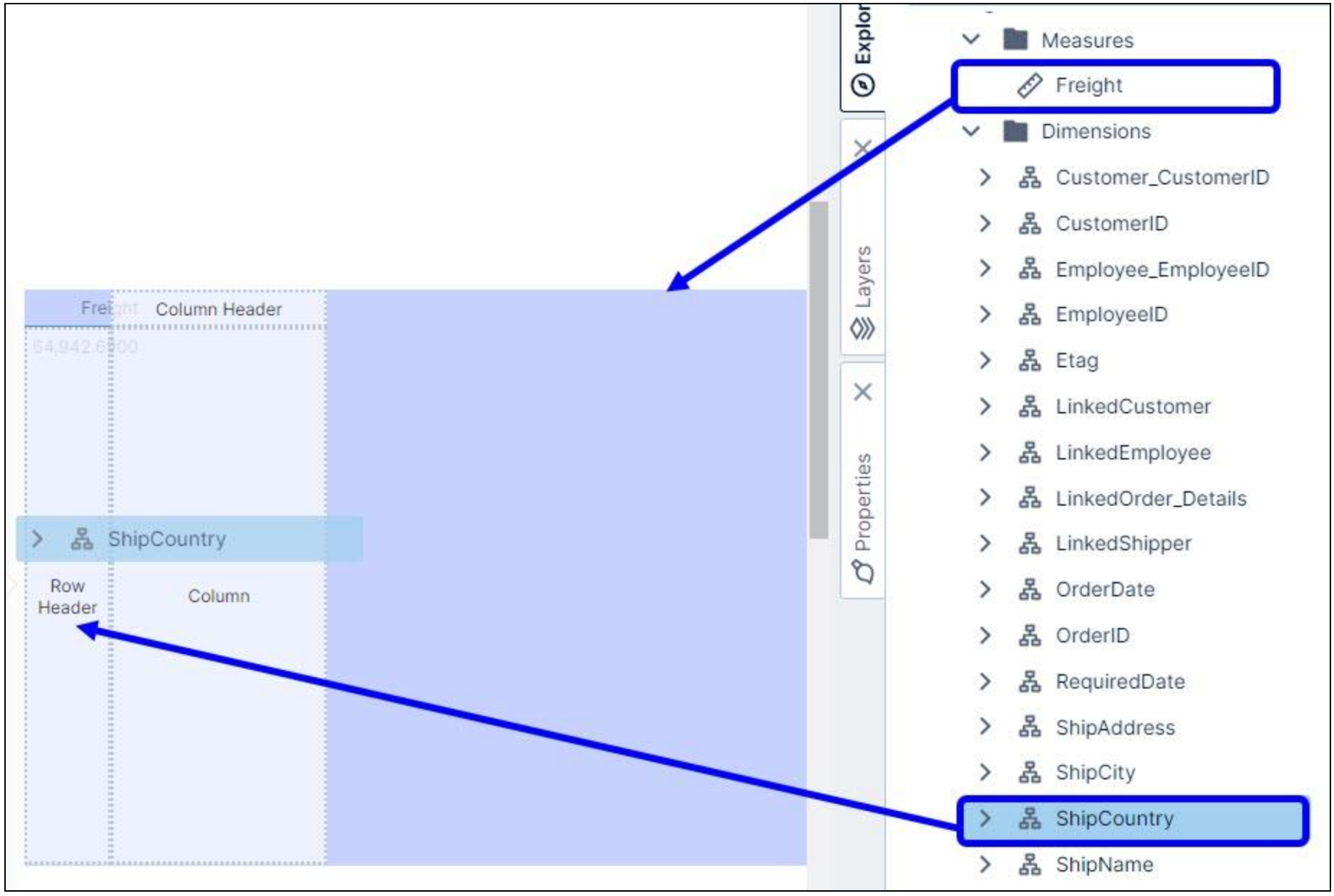
Create a data cube

1. Log in as a system admin or tenant admin.
2. Create a new data cube using the **Blank** option.
3. Drag table from a data connector in the Explore window to the canvas. Two transforms are added: SQL Select and Process Result.
4. Select the Process Result transform, then the **Data Preview** window.
5. Decide which column to use for filtering and make a note of the column name to use as a dimension later. in this example, we're using **ShipCountry**.

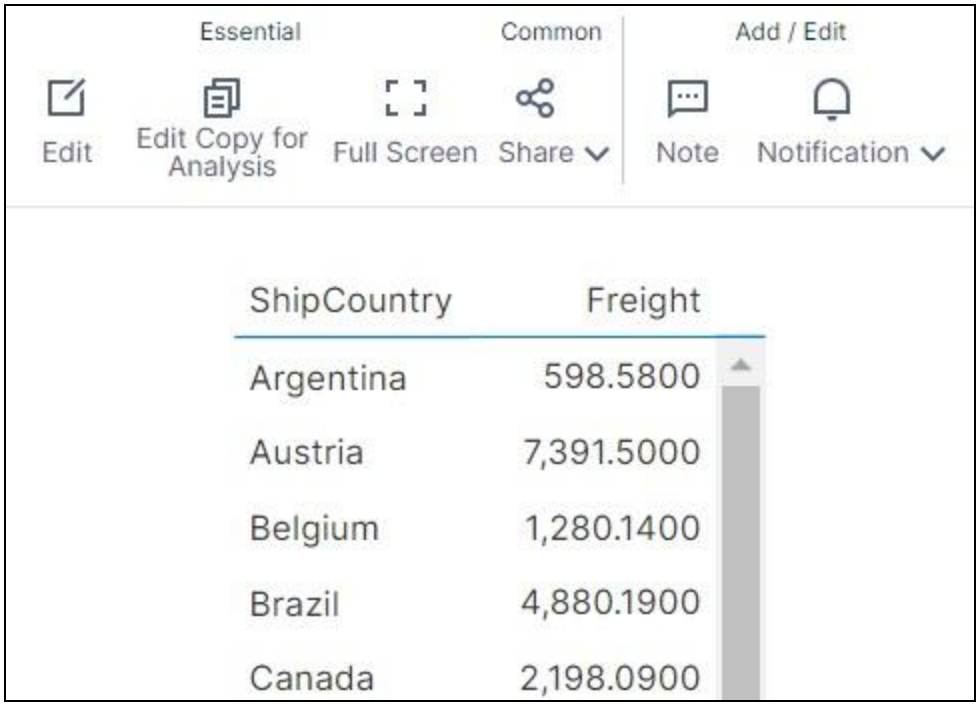


Create a new dashboard

1. Create a new dashboard using the **Blank** template.
2. Open the Export window, locate the new data cube, and drag a measure to the canvas, which appears as a table visualization. In this example, **Freight**.
3. Drag the column you selected earlier over as a dimension to the **Row Header** drop zone on the table.

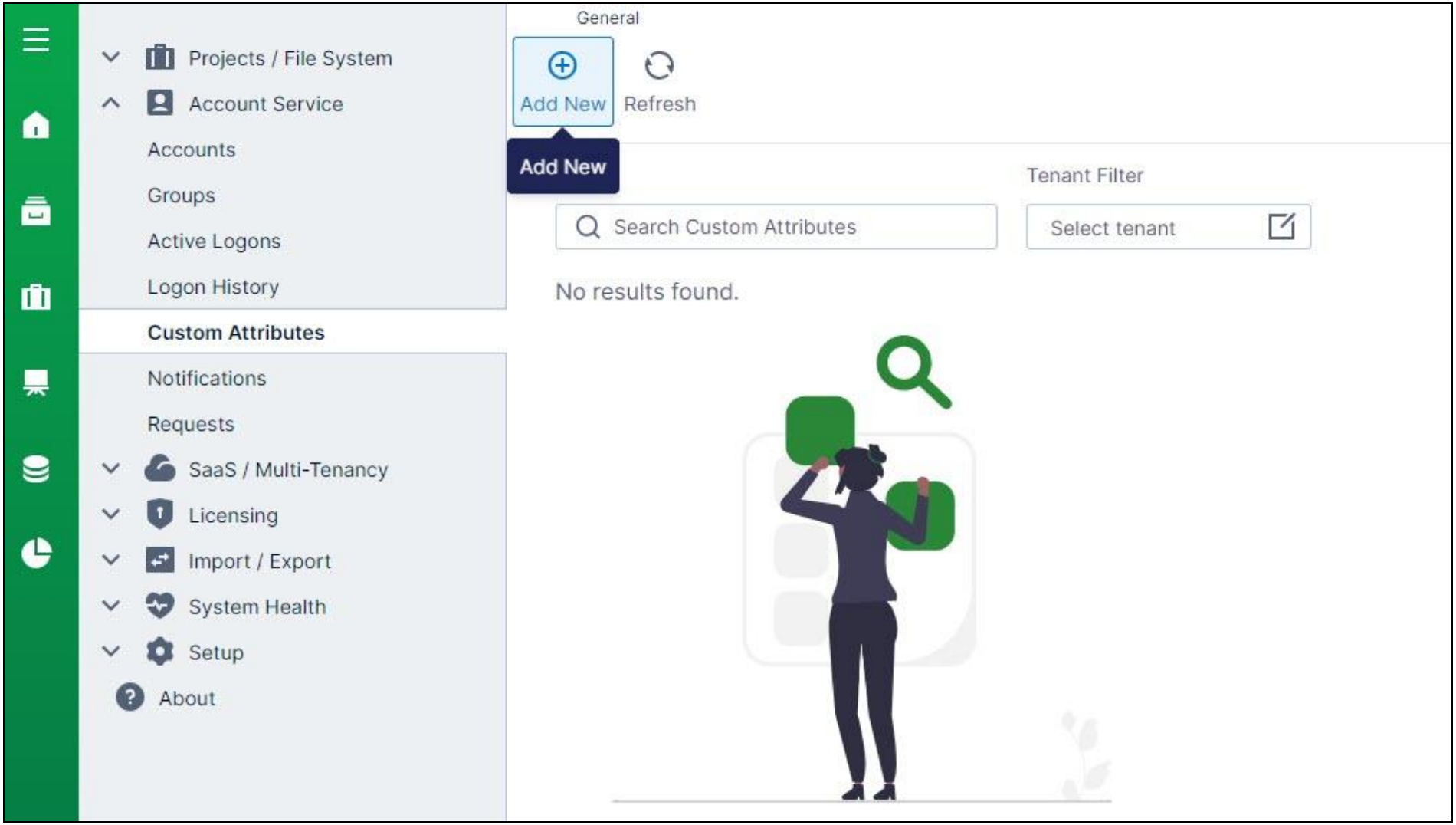


4. In the **ShipCountry** column, verify that the same information is shown here as in the data preview for the data cube.



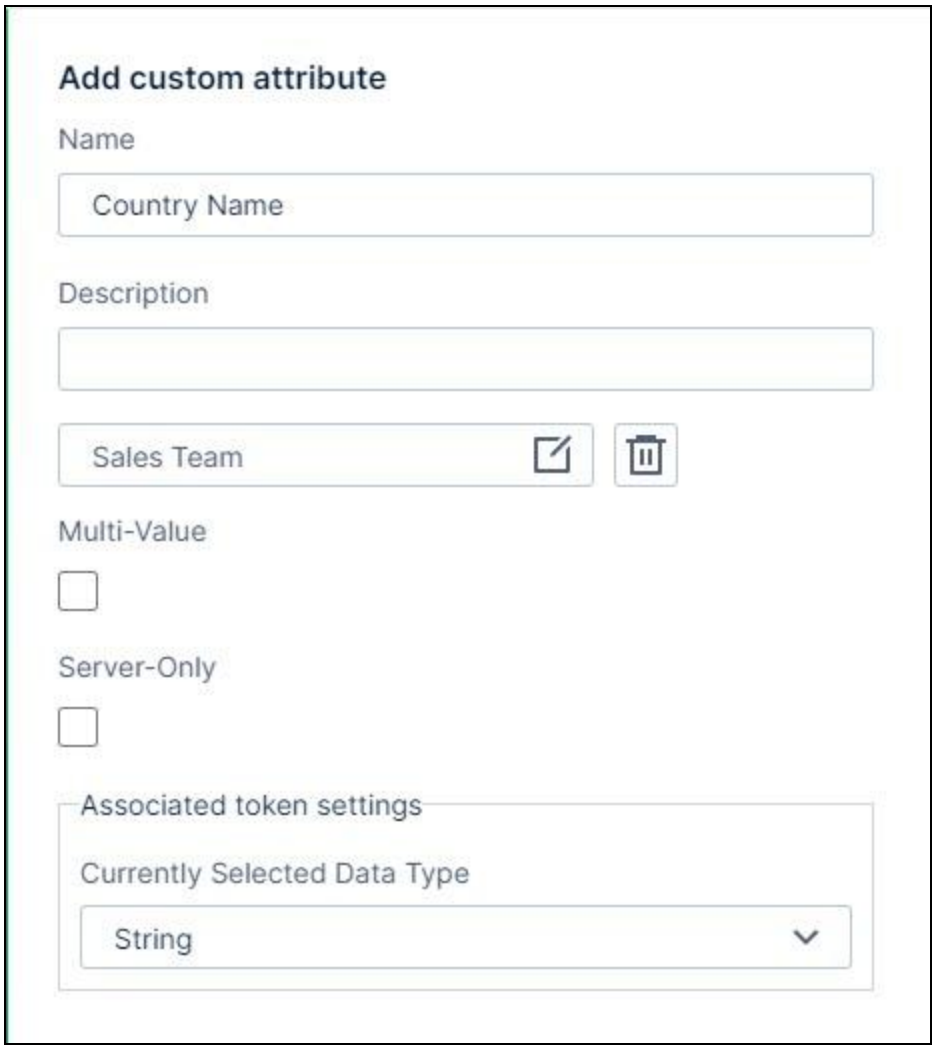
Add a Custom Attribute

In Symphony Administration, select **Account Service** to expand its items and choose **Custom Attributes**, then select **Add New** to add a new custom attribute.



In the **Add Custom Attribute** work area, make the **Name** your preferred name and check that the **Currently Selected Data Type** matches the type of values you will be filtering by. In this example, we use **Country Name** and **String**..

Note: Custom attributes are also applicable in a tenant environment.

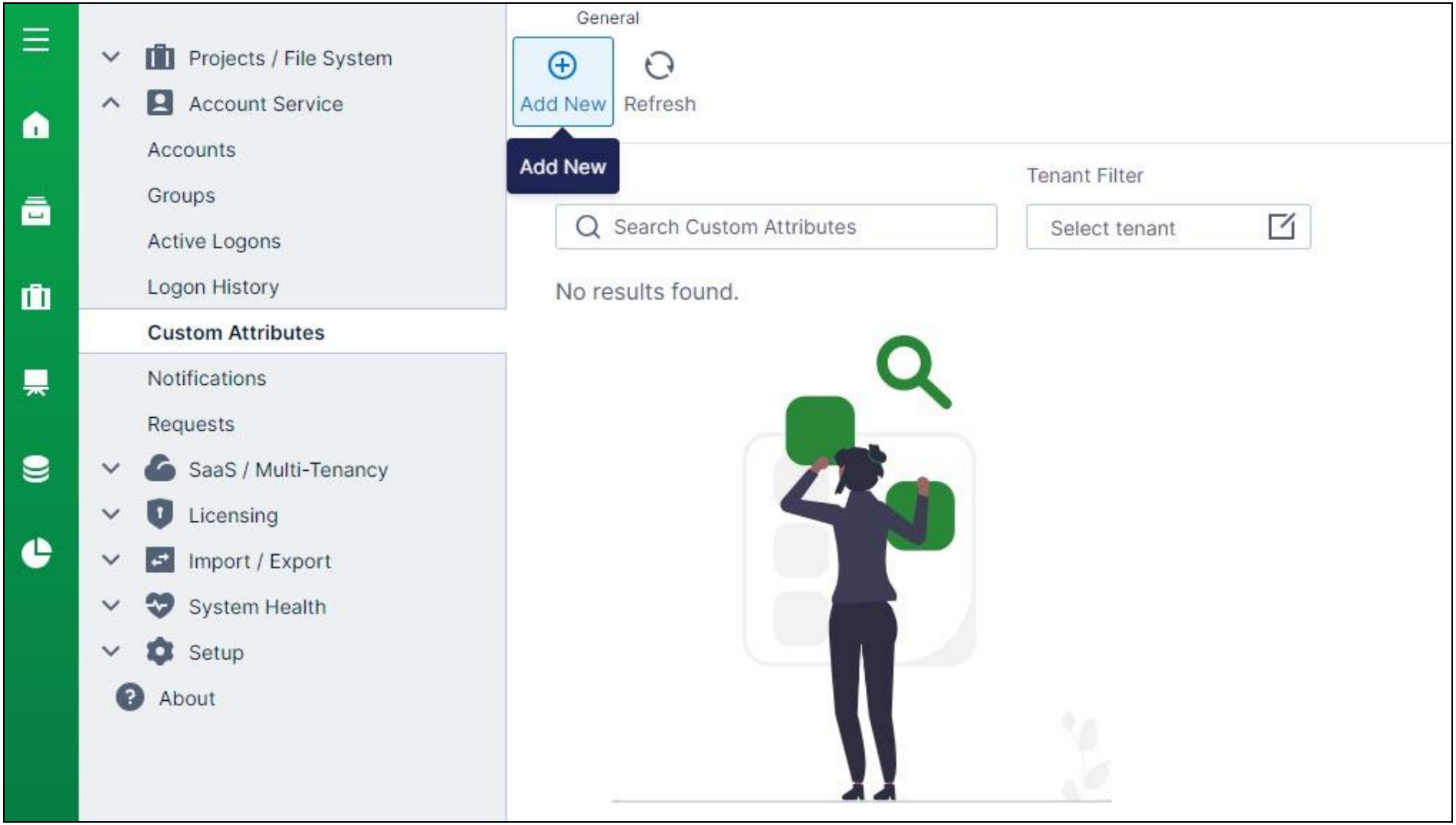


Select **Submit** and the new custom attribute is listed on the page.

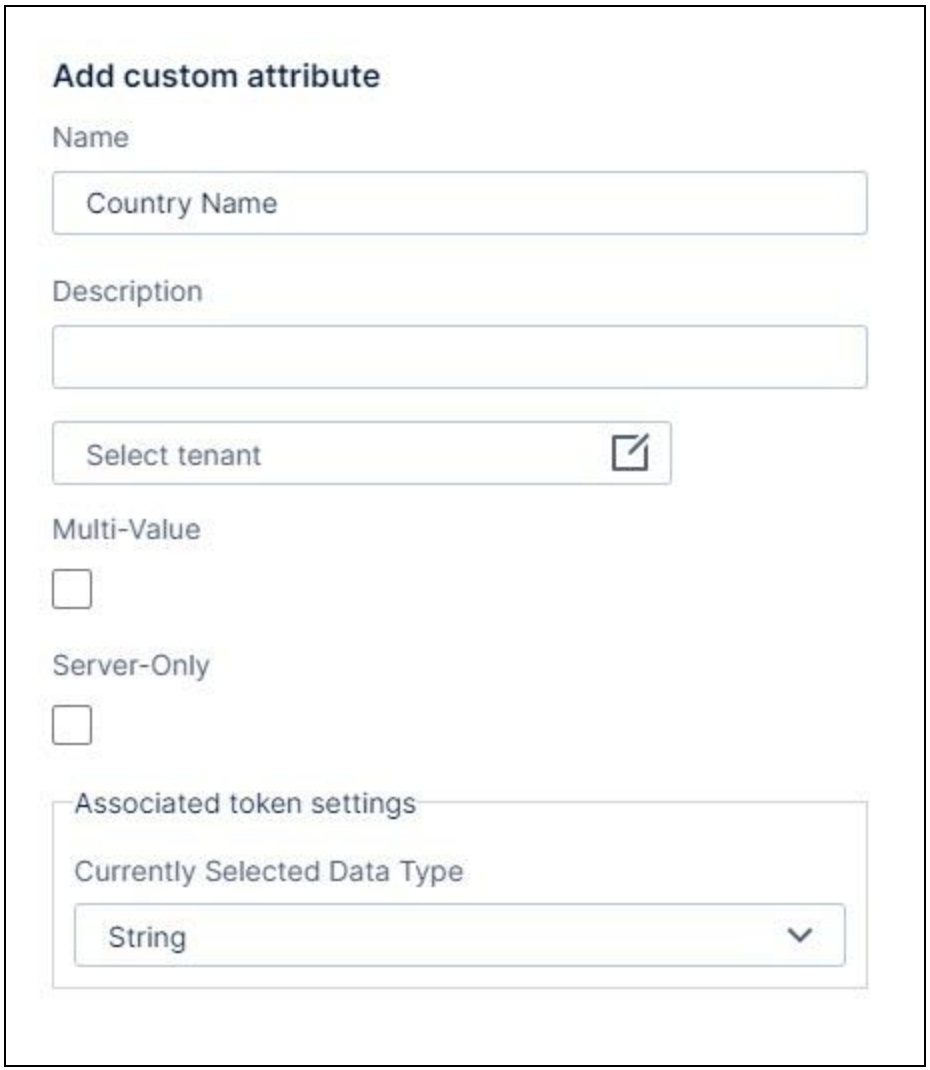
You can return here later and select it to edit it from the toolbar, or you can also check its references to find accounts or groups with values assigned to it or files that are using it.

Add a Custom Attribute

In SymphonyAdministration, select **Account Service** to expand its items and choose **Custom Attributes**, then select **Add New** to add a new custom attribute.



In the *Add Custom Attribute* dialog, set the **Name**and check that the **Currently Selected Data Type** matches the type of values you will be filtering by. **Country Name** and **String** in our example.



Select **Save**. The new custom attribute will be listed on the page.

You can return here later and select it to edit it from the toolbar, or you can also check its references to find accounts or groups with values assigned to it or files that are using it.

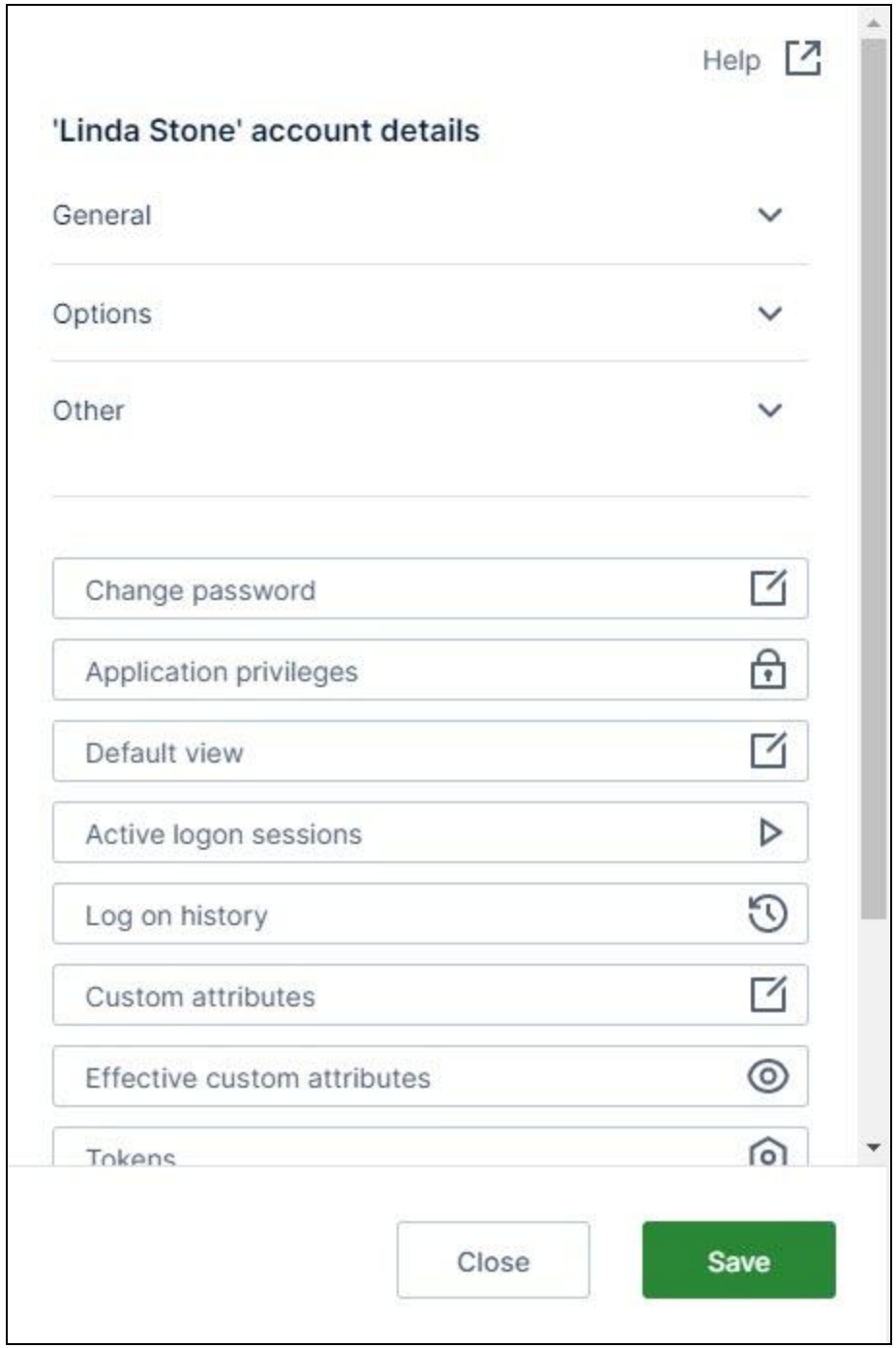
Assign Custom Attribute Values

As an administrator, you can assign the custom attribute values for users, groups of users, and tenants. Assign a value for each user or group that needs to access the data from the data cube that will be filtered.

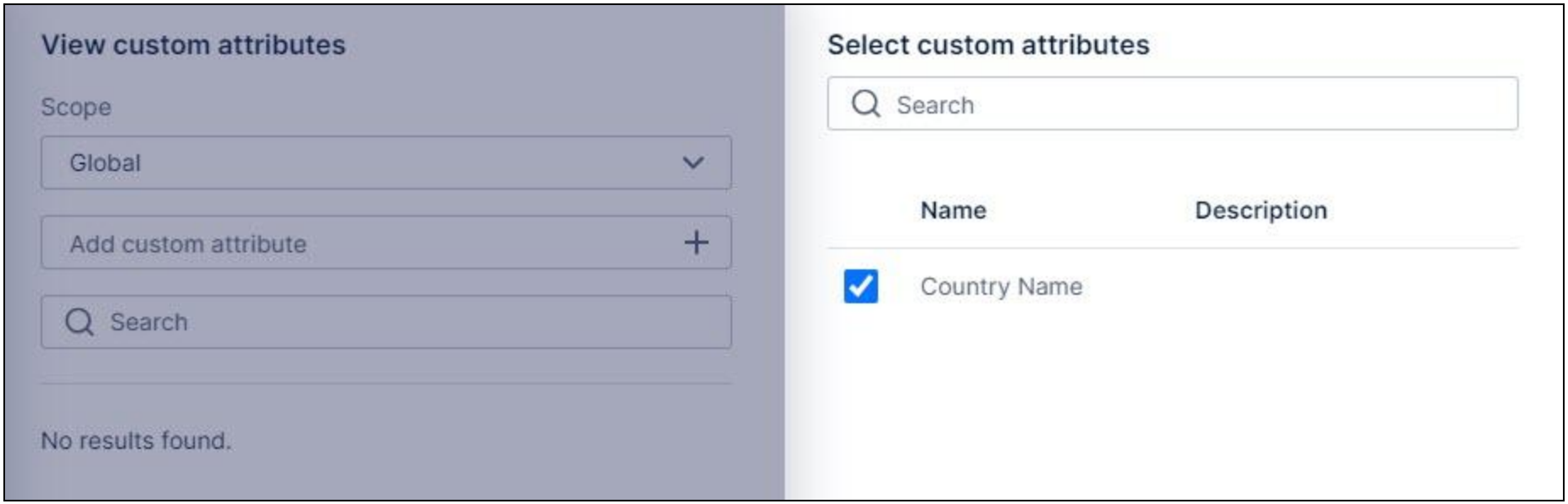
Assign a custom attribute to a user or group

1. Navigate to the Administration work area and select **Accounts** or **Groups** under **Account Service**.
2. Select a user or group, then Edit on the tool bar. A **'*<user name>*' account details** or **'*<group name>*' group details** work area opens.

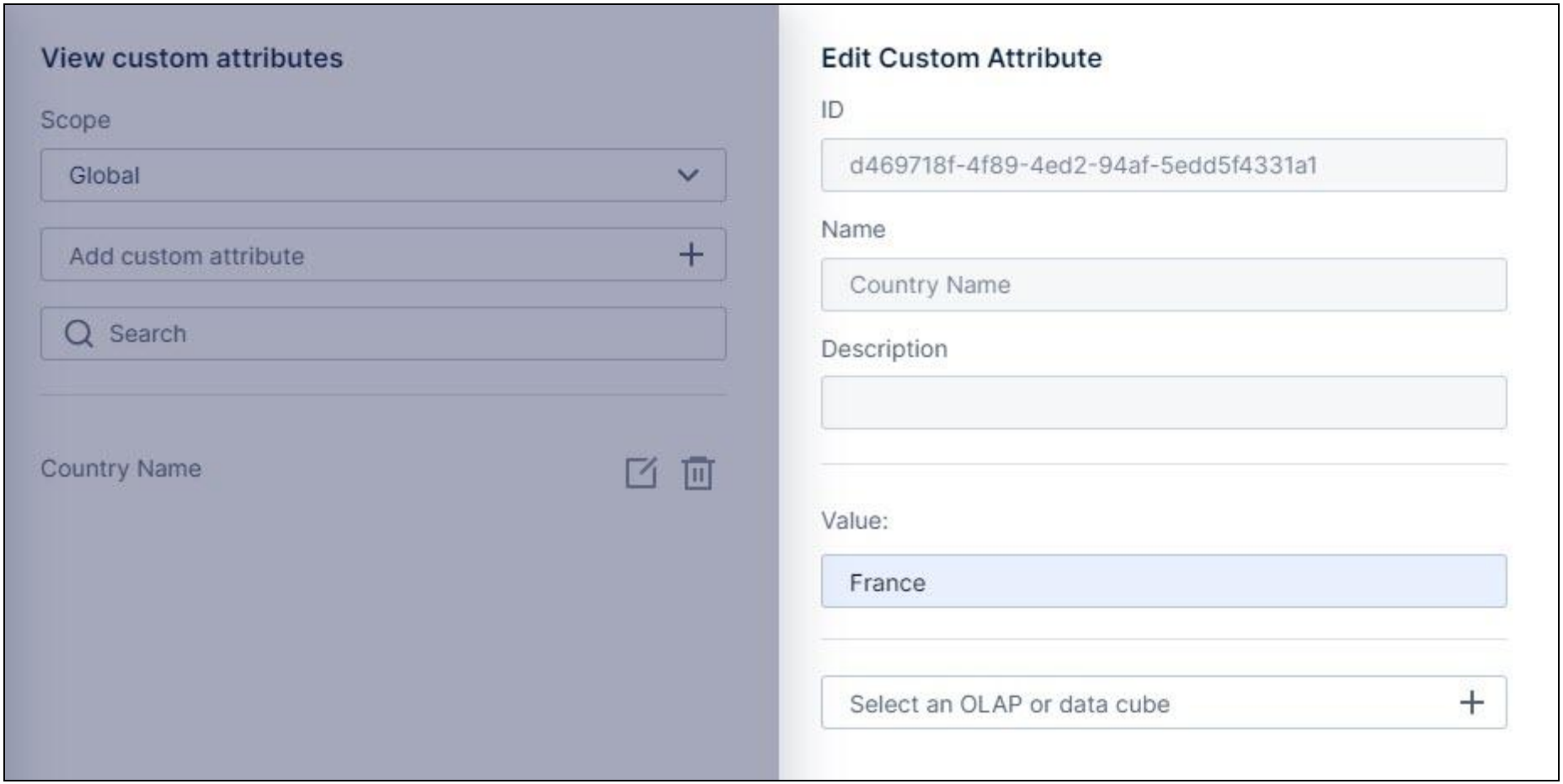
3. Select Custom Attributes to open the **View custom attributes** dialog. Here you can view and update the custom attributes assigned to this user or group.


Help
'Linda Stone' account details
General
Options
Other
Change password
Application privileges
Default view
Active logon sessions
Log on history
Custom attributes
Effective custom attributes
Tokens
Close
Save

4. If applicable, select a **Scope** (Global, or a tenant name).
5. Select **Add custom attribute** to open the **Select custom attributes** dialog.



6. Select the attribute to apply to this user or group, then **Save** your selection. The **Edit Custom Attribute** dialog opens.
7. Enter the value for this custom attribute (or multiple, if mufti-select is applicable to this attribute. In our example, **France**.
8. Optionally, select an OLAP or data cube if security hierarchies are involved. See Using a Security Hierarchy to Filter Data by User.



9. **Save** all of your changes. The custom attribute will affect what the user or group member can see the next time they log in.

Filter a Data Cube Transform

When you edit a data cube, you can configure the SQL Select transform and a Filter to filter the cube's data by each user's custom attribute values. These values may be directly applicable to the user, or secondarily through group or tenant membership.

Add a filter transform to a data cube

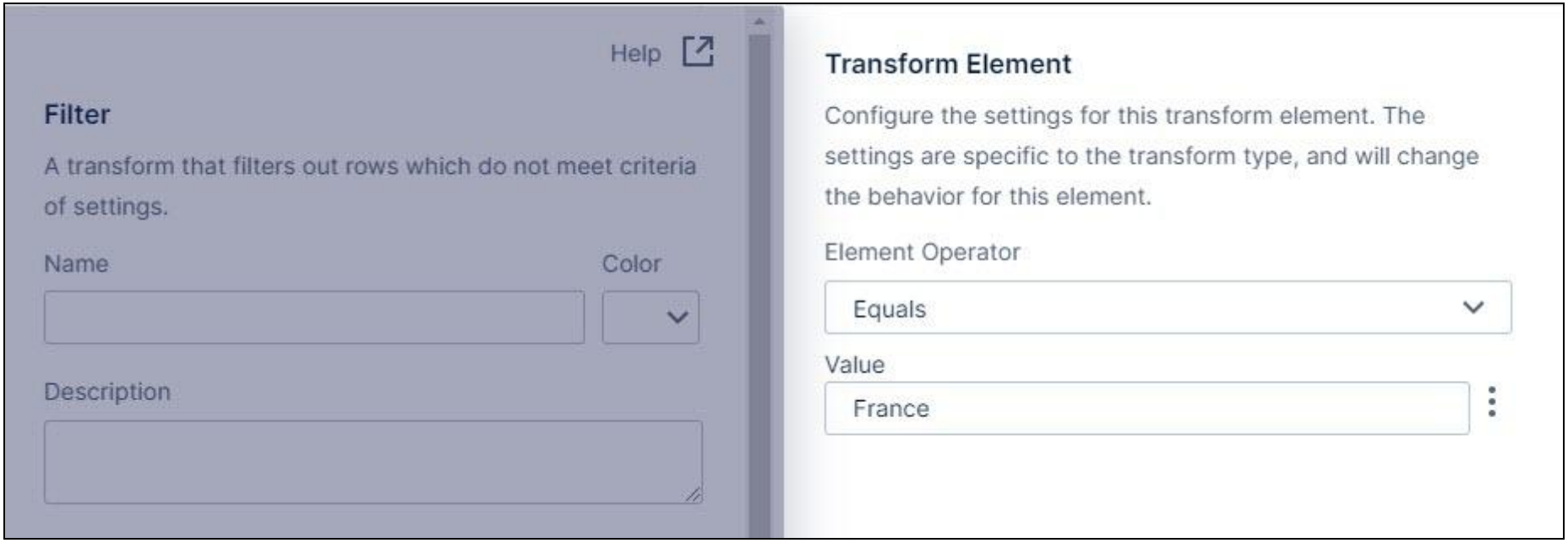
1. Open a data cube that contains a filter or an SQL Select transform. Select the link between two transforms, for example, from a SQL Select transform to a Process Result transform.

2. Add a **Filter** from the **Add / Edit** menu.

3. Select the filter. Using the Contextual menu or the right-click menu, select **Configure** to open a Filter dialog.

4. Scroll through the list of columns (Input Elements) to find an element to filter and edit it to open the **Transform Element** dialog. For our example, this is **ShipCountry**.

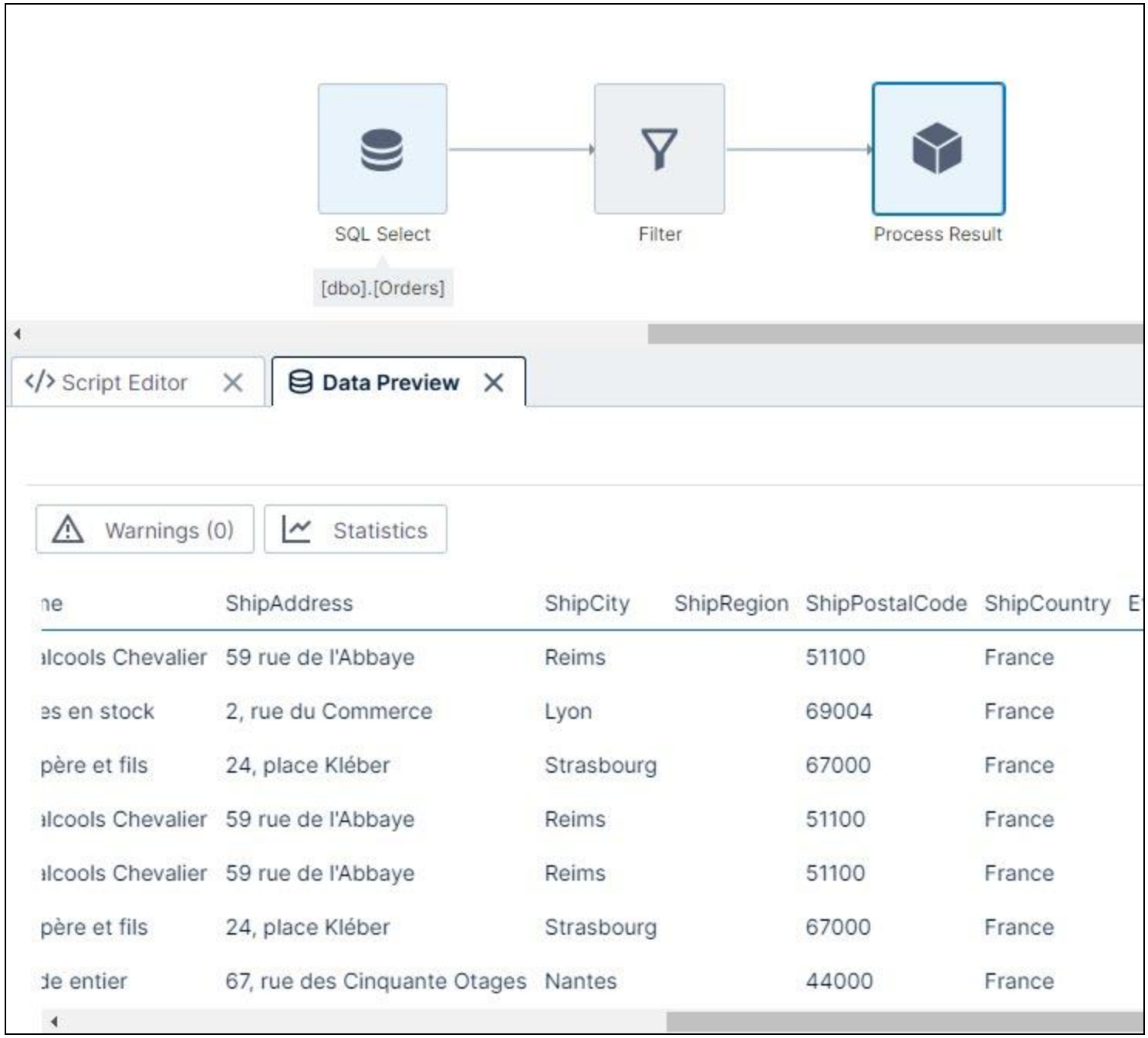
5. Set the Element Operator to select your desired filter option, and a value or values the filter should use. For our example, **Equals** and **France**.



6. Save your changes. This filter value is now applied to the data as it is read from the source transform (**SQL Select**) through to the next transform (in this example, **Process Result**).

7. To verify your results, select the Process Result transform while logged in as the user or the member of a group this custom attribute is applied to. The Data Preview window shows only data that meets the custom attribute defined in the Filter.

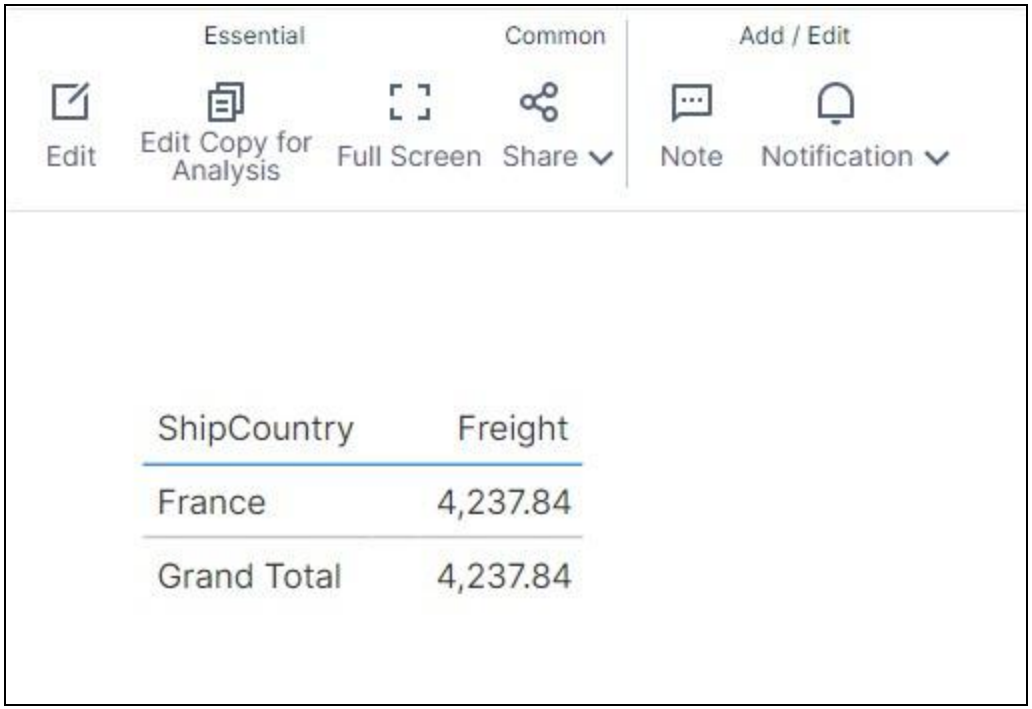
Note: If you've defined this custom attribute for a specific user, group, or tenant, it will only show for that user, members of the specific group, or members of the tenant.



ne	ShipAddress	ShipCity	ShipRegion	ShipPostalCode	ShipCountry	E
lcools Chevalier	59 rue de l'Abbaye	Reims		51100	France	
es en stock	2, rue du Commerce	Lyon		69004	France	
père et fils	24, place Kléber	Strasbourg		67000	France	
lcools Chevalier	59 rue de l'Abbaye	Reims		51100	France	
lcools Chevalier	59 rue de l'Abbaye	Reims		51100	France	
père et fils	24, place Kléber	Strasbourg		67000	France	
de entier	67, rue des Cinquante Otages	Nantes		44000	France	

Verify the Data in a Dashboard

Open the dashboard you created earlier. The table visualization only shows records with a **ShipCountry** of **France**.



Multi-Value Custom Attributes

Custom attributes can hold a single value, or support multiple values.

Define a multi-value custom attribute

1. Create a new custom attribute by navigating to **Administration** > **Account Service** > **Custom Attributes**.

   Note: You also edit an existing custom attribute to make it multi-value.

2. Select to enable (check the check box) **Multi-Value** on the **Add custom attribute** or **Edit custom attribute** dialog.

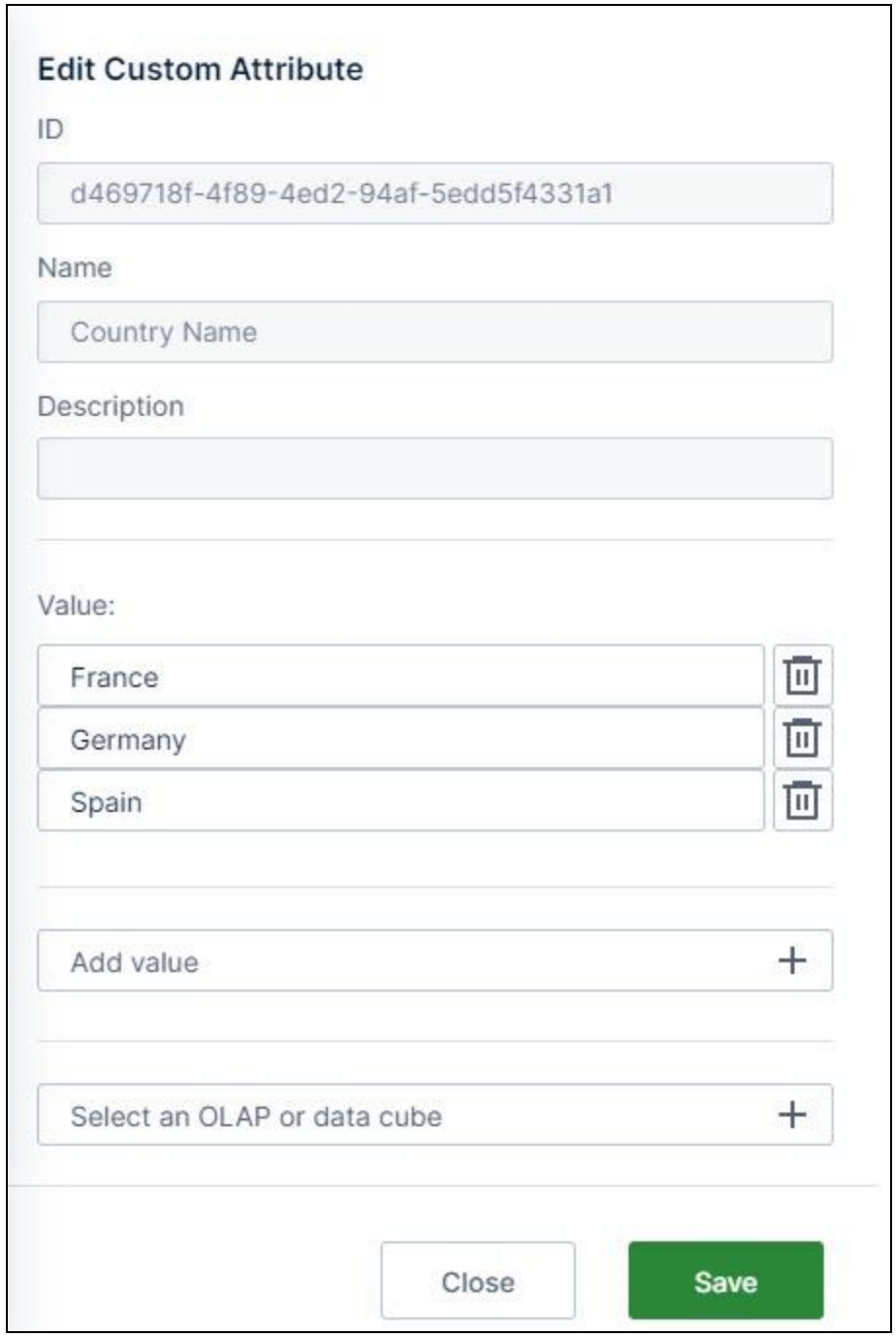
   Important: If you save a custom attribute as multi-value attribute, it can no longer be a single value attribute. Delete it and recreate it as a single-

value attribute.

3. Next, edit values for the custom attribute for the user, group, or tenant account. Navigate to the Administration work area and select **Accounts** or **Groups** under **Account Service**.

4. Select **Custom attributes** on the **'*<user name>*' account details** or **'*<group name>*' group details** work area. The **View custom attribute** dialog opens.

5. Select the attribute to edit. The **Edit Custom Attribute** dialog opens. Select **Add value** to add more values as needed. In this example, **Germany** and **Spain**.


Edit Custom Attribute
ID
d469718f-4f89-4ed2-94af-5edd5f4331a1
Name
Country Name
Description
Value:
France
Germany
Spain
Add value
Select an OLAP or data cube
Close
Save

6. **Save** all of your changes. The custom attribute will affect what the user or group members can see the next time they log in.

Add a parameter to the data cube to use the multi-value custom attribute

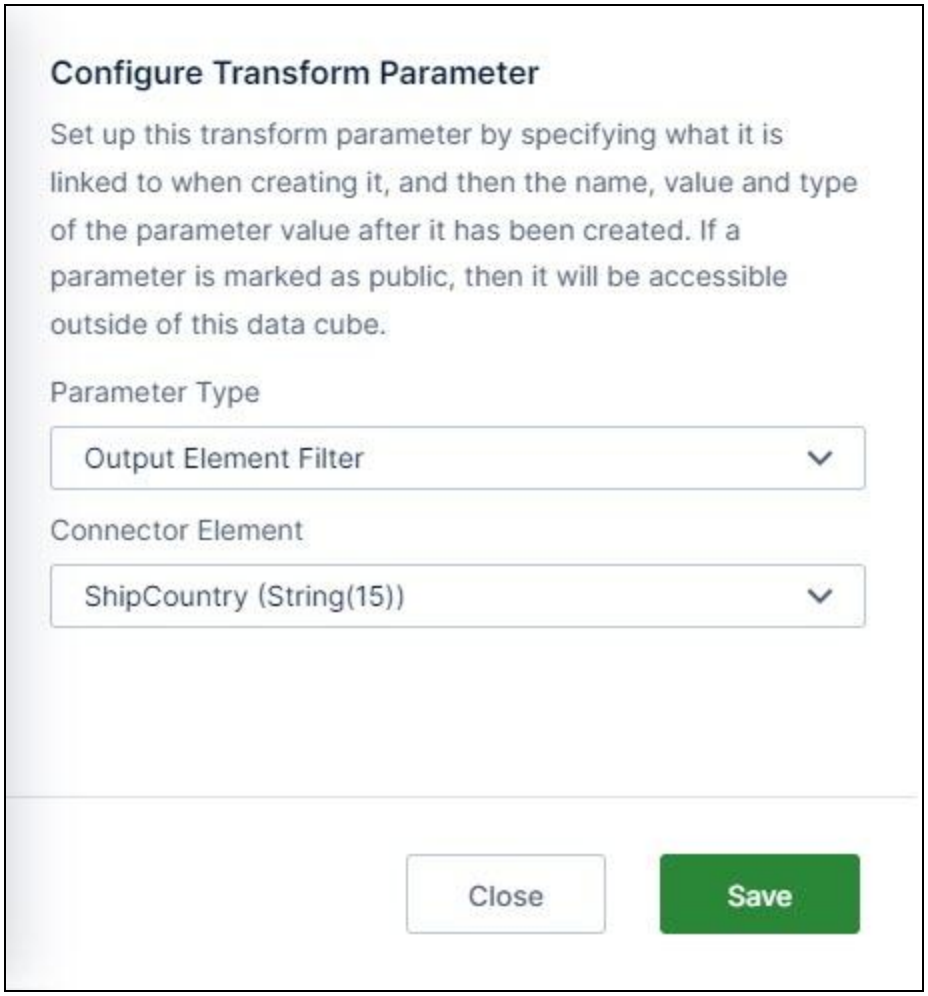
1. Open and edit a data cube that includes at least one SQL Select transform.

   Note: If you use the same data cube created earlier, remove the filter transform.

2. Select the SQL Select transform. Using the Contextual menu or the right-click menu, select **Configure** to open a SQL Select dialog.

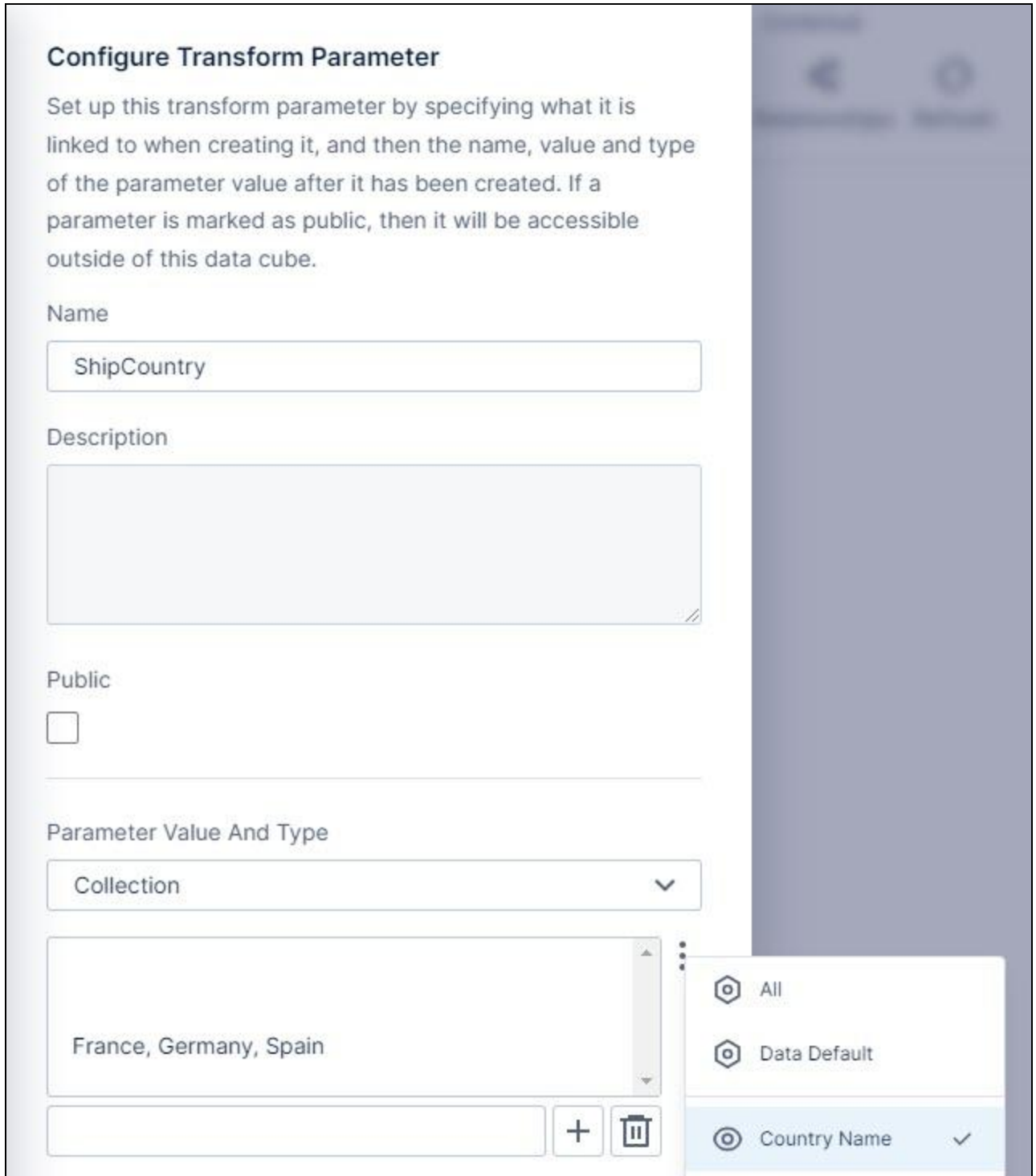
3. Scroll to select and edit **Parameters**. The **Transform Parameters** dialog opens. Select **Add parameter** to open the **Configure Transform Parameter** dialog.

4. Set the Parameter Type you wish to use, and select the Connector Element that is used. In this example, **Output Element Filter** and **ShipCountry (String (15))**.



5. Select **Save**. The **Configure Transform Parameter** work area opens.

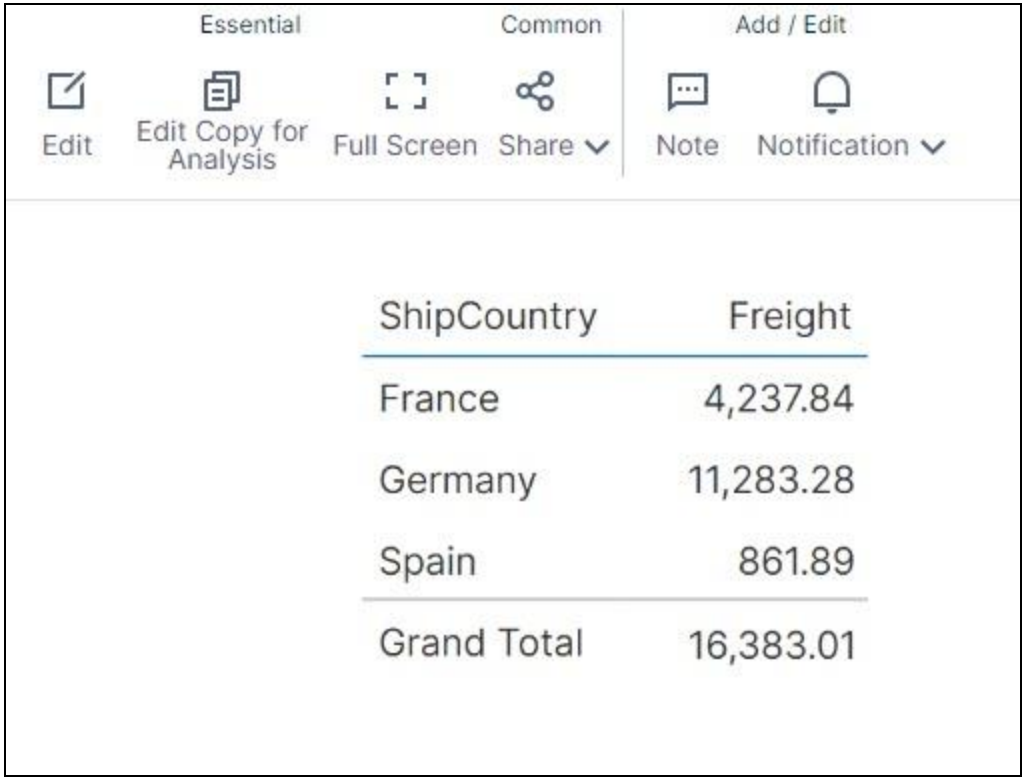
6. Define the Parameter Value and Type as Collection (for multi-value custom attributes), then select the parameter name from the overflow menu. In this example, **Country Name**.


Configure Transform Parameter
Set up this transform parameter by specifying what it is linked to when creating it, and then the name, value and type of the parameter value after it has been created. If a parameter is marked as public, then it will be accessible outside of this data cube.
Name
ShipCountry
Description
Public
Parameter Value And Type
Collection
France, Germany, Spain
All
Data Default
Country Name

7. **Close** all open dialog boxes.

Verify the Data in a Dashboard

Open the dashboard you created earlier. The table visualization only shows records with a **ShipCountry** of **France**, **Germany**, and **Spain**.



- Filtering the raw data using a transform parameter in a data cube is too low-level to determine which values appear to different users in filters connected to a hierarchy, and whether notes attached to hierarchy values can be shared between users. Use custom attributes with a security hierarchy instead to affect the values shown in hierarchy filters and to allow notes to be shared between users when appropriate.

- Select the **Server Only** option to prevent the custom attribute value from being sent to the user's web browser, in case it contains sensitive information or large amounts of data. These custom attribute values can only be read by system administrators, as well as tenant administrators if the custom attribute was

associated with their tenant.

- In the case of a single-value custom attribute or a multi-value value with an inheritance behavior of **Override**, the attribute value set for an account will override any values inherited from groups. If there is no value set on the account, differing values inherited from multiple groups may result in a conflict error.

For more information, see:

- Advanced User Management
- Advanced Group Management
- Data Cubes
- Using a Security Hierarchy to Filter SSAS Data by User
- Using a Security Hierarchy to Filter Data by User
- Multi-Tenancy in Symphony
- Managing Tokens
- Off the Charts: Use Row-Level Security to Filter Data by User

Using Custom Data and Custom Attributes to Filter SSAS Data

This applies to: *Managed Dashboards, Managed Reports*

By connecting to SSAS (SQL Server Analysis Services) using roles impersonation, you can automatically filter data according to the Symphony user who is logged on. However, this approach can become difficult to manage when there are a lot of roles.

Another option is to use the Custom Data setting of SSAS data connectors in conjunction with custom attributes to secure access to the data. This method requires only one role on the SSAS side.

This is an advanced topic for Symphony administrators.

> **Note:** See the article on using a security hierarchy to filter SSAS data by user for an alternative that doesn't require configuration within the database or script.

The following walkthrough uses the Adventure Works DW sample database for illustration.

Set Up a Role in SSAS

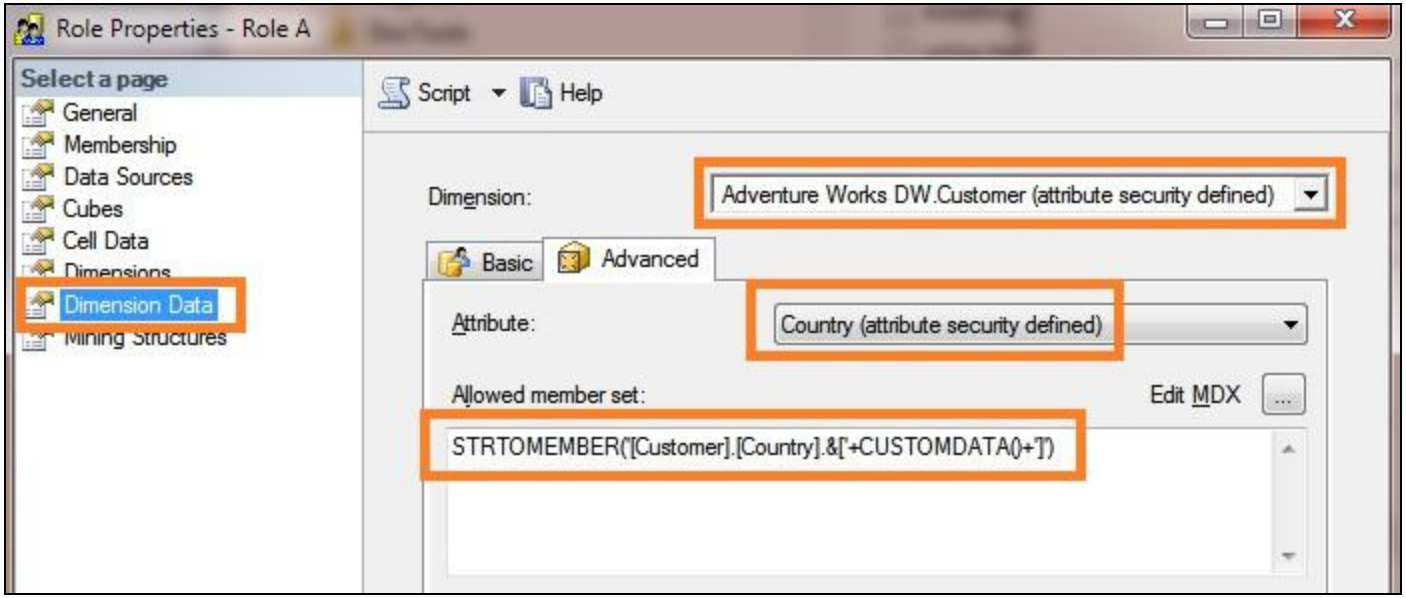
Launch SQL Server Management Studio and connect to Analysis Services.

Create a new role **(Role A)** as described in Using SSAS roles impersonation but with the following differences:

1. In the *Role Properties* dialog, click **Dimension Data** on the left.
2. Set the **Dimension** drop-down to the *Customer* dimension.
3. Set the **Attribute Hierarchy** drop-down to *Country*.
4. Click the **Advanced** tab and enter the following MDX in the **Allowed member set** box.

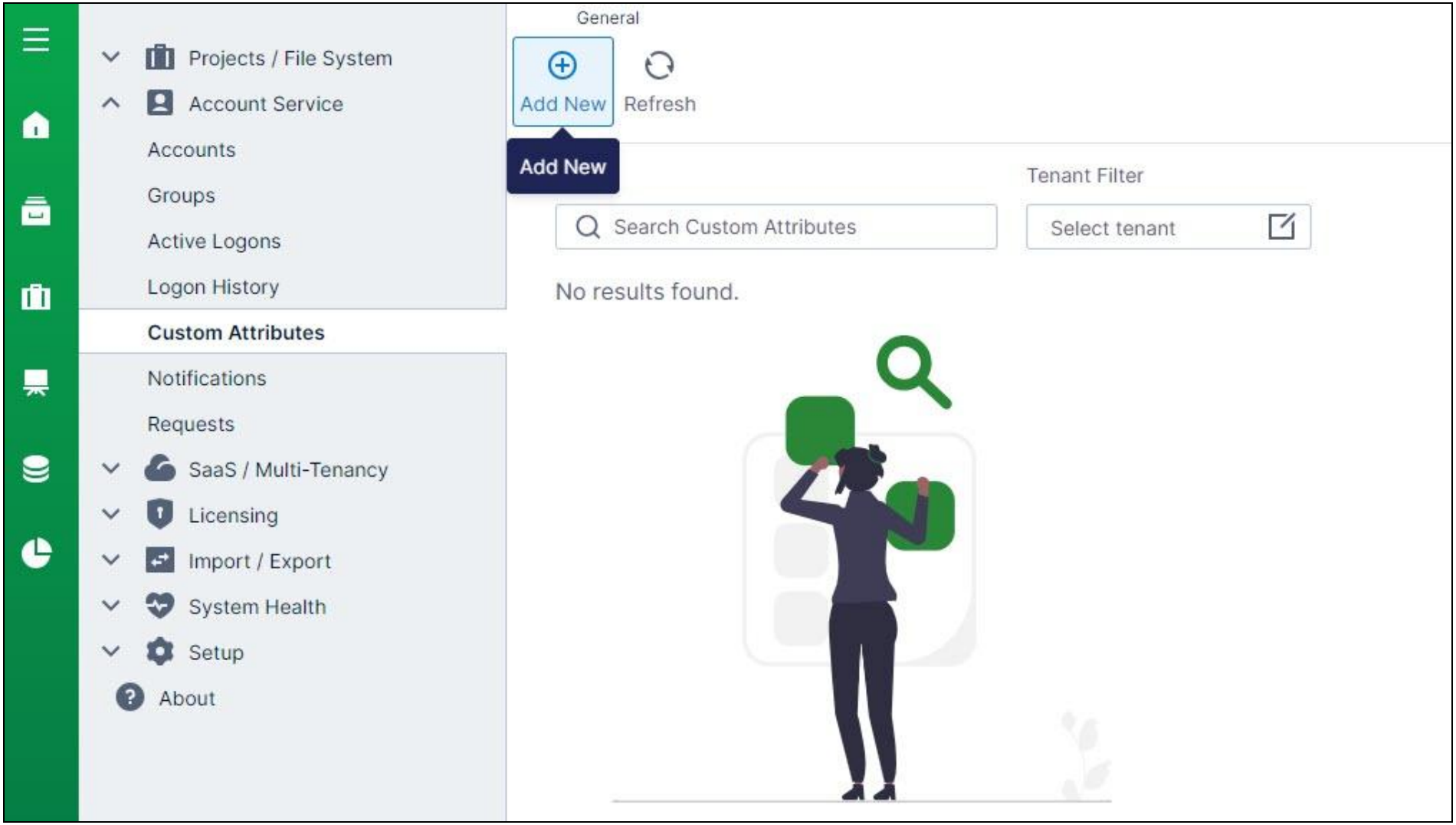
```
STRTOMEMBER('[Customer].[Country].&['+CUSTOMDATA()+']')
```

This MDX is variable because of the `CUSTOMDATA()` function which will return a custom attribute value that has been assigned to a Symphony user. This is the key to how the data will be filtered.



Create a Custom Attribute

In Symphony Administration, click **Account Service** to expand its items and choose **Custom Attributes**, then select **Add New** to add a new custom attribute.

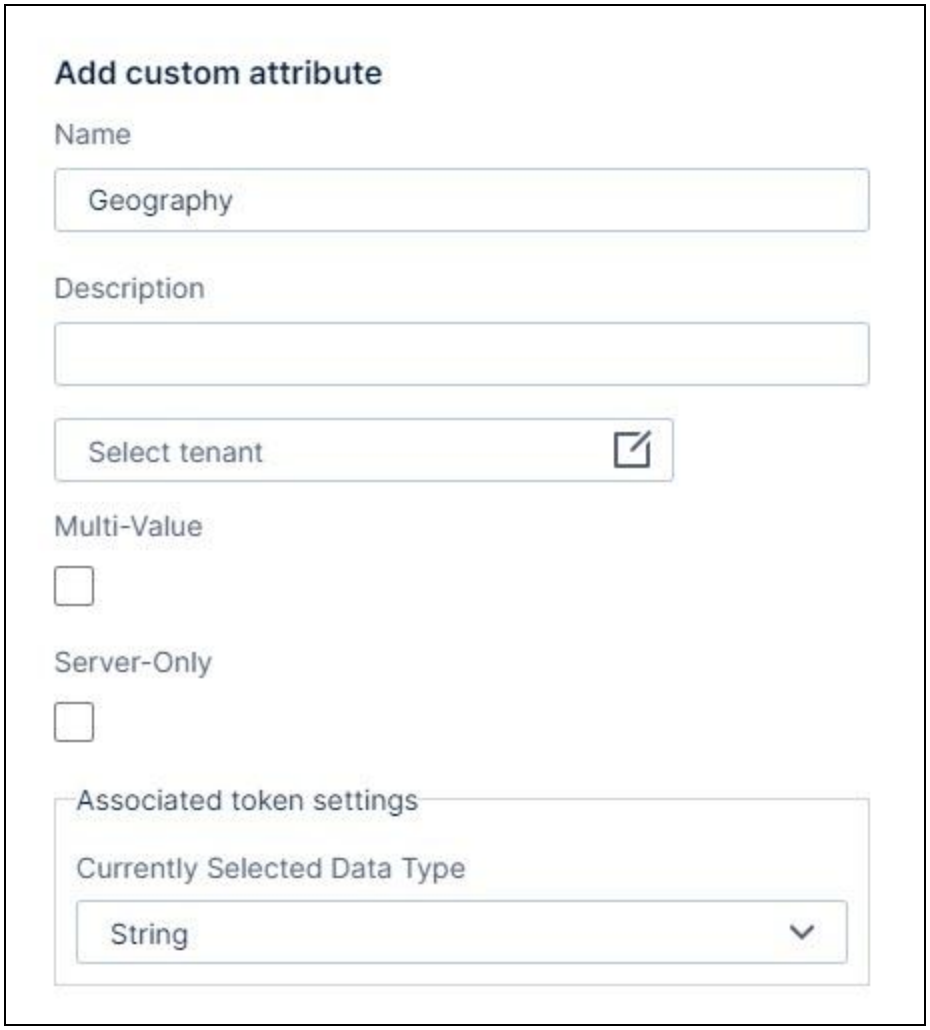


In the **Add Custom Attribute** dialog, make the **Name** of the custom attribute **Geography**,and check that the **Currently Selected Data Type** is **String**.

Custom attributes are also applicable in a tenant environment:

- If you are a system administrator and your environment includes multiple tenants, decide which tenant you'd like to apply the custom attribute to, and add them by selecting **Select tenant**. This opens a list of available tenants. Select a tenant, then **Save** the selection.

- If you are an admin or other user working as a tenant admin or other tenant member, this custom attribute is automatically applied to the your current tenant.



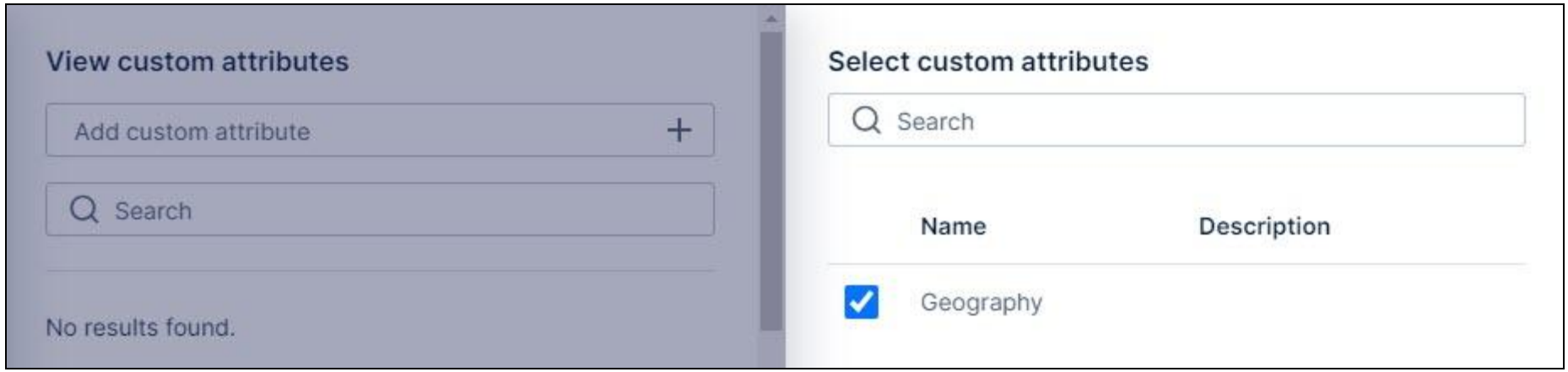
Save the custom attribute. You'll see a message indicating the custom attribute has been saved, and it will be listed in the *Custom Attributes* dialog.

Set Up a User Group and Account

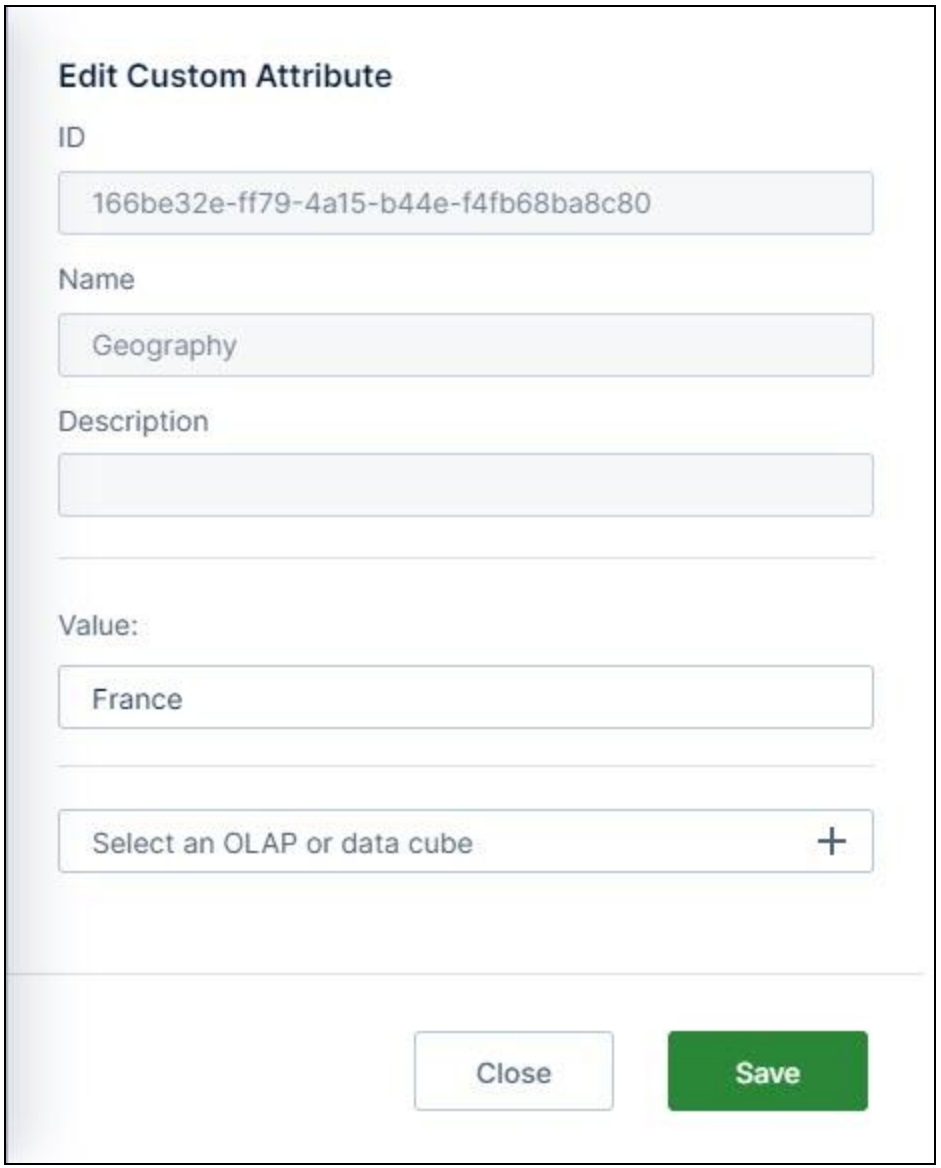
1. Create a new group named **Role A**. This name must match that of the SSAS role exactly.
2. Then, create a user account named *User A* and add as a member of the group **Role A**.
3. Next, assign a custom attribute to the user.

Assign Custom Attributes to a User

1. Open the **Accounts** work area by navigating to **Profile** > **Administration** > **Account Service** > **Accounts**. A list of users opens for your environment, or for the tenant you are working in.
2. Select **User A** and **Edit** in the Contextual menu. The **'User A' account details** work area opens.
3. Scroll to down to **Custom attributes** and select it to open a **View custom attributes** work area.
4. Select **Add custom attribute** to open the **Select custom attributes** dialog. This lists available custom attributes you can assign to this user.



5. Select the checkbox for the **Geography** custom attribute, then Save. An **Edit Custom Attribute** dialog opens.
6. Enter the value for this custom attribute (or multiple, if mufti-select is applicable to this attribute. In our example, **France**. Select **Save** to save this attribute.

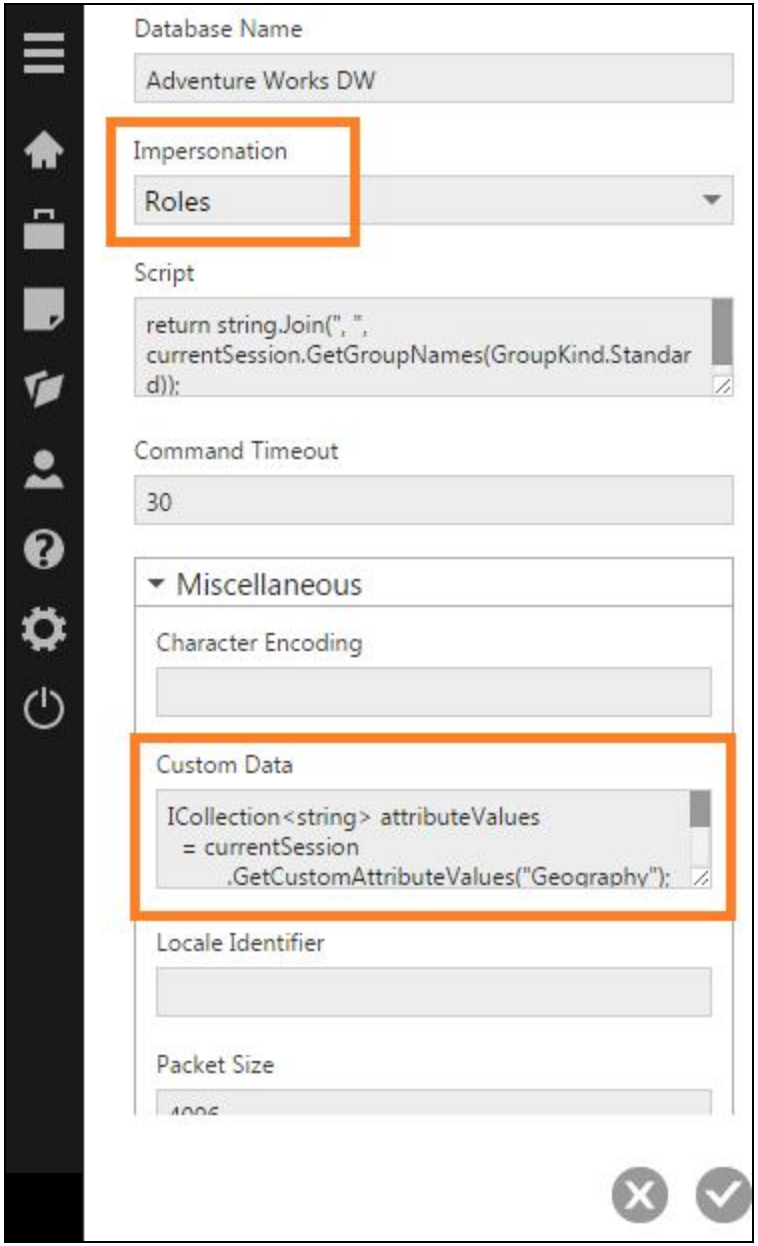


Create a New Data Connector

From the main menu, create a new data connector using the SSAS provider:

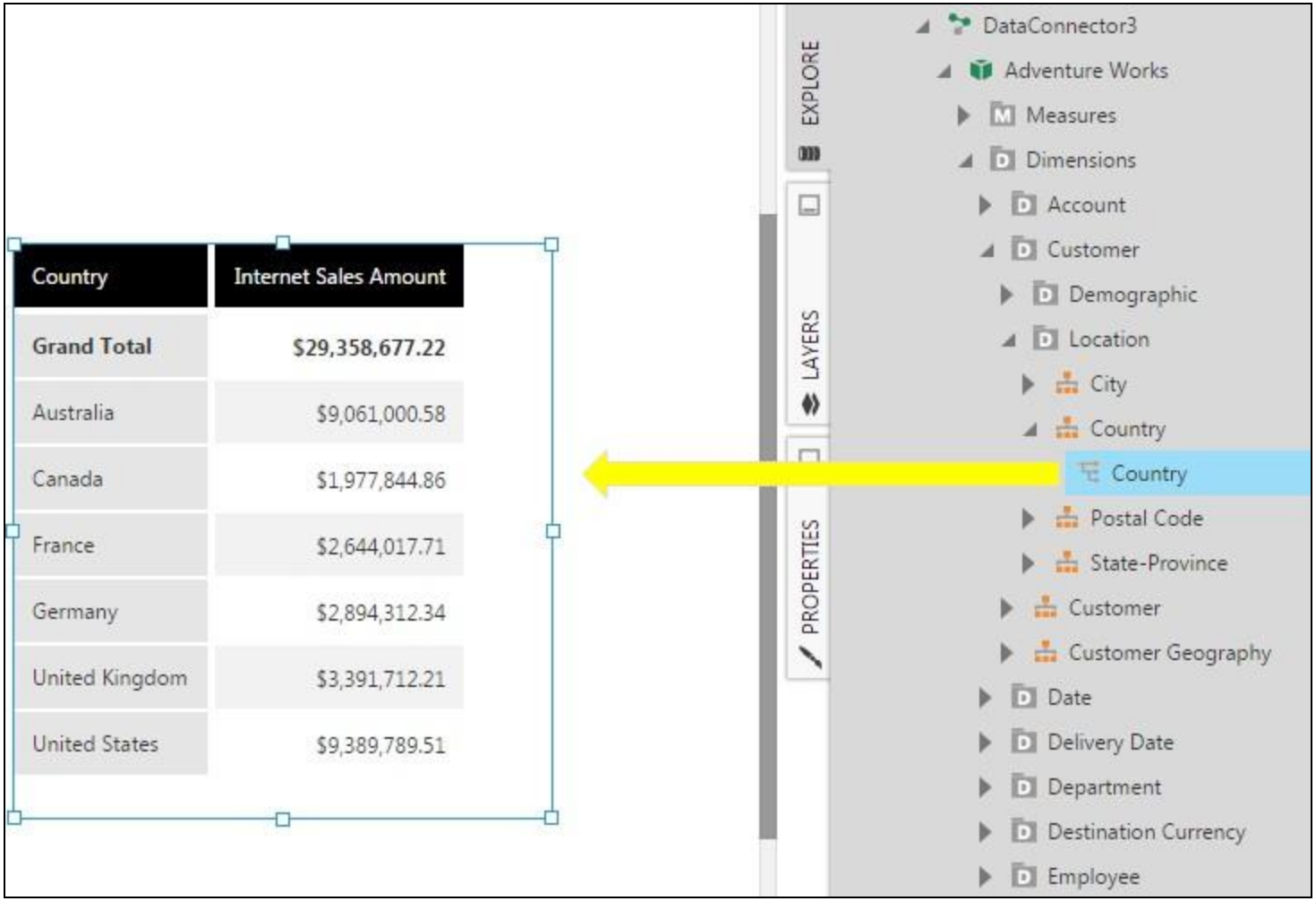
- Set **Windows Impersonation** to *Specified* and enter the domain credentials that were added to the SSAS Membership pages when setting up Role A.
- Set the **Database Name** to the name of the SSAS database.
- Set the **Impersonation** drop-down to *Roles*.
- Expand the **Miscellaneous** section and enter the following script in the **Custom Data** box. This script retrieves the user's *Geography* custom attribute value and returns it to the CUSTOMDATA() function on the SSAS (MDX) side.

```
ICollection<string> attributeValues
       = currentSession
              .GetCustomAttributeValues("Geography");
if (attributeValues != null) { return String.Join(", ", attributeValues); }
else { return String.Empty; }
```


Database Name
Adventure Works DW
Impersonation
Roles
Script
return string.Join(", ",
currentSession.GetGroupNames(GroupKind.Standar
d));
Command Timeout
30
Miscellaneous
Character Encoding
Custom Data
ICollection<string> attributeValues
= currentSession
.GetCustomAttributeValues("Geography");
Locale Identifier
Packet Size

Create a New Dashboard

Create a new dashboard by dragging the *Internet Sales Amount* measure and the *Country* level from the newly created data connector to the dashboard canvas.

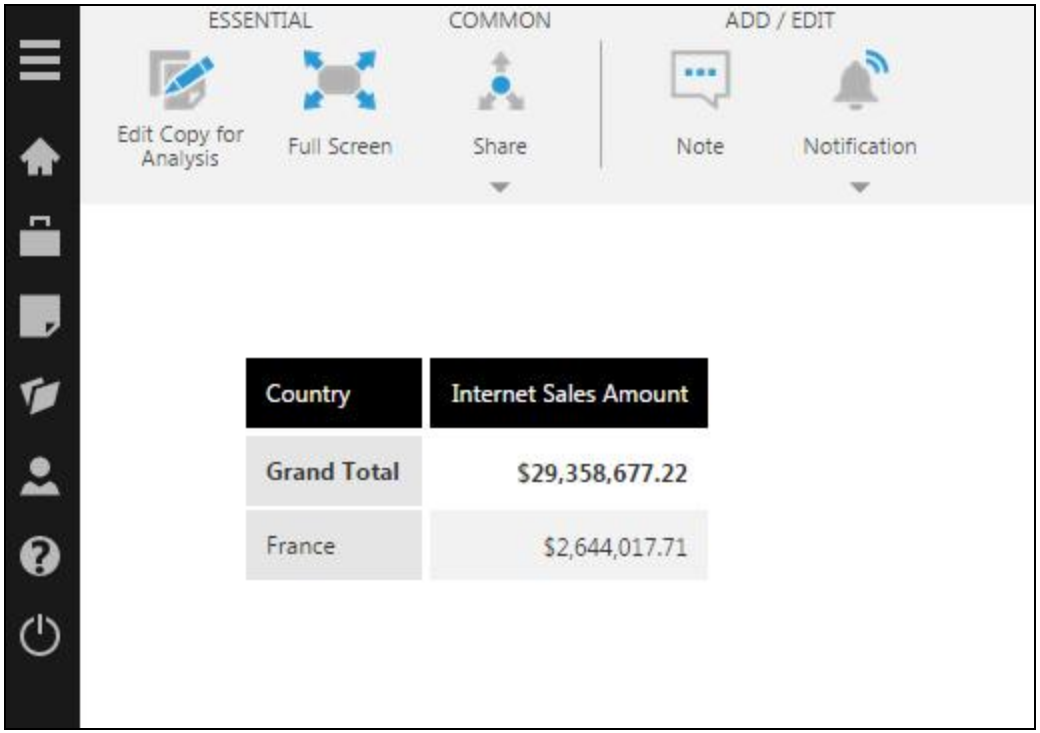


Check In your dashboard so other users can view it.

View the Dashboard

Log out of Symphony and log on as the restricted User A.

Open the dashboard for viewing and observe that the chart shows data for France only.



You can apply a similar process to make use of the *Cell Security* functionality in SSAS; however, you will have to disable certain MDX optimizations. To do so, locate the relevant measure from your cube in the Explore panel, right-click on it, select **Slicer As Subquery**, and select **Disable**.

For more information, see:

- Use Custom Attributes to Filter Data by User
- Using a Security Hierarchy to Filter SSAS Data by User
- Connect to OLAP Data and Apply a Formula
- Advanced User Management
- Advanced Group Management

Using the dt Command Line Tool

This applies to: *Managed Dashboards, Managed Reports*

The **dt** tool lets you perform various admin/configuration tasks from the command-line:

- reset the admin password
- run a health check on the application
- change configuration settings
- encrypt/decrypt the connection information stored in the application's config file

Note: Most of these tasks can be performed within Symphony's Admin interface.

Using dt

On the server where Symphony is installed, open a **Command Prompt** window (**Terminal** on Linux) and navigate to the **tools** installation subfolder. On Windows, type *dt* followed by a command, and on Linux, type *./dt.sh* followed by a command.

For example, type *dt help* or *./dt.sh* help to get the help page for this tool.

```
Dundas BI Tools version 24.4.0.0-w.[redacted]
Copyright (c) 2014-2024 Dundas Data Visualization, Inc. All rights reserved.

Type dt.exe help <command name> for command description.

Commands:
dt help                    Type dt.exe help <command name> for command description.

dt createAppDb             Creates a new application database or initializes a previously-created empty application database.

dt createWarehouseDb       Creates a new data warehouse database or initializes an empty one created before.

dt scriptDb                Generates creation scripts for the application or warehouse database.

dt upgradeDatabases        Upgrades the application and warehouse databases.

dt resetAdminPassword      Resets the password for the built-in administrator account.

dt setConfigValue          Sets the global value or resets all scope and target values of a configuration setting.

dt healthCheck             Performs an application health check.

dt reviveAppDb             Revives an application database containing only data.

dt reviveWarehouseDb       Revives a warehouse database containing only data.

dt configFile              Performs operations related to the dbi.config file.

dt installLicense          Installs a license.

dt getExportConfigFile     Gets export configuration as a file.

dt export                  Exports application data into a DBIE file.

dt import                  Imports application data from a DBIE file.

dt deleteOldEntityData     Deletes old entity revisions checked in before a specified date. The most current revision is never deleted.

dt generateViewThumbnails  Generates thumbnails for views which don't already have them.

dt migrateTenantData       Migrates tenant data to or from tenant warehouse database.

dt manageAppResources      Lists, gets, stores or deletes standard application resources.

dt manageLocalizations     Lists, gets, stores or deletes localization resources.

dt manageExtensions        Lists, gets, stores or deletes extensions.

dt anonymizeWarehouse      Creates a warehouse database with anonymized data.
```

Each command has further help, which you can view by adding typing the command name after *help*.

For example, enter *dt help setConfigValue* on Windows to see the syntax for setting a configuration value.

```
Dundas BI Tools version 7.0.0.1-20190925145340
Copyright (c) 2019 Dundas Data Visualization, Inc. All rights reserved.

Sets the global value of a configuration setting.

Syntax:
dt.exe setConfigValue [/appcs:<application database connection string>] [/appStorage:<application database server type>]
                      /settingId:<setting identifier> /value:<new value>

  <application database connection string> - The application database connection string. If not specified, the value will be
taken from the dbi.config file located in the App_Data folder specified in the dt.exe.config file. The argument is optional.
  <application database server type> - The application database server type. If not specified, the value will be taken from t
he dbi.config file located in the App_Data folder specified in the dt.exe.config file. The argument is optional. Valid values
: "SqlServer", "Postgres".
  <setting identifier> - A string identifying the configuration setting. This may be the setting ID (in the case of core or e
xtension settings), or for other settings, in the format "moduleId:settingName". The argument is mandatory.
  <new value> - The new value of the setting. The argument is mandatory.

Basic Example:
dt.exe setConfigValue /settingId:c6e739e5-a58a-49af-be1b-92b1f0fa62a2 /value:"abc"

Full Example:
dt.exe setConfigValue /appcs:"Data Source=localhost; Initial Catalog=DundasApp; Integrated Security=True" /appStorage:SqlServ
er /settingId:c6e739e5-a58a-49af-be1b-92b1f0fa62a2 /value:"abc"

C:\Program Files\Dundas Data Visualization Inc\Dundas BI\Instances\v7ML\tools>
```

Commands

resetAdminPassword

This command lets you reset the administrator password for Symphony.

See How to Reset the Admin Password.

setConfigValue

Use this command to set a configuration value.

See Set a Configuration Value From the Command Line.

healthCheck

Perform a health check on the Symphony application and its databases with option to fix errors.

See Health Check.

configFile

Encrypts or decrypts the sensitive information stored in the dbi.config file, such as application database connection information.

Note: Use for Symphony 24.4 and later. For earlier versions of Symphony, use `connectionConfig` instead.

connectionConfig

Encrypts or decrypts the connection information for the application database stored in Symphony Managed Dashboards and Reports Config File.

Note: Use for Symphony 24.3 and earlier. For later versions of Symphony, use `configFile` instead.

Examples:

To encrypt the application database connection string:

```
dt connectionConfig decrypt
```

To decrypt the application database connection string:

```
dt connectionConfig decrypt
```

export

Exports the application data into a DBIE file. Syntax:

```
dt export [/appcs:<application database connection string>] [/appStorage:<application database server type>] /ecf:<export
configuration fi le> /ecid:<export configuration identifier> /dbie:<DBIE export file> [/report:<export report file>]
```

- <application database connectionstring> – The connection string of the application database. If not specified, the value will be taken from the dbi.config file located in the App_Data folder specified in the dt.exe.config file.
- <application database storage type> – The application database server type. If not specified, the value will be taken from the dbi.config file located in the App_ Data folder specified in the dt.exe.config file. The argument is optional. Valid values: "SqlServer", "Postgres".
- <export configuration file> – The export configuration input file, generated using *getExportConfigFile* (see below). The argument is mandatory, unless the alternative argument <export configuration identifier> is provided. If this or an alternative argument is not explicitly provided, the value is read from standard input.
- <export configuration identifier> – The ID of the export configuration saved in the application. The argument is mandatory, unless the alternative argument <export configuration file> is provided. To find its ID, select the existing configuration and click **Details** in the toolbar.
- <DBIE export file> – The output DBIE export file name (mandatory).
- <export report file> – The export report file name (optional).

Example using an export configuration file:

```
dt export /ecf:"C:\temp\Export Configuration 1.json" /dbie:"C:\temp\Export 1.dbie" /report:"C:\temp\Export 1 report.txt"
```

Example specifying optional connection information and using a saved export configuration ID:

```
dt.exe export /appcs:"Data Source=localhost; Initial Catalog=DundasApp; Integrated Security=True" /appStorage:SqlServer
/ecid:fab25279-e3a d-4885-8b8c-11d73a38ae62 /dbie:"C:\temp\Export 1.dbie"
```

getExportConfigFile

Generates an export configuration file that can be used to export (see above).

Syntax:

```
dt getExportConfigFile [/appcs:<application database connection string>] [/appStorage:<application database server type>]
/name:<export co nfiguration name> /file:<export configuration output file>
```

- <application database connectionstring> – The connection string of the application database. If not specified, the value will be taken from the dbi.config file located in the App_Data folder specified in the dt.exe.config file.
- <application database storage type> – The application database server type. If not specified, the value will be taken from the dbi.config file located in the App_Data folder specified in the dt.exe.config file. The argument is optional. Valid values: "SqlServer", "Postgres".
- <export configuration name> – The name of the existing export configuration (mandatory). For details on creating an export configuration see Import and Export a Project.
- <the export configuration output file> – The export configuration output file (mandatory). Will be created if does not exist or overwritten if exists.

Example:

```
dt getExportConfigFile /name:"Export Configuration 1" /file:"C:\temp\Export Configuration 1.json"
```

import

Imports application data from a DBIE file.

Syntax:

```
dt import [/appcs:<application database connection string>] [/appStorage:<application database server type>] [/dbie:]<DBIE
export file> [/ report:<import report file>]
```

- <application database connectionstring> – The connection string of the application database. If not specified, the value will be taken from the dbi.config file located in the App_Data folder specified in the dt.exe.config file.
- <application database storage type> – The application database server type. If not specified, the value will be taken from the dbi.config file located in the App_Data folder specified in the dt.exe.config file. The argument is optional. Valid values: "SqlServer", "Postgres".

- <DBIE export file> – The input DBIE export file. If not provided, the value will be read from standard input.
- <import report file> – The output import report file (optional).

Example:

```
dt import /report:"C:\temp\Import 1 report.txt"
```

deleteOldEntityData

Deletes old entity revisions.

Syntax:

```
dt deleteOldEntityData [/appcs:<application database connection string>] [/appStorage:<application database server type>]
[/beforeDate:<be fore date>] [/entityIds:<entity IDs>] [/tenantIds:<tenant IDs>]
```

- <application database connection string> – The application database connection string (optional). If not specified, the value will be taken from the dbi.config file located in the App_Data folder specified in the dt.exe.config file.
- <application database storage type> – The application database server type. If not specified, the value will be taken from the dbi.config file located in the App_Data folder specified in the dt.exe.config file. The argument is optional. Valid values: "SqlServer", "Postgres".
- <before date> – Only revisions created before this date will be processed (optional). If not specified, all revisions will be processed. Parsed as local time.
- <entity IDs> – A comma-separated list containing the IDs of entities to process (optional). If not specified, all entities will be processed.
- <tenant IDs> – A comma-separated list containing the IDs of tenants to which the operation will be limited (optional). If not specified, all tenants will be included.

Example:

```
dt deleteOldEntityData /beforeDate:"2017-01-02 00:12:00" /entityIds:1b7c71af-4704-430c-b647-6046aa40728a,65f5f5ad-dfdb-
4302-94ea-1593f1737456 /tenantIds:306fcf43-a2ad-4c99-b2db-27f89b7da895,c24e7c1b-0d53-4057-8f12-9318cf8e4935
```

manageExtensions

Use this command to manage extensions.

Example:

- To view the list of extensions (custom extensions display *Resource* in the *IsResource* column):

```
dt manageExtensions List
```

For more information, see:

- Symphony Managed Dashboards and Reports Config File

View Active Logon Sessions

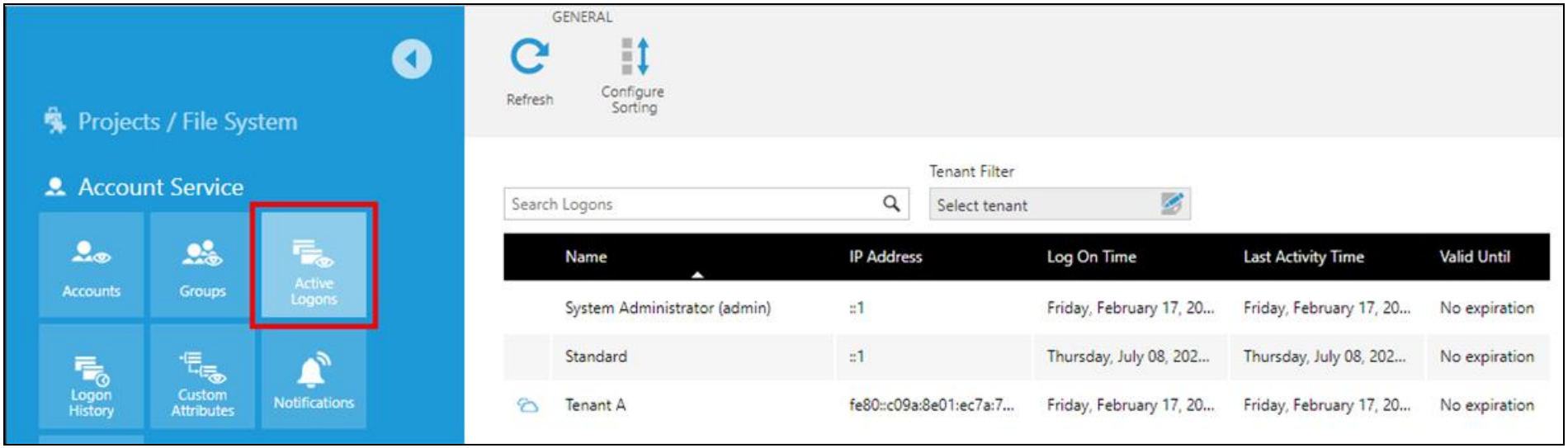
This applies to: *Managed Dashboards, Managed Reports*

This article shows you how to view and manage active logon sessions in Symphony.

View the List of Sessions

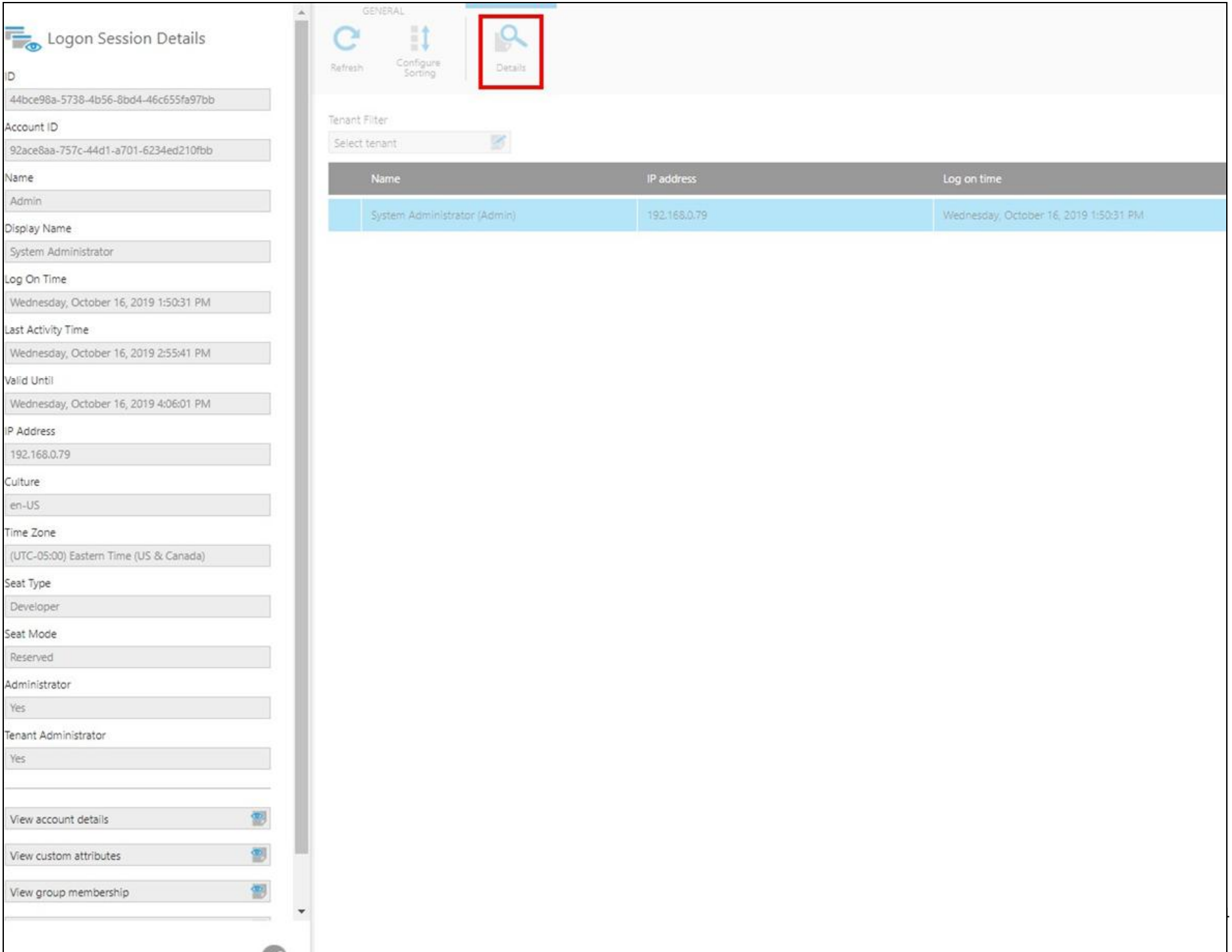
Expand **Account Service** in the Admin screen and click **Active Logons**.

The active logon sessions are listed, including the account name, IP address, and last activity time. You can search by any identifying details including session or account ID. Any impersonated sessions will appear with a distinct icon.



If you click to select a session other than your own in the list, the option to **Terminate Session** appears in the toolbar.

Choose **Details** in the toolbar with a session selected to open the *Logon Session Details* dialog.


Logon Session Details
ID
44bce98a-5738-4b56-8bd4-46c655fa97bb
Account ID
92ace8aa-757c-44d1-a701-6234ed210fbb
Name
Admin
Display Name
System Administrator
Log On Time
Wednesday, October 16, 2019 1:50:31 PM
Last Activity Time
Wednesday, October 16, 2019 2:55:41 PM
Valid Until
Wednesday, October 16, 2019 4:06:01 PM
IP Address
192.168.0.79
Culture
en-US
Time Zone
(UTC-05:00) Eastern Time (US & Canada)
Seat Type
Developer
Seat Mode
Reserved
Administrator
Yes
Tenant Administrator
Yes
View account details
View custom attributes
View group membership
GENERAL
Refresh
Configure Sorting
Details
Tenant Filter
Select tenant
Name
IP address
Log on time
System Administrator (Admin)
192.168.0.79
Wednesday, October 16, 2019 1:50:31 PM

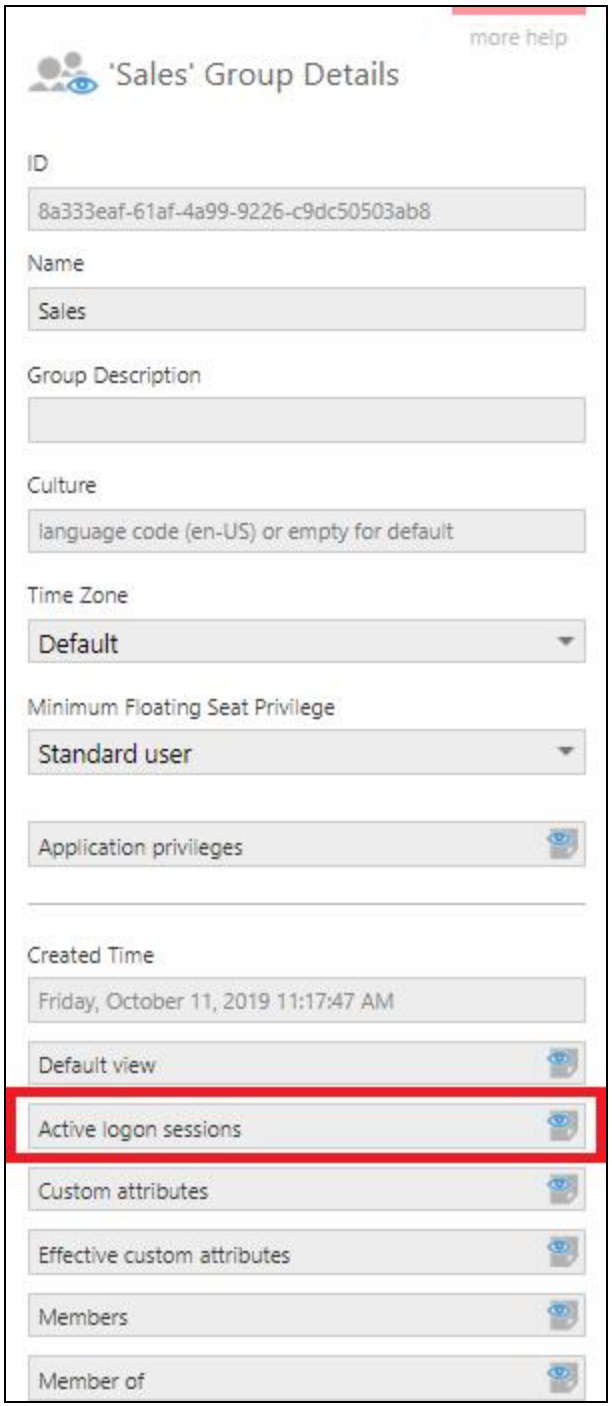
You can access various details about the session and its user account, including access to the full Account Details dialog by clicking **View account details**.

Sessions Associated With a User or Group

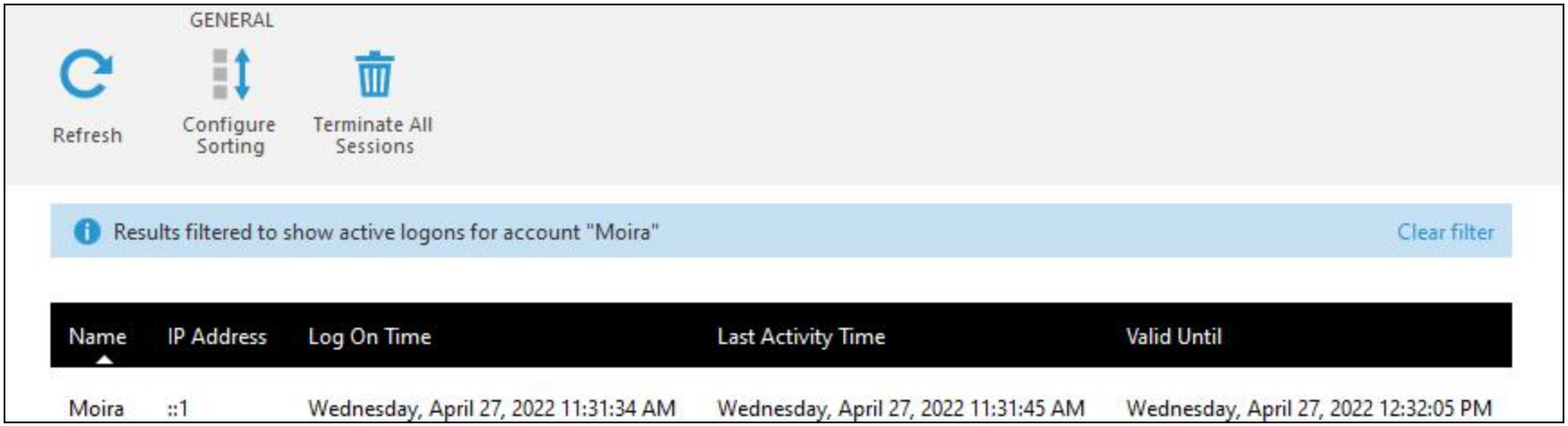
You can filter the list of active sessions either by user or by a group of users:

- Open an *Account Details* dialog either from the *Logon Session Details* dialog.
- Or, open a *Group Details* dialog from the Groups page.

Scroll down in the dialog if necessary and click **Active logon sessions**.


more help
'Sales' Group Details
ID
8a333eaf-61af-4a99-9226-c9dc50503ab8
Name
Sales
Group Description
Culture
language code (en-US) or empty for default
Time Zone
Default
Minimum Floating Seat Privilege
Standard user
Application privileges
Created Time
Friday, October 11, 2019 11:17:47 AM
Default view
Active logon sessions
Custom attributes
Effective custom attributes
Members
Member of

This reopens the active logons page filtered to the specific users or groups.



The option to **Terminate All Sessions** may appear in the toolbar when the list is filtered to a different account than your own.

For more information, see:

- Advanced User Management
- Advanced Group Management
- Logon History
- Use the Administration Homepage

White Labeling the Application

This applies to: *Managed Dashboards, Managed Reports*

This article shows how to use CSS, images, HTML, JavaScript, and other custom files for integrating, extending, or applying corporate branding (white labeling) to Symphony.

As a Symphony system administrator, you can:

- Customize the Symphony web application's styling and appearance
- Add JavaScript or HTML to be included on each page in the application
- Add your own files to refer to, such as images or additional CSS or JS files
- Customize displayed text using localization overrides

Custom CSS

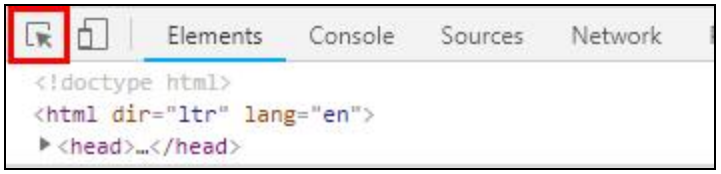
Selecting Styles

All browsers have developer tools you can use to extract IDs and classes from page elements. As an example, we are going to use Google Chrome to select the element used as the background of the login page to change its color.

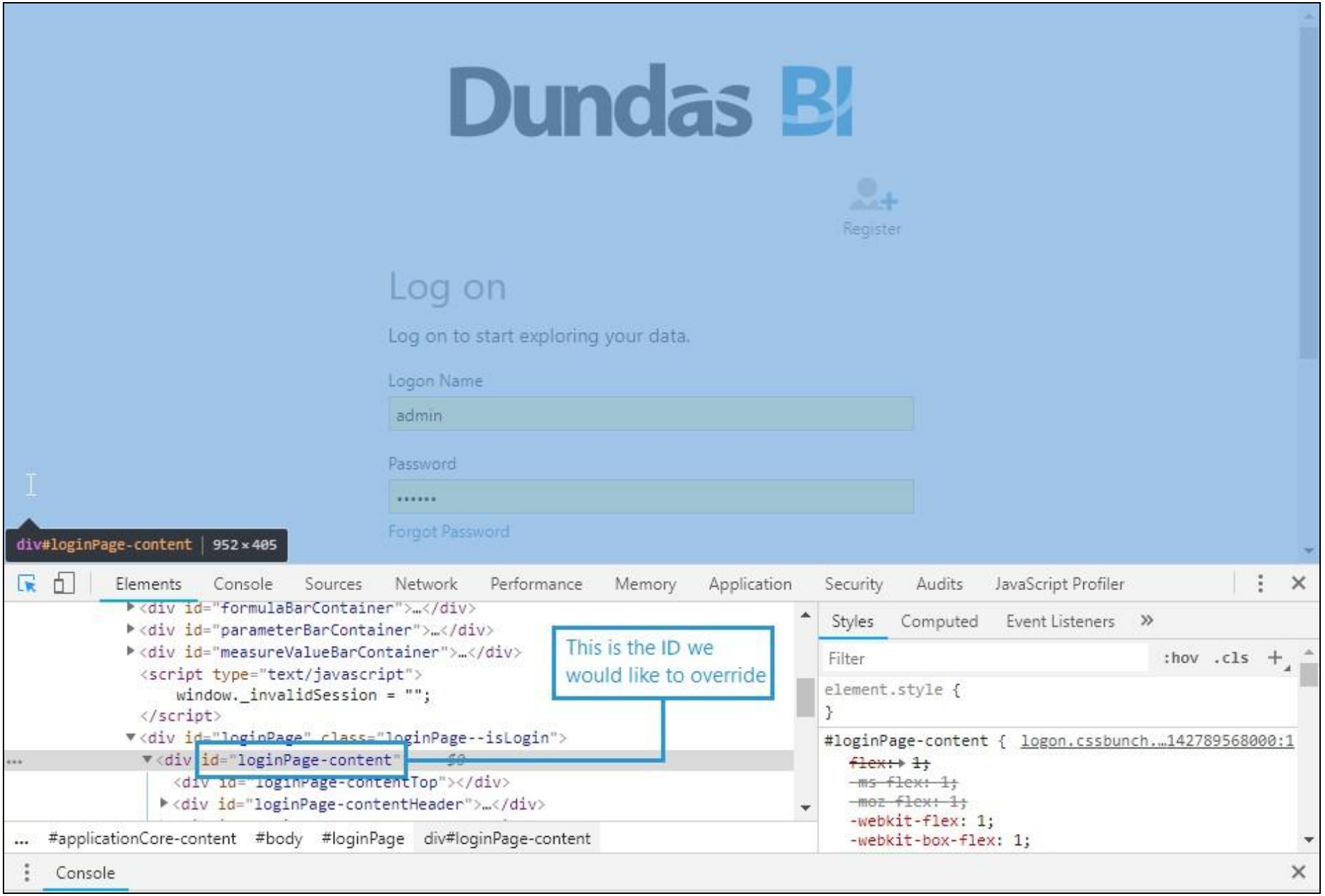
Pull up the Symphony login page.

Press *F12*, or open the developer tools from the browser menu.

In the *Elements* tab, click the element inspector icon next to the tabs in the toolbar (if using Chrome):



Now click on the page background. You will notice that it selects the page element * *. We will now modify the element with this ID in our style override resource.

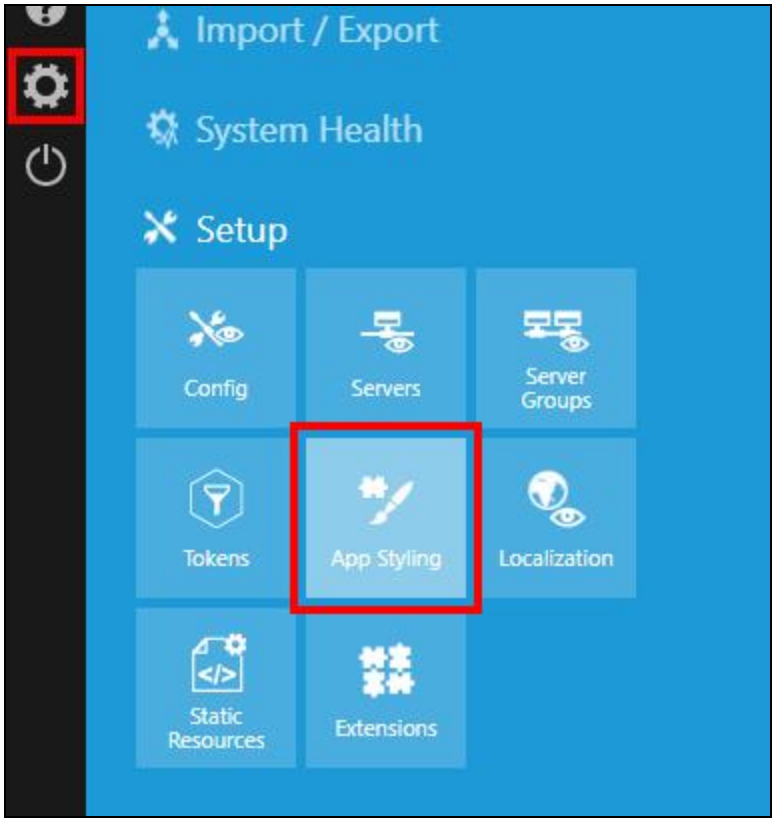

Dundas BI
Register
Log on
Log on to start exploring your data.
Logon Name
admin
Password
Forgot Password
div#loginPage-content | 952 × 405
Elements
Console
Sources
Network
Performance
Memory
Application
Security
Audits
JavaScript Profiler
…
…
…
<script type="text/javascript">
window._invalidSession = "";
</script>

<div id="loginPage-content"

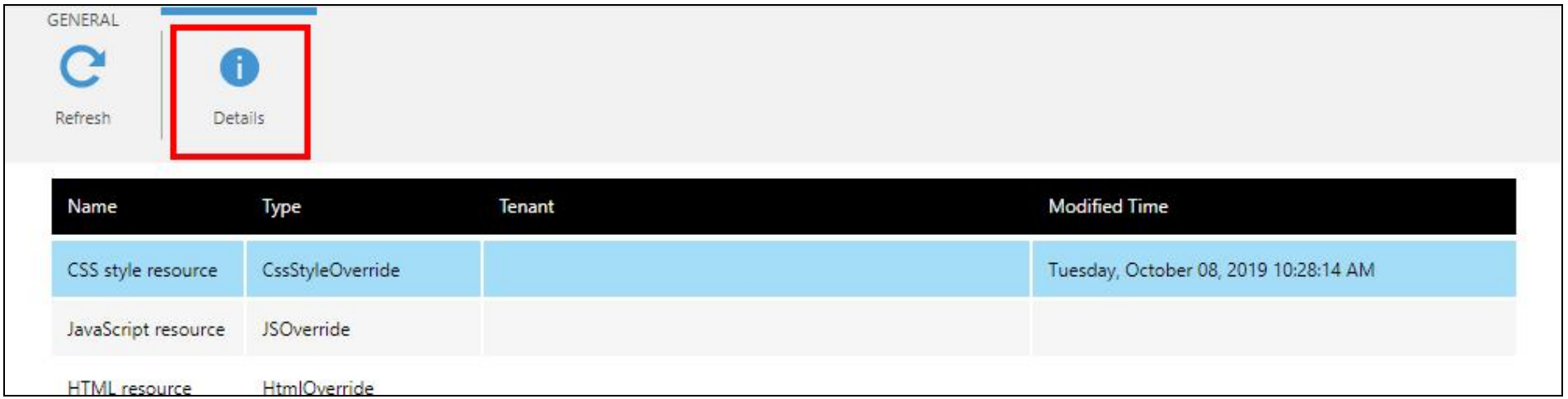
…
This is the ID we would like to override
Styles
Computed
Event Listeners
Filter
:hov .cls
element.style {
}
#loginPage-content { logon.cssbunch.…142789568000:1
flex: 1;
-ms-flex: 1;
-moz-flex: 1;
-webkit-flex: 1;
-webkit-box-flex: 1;
#applicationCore-content
#body
#loginPage
div#loginPage-content
Console

Modifying Styles

In the Administration area, expand **Setup** and then click **App Styling**.



Select the *CSS* style resource from the list and click **Details** on the toolbar.



In the *Application Styling Resource* dialog, enter the following CSS in the editor to modify the background on the login page. You can also download the resource as a file, update it in another tool, then upload it or copy and paste:

```
/* Add any CSS overrides in this document */
/* Main page background */
#loginPage-content
{
    background-color: #e8f0ff;
}
```

For class names, prefix the name with a period (.) instead of a hash (#).

Note: Some styles may require adding !important after the value for it to take precedence.

Click **Submit** to apply the changes.

Custom HTML

Similar to customizing the CSS style resource, you can add HTML to be included in every page of the application, including *<script>* or *<link>* elements that refer to separate JS or CSS files.

Under the expanded **Setup** section in Administration, click on the **App Styling** page and then select the *HTML resource*.

Click **Details** and enter or upload your HTML into the *Application Styling Resource* dialog.

Custom JavaScript

You can also add JavaScript to be executed when any page loads. In addition to customizing the application, this could provide a set of common functions in a global variable that can then be called from the script editor in dashboards and other views.

On the **App Styling** page in Administration, select the *JavaScript resource*. Click **Details**, then enter or upload your JavaScript. For example:

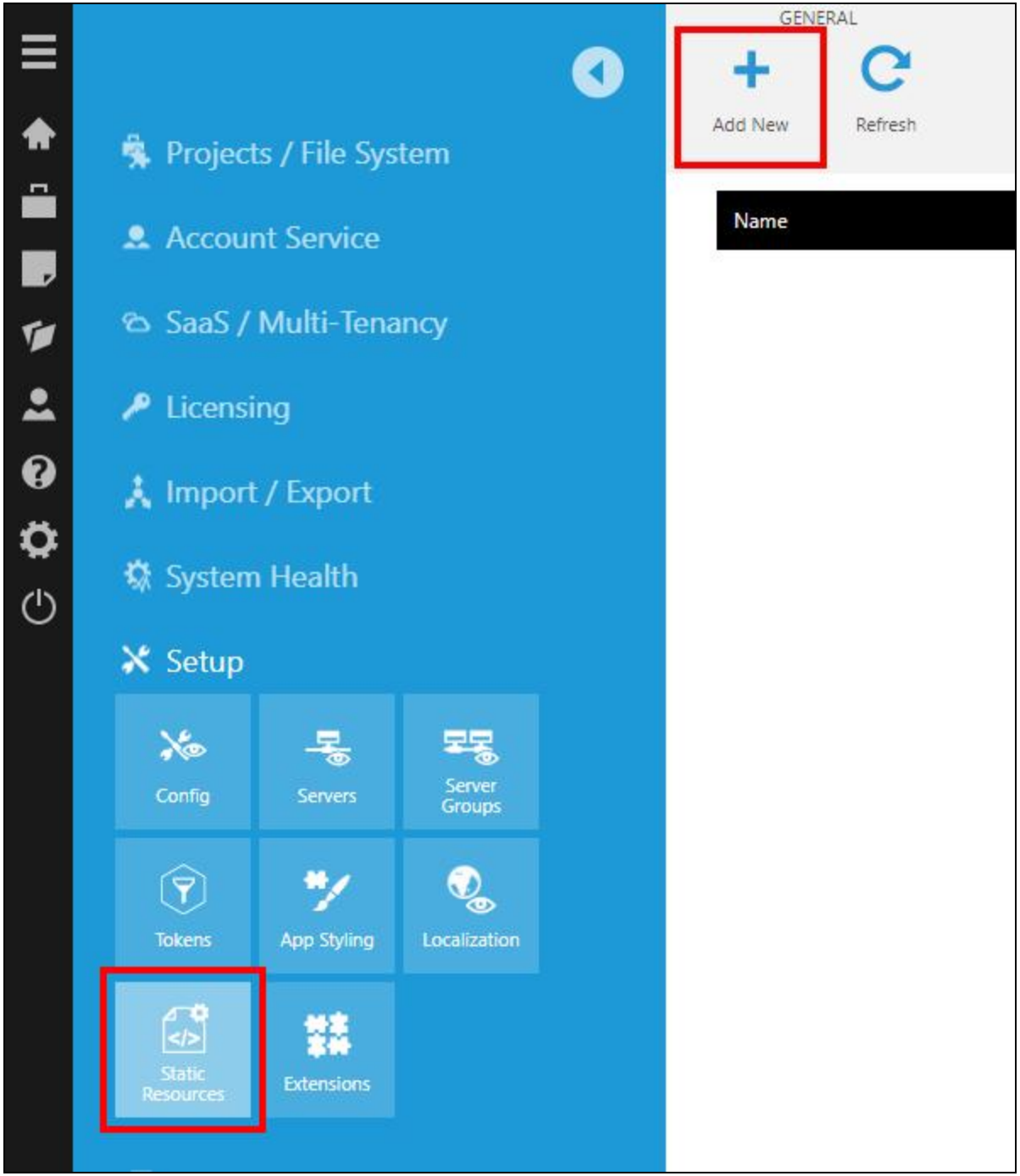
```
window.corporateLibrary = {

    palette: ["#418cf0", "#fcb441", "#e0400a", "#056492", "#bfbfbf", "#1a3c69", "#e1e480", "#119cdd", "#cb6a49", "#005cdb",
"#f4d288", "#506381", "#f1b9a8", "#e0830a", "#7893be"],

    applyPaletteColors: function (colorRules) {
        var discreteRules = colorRules.filter(function (rule) {
            return rule instanceof dundas.controls.DiscreteColorRule;
        });
        discreteRules.forEach(function (rule, index) {
            var colorString = corporateLibrary.palette[index % corporateLibrary.palette.length];
            rule.value = dundas.controls.Color.fromString(colorString);
        });
    }
};
```

Note: If you make a mistake that prevents pages from being able to open, you can add `?ignoreBuiltInResources=true` to the end of the URL in your browser's address bar to temporarily prevent app styling resources from loading.

Images and Other Custom Files

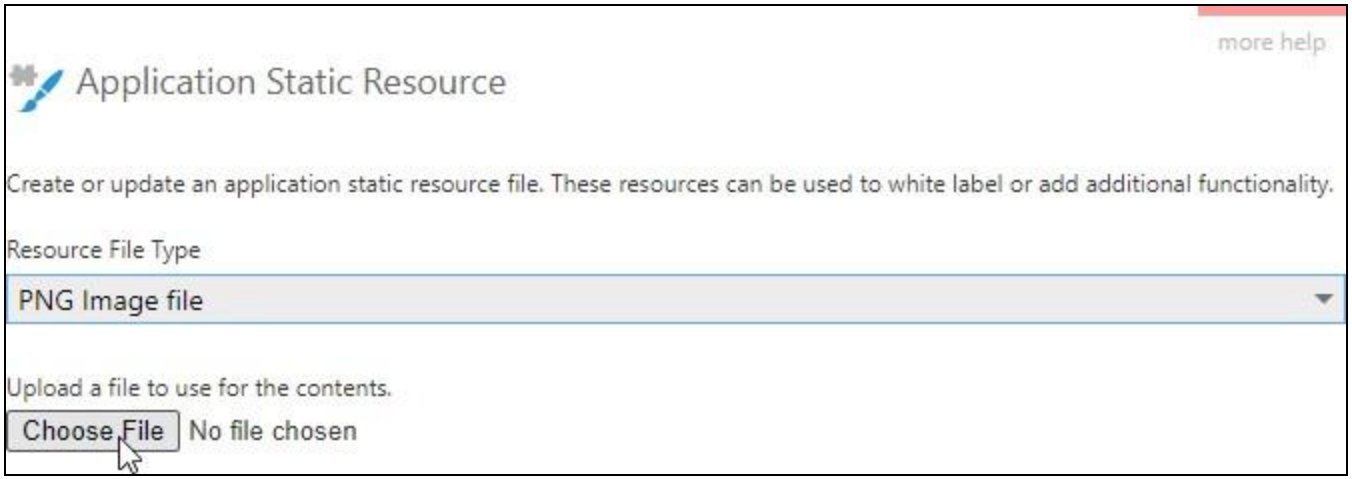
You can add your own files to the Symphony web application to refer to in CSS, HTML, and JavaScript, including images or separate CSS or JavaScript files.

Under the expanded **Setup** section in Administration, click **Static Resources**, and then **Add New** in the toolbar.

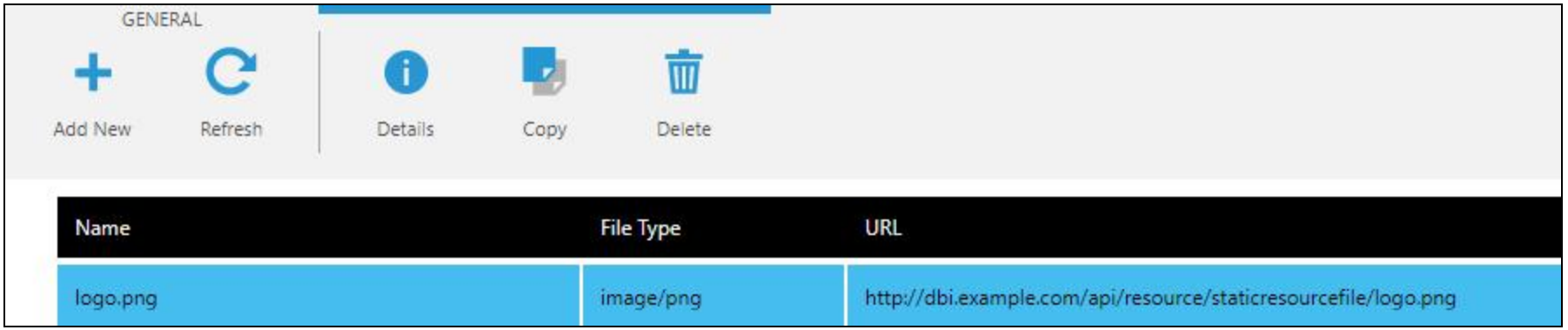

GENERAL
Add New
Refresh
Name
Projects / File System
Account Service
SaaS / Multi-Tenancy
Licensing
Import / Export
System Health
Setup
Config
Servers
Server Groups
Tokens
App Styling
Localization
Static Resources
Extensions

In the *Application Static Resource* dialog, set the **Resource File Type** to one of the common types listed, or choose *Custom file* and set the **Custom Resource Type** to the appropriate MIME type for your file.

Click **Choose File** to browse to and upload your file.



After the file uploads, it will be listed along with the full URL you can use to refer to it. To copy this URL, click to select the row and click **Copy** in the toolbar.



As an example of using static resources, the web browser tools shown above can inspect the image element used to display the logo on the logon page to find its class.

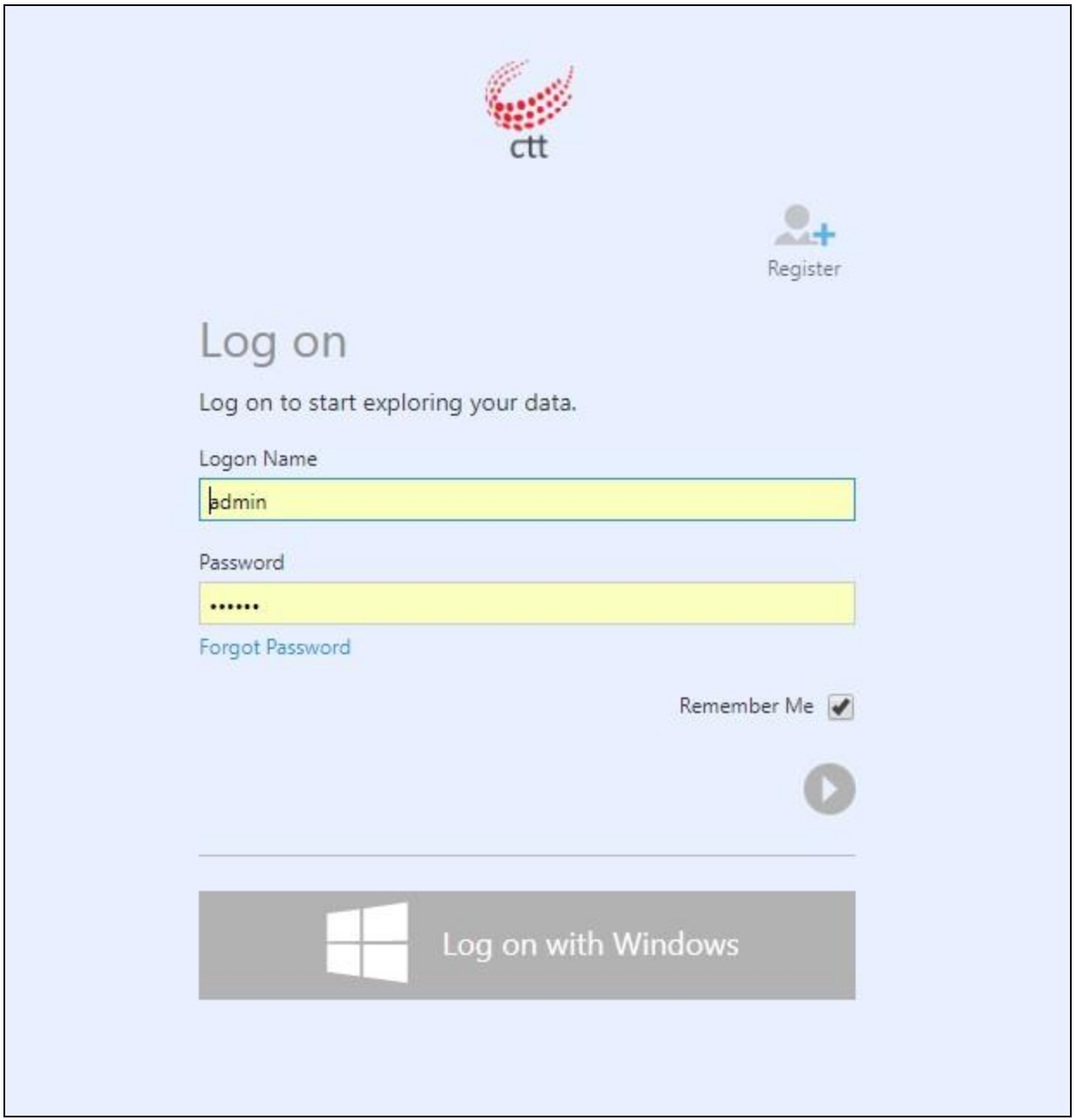
The logo has the class *loginPage-logo*, and is located inside an element with the ID *loginPage-contentHeader*.

After uploading a custom *logo.png*, we can target the logo element in the CSS style resource with the following CSS that refers to our static resource using a root relative path beginning with a forward slash:

```
/* Logo */
#loginPage-contentHeader .loginPage-logo
{
    background-image: url(/api/resource/staticresourcefile/logo.png);
    background-position: center center;
    background-repeat: no-repeat;
    background-size: contain;
}
```

You could also use an absolute path. When using relative paths, note that the application styling resources like this CSS resource are located under the */Resource/* subfolder of your Symphony website rather than */api/resource/* like static resources.

The next time the logon page loads, the custom CSS is included that refers to the custom image:

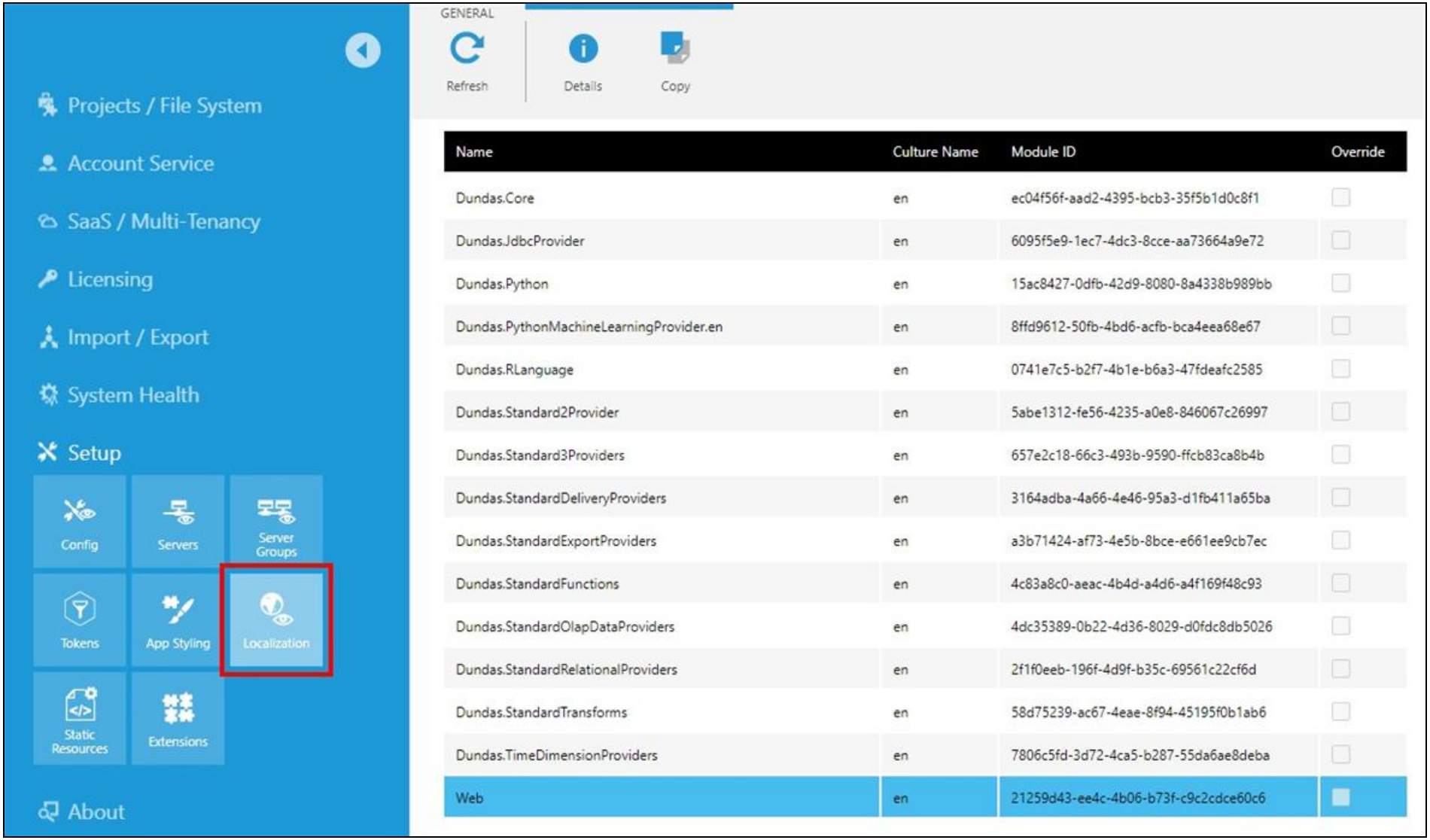

ctt
Register
Log on
Log on to start exploring your data.
Logon Name
admin
Password
Forgot Password
Remember Me
Log on with Windows

Customizing Text

You can use Symphony's localization support to customize any of the predefined text displayed in its interface. In addition to translating it into other languages, you can override existing languages such as *en* (English) to customize some of its text.

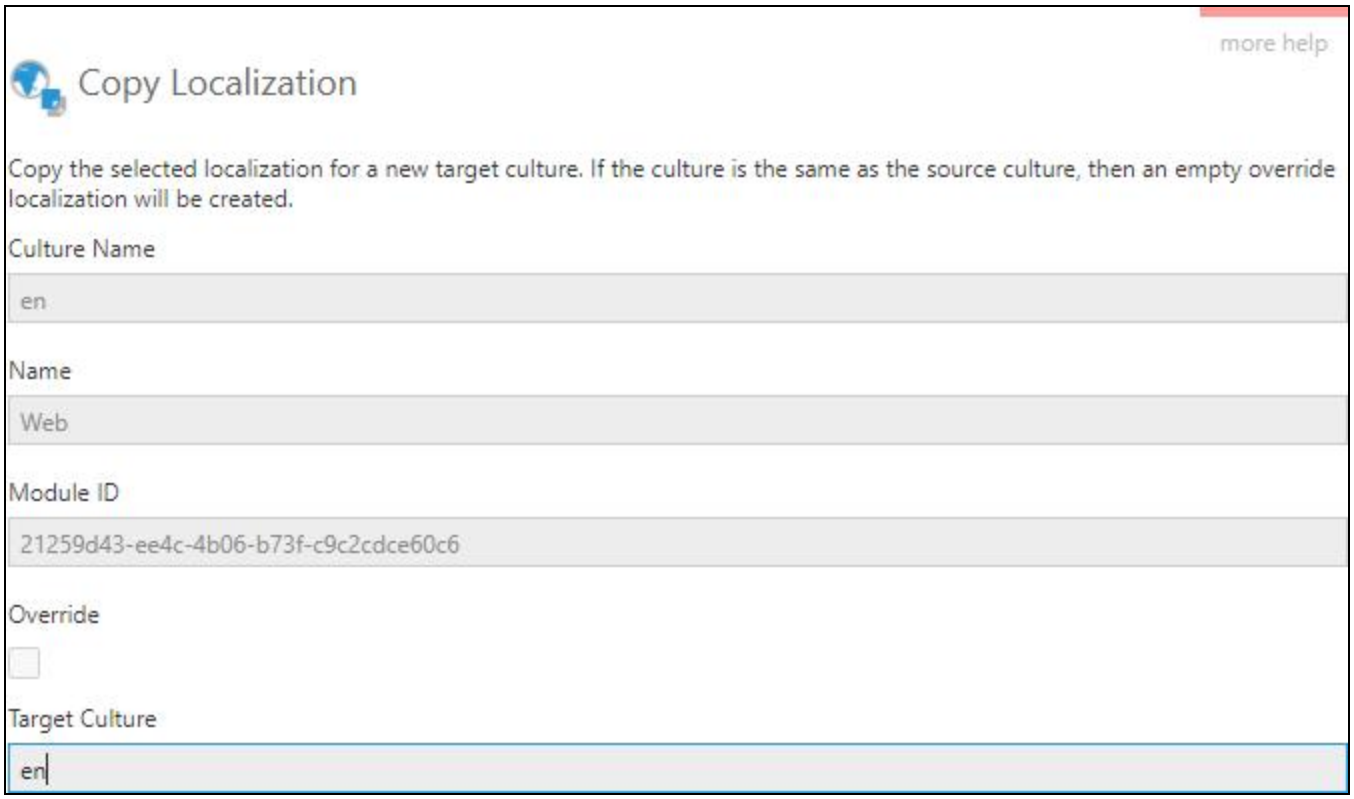
As an example, we can localize the text *Log on to Symphony* in the page title.

Under the expanded **Setup** section in Administration, click **Localization**. A list of localization resources is displayed on the right.



You can select existing resources and open its **Details** from the toolbar, then download and search through its existing XML to help locate which resource you need to override.

In our example, the *Web* resource contains the page title. Select it from the list, then click **Copy** in the toolbar to create an override.



To override existing text, enter the same **Target Culture** name as the original localization resource (for example, *en* for English). Entering a different culture name can be used instead when translating the application's text into another language as described in the article localization and multi-language support.

Click **Submit**. The newly created localization resource is displayed on the list. It will be identified as an *Override* if the target culture is the same as the original localization.

Select and open the **Details** for the new resource. In the Localization dialog, you can update the resource directly in the editor, or you can upload a new localization resource file containing the required overrides by clicking the **Choose File** button.

When you populate the override, it should be the same format as the regular localization resources, but only needs to contain the strings you want to override. For example

```
<?xml version="1.0" encoding="utf-8" ?>
<localization xmlns="http://dundas.com/schemas/BI/localization.xsd"
                  culture="en"
```

```
                moduleId="21259D43-EE4C-4B06-B73F-C9C2CDCE60C6">
    <group name="LogOnView">
        <string key="GS_LogOn_Title">Log on to CTT</string>
    </group>
    <group name="DesignerHome" tags="client">
        <string key="GS_DesignerHome_Title">CTT Home</string>
    </group>
</localization>
```

Note: Some keys are located inside groups with the tag client so that they are downloaded and accessible in the browser rather than the server.

Click **Submit** and navigate to the logon page or the home page to see the changes above.

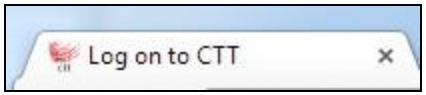
Note: You can also white label the default names of files created by Symphony. For example, override the value of *GS_ImportExport_FilePrefix* (you can find it in *Dundas.Core*) to change the prefix of exported DBIE files.

Modifying the Favicon

To modify the favorite icon displayed next to the page title by the browser, an option for installations of Symphony is to modify all of the images located in the folder **[YourWebsite]\wwwroot\Content\Images\favicon**.

Note: These images will not be replaced during upgrade.

As an alternative, you can use the JavaScript resource to add or change the *<link>* and *<meta>* DOM elements within the header element on the page as needed.



For more information, see:

- Import and Export a Project
- Configuring Notifications and Other Scheduling Features