InterSystems
Creative data technology

Administration Guide

Version 2.4
2024-05-06

InterSystems Corporation 1 Memorial Drive Cambridge MA 02142 www.intersystems.com

Administration Guide
InterSystems Version 2.4 2024-05-06

For Support questions about any InterSystems products, contact:

InterSystems Worldwide Response Center (WRC)
Tel: +1-617-621-0700
Tel: +44 (0) 844 854 2917
Email: support@InterSystems.com

Table of Contents

1

Welcome, System Administrators

As a system administrator for your InterSystems TotalView™ For Asset Management solution, your job is to take care of a small set of administrative tasks, outlined here.

Tip: A key first step is defining an initial set of users and data sources, so that data engineers can start creating data pipelines.

1.1 Data Source Management

A core purpose of InterSystems TotalView is to provide easy access to data sources. Managing these data sources consists of two tasks:

- Defining the credentials that the system will use to access the data sources
- Defining the data sources, which consists of providing the connection information for these sources

The data sources may be external APIs, databases accessed via JDBC, or files written directly to the file system used by your solution.

1.2 Security

Defining security consists mainly of the following tasks:

- Specifying the SSO configuration
- Defining the users
- Defining the user roles, which includes specifying access to SQL tables and functions
- Defining the SSO rules, which connect users and user roles, so that each user has the privileges associated with those roles

1.3 Other Configuration

There are options for a handful of additional configuration items:

- Configuring the connection to AtScale (InterSystems IRIS® Adaptive Analytics)
- Customizing the application menus
- Customizing the system configuration settings
- Defining email distribution lists

1.4 See Also

- About Your Solution: What Is Not Documented

2

Managing Data Source Credentials

A data source credential is a saved username and password that can be used to access a data source. In general, you need a data source credential for each database and each API (for example, Salesforce) that you access.

2.1 Defining a Credential

To create a credential:

1. Click the Management ⚙ icon in the application menu.
2. In the **Data Loader** section, click **Credentials**.

   The page then displays a table of the existing credentials.
3. Click **New Credential** in the upper right, above the table of credentials.

   The system displays a popup dialog box.
4. Enter the following values into the dialog box:
   - **Name**—The unique name for this set of credentials. This is the name by which you will refer to the username/password combination.
   - **Username**—A username.
   - **Password** and **Confirm Password**—The password associated with this username.

     This information is masked when you type it in, and is not displayed in any user interface.
5. Click **Submit**.

2.2 Editing a Credential

To edit a credential:

1. Click the Management ⚙ icon in the application menu.
2. In the **Data Loader** section, click **Credentials**.

The page then displays a table of the existing credentials.

3. Click the Edit icon in the applicable row.

   The system displays a popup dialog box.

4. Make edits as follows:

   - To modify the username, type the new username into **Username**.
   - To enter a new password, click **Enter New Password** and then type the new password into **Password** and **Confirm Password**.

5. Click **Submit**.

2.3 Deleting a Credential

To edit a credential:

1. Click the Management icon in the application menu.
2. In the **Data Loader** section, click **Credentials**.

   The page then displays a list of the existing credentials.

3. Click the Delete icon in the applicable row.

   The system displays a popup dialog box to confirm this action.

4. Click **Delete**.

2.4 See Also

- Defining Data Sources

3

Defining Data Sources

Before any user can load data from a data source, that data source must be defined within InterSystems TotalView™. The data source definition includes all the information needed to access the data source and retrieve information about the structure of available items in that data source.

3.1 Defining a Data Source

To create a data source:

1. Click the Management icon in the application menu.
2. In the **Data Loader** section, click **Data Sources**.

   The page then displays a list of the types of data sources.
3. Click one of the types.

   The right area then displays a table of the data sources of that type.
4. Click the **New** button in the upper right, above that list. (The name of the button depends on the type of data source you are looking at.)
5. In the right area, enter values as appropriate for that type (see later sections on this page).
6. Click **Submit**.

3.2 Editing a Data Source

To edit a data source:

1. Click the Management icon in the application menu.
2. In the **Data Loader** section, click **Data Sources**.

   The page then displays a list of the types of data sources.
3. Click one of the types.

   The right area then displays a table of the data sources of that type.

4. Click the Edit icon in the row for the data source that you want to edit.
5. In the right area, enter values as appropriate for that type (see later sections on this page).
6. Click **Submit**.

3.3 Testing a Data Source

To test a data source:

1. Click the Management icon in the application menu.
2. In the **Data Loader** section, click **Data Sources**.

   The page then displays a list of the types of data sources.
3. Click one of the types.

   The right area then displays a table of the data sources of that type.
4. Click the Edit icon in the row for the data source that you want to test.
5. If the page displays a **Test Connection** button, click that to ensure that you have entered the correct data.

   If the test is successful, the system displays the message **Connection Test Succeeded!** at the top of the page.

   If the test is not successful, the system displays a popup message indicating the connection failed.

3.4 Deleting a Data Source

To delete a data source:

1. Click the Management icon in the application menu.
2. In the **Data Loader** section, click **Data Sources**.

   The page then displays a list of the types of data sources.
3. Click one of the types.

   The right area then displays a table of the data sources of that type.
4. Click the Delete icon in the row for the data source that you want to delete.

   The system displays a popup dialog box to confirm this action.
5. Click **Delete**.

When you delete a data source, the system automatically deletes any associated data schema definitions from the Data Catalog and (if applicable) removes its file interface path, including archived files.

3.5 See Also

- Data Source Details
- Managing Data Source Credentials

4 Data Source Details

This page provides details for each type of data source for InterSystems TotalView™.

4.1 ExcelSingleFileDir

A ExcelSingleFileDir source is a source that provides data via Microsoft Excel files, periodically written to a specific directory within the file system accessible by InterSystems TotalView. Apart from the format of the file, this data source is the same as FileDir.

4.2 FileDir

A FileDir source is a source that provides data via files, periodically written to a specific directory within the file system. The file should contain data separated by delimiters; a common example is a comma-separated value (CSV) file. Another common delimiter is the tab.

For a FileDir source, specify the following details:

Data Source Name

Required. The unique name of this data source. This is the name that users see when they browse the Data Catalog.

Interface Path Location

Required. The directory in which these files will be found, relative to the system base path. Because this is a relative path, it should not start with / or \ (but any leading path separator is automatically removed).

To avoid confusion, this directory should not be used by any other data source.

When you create a FileDir source, the system automatically creates the directory named by **Interface Path Location**, as well as the subdirectories Samples, Source, Work, and Archive.

4.3 JDBC

A JDBC data source provides access to a database via a JDBC connection.

For a JDBC data source, specify the following details:

Data Source Name

Required. The unique name of this data source. This is the name that users see when they browse the Data Catalog.

Credential

Required. The credential that defines the username and password to access the database. Select the applicable credential from the dropdown list.

JDBC URL

Required. Enter the JDBC connection string needed to access the database.

JDBC Database

Required. Select the database vendor and version.

4.4 S3Delimited

An S3Delimited data source provides access to an S3 bucket that contains delimited files.

For an S3Delimited data source, specify the following details:

Data Source Name

Required. The unique name of this data source. This is the name that users see when they browse the Data Catalog.

Credential

Required. The credential that defines the username and password to access the given S3 bucket. Select the applicable credential from the dropdown list.

S3 Bucket Name

Required. The name of the S3 bucket to access.

AWS Session Token

The session token to use when accessing the S3 bucket.

Source Path

Location of the folder from which to load S3 files. You can optionally include %RUNDATE in the path for the ISO date to be injected at the time the files are loaded. The root folder is used if one is not provided.

Samples Path

Location of the folder from which to import S3 file schemas. You can optionally include %RUNDATE in the path for the ISO date to be injected at the time the files are listed. The root folder is used if one is not provided.

Archive Path

Location of the folder to archive previously loaded files in S3. You can optionally include %RUNDATE in the path for the ISO date to be injected at the time of the archiving. The root folder is used if one is not provided.

4.5 Salesforce

A Salesforce data source provides access to a Salesforce instance via the Salesforce API.

For a Salesforce data source, specify the following details:

Data Source Name

Required. The unique name of this data source. This is the name that users see when they browse the Data Catalog.

Credential

Required. The credential that defines the username and password to authenticate the Salesforce API. Select the applicable credential from the dropdown list.

Client ID Credentials

Required. Select the appropriate SDS Datasource (DS) Credentials record for the ClientId and Client Secret.

Authentication Server

Required. Specify the server used for authentication (which does not have to be the same server on which Salesforce is running).

Authentication URL

Required. Specify the end point in the Salesforce API to use in requesting access.

API end-point Server

Required. Specify the server on which the Salesforce API is running.

API URL

Required. Specify the end point in the Salesforce API to use in requesting resources.

Port

Specify the web server port to use, if that is not the standard port number.

4.6 See Also

- Defining Data Sources

5

SSO Configuration

To specify the SSO configuration that governs access to InterSystems TotalView™ :

1. Click the Management icon in the application menu.
2. In the **Security** section, click **SSO Configuration**.
3. Select one of the following:
   - **OAuth 2.0**
   - **IRIS SSO**
4. For **OAuth 2.0**, specify details as appropriate for your OAuth2.0 provider.
5. Click **Save**.

   Or, to discard changes, click **Reset**.

6

Defining Users

This page describes how to define users. After defining users, be sure to specify SSO rules that specify the user roles to which the users belong (thus specifying which permissions the users have).

6.1 Defining a User

To create a user:

1. Click the Management icon in the application menu.
2. In the **Security** section, click **User Registry**.

   The page then displays a table of the existing users.
3. Click **New User** in the upper right, above the table of users.

   The system displays a popup dialog box.
4. Enter the following values into the dialog box:
   - **Username**—The unique name for this user.
   - **First Name**—The first name of the user.
   - **Last Name**—The last name of the user.
   - **Email**—The email address of the user.
   - **Job Title**—The job title of the user. Note that you can define an SSO rule that adds a user role based on the job title held by a user.
   - **Password** and **Confirm Password**—The password for this username.

     This information is masked when you type it in, and is not displayed in any user interface.
5. Optionally disable the user. To do so, clear the **Enabled** check box.

   Only enabled users can log in.
6. Click **Submit**.

6.2 Editing a User

To edit a user:

1. Click the Management icon in the application menu.
2. In the **Security** section, click **User Registry**.

   The page then displays a table of the existing users.

3. Click the Edit icon in the applicable row.

   The system displays a popup dialog box.

4. Optionally edit any of the following values:
   - **First Name**
   - **Last Name**
   - **Email**
   - **Job Title**
5. Optionally enter a new password. To do so, click **Change Password** and then type the new password into **Password** and **Confirm Password**.
6. Optionally disable or enable the user. To do so, clear or select the **Enabled** check box.
7. Click **Submit**.

6.3 Deleting a User

To delete a user:

1. Click the Management icon in the application menu.
2. In the **Security** section, click **User Registry**.

   The page then displays a table of the existing users.

3. Click the Delete icon in the applicable row.

   The system displays a popup dialog box to confirm this action.

4. Click **Delete**.

6.4 See Also

- Defining User Roles
- Defining SSO Rules

7

Defining User Roles

This page describes how to define user roles. After defining user roles (and users), be sure to specify SSO rules to specify the user roles to which the users belong (thus specifying which permissions the users have).

7.1 Defining a User Role

To create a user role:

1. Click the Management icon in the application menu.
2. In the **Security** section, click **User Roles**.

   The page then displays a table of the existing user roles.
3. Click **New User Role** in the upper right, above the table of user roles.

   The system displays a popup dialog box.
4. For **Role Name**, type a unique but descriptive name for this role.

   This name is shown when you define SSO rules.
5. Click **Submit**.

   The new role is then added to the table.
6. Click the Edit icon in the row for the new role.

   This displays the **Role Privileges** page, where you can define the role.

7.2 Editing Role Privileges

To edit the privileges held by a user role:

1. Click the Management icon in the application menu.
2. In the **Security** section, click **Role Privileges**. Then select the role from the **Role** dropdown list.

   Or click **User Roles** and then click the Edit icon in the row for the role.

3. Then make edits as follows:

   - Click **Application Privileges** and then select the privileges this role needs to have within the InterSystems TotalView™ application. The page lists the privileges in groups with explanations of each.

     Click the **Assigned** or **Unassigned** link to see the currently assigned or currently unassigned privileges, respectively, within this set.

   - Click **SQL Capability Privileges** and then select the SQL capabilities this role needs to have.

     Click the **Assigned** or **Unassigned** link to see the currently assigned or currently unassigned privileges, respectively.

   - Click **SQL Schema Privileges** and then specify the privileges needed for specific SQL schemas (sets of tables) within the InterSystems TotalView environment. (Note that you can also specify privileges for specific tables.)

   - Click **SQL Procedure Privileges** and then select the SQL procedures that this role should be able to execute within this environment.

   - Click **SQL Table Privileges** and then specify the privileges needed for specific SQL tables within this environment.

   - Click **SQL View Privileges** and then specify the privileges needed for specific SQL views within this environment.

   For most of these options, you can use filters above the table in order to more easily find particular items.

7.3 Renaming a User Role

To rename a user role:

1. Click the Management icon in the application menu.
2. In the **Security** section, click **User Roles**.

   The page then displays a table of the existing user roles.

3. Click the Rename icon in the applicable row.
4. Type a new name into the dialog box.
5. Click **Submit**.

7.4 Deleting a User Role

To delete a user role:

1. Click the Management icon in the application menu.
2. In the **Security** section, click **User Roles**.

   The page then displays a table of the existing user roles.

3. Click the Delete icon in the applicable row.

   The system displays a popup dialog box to confirm this action.

4. Click **Delete**.

7.5 See Also

- Defining Users
- Defining SSO Rules

8

Defining SSO Rules

SSO rules connect users and user roles, so that each user has the privileges associated with those roles.

8.1 Rule Types

There are three types of SSO rules:

- A user rule directly assigns a specific user to one or more user roles.
- A job title rule adds user roles based on a specific job title. Any user who has the given job title is added to those user roles as well.
- A group rule adds user roles based on Active Directory groups. Any user who belongs to the given group is added to those user roles as well.

8.2 Defining an SSO Rule

To create an SSO rule:

1. Click the Management icon in the application menu.
2. In the **Security** section, click **SSO Rules**.

   The page then displays a table of the existing SSO rules.
3. Click **New SSO Rule** in the upper right, above the table of SSO rules.

   The system displays a popup dialog box.
4. For **Rule Type**, select a rule type.
5. Specify the following details, which depend on rule type:
   - For a **Username** rule, specify **Username**. This must exactly match the name of the user to which it is intended to apply.
   - For a **Job Title** rule, specify **Job Title**. This must exactly match the job title to which it is intended to apply.
   - For a **GroupID** rule, specify **Group**. This must exactly match the Active Directory group to which it is intended to apply.

6. In the **User Roles** section, select the user roles associated with this SSO rule.
7. Click **Submit**.

   The new SSO rule is then added to the table.

8.3 Editing an SSO Rule

To edit an SSO rule:

1. Click the Management icon in the application menu.
2. In the **Security** section, click **SSO Rules**.

   The page then displays a table of the existing SSO rules.
3. Click the Edit icon in the applicable row.

   The system displays a popup dialog box.
4. Edit any value, just as when you create an SSO rule.
5. Click **Submit**.

8.4 Deleting an SSO Rule

To delete an SSO rule:

1. Click the Management icon in the application menu.
2. In the **Security** section, click **SSO Rules**.

   The page then displays a table of the existing SSO rules.
3. Click the Delete icon in the applicable row.

   The system displays a popup dialog box to confirm this action.
4. Click **Delete**.

8.5 See Also

- Defining Users
- Defining User Roles

9

Configuring the Adaptive Analytics Connection

This page describes how to configure InterSystems TotalView™ so that it can call the API for AtScale (InterSystems IRIS® Adaptive Analytics). This enables data engineers to schedule the task of building cubes.

9.1 Configuring the Connection

To configure InterSystems TotalView™ so that it has a connection to AtScale:

1. Click the Analytics icon in the application menu.
2. Click **Configuration**.
3. Specify values as follows:
   - **Use Https**—Select this if you want to use an encrypted connection to the AtScale server.
   - **Server**—Specify the server on which AtScale is running.
   - **Port**—Specify the port to use for communication with AtScale.
   - **BatchAPIPort**—Specify the port to use for batch API calls to AtScale.
   - **Username**—Specify the AtScale username to use when calling the AtScale APIs. The best practice is to define and use a dedicated username for use only by API calls.
   - **Password** and **Confirm Password**—Specify the password for this user. This information is masked when you type it in, and is not displayed in any user interface.
4. Click **Test Connection** to ensure that the connection details are correct.
5. Click **Save**.

9.2 Editing the Connection

Later, if you need to change the password:

1. Click the Analytics icon in the application menu.
2. Click **Configuration**.
3. Click **Edit**.
4. Make changes as described above.

   If you need to change the password, select **Enter New Password**. Then specify the new password in **Password** and **Confirm Password**.
5. Click **Test Connection** to ensure that the connection details are correct.
6. Click **Save**.

10

Customizing the Application Menu

If you hold the appropriate permissions, you can customize the application menu for InterSystems TotalView™, including enabling or disabling items and modifying the order of menu items.

You can edit all system menu items but you cannot delete them.

10.1 Adding a Menu Item

To add a menu item:

1. Click the Management icon in the application menu.
2. In the **Security** section, click **App Menu**.
3. Click **New Menu Item**.
4. Specify details as follows:
   - **Enabled** controls whether this item is enabled (and visible). Clear this if you want the menu item to be hidden for now.
   - **Title** specifies the name of this menu item.
   - **Icon Type**, **Icon Name**, **Icon URL** specify the icon for this menu item.

     Icon Type controls how you specify the icon for this menu item. If you select **Preset**, choose an existing icon from **Icon Name**. If you select **From URL**, specify **Icon URL** as the URL of the icon.
   - **Link** specifies the URL to access when a user clicks this menu item.
   - **Resource Group**
   - **Resource Name** and **Privilege** specify the permission required to use this menu item. A permission consists of a **Privilege** (read, use, or write) for a **Resource Name**. For **Resource Name**, enter the name of a system resource. For **Privilege**, select **R**, **U**, or **W**.
   - **Resource Description** provides a brief description of the permissions required to use this menu item.
   - **Order** controls the position of this menu item. Select an integer.

   All these options are required.
5. Click **Submit**.

10.2 Editing a Menu Item

To edit a menu item:

1. Click the Management icon in the application menu.
2. In the **Security** section, click **App Menu**.
3. In the row for the menu item, click the Edit icon.
4. Modify details as when you add a menu item.
5. Click **Submit**.

10.3 Deleting a Menu Item

To delete a menu item (other than a system menu item):

1. Click the Management icon in the application menu.
2. In the **Security** section, click **App Menu**.
3. In the row for the menu item, click the Delete icon.
4. Click **Delete Menu Item** to confirm.

11

System Configuration Options

InterSystems TotalView™ has a set of miscellaneous configuration options. To modify them:

1. Click the Management icon in the application menu.
2. In the **Security** section, click **System Configuration**.

   The page then displays the current values for the settings.
3. To edit them, click **Edit**.
4. Modify the following values as needed:
   - **BusinessScheduler.Enabled**—Specifies whether the Business Scheduler is enabled; this tool enables data engineers to run recipes, run snapshots, and build cubes.
   - **DataLoader.DeltaSchemaPrefix**—Specifies the schema prefix to precede any tables used to track staging deltas.
   - **DataLoader.FileImportMinimumRows**—Specifies the minimum number of rows required for a file to be loaded, excluded the header row if any.
   - **DataLoader.MaxPermissibleColumnsInSchema**—Specifies the maximum number of columns that a table can have when loaded.
   - **DataLoader.SnapshotDataRetentionInDays**—Specifies the number of days for which a snapshot will be kept until it is deleted. Use –1 to retain snapshots indefinitely.
   - **DataLoader.StagingDataRetentionInDays**—Specifies the number of days for which batch of staging data will be kept until it is deleted. Use –1 to retain staging data indefinitely.
   - **DataLoader.StagingSchemaPrefix** —Specifies the prefix used for the table name for all staging tables. Changing this has no effect on previously generated tables.
   - **LogsRetentionInDays**—Specifies the number of days for which entries in the Messages Log kept until they are deleted. Use –1 to retain Message Log entries indefinitely.
   - **Recipes.ReconciliationReportRowCount**—Specifies the number of rows to be sampled for every failed reconciliation rule when generating the reconciliation report.
   - **SnapshotSchema** —Specifies the prefix used for the first part of the name for all snapshot tables. Changing this has no effect on previously generated tables.
5. Click **Save**.

12

Email Distribution Lists

When a task is scheduled, it can be configured to send email upon success, send email upon failure, or both. Specifically, the task is configured to use email distribution lists defined within InterSystems TotalView™, as described on this page.

12.1 Creating an Email List

To create an email list:

1. Click the Management icon in the application menu.
2. In the **Email** section, click **Email Distribution Lists**.
3. Click **Create List**.
4. Enter a unique list name and click **Submit**.
5. Click **Add Members**.
6. For each member of the list, specify the following:
   - **Email**—A complete email address
   - **Name**—A full name in any format (this is just for display purposes)

   Then click **Submit** to add this email address.

12.2 Editing an Email List

To edit an email list:

1. Click the Management icon in the application menu.
2. In the **Email** section, click **Email Distribution Lists**.
3. Click the list you want to edit.

Now you can make any of the following changes:

- Change the name of the list. To do this, click **Edit List**, enter a new value for **List Name**, and then click **Submit**.

- Add new list members, in the same way as when you create an email list.
- Edit a list member. To do this, click the Edit icon next to the list member, edit the **Email** and **Name** values, and then click **Submit**
- Delete a list member. To do this, click the Delete icon next to the list member and then click **Delete** to confirm.

12.3 Deleting an Email List

To delete an email list:

1. Click the Management icon in the application menu.
2. In the **Email** section, click **Email Distribution Lists**.
3. Click the list you want to delete.
4. Click **Delete List** and then click **Delete** to confirm.

12.4 See Also

- Scheduling Tasks