



Administration Guide

Version 2.10
2025-03-13

Administration Guide

PDF generated on 2025-03-13

InterSystems Version 2.10

Copyright © 2025 InterSystems Corporation

All rights reserved.

InterSystems®, HealthShare Care Community®, HealthShare Unified Care Record®, IntegratedML®, InterSystems Caché®, InterSystems Ensemble®, InterSystems HealthShare®, InterSystems IRIS®, and TrakCare are registered trademarks of InterSystems Corporation. HealthShare® CMS Solution Pack™, HealthShare® Health Connect Cloud™, InterSystems® Data Fabric Studio™, InterSystems IRIS for Health™, InterSystems Supply Chain Orchestrator™, and InterSystems TotalView™ For Asset Management are trademarks of InterSystems Corporation. TrakCare is a registered trademark in Australia and the European Union.

All other brand or product names used herein are trademarks or registered trademarks of their respective companies or organizations.

This document contains trade secret and confidential information which is the property of InterSystems Corporation, One Congress Street, Boston, MA 02114, or its affiliates, and is furnished for the sole purpose of the operation and maintenance of the products of InterSystems Corporation. No part of this publication is to be used for any other purpose, and this publication is not to be reproduced, copied, disclosed, transmitted, stored in a retrieval system or translated into any human or computer language, in any form, by any means, in whole or in part, without the express prior written consent of InterSystems Corporation.

The copying, use and disposition of this document and the software programs described herein is prohibited except to the limited extent set forth in the standard software license agreement(s) of InterSystems Corporation covering such programs and related documentation. InterSystems Corporation makes no representations and warranties concerning such software programs other than those set forth in such standard software license agreement(s). In addition, the liability of InterSystems Corporation for any losses or damages relating to or arising out of the use of such software programs is limited in the manner set forth in such standard software license agreement(s).

THE FOREGOING IS A GENERAL SUMMARY OF THE RESTRICTIONS AND LIMITATIONS IMPOSED BY INTERSYSTEMS CORPORATION ON THE USE OF, AND LIABILITY ARISING FROM, ITS COMPUTER SOFTWARE. FOR COMPLETE INFORMATION REFERENCE SHOULD BE MADE TO THE STANDARD SOFTWARE LICENSE AGREEMENT(S) OF INTERSYSTEMS CORPORATION, COPIES OF WHICH WILL BE MADE AVAILABLE UPON REQUEST.

InterSystems Corporation disclaims responsibility for errors which may appear in this document, and it reserves the right, in its sole discretion and without notice, to make substitutions and modifications in the products and practices described in this document.

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 (2.10)	1
1.1 Data Source Management	1
1.2 Security	1
1.3 Other Configuration	2
1.4 See Also	2
2 Managing Data Source Credentials (2.10)	3
2.1 Defining a Credential	3
2.2 Editing a Credential	3
2.3 Deleting a Credential	4
2.4 See Also	4
3 Defining Data Sources (2.10)	5
3.1 Defining a Data Source	5
3.2 Editing a Data Source	5
3.3 Testing a Data Source	6
3.4 Deleting a Data Source	6
3.5 See Also	7
4 Data Source Details (2.10)	9
4.1 ExcelSingleFileDir	9
4.2 FileDir	9
4.3 Guardian	10
4.4 JDBC	10
4.5 NYT	11
4.6 RSS	11
4.7 S3Delimited	11
4.8 Salesforce	12
4.9 SftpDelimited	13
4.10 See Also	13
5 SSO Configuration (2.10)	15
6 Defining Users (2.10)	17
6.1 Defining a User	17
6.2 Editing a User	18
6.3 Deleting a User	18
6.4 See Also	18
7 Defining User Roles (2.10)	19
7.1 Defining a User Role	19
7.2 Filter Options in Role Privileges	19
7.3 Editing Role Privileges	20
7.4 Schema Wildcard Privileges	20
7.5 Renaming a User Role	21
7.6 Deleting a User Role	21
7.7 See Also	22
8 Defining SSO Rules (2.10)	23
8.1 Rule Types	23
8.2 Defining an SSO Rule	23

8.3 Editing an SSO Rule	24
8.4 Deleting an SSO Rule	24
8.5 See Also	24
9 Configuring the Adaptive Analytics Connection (2.10)	25
9.1 Configuring the Connection	25
9.2 Editing the Connection	25
10 Customizing the Application Menu (2.10)	27
10.1 Adding a Menu Item	27
10.2 Editing a Menu Item	28
10.3 Deleting a Menu Item	28
11 System Configuration Options (2.10)	29
11.1 Modifying Settings	29
11.2 Business Scheduler Settings	29
11.3 Data Loader Settings	29
11.4 Recipes Settings	30
11.5 Snapshots Settings	30
11.6 Streaming Settings	31
11.7 System Settings	31
12 Email Distribution Lists (2.10)	33
12.1 Creating an Email List	33
12.2 Editing an Email List	33
12.3 Deleting an Email List	34
12.4 See Also	34
13 Email Templates (2.10)	35
13.1 Defining an Email Template	35
13.2 Template Variables	36
13.3 Editing an Email Template	37
13.4 Deleting an Email Template	37
13.5 See Also	37
14 Admin Tools (2.10)	39
14.1 Resetting Tasks	39
14.2 Viewing Log Files	39

1

Welcome, System Administrators (2.10)

As a system administrator for your [InterSystems Data Fabric Studio™](#) 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 Data Fabric Studio 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 application menus
- 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](#), which control things such as how long various data is kept
- Defining [email distribution lists](#)

1.4 See Also

- [About Your Solution: What Is Not Documented](#)


2

Managing Data Source Credentials (2.10)

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 **General** 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 (2.10)

Before any user can load data from a data source, that data source must be defined within InterSystems Data Fabric Studio™. 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](#).
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](#).
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 Test Connection  icon in the row for the data source that you want to test.



Or click the Edit  icon in the row for the data source that you want to test and then click the **Test Connection** button on the right.

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 (2.10)

This page provides details for each type of data source for InterSystems Data Fabric Studio™.

4.1 ExcelSingleFileDir

An ExcelSingleFileDir source is a source that provides data via Microsoft Excel files, periodically written to a specific directory within the file system accessible by Data Fabric Studio. 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. [Using the File Manager](#) explains the purpose of these directories.

4.3 Guardian

A Guardian data source provides access to [The Guardian OpenPlatform](#) news feed, provided by [The Guardian News & Media Limited](#); see <https://open-platform.theguardian.com/documentation/>.

For such a data source, provide 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](#).

APIKEY

Required. The API key needed to access this data source.

4.4 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.

Enable Foreign Tables

If you select this check box, it will be possible to project tables from the selected database as foreign tables within Data Fabric Studio. This is useful when it is not feasible or reasonable to load data directly into Data Fabric Studio. For example, a table may be extremely large and might not be queried frequently. A foreign table is read-only but can otherwise be accessed in the same way as local tables.

If you select this check box, also specify **JDBC Foreign Table Local Schema**, which is the default name of the schema to contain any foreign tables from this data source.

4.5 NYT

An NYT data source provides access to a [news feed API](#) provided by [The New York Times Company](#); see <https://developer.nytimes.com/get-started>.

For such a data source, provide 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](#).

APIKEY

Required. The API key needed to access this data source.

4.6 RSS

An RSS data source provides access to an RSS feed. For such a data source, provide 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](#).

RSSFeedURL

Required. The URL of the RSS feed.

Timeout

Required. The length of time to wait, in seconds, for a response from the RSS feed URL before throwing an error.

4.7 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 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 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. 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.

Target Path

Location of the folder to write files to, in the case when a recipe promotes data to a file on the given S3 bucket.

4.8 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.

4.9 SftpDelimited

An SftpDelimited data source provides access to an SFTP server that contains delimited files.

For an SftpDelimited 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 SFTP server. Select the applicable credential from the dropdown list.

Certificate File Path

Location of the certificate file to use when authenticating with the given SFTP server.

Host

Required. The host name of the SFTP server.

Port

Required. The port to use on the SFTP server.

Source Path

Location of the folder from which to load 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 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. 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.

Target Path

Location of the folder to write files to, in the case when a recipe promotes data to a file on this server.


4.10 See Also

- [Defining Data Sources](#)

5

SSO Configuration (2.10)

To specify the SSO configuration that governs access to InterSystems Data Fabric Studio™:

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 (2.10)

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 (2.10)

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 list 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 Filter Options in Role Privileges


When you view or edit role privileges, you can use filters in order to find particular items more easily. The filter options vary by item, but collectively are as follows:

- **Search box**—Type a string to display only items containing this text.
- **Schema** dropdown box—Select an SQL schema to show only items for that schema.
- **All**—Click this link to remove any filtering by role assignment.

- **Assigned**—Click this link to see only the items currently assigned to the role you are viewing. This option applies to application privileges and SQL capability privileges.
- **Unassigned**—Click this link to see only the items not currently assigned to the role you are viewing. This option applies to application privileges and SQL capability privileges.
- **With Privileges**—Click this link to see only the items for which the role currently has privileges. This option applies to SQL schemas, tables, procedures, and views.
- **Only Wildcards**—Click this link to see only [schema wildcards](#). This option applies to SQL schemas.

7.3 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 Data Fabric Studio. The page lists the privileges in groups with explanations of each.
 - Click **SQL Capability Privileges** and then select the SQL capabilities this role needs to have.
 - Click **SQL Schema Privileges** and then specify the privileges needed for specific SQL schemas (sets of tables) within Data Fabric Studio. (Note that you can also specify privileges via [schema wildcards](#) and you can specify privileges for specific tables.)

If the row for a given schema is grayed out, look for a [schema wildcard](#) that controls access to the schema. You can create an override. To do so, click the **OVERRIDE** check box and then specify privileges as needed.

- Click **SQL Procedure Privileges** and then select the SQL procedures that this role should be able to execute.
- Click **SQL Table Privileges** and then specify the privileges needed for specific SQL tables.
- Click **SQL View Privileges** and then specify the privileges needed for specific SQL views.

This page provides [filters](#) you can use to find items more easily.

4. Click **Save**.
The system displays a message summarizing the changes it will make.
5. Click **Apply** to confirm the changes.

7.4 Schema Wildcard Privileges

A *schema wildcard* enables you to give access to multiple schemas, including schemas that have not yet been created but that will follow a naming convention. To add privileges using a schema wildcard:

1. Click **Add Wildcard Schema**.



- For **Schema Name**, specify a schema name that includes an asterisk, which will represent any character. For example: `Staging*`
- Press **Submit**.
This adds a row at the start of the schema privilege table.
- In this new row, click the check box in the **ENABLED** column. This action enables you to specify privileges of different types for this schema wildcard.
- In the same row, click the check box for each privilege you want to enable, for all schemas with names matching the given pattern. When you do so, the page also automatically selects the check box for each schema that matches the wildcard.

To disable a schema wildcard, clear the check box in the **ENABLED** column. When you do so, the page also automatically clears the check boxes for the schemas that matches the wildcard, showing these rows in a contrasting color so that you can find them easily.

To delete a schema wildcard, click **Delete** in the row for the schema wildcard. Then click **Delete** to confirm this action.



7.5 Renaming a User Role

To rename a user role:

- Click the Management  icon in the application menu.
- In the **Security** section, click **User Roles**.
The page then displays a table of the existing user roles.
- Click the Rename  icon in the applicable row.
- Type a new name into the dialog box.
- Click **Submit**.

7.6 Deleting a User Role

To delete a user role:

- Click the Management  icon in the application menu.
- In the **Security** section, click **User Roles**.
The page then displays a table of the existing user roles.
- Click the Delete  icon in the applicable row.
The system displays a popup dialog box to confirm this action.
- Click **Delete**.

7.7 See Also

- [Defining Users](#)
- [Defining SSO Rules](#)

8

Defining SSO Rules (2.10)

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 groups defined by an identity provider (such as Active Directory). 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 identity provider group to which it is intended to apply.



Also specify **User Group Description**, which should be a name for this group within this application. This name is shown in **Rule Details** on the SSO Rules page.

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 (2.10)

This page describes how to configure InterSystems Data Fabric Studio™ 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 Data Fabric Studio 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 (2.10)

If you hold the appropriate permissions, you can customize the application menu for InterSystems Data Fabric Studio™, 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.
 - **Group**
 - **Privilege 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 (2.10)

This page describes additional configuration options and how to modify them.

11.1 Modifying Settings

To modify settings:

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

The page then displays the current values for the settings.

Below the **Settings** headings, there is a list of names, each of which corresponds to a group of related settings.

3. Optionally click a group name to quickly scroll to that group.
4. Make edits as needed. See the reference information later on this page.
5. Click **Save**.

Or click **Revert** to cancel your edits.

11.2 Business Scheduler Settings

The **Business Scheduler** group includes one setting:

- **Enabled**—Specifies whether the Business Scheduler is enabled; this tool enables data engineers to run recipes, run snapshots, and build cubes.

11.3 Data Loader Settings

The **Data Loader** group includes the following settings:

- **Delta Schema Prefix**—Specifies the schema prefix to precede any tables used to track staging deltas.

- **File Import Minimum Rows**—Specifies the minimum number of rows required for a file to be loaded, excluded the header row if any.
- **Max Permissible Columns In Schema**—Specifies the maximum number of columns that a table can have when loaded.
- **Snapshot Data Retention In Days**—Specifies the number of days for which a snapshot will be kept until it is deleted. Use -1 to retain snapshots indefinitely.
- **Staging Data Retention In Days**—Specifies the number of days for which staging data will be kept until it is deleted. Use -1 to retain staging data indefinitely.
- **Staging Schema Prefix**—Specifies the schema prefix used for the names for all [staging tables](#). Changing this has no effect on previously generated tables.

11.4 Recipes Settings

The **Recipes** group includes the following settings:

- **Dropped Records Report Path**—Specifies where to generate reports about dropped records.
- **Dropped Records Report Retention In Days**—Specifies the number of days for which a dropped records report will be kept until it is deleted. Use -1 to retain these reports indefinitely.
- **Max Dropped Records**—Specifies the maximum number of records to drop when using SQLQuickLoad before reverting the load.
- **Reconciliation Report Path**—Specifies where to generate reconciliation reports.
- **Reconciliation Report Retention In Days**—Specifies the number of days for which a reconciliation report will be kept until it is deleted. Use -1 to retain these reports indefinitely.
- **Reconciliation Report Row Count**—Specifies the number of rows to be sampled for every failed reconciliation rule when generating the reconciliation report.
- **Validation Report Path**—Specifies where to generate validation reports.
- **Validation Report Retention In Days**—Specifies the number of days for which a validation report will be kept until it is deleted. Use -1 to retain these reports indefinitely.
- **Role For Pending Index Build Tasks**—Specifies the workflow row to receive workflow tasks for pending index builds.
- **Role For Recipe Reset Tasks**—Specifies the workflow row to receive workflow tasks for [resetting recipes](#).

11.5 Snapshots Settings

The **Snapshots** group includes the following setting:

- **Snapshot Schema**—Specifies the prefix used for the first part of the name for all [snapshot tables](#). Changing this has no effect on previously generated tables.

11.6 Streaming Settings

The **Streaming** group includes the following setting:

- **Persister Table Projection Timeout**—Specifies the maximum length of time to wait (in seconds) for a table projection to occur before streaming data into the table. If the table is not found within this timeout period, streaming does not occur.

11.7 System Settings

The **System** group includes the following settings:

- **Connector Temp Files Base Path**—Specifies where data connectors will store files before loading them. Applies to only some connectors.
- **Log File Lines Per Page**—Specifies the number of lines to display per page when displaying [system log files](#).
- **Logs Retention In Days**—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.
- **Session Timeout In Minutes**—Specifies how long to wait for user action on a page before a refresh is required. This option applies only to pages that automatically poll the server, such as the Business Scheduler Dashboard.


12

Email Distribution Lists (2.10)

When a task is [scheduled](#), it can be configured to send email using email distribution lists defined within InterSystems Data Fabric Studio™, 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 **New 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 the Edit  icon *in the upper right*, 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 the Delete  icon in the upper right and then click **Delete** to confirm.

12.4 See Also

- [Email Templates](#)
- [Scheduling Tasks](#)


13

Email Templates (2.10)

When a task is [scheduled](#), it can be configured to send email that uses a template defined within InterSystems Data Fabric Studio™, as described on this page.

13.1 Defining an Email Template

To define an email template:

1. Click the Management  icon in the application menu.
2. In the **Email** section, click **Email Templates**.
3. Click **New Template**.

Now use the middle area of the page to define the template (as described next), and view the preview on the right side of the page.

4. For **Template Type**, select either **Business Scheduler Task Error** or **Business Scheduler Task Success**, depending on whether this template is meant for use in the case of errors or in the case of success, respectively.
5. For **Template Name**, specify a unique name for this template (within the given type—it is possible to have templates with the same name if they have different types). Users will see this template name when [scheduling](#) tasks.
6. For **Subject**, specify the subject line of the email message. The most useful format consists of a combination of text (included as is) and variables (which get replaced when the message is generated).

For example, the default task error subject line is as follows:

```
ERROR: {{ Subject }}
```

The variable `{{ Subject }}` is automatically replaced with appropriate text based on the task.

Similarly, the default task success subject line is as follows:

```
SUCCESS: {{ Subject }}
```

To edit the value in the **Subject** field, you can type directly and you can use the buttons listed under **Variables** to insert variables. To insert a variable, first move the cursor to the position where you want the variable to be, and then press the variable button.

7. For **Body**, specify the body of the email message. You can use the same techniques as in the **Subject** field, except that you have more space here for details.

8. Click **Save Template**.

13.2 Template Variables

This section provides reference information on the variables you can use within an [email template](#). These are listed under **Variables**. To insert a variable, first move the cursor to the position where you want the variable to be, and then press the variable button. You can also type these.

{{Actions}}

Replaced with a comma-separated list of possible actions. This variable applies only to **Business Scheduler Task Error** templates.

{{Application}}

Replaced with TotalView.

{{Environment}}

Replaced with the name of the [environment](#) in which the task was running, for example DEV.

{{Message}}

For a successful task run, this variable is replaced with generated text of the following form, depending on the task and the name of the item:

The scheduled task, Recipe 'TUES', has been completed successfully

For an unsuccessful task run, this variable is replaced with a detailed error message, depending on the problem that occurred.

{{ResourceName}}

Replaced with the short name of the recipe.

{{ResourceType}}

Replaced with the name of the server on which the task was running.

{{SessionId}}

Replaced with the internal session ID (generally useful only for your application partner).

{{Subject}}

Replaced with a short summary, meant for use in an email subject line. For a successful task run, this variable is replaced with the following text:

Scheduled task completed

For an unsuccessful task run, this variable is replaced with the following text:

Unexpected error when running scheduled task

{{UTCTime}}


Replaced with the date and time when the task run finished (either successfully or not), in UTC time.

{{WorkflowRole}}

Replaced with name of the workflow role for which the message was generated. This role is specified when the task is scheduled.



13.3 Editing an Email Template

To edit an email template:

1. Click the Management  icon in the application menu.
2. In the **Email** section, click **Email Templates**.
3. Click the template you want to edit.
4. Modify the [details](#) as needed.
5. Click **Save Template**.

13.4 Deleting an Email Template

To delete an email template (other than the default templates, which cannot be deleted):

1. Click the Management  icon in the application menu.
2. In the **Email** section, click **Email Templates**.
3. Click the template you want to delete.
4. Click the Delete  button and then click **Delete** to confirm.

13.5 See Also

- [Email Distribution Lists](#)
- [Scheduling Tasks](#)


14

Admin Tools (2.10)

InterSystems Data Fabric Studio™ provides tools that you can use to [reset tasks](#) and to [view system log files](#).


14.1 Resetting Tasks

If a recipe or a snapshot appears to be hung, but you know that it is not actually hung, you can reset it so that you can try again to run it. To do so:

1. Click the Management  icon in the application menu.
2. In the **Admin Tools** section, click **Reset Resources**.
3. For **Choose a task to reset**, click the name of a recipe or snapshot.
The page then shows the current status of this item.
4. Click **Reset** in the last column in the table.
5. Click **Reset** to confirm.

14.2 Viewing Log Files

When working with your InterSystems support team, you may be asked to display log files and look for specific kinds of information. To view system log files:

1. Click the Management  icon in the application menu.
2. In the **Admin Tools** section, click **Log Files**.
The page then lists the existing log files.
3. To view a log file, click **Open Log** in the last column in the table.
4. Use the buttons at the bottom of the page to display different parts of the log.

The details of these log files are beyond the current scope of the documentation.

