



Xperiflow

Administration Tools Guide

Copyright © 2025 OneStream Software LLC. All rights reserved.

All trademarks, logos, and brand names used on this website are the property of their respective owners. This document and its contents are the exclusive property of OneStream Software LLC and are protected under international intellectual property laws. Any reproduction, modification, distribution or public display of this documentation, in whole or part, without written prior consent from OneStream Software LLC is strictly prohibited.

Table of Contents

Overview	1
Access Control & Identity Management	1
Version Management	2
Setup and Installation	3
Dependencies	3
Set Up Xperiflow Administration Tools	3
Xperiflow Set Up (Required)	5
Solution Access	7
Settings	8
Global Settings	8
Uninstall	9
Solution Info	10
Navigate in Xperiflow Administration Tools	11
Xperiflow Administration Tools Home Page	11

Table of Contents

Xperiflow Administration Tools Sections	12
Toolbar Icons	13
Identity	14
Users	14
Create a User	15
Groups	16
Create a Group	17
Identities	18
Roles	19
Create a Role	21
Permissions	22
Create a Permission	24
Assign a Permission	25
RSI Assignments	25
Create an RSI Assignment	26

Table of Contents

Scope 32

 Scope Types 32

 Scopes 34

 RSI Assignments 35

Version Management 37

 Installed Dependencies 37

 Installed Solutions 38

Help and Miscellaneous Information 39

 Display Settings 39

 Package Contents and Naming Conventions 39

 OneStream Solution Modification Considerations 40

Overview

This document details the Xperiflow Admin Tools user interface, including functionality and requirements of each page. Information includes:

- How to interact with a page.
- What happens in the AI Services engine based on user interactions.
- What a complete access control is within AI Services.

Access Control & Identity Management

One major section of XAT focuses on permissions and access management. Administrators can control access for individual users or groups across various Scopes. The access control portion of XAT is divided into three main sections: Identity (who is being given access), Role (what permissions they have), and Scope (where the access is being applied, such as within a specific SensibleAI Forecast project or globally).

These three factors combine to form an RSI (Role/Scope/Identity) Assignment. Access is determined by how these elements are configured together. An RSI Assignment, which must include one Identity, one Role, and one Scope, is required to establish access control.

For initial setup, it is recommended to configure each section (Identity, Role, Scope) individually before creating RSI assignments, as a complete control requires all three elements. The sections can be set up in any order, either sequentially or in parallel, potentially by different teams. For more detailed guidance, refer to the specific sections on Identity, Role, and Scope.

Definitions

- **Identity:** Identifies the user or group to whom access is being controlled for.
- **Role:** Defines the specific permissions that a user or group can have, for example read, write, and limits.
- **Scope:** Specifies the context or location where a role applies, for example application or project.
- **RSI Assignment:** A configuration that links an Identity, Role, and Scope together to create a complete access control within the system. Without this assignment, no access can be granted.

Version Management

In addition to access controls, XAT includes a Version Management section. This section provides a display of each AI Services solution currently installed and shows its compatibility with the dependencies installed in the environment. This allows administrators to monitor the current state of system solutions and ensure that all dependencies are compatible, helping to streamline the upgrade process.

Setup and Installation

This section contains details for planning, configuring, and installing the Xperiflow Administration Tools solution. Before you install the solution, familiarize yourself with these details.

See [OneStream Solution Modification Considerations](#)

Dependencies

Component	Description
OneStream 9.1.0 or later	Minimum OneStream Platform version required to install this version of Xperiflow Administration Tools.
Xperiflow 4.1.0 or later	Minimum version required to install this version of Administration Tools.
Xperiflow Business Rules V210 (XBR)	External API client library to allow Xperiflow Administration Tools to interface with the Xperiflow Engine. The required version of XBR is packaged with all Xperiflow Administration Tools versions.

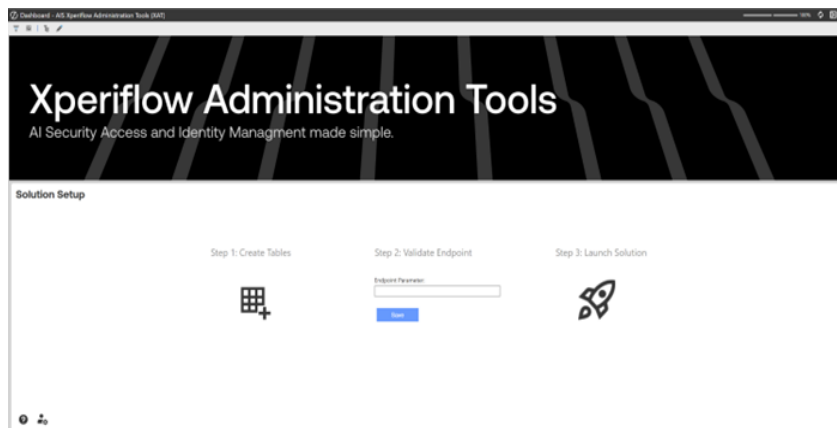
Set Up Xperiflow Administration Tools

Follow these steps to set up Xperiflow Administration Tools:

Setup and Installation

NOTE: Only Administrators or users in the XAT Administration user groups can access the Xperiflow Administration Tools solution.

1. Download the Xperiflow Administration Tools Solution from the OneStream SolutionExchange.
2. After the OneStream support team ensures that the proper contract is in place, a link is sent to download the Xperiflow Administration Tools solution and a meeting request to complete the setup, which includes setting the endpoint parameter.
3. Follow the outlined Solution Setup steps:



- a. Create Tables
 - b. Validate Endpoint
 - c. Launch Solution
4. When you reach the **Home** page displayed in [Xperiflow Administration Tools Home Page](#), Xperiflow Administration Tools is set up correctly and functioning properly.

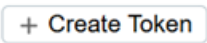
Xperiflow Set Up (Required)

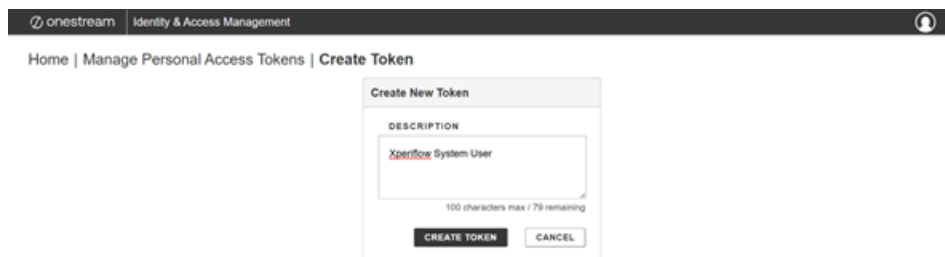
For the AI Services Solutions to function properly, a Personal Access Token (PAT) must be configured for the System User upon initial set up of XAT. This must be done by a OneStream user that is part of the Administrators group. Follow these steps to properly configure the token:

- Open the Identity & Access Management Home page by clicking the following icon at the

top of the OneStream application.



- Navigate to the **Manage Personal Access Tokens** page.
- Click the Create Token button. 
- Create a token for the Xperiflow System User:



onestream | Identity & Access Management

Home | Manage Personal Access Tokens | Create Token

Create New Token

DESCRIPTION

Xperiflow System User

100 characters max / 79 remaining

CREATE TOKEN CANCEL

- After creating the token, copy the token and navigate to the Users page of XAT.

Setup and Installation

onestream Identity & Access Management

Home | Manage Personal Access Tokens | Create Token

⚠ Remember to copy your token ID with the copy button. After you leave this page, you will not be able copy it again.

Token Created

Use the copy button to copy the token ID.

TOKEN ID
*****2766-1

DESCRIPTION
Xperiflow System User

EXPIRATION DATE
5/29/2026

[BACK TO TOKENS](#)

- Select the **System User** from the Users grid on the left and click the edit icon.

Dashboard - Xperiflow Administration Tools (XAT)

Identity Users Groups IdentityFlow

Users

Drag a column/header and drop it here to group by that column

Username	First Name	Last Name	Email	Creation Type	Creation
Administrator	Administrator		admin@onestreamsoftware.com	Custom	5/16/2025
Jane Smith	Jane	Smith	jane@onestreamsoftware.com	Custom	5/16/2025
John Doe	John	Doe	jdoe@onestreamsoftware.com	Custom	5/16/2025
System	System	System	systemuser@onestream.com	System	5/16/2025

Username: System

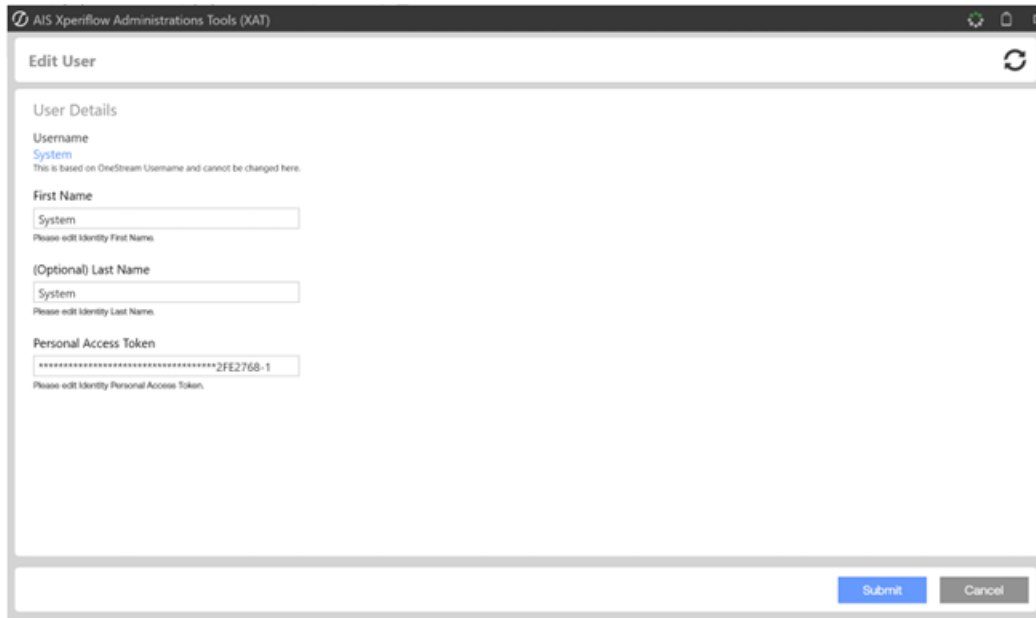
Create Edit Delete

Details

RSI Assignments

Group Assignments

- Paste the PAT token into the **Personal Access Token** field and click Submit.



The screenshot shows a web application window titled "AIS Xperiflow Administrations Tools (XAT)". Inside the window is a form titled "Edit User". The form contains the following fields:


- Username:** The value is "System". A note below the field states: "This is based on OneStream Username and cannot be changed here."
- First Name:** The value is "System". A note below the field states: "Please edit Identity First Name."
- (Optional) Last Name:** The value is "System". A note below the field states: "Please edit Identity Last Name."
- Personal Access Token:** The value is "*****2FE2768-1". A note below the field states: "Please edit Identity Personal Access Token."

At the bottom right of the form, there are two buttons: "Submit" (in blue) and "Cancel" (in grey).

Solution Access

Upon initial installation of XAT onto an OneStream environment, only users within an OneStream Administrators group will have access to the solution. There is the ability to assign a Power User Group that will grant access to the solution for other users. Any additional users that attempt to access XAT will be blocked upon entry.

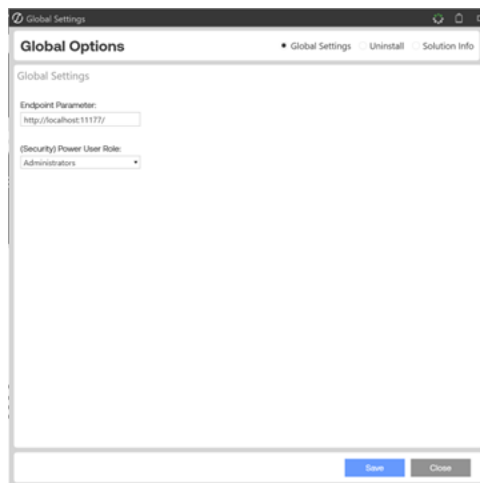
Settings

To access the Global Options page, click **Settings**  in the bottom left corner of the **Home** page or the **Version** page.

Global options include:

- [Global Settings](#)
- [Uninstall](#)
- [Solution Info](#)

Global Settings



The screenshot shows a window titled "Global Settings" with a tabbed interface. The "Global Settings" tab is active, showing a form with two fields: "Endpoint Parameter:" with a text input containing "http://localhost:11177/" and "(Security) Power User Role:" with a dropdown menu showing "Administrators". At the bottom right of the dialog are "Save" and "Close" buttons.

Endpoint Parameter

Predefined endpoint to access the application.

IMPORTANT: Do not make changes to this value unless instructed to do so.

(Security) Power User Role

Select who can access the solution and access the Global Settings content. The default is Administrators.

Uninstall



There are two uninstall options:

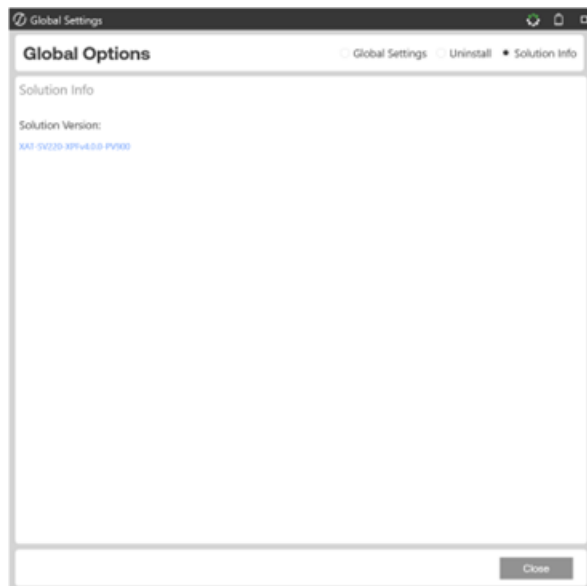
CAUTION: Uninstall procedures are irreversible.

Uninstall UI removes Xperiflow Administration Tools, including related dashboards and business rules, but leaves the database and related tables in place. Choose this option if you want to accept a Xperiflow Administration Tools update without removing data tables.

Uninstall Full removes all related data tables, data, Xperiflow Administration Tools dashboards, and business rules. Choose this option to completely remove Xperiflow Administration Tools or to perform an upgrade that is so significant in its changes to the data tables that this method is required.

Solution Info

Under Solution Version, there is a Solution Code. This code is comprised of the Solution Code, Solution Version, and OneStream platform version (Solution Code-Solution Version-OneStream platform version).

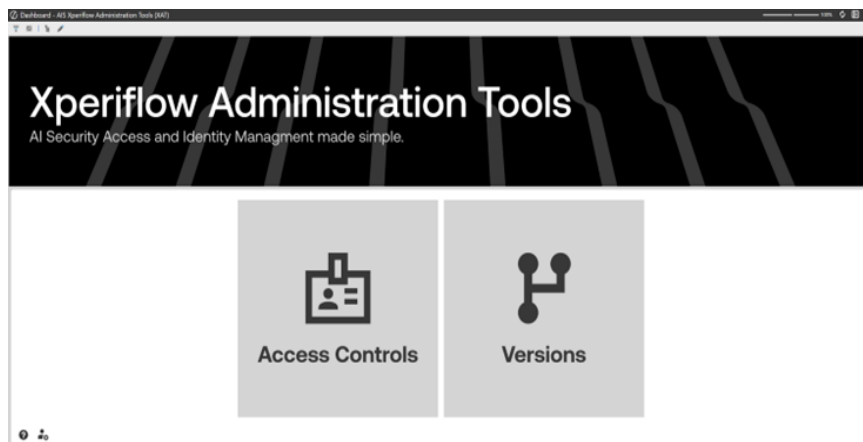


Navigate in Xperiflow Administration Tools

The following sections describe the ways to navigate in Xperiflow Administration Tools.




Xperiflow Administration Tools Home Page

The Home page displays the different administration tools available to the user.



Use the Home page to:

- Navigate to a section:
 - [Identity](#) (Access Controls)
 - [Versions](#) (Version Management)
- Access the following toolbar icons:

Icon	Description
	Opens the AI Services Activity Log
	Open theXperiflow Administration ToolsGuide
	Opens theXperiflow Administration Toolsettings. Configure Global Settings options and uninstall the solution. See Settings .

Xperiflow Administration Tools Sections

The left side navigation includes different sections and the top left navigation shows the pages available in the selected section. Below are the different sections with their respective pages:

Access Controls & Identity Management




- [Identity](#)
 - [Users](#)
 - [Groups](#)
 - [Identities](#)
- [Role](#)
 - [Roles](#)
 - [Permissions](#)
- [RSI Assignments](#)

- [Create RSI Assignments](#)
- [Scope](#)
 - [Scopes](#)
 - [RSI Assignments](#)

Version Management

- [Version Management](#)

Toolbar Icons

Icon	Description
	HOME - Navigates to the Home page.
	HELP - Opens theXperiflow Administration ToolsGuide
	SETTINGS - Opens theXperiflow Administration Toolssettings. Configure Global Settings options and uninstall the solution. See Settings .

Each section page includes a **Home** button at the top right of the page and a set of buttons at the bottom left of the page that provide additional navigation, settings, or help. Additionally, there are action or CRUD-type (create, update/edit, delete- no read) buttons in the top middle of each section.

Identity

An Identity refers to a single user or a group. Users can belong to one or more groups, and groups can include other sub-groups, creating a parent-child relationship. This structure allows for hierarchical organization of users and groups within the system.

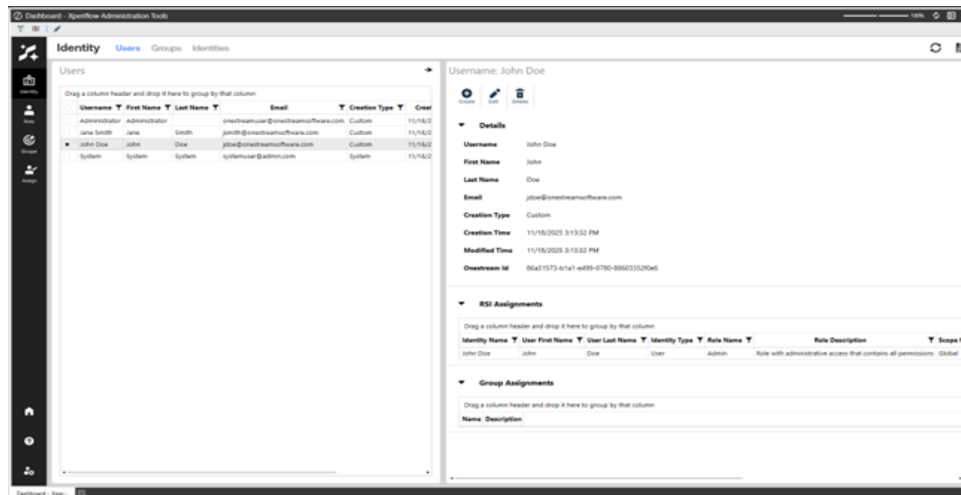
The Identity section is comprised of:

- [Users](#)
 - [How to Create a User](#)
- [Groups](#)
 - [How to Setup a Group](#)
 - [Identity Assignment \(for existing Groups\)](#)
- [Identities](#)

Users

Create, edit, delete, and view existing XAT users. Additionally, you can access user-specific details, such as existing RSI Assignments that have already been made for a particular user. These assignments only appear after they have been created.

Identity



Create a User

To manage OneStream users, the OneStream Administration Security settings for creation of users for Xperiflow Administration Tools can be utilized. This can be found within the OneStream Administration tab below.

To verify users are configured properly, check user settings within the OneStream application before attempting to create an Xperiflow user.

Identity

Security - User, John Doe

Filter

System Security Roles

Users (3)

- Administrator
- Jane Smith
- John Doe

Groups (3)

Exclusion Groups

General

Name	John Doe
Description	
User Type	Interactive
Is Enabled	True

Status

Last Login Time	
Time Enabled	5/28/2023 3:28:33 PM
Enabled By	
Time Disabled	
Disabled By	
Login Inactivity Threshold	
Time Since Last Activity	17 Hours
Remaining Allowed Inactivity	

Authentication

External Authentication Provider	(Not Used)
External Provider User Name	jdoe@onestreamsoftware.com
Internal Provider Password	*****

Preferences

Email	jdoe@onestreamsoftware.com
Culture	English (United States)
Grid Rows Per Page	50

Custom Test

Test 1	
Test 2	
Test 3	
Test 4	

Group Membership

	<input checked="" type="checkbox"/>
	<input checked="" type="checkbox"/>

Parent Groups That Contain This User

To create a user within XAT:

1. Select the **Create** button.
2. Select the OneStream user.
3. Follow the remaining confirmation steps until the user is created.

NOTE: If you receive an email error, ensure email is setup correctly within OneStream System Administration as either a preference or External Provider User Name.

Once complete, a User Identity is available for assignment to Group Identities or RSI Assignments.

Groups

Groups are used to contain User Identities for RSI Assignments.

Create a Group



Create a Group

Add Group

Group Details

Name

Please provide a Name for the new Group.

(Optional) Description

Please provide a Description for the new Group.

Submit Cancel

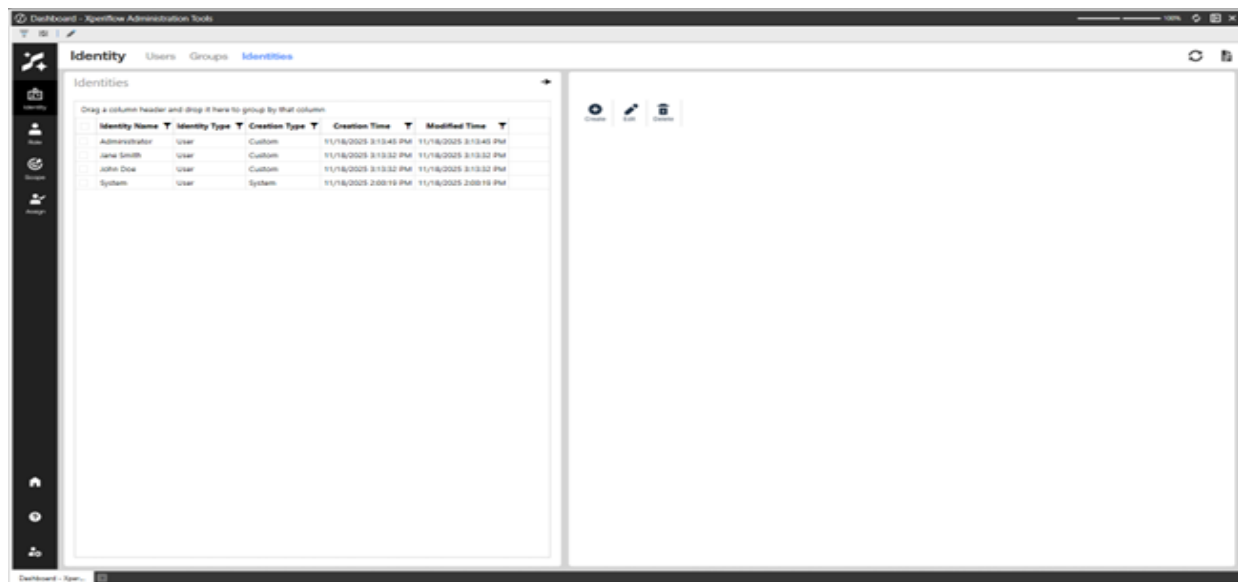
From the Groups Create dialogue box:

1. Enter a **Name** for the group.
2. Enter a **Description** (Optional).
3. Click **Submit**.

Creating an empty group does not result in an effective RSI Assignment. While the RSI Assignment can be made, it does not establish access control for any users unless User Identities or a group containing User Identities are assigned as children. Once the Group Identity container is created, assign User Identities or other groups to it.

Identities

The Identities page brings together the functionality from the Users and Groups pages since they are both Identity types. All functionality present within the Users and Groups pages are available within the Identities page in a combined format.



Creating an Identity is similar to the Users and Groups workflow, except you are asked which Identity type to create.

You can use the pages in any combination as they all reconcile with each other. To see all Identities together, use the Identities page. To view them by Identity type, use the individual Identity pages or filter the Identities grid view by Identity Type.

Roles

A Role is a container of permissions that can be assigned to an identity under a scope. Each role can have a number of permissions that will dictate what an identity can do. Without assigning permissions to a Role, the Role has no effect. To see which permissions are assigned to a role, click on it and view the “Assigned Permissions” dropdown.

The screenshot displays the Xperiflow Administration Tools interface. On the left, a sidebar contains navigation icons for Home, Roles, Permissions, and Settings. The main content area is divided into two panels. The left panel, titled 'Roles', contains a table with columns: Name, Description, Creation Type, and Category. It lists four roles: Admin, Editor, Manager, and Viewer. The right panel, titled 'Role: Admin', shows details for the Admin role, including its Name, Description, Type, and Category. Below this, the 'Assigned Permissions' section lists various permissions such as Admin CPU Limit, Admin Job Limit, Admin Job Type, Admin Memory Limit, Admin Project Limit, Admin Project Target Limit, Admin Scheduled Job Limit, Admin Task Limit, Admin Total Target Limit, Admin Web Service Limit, Delete, Read, and Write.

Name	Description	Creation Type	Category
Admin	Role with administrative access that contains all permissions	System	Generic
Editor	Read and write	System	Generic
Manager	Read, write and delete	System	Generic
Viewer	Read only	System	Generic

Permission Name	Permission Type	Permission Description	Permission Creation Type
Admin CPU Limit	CPULimit	CPU Limit Permission	System
Admin Job Limit	JobLimit	Job Limit Permission	System
Admin Job Type	JobType	All Job Types Permission	System
Admin Memory Limit	MemoryLimit	Memory Limit Permission	System
Admin Project Limit	ProjectLimit	Project Limit Permission	System
Admin Project Target Limit	ProjectTargetLimit	Project Target Limit Permission	System
Admin Scheduled Job Limit	ScheduledJobLimit	Scheduled Job Limit Permission	System
Admin Task Limit	TaskLimit	Task Limit Permission	System
Admin Total Target Limit	TotalTargetLimit	Total Target Limit Permission	System
Admin Web Service Limit	WebServiceLimit	Request Limit Permission	System
Delete	Delete	Delete Permission	System
Read	Read	Read Permission	System
Write	Write	Write Permission	System

The default roles that come with XAT are Admin; Viewer; Editor; and Manager. These are “System” roles that cannot be modified or deleted, but can be assigned to identities.

Admin

This role contains permissions that allow for maximum access across the AI Services environment.

Roles

Example: To create an administrators' group, create a group called "Administrators", add Users who require administrator rights. Then, go to the RSI Assignments page and assign the Admin role to the Administrators group under the Global scope. The group can be modified at any time by adding or removing Users from this group.

Viewer

This role contains the "Read" permission. This allows you to read anything within the scope that the role is applied.

Example: Give a User the Viewer permission inside of a SensibleAI Forecast Project Scope by setting those three items as an RSI assignment. This User would only have read permissions inside of the Project, but not write or delete permissions.

Editor

This role contains both the "Read" and "Write" permissions.

Example: Give a User the Editor permission inside of a SensibleAI Forecast Project Scope by setting those three items as an RSI assignment. This User would have read and write permissions inside of the Project, run jobs (write to the project), but not delete permissions.

Manager

This role contains the "Read", "Write", and "Delete" permissions. This role allows for any of these actions to be used under the scope it is applied.

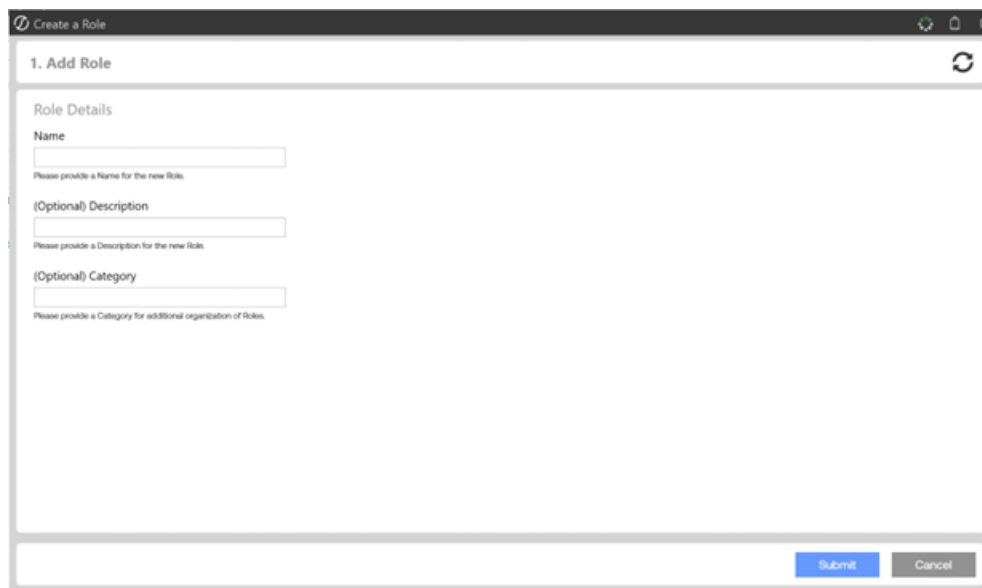
Roles

NOTE: When creating a SensibleAI Forecast Project, this Role is automatically applied to the User that creates the project and cannot be deleted. This ensures that the creator always has the ability to manage the project.

Grant Users access by creating an RSI Assignment of any of these three roles to an Identity and that project's scope. The role can also be applied globally by assigning it to the Global scope. This would apply to all project scopes, as the project scopes are all children of the global scope.

NOTE: When creating a SensibleAI Forecast Project, you are given the option to assign which Identities will have Viewer, Editor, and Manager roles inside of this project.

Create a Role



The screenshot shows a web application window titled "Create a Role". Inside the window, there is a section titled "1. Add Role" with a refresh icon. Below this is a "Role Details" section containing three input fields: "Name", "(Optional) Description", and "(Optional) Category". Each field has a placeholder text below it: "Please provide a Name for the new Role", "Please provide a Description for the new Role", and "Please provide a Category for additional organization of Roles". At the bottom right of the form, there are two buttons: "Submit" (blue) and "Cancel" (grey).

From the Roles page:

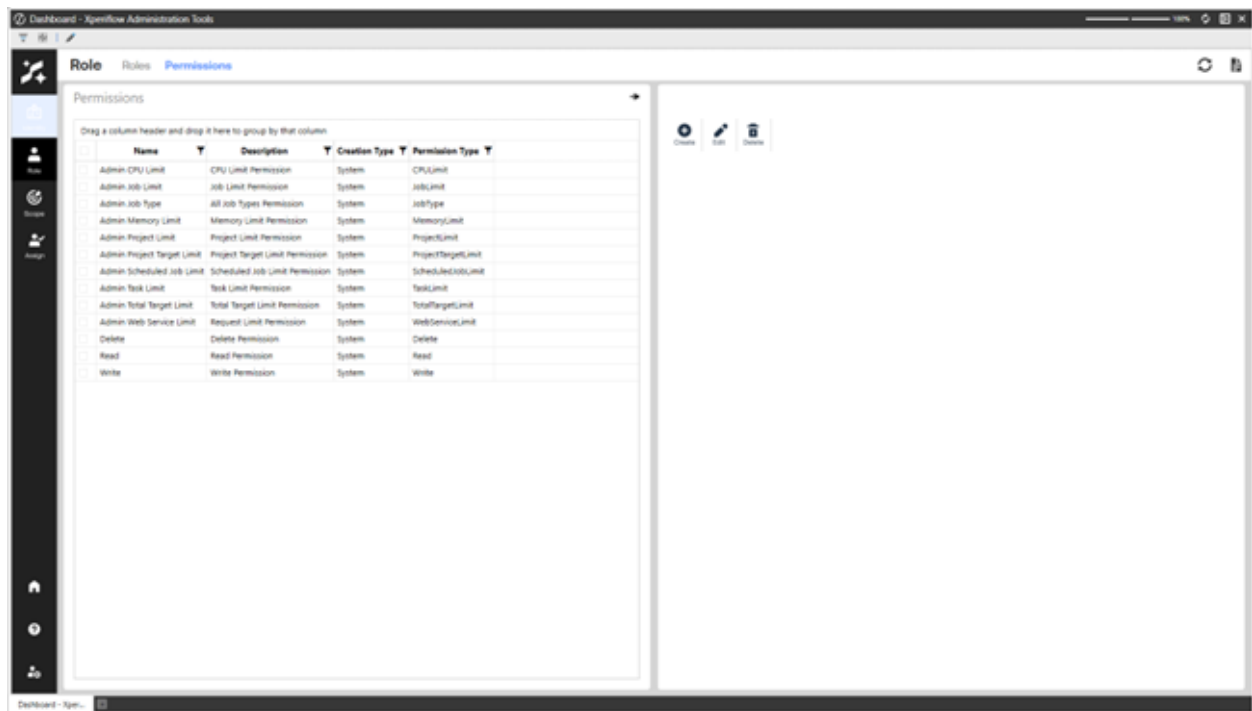
Roles

1. Select the Create button.
2. Enter a **Name**, **Description** (Optional), and **Category** (Optional)
3. Click **Submit**
4. Follow the remaining confirmation steps until the Role is created.

IMPORTANT: For a role to function, assign permissions and use in an RSI Assignment.

Permissions

For a Role to function, it must have a Permissions assigned to it.



There are two categories of Permissions:

Limit Permissions

These limit a user from doing an action too many times. There are Project Limits, Job Limits, and Memory Limits. These types of limits are validated against all identities across groups.

Example: If an Identity has a project limit of 10, but is in a group with a project limit of 5, that Identity can only create 5 projects. The associated group is taken into the equation when granting access to create a new project. In order for the user to be able to create 10 projects, they would have to be taken out of any other groups or RSI Assignments with a more restricted role than 10 projects.

Existential Permissions

These are permissions that are granted differently than limits. Read, Write, Delete, and JobType permissions are all considered existential permissions. They are not validated against all identities across groups.

Create a Permission

Create a Permission

1. Add Permission > 2. Configure Permission > 3. Verify Permission

Permission

Name

3 Concurrent Job Limit

Please provide a Name for the new Permission.

(Optional) Description

This permission allows 3 concurrent jobs to run.

Please provide a Description for the new Permission.

Permission Type	Description
Null Parameters	A null parameter input when no input parameters are required..
Job Type Permission	Holds a list of Job Types, or All.
AI Unit Limit Permission Creation	Manage AI Unit spending by setting optional limits over a stationary window of time.
CPU Limit Permission	Percentage of CPUs that can run at once.
Job Limit Permission	Number of jobs that can run concurrently.
Memory Limit Permission	Total concurrent memory allocation allowed.
Project Limit Permission	Total number of projects allowed to be created.
Project Target Limit Permission	Total number of targets allowed to be created per Sensible Machine Learning project.
Scheduled Job Limit Creation	Fill out Scheduled Job Limit information.
Task Limit Permission	Number of tasks that can run at once.

Next Cancel

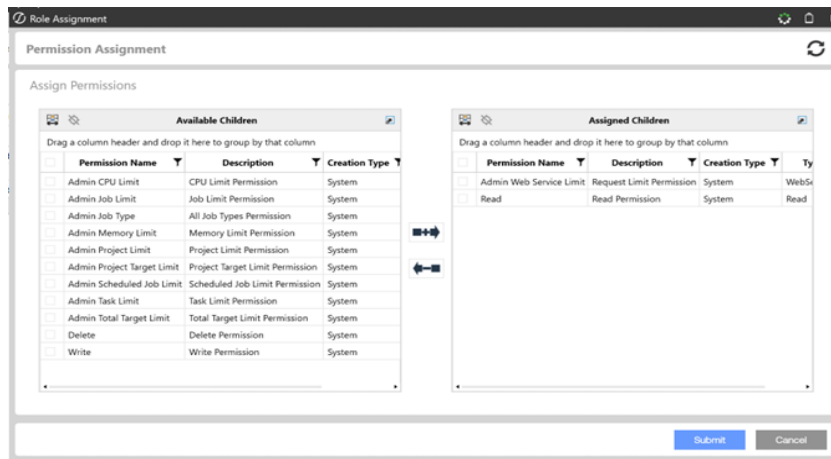
From the Permissions page:

1. Select the **Create** button.
2. Enter a **Name** and **Description** (Optional),
3. Click **Next**.
4. Follow the remaining confirmation steps until the Permission is created.

It is recommended to name the permission to detail its function.

Example: Create a ProjectLimit permission that limits the number of project to 5 named "5 Project Limit".

Assign a Permission



From the Roles page:

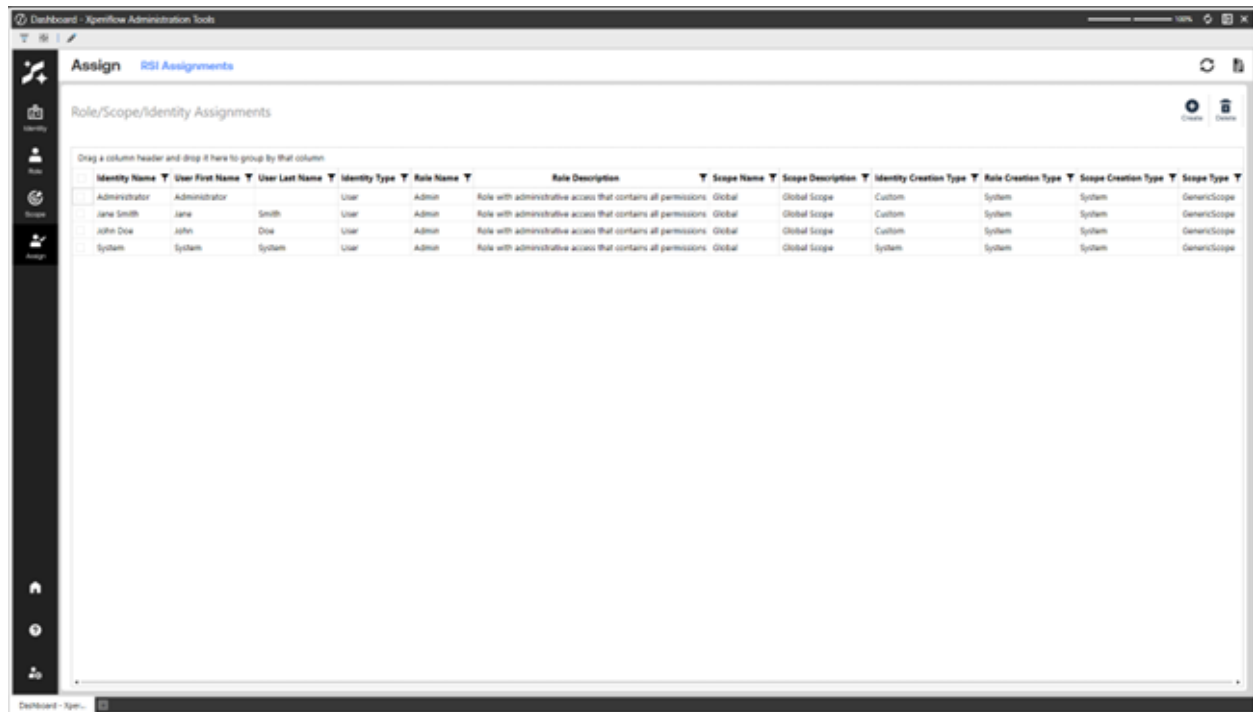
1. Select a Role.
2. Click **Permission Assignment**.
3. Move permissions to the right side.
4. Click **Submit**.

NOTE: Only one Permission of each permission type can be assigned to a Role.

RSI Assignments

An RSI Assignment is a Role, Scope, and Identity assignment. From the RSI Assignments page, user create, edit, delete, and view existing XAT RSI Assignments. This is what adds function to these items. To grant access, user must create RSI assignments. This assigns a specific Role to an Identity under a given scope.

Roles



Identity Name	User First Name	User Last Name	Identity Type	Role Name	Role Description	Scope Name	Scope Description	Identity Creation Type	Role Creation Type	Scope Creation Type	Scope Type
Administrator	Administrator		User	Admin	Role with administrative access that contains all permissions.	Global	Global Scope	Custom	System	System	GenericScope
Jane Smith	Jane	Smith	User	Admin	Role with administrative access that contains all permissions.	Global	Global Scope	Custom	System	System	GenericScope
John Doe	John	Doe	User	Admin	Role with administrative access that contains all permissions.	Global	Global Scope	Custom	System	System	GenericScope
System	System	System	User	Admin	Role with administrative access that contains all permissions.	Global	Global Scope	System	System	System	GenericScope

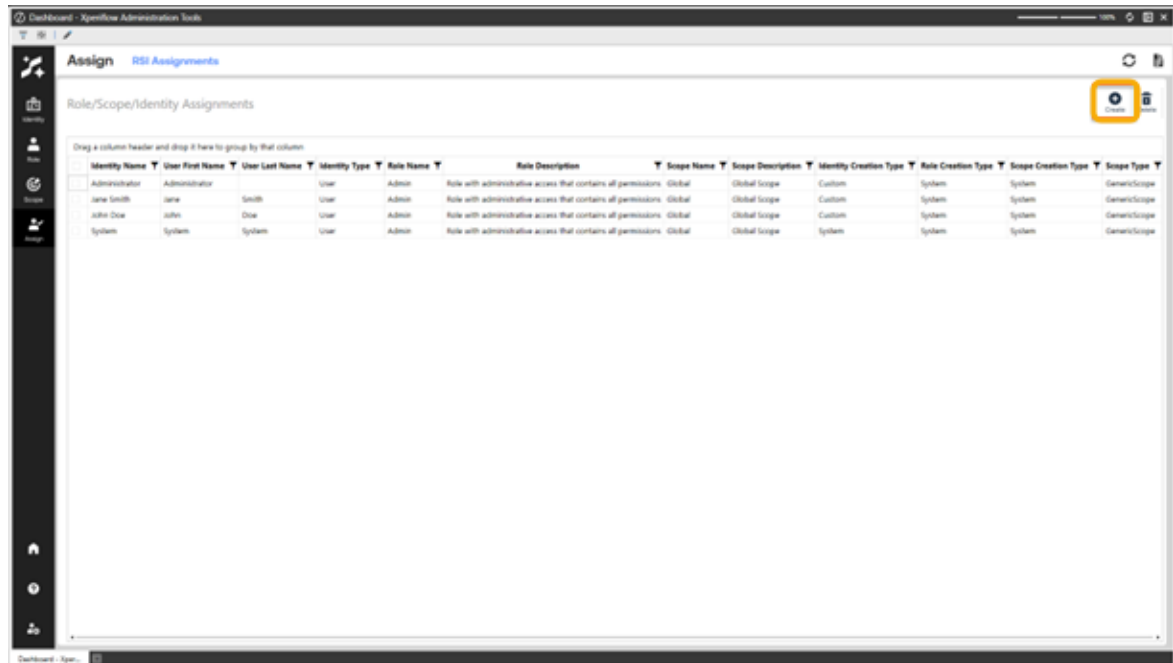
Example: To give the Viewer Role to a User within a Project scope, create an RSI Assignment with the Viewer Role, the chosen User, and a Project scope. To give a User the Viewer Role across all scopes, create an RSI Assignment with the Viewer Role, the chosen User, and the Global scope. This gives Viewer access to all Projects because all projects live within the Global scope.

Create an RSI Assignment

From the RSI Assignments page:

Roles

1. Select the **Create** button.



2. Select a scope.

Roles

AIS Xpenflow Administrations Tools (XAT)

1. Select Scope > 2. Select Role > 3. Select Identities > 4. Verify RSI Assignment

Scope

Drag a column header and drop it here to group by that column

Name	Scope Type	Description	Creation Type	Category
Global	GenericScope	Global Scope	System	Generic
XAT - AISDev1	AppSolution	Scope for XAT in AISDev1	Custom	General

Next Cancel

3. Select a role.

Roles

1. Select Scope > 2. Select Role > 3. Select Identities > 4. Verify RSI Assignment

Role

Drag a column header and drop it here to group by that column

Name	Description	Creation Type	Category
Admin	Role with administrative access that contains all permissions	System	Generic
Editor	Read and write	System	Generic
Manager	Read, write and delete	System	Generic
Viewer	Read only	System	Generic

Previous Next Cancel

4. Select identities. One or more identities can be selected to create the same RSI assignment.

Roles

The screenshot shows the 'AIS Xperiflow Administrations Tools (XAT)' window. The breadcrumb trail at the top indicates the current step: '1. Select Scope > 2. Select Role > 3. Select Identities > 4. Verify RSI Assignment'. The main area is titled 'Identities' and contains a table with the following data:

	Identity Name	Identity Type	Creation Type	Creation Time	Modified Time
<input type="checkbox"/>	Administrator	User	Custom	11/18/2025 3:13:45 PM	11/18/2025 3:13:45 PM
<input checked="" type="checkbox"/>	Jane Smith	User	Custom	11/18/2025 3:13:32 PM	11/18/2025 3:13:32 PM
<input checked="" type="checkbox"/>	John Doe	User	Custom	11/18/2025 3:13:32 PM	11/18/2025 3:13:32 PM
<input type="checkbox"/>	System	User	System	11/18/2025 2:00:19 PM	11/18/2025 2:00:19 PM

At the bottom of the window, there are three buttons: 'Previous', 'Next', and 'Cancel'.

5. Verify the created RSI assignments. Click the **Submit** button.

Roles

AIS Xperiflow Administrations Tools (XAT)

1. Select Scope > 2. Select Role > 3. Select Identities > 4. Verify RSI Assignment

Final Details

Scope
Global

Role
Admin

Identities

Drag a column header and drop it here to group by that column

Name	Identity Type
Jane Smith	User
John Doe	User

Previous

Submit

Cancel

Scope

Think of a Scope as the “where” within the who (Identity), what (Role), and where of a complete RSI Assignment access control. It defines the boundaries for which access is granted or where the specific policies (granted to Roles) are applied. A Scope can be an application, file, project, and more. For more information, see [Scope Types](#).

By default, XAT includes a global scope, under which all RSI assignments can be made. This is the most popular way to create access controls. Scopes can also have a parent/child relationship. Creating custom scopes and assigning these relations can give finer control within an environment.

NOTE: When creating a custom scope, it is best to assign it as a child to the global scope.

Scope Types

The OneStream Scope Types have varying attributes each that can be combined with parent-child hierarchical assignment.

Generic Scope

A broad, or flexible, Scope that is not tied to any specific resource type. It is used to define boundaries for a variety of contexts, such as group configurations or operations that apply to multiple types of objects or resources.

Scope

Project Scope

This Scope controls access to a specific SensibleAI Forecast project and contains a project ID which is unique to each individual project. When a SensibleAI Forecast project is created, a Project Scope is automatically created. Additionally, a Manager role (read, write and delete) is given to the identity who created the project. This can be found in the RSI Assignments page. The Project Scope name will contain the project name. This scope will be deleted when the project is deleted.

NOTE: To grant viewer access to a specific project, find the project scope and create an RSI assignment with the Viewer role, the identity in question, and the project scope in question.

IMPORTANT: The following scopes are created by the AI Services applications themselves. Do not modify them in XAT under any circumstances

Application (App Scope) Scope

This Scope controls access to specific Applications.

App Solution Scope

This Scope contains attributes for controlling access to both an Application and Scope within a single Scope.

Solution Scope

This Scope contains access for a single solution.

Scope

Create a Scope

1. Add Scope > 2. Configure Scope > 3. Verify Scope

Scope Details

Name

Please provide a Name for the new Scope.

(Optional) Description

Please provide a Description for the new Scope.

(Optional) Category

Please provide a Category for additional organization of Scopes.

Scope Type	Description
App Scope	Scope of an application.
App Solution Scope	Scope of an app and solution combination.
Generic Scope	Generic scope that has no extra attributes.
Project Scope	Scope of a Sensible Machine Learning Project.
Solution Scope	Scope of a solution.

Please select a Scope Type from the grid view.

Next **Cancel**

Scopes

On the Scopes page, users can view, create, edit, delete, and assign Scopes. OneStream provided Scopes are System Creation Types and User/Administrator created are custom. For single selections, users can expand views below to see Details, Assigned Scopes, and RSI Assignments.

Scope

Dashboard - Xperiflow Administration Tools

Scope

Scopes

Drag a column header and drop it here to group by that column

Name	Scope Type	Description	Creation Type	Category
Global	GenericScope	Global Scope	System	Generic
XAF - AISDev1	AppSolution	Scope for XAF in AISDev1	Custom	General

Scope: Global

Create Edit Assign Delete

Details

Name: Global

Description: Global Scope

Creation Type: System

Category: Generic

Assigned Children

Drag a column header and drop it here to group by that column

Name	Creation Type	Scope Type
XAF - AISDev1	Custom	AppSolution

RSI Assignments

Drag a column header and drop it here to group by that column

Identity Name	User First Name	User Last Name	Identity Type	Role Name	Role Description
System	System	System	User	Admin	Role with administrative access that contains all
Jane Smith	Jane	Smith	User	Admin	Role with administrative access that contains all
John Doe	John	Doe	User	Admin	Role with administrative access that contains all
Administrator	Administrator	Administrator	User	Admin	Role with administrative access that contains all

RSI Assignments

View RSI Assignments and filter by Scope Creation Type in the RSI assignment section.

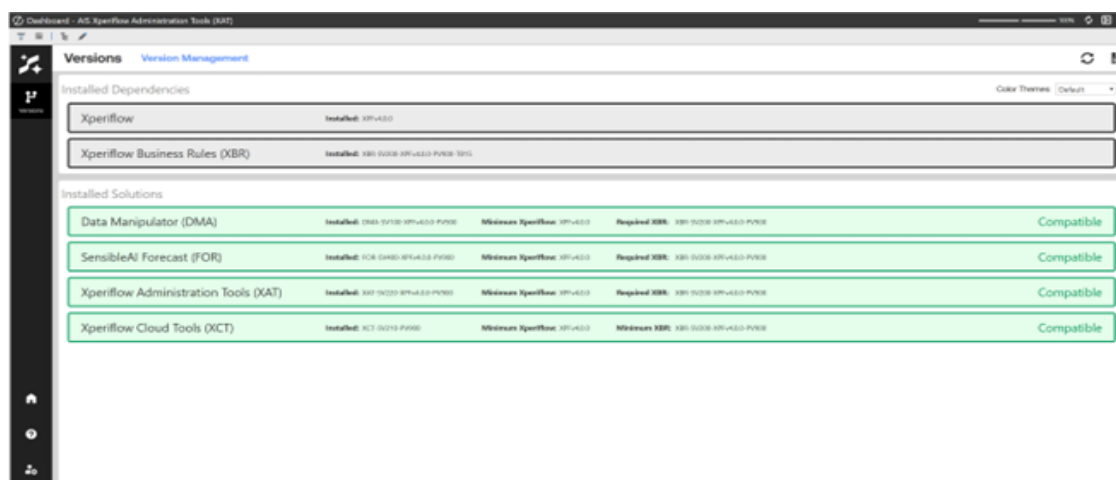
Scope

The screenshot displays the 'Assign' page within the Xperiflow Administration Tools interface. The page title is 'Assign' with a sub-header 'RSI Assignments'. Below the title, there is a section for 'Role/Scope/Identity Assignments' with 'Create' and 'Delete' buttons. A table lists assignments with columns for Identity Name, User First Name, User Last Name, Identity Type, Role Name, Role Description, Scope Name, Scope Description, Identity Creation Type, Role Creation Type, Scope Creation Type, and Scope Type. The table contains four rows of data. A filter sidebar on the right allows for filtering by Scope Creation Type, with options like 'Select All', 'System', and 'is equal to'.

Identity Name	User First Name	User Last Name	Identity Type	Role Name	Role Description	Scope Name	Scope Description	Identity Creation Type	Role Creation Type	Scope Creation Type	Scope Type
Administrator	Administrator		User	Admin	Role with administrative access that contains all permissions.	Global	Global scope	Custom	System	System	
Jane Smith	Jane	Smith	User	Admin	Role with administrative access that contains all permissions.	Global	Global scope	Custom	System	System	
John Doe	John	Doe	User	Admin	Role with administrative access that contains all permissions.	Global	Global scope	Custom	System	System	
System	System	System	User	Admin	Role with administrative access that contains all permissions.	Global	Global scope	System	System	System	

Version Management

The Version Management section of XAT allows for an administrator to easily view a snapshot of what the current versions of AI Services solutions are installed, as well as, their compatibility with each dependency installed on the environment. Below are further details on how to effectively use this page.



Installed Dependencies

The “Installed Dependencies” section, displays the current versions of each dependency installed on the AI Services environment. Upon set up an AIS environment, there are the following dependencies installed:

- **Xperiflow:** The machine learning engine used throughout all of the AI Services solutions.
- **Xperiflow Business Rules (XBR):** Shared library of functions used to interface with the Xperiflow Engine.

Installed Solutions

The “Installed Solutions” section, displays the current versions of each AI Services solution. Each installed solution displays the following:

- **Installed:** The installed version of the solution.
- **Minimum Xperiflow:** The minimum version of Xperiflow that is required for the currently installed version of the solution to be able to run.
- **Required/Minimum XBR:** The minimum or required version of XBR for the currently installed version of the solution to be able to run.
- **Compatibility Label:** An indicator of whether or not the currently installed version of the solution is compatible with the dependencies listed in the “Installed Dependencies” section.

Below are the options that will display for this label:

- **Compatible:** All of the required or minimum dependencies are installed for this solution.
- **Not Compatible:** One or multiple of the required or minimum dependencies are not installed for this solution.

NOTE: Each solution card will be color coded base on if it is “Compatible” (Green) or “Not Compatible” (Red). There is also the ability to update the Color Theme of the page for users that may need different colors than green and red.

Help and Miscellaneous Information

Display Settings

OneStream Solutions frequently require the display of multiple data elements for proper data entry and analysis. Therefore, the recommended screen resolution is a minimum of 1920 x 1080 for optimal rendering of forms and reports.

Additionally, OneStream recommends that you adjust the Windows System Display text setting to 100% and do not apply any Custom Scaling options.

Package Contents and Naming Conventions

The package file name contains multiple identifiers that correspond with the platform. Renaming any of the elements contained in a package is discouraged in order to preserve the integrity of the naming conventions.

Example Package Name: XAT_PV9.1.0_SV230_PackageContents.zip

Identifier	Description
XAT	Solution ID
PV9.1.0	Minimum Platform version required to run solution

Identifier	Description
SV230	Solution version
PackageContents	File name

OneStream Solution Modification Considerations

A considerations regarding the modification of OneStream Solutions:

- Major changes to business rules or custom tables within a OneStream Solution will not be supported through normal channels as the resulting solution is significantly different from the core solution.
- If changes are made to any dashboard object or business rule, consider renaming it or copying it to a new object. If an upgrade is applied to the OneStream Solution, this could overlay and wipe out the changes. This also applies when updating any of the standard reports and dashboards.
- If modifications are made to a OneStream Solution, upgrading to later versions could be more complex. Changes such as changing a logo or colors on a dashboard do not impact upgrades significantly. Making changes to the custom database tables and business rules, which should be avoided, could increase upgrade complexity.