S onestream

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	
Xperiflow Set Up (Required)	5
Solution Access	7
Settings	
Global Settings	
Uninstall	9
Solution Info	
Navigate in Xperiflow Administration Tools	11
Xperiflow Administration Tools Home Page	11

Xperiflow Administration Tools Sections	
Toolbar Icons	13
Identity	14
Users	14
Create a User	
Groups	16
Create a Group	17
Identities	
Roles	
Create a Role	21
Permissions	
Create a Permission	
Assign a Permission	
RSI Assignments	
Create an RSI Assignment	

Scope	
Scope Types	
Scopes	
RSI Assignments	
Version Management	
Installed Dependencies	
Installed Solutions	
Help and Miscellaneous Information	
Display Settings	
Package Contents and Naming Conventions	
OneStream Solution Modification Considerations	

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 Al 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 9.0.0 or later	Minimum OneStream Platform version required to install this version of Xperiflow Administration Tools.
Xperiflow 4.0.0 or later	Minimum version required to install this version of Administration Tools.
Xperiflow Business Rules V200 (XBR)	External API client library to allowXperiflow Administration Toolsto interface with the Xperiflow Engine. The required version of XBR is packaged with allXperiflow Administration Toolsversions.

Set Up Xperiflow Administration Tools

Follow these steps to set up Xperiflow Administration Tools:

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:

Xperiflow Adminis Al Security Access and Identity Managment made	tration Toc	bls
Solution Setup		
Step 1: Create Tables	Step 2: Validate Endpoint	Step 3: Launch Solution
毘	Indpoint Parameter:	S
, r		
o 2.		

- a. Create Tables
- b. Validate Endpoint
- c. Launch Solution
- 4. When you reach the **Home** page displayed in <u>Xperiflow Administration Tools Home Page</u>, 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



- Navigate to the Manage Personal Access Tokenspage.
- Click the Create Token button. + Create Token
- Create a token for the Xperiflow System User:



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

.

Ø onestream Identity & Access Management		0							
Home Manage Personal Access Tokens Crea									
A 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 ********2768-1 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.

@ Dealfd	board -	AS Xperifice A	dministration To	ob (KAT)					•	08 ×
ΥB	1									
x	Id	entity	Jsers Grou	pa Identiti	85				0	B
	5	sars						User	name: Suctem	_
đ	Ľ	2512								
ov th		Drag a column he	ader and drop it!	here to group by	that column			0		
÷.		Usersame	First Name 7	Last Name T	feal T	Creation Type T	Greation			
***		Administration	 Administrator 	6-34	arolain@onestreamsoftware.com	Gutton	\$2992025	L • .	Details	
C		John Doe	Jahr I	Doe	deforeiterteiterteiterte	Cators	5/08/2025			
the spectrum	l r	 System 	Spokern	System	system.ser@admin.com	System	5/25/2025			
	11							11	RSI Assignments	
								L • .	Group Assignments	
•										
"										
•										
*0	1.1									

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

AIS Xperiflow Administrations Tools (XAT)	0 C
dit User	:
Jser Details	
Isername ystem is is based on OneSteam Usemane and cannot be changed here.	
irst Name	
System Naae odt Sonttly Feet Name.	
Optional) Last Name	
System	
lease edit lävritij Last Name. *ersonal Access Token	
2FE2768-1	
aase odt Identity Personal Access Token.	
	Submit Cancel

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

Global Options	Global Settings Uninstall Solution Info
ilobal Settings	
indpoint Parameter:	
http://localhost11177/	
Security) Power User Role:	
Administrators •	

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:

lcon	Description
Ì	Opens the AI Services Activity Log
0	Open theXperiflow Administration ToolsGuide
•	Opens theXperiflow Administration Toolssettings. Configure Global Settings options and uninstall the solution. See <u>Settings</u> .

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

• <u>Scope</u>

- <u>Scopes</u>
- RSI Assignments

Version Management

Version Management

Toolbar Icons

lcon	Description
¢	HOME - Navigates to the Home page.
ଡ	HELP- Opens theXperiflow Administration ToolsGuide
* ¢	SETTINGS - Opens theXperiflow Administration Toolssettings. Configure Global Settings options and uninstall the solution. See <u>Settings</u> .

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
 - ^o 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.

⑦ Dashbo	ard - A	S Xperiflow Ac	ministration To	ols (XAT)						-	<u> </u>	¢ E	×
X	Ide	ntity u	sers Grou	ps Identitie	15							c	Ð
đ	Us	ers					•	Userna	me: Jo	hn (Doe		٦
carety.	D	ag a column hei	der and drop it h	ere to group by t	hat column			O. marke	£				
÷		Username 1	First Name T	Last Name T	Email T	Creation Type T	Creation Time T						
~~		Jane Smith	Jane	Smith	jumith@onestreamsoftware.com	Custom	5/28/2025 7:30:52 PM		Details				1
C	18	John Doe	John	Doe	jdoe@onestreamsoftware.com	Custom	5/28/2025 7.3053 PM	Uner			Line Pro		
forge		oystem	aystem	opseen	spienzie gaunicium	system	NORCHED LEVENS PR	- Chan					
								First	Name		John		
								Last?	Name	0	Doe		
								Email)	doe@onestreamsoftware.com		
								Creat	ion Type		Custom		
								Creat	ion Tim		5/28/2025 7:30:53 PM		
								Med	fied Tim		5/28/2825 7:30:53 PM		
								Later.	and during				
								Provi	der der				
								Exter	nal name)	doe@onestreamsoftware.com		
								Ois le					
								Ones	tream Id	1	1d329511-c54b-42cc-b810-8bdefe0c1f70		
•								-					1
									RSI Ass	91/114	ents		1
0								Drag	a column	heade	r and drop it here to group by that column		11
								Identi	ity Name	Ident	Ity Type Role Name Role Description Scope Name Scope Description Identity Creation Type Role Creation Type Scope Creation Type	pe 500g	41
*	1							-					2

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.

🕖 Security - User, John Do		
1 9 9 X 8 0	H 0 2 0	
Filter	8 General	· · · · · · · · · · · · · · · · · · ·
System Security Roles	Name	John Dee
Users (3)	User Type	Internation
Administrator	Is Enabled	ha
Jane Smith	() Status	
John Doe	Last Logon Time	
Groups (3)	Time Enabled	5/28/28/5 3/28/3 PM
Exclusion Groups	Enabled By	
	Time Disabled	
	Disabled By	
	Logon Inactivity Threshold	
	Time Since Last Activity	17 Hours
	Remaining Allowed Inactivity	
	B Authentication	
	External Authentication Provider	(Not Used)
	External Provider User Name	jdoe@onetheamschware.com
	Internal Provider Password	
	D Preferences	
	Email	jdoe@onestneamsoftware.com
	Culture	English (United States)
	Grid Rows Per Page	90
	() Custom Text	
	Text 1	
	Text 2	
	Text 3	
	Text 4	
	El Group Membership	
		Y X
	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	000
Add Group	C
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.

1. /											 	-
Rol	e Rol	RSI Assignments Permissions									0	
Role	es			•	Role: A	dmin						
Dra	eg a column	header and drop it here to group by that column			0	1 1	d 🖬					
	Name T	Description T	Creation Type T	Category T	Creater	- CAR A4	Assign Deters	0#				
	Admin	Role with administrative access that contains all permissions	System	Generic		Details						
	Editor	Read and write	System	Generic		Detail						
	Manager	Read, write and delete	System	Generic	Name	•	Admin					
	Vewer	Read only	System	Generic	Descr	tinting	Rolewith	h administrative acc	rest that contains all permission			
					•	Assigned P	Permission	es it here to group 1	by that column			
					Draga	Assigned P a column her	Permission	ns op it here to group b Permission Type T	by that column Permission Description	Permission Creation Type T		
					Drag a Per Admin	Assigned P a column hea mission Nan	Permission eader and dre ame T P	ens op it here to group it fermission Type T CPULinit	Permission Description	Permission Creation Type T		
					Drag a Pere Admin	Assigned P a column hes mission Nam n CPU Limit n Job Limit	Permission eader and dre une T Pe	ens op it here to group b termission Type T CPULimit ObLimit	Permission Description T CPU Limit Permission Job Limit Permission	Permission Creation Type T System System		
					Drag A Peri Admin Admin Admin	Assigned P a column hea mission Nam h CPU Limit n Job Limit n Job Type	Permission eader and dre me T Pe Cl M N	ns op it here to group b termision Type T Potimit oblimit oblimit	by that column Permission Description TPU Limit Permission All Job Types Permission	Permission Creation Type T System System System		
					Drag J Per Adreis Adreis Adreis	Assigned P a column hea mission Nam n CPU Limit n Job Limit n Job Type n Mamory Lin	Permission eader and dro une T Pe Ci Ar Ar Ar Ar	ns op it here to group it terminision Type T Pottenit oblimit oblimit detropytimit	by that column Permission Description 700 Limit Permission All Job Types Permission All Job Types Permission Memory Limit Permission	Permission Creation Type T System System System System		
					Drag a Pear Admin Admin Admir Admir Admir	Assigned P a column hea mission Nam n CPU Limit n Job Limit n Job Limit n Job Type n Memory Lim n Project Limi	Permission eader and dre ame T Pe Jo Jo Jo Jo Jo Jo Jo Jo Jo Jo Jo Jo Jo	ns ap it here to group it wministen Type Y Puttent obtimit obtimit wmorytimit ProjectLimit	by theit column Permission Description 7 CPU Limit Premission 30 Limit Premission All 30b Types Permission Project Limit Premission Project Limit Permission	Permission Creation Type T System System System System System		
					Oraga Para Admin Admin Admin Admin Admin	Assigned P a column her mission Nam 5 CPU Limit 5 Job Limit 5 Job Type 5 Memory Lin 6 Project Limi 6 Project Targ	Permission eader and des une Y Pe Cl 20 30 30 30 30 30 30 30 30 30 30 30 30 30	ns op it here to group b kensission Type T Statisti obType demogramit hogestfilmit hogestfilmit	by that column Permission Description CPU Limit Permission Allob Types Permission Memory Limit Permission Project Limit Permission Project Limit Permission	Permission Creation Type T System System System System System System		
					Drag J Peer Admin Admin Admin Admin Admin Admin	Assigned P a column hea mission Nam n CPU Umit n Job Umit n Job Type n Memory Um n Project Targ n Scheduled J	Permission eader and dre ume Y Pe 30 30 30 30 30 30 30 30 30 30 30 30 30	ns up it here to group it termission Type T PCLient obLimit obSype AemoryLimit hojectSingestLimit icheduledJobLimit	by that column Permission Description T CPU Limit Permission Jab Limit Permission Memory Limit Permission Memory Limit Permission Poject Limit Permission Poject Limit Permission Scheduled Job Limit Permission	Permission Creation Type T System System System System System System System System		
					Drag 4 Part Admin Admin Admin Admin Admin Admin Admin Admin	Assigned P a column her mission Nam o CPU Limit n Job Type n Memory Lim n Project Limit n Scheduled J n Task Limit	Permission and and dra and T Pe Ol anit M nit M sit Pe 1 Job Limit Se 1 Job Limit Se	ns op it here to group is vernission Type T StUimit obType AnnoryCimit vojectLimit VojectLimit hoduletSublimit laskLimit	by that column Permission Description CPU Link Permission Ad Job Sypen Permission Memory Link Permission Pojpet Linget Permission Scheduled Job Link Permission Scheduled Job Link Permission	Permission Creation Type T System System System System System System System System System System		
					Drag a Pert Admin Admin Admin Admin Admin Admin Admin Admin Admin	Assigned P a column her mission Nam o CPU Limit n 30b Type n Memory Lim n Project Limit n Scheduled J n Task Limit n Total Target	Permission and T Pe of Ci an an an mit M nit Pr oget Limit Pr Job Limit Si tab Limit Si tab	ns op. it here to group it termination Type T PCLink: PCLink: PCLink: obSyse AnnoryCimit tojetflargetLink: CreduleD06Link: IcheduleD06Link: IcheduleD06Link: IcheduleD06Link: IcheduleD06Link: IcheduleD06Link:	Ay that column Permission Description CPU Link Permission Juli Link Permission All Julo Sypes Permission Project Link Permission Project Link Permission Scheduled Juli Link Permission Task Link Permission Task Link Permission	Permission Creation Type 7 System System System System System System System System System 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.

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.

NOTE: When creating a SensibleAl 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 SensibleAl 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

🖉 Create a Role	000
1. Add Role	C
Role Details	
Name	
Please provide a Name for the new Role.	
(Optional) Description	
Please provide a Description for the new Role.	
(Optional) Category	
Please provide a Category for additional organization of Roles.	
	Submit Cancel
	Carcer

From the Roles page:

- 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.

					 0 0 0				
Drag	p a column header and drop Name T	Description	Creation Type T	Permission Type T	 Create Lat Deset				
	Admin CPU Limit	CPU Limit Permission	System	CPULimit	-				
	Admin Job Limit	Job Limit Permission	System	JobGimit	 + Details				
	Admin Job Type	All Job Types Permission	System	JobType	Name	Read			
	Admin Memory Limit	Memory Limit Permission	System	MemoryLimit	 -				
	Admin Project Limit	Project Limit Permission	System	ProjectLimit	Description	Read Permission			
	Admin Project Target Limit	Project Target Limit Permission	System	ProjectTargetLimit	 Creation Type	System			
	Admin Scheduled Job Limit	Scheduled Job Limit Permission	System	Scheduled/obLimit	Colonia	in the second			
	Admin Task Limit	Task Limit Permission	System	TaskLimit	Canagory	Contract strate			
	Admin Total Target Limit	Total Target Limit Permission	System	TotalTargetLimit					
	Admin Web Service Limit	Request Limit Permission	System	WebServiceLimit	 -				
	Delete	Delete Permission	System	Delete	 Assigned Hot 				
-	Read	Read Permission	System	Read	 Dran a column beade	and doop it have to a	nown ins that column		
	Write	Write Permission	System	Write					
					 Permission reame	Permission type 1	Permission Description 1	Permission Creation Type 1	
					 Read	Read	Read Permission	System	
					 Read	head	Read Permission	System	
					 No. 4	ness.	Read Permission	system	
					 nead	Mead .	News Permission	system	

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

. Add Permission > 2.0	Configure Permission > 3. Verify Permission	
Permission		
land		
vame		
3 Concurrent Job Limit		
Optional) Description This permission allows 3 concurrent tesse provide a Description for the new Perm	nt jobs to run.	
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.	
Al Unit Limit Permission Creation	Manage AI Unit spending by setting optional limits over a stationary window of tim	
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 proje	
Scheduled Job Limit Creation	Fill out Scheduled Job Limit information.	
Task Limit Permission	Number of tasks that can run at once.	

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

sigi	n Permissions								
3	8 A1	vailable Children			1	8	Assigned Children		
Dra	g a column header and drop i	it here to group by that column			Dra	g a column header and dro	p it here to group by that	column	
	Permission Name	Description T	Creation Type			Permission Name	Description T	Creation Type T	т
	Admin CPU Limit	CPU Limit Permission	System			Admin Web Service Limit	Request Limit Permission	System	Web5
	Admin Job Limit	Job Limit Permission	System			Read	Read Permission	System	Read
	Admin Job Type	All Job Types Permission	System						
	Admin Memory Limit	Memory Limit Permission	System	=+ +					
	Admin Project Limit	Project Limit Permission	System						
	Admin Project Target Limit	Project Target Limit Permission	System	+- =					
	Admin Scheduled Job Limit	Scheduled Job Limit Permission	System						
	Admin Task Limit	Task Limit Permission	System						
	Admin Total Target Limit	Total Target Limit Permission	System						
	Delete	Delete Permission	System						

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.

Ø Dech	board -	AIS Xperiflow Admir	vistration Tools (X	AT)						_	100	. 0	D ×
×	R	ole Roles F	Permissione	RSI Assignm	sente							С	ħ
42	R	ole/Scope/Iden	tity Assigner	nents •							0	0	0
R.B	4	hag a column header a	nd drop it here to	group by that col	unn								
ଁ		Identity Name Y	Meetity Type T	Rale Norse Y	Rale Description Y	Scope Name	Scope Description	Meetity Creation Type T	Role Creation Type Y	Scope Creation Type 7	Scope Type 🕈		
tenne		System	Utan	Admin	Role with administrative access that contains all permissions	Global	Ginibal Scope	System	System	System.	GenericScope		
		Administrator	User	Admin	Role with administrative access that contains all permissions	Global	Global Scope	Curtors	System	System	GenericScope		
	1.5	Jane Smith	User	Viewer	Read only	XAT - AS Development	1 Scope for XAT in AlS Development	1 Custom	System	Custom	AppColution		
		John Doe	User	Viewor	Read only	XAT - AS Development	1 Scape for XAT in AlS Development 1	1 Custom	System	Custom	applektion		
•													
20													

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:

- 1. Select the **Create** button.
- 2. Select a Role, Identity, and Scope.

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 parentchild 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.

Project Scope

This Scope controls access to a specific SensibleAl Forecast project and contains a project ID which is unique to each individual project. When a SensibleAl 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.

	a	
Add Scope 2	2. Configure Scope > 3. Verify	y Scope
cope Details		
ame		
use provide a Name for th	te new Scope.	
ptional) Descriptio	n	
ase provide a Description	for the new Scope.	
ntional Category		
ptional) Category		
ease provide a Category %	r additional organization of Scopes.	
see provide a Category fo	r additional organization of Scopes.	т
ase provide a Category to Scope Type T App Scope	e additional organization of Scopes. Description Scope of an application.	T
App Solution Scope	r additional organization of Scopes. Description Scope of an application. Scope of an app and solution combination.	
App Solution Scope	r additional organization of Scopes. Description Scope of an application. Scope of an app and solution combination. Generic scope that has no extra attributes.	
see provide a Category fo Scope Type T App Scope Upp Solution Scope Generic Scope Project Scope	r additional organization of Scopes. Description Scope of an application. Scope of an app and solution combination. Generic scope that has no extra attributes. Scope of a Sensible Machine Learning Proje	Image: Text of the second seco
Scope Type T App Scope App Solution Scope Generic Scope Project Scope Solution Scope	r additional organization of Scopes.	Image: Constraint of the second se
Asso provide a Category fo Scope Type T App Scope App Scope Seneric Scope Project Scope Solution Scope base sulect a Scope Type	v additional organization of licopee. Description Scope of an application. Scope of an app and solution combination. Generic scope that has no extra attributes. Scope of a Sensible Machine Learning Proji Scope of a solution. Ition the grid wex.	Image: Constraint of the second se
see provide a Category IX Scope Type T App Scope pp Solution Scope Seneric Scope troject Scope toution Scope team infect a Scope Type	v additional organization of ticopes. Description Scope of an application. Scope of an app and solution combination. Generic scope that has no extra attributes. Scope of a Sensible Machine Learning Proje Scope of a solution. Itom the grst view.	Image: Constraint of the second se
see provide a Category & Scope Type T App Scope App Solution Scope Beneric Scope Project Scope Isolution Scope Isolation Scope Type	e additional organization of Bioppes. Description Scope of an application. Scope of an app and solution combination. Generic scope that has no extra attributes. Scope of a Sensible Machine Learning Proj Scope of a solution. Itom the grid view.	T L ect

Scopes

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



RSI Assignments

View RSI Assignments and filter by Scope Creation Type.

× /												
Scope 5000	ns RSI Assign	ments										
Role/Scope/Ider	ntity Assignm	ents •]										0
Diag a column header	and shop it have to p	map by the col	Laman.									
Industrity Manuel 7	Indensity Tape T	Bala States 7	Rule Description T		Surger Name		Sumpt Description T	Manufilly Constitute Taper T	Bala Counting Type 7	Sumper Constitute Type: 7	Score Sport 7	
Surgers .	1. Tomate	Admin	Pole with administrative poless that contains of permissions			-	initial Scope	Surgers .	Systems	Spectrum.	Generationpe	
Advantation	1,00mm	Admin	Role with administrative access that contains of permissions	-	and a	-	Status Scrape	Custom	Symmetry	Spectrum.	Generationpe	
Contract Streams	Unar	Variation	Final only	NAT	- Arth Development	1.00	imperfor 847 in All Development 1	Custores	Taxabar III	Custors	Applications	
Autor Dee	1/her	Variation	Pleased contry	IN ALT	- AND Descriptions	1. 24	come for AAT in ART Convelopment 1	Custore	Taxable m.	Custors	Application	

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.

O Dealth	ind V	- AS Xperflow Administration Tools (XX7)				m 0	19 ×
×	v	Versions Version Management				0	Б
P	In	stalled Dependencies				Calor Themes: Oxfault	•
where the	Xperiflow Indukt 17/400						
	[Xperiflow Business Rules (XBR)	Installed: XIII 97208-39544.0.0-97408-3855				
	In	stalled Solutions					-
		Data Manipulator (DMA)	Installed: (NEA-57130-XPV-600-97930	Minimum Xperiflows X794600	Required XBR: 231-94200 319-4410-94508	Compatible	•
		SensibleAl Forecast (FOR)	Installed: FOR SHID XPT-4.03 PV900	Minimum XperHose 309-400	Required XBR: XBR 04200 XPV+LO PVKH	Compatible	•
		Xperiflow Administration Tools (XAT)	Installed: 200 59220 879-4330 79500	Minimum Xperiflow: XPv450	Required XBR: 3311 (V200 379-4110 PV901	Compatible	
		Xperiflow Cloud Tools (XCT)	Installed: XCT-0/210-P/000	Minimum Xperiflow: X01/400	Ninimurs XIP; 330-9/008-395-410-P/908	Compatible	
•							
0							
2.							

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.

ldentifier	Description
ХАТ	Solution ID
PV9.0.0	Minimum Platform version required to run solution

Example Package Name: XAT_PV9.0.0_SV221_PackageContents.zip

ldentifier	Description
SV221	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.