onestream

Admin Assist Guide

PV9.0.0 SV100

Copyright © 2026 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

Solution Overview 1

Installation and Landing Page 3

Dependencies 3

Solution Development Location 3

Installation 4

Package Contents 4

Solution Landing Page 5

Settings and Configuration 6

Solution Settings 6

Reporting Settings 6

Security Role 7

Enable Custom Reports 7

Existing Custom Report Dashboard Groups 8

Search Settings 10

Utilities Settings 11
Dimension Comparison Tree View Limit 11
Administration Tasks 12
Upgrading 12
Home Page 13
Reporting 14
Metadata Report Set 14
Base Currency DOES NOT Match Parent Currency 14
Base Entity Currencies DO NOT Match 15
Member Statistics by Dimension 15
Metadata Changes Audit 16
Security Report Set 17
Business Rule Security 17
Certification Questions Security 18
Confirmation Rules Security 20
Cube Security 22

Dimension Metadata Security 31
Dimension Security 33
Form Template Security 35
Journal Template Security 37
Other Security Reports 39
Security Group Analysis 40
Security Hierarchy 42
Transformation Rule Security 44
User Analysis 47
User Inactive List 49
User Last Logon 49
User List 50
User List by Group 52
User Logon By App 52
Workflow Security 53
Workflow Security (Expanded) 55

Formulas Report Set 57
Formula Pass – DUCS Order 57
Member Formulas 58
Database Report Set 59
Data Unit Count 59
Database Object Viewer 60
Database Size 61
Database Tables Size 61
Stage Report Set 61
Export All Workflows 61
Bypassed Records 62
Bypassed Records for All Workflows 62
Source/Target Fields - All Dimensions 63
Source/Target with Attribute Fields 63
Transformation Rules by Workflow Profile 63
Transformation Rules List 64

Unmapped Records 64
Journal Entry Report Set 64
Journal Entry Analysis Report 65
Search 67
Query Types 67
Standard Query 67
Advanced Query 68
Search Table of Contents 74
Search Report Groups 75
Utilities 76
Metadata Utilities 76
Dimension Comparison 76
Hierarchy Validation 83
Property Change History 85
Member Property Analysis 86
Member Statistics 87

Property Consistency 88

Help and Miscellaneous Information 90

Package Contents and Naming Conventions 90

OneStream Display Settings 91

Solution Modification Considerations 91

Package Contents and Naming Conventions 92

Solution Overview

OneStream Admin Assist (formerly Toolkit) empowers OneStream administrators to support their users more efficiently by providing a centralized access point to analyze security, metadata, and performance data.

The collection of utilities and reports provides OneStream administrators and power users with the ability to save time and perform tasks more efficiently. Empower your team so they have more time to improve and enhance your OneStream investment.

With OneStream Admin Assist, you can:

- Visualize and analyze the security configuration.
    - Security hierarchy
    - User analysis
    - User last logon
    - Security by object – shows security assigned to application objects (cube, dimensions, Cube Views, workflow, etc.)
- Analyze data units and data volumes to streamline and fine-tune your application.
    - Data unit count – analyze data unit records across all dimensions.
    - Database size – analyze database metrics.
    - Database table size – analyze all tables in your application.
- Analyze stage data to analyze and resolve mapping and data loading issues more efficiently.

    - Bypassed records
    - All transformation rules in the application
    - Source/target field for all dimensions
    - Unmapped records
    - Source/target with attribute fields
    - Source/target with maps
- Analyze all member formulas by formula pass.
- View summary and detailed information on journal entries across workflows.
- Easily search, using simple or complex query inputs, across all application objects to identify all areas that need to be updated when making application changes.
- View and analyze metadata characteristics and history.
- Install and start realizing the benefits in minutes.

Installation and Landing Page

This section contains important details about the solution for planning, configuration, and installation. Before you install the solution, familiarize yourself with these details.

Dependencies

Component	Description
OneStream 9.0.0 or later	Minimum OneStream Platform version required to install this version of Admin Assist Solution.

The minimum SQL compatibility level is 130.

Solution Development Location

Before beginning installation, decide whether to build the solution directly in the Production OneStream application or a separate Development OneStream application. This section provides some key considerations for each option.

- **Production OneStream Application**: The primary advantage of building the solution in a Production application is that you will not have to migrate the resulting work from a Development application. However, there are intrinsic risks when making design changes to an application used in a Production capacity, and it is not advised.

> **NOTE:** We strongly recommend that you implement the solution in the Development environment with a fresh copy of the Production application before starting work.

- **Development OneStream Application**: As a best practice, use the Development OneStream application to configure and test the solution initially.

Installation

1. Log in to OneStream.
2. On the **Application** tab, click **Tools** > **Load/Extract**.
3. On the **Load** tab, locate the solution package using the **Select File** button and click **Open**.
4. When the solution file name displays, click **Load**.
5. Click **Close** to complete the installation.

Package Contents

All solution components are within the related application Workspace.

Business Rules

All business rules are contained within Workspace assembly files.

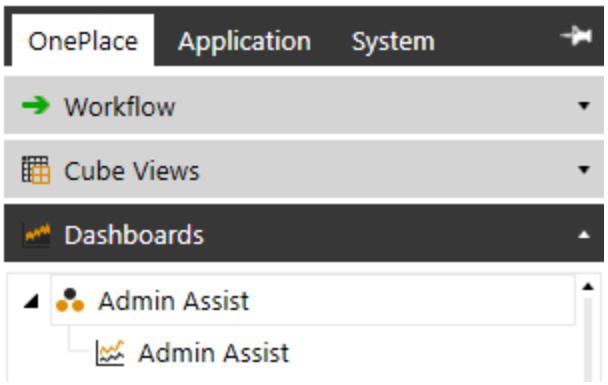
Data Structures

No data tables are created for use with this solution.

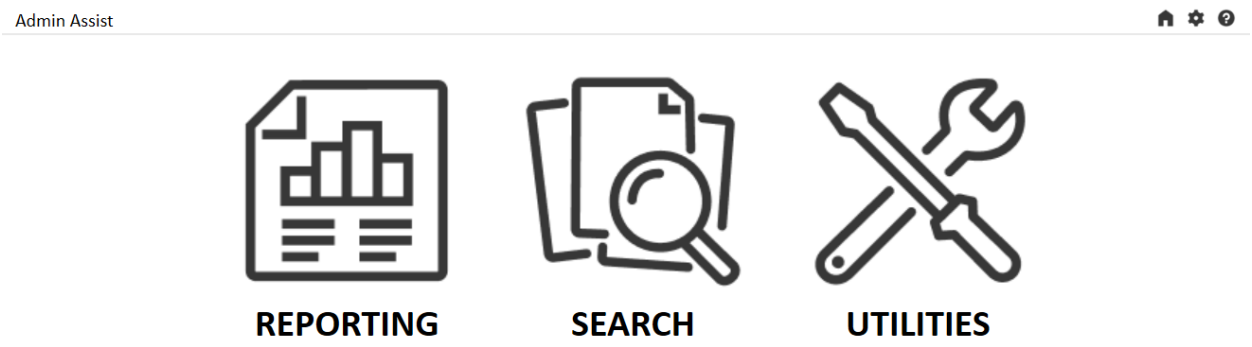
Solution Landing Page

The solution is immediately available after loading the .zip file (installation).

In OneStream, click **OnePlace** > **Dashboards** > **Admin Assist** > **Admin Assist**.



Then, you will be taken to the solution landing page.

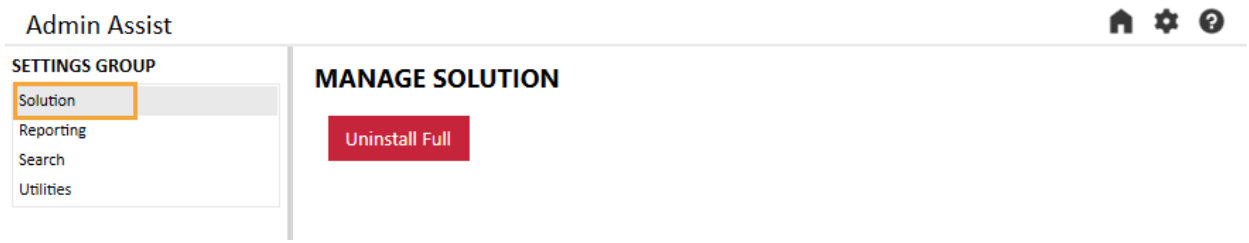


Settings and Configuration

OneStream Admin Assist has minimal settings to get started and is truly plug and play. Any individual utility that does have settings can be configured by selecting the relevant solution from the Admin page, which can be accessed by clicking the gear button in the navigation bar.

Solution Settings

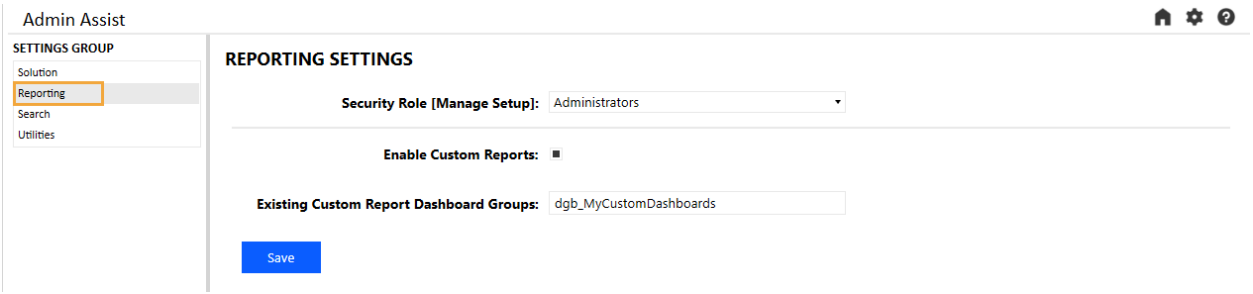
Solution Settings has options for managing the solution. Ensure Solution is selected as the Settings Group.



The Uninstall Full button will remove all the dashboard objects and business rules installed with this solution.

Reporting Settings

Reporting Settings is accessed from the Admin page by selecting the Reporting Settings Group.



Security Role

Optionally, you can select a security role to manage the reporting setup using the drop-down menu. The default will be set to Administrators.

Enable Custom Reports

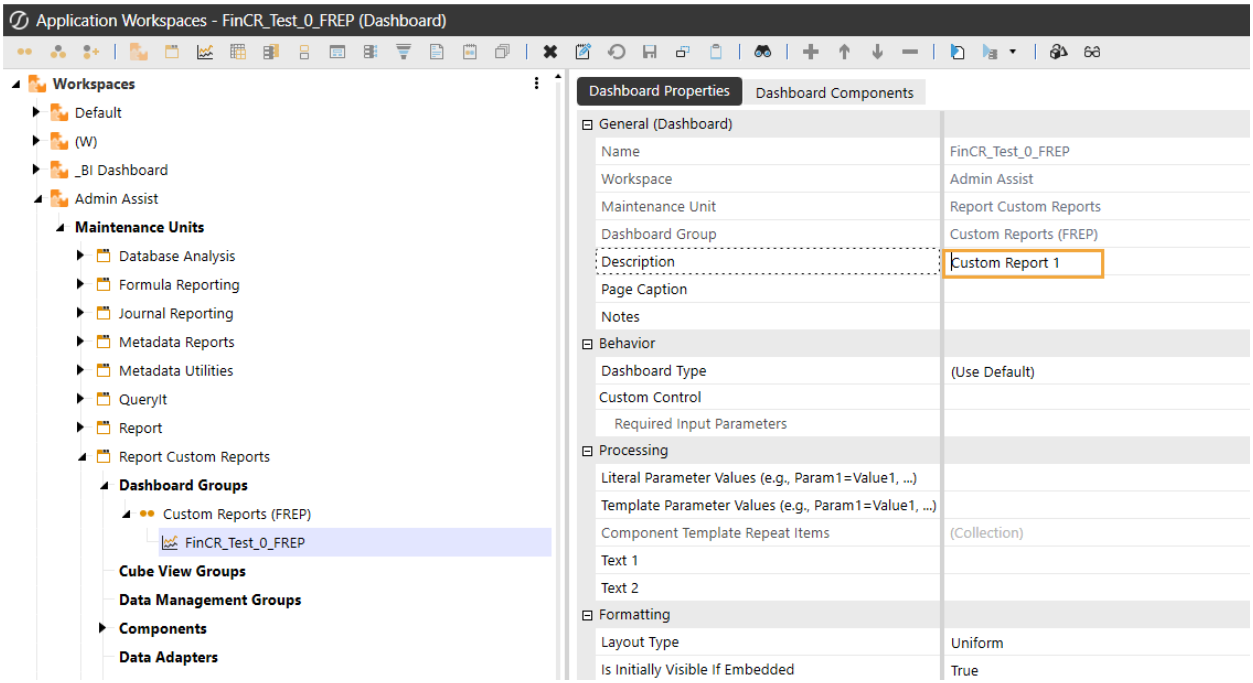
Administrators can add custom security reports using the custom reports settings.

To enable Custom Reports:

1. Click the gear button.
2. Select the **Enable Custom Reports** checkbox.

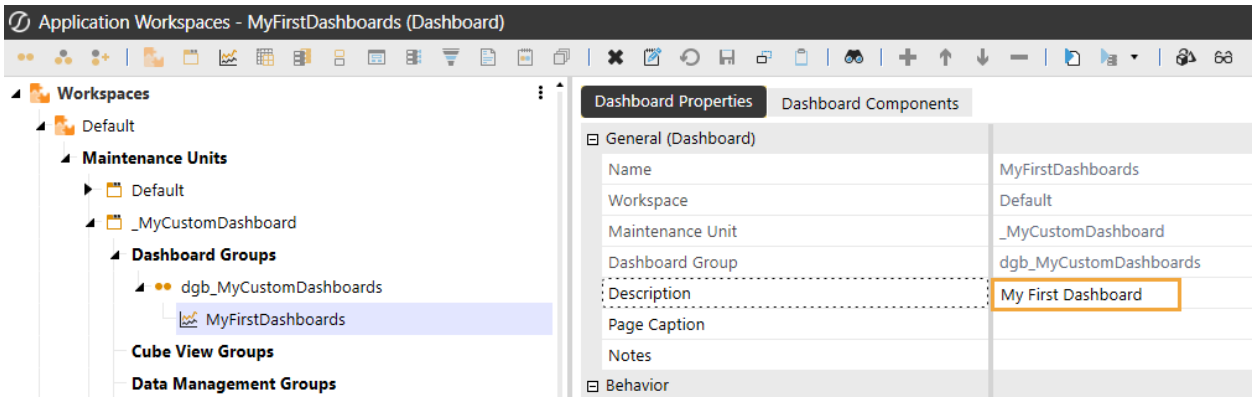
Once Custom Reports are enabled, there are two ways to add reports to the reporting list. The first is to simply add dashboards to the Custom Reports (FREP) dashboard group under the Report Custom Reports dashboard maintenance unit.

> **NOTE:** The description on the dashboard will be what shows up on the Custom Reports set; if you do not see the report in Reporting, ensure the dashboard has a description.



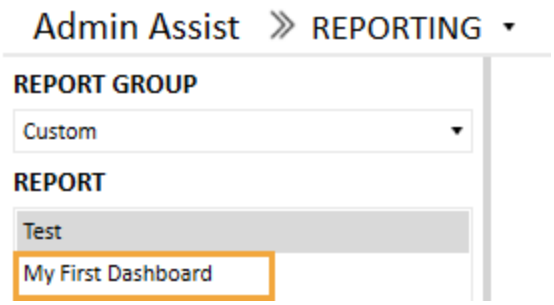
Existing Custom Report Dashboard Groups

The second way to add custom reports is to add the name of each dashboard group to the Existing Custom Report Dashboard Groups field under the Custom Groups settings.



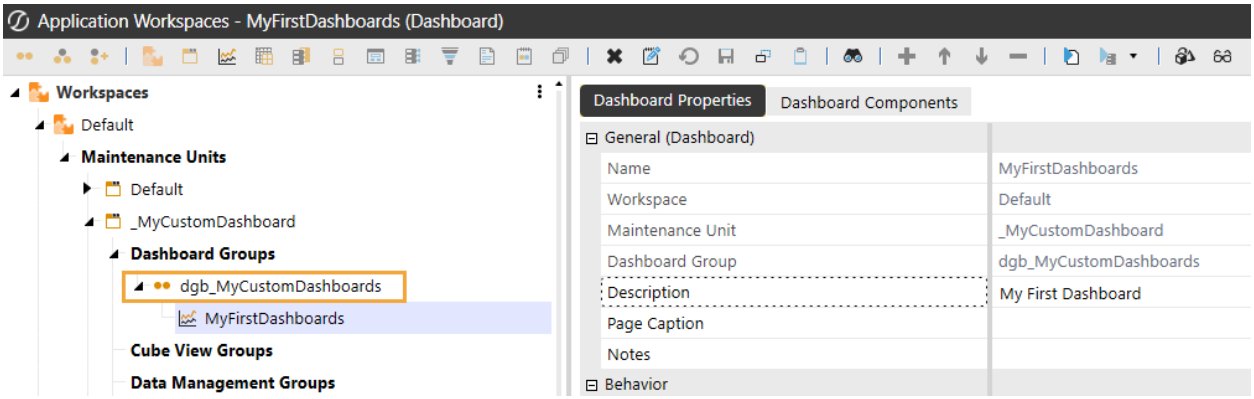
Add the ones you would like to be shown on Custom Reports, separating multiple items with a comma.

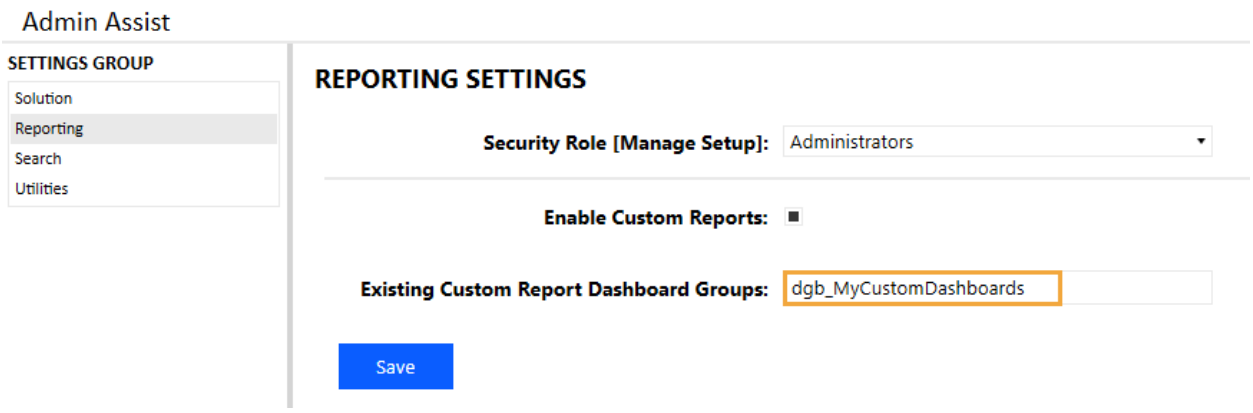
> **NOTE:** Your dashboard group and dashboard must contain a description for reports to display in the report list.



To add a report from outside the Admin Assist Workspace, preface the report name with the dashboard and a period.

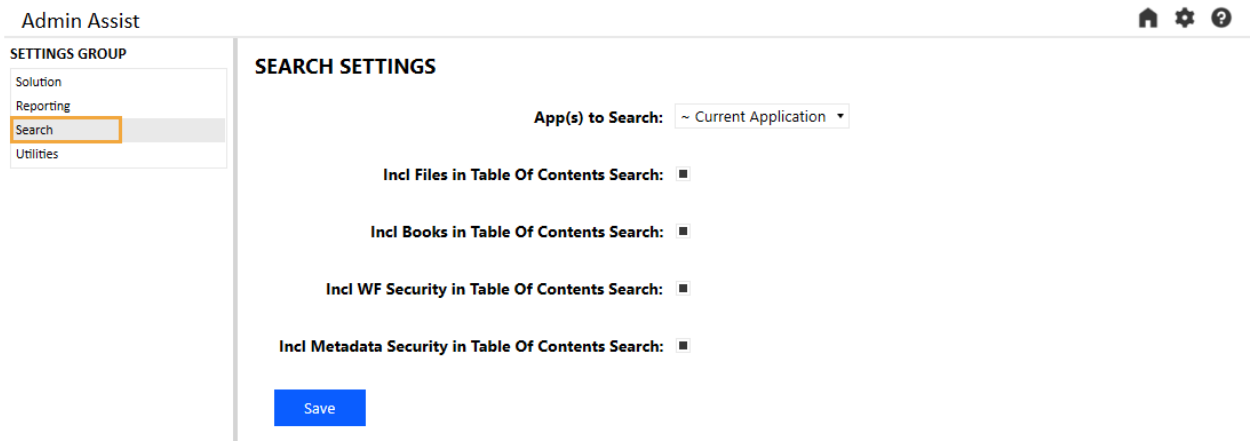
> **Example:** To add the report from the CorporateReports Workspace, enter the string CorporateReports.dgb_ MyCustomDashboards.





Search Settings

Search Settings is accessed from the Admin page by selecting the Search Settings Group.

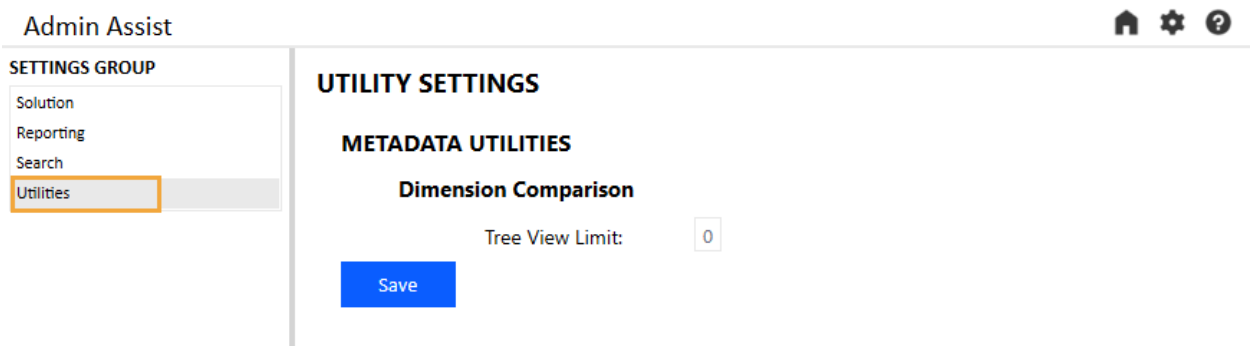


Set the OneStream applications to include in the search and object types you want to include in the Table of Contents results.

> **NOTE:** The default App(s) to Search is the application in which the solution is installed.

Utilities Settings

Utilities Settings is accessed from the Admin page by selecting the Utilities Settings Group.



Dimension Comparison Tree View Limit

This setting relates to the Dimension Comparison Utility and controls the number of tree view items that will be displayed. The default value is 0, which represents unlimited tree view items. This value can be changed to improve the performance of the Dimension Utility.

Administration Tasks

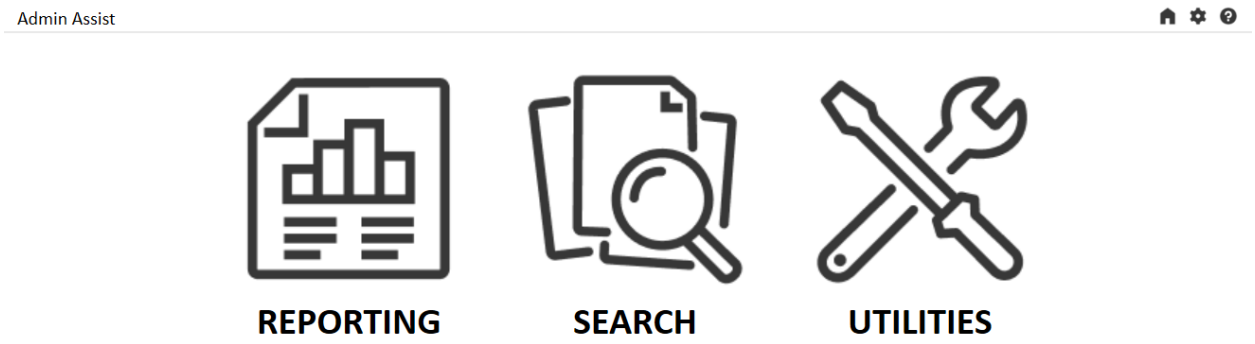
Ongoing maintenance items will depend on the design of the OneStream applications and business processes for administering specific dashboards.

Upgrading

To upgrade the solution, it is recommended to uninstall the previous version first. To uninstall the solution, go to the Admin page, select the Solution Settings Group, click the Uninstall Full button, then follow any pop-ups that display. This will remove all the dashboard objects and business rules installed with this solution.

Home Page

The Home page has buttons to launch the main utilities in OneStream Admin Assist. This launch page will grow as more utilities are added to the solution.



Reporting

See the following sections for detailed information about reporting.

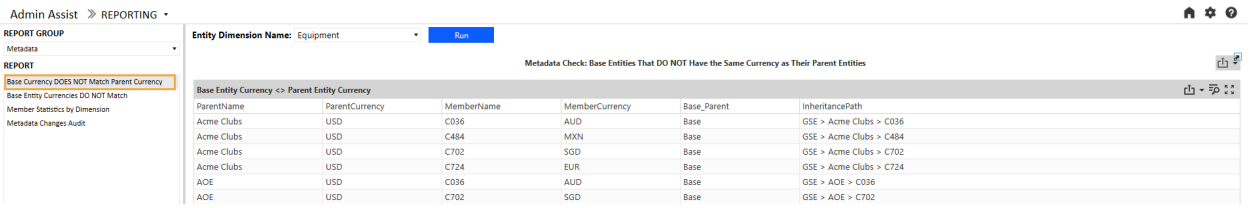
- Metadata Report Set
- Security Report Set
- Formulas Report Set
- Database Report Set
- Stage Report Set
- Journal Entry Report Set

Metadata Report Set

All the reports in the OneStream Admin Assist Metadata Report Set are detailed in this section.

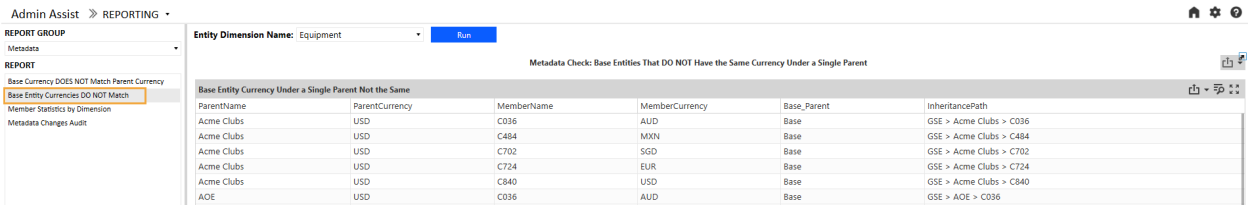
Base Currency DOES NOT Match Parent Currency

The Base Currency DOES NOT Match Parent Currency Metadata report shows, for a select Entity dimension, only base entities whose currency does not match that of its parent.



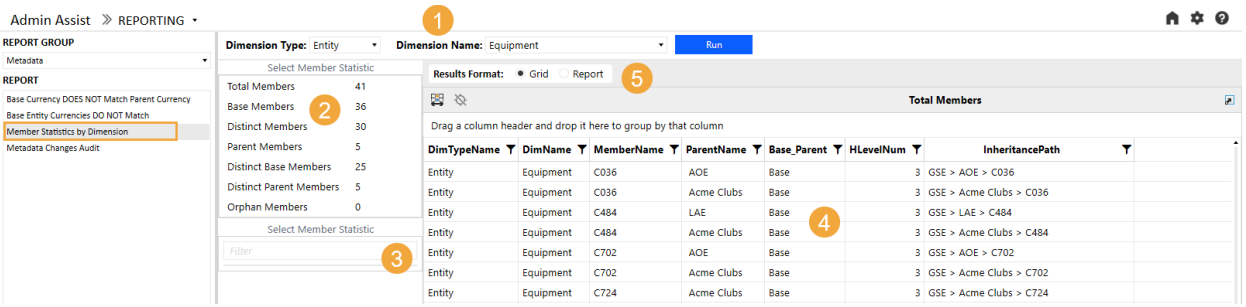
Base Entity Currencies DO NOT Match

The Base Entity Currencies DO NOT Match Metadata report shows, for a select Entity dimension, only base entities whose currency does not match that of its siblings, when those siblings are base entities. Siblings that are parent entities are ignored.



Member Statistics by Dimension

The Member Statistics by Dimension Metadata report shows, for a selected dimension, a list of statistics that can be selected to reveal the associated metadata members.



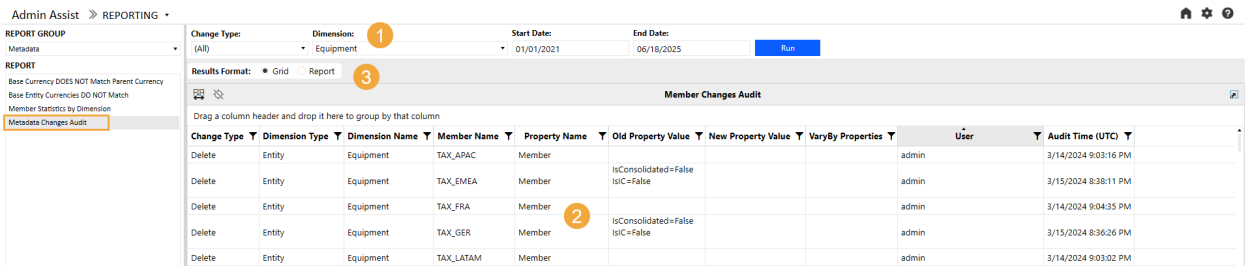
1. **Dimension Selection**: Select a dimension to run statistics for. In the drop-down menus, select a Dimension Type and then a Dimension Name.
2. **Statistics List**: Displays predefined statistics that can be selected to filter the displayed results. Select a statistic to filter the results shown on the members tree on the left (3) and member details report/grid in the center of the screen (4).

3. **Members Tree**: Presents a unique list of member names associated with the statistics selected from the Statistics List (2). When a member in the selected statistic displays more than once, the number of instances is shown to the right of the member name in brackets.
4. **Members Detail Report/Grid**: Displays a list of members that make up the statistics selected from the Statistics List (2) along with additional details for that member.
5. **Results Format**: Radio button that toggles if the member details are shown in a grid or report format.

Metadata Changes Audit

The Metadata Changes Audit report shows, for a selected change type, dimension, and start and end dates, metadata member changes from the OneStream Audit tables. The report combines what can be found in the following OneStream Application Reports (RPTA) and some additional member details as well as an option to view in grid format.

- Member Changes Audit
- Member Property Changes Audit
- Relationship Details Audit
- Entity Relationship Property Audit



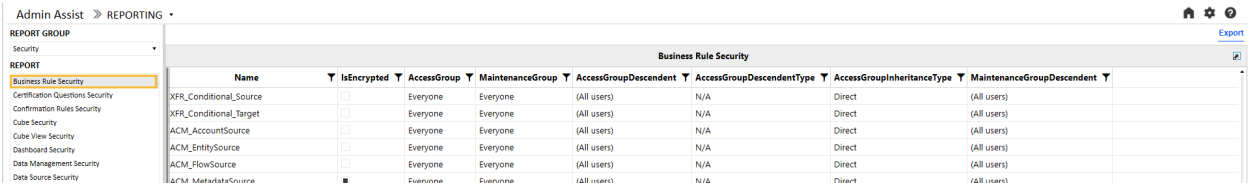
1. **Change Type, Dimension, and Date Range Selection**: Select a Change Type, Dimension, and date range to use for the report. After these selections are made, click the Run button.
2. **Results Grid/Report**: Displays changed member details based on the selected parameters.
3. **Results Format**: Radio button that toggles if the member details are shown in a grid or report format.

Security Report Set

All the reports in the OneStream Admin Assist Security Report Set are detailed in this section.

Business Rule Security

The Business Rule Security report shows a list of business rules in the OneStream application with its associated security attributes.



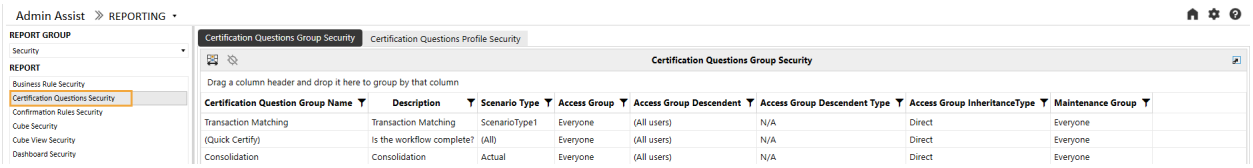
These are the columns on this report:

Attribute	Description
Business Rule Name	Business rule name
Is Encrypted	Indicates if the business rule is encrypted or not

Attribute	Description
Access Group	Indicates access group of users that can see, but not modify, the business rule
Access Group Descendent	For access groups that contain other groups or users, the child group will display here. (Only shown for groups and users detail level)
Access Group Descendent Type	Indicates whether the child is a group or user (only shown for groups and users detail level)
Access Group Inheritance Type	Indicates whether the child is directly assigned or inherits access to the parent
Maintenance Group	Shows group of users that can see the business rule and make modifications to it

Certification Questions Security

The Certification Questions Security report has tabs for group security and profile security for certification questions.

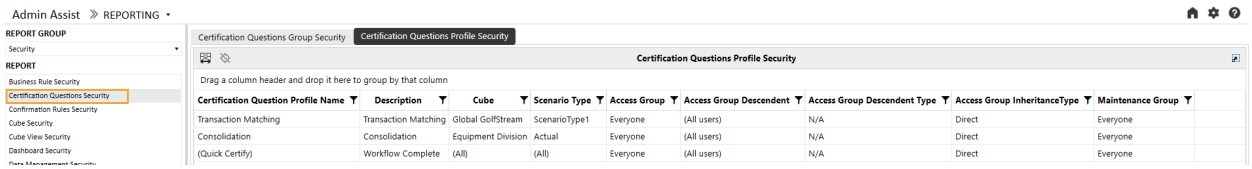


These are the columns on the Certification Questions Group Security report:

Attribute	Description
Certification Question Group Name	Certification question group name
Description	Certification question group description

Attribute	Description
Scenario Type	Indicates the Scenario Type or Types that the certification question group applies to
Access Group	Indicates access group of users that can see, but not modify, the certification question group
Access Group Descendent	For access groups that contain other groups or users, the child group will display here. (Only shown for groups and users detail level)
Access Group Descendent Type	Indicates whether the child is a group or user (only shown for groups and users detail level)
Access Group Inheritance Type	Indicates whether the child is directly assigned or inherits access to the parent
Maintenance Group	Shows group of users that can see the certification question group and make modifications to it

The second tab is the Certification Questions Profile Security report and shows a list of certification question profiles.



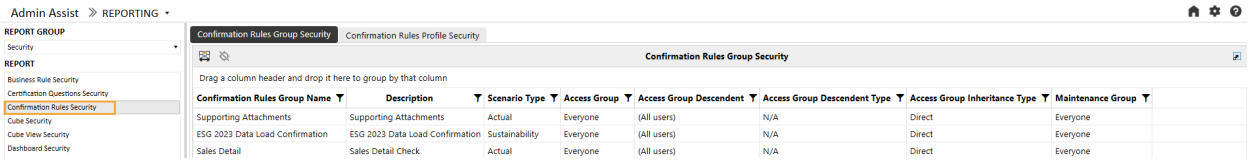
These are the columns on the Certification Questions Profile Security report:

Attribute	Description
Certification Question Profile Name	Certification question profile name

Attribute	Description
Description	Certification question profile description
Cube	Indicates the cube or cubes that the certification question profile applies to
Scenario Type	Indicates the Scenario Type or Types that the certification question profile applies to
Access Group	Indicates access group of users that can see, but not modify, the certification question profile
Access Group Descendent	For access groups that contain other groups or users, the child group will display here. (Only shown for groups and users detail level)
Access Group Descendent Type	Indicates whether the child is a group or user (only shown for groups and users detail level)
Access Group Inheritance Type	Indicates whether the child is directly assigned or inherits access to the parent
Maintenance Group	Shows group of users that can see the certification question profile and make modifications to it

Confirmation Rules Security

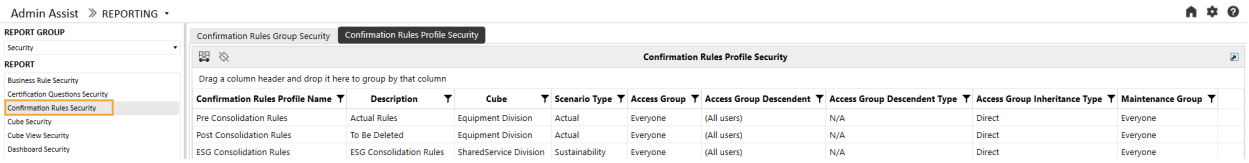
The Confirmation Rules Security report has tabs for group security and profile security for confirmation rules.



These are the columns on the Confirmation Rules Group Security report:

Attribute	Description
Confirmation Rules Group Name	Confirmation rules group name
Description	Confirmation rules group description
Scenario Type	Indicates the Scenario Type or Types that the confirmation rules group applies to
Access Group	Indicates access group of users that can see, but not modify, the confirmation rules group
Access Group Descendent	For access groups that contain other groups or users, the child group will display here. (Only shown for groups and users detail level)
Access Group Descendent Type	Indicates whether the child is a group or user (only shown for groups and users detail level)
Access Group Inheritance Type	Indicates whether the child is directly assigned or inherits access to the parent
Maintenance Group	Shows group of users that can see the confirmation rules group and make modifications to it

The second tab is the Confirmation Rules Profile Security report and shows a list of confirmation rules profiles.

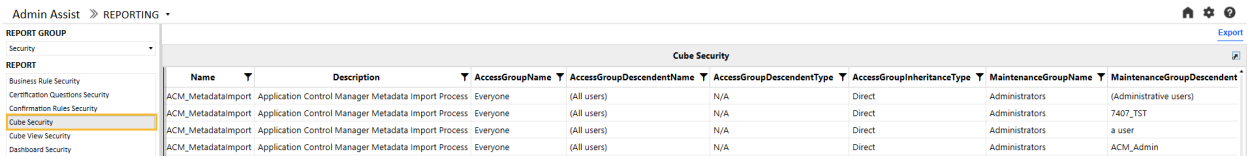


These are the columns on the Confirmation Rules Profile Security report:

Attribute	Description
Confirmation Rules Profile Name	Confirmation rules profile name
Description	Confirmation rules profile description
Cube	Indicates the cube or cubes that the confirmation rules profile applies to
Scenario Type	Indicates the Scenario Type or Types that the confirmation rules profile applies to
Access Group	Indicates access group of users that can see, but not modify, the confirmation rules profile
Access Group Descendent	For access groups that contain other groups or users, the child group will display here. (Only shown for groups and users detail level)
Access Group Descendent Type	Indicates whether the child is a group or user (only shown for groups and users detail level)
Access Group Inheritance Type	Indicates whether the child is directly assigned or inherits access to the parent
Maintenance Group	Shows group of users that can see the confirmation rules profile and make modifications to it

Cube Security

The Cube Security report shows a list of cubes in the OneStream application and access and maintenance group names associated with the cubes.

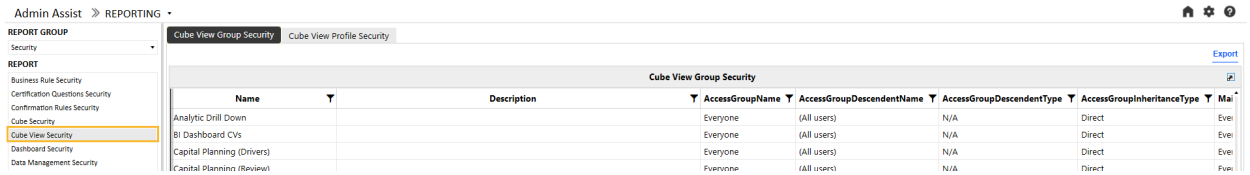


These are the columns on this report:

Attribute	Description
Cube Name	Cube name
Description	Cube description
Access Group	Indicates access group of users that can see, but not modify, the cube
Access Group Descendent Name	For access groups that contain other groups or users, the child group will display here. (Only shown for groups and users detail level)
Access Group Descendent Type	Indicates whether the child is a group or user (only shown for groups and users detail level)
Access Group Inheritance Type	Indicates whether the child is directly assigned or inherits access to the parent
Maintenance Group Name	Shows group of users that can see the cube and make modifications to it

Cube View Security

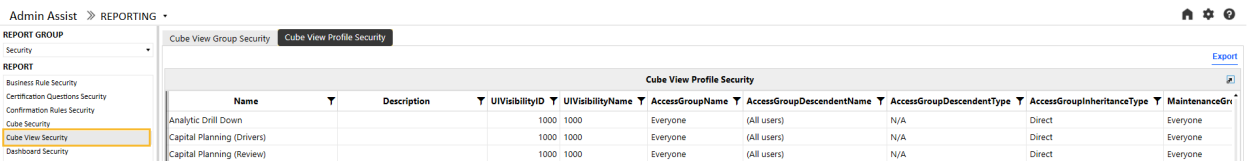
The Cube View Security report has tabs for group security and profile security for Cube Views and enables the user to see the security group setup for Cube View Groups and Cube View Profiles.



These are the columns on the Cube View Group Security report:

Attribute	Description
Cube View Group Name	Cube View Group name
Description	Cube View Group description
Access Group Name	Indicates access group of users that can see, but not modify, the Cube View Group
Access Group Descendent Name	For access groups that contain other groups or users, the child group will display here. (Only shown for groups and users detail level)
Access Group Descendent Type	Indicates whether the child is a group or user (only shown for groups and users detail level)
Access Group Inheritance Type	Indicates whether the child is directly assigned or inherits access to the parent
Maintenance Group Name	Shows group of users that can see the Cube View and make modifications to it

The Cube View Profile Security report tab shows a list of Cube View Profiles.



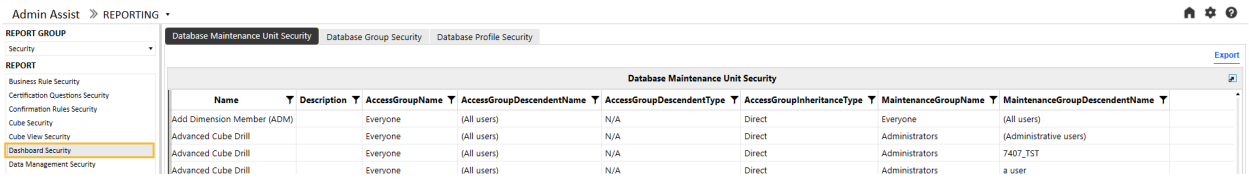
These are the columns on the Cube View Profile Security report:

Attribute	Description
Cube View Profile Name	Cube View Profile name

Attribute	Description
Description	Cube View Profile description
Visibility	Indicates the visibility settings for the Cube View Profile. This setting controls whether the Cube View Profile is visible in OnePlace, Workflows, Excel, etc.
Access Group Name	Indicates access group of users that can see, but not modify, the Cube View Group Profile
Access Group Descendent Name	For access groups that contain other groups or users, the child group will display here. (Only shown for groups and users detail level)
Access Group Descendent Type	Indicates whether the child is a group or user (only shown for groups and users detail level)
Access Group Inheritance Type	Indicates whether the child is directly assigned or inherits access to the parent
Maintenance Group Name	Shows group of users that can see the Cube View Group Profile and make modifications to it

Dashboard Security

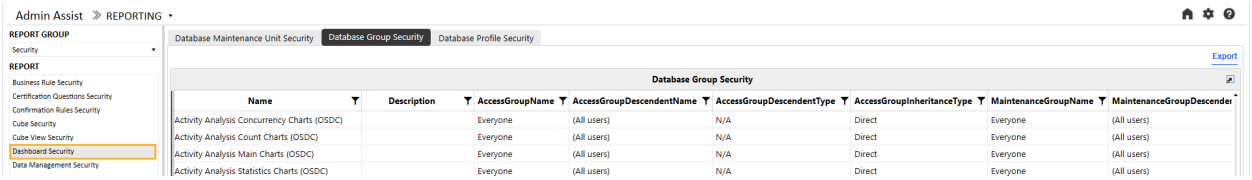
The Dashboard Security report has tabs for dashboard maintenance unit security, dashboard group security, and dashboard profile security.



These are the columns on the Dashboard Maintenance Unit Security report:

Attribute	Description
Dashboard Maintenance Unit Name	Dashboard maintenance unit name
Description	Dashboard maintenance unit description
Access Group Name	Indicates access group of users that can see, but not modify, the Dashboard Maintenance Unit
Access Group Descendent Name	For access groups that contain other groups or users, the child group will display here. (Only shown for groups and users detail level)
Access Group Descendent Type	Indicates whether the child is a group or user (only shown for groups and users detail level)
Access Group Inheritance Type	Indicates whether the child is directly assigned or inherits access to the parent
Maintenance Group Name	Shows group of users that can see the dashboard maintenance unit and make modifications to it

The Dashboard Group Security report tab shows a list of dashboard groups.

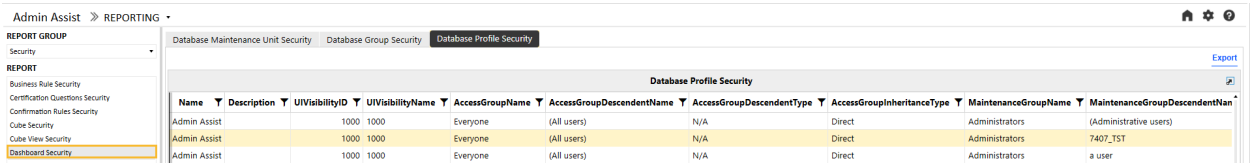


These are the columns on the Dashboard Group Security report:

Attribute	Description
Dashboard Group Name	Dashboard group name

Attribute	Description
Description	Dashboard group description
Access Group Name	Indicates access group of users that can see, but not modify, the dashboard group
Access Group Descendent Name	For access groups that contain other groups or users, the child group will display here. (Only shown for groups and users detail level)
Access Group Descendent Type	Indicates whether the child is a group or user (only shown for groups and users detail level)
Access Group Inheritance Type	Indicates whether the child is directly assigned or inherits access to the parent
Maintenance Group Name	Shows group of users that can see the dashboard and make modifications to it

The Dashboard Profile Security report tab shows a list of Dashboard Profiles.



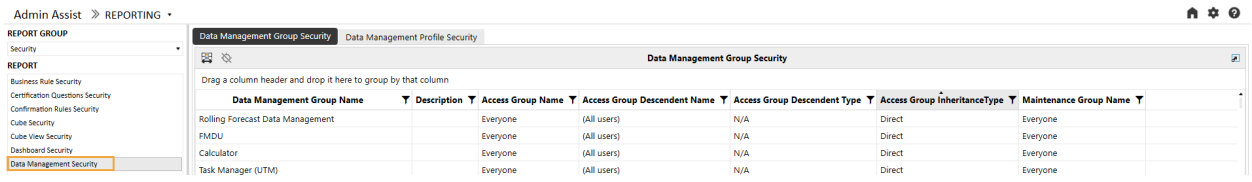
These are the columns on the Dashboard Profile Security report:

Attribute	Description
Dashboard Profile Name	Dashboard profile name
Description	Dashboard profile description
Visibility	Indicates the visibility settings for the dashboard profile. This setting controls whether the dashboard profile is visible in OnePlace, Workflows, Excel, etc.

Attribute	Description
Access Group Name	Indicates access group of users that can see, but not modify, the dashboard profile
Access Group Descendent Name	For access groups that contain other groups or users, the child group will display here. (Only shown for groups and users detail level)
Access Group Descendent Type	Indicates whether the child is a group or user (only shown for groups and users detail level)
Access Group Inheritance Type	Indicates whether the child is directly assigned or inherits access to the parent
Maintenance Group Name	Shows group of users that can see the dashboard profile and make modifications to it

Data Management Security

The Data Management Security report has tabs for group security and profile security for data management jobs and enables the user to see the security group setup for data management groups and data management profiles.



These are the columns on the Data Management Group Security report:

Attribute	Description
Data Management Group Name	Data management group name
Description	Data management group description
Access Group Name	Indicates access group of users that can see, but not modify, the data management group
Access Group Descendent Name	For access groups that contain other groups or users, the child group will display here. (Only shown for groups and users detail level)
Access Group Descendent Type	Indicates whether the child is a group or user (only shown for groups and users detail level)
Access Group Inheritance Type	Indicates whether the child is directly assigned or inherits access to the parent
Maintenance Group Name	Shows group of users that can see the data management job and make modifications to it

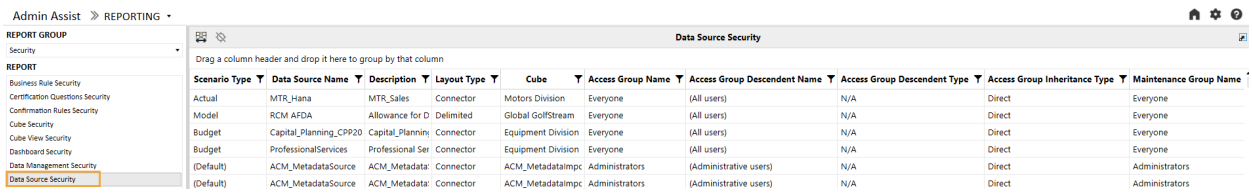
The Data Management Profile Security report tab shows a list of data management profiles. These are the columns on the Data Management Profile Security report:

Attribute	Description
Data Management Profile Name	Data management profile name
Description	Data management profile description
Access Group Name	Indicates access group of users that can see, but not modify, the data management profile
Access Group Descendent Name	For access groups that contain other groups or users, the child group will display here. (Only shown for groups and users detail level)

Attribute	Description
Access Group Descendent Type	Indicates whether the child is a group or user (only shown for groups and users detail level)
Access Group Inheritance Type	Indicates whether the child is directly assigned or inherits access to the parent
Maintenance Group Name	Shows group of users that can see the data management profile and make modifications to it

Data Source Security

The Data Source security report shows a list of all data sources in the OneStream application. Because data sources can vary by Scenario Type, the Scenario Type attribute is also included in the report. The following example shows the report and a table of the attributes.



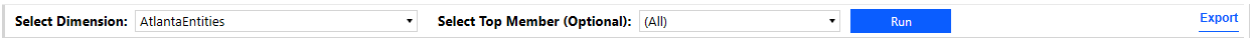
Attribute	Description
Scenario Type	This allows the profile to be assigned to a specific Scenario Type or All Scenario Types. If the data source is assigned to a specific Scenario Type, it will only be available when assigned to the Workflow Profile.
Data Source Name	Name of the data source
Description	Description of the data source (if available)
Layout Type	The layout type of the data source. It will be Fixed, Delimited, Connector, or DataMgmtExportSequence.

Attribute	Description
Cube	The cube associated with this data source, which will dictate the available dimensions that can be used
Access Group Name	Members of the assigned group have the authority to access the data source.
Access Group Descendent Name	For access groups that contain other groups or users, the child group will display here. (Only shown for groups and users detail level)
Access Group Descendent Type	Indicates whether the child is a group or user (only shown for groups and users detail level)
Access Group Inheritance Type	Indicates whether the child is directly assigned or inherits access to the parent
Maintenance Group Name	Members of the assigned group have the authority to maintain the data source.

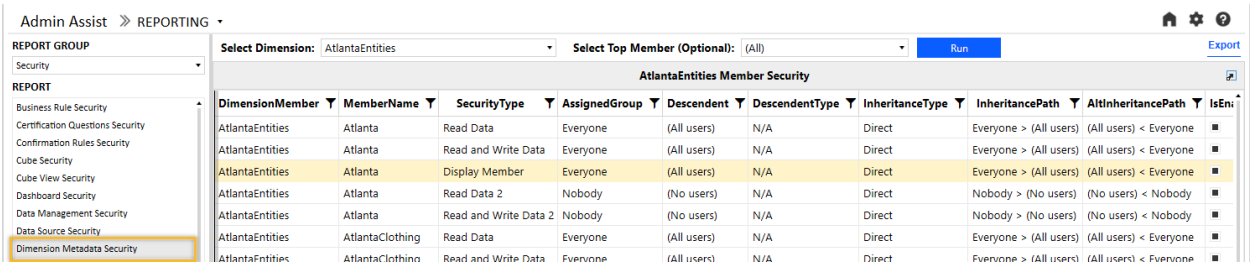
Dimension Metadata Security

The Dimension Metadata Security report enables a user to run a report that shows access to dimension members down to the user level. This report is useful to an administrator looking to see what entities a user has access to, for example, and can be used to trace security setup issues. It is also useful as an audit report to show who has access to what metadata in the application.

Select a dimension in the drop-down menu and optionally the top member in the dimension that you would like to run the report for. Then, click the Run button to generate a report as shown in the following example. For large dimensions, this may take several minutes.



The following example shows the output:



These are the columns on this report:

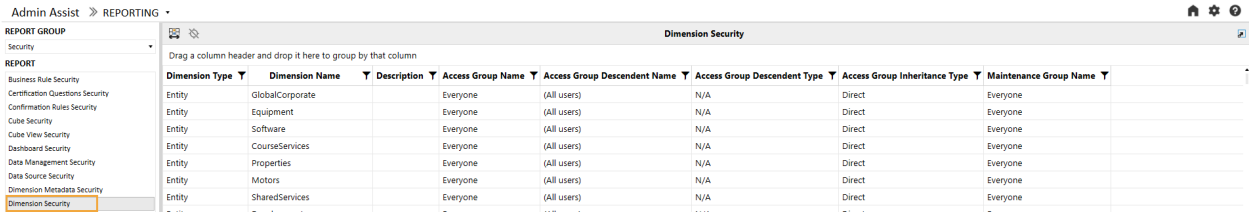
Attribute	Description
Dimension Name	The name of the dimension selected when running the report
Member Name	Member name
Security Type	This includes all applicable security groups for the selected dimension.
Assigned Group	The security group applied for the specified group type. The group that is explicitly assigned in the metadata will show as Direct under assignment type.
Descendent	For groups that contain other groups or users, the child group will display here. (Only shown for groups and users detail level)
Descendent Type	Indicates whether the child is a group or user (only shown for groups and users detail level)
Inheritance Type	Indicates whether the child is directly assigned or inherits access to the parent

Attribute	Description
Inheritance Path	This column shows how the group or user received access through an inheritance path. The first group listed is the group that the descendent has access to. Reading the inheritance path to the right will show how groups are nested to ultimately arrive to the ancestor. In the previous example, the Everyone group contains (All users).
Alternate Inheritance Path	This column shows how the group or user received the access through an inheritance path but in reversed order to show from child to parent. The first item will be the descendent. Reading the inheritance path to the right will show how groups are nested to ultimately arrive at the ancestor. In the previous example, (All users) are a member of the Everyone group.
Child Enabled	Whether or not the child is enabled for provisioning

The report has the potential to generate thousands of records because it drills down to user-level access for all members of a dimension. Therefore, large dimensions with complex security group structures will be slower to generate. To help with performance, the Everyone and Nobody groups will not drill down to user-level access. If details on the Everyone group are required, navigate to the User Analysis report. The list of users can be exported to Excel as a supplement to the Dimension Metadata Security report. For dimensions with many members, it is recommended to pre-filter the report by selecting a parent member.

Dimension Security

The Dimension Security report shows the access group and maintenance group security associated with all dimensions in the OneStream application. The following example shows this report.



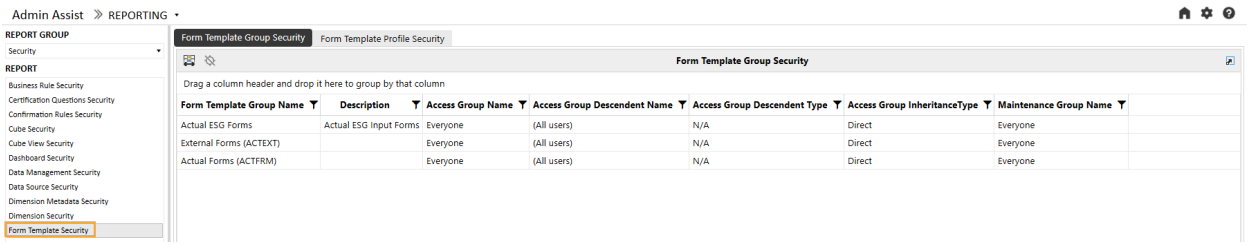
These are the columns on this report:

Attribute	Description
Dimension Type	This is the type of the dimension, such as Entity, Account, UD1, etc. Only the customizable dimensions will be shown on this report. The Parent, Cons, Origin, IC, View, and Time dimensions are not securable and therefore will not display here.
Dimension Name	Dimension name
Description	Dimension description (if available)
Access Group Name	Security group that has access to the dimension but cannot modify it
Access Group Descendent Name	For access groups that contain other groups or users, the child group will display here. (Only shown for groups and users detail level)
Access Group Descendent Type	Indicates whether the child is a group or user (only shown for groups and users detail level)
Access Group Inheritance Type	Indicates whether the child is directly assigned or inherits access to the parent

Attribute	Description
Maintenance Group Name	Security group that has access and can make changes to the dimension

Form Template Security

The Form Template Security report has tabs for group security and profile security for form templates and enables the user to see the security group setup for form template groups and form template profiles.

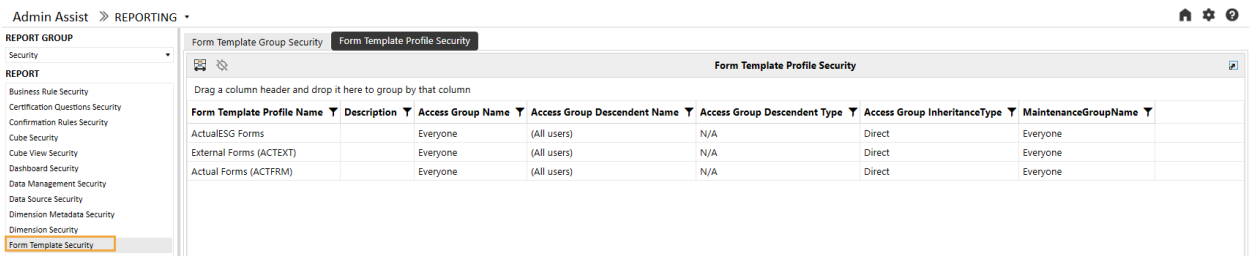


These are the columns on the Form Template Group Security report:

Attribute	Description
Form Template Group Name	Form template group name
Description	Form template group description
Access Group Name	Indicates access group of users that can see, but not modify, the form template group
Access Group Descendent Name	For access groups that contain other groups or users, the child group will display here. (Only shown for groups and users detail level)
Access Group Descendent Type	Indicates whether the child is a group or user (only shown for groups and users detail level)

Attribute	Description
Access Group Inheritance Type	Indicates whether the child is directly assigned or inherits access to the parent
Maintenance Group Name	Shows group of users that can see the form template group and make modifications to it

The Form Template Profile Security report tab shows a list of form template profiles.



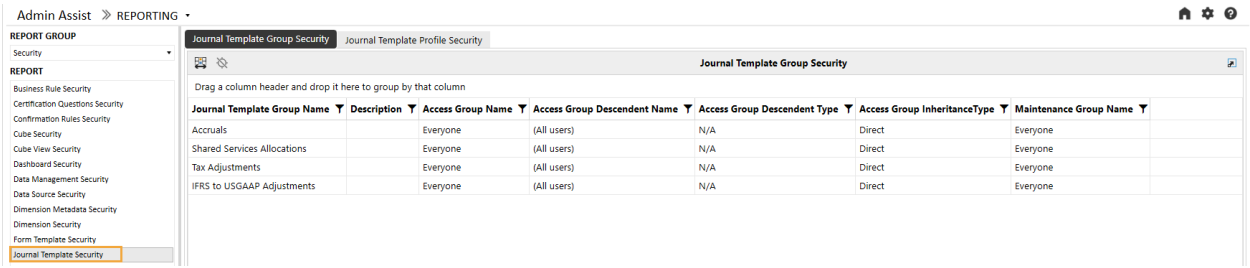
These are the columns on the Form Template Profile Security report:

Attribute	Description
Form Template Profile Name	Form template profile name
Description	Form template profile description
Access Group Name	Indicates access group of users that can see, but not modify, the form template profile
Access Group Descendent Name	For access groups that contain other groups or users, the child group will display here. (Only shown for groups and users detail level)
Access Group Descendent Type	Indicates whether the child is a group or user (only shown for groups and users detail level)
Access Group Inheritance Type	Indicates whether the child is directly assigned or inherits access to the parent

Attribute	Description
Maintenance Group Name	Shows group of users that can see the form template profile and make modifications to it

Journal Template Security

The Journal Template Security report has tabs for group security and profile security for journal templates and enables the user to see the security group setup for journal template groups and journal template profiles.

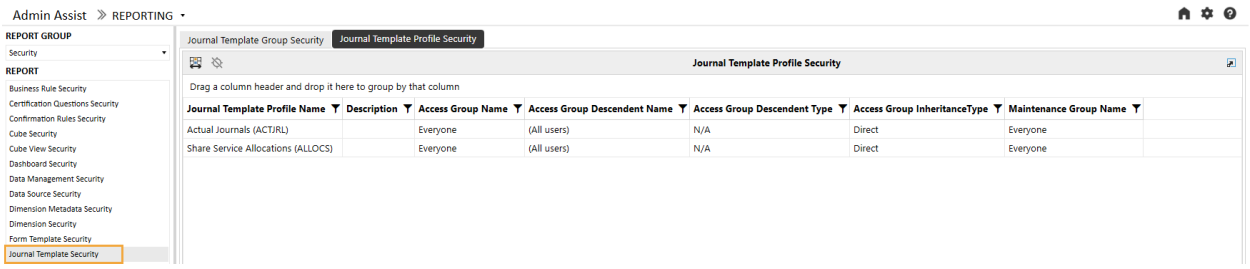


These are the columns on the Journal Template Group Security report:

Attribute	Description
Journal Template Group Name	Journal template group name
Description	Journal template group description
Access Group Name	Indicates access group of users that can see, but not modify, the journal template group
Access Group Descendent Name	For access groups that contain other groups or users, the child group will display here. (Only shown for groups and users detail level)
Access Group Descendent Type	Indicates whether the child is a group or user (only shown for groups and users detail level)

Attribute	Description
Access Group Inheritance Type	Indicates whether the child is directly assigned or inherits access to the parent
Maintenance Group Name	Shows group of users that can see the journal template group and make modifications to it

The Journal Template Profile Security report tab shows a list of journal template profiles.



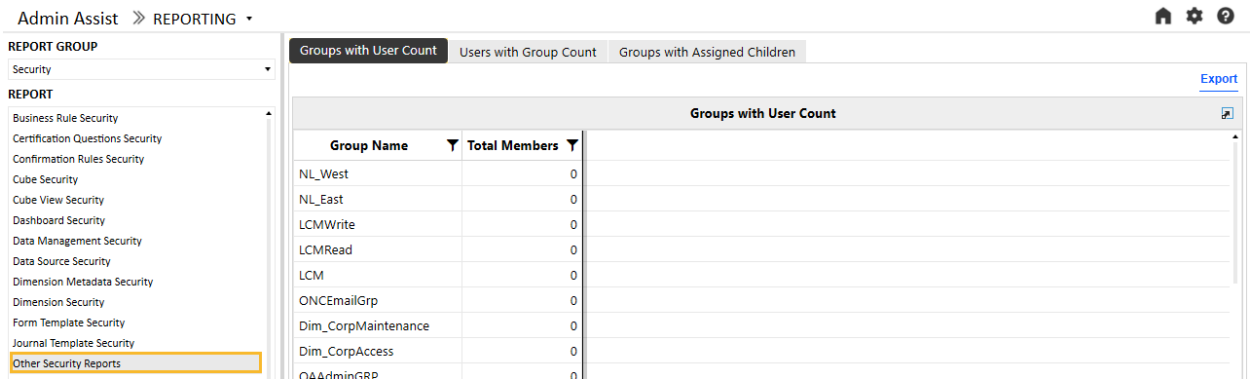
These are the columns on the Journal Template Profile Security report:

Attribute	Description
Journal Template Profile Name	Journal template profile name
Description	Journal template profile description
Access Group Name	Indicates access group of users that can see, but not modify, the journal template profile
Access Group Descendent Name	For access groups that contain other groups or users, the child group will display here. (Only shown for groups and users detail level)
Access Group Descendent Type	Indicates whether the child is a group or user (only shown for groups and users detail level)
Access Group Inheritance Type	Indicates whether the child is directly assigned or inherits access to the parent

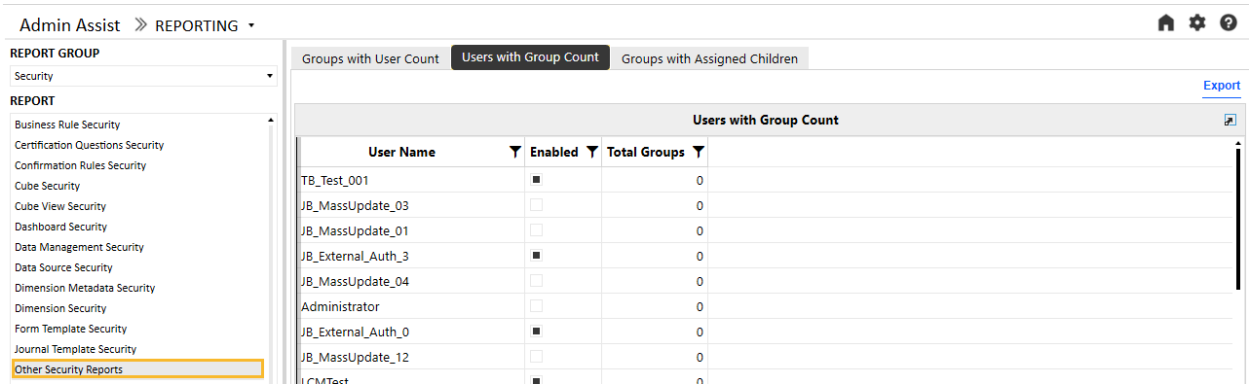
Attribute	Description
Maintenance Group Name	Shows group of users that can see the journal template profile and make modifications to it

Other Security Reports

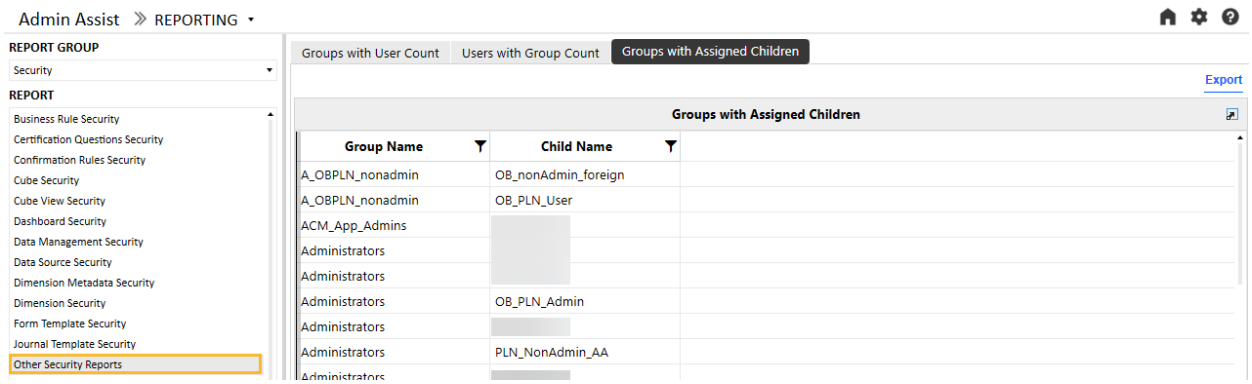
The Other Security Reports group contains additional reports for analytics and review purposes. The Groups with User Count tab lists all security groups in the system with the number of members in the group (either users or other groups). This can be helpful for removing unnecessary groups that do not contain members. The following example shows the output.



The Users with Group Count tab shows a list of users in the system, a flag that indicates if the user is enabled, and the number of total groups the user belongs to. Like the Groups with User Count report, this report can identify users that need to be disabled when they do not belong to any groups.

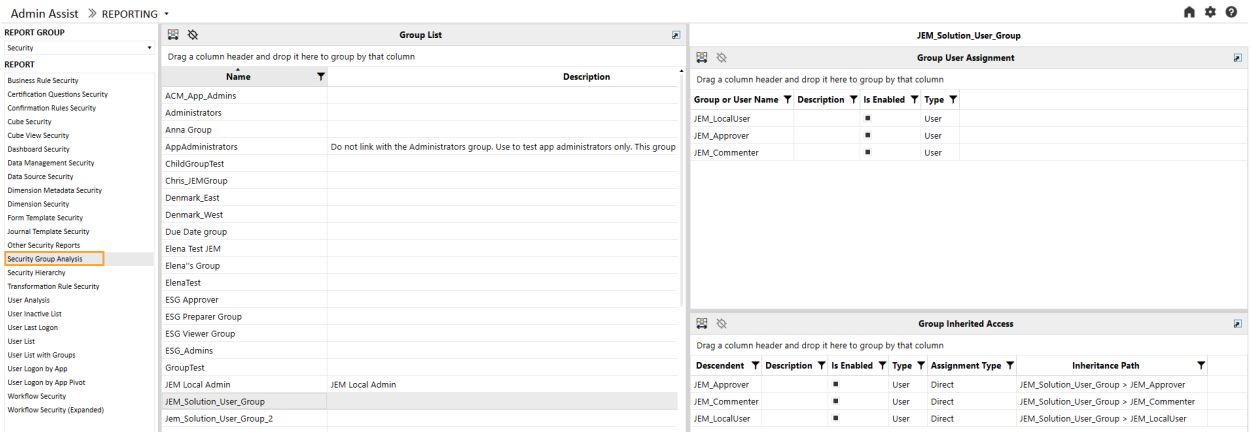


The Groups with Assigned Children tab shows the groups and related users within each group.



Security Group Analysis

The Security Group Analysis report shows a list of current groups in the system. More details on a group can be accessed by clicking on the name in the list in the left panel. This will update the reports in the right panel, as shown in the following example:



The top panel shows which users or groups have been provisioned in the selected group. In the previous example, JEM_LocalUser, JEM_Approver, and JEM_Commentator have been directly assigned to JEM_Solution_User_Group. This report has columns Group or User Name, Description, Is Enabled (True or False), and Type (User or Group).

The bottom panel shows which groups or users inherit access to the group based on their direct provisioning. In addition to the Descendent, Description, Is Enabled, and Type columns, this report has additional columns:

Attribute	Description
Assignment Type	Direct indicates that the group or user has been directly provisioned in the group. Inherited indicates that the group or user receives access to this group indirectly through nested security groups.
Inheritance Path	This column shows how the group or user received access through an inheritance path. The first group listed is the group that the descendent has access to. Reading the inheritance path to the right will show how groups are nested to ultimately arrive at the ancestor. In the previous example, the first record shows that JEM_Solution_User_Group contains JEM_Approver.

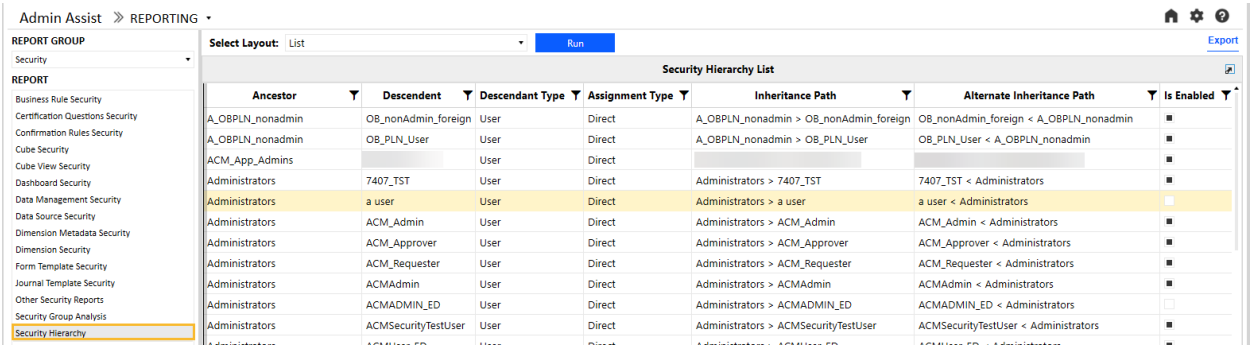
Security Hierarchy

The Security Hierarchy report enables users to see the full security assignment structure for the application. The report has List View and Hierarchy View. To run, select the layout of the report t o view, then click the Run button.

List View

The List View shows a flat list of parent-child relationships in the security structure. This view is useful for exporting the data to Excel and using a pivot table to analyze the data.

> **NOTE:** Only groups with provisioned users or groups will display in this report. The following example is a sample of the report.

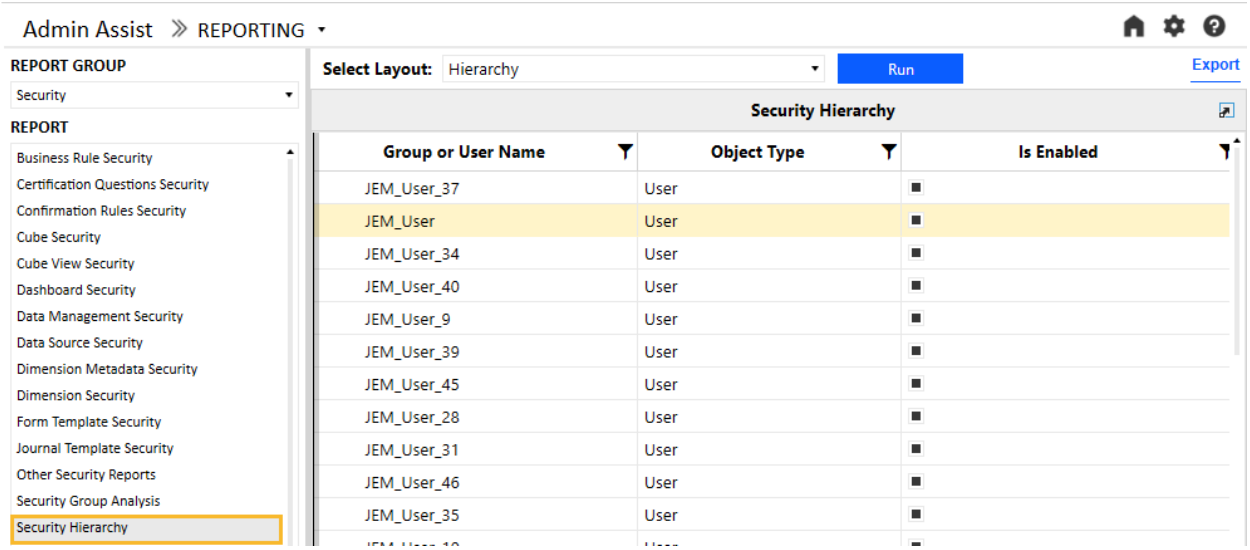


Attribute	Description
Ancestor	Security group that has groups or users provisioned
Descendent	Security group or user that has access to the parent group
Descendent Type	Indicates whether the child is a group or user
Assignment Type	Indicates whether the child is directly assigned or inherits access to the parent

Attribute	Description
Inheritance Path	This column shows how the group or user received access through an inheritance path. The first group listed is the group that the descendent has access to. Reading the inheritance path to the right will show how groups are nested to ultimately arrive to the ancestor. In the previous example, the first record shows that Administrators contains ACM_Admin. Focusing on the ACM_ Admin user, there are several parents that contain the Administrators group. Therefore, the security settings for those parents will be inherited by the Administrators group and ultimately by the ACM_Admin user.
Alternate Inheritance Path	This column shows how the group or user received the access through an inheritance path but in reversed order to show from child to parent. The first item will be the descendent. Reading the inheritance path to the right will show how groups are nested to ultimately arrive to the ancestor. In the previous example, the first record shows that ACM_Admin is a member of Administrators.

Hierarchy View

The Hierarchy view shows how security groups are nested and whether inherited security is in effect. The following example is a sample of this report. It shows which groups or users belong to each group and will inherit that security profile.

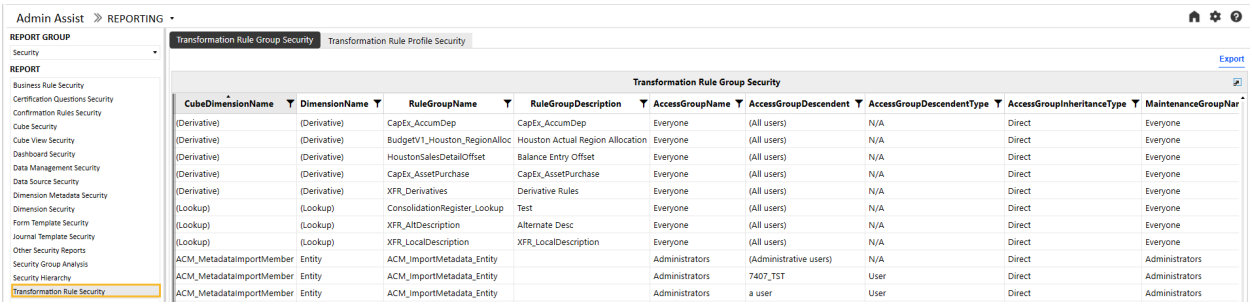


This report has these columns:

Attribute	Description
Group or User Name	Name of the group or user
Object Type	Indicates if the object is a group or a user
Is Enabled	Whether or not the object is enabled for provisioning

Transformation Rule Security

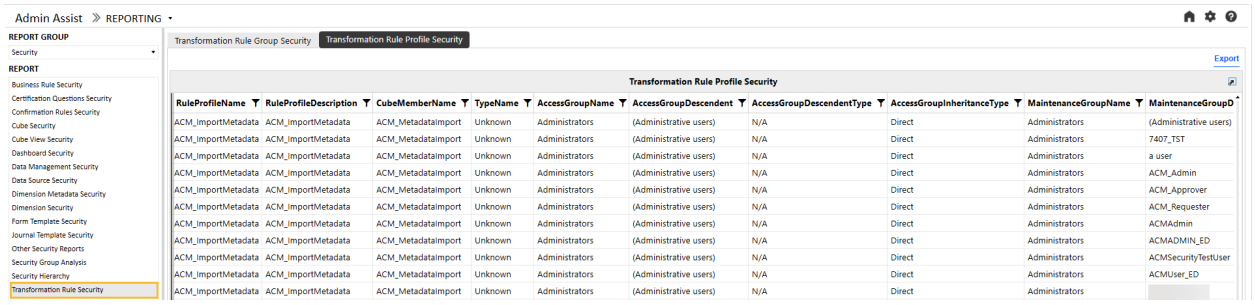
The Transformation Rule Security report shows tabs for transformation rule group security and transformation rule profile security.



These are the columns on the Transformation Rule Group Security report:

Attribute	Description
Cube Dimension Name	Dimension to which the rule group is assigned
Dimension Name	Dimension type (for example, Entity, Account)
Rule Group name	Name of the rule group
Rule Group Description	Description of the rule group (if applicable)
Access Group Name	Members of this group will have access to the transformation rule group
Access Group Descendent Name	For access groups that contain other groups or users, the child group will display here. (Only shown for groups and users detail level)
Access Group Descendent Type	Indicates whether the child is a group or user (only shown for groups and users detail level)
Access Group Inheritance Type	Indicates whether the child is directly assigned or inherits access to the parent
Maintenance Group Name	Members of this group have the authority to maintain the transformation rule group.

The Transformation Rule Profile Security report tab shows a list of transformation rule profiles.



These are the columns on the Transformation Rule Profile Security report:

Attribute	Description
Rule Profile Name	Name of the rule profile
Rule Profile Description	Description of the rule profile (if applicable)
Cube Name	Cube to which the rule profile is assigned
Scenario Type	Scenario Type to which the rule profile is assigned
Access Group Name	Members of this group will have access to the transformation rule profile
Access Group Descendent Name	For access groups that contain other groups or users, the child group will display here. (Only shown for groups and users detail level)
Access Group Descendent Type	Indicates whether the child is a group or user (only shown for groups and users detail level)
Access Group Inheritance Type	Indicates whether the child is directly assigned or inherits access to the parent
Maintenance Group Name	Members of this group have the authority to maintain the transformation rule profile.

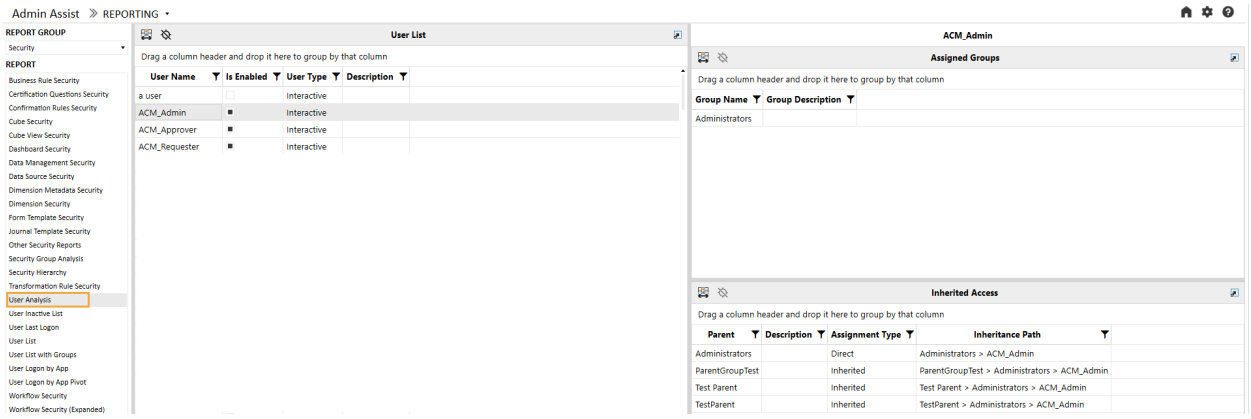
User Analysis

The User Analysis report shows a list of current users in the system and includes the following attributes:

Attribute	Description
Is Enabled	If selected, the user is enabled and can be provisioned in security groups. If clear, the user is not enabled and cannot be provisioned.
User Type	**Interactive**: Allows all functionality. The user type defaults to Interactive for new users and upgrades. **View**: Allows users to view all data, reports, and dashboards in the production environment and the derived database. The View user privileges do not permit the authorized user to load, calculate, consolidate, certify, or change data. **Restricted**: Assigns contractual limits for certain functional tasks, such as limiting rights to solutions, for example, Account Reconciliation or Lease. **Third Party Access**: Allows OneStream access using a named account, logging on interactively using a third-party application. There is no access using the OneStream Windows application or the OneStream Modern Browser Experience. The user cannot change data or modify OneStream application artifacts. **Financial Close**: Allows users to perform Account Reconciliation solutions and Transaction Matching.

More details on a user can be accessed by selecting the user name in the list in the left panel. This will update the reports in the right panel, as shown in the following example:

Select a user name to see additional provisioning details.



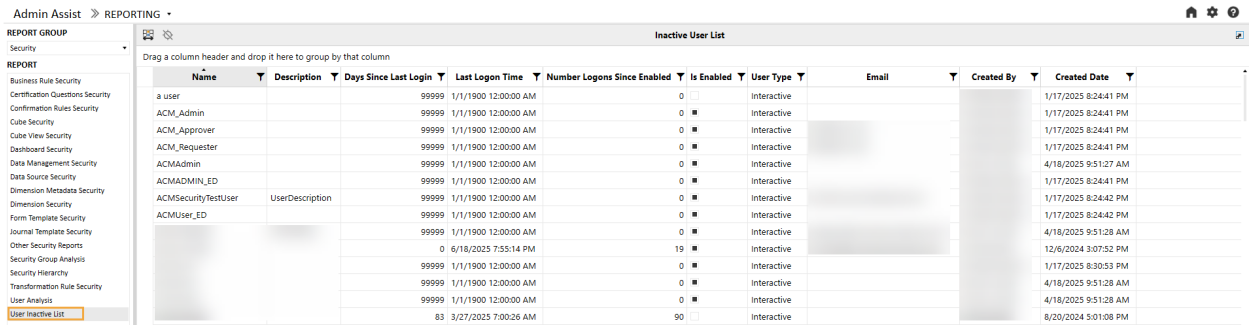
The top panel shows which groups the user has been directly provisioned in. In the previous example, ACM_Admin has been directly assigned to Administrators. This report has columns Group Name and Group Description.

The bottom panel shows which groups the user inherits based on their direct provisioning. In addition to the Parent and Description columns, this report has additional columns:

Attribute	Description
Assignment Type	Direct indicates that the user has been directly provisioned in the group. Inherited indicates that the user receives access to this group indirectly through nested security groups.
Inheritance Path	This column shows how the user received access through an inheritance path. The first group on the left shows the group that the user is directly assigned to (for direct assignments, this will be the only group). Reading the inheritance path to the right will show how groups are nested to ultimately arrive at the top group. In the previous example, ACM_Admin is directly assigned to Administrators, and it inherits access to ParentGroupTest, Test Parent, and TestParent.

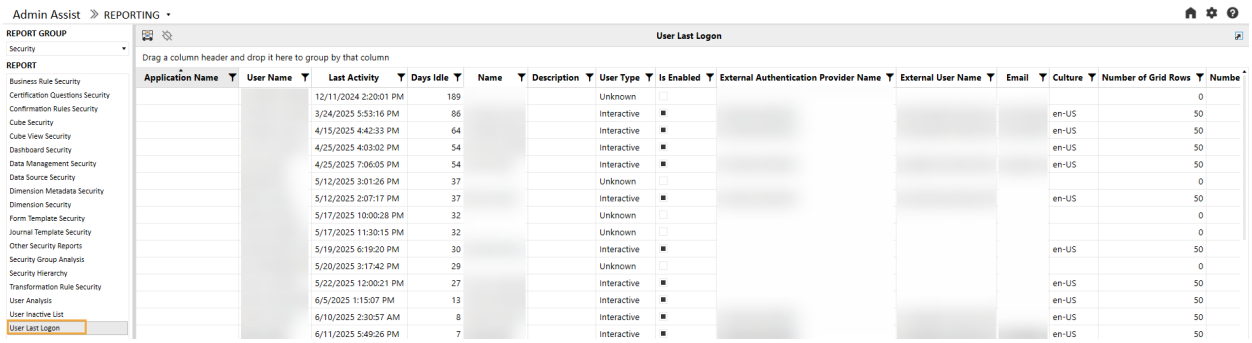
User Inactive List

The User Inactive List shows a list of all users with no login history in the OneStream environment.



User Last Logon

The User Last Logon report shows a list of all users in the OneStream environment and the last time they logged in to the system.



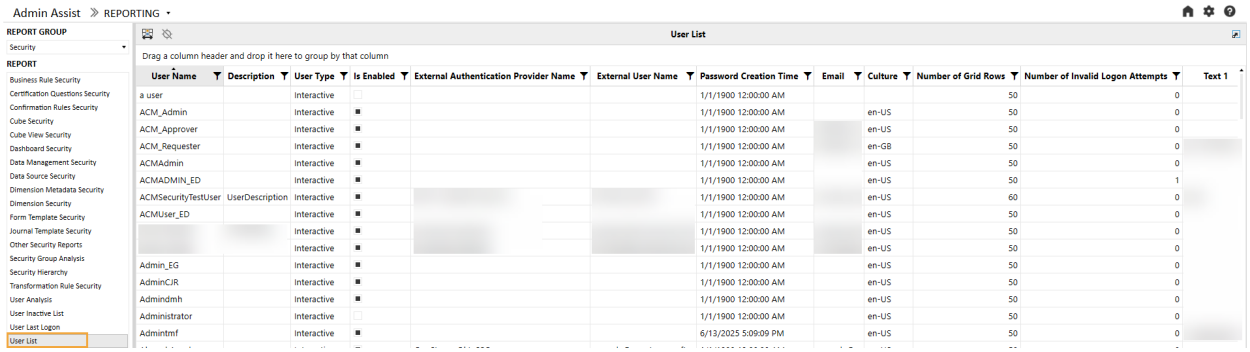
The following additional attributes are available on the report:

Attribute	Description
Application Name	Last application the user logged on to
Last Activity	Time stamp of last activity

Attribute	Description
Days Idle	Calculation of days idle
Name	Name on the audit log (will be blank if the user has been deleted)
Description	User description
User Type	User type (will be Unknown if user has been deleted)
Is Enabled	If the user is enabled within the system or has been deactivated
External Authentication Provider Name	Name of the external authentication provider (for example, Azure AD)
External User Name	User name from the external authentication provider
Email	Email from Preferences section of profile
Culture	Culture from Preferences section of profile
Number of Grid Rows	Grid Rows Per Page under Preferences section of profile
Number of Invalid Logon Attempts	Number of invalid logon attempts by the user
Text 1 – 4	Text fields associated with the user profile

User List

The User List report is a comprehensive list of all users in the system and the attributes associated with their user profile.

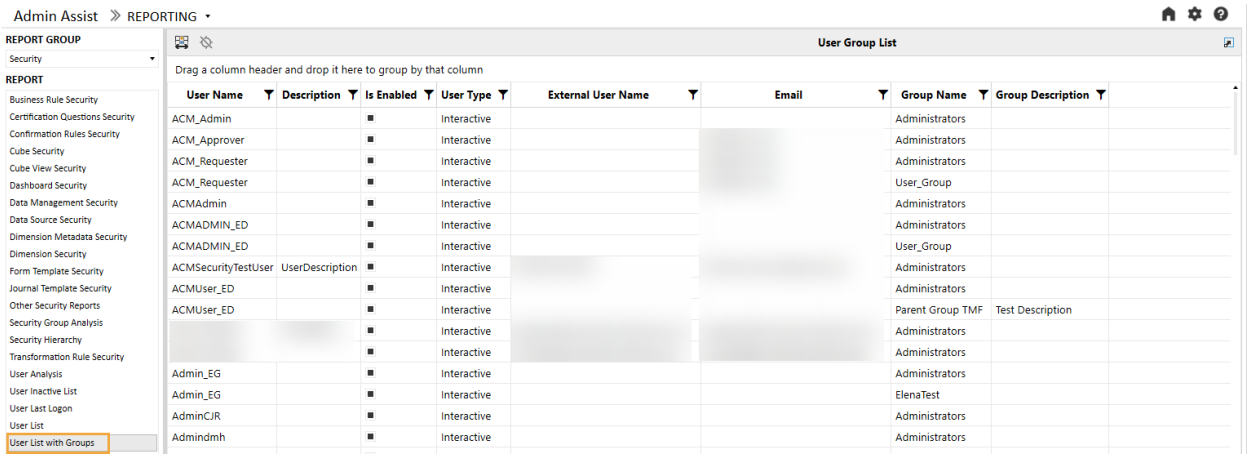


For each user, the following attributes are available in the report.

Attribute	Description
Description	User description
User Type	User type (will be Unknown if user has been deleted)
Is Enabled	If the user is enabled within the system or has been deactivated
External Authentication Provider Name	Name of the external authentication provider (for example, Azure AD)
External User Name	User name from the external authentication provider
Password Creation Time	Password creation time (will be empty if external authentication)
Email	Email from Preferences section of profile
Culture	Culture from Preferences section of profile
Number of Grid Rows	Grid Rows Per Page under Preferences section of profile
Number of Invalid Logon Attempts	Number of invalid logon attempts by the user
Text 1 – 4	Text fields associated with the user profile
User's Groups	Groups that the user is directly assigned to

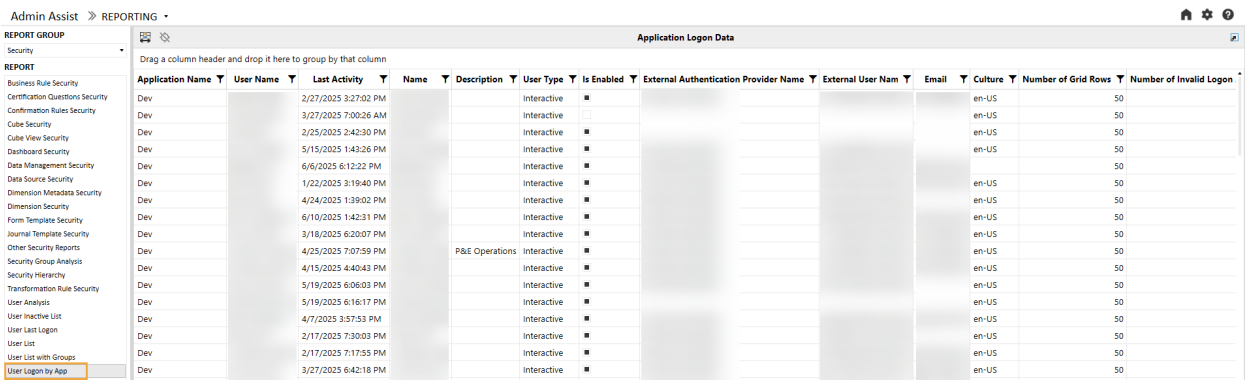
User List by Group

The User List by Group report is identical to the User List report with the addition of Group Name and Group Description fields.



User Logon By App

The User Logon By App report is a detailed list of all applications and the last logon by user. Unlike the User Last Logon report, which lists the last time a user logged on, this report will show the last time a user logged on by application. This may be helpful if multiple applications are used in the environment.



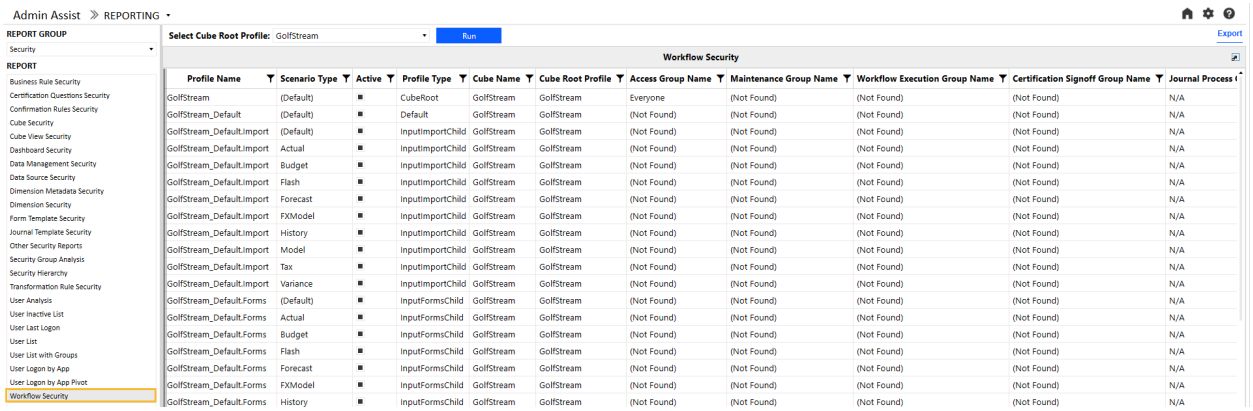
The following additional attributes are available on the report:

Attribute	Description
Application Name	Name of the application the user logged on to
Last Activity	Time stamp of last activity by app
Name	Name on the audit log (will be blank if the user has been deleted)
Description	User description
User Type	User type (will be Unknown if user has been deleted)
Is Enabled	If the user is enabled within the system or has been deactivated
External Authentication Provider Name	Name of the external authentication provider (for example, Azure AD)
External User Name	User name from the external authentication provider
Email	Email from Preferences section of profile
Culture	Culture from Preferences section of profile
Number of Grid Rows	Grid Rows Per Page under Preferences section of profile
Number of Invalid Logon Attempts	Number of invalid logon attempts by the user
Text 1 – 4	Text fields associated with the user profile

Workflow Security

The Workflow Security report shows all security group assignments associated with all workflows and Scenario Types in the OneStream application. Users can also filter the workflows to a specific Cube Root Profile and further filter it to a specific workflow and its dependents. The following example shows this report with a table of the attributes.

NOTE: When the Active flag is false and all groups use the default group settings, the Workflow Profile-Scenario Type combination will not display on the report. However, if a Workflow Profile has any security group assigned, even if it is not active, it will show up on the report.



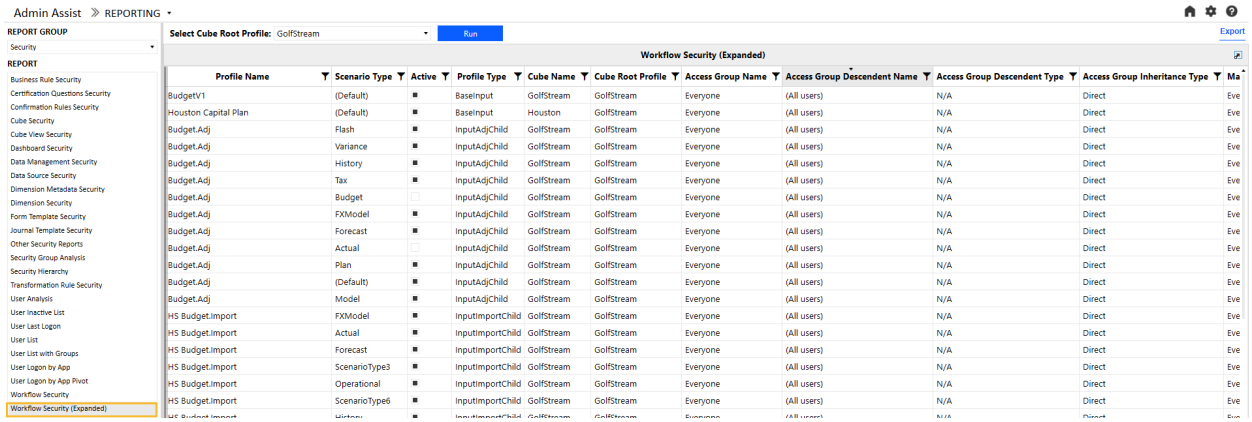
Attribute	Description
Profile Name	Workflow Profile name
Scenario Type	Scenario Type
Active	Indicates if the profile is active or not
Profile Type	Workflow Profile type
Cube Name	Name of the cube associated with the workflow
Access Group Name	Controls the user or users that will have access to the Workflow Profile at runtime to view results
Maintenance Group Name	Controls the user or users that will have access to maintain and administer the Workflow Profile group

Attribute	Description
Workflow Execution Group Name	This group is configured for data loaders and allows users to run the workflow.
Certification Signoff Group Name	This group is configured for certifiers and allows users to sign off on the workflow. This group can be used to separate duties between a data loader and certifier.
Journal Process Group Name	Access to this group allows users to process a journal.
Journal Approval Group Name	Access to this group allows users to approve a journal.
Journal Post Group Name	Access to this group allows users to post a journal.

Workflow Security (Expanded)

The expanded Workflow Security (Expanded) report shows all security group assignments associated with all workflows and Scenario Types in the OneStream application. Users can also filter the workflows to a specific Cube Root Profile and further filter it to a specific workflow and its dependents. The following example shows this report with a table of the attributes.

> **NOTE:** When the Active flag is false and all groups use the default group settings, the Workflow Profile-Scenario Type combination will not display on the report. However, if a Workflow Profile has any security group assigned, even if it is not active, it will show up on the report.



Attribute	Description
Profile Name	Workflow Profile name
Scenario Type	Scenario Type
Active	Indicates whether the profile is active or not
Profile Type	Workflow Profile type
Cube Name	Name of the cube associated with the workflow
Access Group Name	Controls the user or users that will have access to the Workflow Profile at runtime to view results
Access Group Descendent Name	For access groups that contain other groups or users, the child group will display here. (Only shown for groups and users detail level)
Access Group Descendent Type	Indicates whether the child is a group or user (only shown for groups and users detail level)
Access Group Inheritance Type	Indicates whether the child is directly assigned or inherits access to the parent

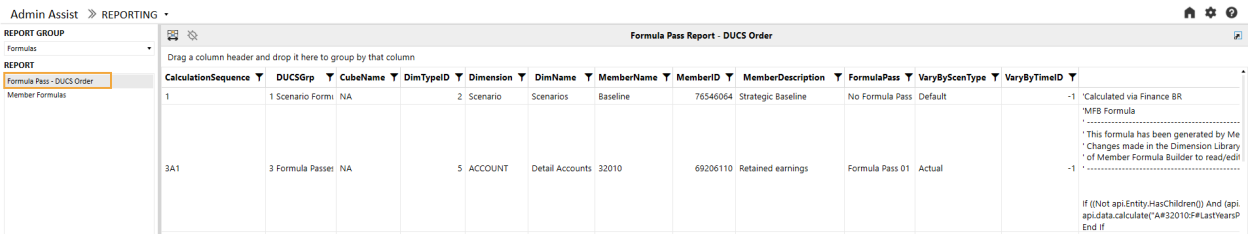
Attribute	Description
Maintenance Group Name	Controls the user or users that will have access to maintain and administer the Workflow Profile group
Workflow Execution Group Name	This group is configured for data loaders and allows users to run the workflow.
Certification Signoff Group Name	This group is configured for certifiers and allows users to sign off on the workflow. This group can be used to separate duties between a data loader and certifier.
Journal Process Group Name	Access to this group allows users to process a journal.
Journal Approval Group Name	Access to this group allows users to approve a journal.
Journal Post Group Name	Access to this group allows users to post a journal.

Formulas Report Set

The Formula reports help to analyze the OneStream member formulas.

Formula Pass – DUCS Order

The Formula Pass – DUCS Order report displays member formulas (excluding dynamic formulas) and cube business rules sorted based on the data unit calculation sequence (DUCS). The report enables you to easily see the order of operations for when certain logic is run.

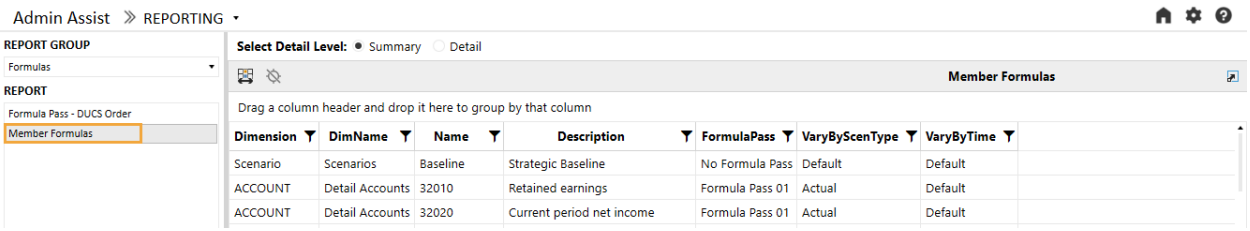


Member Formulas

The Member Formulas report enables you to analyze all Member Formulas by formula pass in one place with the ability to group and filter to assist in troubleshooting Member Formulas. There are Summary and Detail views. The Detail view includes the text value of the Member Formula as well.

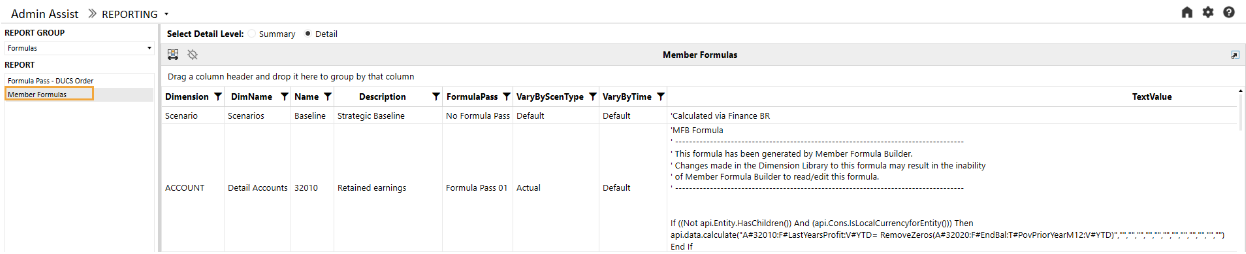
Summary Level

This example shows the data grouped by formula pass and then filtered by dimension name.



Detail Level

This example shows the same data as Summary, grouped by formula pass and then filtered by dimension name, and includes the text value of the Member Formula.

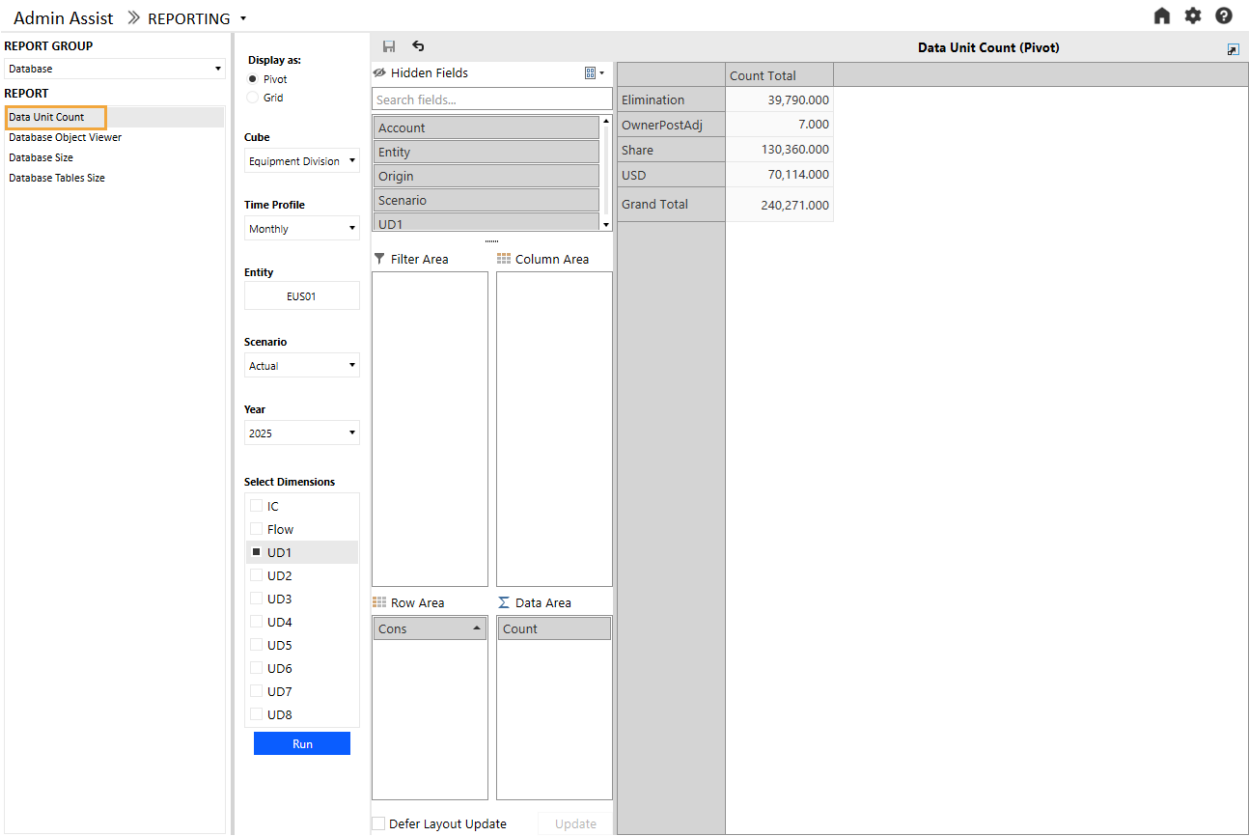


Database Report Set

The Database reports help to analyze the impact of data on an application, including Data Units and Data Volumes, to streamline and fine-tune your application.

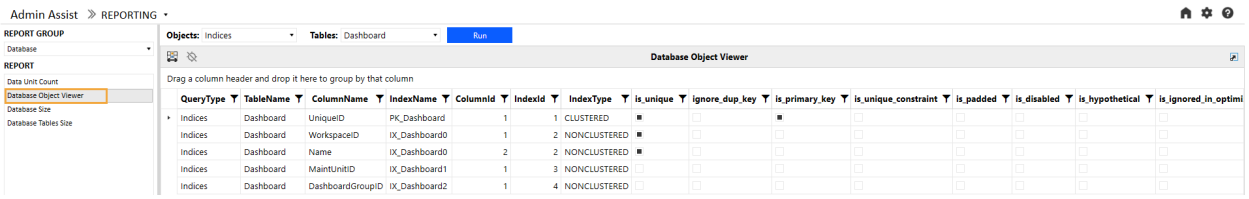
Data Unit Count

Analyze Data Unit records across all dimensions in a grid or pivot table format.



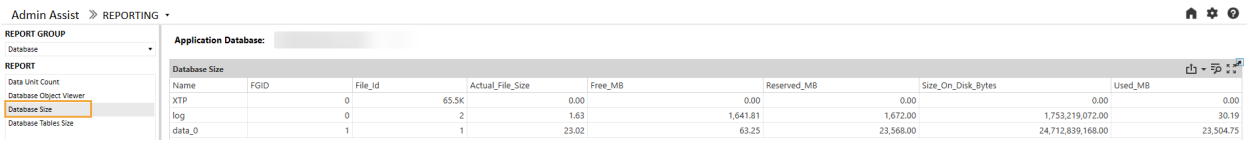
Database Object Viewer

Easily view database objects, such as indices, foreign keys, constraints, and partitions, across all database tables in your OneStream application, including custom tables.



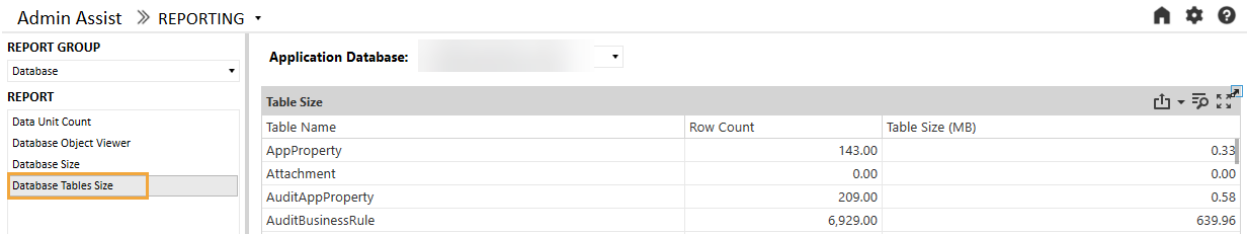
Database Size

Analyze and summarize key database metrics, such as free MB, size on disk bytes, and used MB, for any application in your OneStream environment.



Database Tables Size

Analyze and summarize key database tables metrics, such as row count and table size (MB), across all tables in your application.



Stage Report Set

The Stage reports bring together the Stage data tables to analyze and resolve mapping and data loading issues more efficiently.

Export All Workflows

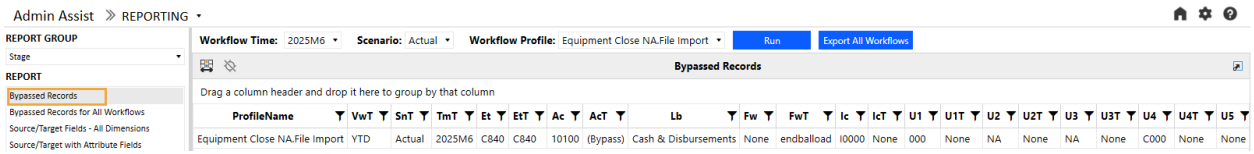
Stage reports that provide an option to select a workflow to filter results have an additional button in the parameters section titled Export All Workflows.

Export All Workflows

This button will export the same data that can be viewed in the report grid in a .csv file and contain data for all available workflows. The export can be run independently of clicking the Run button if all other parameters, besides the workflow, are selected. Once the .csv file is created after clicking the Export All Workflows button, the file will open in the application you have associated with .csv files, typically Excel. Then, you can save the file locally as needed.

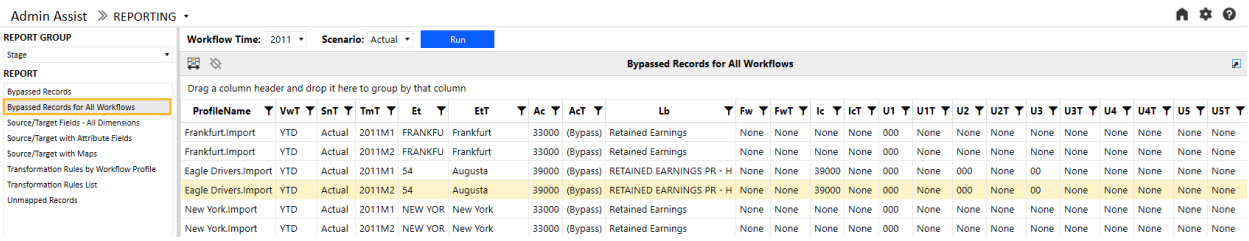
Bypassed Records

View bypassed records for a specific Workflow Time, Scenario, and Workflow Profile.



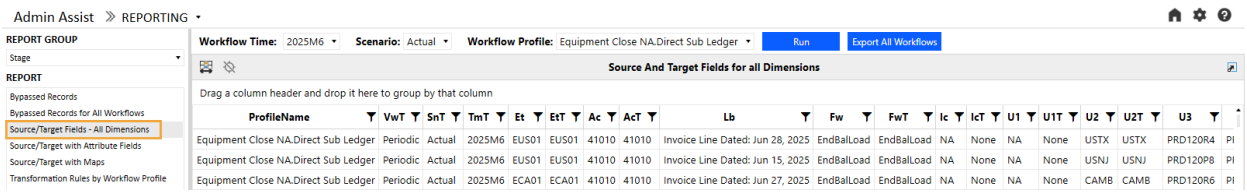
Bypassed Records for All Workflows

View bypassed records for all workflows for a specific times and scenarios.



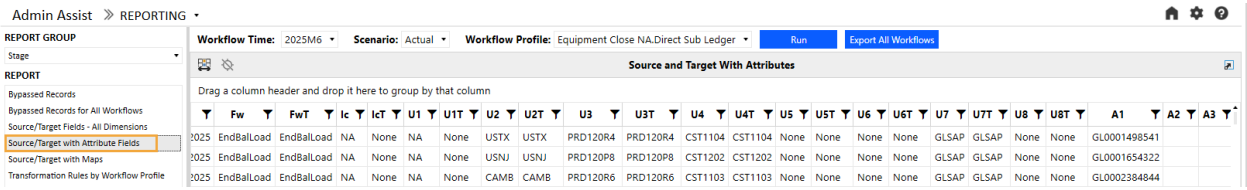
Source/Target Fields - All Dimensions

View source and target fields for all dimensions for a specific Workflow Time, Scenario, and Workflow Profile.



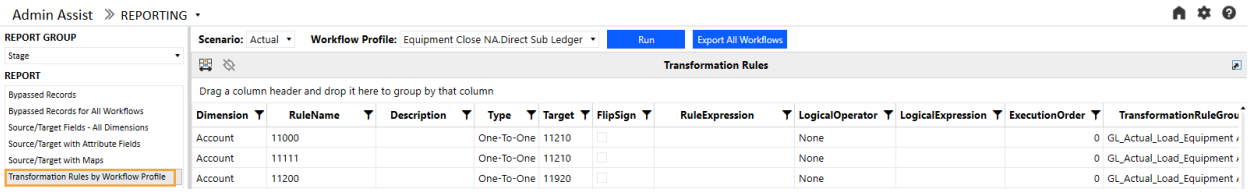
Source/Target with Attribute Fields

View source and target fields with attributes for a specific Workflow Time, Scenario, and Workflow Profile.



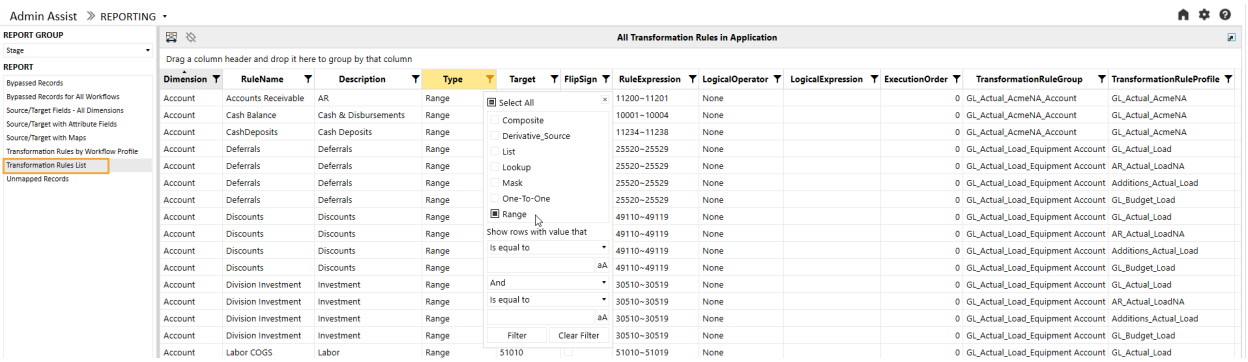
Transformation Rules by Workflow Profile

View all transformation rules for a specific Scenario and Workflow Profile.



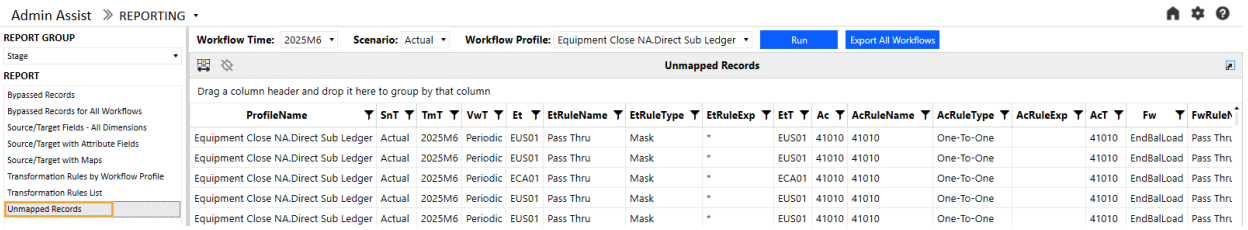
Transformation Rules List

View all transformation rules in one place, and easily group by and filter on any column to resolve mapping issues.



Unmapped Records

View unmapped records for a specific Workflow Time, Scenario, and Workflow Profile.



Journal Entry Report Set

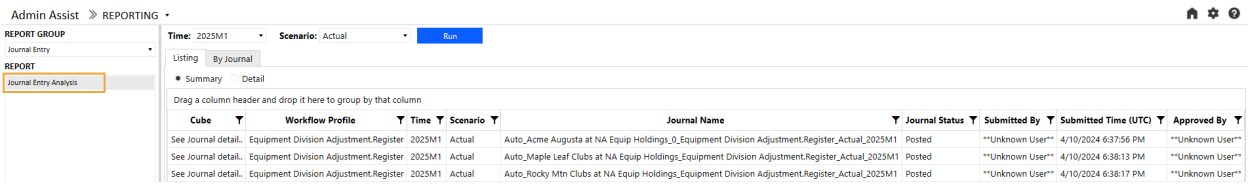
The Journal Entry reports provide summaries and detailed analyses of journal entries across workflows.

Journal Entry Analysis Report

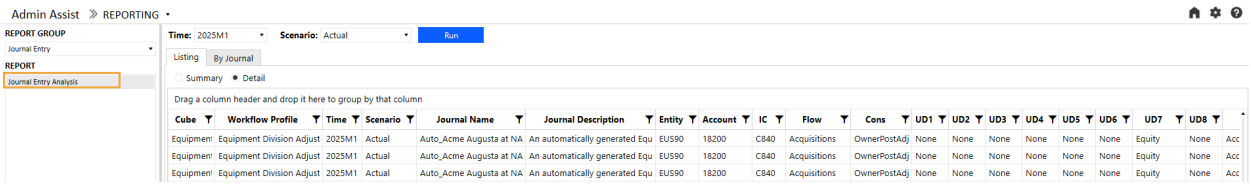
The Journal Entry Analysis report provides journal entries across all workflows in multiple formats for a selected Time and Scenario.

Listing Tab

The Listing tab provides data in a grid format. The default view shows summary data for the journal.

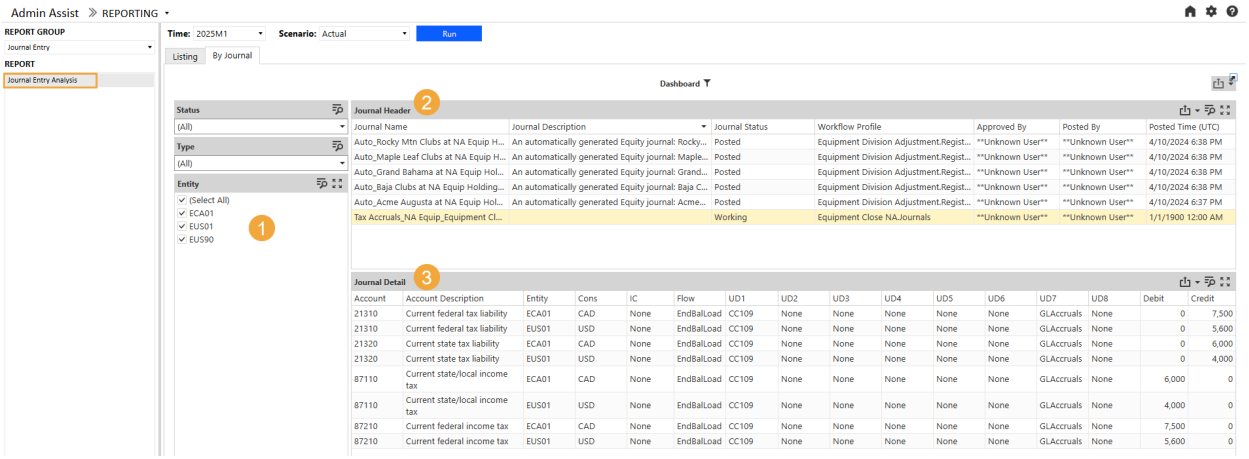


Click the Detail radio button for additional details for the journals, including all dimension data and a complete audit history.



By Journal tab

The By Journal tab provides an interactive way to filter and analyze results by journal.



In the previous example, the selections in the left panel (1) will filter the results in panels 2 and 3. By selecting a single journal in the Journal Header panel (2), the Journal Detail panel (3) will be updated to reflect the selected journal and provide additional details.

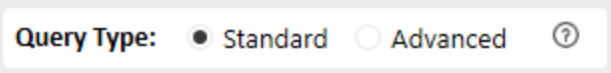
Search

The Search utility is an extremely powerful string searching utility that enables the solution to easily search across all application objects, including Member Formulas, business rules, text attributes, constraints, Cube Views, parameters, and more, to identify all areas that need to be updated when making application changes.

This utility is designed to increase visibility regarding where an item is being used throughout an application. This is most often helpful when renaming a member or item or when substituting one value for another (for example, Forecast for Budget).

Query Types

These are the types of queries that can be performed: Standard and Advanced.



Standard Query

In most instances, the Standard search option will meet the search needs. This option searches for the occurrence of a text string without regard for the case of any of the characters. In addition, it does not except any special or wildcard characters. Performing a Standard search for the text income will yield the same result as an Advanced search using the string %income % and LIKE operator with the case option set to the default of No.

Advanced Query

Advanced search offers additional wildcard capabilities, including the option to escape special characters, as well as control over the case sensitivity of a search. In addition, unlike Standard search, which is fixed to using LIKE operators, Advanced search offers additional operators to use in your query. The following tables include explanations and examples for these additional wildcard characters, operators, and search capabilities. These are some examples of how to use LIKE operators, escape wildcard characters, and the impact of case sensitive searches.

LIKE Operators

Metacharacter	Description	Examples		
		Search Text	Description	Matches
%	The percent sign represents zero, one, or multiple characters. It can be used at the beginning, end, or middle of a pattern.	c%	Matches any value that begins with "c", followed by no or any characters	chart, crate, creation
		%ca%	Matches any value that contains "ca" anywhere within it	cash, seneca, recapture

Metacharacter	Description	Examples		
		Search Text	Description	Matches
_	The underscore represents a single character. It is used to match any single character in a specific position within the pattern.	ca_	Matches any value that starts with "ca" and is followed by any single character	cat, car
		%ca_	Matches any value that begins with no or any characters, followed by "ca" and then any single character	African, bobcat

Metacharacter	Description	Examples		
		Search Text	Description	Matches
[]	Square brackets are used to specify a range of characters to match. For example, "[a-z]" will match any lowercase letter, " [0-9]" will match any digit, and " [abc]" will match "a", "b", or "c".	[c-p]ars[eo]n	Matches any value ending with "arsen" or "arson" and starting with any single character between c and p	Carson, Larson, Karsen
		[a-c]%	Matches any value that starts with "a", "b", or "c"	Argentina, Brazil, Canada

Metacharacter	Description	Examples		
		Search Text	Description	Matches
^	A caret (^) character within square brackets ([]) can be used to negate a range. For example, "[^0-9]" will match any character that is not a digit.	[^a-c]%	Matches any value that does not start with "a", "b", or "c" and is followed by no or any characters	Denmark, Egypt, France
		%[^1-3]	Matches any value that begins with no or any characters, followed by a character that is not "1", "2", or "3"	product4

Case Sensitive Search

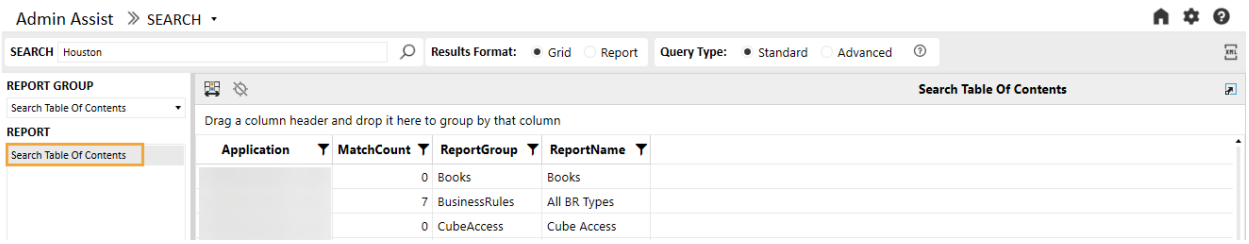
Description	Examples		
	Search Text	Description	Matches
By default, SQL Server performs case-insensitive searches. However, if you want to perform a case-sensitive search in SQL Server, select this option.	c%	Matches any value that begins a lowercase "c" followed by no or any characters	chart, crate, creation

Escaping Wildcard Characters

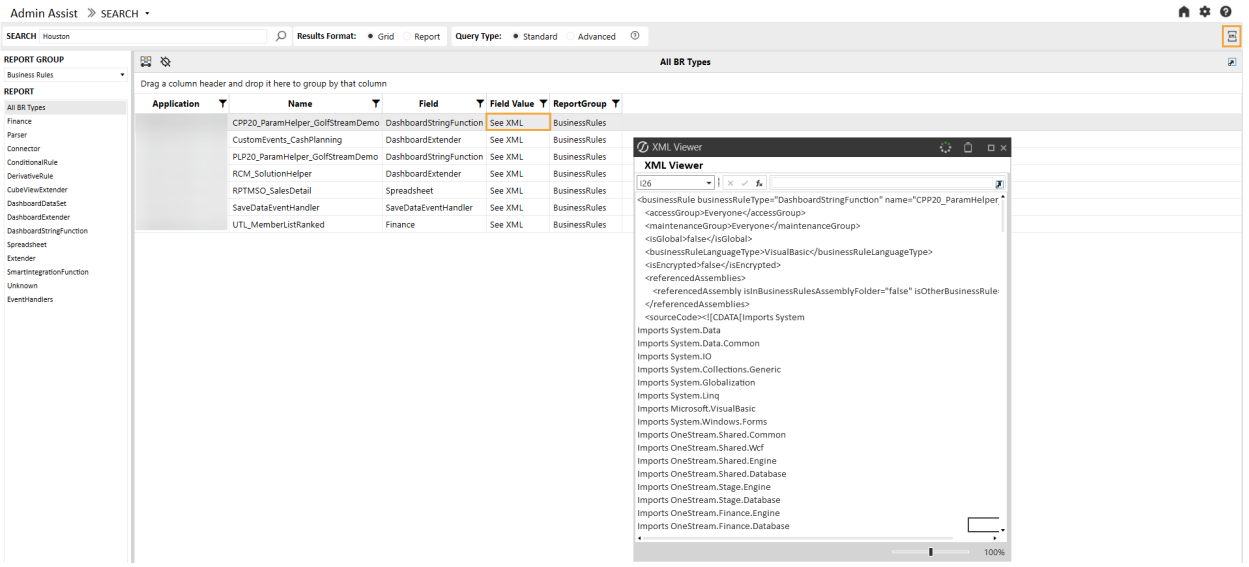
Metacharacter	Description	Examples		
		Search Text	Description	Matches
/	Use brackets custom defined character to treat the wildcard characters as the regular characters.	%ca/%	Matches any value that ends with "ca %"	Africa%

Search Table of Contents

This is a high-level search to identify the main areas where the string was found.



Find the exact object by digging further into each application object report group and even see the XML of the object, if applicable.



Search Report Groups

- Cube Access
- Metadata
- Workflows
- Cube Views
- Forms
- Journals
- Dashboards
- Business Rules
- Data Management
- Books
- Files
- System

Utilities

See the following sections for detailed information about each Metadata Utility.

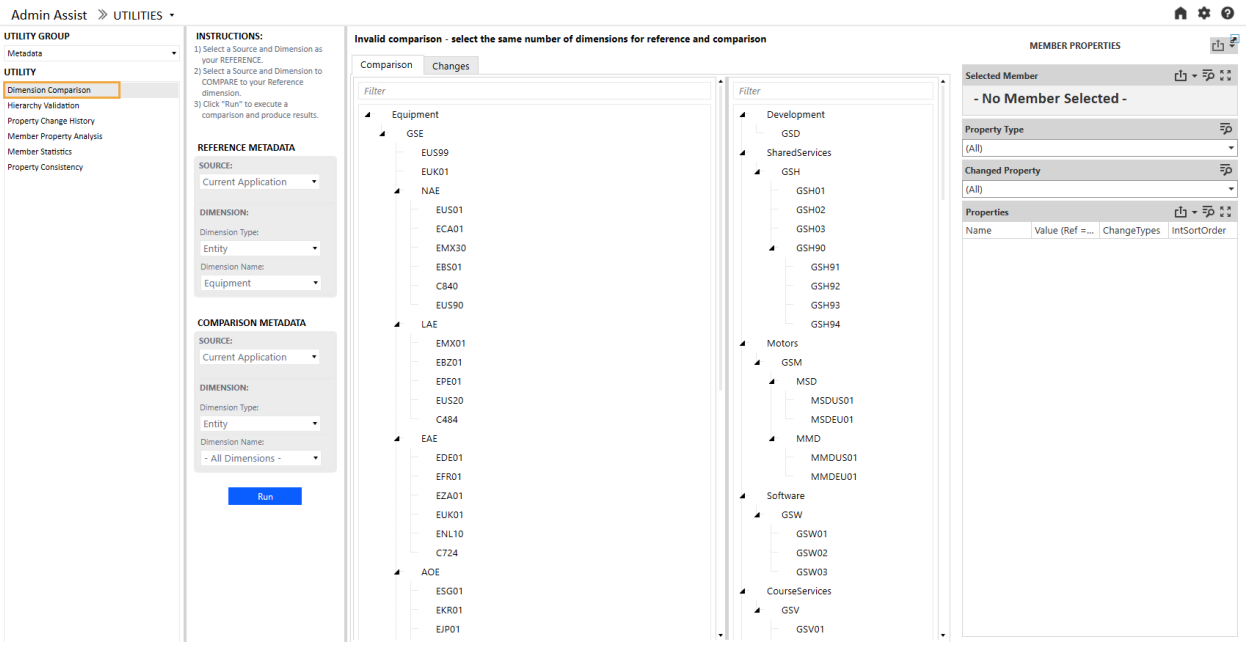
- Dimension Comparison
- Hierarchy Validation
- Property Change History
- Member Property Analysis
- Member Statistics
- Property Consistency

Metadata Utilities

The Metadata Utility provides several utilities to compare, validate, analyze, and generate statistics for metadata members.

Dimension Comparison

The Dimension Comparison utility enables a user to compare metadata of similar dimension type or types from different sources and obtain a detailed list of changes between the reference and comparison metadata sets. A metadata source can be an entire application metadata set or a single dimension.



Metadata Sources

There are three metadata sources that can be used.

Current Application

The current application refers to the currently logged in application. Any metadata from this application can be selected with this option.

XML File

An .xml file can also be used as a metadata source. This is useful, for example, when you want to compare metadata from archived metadata or from an application that resides outside the environment in which OneStream Admin Assist is installed.

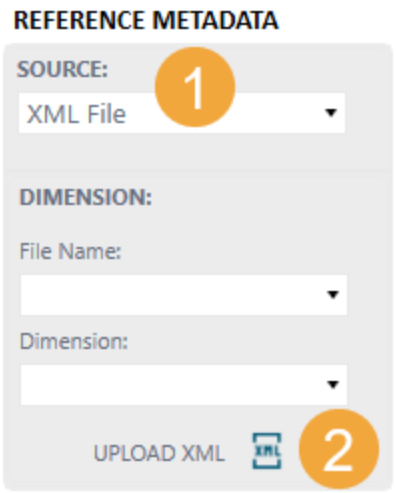
Other Application

In addition, metadata can be used from any application residing within the environment in which OneStream Admin Assist is installed.

Uploading an XML File

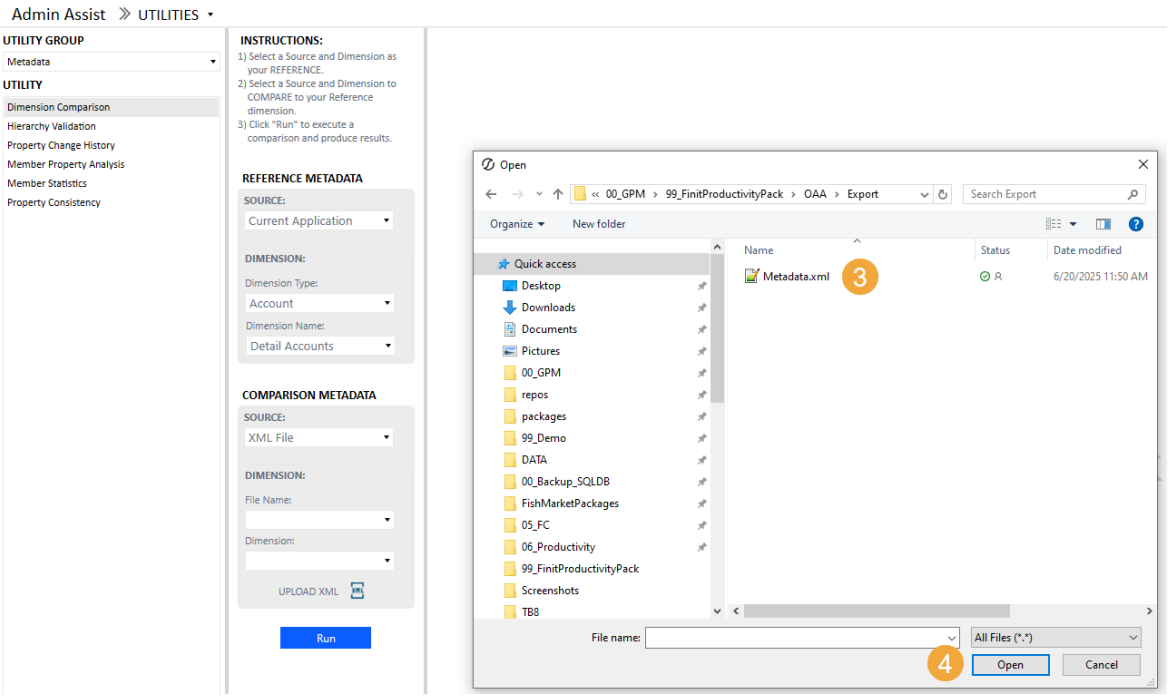
To upload a metadata .xml file:

1. In either the Reference or Comparison section (1), in the **SOURCE** drop-down menu, select **XML File**.

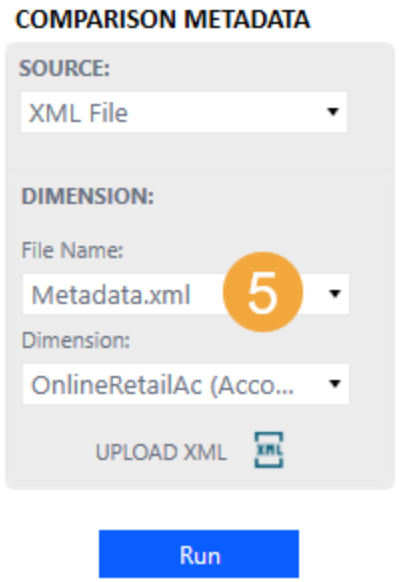


2. Click the **UPLOAD XML** button (2).
3. A Windows Explorer dialog box will display. Select a metadata file in .xml format (3).

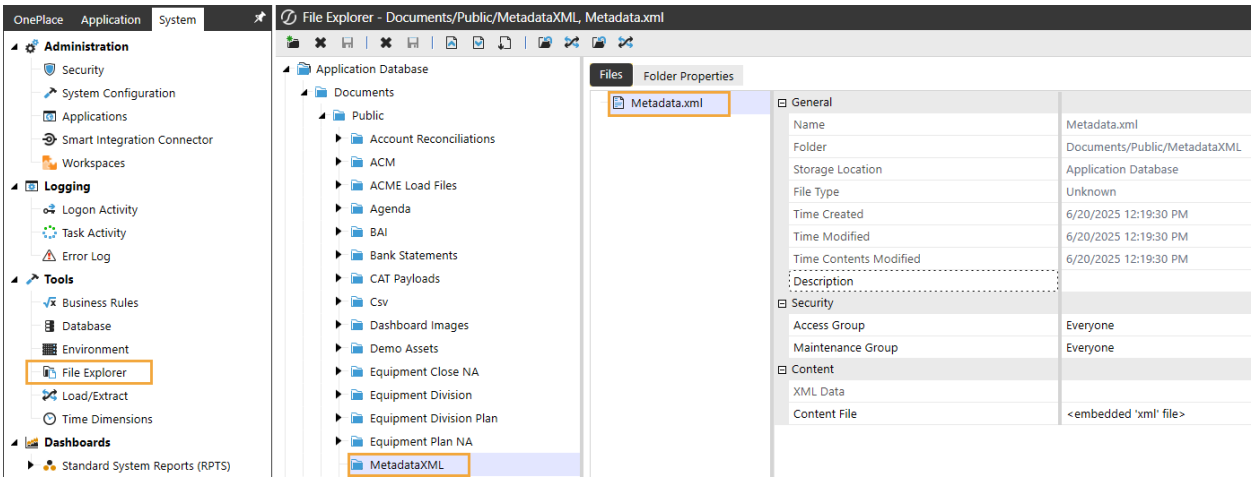
4. Click the **Open** button (4).



5. After the file has completed loading in OneStream, the **File Name** drop-down menu will populate with the file (5), and you are ready to use the metadata in the utility.



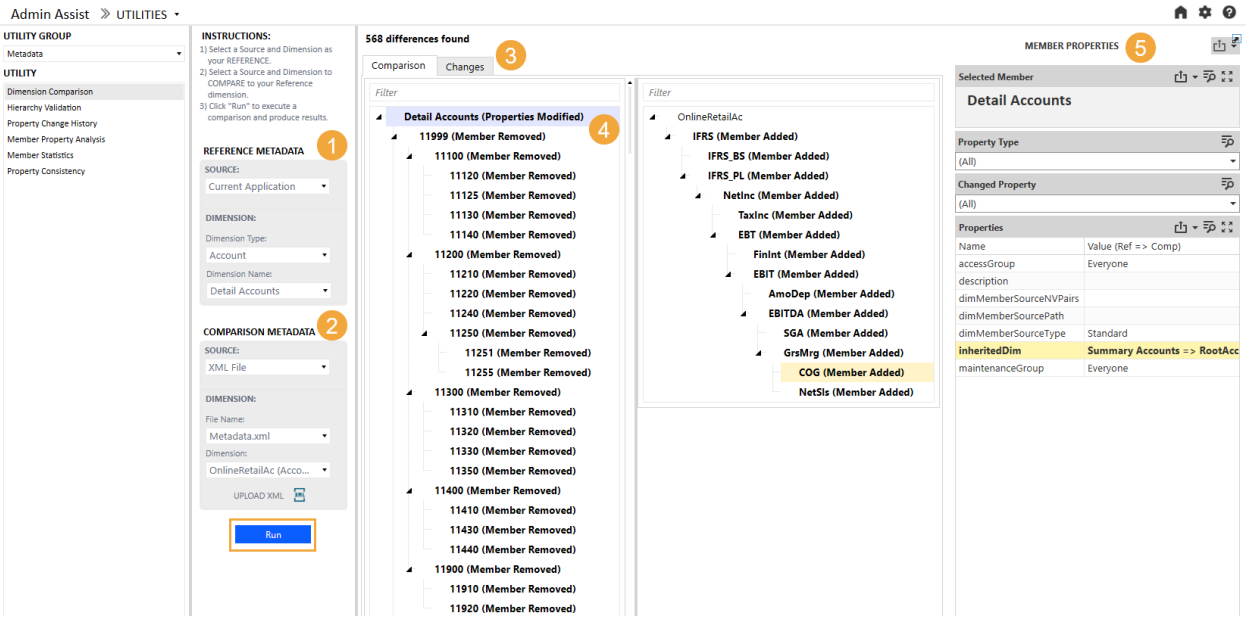
All files uploaded are stored in the Documents/Public/MetadataXML folder. Files can alternatively be uploaded directly to this folder, and they will be accessible by the utility.



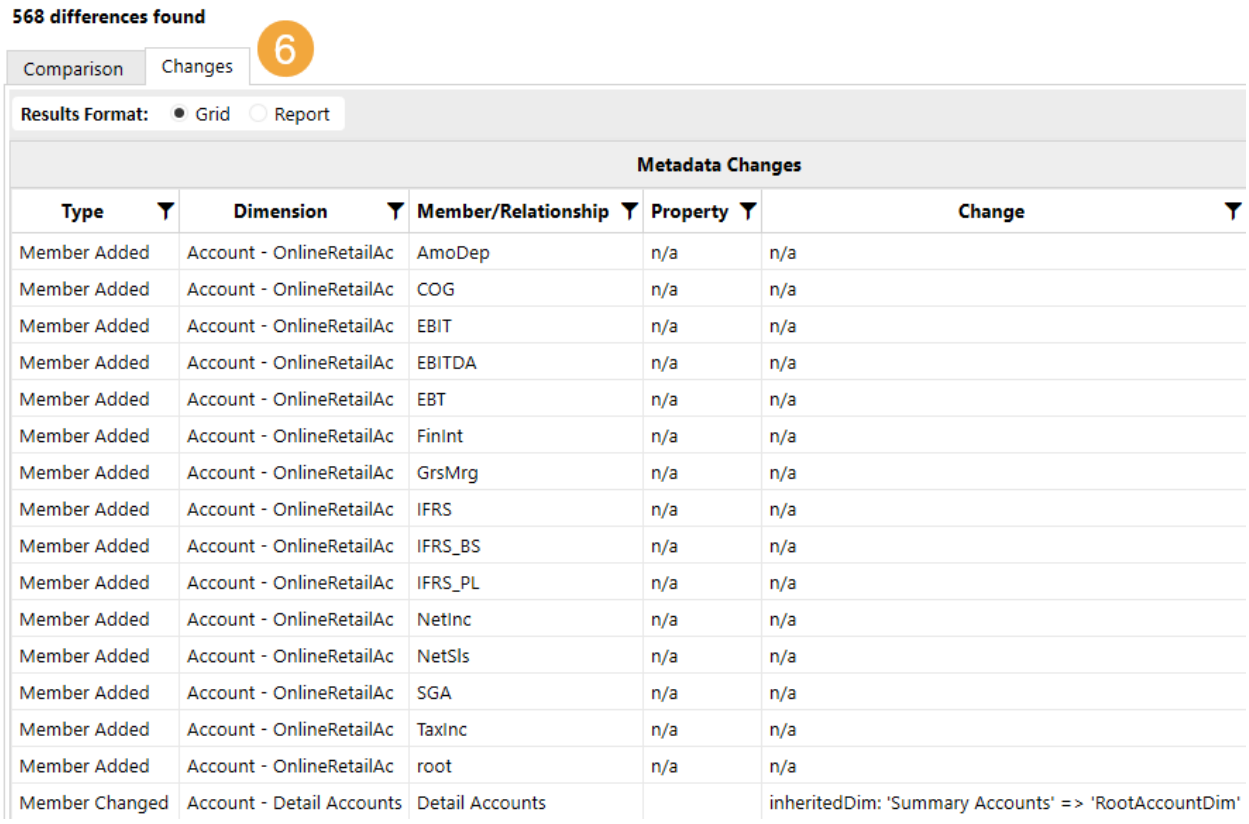
Comparison Results

To create a Dimension Comparison:

1. In **REFERENCE METADATA** (1), fill in the parameters.
2. In **COMPARISON METADATA** (2), fill in the parameters.
3. Click the **Run** button. A dialog box will display indicating the progress of your request and then a screen like the following example will display.
4. These are the result views (3): Comparison and Changes. The default is Comparison. In the Comparison view, a tree view of the reference metadata will display on the left, and a tree view of the reference metadata will display on right with member changes in bold (4). You can select any of the bold members to view details of the change on the right (5).



The Changes view displays in a Grid or Report format (6) the details of the all the noted changes in the metadata.



568 differences found

Comparison | Changes 6

Results Format: Grid Report

Metadata Changes

Type	Dimension	Member/Relationship	Property	Change
Member Added	Account - OnlineRetailAc	AmoDep	n/a	n/a
Member Added	Account - OnlineRetailAc	COG	n/a	n/a
Member Added	Account - OnlineRetailAc	EBIT	n/a	n/a
Member Added	Account - OnlineRetailAc	EBITDA	n/a	n/a
Member Added	Account - OnlineRetailAc	EBT	n/a	n/a
Member Added	Account - OnlineRetailAc	FinInt	n/a	n/a
Member Added	Account - OnlineRetailAc	GrsMrg	n/a	n/a
Member Added	Account - OnlineRetailAc	IFRS	n/a	n/a
Member Added	Account - OnlineRetailAc	IFRS_BS	n/a	n/a
Member Added	Account - OnlineRetailAc	IFRS_PL	n/a	n/a
Member Added	Account - OnlineRetailAc	NetInc	n/a	n/a
Member Added	Account - OnlineRetailAc	NetSls	n/a	n/a
Member Added	Account - OnlineRetailAc	SGA	n/a	n/a
Member Added	Account - OnlineRetailAc	TaxInc	n/a	n/a
Member Added	Account - OnlineRetailAc	root	n/a	n/a
Member Changed	Account - Detail Accounts	Detail Accounts		inheritedDim: 'Summary Accounts' => 'RootAccountDim'

Difference Types

These are the Dimension Comparison changes categories. The following list includes the attributes and an example description of the change using an Entity dimension member.

Attribute	Example Change
Member Changed	Description changed for a particular member from Corporate to Total Consolidate
Member Added	• Added new base Entity within the dimension • The change that would display under EastPA when Philadelphia is moved there from SouthPA

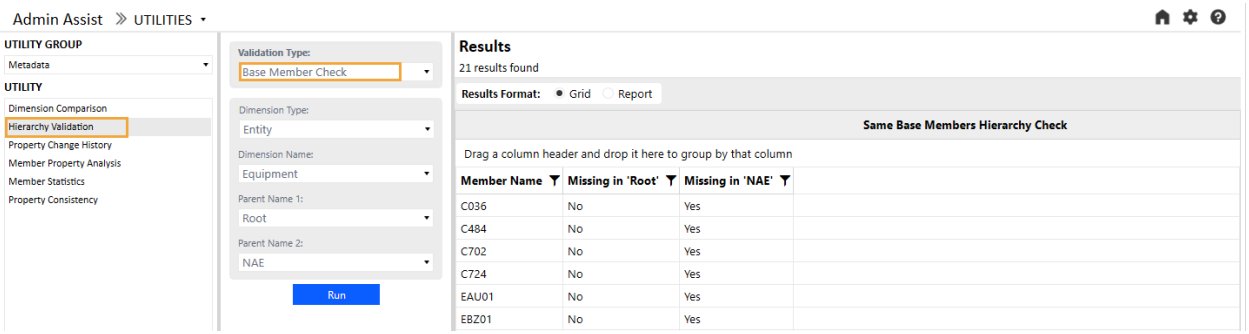
Attribute	Example Change
Member Removed	• Deleted a base Entity within the dimension ◦ The change that would display under SouthPA when Philadelphia is moved from there to EastPA
Member Property Added	Added the string CashFlow to the Text1 Member Properties field of the Corporate base Entity member for the default Scenario Type and Time
Member Property Removed	Deleted the string Active from the Text2 Member Property field of the WestCoast base Entity member for the default Scenario Type and Time
Relationship Changed	Changed the Percent Consolidation field for an Entity member from 100 to 90
Relationship Added	Member Philadelphia added to AltEastPA as a shared member
Relationship Removed	Member Philadelphia removed from AltSouthPA
Relationship Property Added	Added the string Sold to the Text7 Relationship Properties field of the Corporate base Entity member for the default Scenario Type and Time
Relationship Property Removed	Deleted the string Sold to the Text7 Relationship Properties field of the Corporate base Entity member for the default Scenario Type and Time

Hierarchy Validation

The Hierarchy Validation can be used to perform certain metadata validations and can be viewed in a grid or report format.

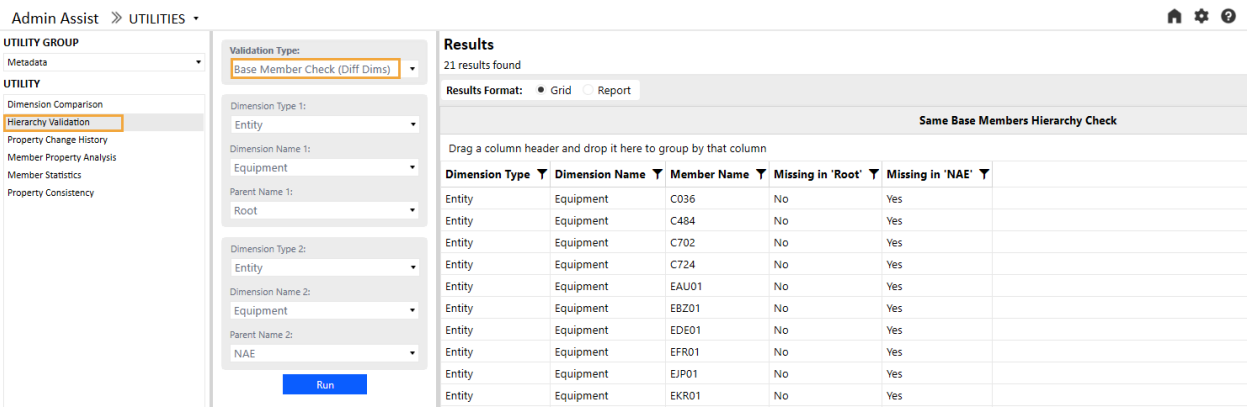
Base Member Check

The Base Member Check type checks the agreement of base entities between two different parents within a selected dimension. An entire dimension can be evaluated by selecting the root parent. If the base members are not identical, the same between the two parents selected, the exceptions are identified along with noting the parent from which they are missing.



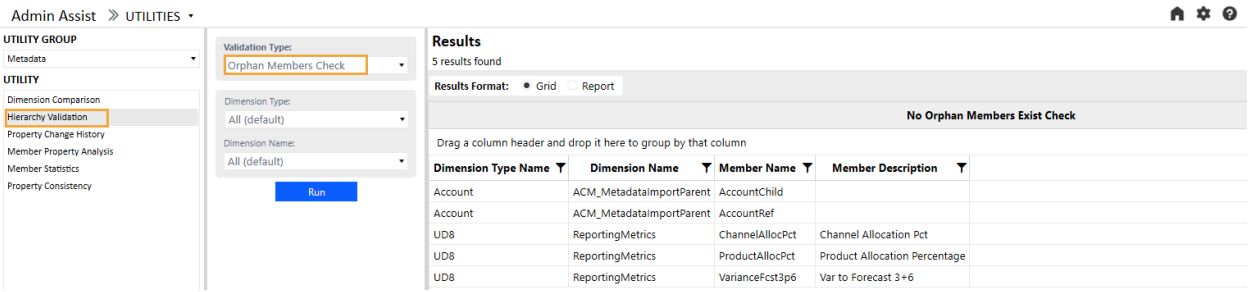
Base Member Check (Diff Dims)

The Base Member Check (Diff Dims) is the same as the Base Member Check type except that the parents do not need to be within the same dimension, so there is an additional drop-down menu to select the dimension name for each parent.



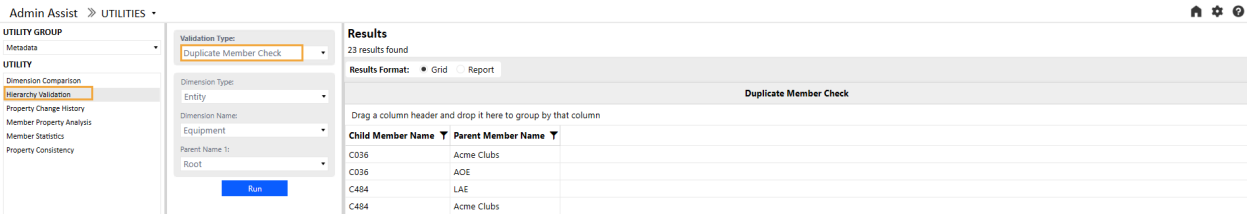
Orphan Members Check

The Orphan Members Check type identifies any members that are not part of a dimension hierarchy (that is, orphan member). The report can be run for a particular dimension, all dimensions, a dimension type, or all dimensions across all dimension types.



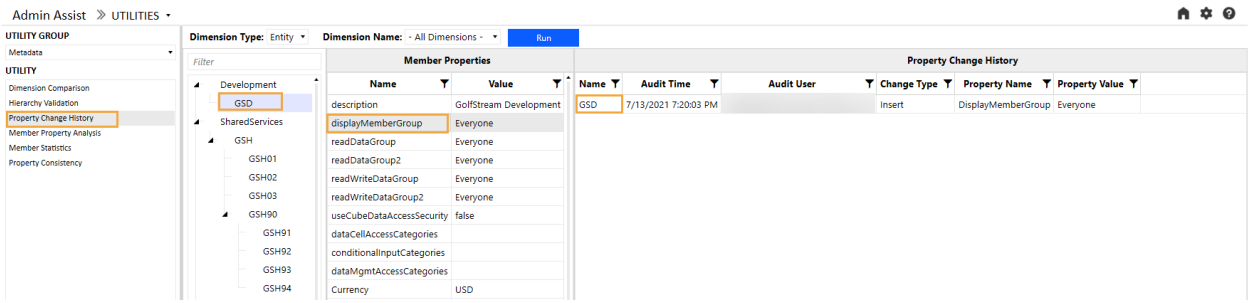
Duplicate Member Check

The Duplicate Member Check type identifies any duplicate members under a particular dimension and lists its name and the name of its parent in a grid or report format.



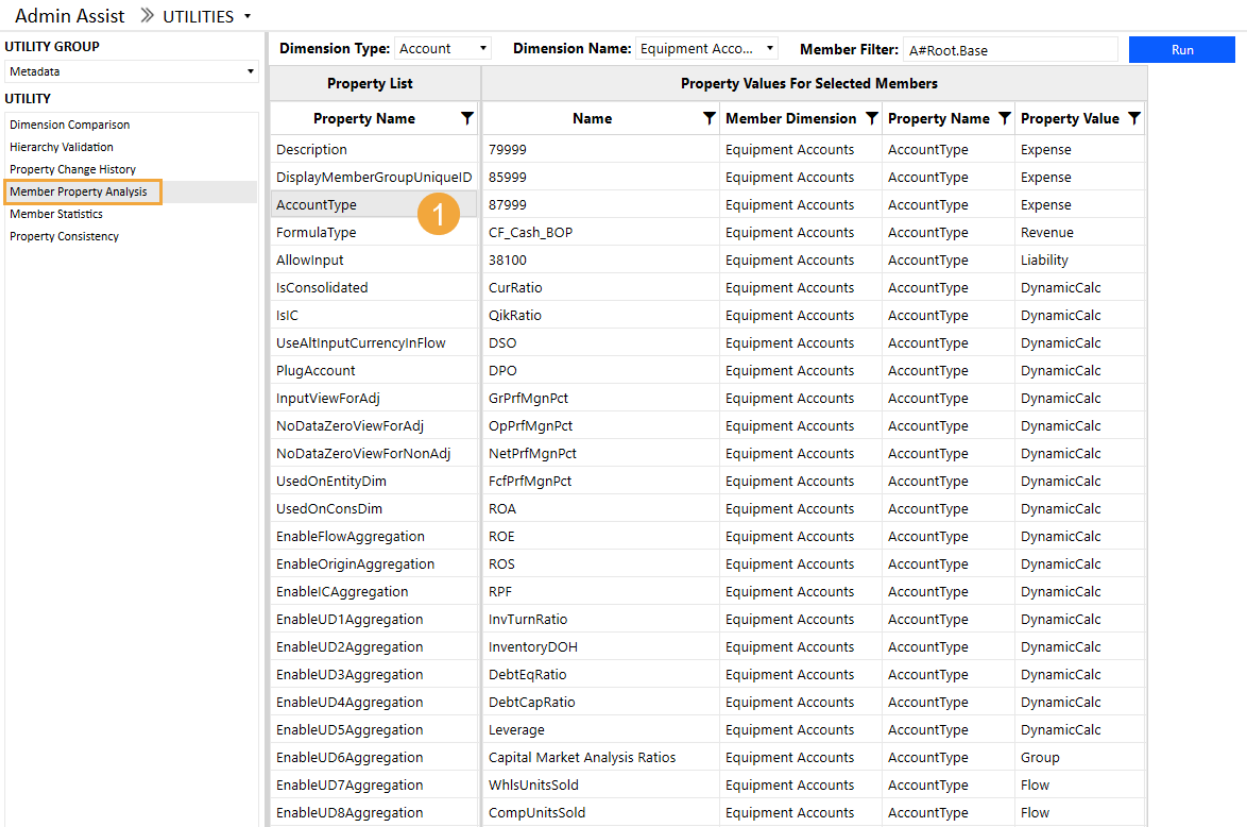
Property Change History

The Property Change History report can be used to view the change history quickly and easily for a particular metadata member and property. Select a dimension, hierarchy member, and property to view details of all changes to that member and property in the OneStream Audit tables.



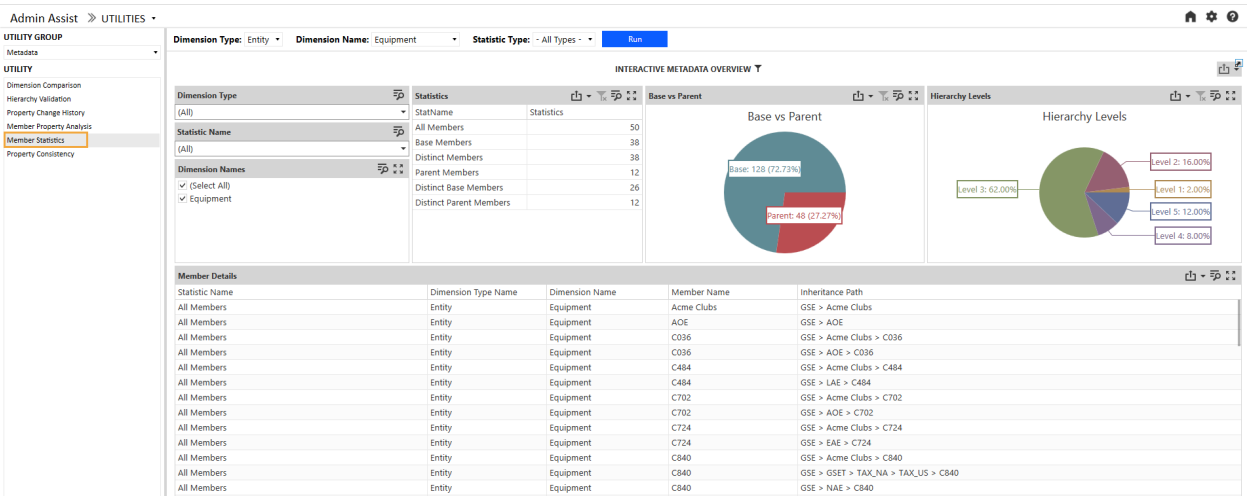
Member Property Analysis

The Member Property Analysis report can be used to quickly navigate property values for multiple members. Make the necessary parameter selections and then click the Run button. All available properties will be listed under Property List. Select a property (1) to view that property value for all the members that meet the parameter criteria.



Member Statistics

The Member Statistics report displays, in a user-friendly dashboard format, statistics for all application dimensions and members or subset. Select a Dimension Type, Dimension Name, and Statistic Type, and click the Run button.

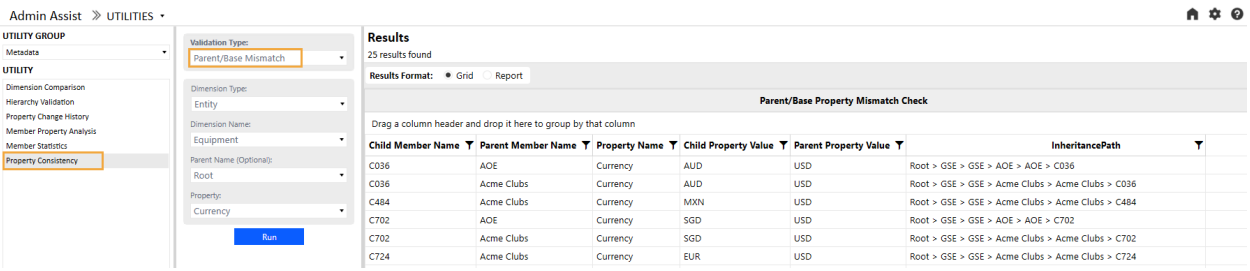


Property Consistency

The Property Consistency report can be used to perform certain metadata property validations and searches in both grid and report format. These checks and searches include the following types.

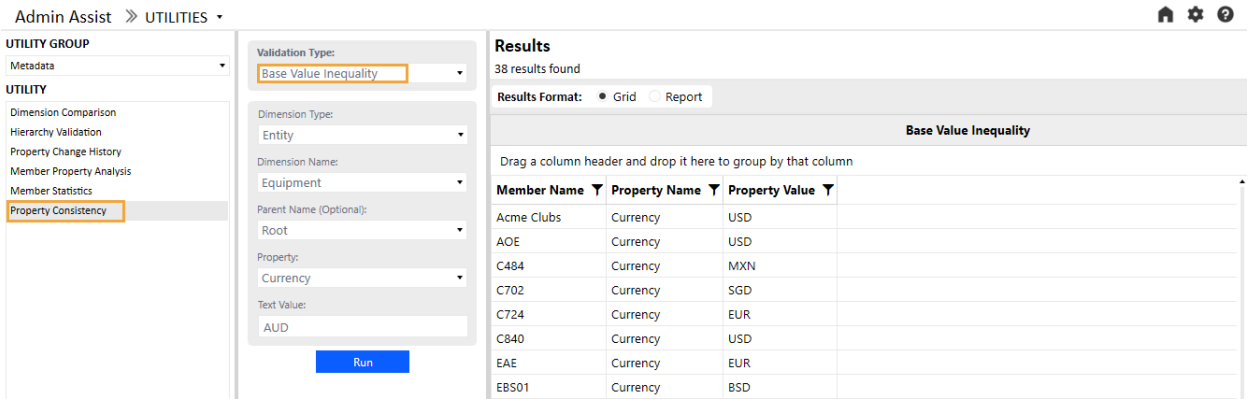
Parent/Base Mismatch

The Parent/Base Mismatch validation can be used to check the alignment of a particular property between a parent member and its children. In the following example, the report identifies any base member of the parent whose currency does not match that of the parent. If the parent is selected, all parent-child relationships within the hierarchy are evaluated.



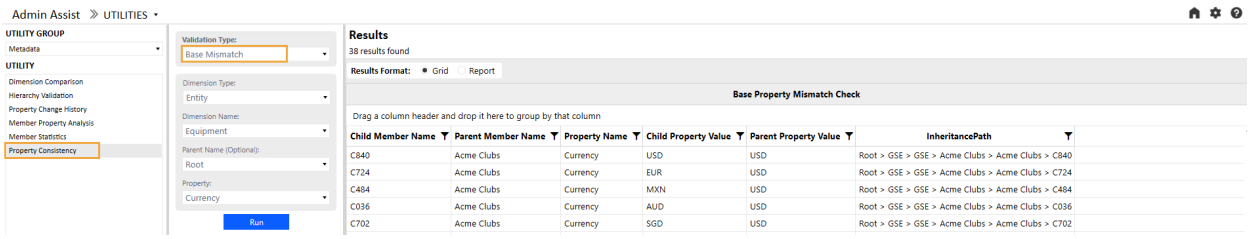
Base Value Inequality

Th Base Value Inequality validation can be used to check if the base members of a particular parent equal a provided value. In the following example, the report identifies any base member of the parent Root that does not have a currency of AUD.



Base Mismatch

The Base Mismatch validation can be used to check the alignment of a particular property between base members of a selected parent. In the following example, the report identifies any base member of the parent whose Currency value does not match that of all other base members.



Help and Miscellaneous Information

This page contains solution documentation.

See the following sections for additional information.

- OneStream Display Settings
- Solution Modification Considerations

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: `OAA_PV9.0.0_SV100_PackageContents.zip`

Identifier	Description
BAI	Solution ID
PV9.0.0	Minimum Platform version required to run solution
SV100	Solution version

Identifier	Description
PackageContents	File name

OneStream Display Settings

OneStream solutions frequently require displaying 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.

Solution Modification Considerations

It is not recommended to rename or modify the included dashboards, components, business rules, etc. unless specified and adequately documented in the implementation documentation for a solution project for future reference when upgrading solutions.

A few cautions and disclaimers when modifying a solution:

- Significant changes to business rules or custom tables within a 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 first. This is important because if there is an upgrade to the solution in the future and the customer applies the upgrade, this will overlay and wipe out the changes. This also applies when updating any of the standard reports and dashboards.

- If modifications are made to a solution, upgrading to later versions will be more complex, depending on the degree of customization. Simple changes, such as changing a logo or colors on a dashboard, have a relatively minor impact on upgrades. Changing any custom database tables or business rules should be avoided and will make an upgrade even more complicated.

Package Contents and Naming Conventions

The package file name contains multiple identifiers that correspond with the platform. Renaming any elements included in the package is discouraged to preserve the naming conventions and solution integrity.

> **Example:** OAA_PV9.0.0_SV100_PackageContents.zip

Identifier	Description
OAA	Solution ID
PV9.0.0	Minimum Platform version required to run solution
SV100	Solution version
PackageContents	File name