Toolkit

Advanced Admin Toolkit Guide

PV730 SV100

Finit

Copyright © 2023 The Finit Group LLC DBA Finit. All rights reserved.

Any warranty with respect to the software or its functionality will be expressly given in the Subscription License Agreement or Software License and Services Agreement between Finit and the warrantee. This document does not itself constitute a representation or warranty with respect to the software or any related matter.

Contents

Solution Overview 3
Installation & Initial Setup 4
Dependencies 4
Solution Development Location 4
Installation 4
Initial Setup 6
Settings & Configuration 8
Admin Page 8
Search Settings 9
Reporting Settings 9
Administration Tasks 11
Upgrading 11
Home Page 11
Reporting 12
Security Report Set 12
Metadata Report Set 36
Database Report Set 37
Stage Report Set 39
Utilities 41
Search 41
Help and Miscellaneous Information 43
Troubleshooting & FAQs 43
OneStream Display Settings 43
Solution Modification Considerations 43

Solution Overview

ToolkIt empowers OneStream administrators to more efficiently support their users by providing a centralized access point to analyze security, metadata, and performance data.

Finit's collection of utilities and reports provides OneStream administrators and power users with the ability to save time and perform tasks more efficiently. Based on the tools that made Finit the leading implementer of OneStream software, empower your team so they have more time to improve and enhance your OneStream investment.

With ToolkIt, you can:

- Visualize and Analyze 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 more efficiently analyze and resolve mapping and data loading issues
    - Bypassed Records
    - Constraint Violations
    - All Transformation Rules in Application
    - Source/Target Field All Dimensions
    - Unmapped Records
    - Source/Target with Attribute Fields
    - Source/Target with Maps
- Analyze all member formulas by formula pass
- Easily Search across all application objects to identify all areas that needed updated when making application changes
- Install and start realizing the benefits in minutes.

Installation & Initial Setup

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

Dependencies

Component	Description
OneStream 7.3.0 or later	Minimum OneStream Platform version required to install this version of the solution

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 not advised.

Note: Finit strongly recommends 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 into OneStream.
2. On the **Application** tab, click **Tools > Load/Extract**.
3. On the **Load** tab, locate the solution package using the **Select File** icon and click **Open**.
4. When the solutions file name appears, click **Load**.
5. Click **Close** to complete the installation.

Package Contents

Finit Toolkit (FFTK) is the main solution dashboard.

BUSINESS RULES

The following Business Rules are included:

- FDBA_HelperQueries
- FDBA_SolutionHelper
- FDBA_ParamHelper
- FFTK_HelperQueries
- FFTK_SolutionHelper
- FFTK_ParamHelper
- FFTK_GlobalRoutines
- FFTK_Licensing
- FFTK_Setup
- FMRP_HelperQueries
- FREP_HelperQueries
- FREP_SolutionHelper
- FREP_ParamHelper
- FSRP_HelperQueries
- FSRP_SolutionHelper
- FSSU_HelperQueries
- FSSU_SolutionHelper
- FSSU_ParamHelper
- FSTG_HelperQueries
- FSTG_ParamHelper

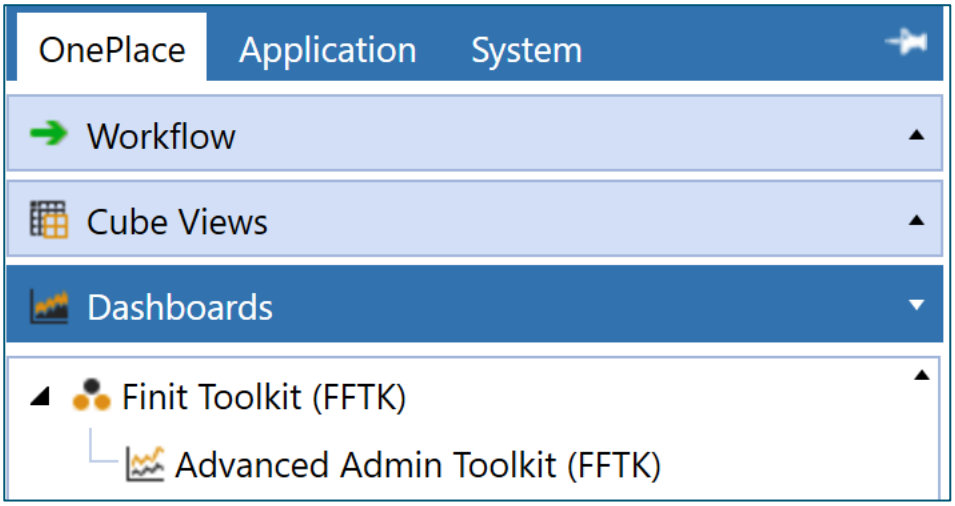
DATA STRUCTURES

No Data Tables are created for use with this solution.

Initial Setup

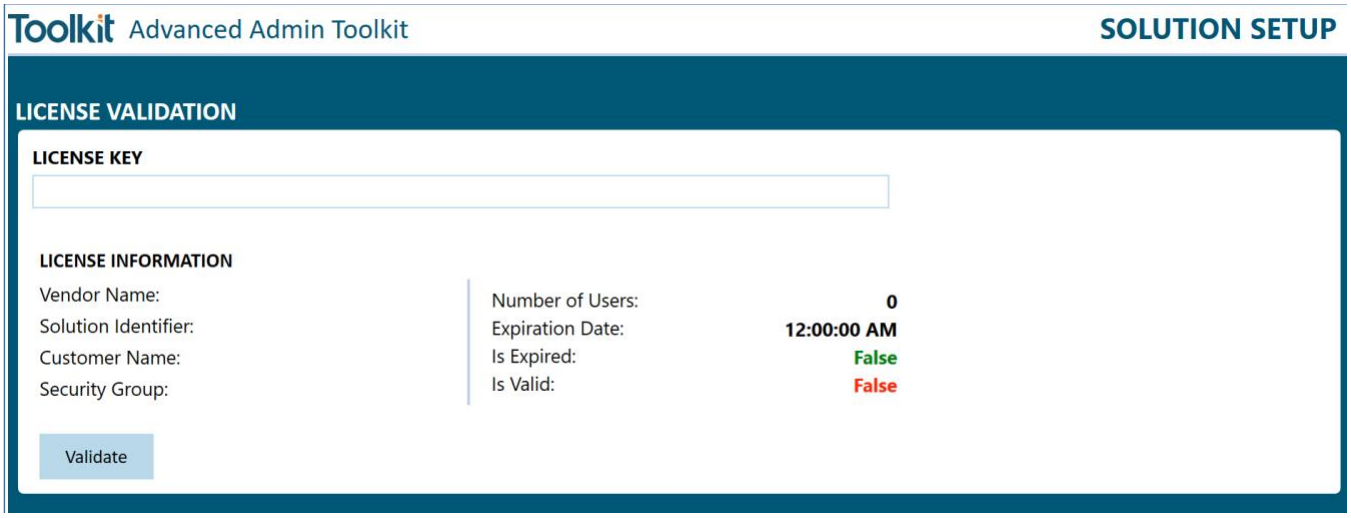
The first time you run the solution, you are guided through the solution setup process.

In OneStream, click **OnePlace > Dashboards > Finit Toolkit (FFTK) > Advanced Admin Toolkit (FFTK).**

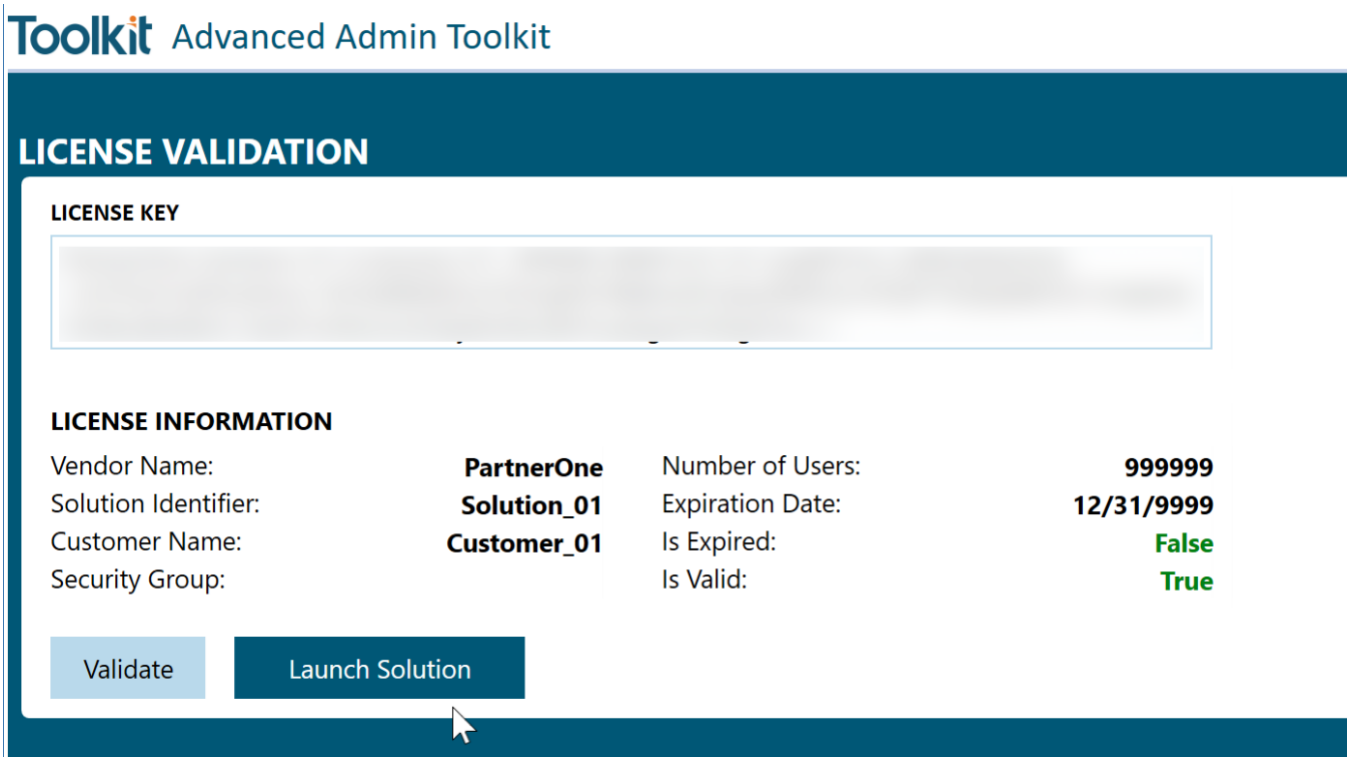


License Validation

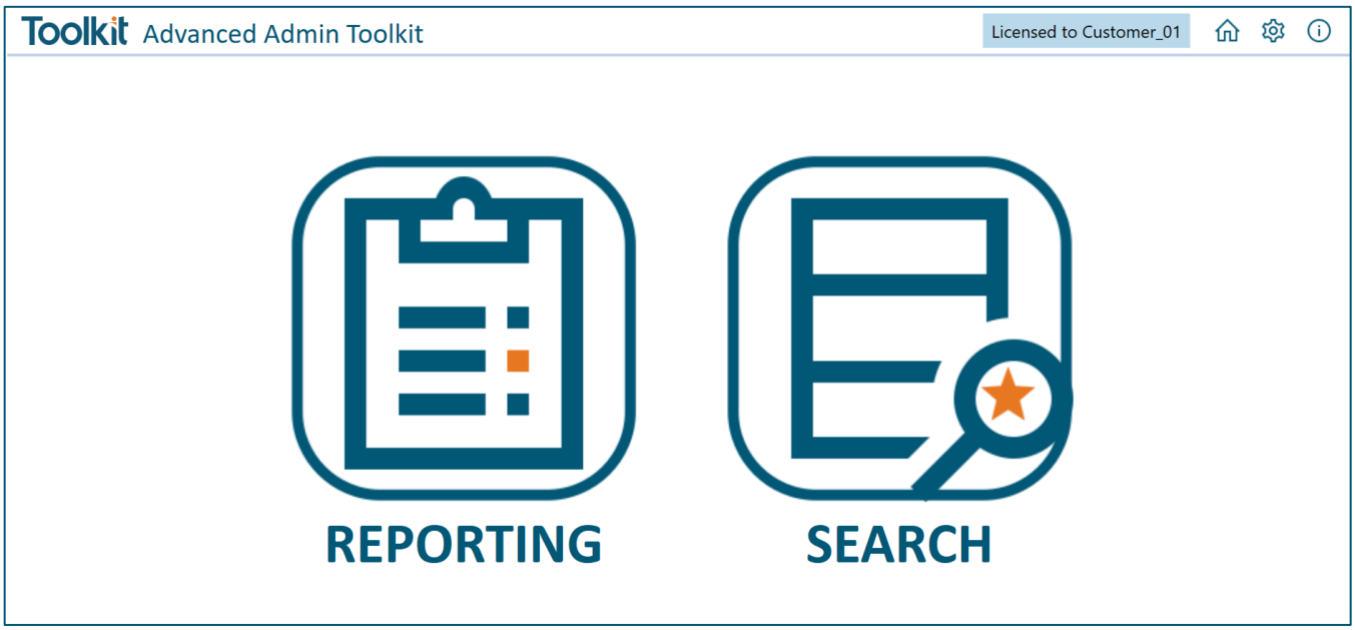
Enter a valid license key obtained from the OneStream PartnerPlace team



- Click Validate



A valid license will populate the License Information fields, and you can now launch the solution.

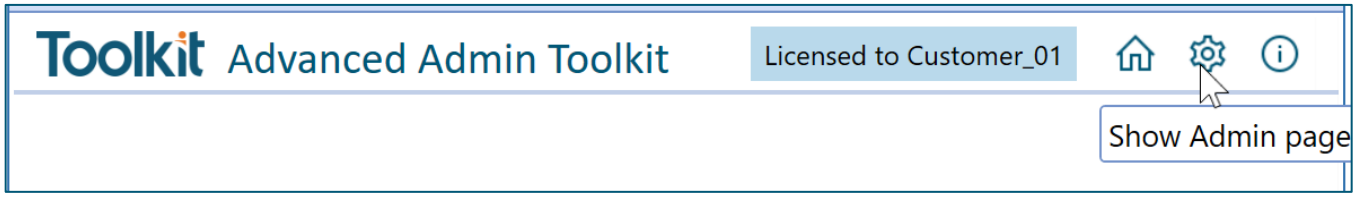


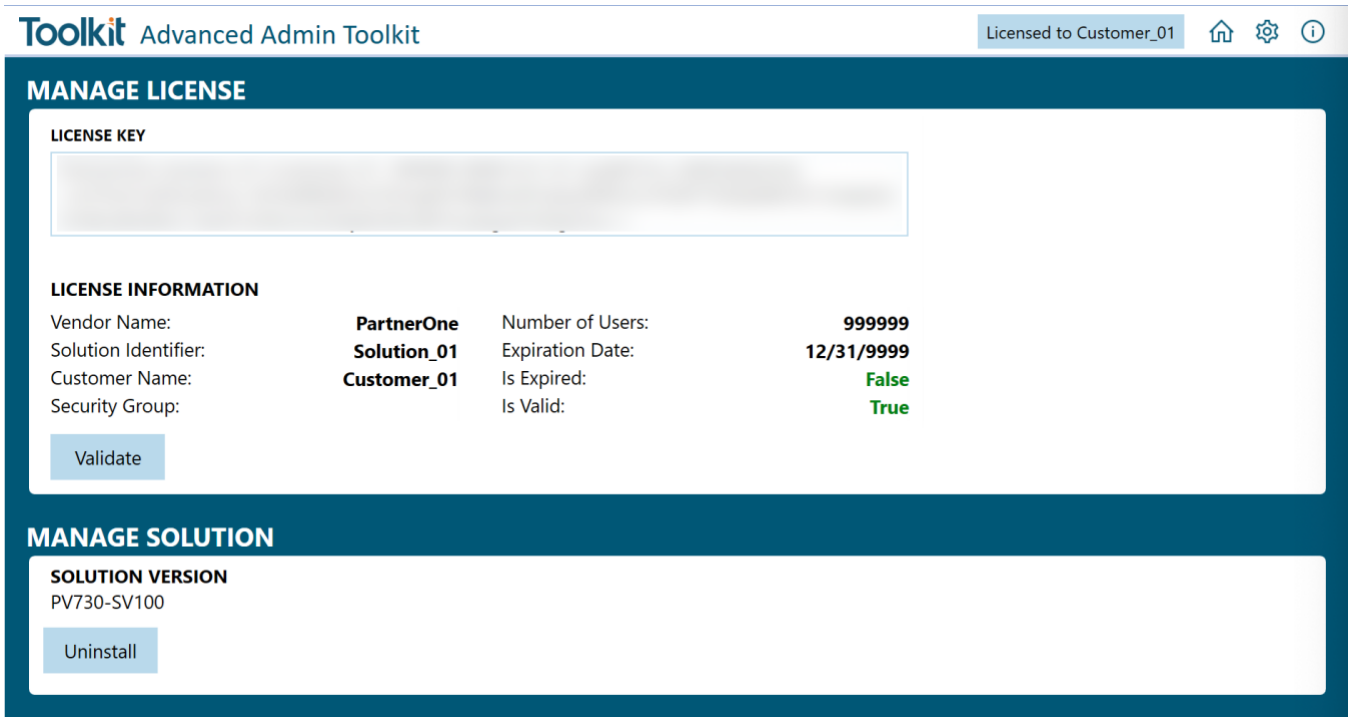
Settings & Configuration

Toolkit has minimal settings to get started and is truly plug-and-play. If an individual Utility can be configured, the settings can be accessed using the gear icon in the navigation bar from the respective Utility's page.

Admin Page

The Admin page, accessed from the Home page using the gear icon in the main navigation bar, has options for managing the license key and the solution installation and initial configuration.





Manage License

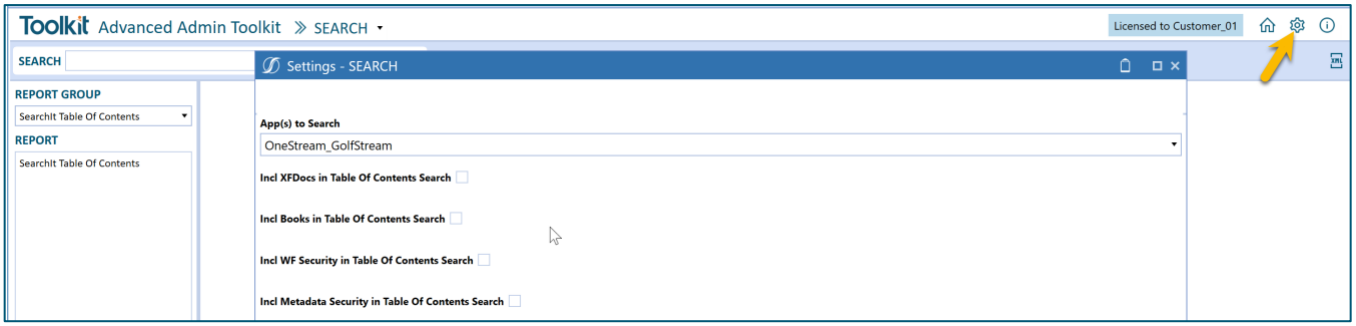
This is the area where you can administer the license key.

Manage Solution

UNINSTALL

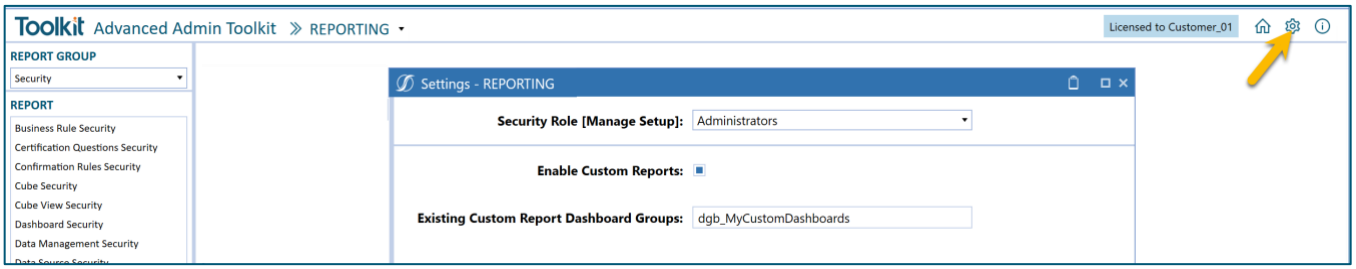
The Uninstall button will remove all the Dashboard Objects and Business Rules installed with this solution.

Search Settings



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

Reporting Settings



Security Role

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

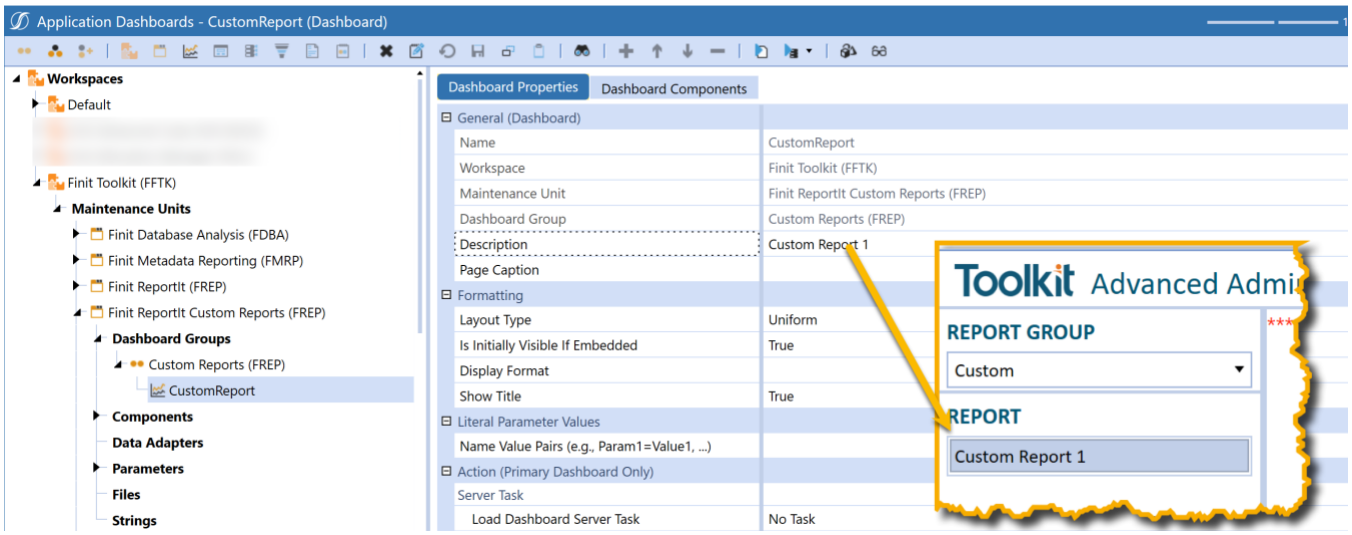
Enable Custom Reports

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

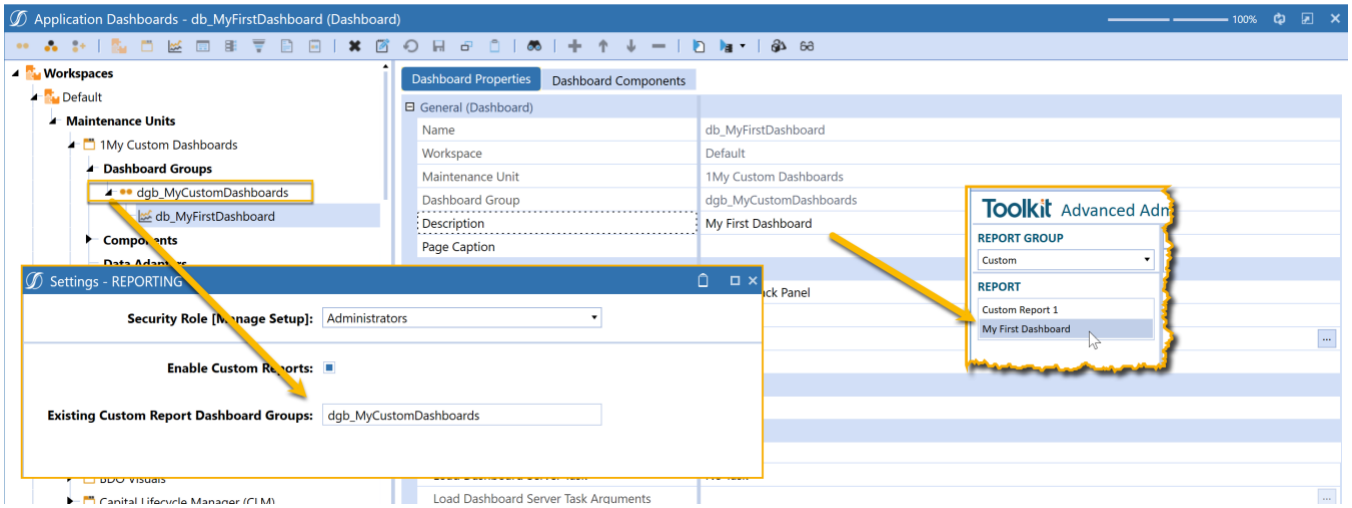
First, enable Custom Reports by clicking on the gear icon, then checking the box next to “Enable Custom Reports.”

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 Finit ReportIT Custom Reports (FREP) dashboard maintenance unit.

Note: The description on the dashboard will be what shows up on the Custom Reports set; if you don’t see the report in ReportIt, double check that the dashboard has a description.



The second way to add custom reports is to add the name(s) of the dashboard group(s) 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 appear in the report list.**



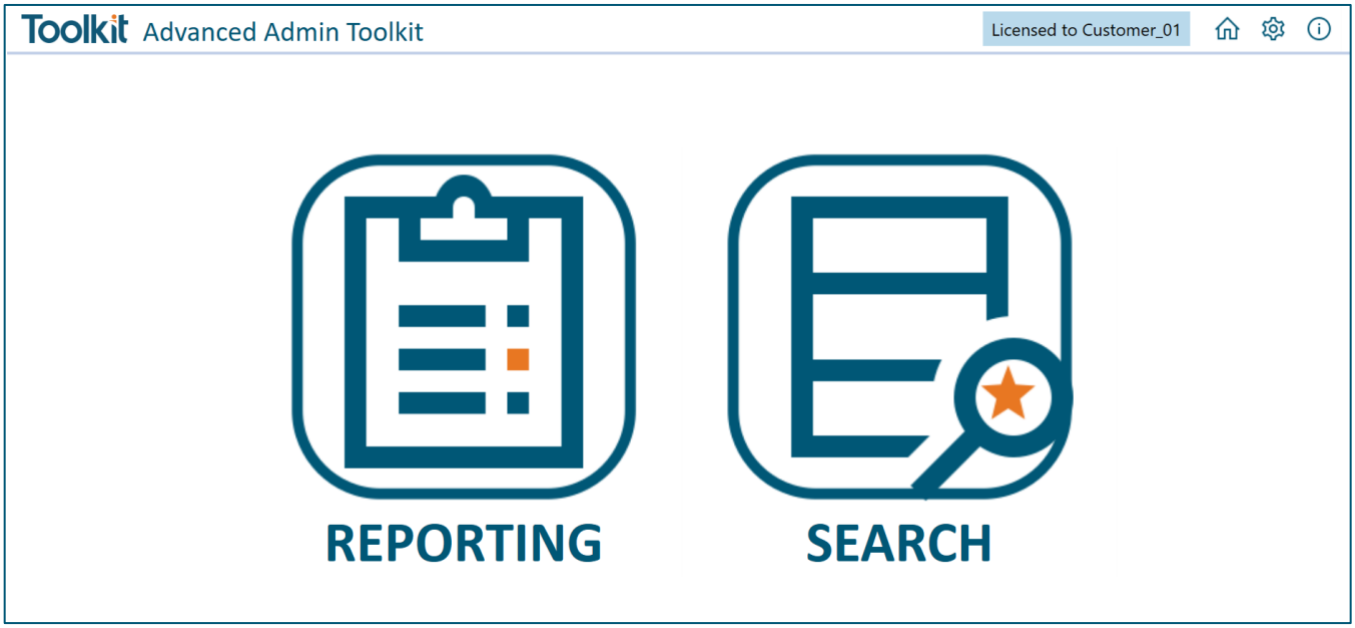
Administration Tasks

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

Upgrading

When upgrading the solution, it is recommended to uninstall the prior version first. This process can be completed by navigating to the Administration page and selecting the “Uninstall” button, then following any popups that appear after doing so.

Home Page



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

Reporting

Security Report Set

All the reports in the Finit Security Report Set are detailed below:

Business Rule Security

The Business Rule Security report shows a listing of business rules in the OneStream application with its associated security attributes. An example of this report is below. The **Is Encrypted** column indicates if the business rule is encrypted or not. The **Access Group** is the group of users that has the ability to see the business rule but cannot modify it. The **Maintenance Group** is the group of users that can see the business rule and make modifications to it.

Business Rule Security

Business Rule Security

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

Business Rule Name	Is Encrypted	Access Group	Maintenance Group
XFR_Conditional_Source	☐	Everyone	Everyone
XFR_Conditional_Target	☐	Everyone	Everyone
CPP_CapitalPlanningData	☐	Everyone	Everyone
CPP_CapitalPlanningData_EntityTin	☐	Everyone	Everyone
CPP_CapitalPlanningData_EntityTout	☐	Everyone	Everyone
CSP_CashPlanningData	☐	Everyone	Everyone

Certification Questions Security

The Certification Questions Security report has two tabs, one for group security and another for profile security for Certification Questions.

The "Certification Questions Group Security" tab shows a list of Certification Questions Group names and their descriptions, the scenario(s) associated with the group, and the Access Group and Maintenance Group associated with them. An example of this report can be seen below. The **Access Group** allows users to see the certification questions group. The **Maintenance Group** allows users to see and modify the certification questions group.

Certification Questions Group Security | Certification Questions Profile Security

Certification Questions Group Security

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

Certification Question Group Name	Description	Scenario Type	Access Group	Maintenance Group
(Quick Certify)	Is the workflow complete?	(All)	Everyone	Everyone
SOX AP Manager	SOX Accounts Payable Mgr	(All)	Everyone	Everyone
SOX Group Controller	SOX Group Controller	(All)	Everyone	Everyone
SOX AR Manager	SOX Accounts Receivable Mgr	(All)	Everyone	Everyone
SOX Plant Controller	SOX Plant Controller	(All)	Everyone	Everyone

The second tab is the "Certification Questions Profile Security" report and shows a list of Certification Question Profiles. In addition to the attributes that appear on the Certification Questions Group report, the **Cube** column indicates the cube(s) associated with the profile.

Certification Questions Group Security | Certification Questions Profile Security

Certification Questions Profile Security

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

Certification Question Profile Name	Description	Cube	Scenario Type	Access Group	Maintenance Group
Group Certification	Group Certification	(All)	(All)	Everyone	Everyone
Plant Certification	Plant Certification	(All)	(All)	Everyone	Everyone
(Quick Certify)	Workflow Complete	(All)	(All)	Everyone	Everyone

Confirmation Rules Security

The Confirmation Rules Security report has two tabs, one for group security and another for profile security for Confirmation Rules.

The "Confirmation Rules Group Security" tab shows a list of Confirmation Rules Groups names and their descriptions, the scenario(s) associated with the group, and the Access Group and Maintenance Group associated with them. An example of this report can be seen below. The **Access Group** allows users to see the confirmation rules group. The **Maintenance Group** allows users to see and modify the confirmation rules group.

Confirmation Rules Group Security | Confirmation Rules Profile Security

Confirmation Rules Group Security

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

Confirmation Rules Group Name	Description	Scenario Type	Access Group	Maintenance Group
Budget OperExp Constraints	Operating Expense Budget Constraints	(All)	Everyone	Everyone
Form Validation	Form Validation	(All)	Everyone	Everyone
Headcount Data	Headcount Data	(All)	Everyone	Everyone
Key Data Review	Key Data Review	(All)	Everyone	Everyone
Budget Revenue Constraints (Clubs)	Revenue Budget Constraints	(All)	Everyone	Everyone
US Supplemental (Houston)	US Supplemental (Houston)	Actual	Everyone	Everyone

The second tab is the "Confirmation Rules Profile Security" report and shows a list of Confirmation Rules Profiles. In addition to the attributes that appear on the Confirmation Rules Group report, the **Cube** column indicates the cube(s) associated with the profile.

Confirmation Rules Group Security | Confirmation Rules Profile Security

Confirmation Rules Profile Security

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

Confirmation Rules Profile Name	Description	Cube	Scenario Type	Access Group	Maintenance Group
Key Data Rules	Review Key Data	GolfStream	(All)	Everyone	Everyone
EBITDA Variance Rules	Variance EBITDA	(All)	(All)	Everyone	Everyone
Forecast Oper Exp Constraints	Operating Expense Forecast Constraints	(All)	(All)	Everyone	Everyone
Simple Form Rules	Simple Form Validation	GolfStream	(All)	Everyone	Everyone
Budget Rev Constraints (Course Mgmt)	Revenue Budget Constraints	(All)	(All)	Everyone	Everyone
Forecast Rev Contraints (Clubs)	Revenue Forecast Contraints (Clubs)	(All)	(All)	Everyone	Everyone

Cube Security

The Cube Security report shows a listing of cubes in the OneStream application and access and maintenance group names associated with the cubes. The **Access Group** allows users within the group to view the cube object. The **Maintenance Group** can see the cube and edit or delete them. An example of this report is shown below.

Cube Security

Cube Security

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

Cube Name	Description	Access Group Name	Maintenance Group Name
Houston	Houston Clubs	Everyone	Everyone
Ottawa	Ottawa Golf Balls	Everyone	Everyone
NewYork	New York Services & Course Design	Everyone	Everyone
Atlanta	Atlanta Apparel	Everyone	Everyone
Austin	Austin Apparel	Everyone	Everyone
GolfStream	Corporate	Everyone	Everyone
Drivers	Cost and Revenue Factors to Drive Values in Budget, Plan and Forecast	Everyone	Everyone

Cube View Security

The Cube View Security Report allows the user to see the security group setup for Cube View Groups and Cube View Profiles.

The "Cube View Group Security" tab shows a list of Cube View Groups along with the Access Group and Maintenance Group associated with them. An example of this report can be seen below. As with other security groups in the system, the **Access Group** allows users to see and run cube views in a cube view group or profile. The **Maintenance Group** allows users to see and run cube views as well as modify settings for cube view groups and profiles.

Cube View Group Security | Cube View Profile Security

Cube View Group Security

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

Cube View Group Name	Description	Access Group Name	Maintenance Group Name
Process (Flash)		Everyone	Everyone
Process (Profitability)		Everyone	Everyone
Data Entry (Profitabilty)		Everyone	Everyone
Process (Budget Revenue Course Mgmt)	Cubeviews for Budget Operating Expenses	Everyone	Everyone
XFR Member Filters (C) Time		Everyone	Everyone
Data Entry (Budget Oper Sales)	Operating Sales Budget Data Entry Forms (Intend	Everyone	Everyone
XFT Budget Manager (BMR)		Everyone	Everyone

The second tab is the "Cube View Profile Security" report and shows a list of Cube View Profiles. In addition to the attributes that appear on the Cube View Group report, the **Visibility** column indicates visibility settings for the cube view profile. This setting controls whether the cube view profile is visible in OnePlace, Workflows, Excel, etc. An example of this report can be seen on the following page.

Cube View Group Security | Cube View Profile Security

Cube View Profile Security

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

Cube View Profile Name	Description	Visibility	Access Group Name	Maintenance Group N
XFT Guided Reporting (GRT)		Dashboards	Everyone	Everyone
XFT Workspaces (AWS)		Dashboards	Everyone	Everyone
Excel Analysis		Excel	Everyone	Everyone
Data Entry (Budget Revenue Course Mgmt)	Budgeted Revenue Input	FormsExcel	Everyone	Everyone
Data Entry (Drivers)		Forms	Everyone	Everyone
Data Entry (Budget Revenue Clubs)	Budgeted Revenue Input	FormsExcel	Everyone	Everyone
Process (Budget Oper Exp)	Budget Submission Review	Workflow	Everyone	Everyone
Process (Flash)		Workflow	Everyone	Everyone

Dashboard Security

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

The "Dashboard Maintenance Unit Security" tab shows a list of Dashboard Maintenance Units with the name, description and the Access Group and Maintenance Group associated with them. An example of this report can be seen below. The **Access Group** allows users to see the maintenance unit. The **Maintenance Group** allows users to see and modify any object within the maintenance unit.

Dashboard Maintenance Unit Security | Dashboard Group Security | Dashboard Profile Security

Dashboard Maintenance Unit Security

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

Dashboard Maintenance Unit Name	Description	Access Group Name	Maintenance Group Name
Add Dimension Member (ADM)		Everyone	Everyone
CFModel_DB		Everyone	Everyone
Demo_Exec_Overview		Everyone	Everyone
Driver Based Planning (DBP)		Everyone	Everyone
Dynamic Rates Comparison (DRC)		Everyone	Everyone
External System (Revenue Mgmt Houston)	Houston Revenue Mgmt System	(Not Found)	Administrators
FIN_SecurityReporting	Finit Security Reporting	Everyone	Everyone
Finit Consulting Toolkit (FCTK)		Everyone	Everyone
Finit ReportIt (FREP)		Everyone	Everyone

The “Dashboard Group Security” tab shows a list of Dashboard Groups with the name, description and the Access Group associated with each group. An example of this report can be seen below. The **Access Group** allows users to see the dashboards within the dashboard group.

Dashboard Maintenance Unit Security | Dashboard Group Security | Dashboard Profile Security

Dashboard Group Security

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

Dashboard Group Name	Description	Access Group Name
Settings (AWSe1)		Everyone
Shared WFStatusBU (AWSe2)		Everyone
Request Content (FRIT)		Everyone
OnePlace (AWSe2)		Everyone
Workflow Analysis (CPP)		Everyone
WF_DataEntryDetail	Data Entry Detail Reports	Everyone
Train Me Admin (TRM)		Everyone

Finally, the “Dashboard Profile Security” tab shows a list of Dashboard Profiles with the name, description, visibility level, and access and maintenance groups associated with each profile. An example of this report can be seen below. The **Visibility** shows where in OneStream the user will be able to see the profile, such as in OnePlace, in a workflow, or both places when the setting is Always. The **Access Group** allows users to see the profile; the **Maintenance Group** allows the user to both see and modify the profile.

Dashboard Maintenance Unit Security | Dashboard Group Security | Dashboard Profile Security

Dashboard Profile Security

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

Dashboard Profile Name	Description	Visibility	Access Group Name	Maintenance Group Name
XFW Reconciliation Manager (RCM)		OnePlace	Everyone	Everyone
World Review		Workflow	Everyone	Everyone
WF_Certification_GC	Certification Group Controllers	Workflow	Everyone	Everyone
XFW Cash Planning (CSP)	Cash Planning (CSP)	OnePlace	Everyone	Administrators
WF_Certification_PC	Certification Plant Controllers	Workflow	Everyone	Everyone
XFS WF Data Entry	Data Entry	OnePlace	Everyone	Everyone

Data Management Security

The Data Management Security report shows two tabs for security on Data Management Groups and Data Management Profiles. In addition to **Name** and **Description**, these two reports also include **Access Group** (who can view the group or profile) and **Maintenance Group** (who can edit or delete the group or profile). An example of the two tabs on this report is shown below.

Data Management Group Security | Data Management Profile Security

Data Management Group Security

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

Data Management Group Name	Description	Access Group Name	Maintenance Group Name
Profitability		Everyone	Everyone
Reconciliation Manager (RCM)		Everyone	Administrators
Metadata Migration (FRIT)		Administrators	Administrators
System Consolidation		Everyone	Everyone

Data Management Group Security | Data Management Profile Security

Data Management Profile Security

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

Data Management Profile Name	Description	Access Group Name	Maintenance Group Name
dm_CopyData		Everyone	Everyone

Data Source Security

The Data Source security report shows a listing 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. An example of the report is included below, along with a table of the attributes.

Data Source Security

Data Source Security

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

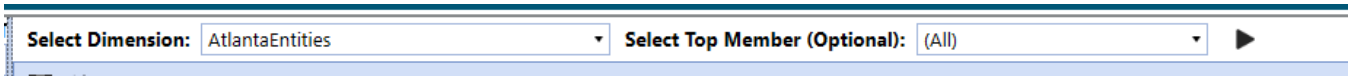
Scenario Type	Data Source Name	Description	Layout Type	Cube	Access Group Name	Maintenance Group Name
(Default)	FRIT_AccountSource	FRIT_AccountSource	Connector	FRIT_MetadataImport	Administrators	Administrators
(Default)	Legacy System CashFlow	Legacy System Cash Flow	Fixed	CashFlow	Everyone	Everyone
(Default)	XFR_EnterpriseExtract12Period	Load historical data	Delimited	XFR_DataSources	Everyone	Everyone
(Default)	SeedBudgetV1	Initialize Budget Version 1 Data	DataMgmtExportSequence	GolfStream	Everyone	Everyone
(Default)	FixedAssets	FixedAssets	Connector	CapEX	Everyone	Everyone

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. Will be Fixed, Delimited, Connector, or DataMgmtExportSequence
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
Maintenance Group Name	Members of the assigned group have the authority to maintain the Data Source.

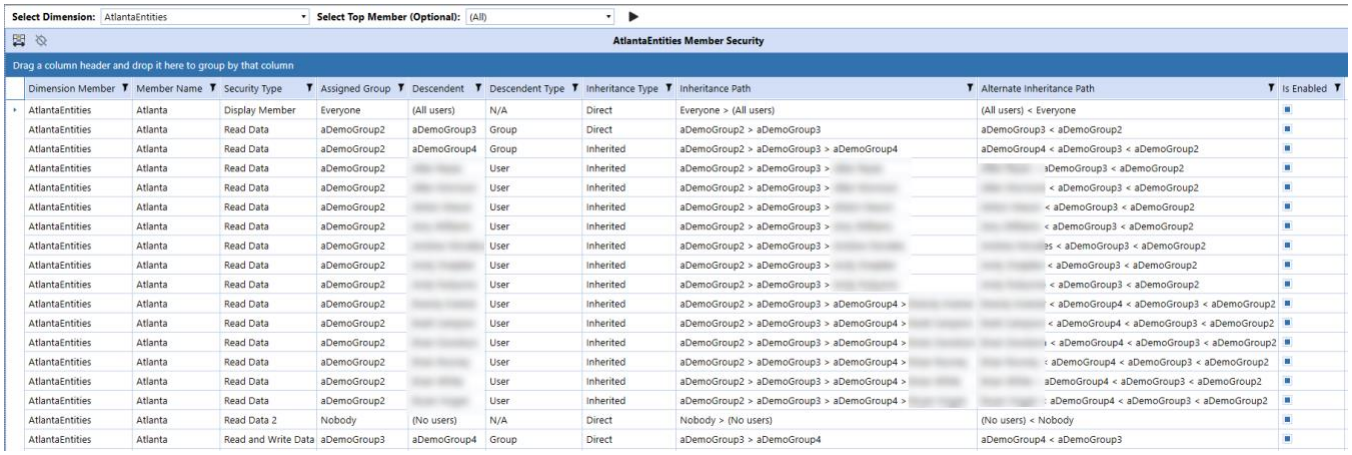
Dimension Metadata Security

The dimension metadata security allows 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 Play button to “Run Report.” The report will generate below. For large dimensions, this may take several minutes.



An example of the output is below:



Dimension Member	Member Name	Security Type	Assigned Group	Descendent	Descendent Type	Inheritance Type	Inheritance Path	Alternate Inheritance Path	Is Enabled
AtlantaEntities	Atlanta	Display Member	Everyone	(All users)	N/A	Direct	Everyone > (All users)	(All users) < Everyone	
AtlantaEntities	Atlanta	Read Data	aDemoGroup2	aDemoGroup3	Group	Direct	aDemoGroup2 > aDemoGroup3	aDemoGroup3 < aDemoGroup2	
AtlantaEntities	Atlanta	Read Data	aDemoGroup2	aDemoGroup4	Group	Inherited	aDemoGroup2 > aDemoGroup3 > aDemoGroup4	aDemoGroup4 < aDemoGroup3 < aDemoGroup2	
AtlantaEntities	Atlanta	Read Data	aDemoGroup2	[illegible]	User	Inherited	aDemoGroup2 > aDemoGroup3 > [illegible]	[illegible] aDemoGroup3 < aDemoGroup2	
AtlantaEntities	Atlanta	Read Data	aDemoGroup2	[illegible]	User	Inherited	aDemoGroup2 > aDemoGroup3 > [illegible]	[illegible] < aDemoGroup3 < aDemoGroup2	
AtlantaEntities	Atlanta	Read Data	aDemoGroup2	[illegible]	User	Inherited	aDemoGroup2 > aDemoGroup3 > [illegible]	[illegible] < aDemoGroup3 < aDemoGroup2	
AtlantaEntities	Atlanta	Read Data	aDemoGroup2	[illegible]	User	Inherited	aDemoGroup2 > aDemoGroup3 > [illegible]	[illegible] < aDemoGroup3 < aDemoGroup2	
AtlantaEntities	Atlanta	Read Data	aDemoGroup2	[illegible]	User	Inherited	aDemoGroup2 > aDemoGroup3 > [illegible]	[illegible] < aDemoGroup3 < aDemoGroup2	
AtlantaEntities	Atlanta	Read Data	aDemoGroup2	[illegible]	User	Inherited	aDemoGroup2 > aDemoGroup3 > [illegible]	[illegible] < aDemoGroup3 < aDemoGroup2	
AtlantaEntities	Atlanta	Read Data	aDemoGroup2	[illegible]	User	Inherited	aDemoGroup2 > aDemoGroup3 > aDemoGroup4 > [illegible]	[illegible] < aDemoGroup4 < aDemoGroup3 < aDemoGroup2	
AtlantaEntities	Atlanta	Read Data	aDemoGroup2	[illegible]	User	Inherited	aDemoGroup2 > aDemoGroup3 > aDemoGroup4 > [illegible]	[illegible] < aDemoGroup4 < aDemoGroup3 < aDemoGroup2	
AtlantaEntities	Atlanta	Read Data	aDemoGroup2	[illegible]	User	Inherited	aDemoGroup2 > aDemoGroup3 > aDemoGroup4 > [illegible]	[illegible] < aDemoGroup4 < aDemoGroup3 < aDemoGroup2	
AtlantaEntities	Atlanta	Read Data	aDemoGroup2	[illegible]	User	Inherited	aDemoGroup2 > aDemoGroup3 > aDemoGroup4 > [illegible]	[illegible] : aDemoGroup4 < aDemoGroup3 < aDemoGroup2	
AtlantaEntities	Atlanta	Read Data	aDemoGroup2	[illegible]	User	Inherited	aDemoGroup2 > aDemoGroup3 > aDemoGroup4 > [illegible]	[illegible] aDemoGroup4 < aDemoGroup3 < aDemoGroup2	
AtlantaEntities	Atlanta	Read Data	aDemoGroup2	[illegible]	User	Inherited	aDemoGroup2 > aDemoGroup3 > aDemoGroup4 > [illegible]	[illegible] : aDemoGroup4 < aDemoGroup3 < aDemoGroup2	
AtlantaEntities	Atlanta	Read Data 2	Nobody	(No users)	N/A	Direct	Nobody > (No users)	(No users) < Nobody	
AtlantaEntities	Atlanta	Read and Write Data	aDemoGroup3	aDemoGroup4	Group	Direct	aDemoGroup3 > aDemoGroup4	aDemoGroup4 < aDemoGroup3	

There are ten 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 appear 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.
Inheritance Path	This column shows how the group or user received the 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, this will show how groups are nested to ultimately arrive to the ancestor. In the example above, the third record shows that aDemoGroup2 contains aDemoGroup3 which contains aDemoGroup4.
Alternate Inheritance Path	This column shows how the group or user received the access through an inheritance path but is reversed order to show from child to parent. The first item will be the descendent. Reading the inheritance path to the right, this will show how groups are nested to ultimately arrive to the ancestor. In the example above, the third record shows that aDemoGroup4 is a member of aDemoGroup3, which is a member of aDemoGroup2.
Child Enabled	Whether or not the child is enabled for provisioning.

The report has the potential to generate thousands of records because 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 detail on the Everyone group is required, simply navigate back 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. An example of this report is shown below.

Dimension Security

Dimension Security

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

Dimension Type	Dimension Name	Description	Access Group Name	Maintenance Group Name
Entity	AtlantaEntities		Everyone	Everyone
Entity	AustinEntities		Everyone	Everyone
UD2	AustinProducts		Everyone	Everyone
UD4	AustinSalesChannel		Everyone	Everyone
Account	CAPEX		Everyone	Everyone

There are five 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 appear here.
Dimension Name:	The dimension name
Description	The dimension description (if available)
Access Group Name	The security group that has access to the dimension but cannot modify it
Maintenance Group Name	The security group that has access and can make changes to the dimension.

Form Template Security

The Form Template Security report shows two tabs for security on Form Template Groups and Form Template Profiles. In addition to **Name** and **Description**, these two reports also include **Access Group** (who can view the group or profile) and **Maintenance Group** (who can edit or delete the group or profile). An example of the two tabs on this report is shown below.

Form Template Group Security | Form Template Profile Security

Form Template Group Security

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

Form Template Group Name	Description	Access Group Name	Maintenance Group Name
Specialty Planning Drivers		Everyone	Everyone
Forecast Rev (Clubs NA)	Forecast Revenue Input Forms NA Cllubs	Everyone	Everyone
Budget Drivers	Budget Drivers	Everyone	Everyone
Profitability Data		Everyone	Everyone
Flash		Everyone	Everyone
People Planning Drivers	People Planning Drivers	Everyone	Everyone

Form Template Group Security | Form Template Profile Security

Form Template Profile Security

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

Form Template Profile Name	Description	Access Group Name	Maintenance Group Name
Profitability Data		Everyone	Everyone
Detail Entry		Everyone	Everyone
Profitability Drivers		Everyone	Everyone
Budget Revenue (Course Mgmt NA)	Revenue Input for Service Type and Region	Everyone	Everyone
MultiCurrency		Everyone	Everyone
Budget Drivers	Budget Drivers	Everyone	Everyone
Capital Planning Drivers		Everyone	Everyone

Journal Template Security

The Journal Template Security report shows two tabs for security on Journal Template Groups and Journal Template Profiles. In addition to **Name** and **Description**, these two reports also include **Access Group** (who can view the group or profile) and **Maintenance Group** (who can edit or delete the group or profile). An example of the two tabs on this report is shown below.

Journal Template Group Security | Journal Template Profile Security

Journal Template Group Security

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

Journal Template Group Name	Description	Access Group Name	Maintenance Group Name
Top Side Adj US		Everyone	Everyone
Accruals		Everyone	Everyone
Top Side Adj		Everyone	Everyone
Houston Allocations		Everyone	Everyone
IFRS Adjustments		Everyone	Everyone
Other Accruals		Everyone	Everyone

Journal Template Group Security | Journal Template Profile Security

Journal Template Profile Security

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

Journal Template Profile Name	Description	Access Group Name	Maintenance Group Name
Top Side Adj US		Everyone	Everyone
Typical Adjusting Entries		Everyone	Everyone
Adjusting Entries		Everyone	Everyone
Top Side Adj		Everyone	Everyone
Houston Journals	Houston Journals	Everyone	Everyone

Other Security Reports

The Other Security Reports group contains two additional reports for analytics and review purposes. The first tab is called “Groups with User Count,” which 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. An example of the output for this is below.

Groups with User Count | Users with Group Count | Groups with Assigned Children

Groups with User Count

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

Group Name	Total Members
2595_Mod	2
2AUSTAT_VIEW	3
2BRAZSTA_VIEW	0
2HNKGSTA_VIEW	1
2INDSTAT_VIEW	0
2JAPSTAT_VIEW	0
2KORSTAT_VIEW	0

The second tab, “Users with Group Count” shows a listing of users in the system, a flag that indicates if the user is enabled, and how many 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.

Groups with User Count | Users with Group Count | Groups with Assigned Children

Users with Group Count

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

User Name	Enabled	Total Groups
Test4	■	0
Administrator	■	0
TestUser5	■	1
TestUser3	■	1
test111	■	1

The third tab, “Groups with Assigned Children” shows a listing of users in the system, a flag that indicates if the user is enabled, and how many 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.

Groups with User Count | Users with Group Count | Groups with Assigned Children

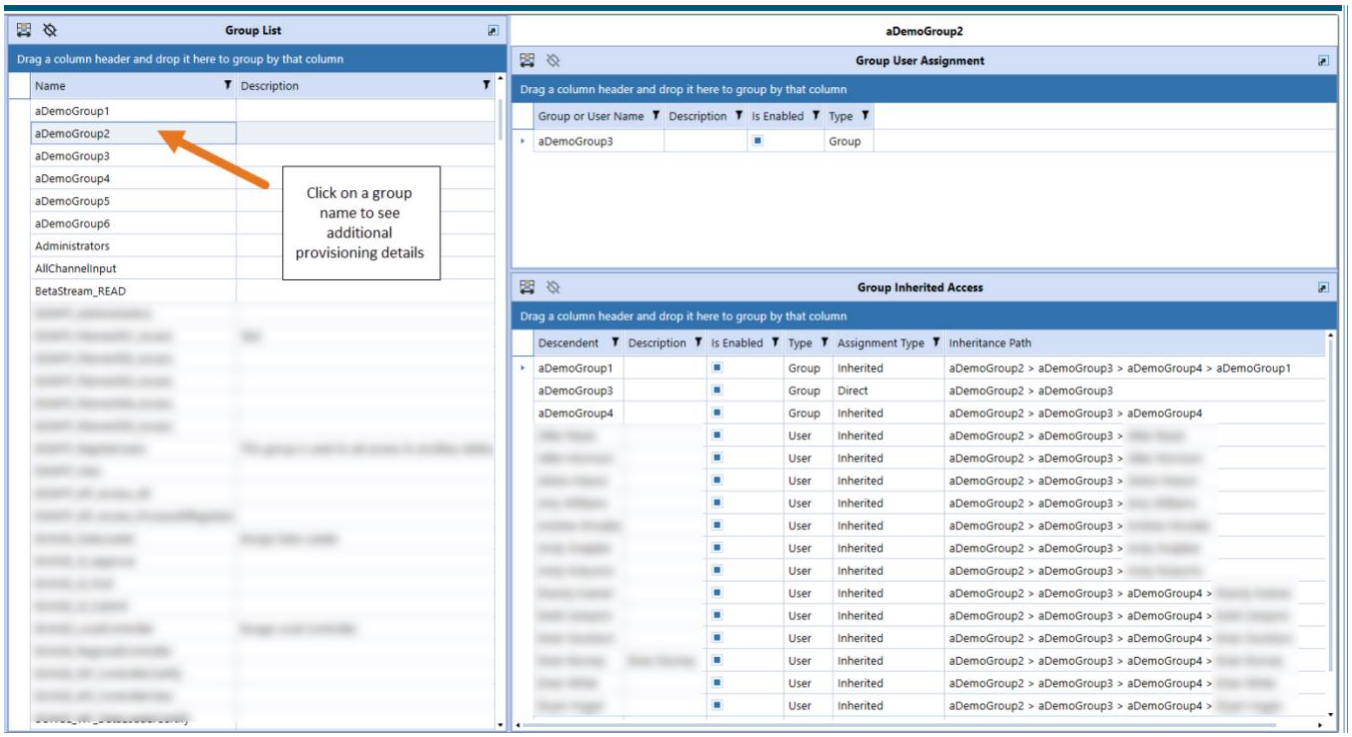
Groups with Assigned Children

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

Group Name	Child Name
2595_Mod	kmtest12
2595_Mod	test11
2AUSTAT_VIEW	test111
2AUSTAT_VIEW	Testuser1

Security Group Analysis

The Security Group Analysis report shows a listing 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 example below:



The top panel shows what users or groups have been provisioned in the selected group. In the example above, aDemoGroup3 has been directly assigned to aDemoGroup2. This report has three columns: **Group or Username**, **Is Enabled** (True or False), and **Type** (User or Group).

The bottom panel shows what groups or users *inherit* access to the group based on their direct provisioning. In addition to the **Group Or Username**, **Is Enabled**, and **Type** columns, this report has two additional columns:

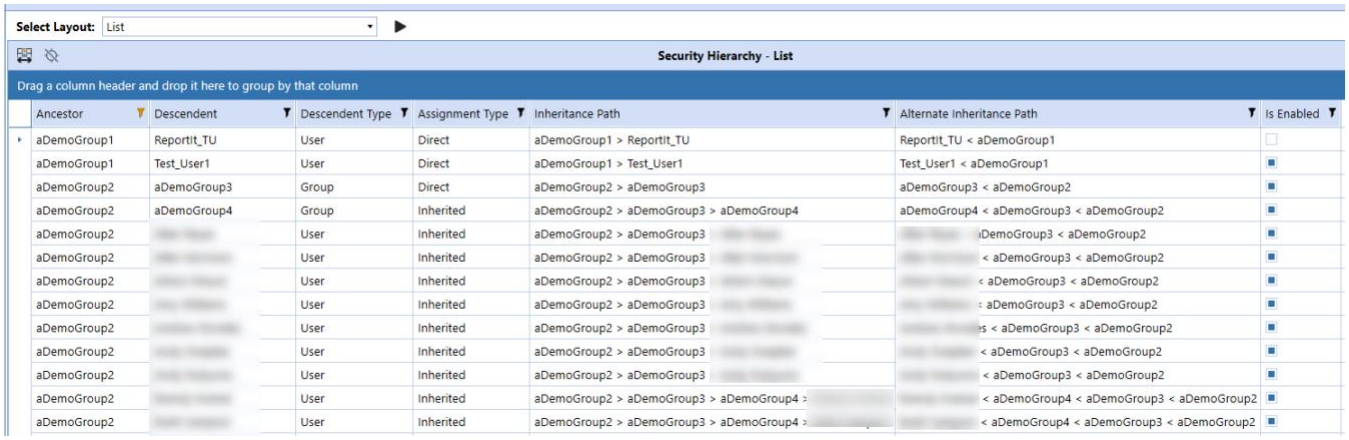
Attribute	Description
Assignment Type	*Direct* indicates that the group or user has been directly provisioned in the group. *Inherited* indicates that the group user receives access to this group indirectly through nested security groups.
Inheritance Path	This column shows how the group or user received the 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, this will show how groups are nested to ultimately arrive to the ancestor. In the example above, the second record shows that aDemoGroup2 contains aDemoGroup3 which contains aDemoGroup4.

Security Hierarchy

The Security Hierarchy report allows the user to see the full security assignment structure for the application. The report has two views: List View and Hierarchy View. To run, first select the layout of the report you'd like to see, then click "Run Report."

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 appear on this report. A sample of the report can be seen below.



Select Layout: List

Security Hierarchy - List

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

Ancestor	Descendent	Descendent Type	Assignment Type	Inheritance Path	Alternate Inheritance Path	Is Enabled
aDemoGroup1	Reportit_TU	User	Direct	aDemoGroup1 > Reportit_TU	Reportit_TU < aDemoGroup1	☐
aDemoGroup1	Test_User1	User	Direct	aDemoGroup1 > Test_User1	Test_User1 < aDemoGroup1	■
aDemoGroup2	aDemoGroup3	Group	Direct	aDemoGroup2 > aDemoGroup3	aDemoGroup3 < aDemoGroup2	■
aDemoGroup2	aDemoGroup4	Group	Inherited	aDemoGroup2 > aDemoGroup3 > aDemoGroup4	aDemoGroup4 < aDemoGroup3 < aDemoGroup2	■
aDemoGroup2	[illegible]	User	Inherited	aDemoGroup2 > aDemoGroup3 [illegible]	[illegible] aDemoGroup3 < aDemoGroup2	■
aDemoGroup2	[illegible]	User	Inherited	aDemoGroup2 > aDemoGroup3 [illegible]	[illegible] < aDemoGroup3 < aDemoGroup2	■
aDemoGroup2	[illegible]	User	Inherited	aDemoGroup2 > aDemoGroup3 [illegible]	[illegible] < aDemoGroup3 < aDemoGroup2	■
aDemoGroup2	[illegible]	User	Inherited	aDemoGroup2 > aDemoGroup3 [illegible]	[illegible] < aDemoGroup3 < aDemoGroup2	■
aDemoGroup2	[illegible]	User	Inherited	aDemoGroup2 > aDemoGroup3 [illegible]	[illegible]s < aDemoGroup3 < aDemoGroup2	■
aDemoGroup2	[illegible]	User	Inherited	aDemoGroup2 > aDemoGroup3 [illegible]	[illegible] < aDemoGroup3 < aDemoGroup2	■
aDemoGroup2	[illegible]	User	Inherited	aDemoGroup2 > aDemoGroup3 [illegible]	[illegible] < aDemoGroup3 < aDemoGroup2	■
aDemoGroup2	[illegible]	User	Inherited	aDemoGroup2 > aDemoGroup3 > aDemoGroup4 > [illegible]	[illegible] < aDemoGroup4 < aDemoGroup3 < aDemoGroup2	■
aDemoGroup2	[illegible]	User	Inherited	aDemoGroup2 > aDemoGroup3 > aDemoGroup4 > [illegible]	[illegible] < aDemoGroup4 < aDemoGroup3 < aDemoGroup2	■

Attribute	Description
Ancestor	A security group that has groups or users provisioned.
Descendent	A 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.
Inheritance Path	This column shows how the group or user received the 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, this will show how groups are nested to ultimately arrive to the ancestor. In the example above, the fourth record shows that aDemoGroup2 contains aDemoGroup3 which contains aDemoGroup4.
Alternate Inheritance Path	This column shows how the group or user received the access through an inheritance path but is reversed order to show from child to parent. The first item will be the descendent. Reading the inheritance path to the right, this will show how groups are nested to ultimately arrive to the ancestor. In the example above, fourth record shows that aDemoGroup4 is a member of aDemoGroup3, which is a member of aDemoGroup2.

HIERARCHY VIEW

The “Hierarchy view” provides visualization how security groups are nested and if inherited security is in effect. A sample of this report can be seen below.

Group or User Name	Object Type	Is Enabled
aDemoGroup2	Group	■
aDemoGroup3	Group	■
aDemoGroup4	Group	■
[illegible]	User	■
[illegible]	User	■
[illegible]	User	■
[illegible]	User	■
[illegible]	User	■
[illegible]	User	■
[illegible]	User	■
[illegible]	User	■
[illegible]	User	■
[illegible]	User	■
[illegible]	User	■
[illegible]	User	■
[illegible]	User	■
[illegible]	User	■

This report has three columns:

Attribute	Description
Group or User Name	The 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 two tabs for transformation rule groups and transformation rule profiles.

TRANSFORMATION RULE GROUP SECURITY

The first tab shows a listing of Transformation Rule Groups. Below is an example of the report along with a table of the attributes.

Transformation Rule Group Security | Transformation Rule Profile Security

Transformation Rule Group Security

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

Cube Dimension Name	Dimension Name	Rule Group Name	Rule Group Description	Access Group Name	Maintenance Group Name
(Derivative)	(Derivative)	CapEx_AccumDep	CapEx_AccumDep	Everyone	Everyone
(Derivative)	(Derivative)	BudgetV1_Houston_RegionAlloc	Houston Actual Region Allocation	Everyone	Everyone
(Derivative)	(Derivative)	HoustonSalesDetailOffset	Balance Entry Offset	Everyone	Everyone
(Derivative)	(Derivative)	CapEx_AssetPurchase	CapEx_AssetPurchase	Everyone	Everyone
(Derivative)	(Derivative)	XFR_Derivatives	Derivative Rules	Everyone	Everyone

Attribute	Description
Cube Dimension Name	The specific Dimension to which the Rule Group is assigned.
Dimension Name	The dimension type (e.g., 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
Maintenance Group Name	Members of this group have the authority to maintain the Transformation Rule Group

TRANSFORMATION RULE PROFILES

The second tab shows a list of the Transformation Rule Profiles, which has similar columns as the first tab. **Cube Name** is the cube that the rule group is associated with, and **Scenario Type** shows what scenario type the rule group will be associated with. An example of this report is below.

Transformation Rule Group Security | Transformation Rule Profile Security

Transformation Rule Profile Security

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

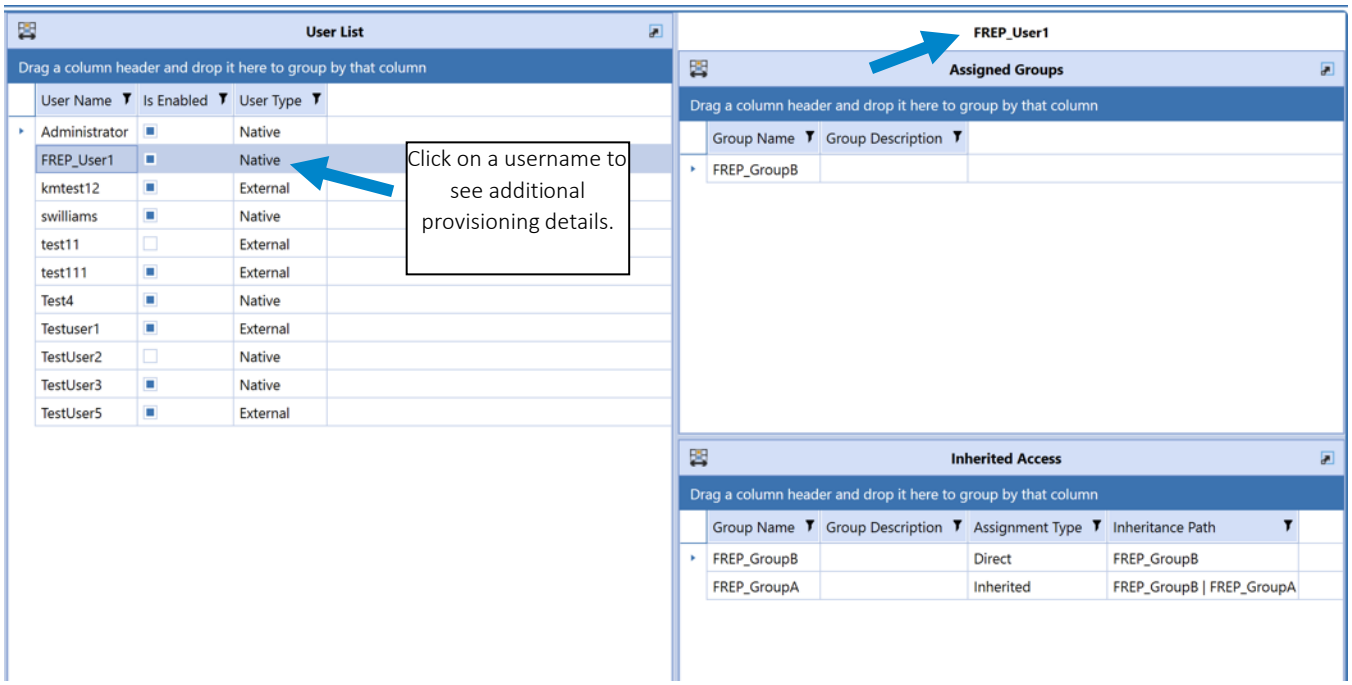
Rule Profile Name	Rule Profile Description	Cube Name	Scenario Type	Access Group Name	Maintenance Group Name
BudgetVx	Budget Vx to Budget Vy	GolfStream	(Default)	Everyone	Everyone
HoustonRules	HoustonRules	Houston	(Default)	Everyone	Everyone
FRIT_ImportMetadata	FRIT_ImportMetadata	FRIT_MetadataImport	(Default)	Administrators	Administrators
CapEx_Deprec	CapEx_Deprec	CapEX	(Default)	Everyone	Everyone
CorpRules	CorpRules	GolfStream	(Default)	Everyone	Everyone

User Analysis

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

Attribute	Description
Is Enabled	A *check* in this column means that the user is enabled and can be provisioned in security groups. *Unchecked* means that 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 such as Account Reconciliation, Lease, or other. *Third Party Access*: Allows OneStream access using a named account, logging on interactively via a third-party application. There is no access using the OneStream Windows application or the OneStream browser interface. The user cannot change data or modify OneStream application artifacts. *Financial Close*: Allows users to perform Account Reconciliation solutions and or Transaction Matching.

More details on a user 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 example below:



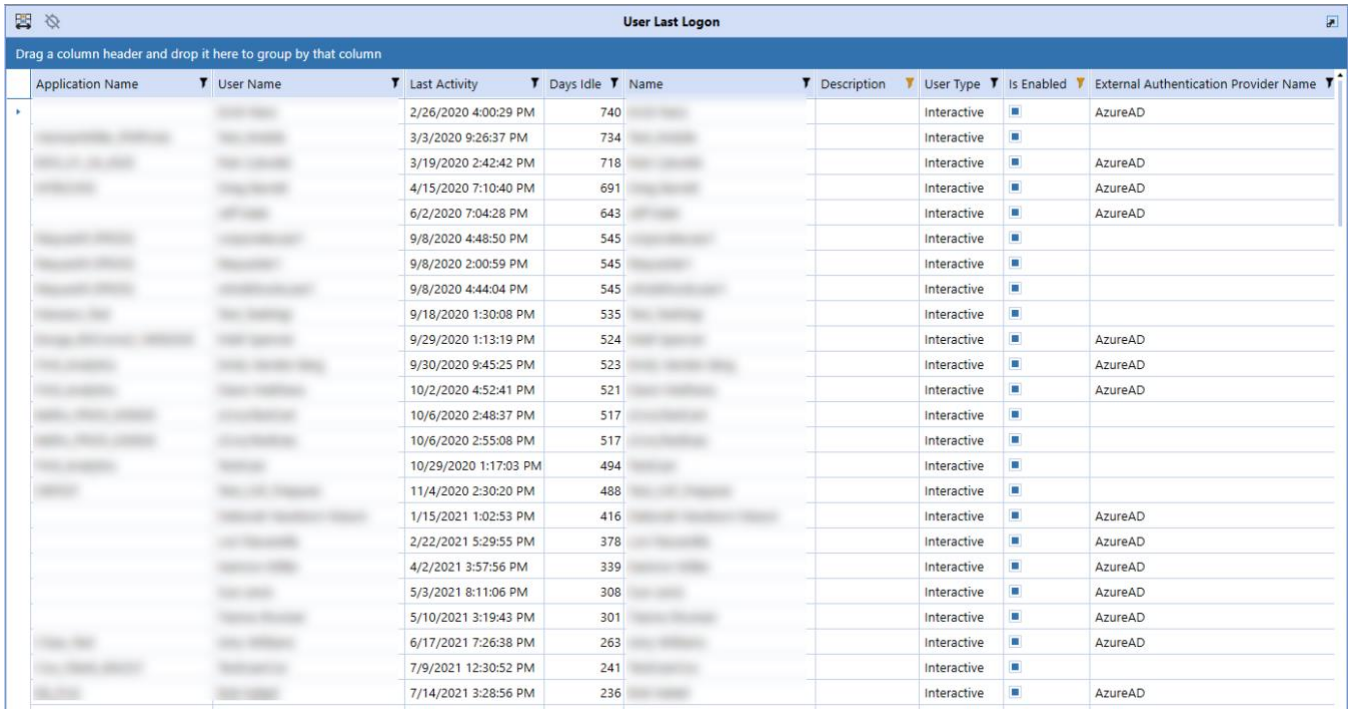
The top panel shows what groups the user has been directly provisioned in. In the example above, FREP_User1 has been directly assigned to FREP_GroupB. This report has two columns: **Group Name** and **Group Description**.

The bottom panel shows what groups the user *inherits* based on their direct provisioning. In addition to the **Group Name** and **Group Description** columns, this report has two 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 the 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, this will show how groups are nested to ultimately arrive to the top group. In the example above, FREP_User1 is *directly* assigned to FREP_GroupB, and it *inherits* access to FREP_GroupA because FREP_GroupB is assigned to FREP_GroupA.

User Last Logon

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



User Last Logon

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

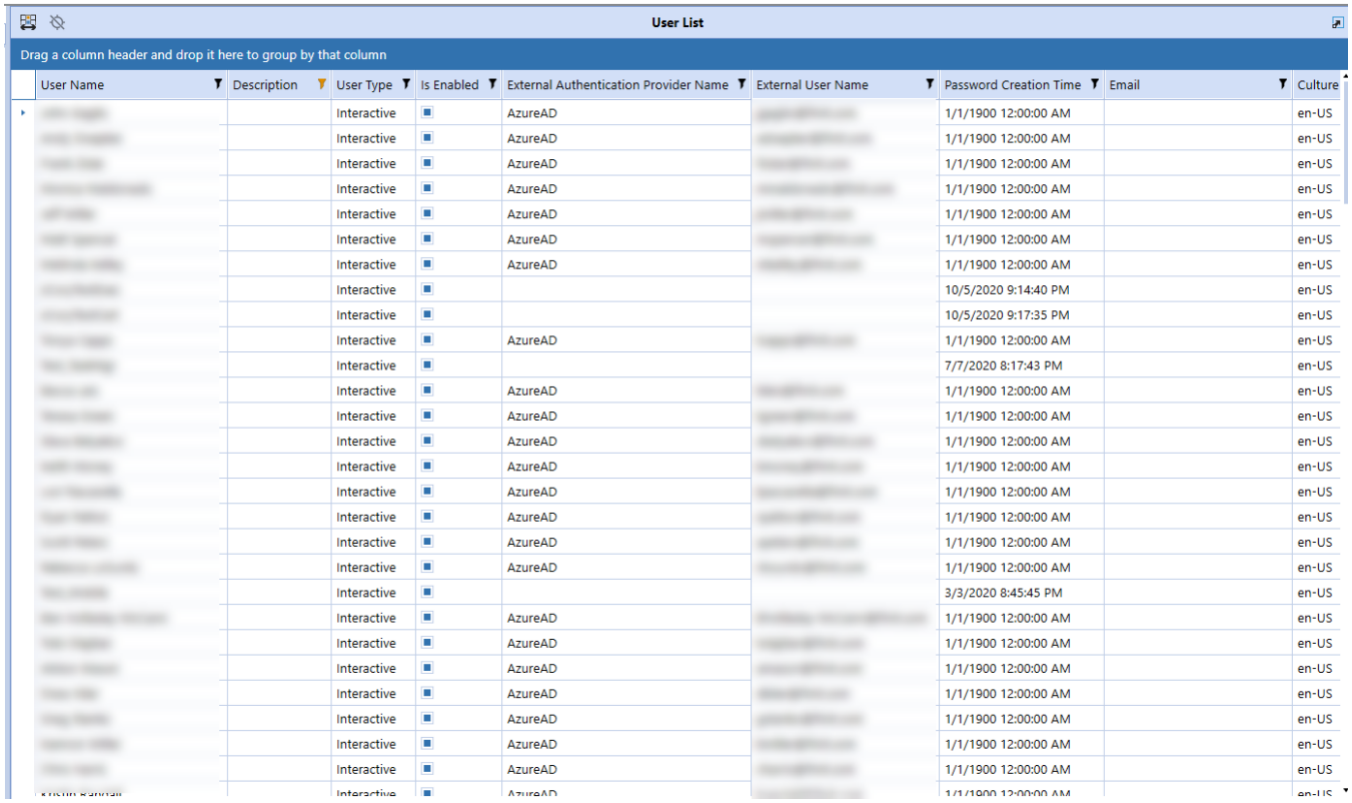
Application Name	User Name	Last Activity	Days Idle	Name	Description	User Type	Is Enabled	External Authentication Provider Name
		2/26/2020 4:00:29 PM	740			Interactive	■	AzureAD
		3/3/2020 9:26:37 PM	734			Interactive	■	
		3/19/2020 2:42:42 PM	718			Interactive	■	AzureAD
		4/15/2020 7:10:40 PM	691			Interactive	■	AzureAD
		6/2/2020 7:04:28 PM	643			Interactive	■	AzureAD
		9/8/2020 4:48:50 PM	545			Interactive	■	
		9/8/2020 2:00:59 PM	545			Interactive	■	
		9/8/2020 4:44:04 PM	545			Interactive	■	
		9/18/2020 1:30:08 PM	535			Interactive	■	
		9/29/2020 1:13:19 PM	524			Interactive	■	AzureAD
		9/30/2020 9:45:25 PM	523			Interactive	■	AzureAD
		10/2/2020 4:52:41 PM	521			Interactive	■	AzureAD
		10/6/2020 2:48:37 PM	517			Interactive	■	
		10/6/2020 2:55:08 PM	517			Interactive	■	
		10/29/2020 1:17:03 PM	494			Interactive	■	
		11/4/2020 2:30:20 PM	488			Interactive	■	
		1/15/2021 1:02:53 PM	416			Interactive	■	AzureAD
		2/22/2021 5:29:55 PM	378			Interactive	■	AzureAD
		4/2/2021 3:57:56 PM	339			Interactive	■	AzureAD
		5/3/2021 8:11:06 PM	308			Interactive	■	AzureAD
		5/10/2021 3:19:43 PM	301			Interactive	■	AzureAD
		6/17/2021 7:26:38 PM	263			Interactive	■	AzureAD
		7/9/2021 12:30:52 PM	241			Interactive	■	
		7/14/2021 3:28:56 PM	236			Interactive	■	AzureAD

The following additional attributes are available on the report:

Attribute	Description
Application Name	The last application the user logged on to.
Last Activity	Timestamp of last activity
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	The name of the external authentication provider (e.g., 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.



User List

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

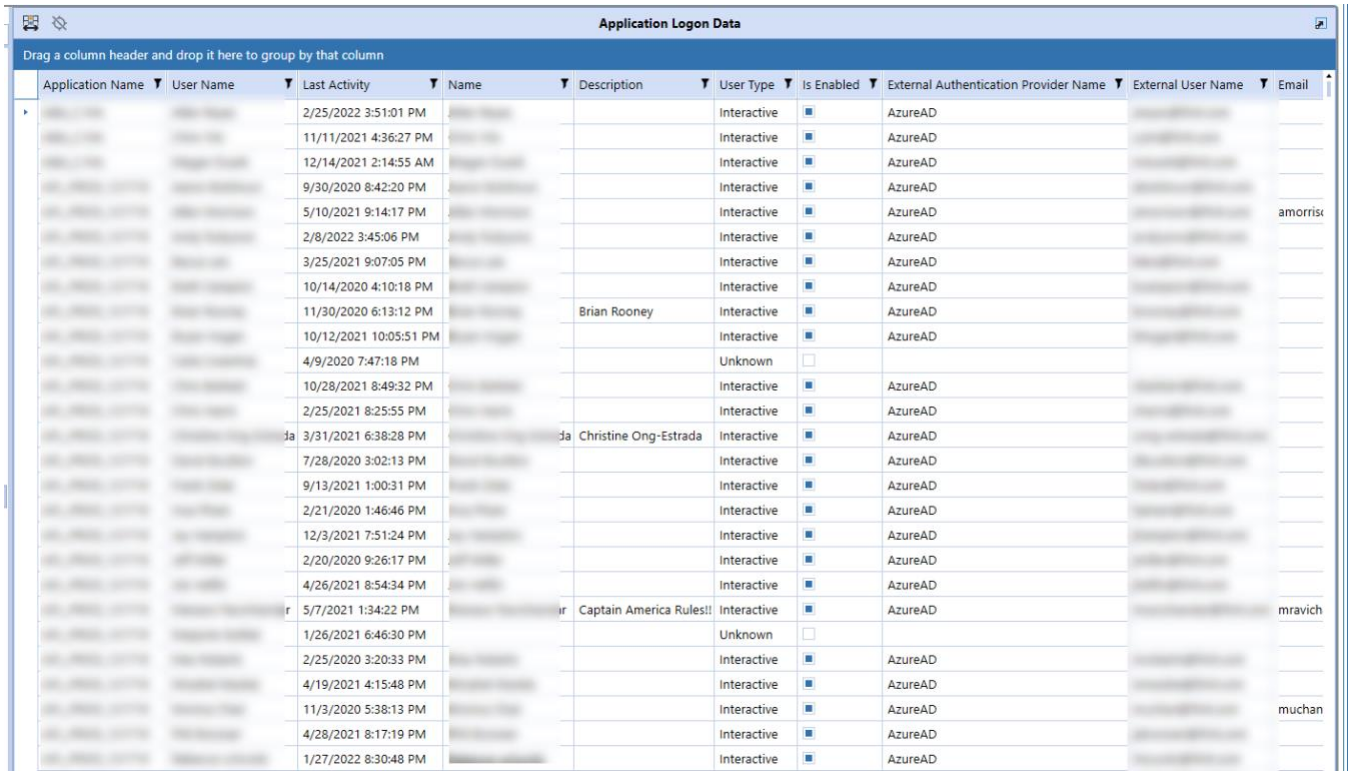
User Name	Description	User Type	Is Enabled	External Authentication Provider Name	External User Name	Password Creation Time	Email	Culture
[illegible]		Interactive	■	AzureAD	[illegible]	1/1/1900 12:00:00 AM		en-US
[illegible]		Interactive	■	AzureAD	[illegible]	1/1/1900 12:00:00 AM		en-US
[illegible]		Interactive	■	AzureAD	[illegible]	1/1/1900 12:00:00 AM		en-US
[illegible]		Interactive	■	AzureAD	[illegible]	1/1/1900 12:00:00 AM		en-US
[illegible]		Interactive	■	AzureAD	[illegible]	1/1/1900 12:00:00 AM		en-US
[illegible]		Interactive	■	AzureAD	[illegible]	1/1/1900 12:00:00 AM		en-US
[illegible]		Interactive	■	AzureAD	[illegible]	1/1/1900 12:00:00 AM		en-US
[illegible]		Interactive	■			10/5/2020 9:14:40 PM		en-US
[illegible]		Interactive	■			10/5/2020 9:17:35 PM		en-US
[illegible]		Interactive	■	AzureAD	[illegible]	1/1/1900 12:00:00 AM		en-US
[illegible]		Interactive	■			7/7/2020 8:17:43 PM		en-US
[illegible]		Interactive	■	AzureAD	[illegible]	1/1/1900 12:00:00 AM		en-US
[illegible]		Interactive	■	AzureAD	[illegible]	1/1/1900 12:00:00 AM		en-US
[illegible]		Interactive	■	AzureAD	[illegible]	1/1/1900 12:00:00 AM		en-US
[illegible]		Interactive	■	AzureAD	[illegible]	1/1/1900 12:00:00 AM		en-US
[illegible]		Interactive	■	AzureAD	[illegible]	1/1/1900 12:00:00 AM		en-US
[illegible]		Interactive	■	AzureAD	[illegible]	1/1/1900 12:00:00 AM		en-US
[illegible]		Interactive	■	AzureAD	[illegible]	1/1/1900 12:00:00 AM		en-US
[illegible]		Interactive	■	AzureAD	[illegible]	1/1/1900 12:00:00 AM		en-US
[illegible]		Interactive	■			3/3/2020 8:45:45 PM		en-US
[illegible]		Interactive	■	AzureAD	[illegible]	1/1/1900 12:00:00 AM		en-US
[illegible]		Interactive	■	AzureAD	[illegible]	1/1/1900 12:00:00 AM		en-US
[illegible]		Interactive	■	AzureAD	[illegible]	1/1/1900 12:00:00 AM		en-US
[illegible]		Interactive	■	AzureAD	[illegible]	1/1/1900 12:00:00 AM		en-US
[illegible]		Interactive	■	AzureAD	[illegible]	1/1/1900 12:00:00 AM		en-US
[illegible]		Interactive	■	AzureAD	[illegible]	1/1/1900 12:00:00 AM		en-US
[illegible]		Interactive	■	AzureAD	[illegible]	1/1/1900 12:00:00 AM		en-US
[illegible]		Interactive	■	AzureAD	[illegible]	1/1/1900 12:00:00 AM		en-US

For each user, the following attributes are available on 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	The name of the external authentication provider (e.g., 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 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 where multiple applications are used within the environment.



Application Logon Data

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

Application Name	User Name	Last Activity	Name	Description	User Type	Is Enabled	External Authentication Provider Name	External User Name	Email
[illegible]	[illegible]	2/25/2022 3:51:01 PM	[illegible]		Interactive	■	AzureAD	[illegible]	
[illegible]	[illegible]	11/11/2021 4:36:27 PM	[illegible]		Interactive	■	AzureAD	[illegible]	
[illegible]	[illegible]	12/14/2021 2:14:55 AM	[illegible]		Interactive	■	AzureAD	[illegible]	
[illegible]	[illegible]	9/30/2020 8:42:20 PM	[illegible]		Interactive	■	AzureAD	[illegible]	
[illegible]	[illegible]	5/10/2021 9:14:17 PM	[illegible]		Interactive	■	AzureAD	[illegible]	amorris
[illegible]	[illegible]	2/8/2022 3:45:06 PM	[illegible]		Interactive	■	AzureAD	[illegible]	
[illegible]	[illegible]	3/25/2021 9:07:05 PM	[illegible]		Interactive	■	AzureAD	[illegible]	
[illegible]	[illegible]	10/14/2020 4:10:18 PM	[illegible]		Interactive	■	AzureAD	[illegible]	
[illegible]	[illegible]	11/30/2020 6:13:12 PM	[illegible]	Brian Rooney	Interactive	■	AzureAD	[illegible]	
[illegible]	[illegible]	10/12/2021 10:05:51 PM	[illegible]		Interactive	■	AzureAD	[illegible]	
[illegible]	[illegible]	4/9/2020 7:47:18 PM			Unknown	□			
[illegible]	[illegible]	10/28/2021 8:49:32 PM	[illegible]		Interactive	■	AzureAD	[illegible]	
[illegible]	[illegible]	2/25/2021 8:25:55 PM	[illegible]		Interactive	■	AzureAD	[illegible]	
[illegible]	[illegible]da	3/31/2021 6:38:28 PM	[illegible]da	Christine Ong-Estrada	Interactive	■	AzureAD	[illegible]	
[illegible]	[illegible]	7/28/2020 3:02:13 PM	[illegible]		Interactive	■	AzureAD	[illegible]	
[illegible]	[illegible]	9/13/2021 1:00:31 PM	[illegible]		Interactive	■	AzureAD	[illegible]	
[illegible]	[illegible]	2/21/2020 1:46:46 PM	[illegible]		Interactive	■	AzureAD	[illegible]	
[illegible]	[illegible]	12/3/2021 7:51:24 PM	[illegible]		Interactive	■	AzureAD	[illegible]	
[illegible]	[illegible]	2/20/2020 9:26:17 PM	[illegible]		Interactive	■	AzureAD	[illegible]	
[illegible]	[illegible]	4/26/2021 8:54:34 PM	[illegible]		Interactive	■	AzureAD	[illegible]	
[illegible]	[illegible]r	5/7/2021 1:34:22 PM	[illegible]ir	Captain America Rules!!	Interactive	■	AzureAD	[illegible]	mravich
[illegible]	[illegible]	1/26/2021 6:46:30 PM			Unknown	□			
[illegible]	[illegible]	2/25/2020 3:20:33 PM	[illegible]		Interactive	■	AzureAD	[illegible]	
[illegible]	[illegible]	4/19/2021 4:15:48 PM	[illegible]		Interactive	■	AzureAD	[illegible]	
[illegible]	[illegible]	11/3/2020 5:38:13 PM	[illegible]		Interactive	■	AzureAD	[illegible]	muchan
[illegible]	[illegible]	4/28/2021 8:17:19 PM	[illegible]		Interactive	■	AzureAD	[illegible]	
[illegible]	[illegible]	1/27/2022 8:30:48 PM	[illegible]		Interactive	■	AzureAD	[illegible]	

The following additional attributes are available on the report:

Attribute	Description
Application Name	Name of the application the user logged on to
Last Activity	Timestamp 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	The name of the external authentication provider (e.g., 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. An example of this report is shown below 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 appear 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.

Select Cube Root Profile: FIN_WF_BUD **Select Top Workflow** (All)

Workflow Security

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

Profile Name	Scenario Type	Active	Profile Type	Cube Name	Access Group Name	Maintenance Group Name	Workflow Execution Group Name	Certification Signoff Group Name
FIN_WF_BUD_Default	(Default)	■	Default	FIN_WF	Everyone	Everyone	Everyone	Everyone
FIN_WF_BUD_Default.Import	(Default)	■	InputImportChild	FIN_WF	Everyone	Everyone	Everyone	Everyone
FIN_WF_BUD_Default.Import	Budget	■	InputImportChild	FIN_WF	Everyone	Everyone	(Use Default)	(Use Default)
FIN_WF_BUD_Default.Import	Forecast	■	InputImportChild	FIN_WF	Everyone	Everyone	(Use Default)	(Use Default)
FIN_WF_BUD_Default.Forms	(Default)	■	InputFormsChild	FIN_WF	Everyone	Everyone	Everyone	Everyone
FIN_WF_BUD_Default.Forms	Budget	■	InputFormsChild	FIN_WF	Everyone	Everyone	(Use Default)	(Use Default)
FIN_WF_BUD_Default.Forms	Forecast	■	InputFormsChild	FIN_WF	Everyone	Everyone	(Use Default)	(Use Default)
FIN_WF_BUD_Default.Adj	(Default)	■	InputAdjChild	FIN_WF	Everyone	Everyone	Everyone	Everyone
FIN_WF_BUD_Default.Adj	Budget	■	InputAdjChild	FIN_WF	Everyone	Everyone	(Use Default)	(Use Default)
FIN_WF_BUD_Default.Adj	Forecast	■	InputAdjChild	FIN_WF	Everyone	Everyone	(Use Default)	(Use Default)
BASE_B	(Default)	■	BaseInput	FIN_WF	aDemoGroup3	aDemoGroup3	aDemoGroup3	aDemoGroup3
BASE_B	Budget	□	BaseInput	FIN_WF	aDemoGroup3	aDemoGroup3	aDemoGroup4	aDemoGroup4
BASE_B	Forecast	□	BaseInput	FIN_WF	aDemoGroup3	aDemoGroup3	aDemoGroup5	aDemoGroup5
BASE_B.Import	(Default)	■	InputImportChild	FIN_WF	Everyone	Everyone	Everyone	Everyone

Attribute	Description
Profile Name	Workflow profile name
Scenario Type	Scenario Type
Active	Indicator of 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 run time to view results
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 execute 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.

Metadata Report Set

The Metadata reports help to analyze the OneStream metadata

Member Formulas

The Member Formulas report allows 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 two views, Summary, and Detail. 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.

Select Detail Level: Summary Detail

Member Formulas

Grouped by: FormulaPass

Dimension	DimName	Name	Description	FormulaPass	VaryByScenType	VaryByTime
Formula Pass 01						
ACCOUNT	ExampleAccounts	Current Year Net Income	Current Year Net Income	Formula Pass 01	Default	Default
Formula Pass 08						
ACCOUNT	ExampleAccounts	Balance	Balance	Formula Pass 08	Default	Default
ACCOUNT	ExampleAccounts	CTA	CTA	Formula Pass 08	Default	Default
ACCOUNT	ExampleAccounts	EVALSales	Eval_Sales	Formula Pass 08	Default	Default
Formula Pass 09						
ACCOUNT	ExampleAccounts	CF_AP	Increase (decrease) in liabilities (A/P, taxes payable)	Formula Pass 09	Default	Default
ACCOUNT	ExampleAccounts	CF_AR	Decrease (increase) in accounts receivable	Formula Pass 09	Default	Default
ACCOUNT	ExampleAccounts	CF_CAPEX	Capital Expenditures	Formula Pass 09	Default	Default
ACCOUNT	ExampleAccounts	CF_CashCheck	Cash Flow Check Change in Cash	Formula Pass 09	Default	Default
ACCOUNT	ExampleAccounts	CF_DEBT	Increase (decrease) in debt	Formula Pass 09	Default	Default
ACCOUNT	ExampleAccounts	CF_DEPRAMORT	Adjustments for Depreciation and Amortization	Formula Pass 09	Default	Default
ACCOUNT	ExampleAccounts	CF_FIN_OTHER	Other cash flows from financing activities	Formula Pass 09	Default	Default
ACCOUNT	ExampleAccounts	CF_INV	Decrease (increase) in inventory	Formula Pass 09	Default	Default
ACCOUNT	ExampleAccounts	CF_NetInc	Net Income (Loss)	Formula Pass 09	Default	Default
ACCOUNT	ExampleAccounts	CF_Other	Increase (decrease) in other operating activities	Formula Pass 09	Default	Default
ACCOUNT	ExampleAccounts	CF_Stock	Sale (repurchase) of stock	Formula Pass 09	Default	Default
ACCOUNT	ExampleAccounts	CF_CapitalLeasePrincipal	Capital Lease Principal Payment	Formula Pass 09	Default	Default
Formula Pass 10						
ACCOUNT	ExampleAccounts	CF_VAR	Cash Flow Variance	Formula Pass 10	Default	Default

DETAIL LEVEL

This example shows the same data as Summary, grouped by Formula Pass and then filtered by Dimension Name, and also includes the Text Value of the Member Formula.

Select Detail Level: Summary Detail

Member Formulas

Grouped by: FormulaPass

Dimension	DimName	Name	Descript	FormulaPass	VaryBy	VaryByTime	TextValue
Formula Pass 01							
ACCOUNT	ExampleAccounts	Current Year Net Income	Current Yea	Formula Pass 01	Default	Default	api.data.calculate("A#[Current Year Net Income]:F#None:I#NONE = A#NetInc:F#TOP:I#TOP
Formula Pass 08							

ACCOUNT	ExampleAccounts	Balance	Balance	Formula Pass 08	Default	Default	If api.Cons.IsLocalCurrencyforEntity() Then
							Dim entityDimPk As DimPk = api.Pov.EntityDim.DimPk
							Dim entityId As Integer = api.Pov.Entity.MemberPk.MemberId
							If Not api.Members.HasChildren(entityDimPk, entityId, Nothing) Then
							api.data.calculate("A#BALANCE:F#None:I#None = A#TotalAssets:F#Top:I#TOP - A#
							End If
							End if

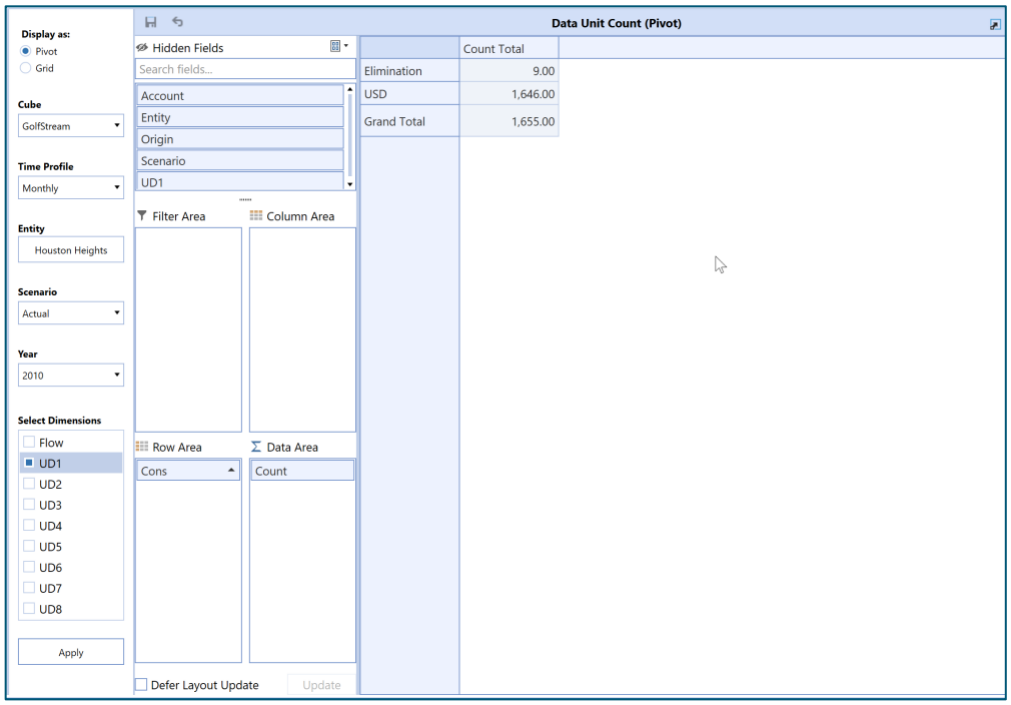
ACCOUNT	ExampleAccounts	CTA	CTA	Formula Pass 08	Default	Default	If (api.Cons.IsCurrency() And Not api.Cons.IsLocalCurrencyforEntity()) Then
							Dim entityDimPk As DimPk = api.Pov.EntityDim.DimPk
							Dim entityId As Integer = api.Pov.Entity.MemberPk.MemberId
							If Not api.Members.HasChildren(entityDimPk, entityId, Nothing) Then
							api.data.calculate("A#CTA:F#None:I#None = A#TotalAssets:F#Top:I#TOP - A#
							END IF
							End if

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.

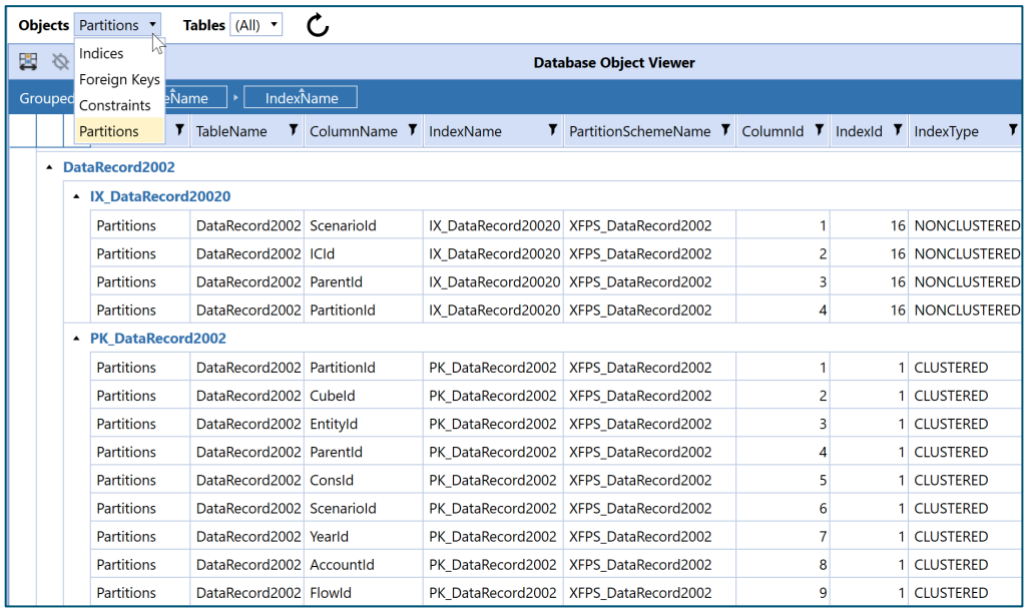
Data Unit Count

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.

Database Size

name	FGID	File_Id	Actual_File_Size	Free_MB	Reserved_MB	Size_On_Disk_Bytes	Used_MB
OneStream_GolfStream_23	1	1	0.85	0.81	871.56	913,899,520.00	870.75
OneStream_GolfStream_23_Audit	4	5	3.30	0.00	3,377.31	3,541,368,832.00	3,377.31
OneStream_GolfStream_23_CalcStatus	14	15	0.05	28.13	47.44	49,741,824.00	19.31
OneStream_GolfStream_23_DataEntryAudit	15	16	0.01	3.50	11.50	12,058,624.00	8.00
OneStream_GolfStream_23_DataRecord	13	14	0.22	13.13	221.50	232,259,584.00	208.38
OneStream_GolfStream_23_Default	2	3	0.24	0.94	245.25	257,163,264.00	244.31
OneStream_GolfStream_23_FileSystem	5	6	0.02	2.63	17.31	18,153,472.00	14.69
OneStream_GolfStream_23_log	0	2	1.06	1,062.87	1,082.81	1,135,411,200.00	19.95
OneStream_GolfStream_23_StageAttribute	12	13	0.04	16.44	40.13	42,074,112.00	23.69
OneStream_GolfStream_23_StageHistory	8	9	0.04	28.31	38.63	40,501,248.00	10.31
OneStream_GolfStream_23_StageSource	9	10	0.13	62.94	134.81	141,361,152.00	71.88
OneStream_GolfStream_23_StageSummary	11	12	0.12	52.75	119.00	124,780,544.00	66.25
OneStream_GolfStream_23_StageTarget	10	11	0.19	81.94	189.44	198,639,616.00	107.50
OneStream_GolfStream_23_Timestamps	3	4	0.00	0.25	2.00	2,097,152.00	1.75
OneStream_GolfStream_23_WorkflowActivity	6	7	0.02	1.56	25.00	26,214,400.00	23.44
OneStream_GolfStream_23_WorkflowHistory	7	8	0.03	9.25	34.13	35,782,656.00	24.88
			Sum = 6.31	Sum = 1,365.45	Sum = 6,457.82	Sum = 6,771,507,200.00	Sum = 5,092.40

Database Tables Size

Analyze and summarize key database tables metrics such as Row Count and table Size (MB) across all tables in your application.

Table Size

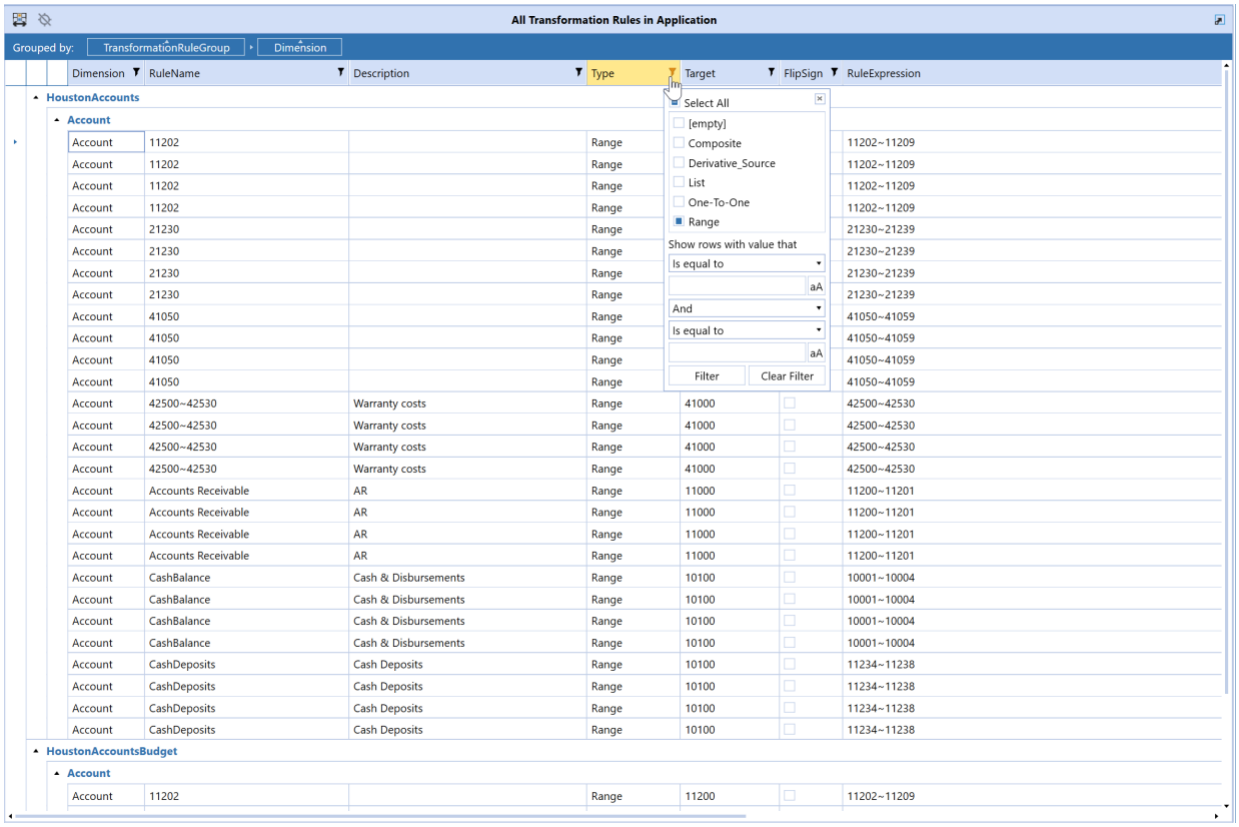
Table Name	Row Count	Table Size (MB)
AppProperty	143.00	0.11
Attachment	0.00	0.00
AuditAppProperty	777.00	0.55
AuditBusinessRule	19,269.00	2,494.72
AuditCertifyGroups	27.00	0.05
AuditCertifyProfileMembers	33.00	0.05
AuditCertifyProfiles	21.00	0.05
AuditCertifyQuestions	6.00	0.05
AuditConfirmGroups	93.00	0.05
AuditConfirmProfileMembers	81.00	0.05
AuditConfirmProfiles	54.00	0.05
AuditConfirmRules	582.00	1.88
AuditCube	219.00	0.40
AuditCubeDataAccess	24.00	0.05
AuditCubeDim	1,965.00	0.31
AuditCubeReference	15.00	0.05
AuditCubeViewGroup	537.00	0.20
AuditCubeViewItem	19,707.00	164.62
AuditCubeViewProfile	306.00	0.13
AuditCubeViewProfileMember	228.00	0.05
AuditDashboard	103,428.00	45.52
AuditDashboardAdapter	15,579.00	51.64
AuditDashboardBusinessRule	0.00	0.00
AuditDashboardCompAdptrMember	14,160.00	2.04
AuditDashboardComponent	374,262.00	464.77
AuditDashboardDbrdCompMember	375,129.00	41.04
AuditDashboardGroup	10,044.00	1.84
AuditDashboardMaintUnit	[illegible]	[illegible]
	Sum = 18,848,279.00	Sum = 5,058.99

Stage Report Set

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

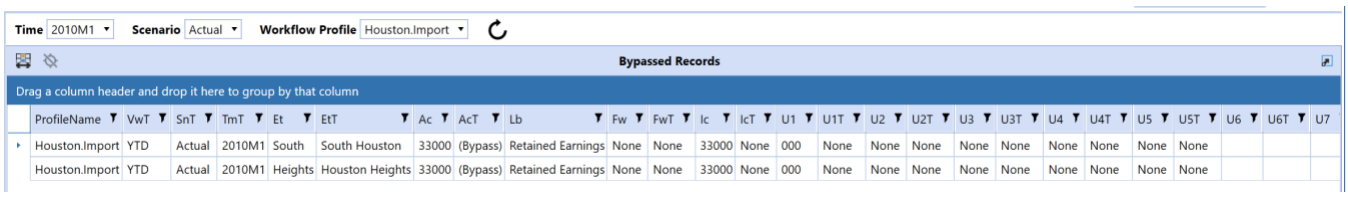
All Transformation Rules in Application

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



Bypassed Records

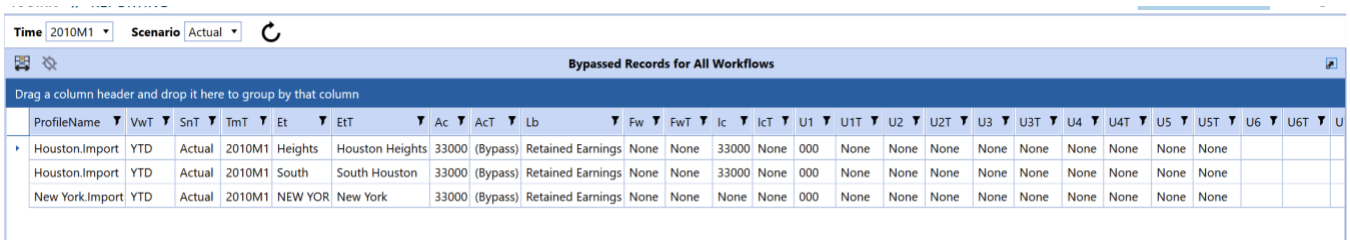
View bypassed records for a specific time, scenario, and workflow profile.



ProfileName	VwT	SnT	TmT	Et	EtT	Ac	AcT	Lb	Fw	FwT	Ic	IcT	U1	U1T	U2	U2T	U3	U3T	U4	U4T	U5	U5T	U6	U6T	U7
Houston.Import	YTD	Actual	2010M1	South	South Houston	33000	(Bypass)	Retained Earnings	None	None	33000	None	000	None	None	None	None	None	None	None	None	None			
Houston.Import	YTD	Actual	2010M1	Heights	Houston Heights	33000	(Bypass)	Retained Earnings	None	None	33000	None	000	None	None	None	None	None	None	None	None	None			

Bypassed Records for All Workflows

View bypassed records for all workflows for a specific time and scenario.



ProfileName	VwT	SnT	TmT	Et	EtT	Ac	AcT	Lb	Fw	FwT	Ic	IcT	U1	U1T	U2	U2T	U3	U3T	U4	U4T	U5	U5T	U6	U6T	U
Houston.Import	YTD	Actual	2010M1	Heights	Houston Heights	33000	(Bypass)	Retained Earnings	None	None	33000	None	000	None	None	None	None	None	None	None	None	None			
Houston.Import	YTD	Actual	2010M1	South	South Houston	33000	(Bypass)	Retained Earnings	None	None	33000	None	000	None	None	None	None	None	None	None	None	None			
New York.Import	YTD	Actual	2010M1	NEW YOR	New York	33000	(Bypass)	Retained Earnings	None	None	None	None	000	None	None	None	None	None	None	None	None	None			

Constraint Violations

View source records related to constraint violations for a specific time, scenario, and workflow profile.

Source/Target Fields – All Dimensions

View source and target fields for all dimensions for a specific time, scenario, and workflow profile.

Time 2010M1 **Scenario** Actual **Workflow Profile** Houston.Import

Source And Target Fields for all Dimensions

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

ProfileName	VwT	SnT	TmT	Et	EtT	Ac	AcT	Lb	Fw	FwT	Ic	IcT	U1	U1T	U2	U2T	U3	U3T	U4	U4T	U5	U5T
Houston.Import	YTD	Actual	2010M1	Heights	Houston Heights	10004	10100	Cash Disbursements - Wells Fargo	None	None	10004	None	000	None	None	None	None	None	None	None	None	None
Houston.Import	YTD	Actual	2010M1	Heights	Houston Heights	10003	10100	Cash Disbursements - Chase Bank	None	None	10003	None	000	None	None	None	None	None	None	None	None	None
Houston.Import	YTD	Actual	2010M1	Heights	Houston Heights	10001	10100	Cash - Operating Chase	None	None	10001	None	000	None	None	None	None	None	None	None	None	None
Houston.Import	YTD	Actual	2010M1	Heights	Houston Heights	10002	10100	Cash - Operating Wells Fargo	None	None	10002	None	000	None	None	None	None	None	None	None	None	None
Houston.Import	YTD	Actual	2010M1	Heights	Houston Heights	11080	10000	Petty Cash	None	None	11080	None	000	None	None	None	None	None	None	None	None	None
Houston.Import	YTD	Actual	2010M1	Heights	Houston Heights	11085	10300	Marketable Securities	None	None	11085	None	000	None	None	None	None	None	None	None	None	None
Houston.Import	YTD	Actual	2010M1	Heights	Houston Heights	11090	10400	Restricted Cash	None	None	11090	None	000	None	None	None	None	None	None	None	None	None
Houston.Import	YTD	Actual	2010M1	Heights	Houston Heights	11200	11000	Trade Receivables - Third Party	None	None	11200	None	000	None	None	None	None	None	None	None	None	None
Houston.Import	YTD	Actual	2010M1	Heights	Houston Heights	11201	11000	Accounts Receivable Trade	None	None	11201	None	000	None	None	None	None	None	None	None	None	None
Houston.Import	YTD	Actual	2010M1	Heights	Houston Heights	11212	62600	Rebillable Expenditures	None	None	11212	None	000	None	None	None	None	None	None	None	None	None

Source/Target with Attribute Fields

View source and target fields with attributes for a specific time, scenario, and workflow profile.

Source/Target with Maps

View source, map, and target fields for a specific time, scenario, and workflow profile.

Time 2010M1 **Scenario** Actual **Workflow Profile** Houston.Import

All Source, Map, and Target Fields for WF Profile

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

ProfileName	SnT	TmT	VwT	Et	EtRuleName	EtRuleType	EtRuleExp	EtT	Ac	AcRuleName	AcRuleType	AcRuleExp	AcT	Fw	FwT	Ic	IcRuleName	IcRuleType
Houston.Import	Actual	2010M1	YTD	Heights	Heights	One-To-One		Houston Heights	10001	CashBalance	Range	10001~10004	10100	None	None	10001	Catch All	Mask
Houston.Import	Actual	2010M1	YTD	Heights	Heights	One-To-One		Houston Heights	10002	CashBalance	Range	10001~10004	10100	None	None	10002	Catch All	Mask
Houston.Import	Actual	2010M1	YTD	Heights	Heights	One-To-One		Houston Heights	10003	CashBalance	Range	10001~10004	10100	None	None	10003	Catch All	Mask
Houston.Import	Actual	2010M1	YTD	Heights	Heights	One-To-One		Houston Heights	10004	CashBalance	Range	10001~10004	10100	None	None	10004	Catch All	Mask
Houston.Import	Actual	2010M1	YTD	Heights	Heights	One-To-One		Houston Heights	11080		Unknown		10000	None	None	11080	Catch All	Mask
Houston.Import	Actual	2010M1	YTD	Heights	Heights	One-To-One		Houston Heights	11085	11085	One-To-One		10300	None	None	11085	Catch All	Mask
Houston.Import	Actual	2010M1	YTD	Heights	Heights	One-To-One		Houston Heights	11090	11090	One-To-One		10400	None	None	11090	Catch All	Mask
Houston.Import	Actual	2010M1	YTD	Heights	Heights	One-To-One		Houston Heights	11200	Accounts Receivable	Range	11200~11201	11000	None	None	11200	Catch All	Mask
Houston.Import	Actual	2010M1	YTD	Heights	Heights	One-To-One		Houston Heights	11201	Accounts Receivable	Range	11200~11201	11000	None	None	11201	Catch All	Mask
Houston.Import	Actual	2010M1	YTD	Heights	Heights	One-To-One		Houston Heights	11212	11212	One-To-One		62600	None	None	11212	Catch All	Mask

Unmapped Records

View unmapped records for a specific time, scenario, and workflow profile.

Time 2010M1 **Scenario** Actual **Workflow Profile** Houston.Import

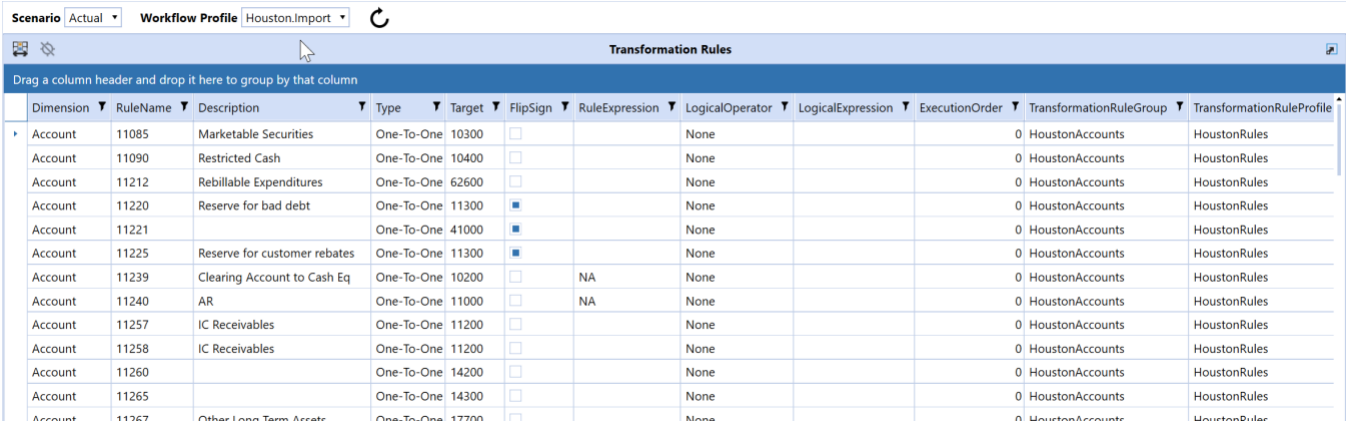
Unmapped Records

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

ProfileName	SnT	TmT	VwT	Et	EtRuleName	EtRuleType	EtRuleExp	EtT	Ac	AcRuleName	AcRuleType	AcRuleExp	AcT	Fw	FwT	Ic	IcRuleName	IcRuleType
Houston.Import	Actual	2010M1	YTD	Heights	Heights	One-To-One		Houston Heights	10001	CashBalance	Range	10001~10004	10100	None	None	10001	Catch All	Mask
Houston.Import	Actual	2010M1	YTD	Heights	Heights	One-To-One		Houston Heights	10002	CashBalance	Range	10001~10004	10100	None	None	10002	Catch All	Mask
Houston.Import	Actual	2010M1	YTD	Heights	Heights	One-To-One		Houston Heights	10003	CashBalance	Range	10001~10004	10100	None	None	10003	Catch All	Mask
Houston.Import	Actual	2010M1	YTD	Heights	Heights	One-To-One		Houston Heights	10004	CashBalance	Range	10001~10004	10100	None	None	10004	Catch All	Mask
Houston.Import	Actual	2010M1	YTD	Heights	Heights	One-To-One		Houston Heights	11080		Unknown		10000	None	None	11080	Catch All	Mask
Houston.Import	Actual	2010M1	YTD	Heights	Heights	One-To-One		Houston Heights	11085	11085	One-To-One		10300	None	None	11085	Catch All	Mask
Houston.Import	Actual	2010M1	YTD	Heights	Heights	One-To-One		Houston Heights	11090	11090	One-To-One		10400	None	None	11090	Catch All	Mask
Houston.Import	Actual	2010M1	YTD	Heights	Heights	One-To-One		Houston Heights	11200	Accounts Receivable	Range	11200~11201	11000	None	None	11200	Catch All	Mask
Houston.Import	Actual	2010M1	YTD	Heights	Heights	One-To-One		Houston Heights	11201	Accounts Receivable	Range	11200~11201	11000	None	None	11201	Catch All	Mask
Houston.Import	Actual	2010M1	YTD	Heights	Heights	One-To-One		Houston Heights	11212	11212	One-To-One		62600	None	None	11212	Catch All	Mask
Houston.Import	Actual	2010M1	YTD	Heights	Heights	One-To-One		Houston Heights	11220	11220	One-To-One		11300	None	None	11220	Catch All	Mask
Houston.Import	Actual	2010M1	YTD	Heights	Heights	One-To-One		Houston Heights	11225	11225	One-To-One		11300	None	None	11225	Catch All	Mask
Houston.Import	Actual	2010M1	YTD	Heights	Heights	One-To-One		Houston Heights	11234	CashDeposits	Range	11234~11238	10100	None	None	11234	Catch All	Mask
Houston.Import	Actual	2010M1	YTD	Heights	Heights	One-To-One		Houston Heights	11238	CashDeposits	Range	11234~11238	10100	None	None	11238	Catch All	Mask

Workflow's Transformation Rules

View all transformation rules for a specific scenario, and workflow profile.



Scenario Actual Workflow Profile Houston.Import

Transformation Rules

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

Dimension	RuleName	Description	Type	Target	FlipSign	RuleExpression	LogicalOperator	LogicalExpression	ExecutionOrder	TransformationRuleGroup	TransformationRuleProfile
Account	11085	Marketable Securities	One-To-One	10300			None		0	HoustonAccounts	HoustonRules
Account	11090	Restricted Cash	One-To-One	10400			None		0	HoustonAccounts	HoustonRules
Account	11212	Rebillable Expenditures	One-To-One	62600			None		0	HoustonAccounts	HoustonRules
Account	11220	Reserve for bad debt	One-To-One	11300	■		None		0	HoustonAccounts	HoustonRules
Account	11221		One-To-One	41000	■		None		0	HoustonAccounts	HoustonRules
Account	11225	Reserve for customer rebates	One-To-One	11300	■		None		0	HoustonAccounts	HoustonRules
Account	11239	Clearing Account to Cash Eq	One-To-One	10200		NA	None		0	HoustonAccounts	HoustonRules
Account	11240	AR	One-To-One	11000		NA	None		0	HoustonAccounts	HoustonRules
Account	11257	IC Receivables	One-To-One	11200			None		0	HoustonAccounts	HoustonRules
Account	11258	IC Receivables	One-To-One	11200			None		0	HoustonAccounts	HoustonRules
Account	11260		One-To-One	14200			None		0	HoustonAccounts	HoustonRules
Account	11265		One-To-One	14300			None		0	HoustonAccounts	HoustonRules
Account	11267	Other Long Term Assets	One-To-One	17700			None		0	HoustonAccounts	HoustonRules

Utilities

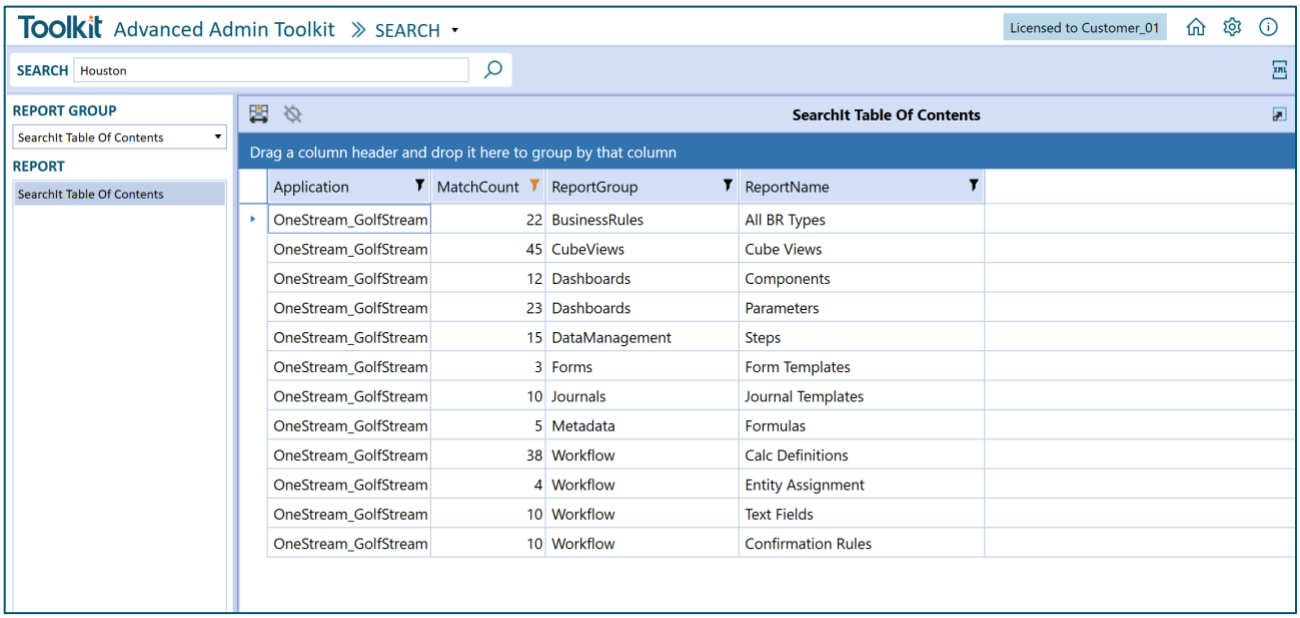
Search

The Search utility is an extremely powerful string searching utility that enables the Admin 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/item, or when substituting one value for another (I.e. Forecast for Budget).

Table of Contents

High-level search to identify the main areas where the string was found.



Toolkit Advanced Admin Toolkit » SEARCH Licensed to Customer_01

SEARCH Houston

REPORT GROUP: SearchIt Table Of Contents

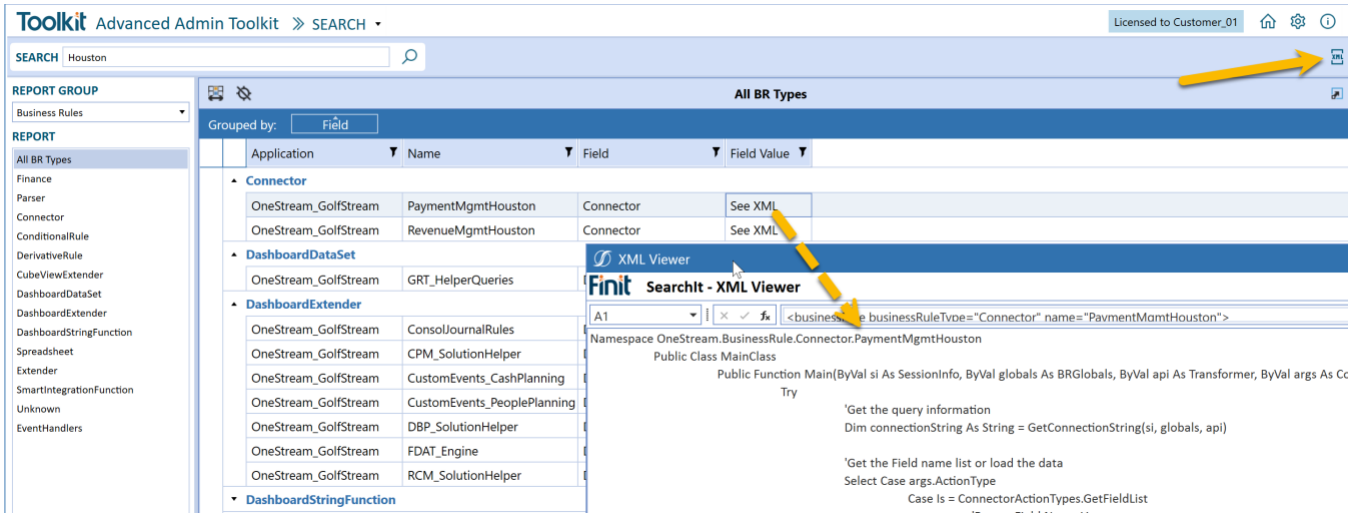
REPORT: SearchIt Table Of Contents

SearchIt Table Of Contents

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

Application	MatchCount	ReportGroup	ReportName
OneStream_GolfStream	22	BusinessRules	All BR Types
OneStream_GolfStream	45	CubeViews	Cube Views
OneStream_GolfStream	12	Dashboards	Components
OneStream_GolfStream	23	Dashboards	Parameters
OneStream_GolfStream	15	DataManagement	Steps
OneStream_GolfStream	3	Forms	Form Templates
OneStream_GolfStream	10	Journals	Journal Templates
OneStream_GolfStream	5	Metadata	Formulas
OneStream_GolfStream	38	Workflow	Calc Definitions
OneStream_GolfStream	4	Workflow	Entity Assignment
OneStream_GolfStream	10	Workflow	Text Fields
OneStream_GolfStream	10	Workflow	Confirmation Rules

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
- XFDoc
- System

Help and Miscellaneous Information

Troubleshooting & FAQs

For the most updated troubleshooting & FAQs, please refer to the Finit Support Portal, https://support.finit.com/.

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 a solution project's implementation documentation 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 Package Name: FFTK_PV7.3.0_SV100_PackageContents.zip

Identifier	Description
FFTK	Solution ID
PV7.3.0	Minimum Platform version required to run solution
SV100	Solution version
PackageContents	File name