onestream

System Administration Guide

9.4.1 Release

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

Overview 1

System Security Roles 2

Application Server Configurations 2

System Roles 3

System Configurations 3

General System Configurations 4

Environment System Configurations 7

Recycling System Configurations 10

Database System Configurations 11

Audits 14

OneStream Database Server Security and SQL Table Access 16

Database Server Security Exposure 16

Provision Database Server Security Roles 17

Security Role Definition 20

Manage System Security 26
Access System Security Roles 26
Manage System Security Users 27
Manage System Security Groups 28
Manage System Security Roles 29
Load and Extract 29
BRApi 30
Combined Roles 30
File Share Security Roles 30
System User Interface Roles 32
System Security Users and Groups 34
Manage Users and Groups Using BRApi Functions 34
International Settings 36
Specify Culture Settings on the Client Machine Operating System 37
Specifying Server Side User Culture Settings 38

Work with System Applications 38
System Dashboards 39
Implementing Security 40
Application Security 40
Security Best Practices 41
Import 46
Forms 46
Adjustments 47
Entity Security 47
Relationship Security 47
Change the Relationship Security 48
Security Configurations 53
System Security 57
Managing a OneStream Environment 58
Disable Inactive Users 59
Set the Inactivity Threshold 59

Review Settings 61

Business Rules 62

System Table 62

How Users are Configured for Authentication 63

About Managing Users and Groups 64

Ways to Add Users and Groups to an Application 64

Create and Manage Users 64

Create and Manage Groups 75

User Culture 83

Alias Dimension Member Descriptions 84

Alias Member Descriptions in Cube Views 85

Alias for Headings: Strings within Dashboard Maintenance Unit 88

Report Alias (Displaying Alternate Descriptions for Members) 91

Report Alias with Spreadsheet and Excel 91

System Tools 97
System Business Rules 97
Sample System Business Rule 98
Database 99
Database Tables 99
Database Administration 101
Key Features 101
Configure Security 101
Enable Database Administration 102
Application Security Roles 103
System Security Roles 103
Database Access Group Security or System Configuration Page 103
Administer Database Tasks 103
Environment 106
Monitoring Environments 107

Specifying General Settings 108
Specifying Monitoring Settings 109
Specifying Metrics Settings 109
Web Servers 111
Configuration 111
Audit 113
Mobile Web Servers 114
Sample Mobile Web Server Configuration 115
Sample Mobile Web Server Audit 115
Web To App Server Connections 116
Work With Application Server Sets 118
Accessing Server Sets Behaviors 119
Server Sets Configuration 120
Using Server Sets Audit 121
Monitoring Server Sets Performance 121
Application Server Behavior 122

Application Server Configuration 123
Application Server Hardware 123
Application Server Audit 124
Application Server Performance 124
Database Servers 125
Behaviors 125
Configuration 126
Hardware 127
Audit 128
Performance 128
Diagnostics 129
OneStream Database Servers (Schema Items) 130
Configuration 130
Audit 131
Diagnostics 131
Azure Configurations 132

Azure Subscription Settings 132
Environment Monitoring 133
Task Load Balancing 137
Database Server Connection 138
Azure Server Sets Settings 139
File Explorer 140
File Share 141
Folders 142
Uploads 147
Supported File Sizes 147
Whitelist File Extensions 148
Overview 148
Whitelist Files Extensions Prerequisites 149
Define the List of File Extensions 149
Add Documents using File Explorer 151
Troubleshooting 152

Conclusion 152

Application Database and System Database 152

Documents 153

Load/Extract System Artifacts 153

Profiler 155

Filter Syntax 161

Profiler Events 162

Event Information 167

BRApi.Profiler Methods 170

Time Dimensions 171

Time Dimension Types 171

Overview

System administration in OneStream is about keeping the platform running securely and reliably. It involves configuring, managing, and monitoring the platform's underlying framework to support efficient operations.

Administrators manage:

- User, group, and role security
- Environment and database configuration
- Application server settings
- Logging and auditing

Tools such as system dashboards and environment monitoring provide insight into:

- System activity
- Task history
- Security audits

These capabilities help administrators control platform behavior, enforce governance, and ensure application reliability.

System Security Roles

The following roles apply to the entire system, not just one application.

Manage System Dashboards: Use to manage all System Dashboards regardless of access to certain Dashboards. This role links the SystemPane Role and the System User Interface Roles section, meaning this security role must include this group in order to be active.

Manage System Database Files: There are two file systems in the Framework database, such as the System database, and each application database. Users with the ManageSystemDatabaseFiles and ManageApplicationDatabaseFiles roles have read and write access to all folders and files in these file systems, respectively. Other users can be given read and write access to specific folders in the database file systems using the folder's security settings. This option ties the FileExplorerPage role from the System User Interface Roles section, meaning this security role must include this group in order to be active.

Manage File Share: The File Share is a Windows folder that Application Servers can read and write. It is configured in the XFAppServerConfig.xml file using the FileShareRootFolder setting. The File Share is a server-side storage area where external systems or IT can stage and upload files. Users with the ManageFileShare role can edit these folders and files using File Explorer.

Application Server Configurations

Application server configurations can be made by administrators and advanced IT users. Common requests that led to support calls can be addressed internally by advanced OneStream users with the required access. This process also eliminates the need for an IIS restart for the changes to take place. Understand that as settings are changed and saved, they are automatically applied every two minutes.

Two system roles manage six categories of configurations. The application maintains an audit trail so changes to the configurations are accessible. After installation, the application server configurations are enabled by default. To mitigate misuse of configuration settings, Customer Support can disable full features, sections, and property changes using XML/App config.

System Roles

Two roles enable administrators and advanced IT users to change server configurations:

System Security Role: ManageSystemConfiguration

- Defaults to Nobody
- Not automatically granted to Administrator

System User Interface Role: SystemConfigurationPage

- Defaults to Administrator Group: Administrators will have read-only rights
- System User Interface Role should be view only to all users assigned

System Configurations

There are six categories of system configurations:

- General
- Environment
- Memory
- Multithreading
- Recycling
- Database Server Connections

> **NOTE:** Memory and Multithreading system configurations must be enabled. You should contact Support to have this configuration change made.

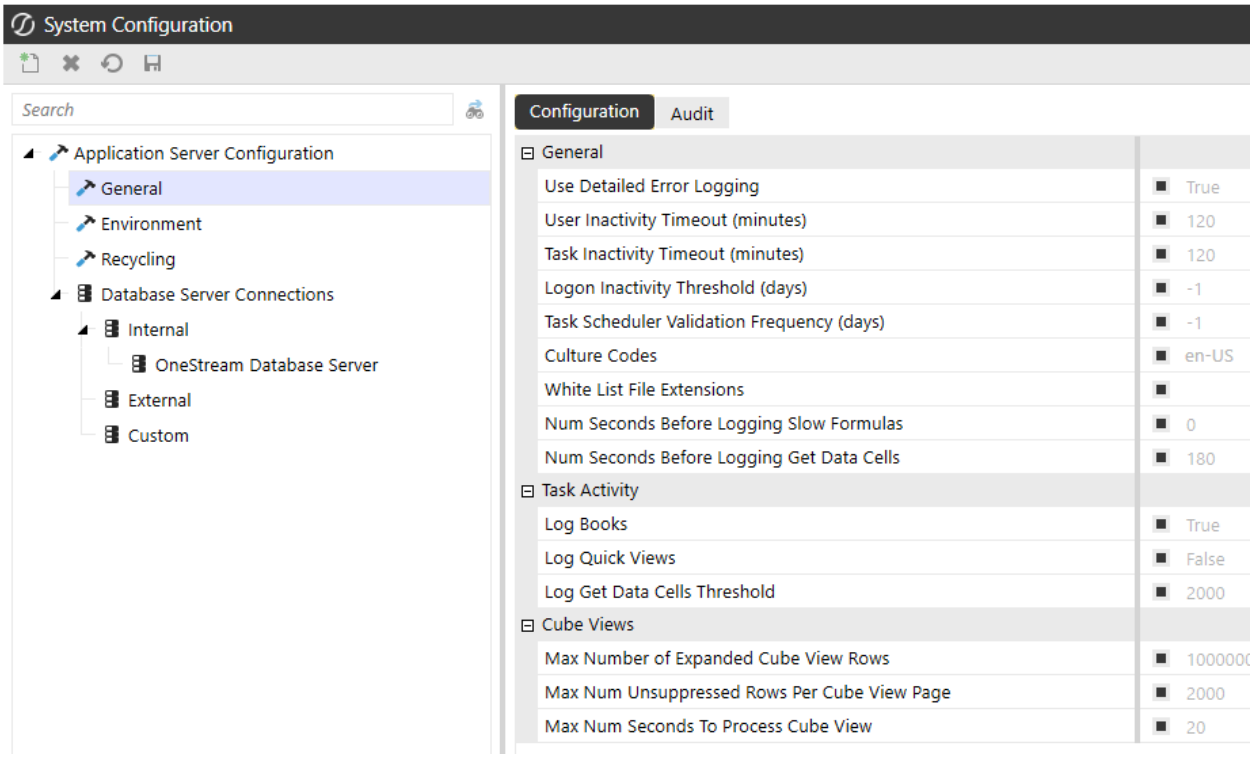
An IIS restart is not required to capture changes as they are automatically applied every two minutes. Saved changes are tracked via the Audit tab, which is available for each server configuration.

When enabled, permitted users can adjust system configurations in app by navigating to **System** > **Administration** > **System Configuration**.

General System Configurations

When the box and setting are gray, the property is set based on the configuration file. Deselect the box to adjust your custom value, then save. This overrides the configuration file. Select the property's box again to default back to the configuration file.

> **NOTE:** Improperly modifying certain server configurations can impact overall environment or application performance. Contact OneStream Support for recommendations.



General Menu

Review the following settings in the General menu:

Use Detailed Error Logging: When set to True, stack trace information is shown. When set to False, stack trace information is not shown.

User Inactivity Timeout (minutes): Set the number of minutes a user is timed out due to inactivity.

Task Inactivity Timeout (minutes): Set the number of minutes a task is timed out due to inactivity.

Logon Inactivity Threshold (days): Set the Logon Inactivity Threshold (days) to the number of days of inactivity before the user can no longer access the system. Set to -1 to disable the setting.

Task Scheduler Validation Frequency (days): Set the number of days in which the Task Scheduler validation runs.

Culture Codes: Set the appropriate code for display settings using the standard Microsoft Local designation for each language. (ex. en-US)

White List File Extensions: When blank, any file type can be saved to a root folder then uploaded. Add custom file types by selecting the box then the ellipsis to restrict the types of files which will be supported in the File Explorer.

Num Seconds Before Logging Slow Formulas: Set the number of seconds before slow formulas are logged. This will enable logging of formulas and impact consolidation performance. Disable when no longer required.

Number Seconds Before Logging Get Data Cells: Set the number of seconds before Get Data Cells are logged. The default is 180 and should only be increased for debugging purposes.

Task Activity Menu

Review the following settings in the Task Activity menu:

Log Books: When set to True by default, a log is created in Task Activity when the items are included as Task Activity steps for that specific book. The intention of this feature is to verify entries in the Task Activity grid and the settings in the configuration file work as expected.

Log Quick Views: When set to True, a log is created in Task Activity when a new Quick View is created or when rows or columns are moved around. The intention of this feature is to analyze data analysis performance.

Log Get Data Cells Threshold: This logs the calls to GetDataCells and GetDataCellsUsingScript. It includes context information such as the Excel file name or the Cube View name. It only creates logs if the number of Data Cells being requested is equal to or greater than the value provided in this field.

Cube Views Menu

The Cube View configurations will impact all Cube Views in an application environment. They are designed to optimize the Cube View performance through managing the page size and initiating paging which will maximize the availability of server resources. These settings can be overridden to customize the design and performance of a specific Cube View, using the General Settings, Common and Paging properties found on each Cube View.

Max Number of Expanded Cube View Rows: Set the max number of rows displayed when using an expanded Cube View.

Max Number of Unsuppressed Row Per Cube View Page: The default value of 2000 is used, which is determined by the settings in the OneStream Server Configuration Utility. The maximum value is 100,000 rows. If the Cube View performs well but you want 2500 rows to display, for example, so that an item in the tree appears on the first page, increase this value.

Max Number Seconds To Process Cube View: This setting impacts paging behavior. The default value of 20 will be used which is determined by the OneStream Server Configuration Utility. The maximum value is 600 seconds.

Environment System Configurations

The configurations allow the Administrator to customize the environment login process for the user by providing a custom label or by triggering an acceptance criteria after each login.

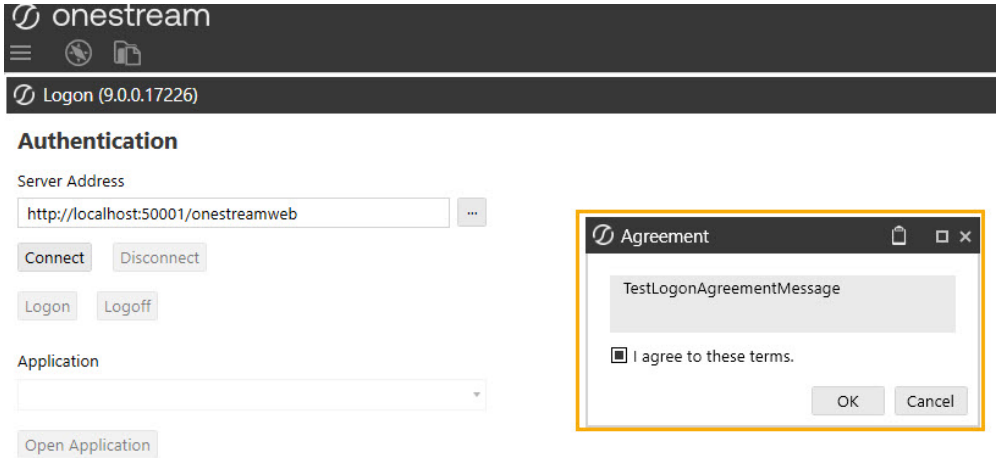


Environment Name: Enter the name to be displayed for the environment. You can enter up to 150 characters.

Environment Color: Specify a provided environment color or enter a hex value to display the name on a colored background.

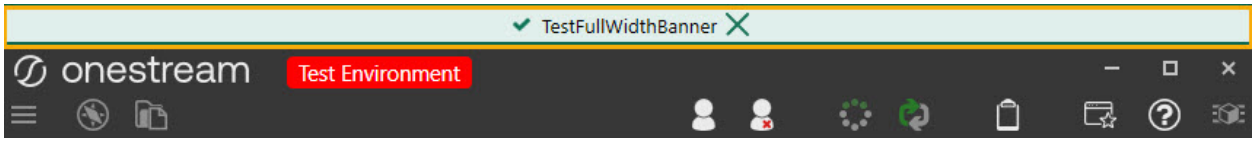
Logon Agreement Type: To display a specific message after a user logs in, select **Custom** and enter the message text.

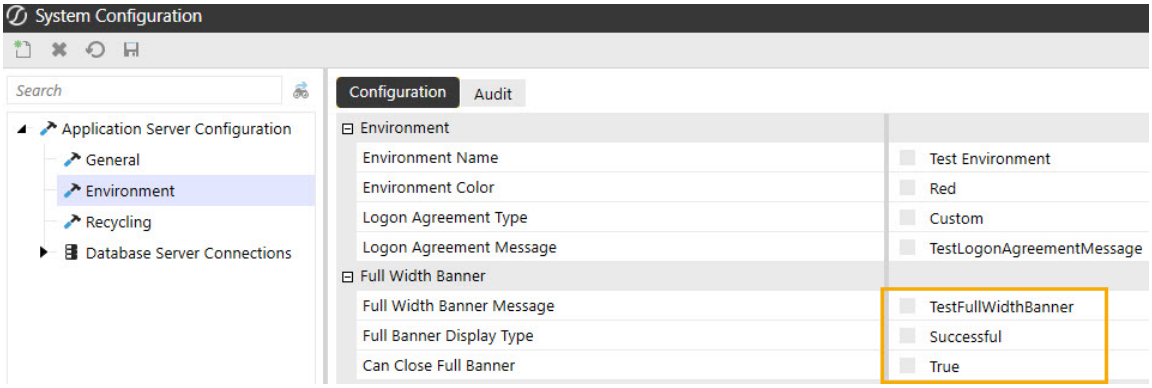
Logon Agreement Message: Enter the message text.



Full Width Banner

The configurations enable you to display information across the top banner indicating varying levels of severity. The banner can be permanently displayed or dismissible.





Full Width Banner Message: Enter the banner message text to display.

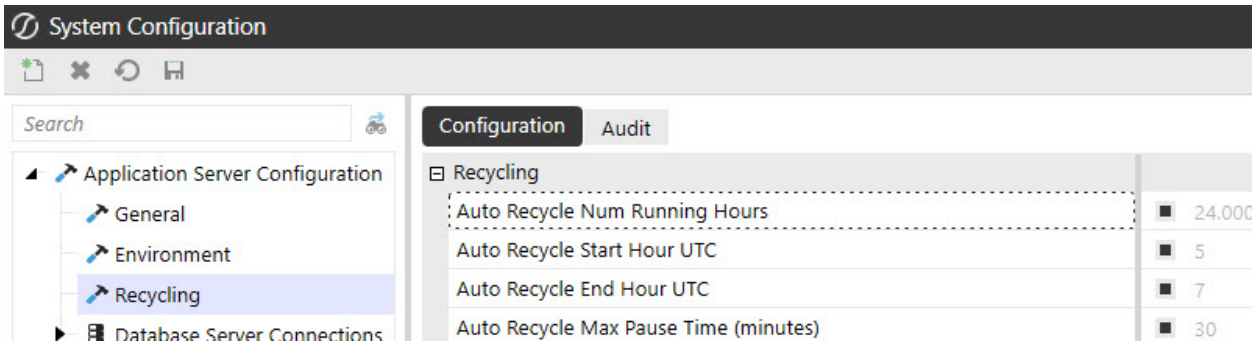
Full Banner Display Type: Indicate the severity of the message by selecting Informational, Warning, Successful, or Critical from the drop-down menu.

Type	Sample
Informational	Informational Banner Sample Text
Warning	Warning Banner Sample Text
Successful	Successful Banner Sample Text
Critical	Critical Banner Sample Text

Can Close Full Banner: When set to True, the banner may be dismissed after log in. When False, the banner cannot be dismissed.

Recycling System Configurations

Over time, server memory may become fragmented, which can affect performance and stability. The default configuration of a daily recycling process is standard. The System Configuration page allows the administrator to customize when these events occur to best suit their implementation.



Recycling Menu

Review the following settings in the Recycling menu:

Auto Recycle Num Running Hours: Default is 24, which means once a day, the server will recycle. Automatic Recycling allows Application Servers a chance to recycle, which is a recommended practice. These first four settings control this behavior.

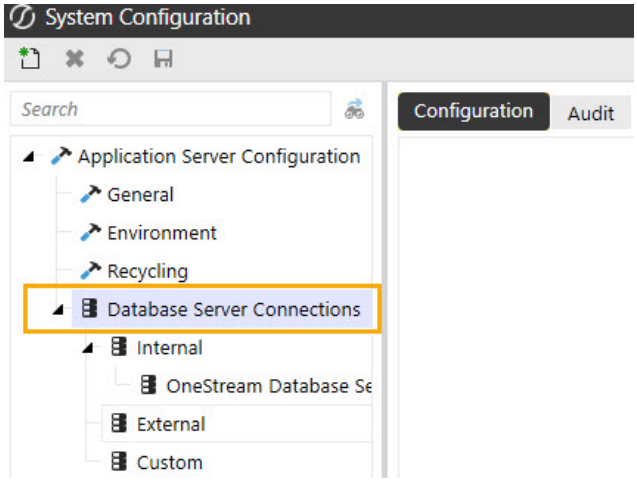
Auto Recycle Start Hour UTC: Default is 5, which means 05:00 UTC time. This is the earliest time in a day when a server can automatically recycle. It is best to set this and the End Hour to be a range of time with the lowest amount of Application Server activity.

Auto Recycle End Hour UTC: Default is 7, which means 07:00 UTC time. This is the latest time in a day when a server can automatically recycle.

Auto Recycle Max Pause Time (minutes): Default is 30, which means that when it is time to recycle a server automatically, it will first pause from accepting more server tasks, but allow for existing assigned tasks to complete processing for 30 minutes before recycling. If there are no active tasks for this server, it will recycle when the time comes.

Database System Configurations

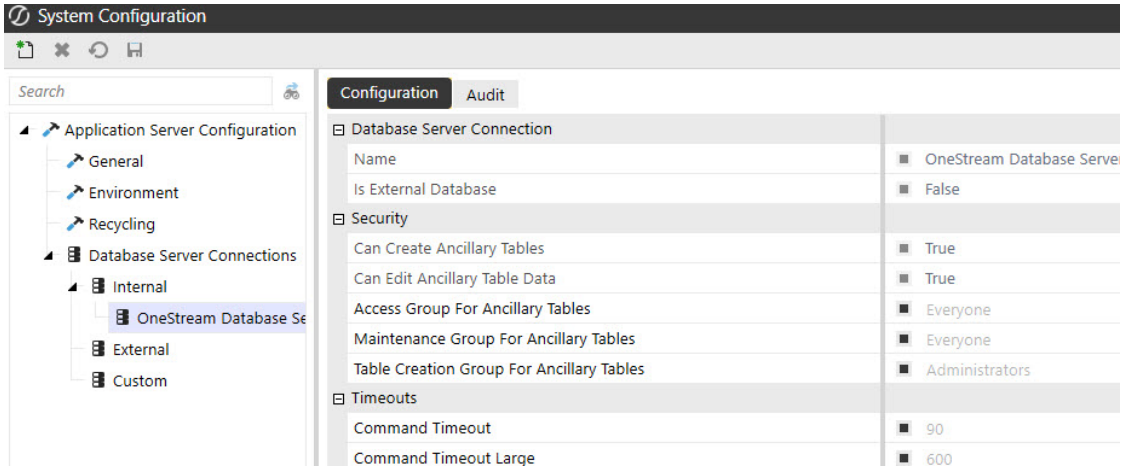
The Database Server Connections provides the administrator with greater visibility into the structure of their environment. Additionally, the administrator can quickly and easily establish database connections to support their model's design requirements.
An IIS restart is not required to capture changes because they are automatically applied every two minutes. Saved changes are tracked using the Audit tab, which is available for each server configuration.



Database Server Connections

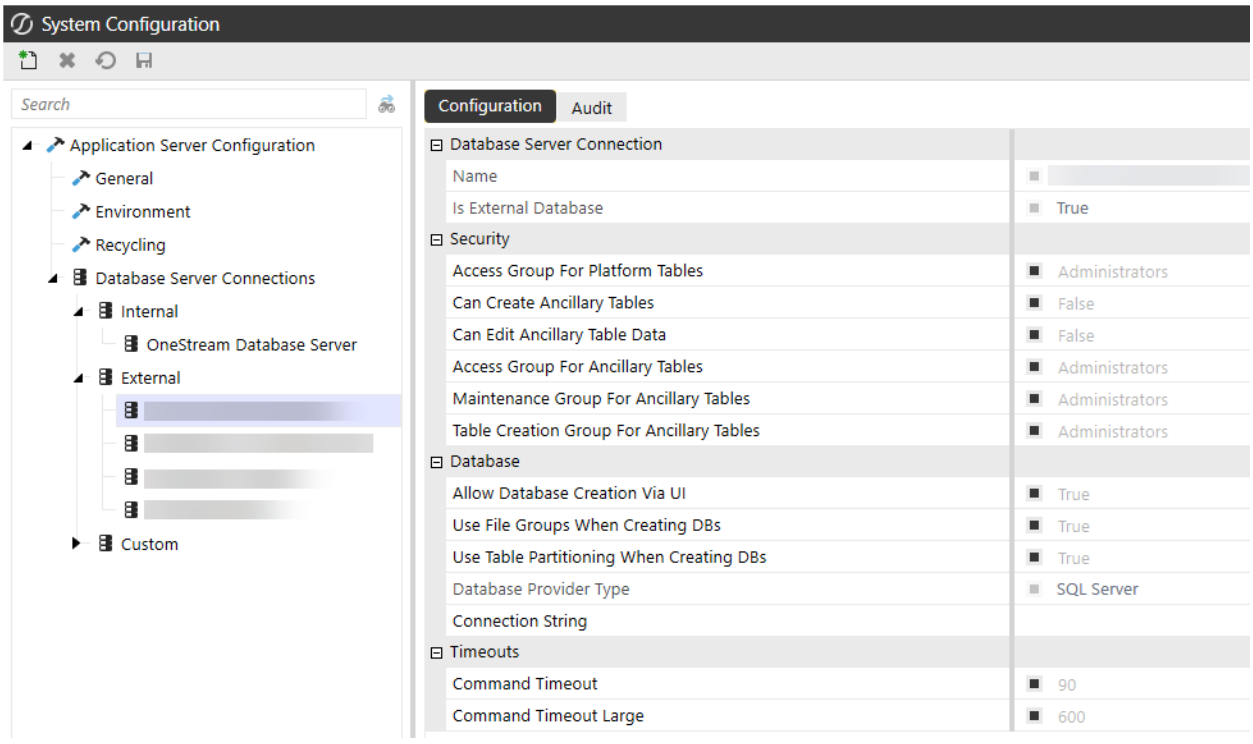
Internal Menu

Configure Database Server Connection, Security, and Timeouts settings from this menu.



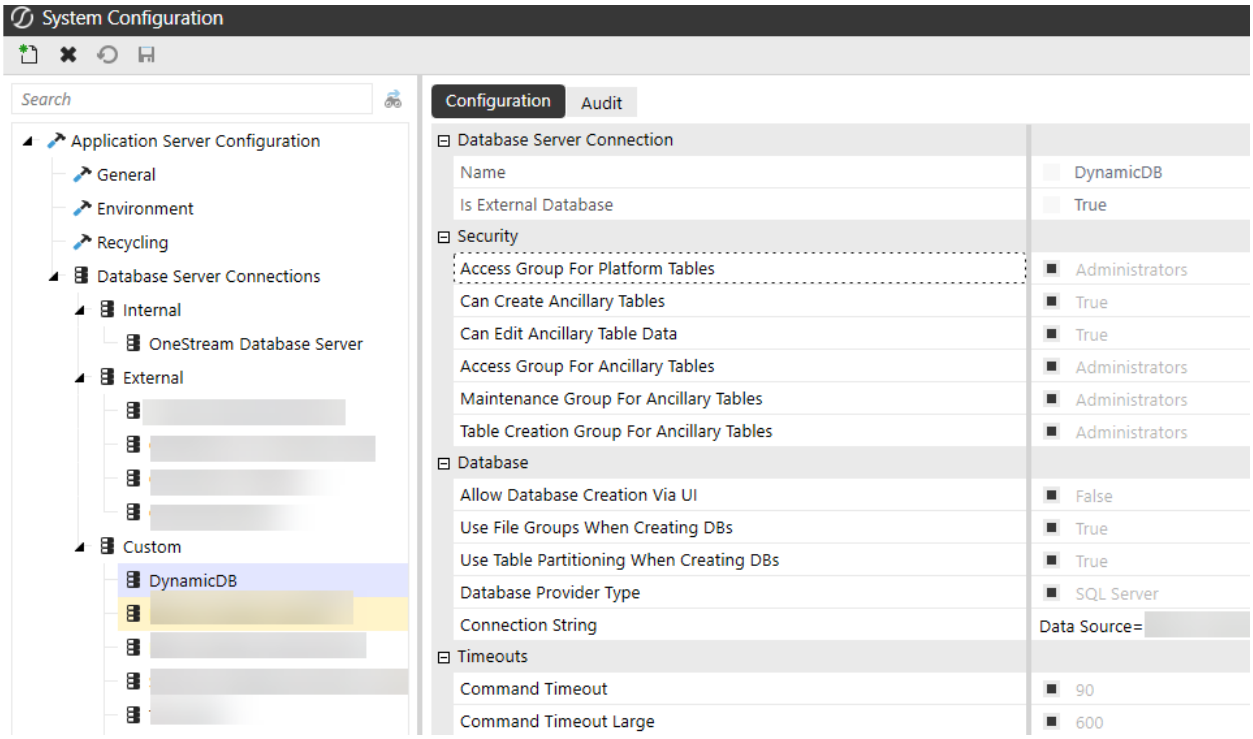
External Menu

Configure Database Server Connection, Security, Database, and Timeouts settings from this menu.



Custom

Configure Database Server Connection, Security, Database, and Timeouts settings from this menu.



Only the External connections and the Connection String property are visible without displaying the password, and you can edit the connection string.

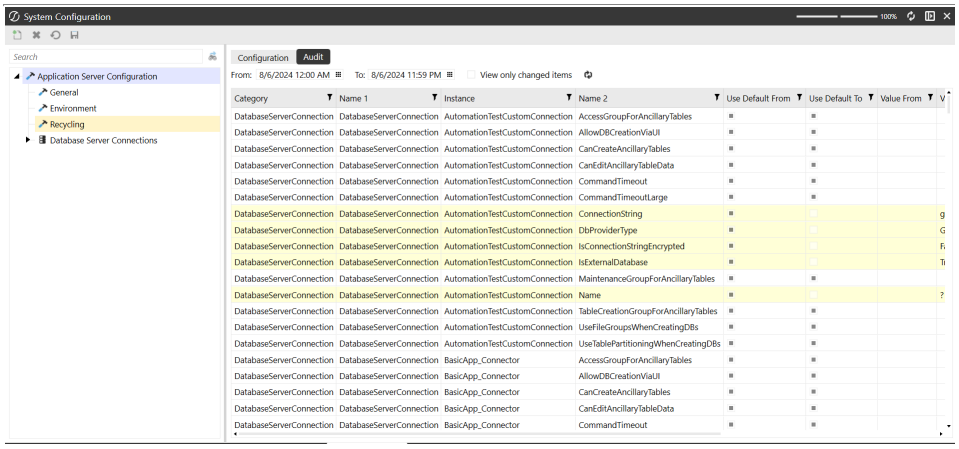
- Connection String will allow for Edits
- Connection String will display “?” where password is used
- Connection String can be modified without changing password and saved with “?” not overriding original password
- Connection String password can be modified and upon save will display “?”

- Connections Strings using the following will be masked: pwd; pass; password
- All others will display password and need to be addressed separately. The majority of connection strings password will be handled above

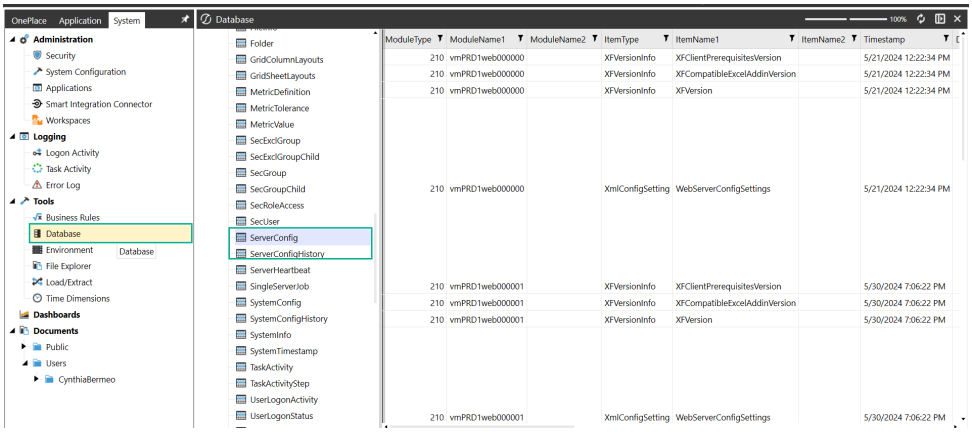
Pre-existing External Connections, when moving over to Customer Connections, should use the previous name to avoid breaking any connections with Task Scheduler or Business Rules.

Audits

Configuration setting changes are tracked using the Audit tab. View changes by navigating to **System** > **System Configuration** > **Audit**.

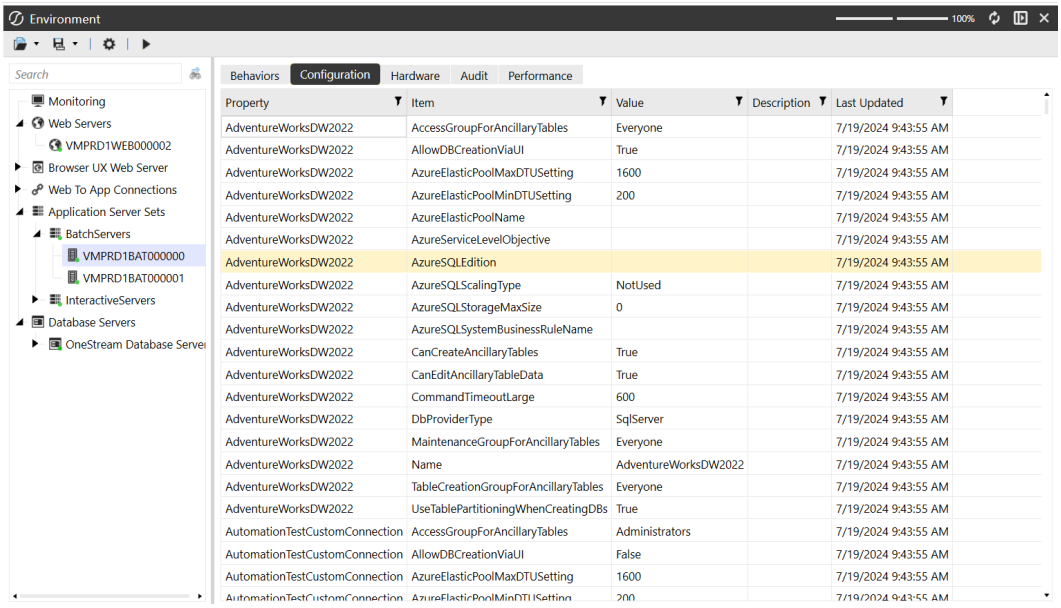


System Database Tables audits are viewed by navigating to **System** > **Tools** > **Database** > **SystemConfig**.



The environment will show what settings the server is currently using. The server updates every two minutes. Here, the user can see what settings are being picked up. The Last Updated column shows the date and time settings were changed. Regardless of what type of connection, such as Internal, External, or Custom, any available configurations that can be changed will show up here.

Environment audits are viewed by navigating to **System** > **Tools** > **Environment** > **Application Server Sets**.



OneStream Database Server Security and SQL Table Access

Database Server Security is a foundational configuration that should be carefully considered during environment design. The associated security roles provide a mechanism for provisioning access to the SQL Table Editor Dashboard Component utilized by certain Solution Exchange solutions, as well as granting users access to content available within the Database Page.

These security properties support role-based provisioning and privilege segregation for database administrators, application administrators, and general users. They control access to Platform, Ancillary, and external database tables and the records in the Database Page and to SQL Table Editor content shown in Dashboards. Database Security can be configured and applied to all databases in each OneStream environment.

- Internal OneStream Database Server
- External or Custom Database Server Connections

Database Server Security Exposure

- **OneStream System Tools Database Page**: Provides access to OneStream database tables to support data management, troubleshooting, and system monitoring
- **OneStream Dashboard Component SQL Table Editor**: Displays SQL table data in a dashboard grid where you can view, filter, sort, and update table data. It also validates access using the Database Server Ancillary Table security properties.

The Security properties allow provisioning of the database content to be segregated across users in the OneStream environment.

For example, you can:

- Segregate duties of the Database Administrator from the Application Administrator
- Enable power users to access the Database Page, but restrict them from accessing sensitive data stored in a solution table
- Segregate access of theOneStreamAdministrator, or other groups, from viewing or editing database table content presented using the SQL Table Editor in a Dashboard

Provision Database Server Security Roles

OneStreamSecurity Groups are used to provision users to each of the Database Server Security roles. The group assignment field supports a custom syntax that allows provisioning logic to be scoped to individual tables or logically associated groups of tables.

Use the custom syntax option to segregate table access within each type of role. For example, within the Platform tables, a group of users can be granted access to view Member tables but be restricted from accessing Data Record tables.

By default, the OneStream Administrators security group does not have permission to the Database Server Security properties. Members must be explicitly provisioned unless access segregation is required.

⊟ Database Server Connection	
Name	OneStream Database Server
Is External Database	False
⊟ Security	
Access Group For Platform Tables	Administrators
Can Create Ancillary Tables	True
Can Edit Ancillary Table Data	True
Access Group For Ancillary Tables	Administrators
Maintenance Group For Ancillary Tables	Administrators
Table Creation Group For Ancillary Tables	Administrators
⊟ Timeouts	
Command Timeout	90
Command Timeout Large	600

Provision Groups

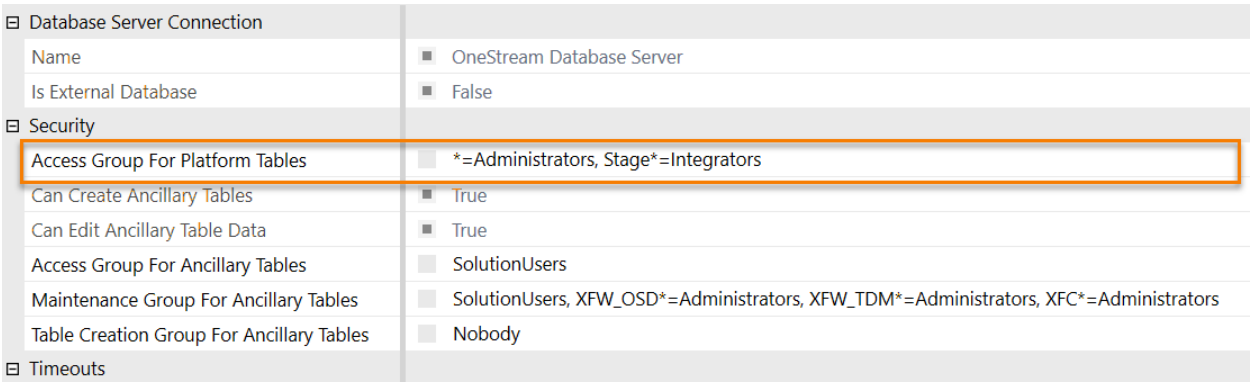
Provisioning of Database Server connections is completed using the System Configuration page.

The System Configuration page initially shows the default security role group defined in the Application Server Configuration file. To override this setting, deselect the role and enter a OneStream Security Group in the text box.

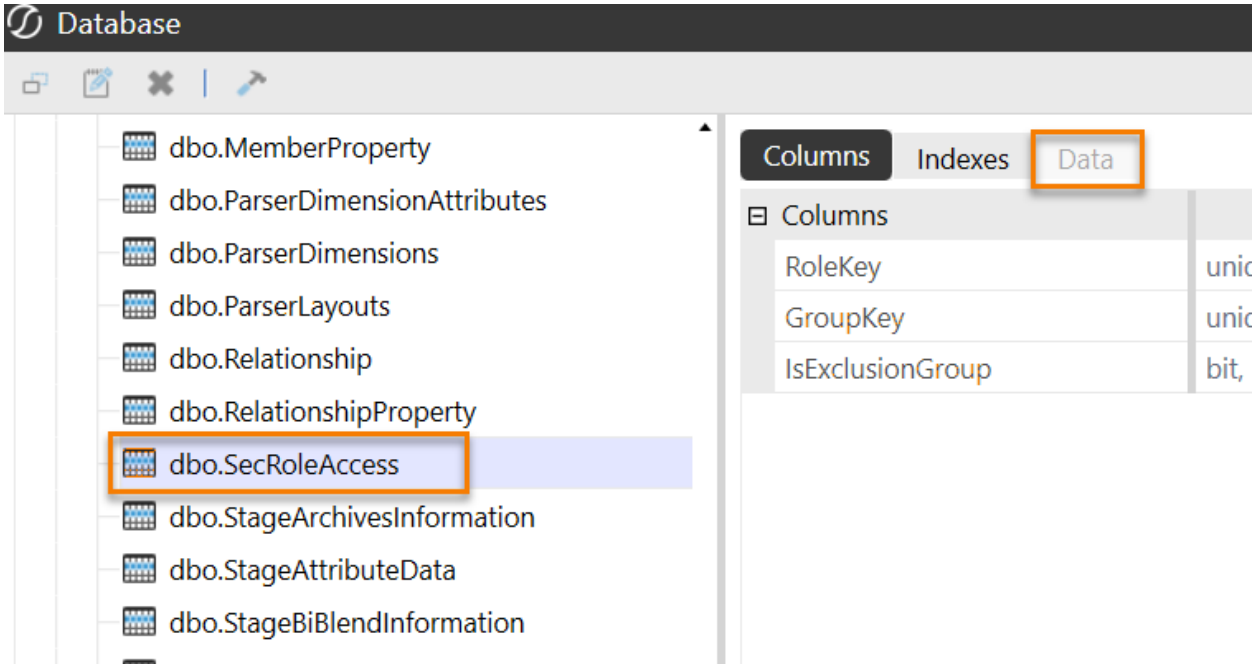
The assignment of Groups to the Security Roles can be designed to grant access or segregate access using table names, wildcard characters, and characters in a comma-delimited list of definitions associated to valid Security Groups.

- When the Database Page, Tools, or Data Records utility is required, you must have access to all Platform Tables on the Access Group for Platform Tables property.
- Nested Groups must be used to provision Groups needing to share the same table access. For example: “*=Administrators, *=PlanningAdmins” is not valid.
- Syntax Examples: * = Security Group, Table* = Security Group, *Table* = Security Group

Security Group Assignment Syntax	Results
AppAdmins	“AppAdmins” Group provisioned to all tables
*=AppAdmins	“AppAdmins” Group provisioned to access all tables
=AppAdmins, Stage=Integrators	“AppAdmins” Group provisioned to access all tables. “Integrators” Group access restricted to table names starting with “Stage”
=AppAdmins, Stage=Integrators, *DataRecord*=Nobody	“AppAdmins” Group provisioned to access all tables. “Integrators” Group access restricted to table names starting with “Stage”. Data Record Tables are restricted for everyone



The table names are always visible in the Database Page. However, the visibility of content on the Data tab will vary depending upon provisioning.



Security Role Definition

Here, we will define Security Roles.

Access Group for Platform Tables

The Access Group for Platform Tables property applies to core Platform tables in the application database. These tables are part of the system architecture and store metadata, transactional data, and system operations.

OneStreamDatabase Server tables are view-only and cannot be edited in the SQL Table Editor.

This property is not supported for external database connections.

- Application Database core Platform tables
- System Database core Platform tables

Ancillary Tables

Ancillary tables are not part of the core Platform schema. They are custom tables created by users or administrators to support business requirements, custom solutions, or Solution Exchange applications. These tables can reside in the Application or System database.

When configuring Database Security Roles for external or custom databases, for example, BI Blend, only Ancillary Security Roles apply to access tables and views in the Database page and SQL Table Editor.

Access Group for Ancillary Tables

The Access Group for Ancillary Tables enables you to view the content of Ancillary tables stored in the Application, System, External, or Custom databases using the Database Page or via the SQL Table Editor in a Dashboard.

Maintenance Group for Ancillary Tables

The Maintenance Group for Ancillary Tables is required to enable the**Allow Inserts**, **Allow Deletes**, and **Allow Updates** functionality found on the SQL Table Editor.

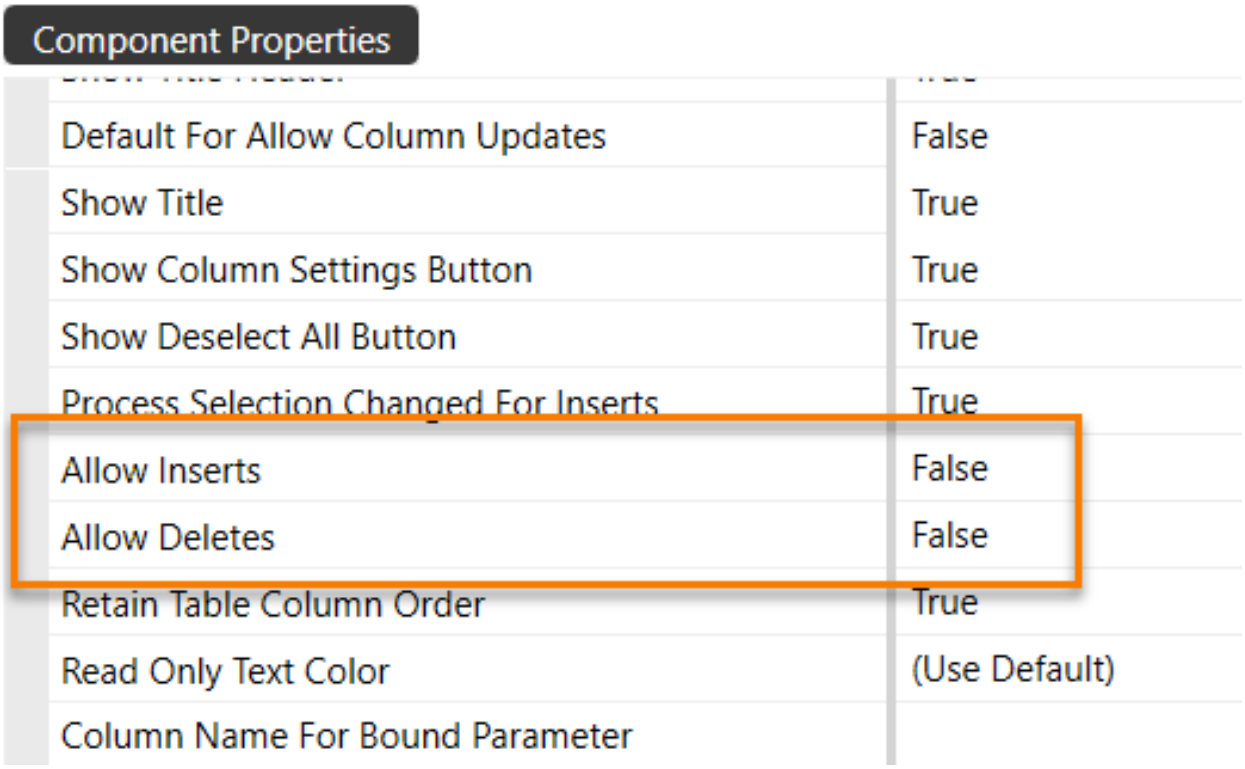
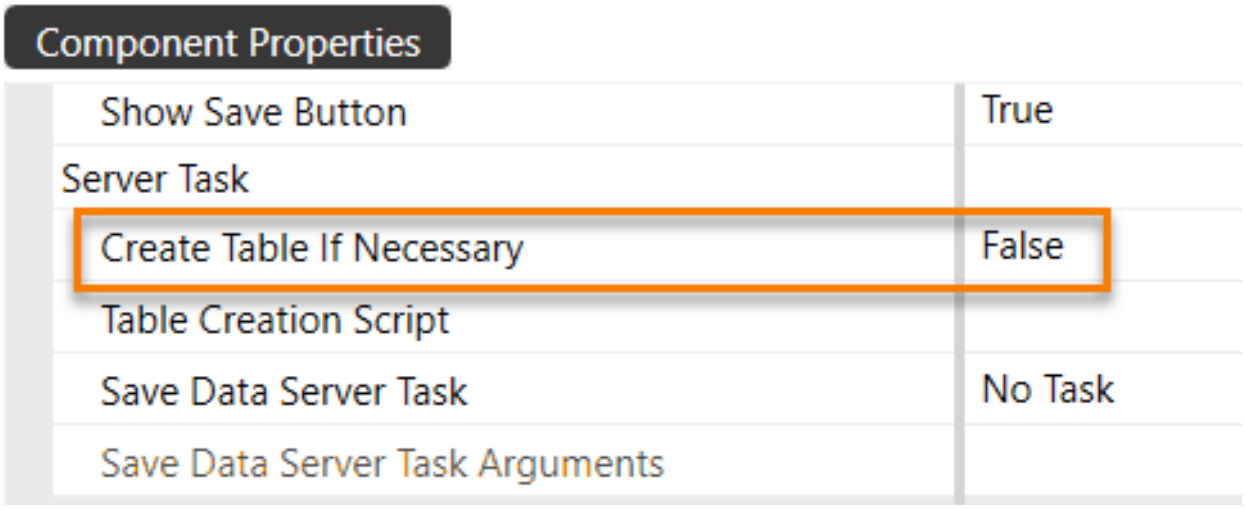




Table Creation Group for Ancillary Tables

The Table Creation Group for Ancillary Tables is required to enable the **Create Table If Necessary** functionality found in the SQL Table Editor.



Administrators Group Segregation for the OneStream Database Server

By default, the OneStream Administrators security group does not have access to Database Server Security properties.OneStreamenvironments include Solution Exchange solutions used by Administrators that require ongoing maintenance. To restrict access to Ancillary Tables used by these solutions, use nested groups, a delimited list, or wildcard methods.

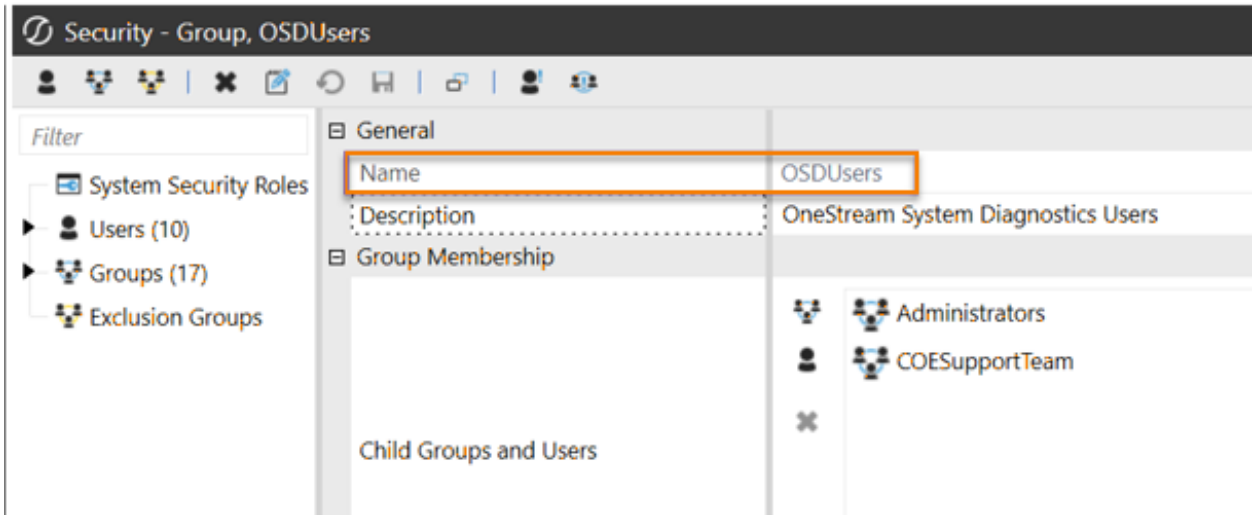
Examples of Minimal Provisioning for Pre-Configured Solutions

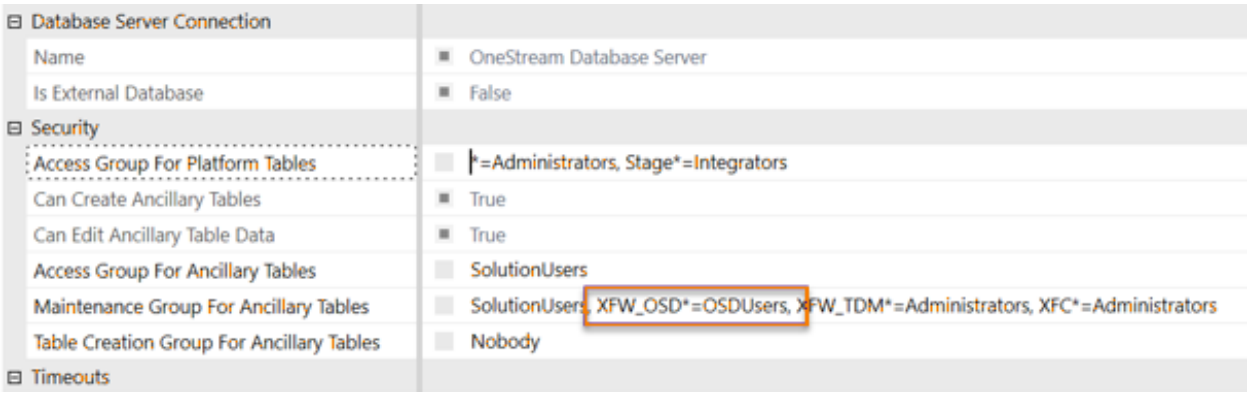
- OneStream System Diagnostics (OSD): XFW_OSD* tables as XFW_OSD*=Administrators
- OneStream Table Data Manager (TDM): XFW_TDM* tables as XFW_ TDM*=Administrators
- XFC* tables as XFC*=Administrators: CustomName* tables as Prefix*=Administrators

Administrator Ancillary Table Access OSD or TDM Example

⊟ Database Server Connection	
Name	OneStream Database Server
Is External Database	False
⊟ Security	
Access Group For Platform Tables	*=Administrators, Stage*=Integrators
Can Create Ancillary Tables	True
Can Edit Ancillary Table Data	True
Access Group For Ancillary Tables	SolutionUsers
Maintenance Group For Ancillary Tables	SolutionUsers, XFW_OSD*=Administrators, XFW_TDM*=Administrators, XFC*=Administrators
Table Creation Group For Ancillary Tables	Nobody
⊟ Timeouts	

Nested Group Ancillary Table Access Example





How To Provision Rights to the System Configuration Page

Limit access to the System Configuration Page to full OneStream Administrators because changes on this page can affect the OneStream environment.

- Navigate to the **System** tab
- Select **System Security Roles**
- Provision full OneStream Administrator to System Configuration Page
    - System Security Roles: **ManageSystemConfiguration**
- Provision non-full OneStream Administrators to System Configuration Page
    - System Security Roles: **ManageSystemConfiguration**, to enable editing
    - System User Interface Roles: **SystemPane**
    - System User Interface Roles: **SystemConfigurationPage**

Administer Database

- Users provisioned for the **Administer Database** feature in the **Database Page** have unrestricted access to Platform and Ancillary tables, which override Database Server security properties see Database Administration.

Manage System Security

Manage System Security allows non-administrators to manage users, roles, and groups and facilitates a comprehensive, function-specific way to separate user and group responsibilities.

By default, administrators have access to all security roles. Assigning other groups to roles does not remove an administrator's complete system access. Users with Manage System Security roles can access to the System User Interface Roles of SystemAdministrationLogon and SystemPane.

Roles are not exclusionary or limiting. If granted, users can get additional functionality through their membership in groups having corresponding role assignments. See System Security Roles.

For example:

- A member of the IT team who is not an administrator might need to manage the system security roles.
- An employee in the Accounting department who reports to the Controller over consolidations may manage groups and not need access to other areas of the system.

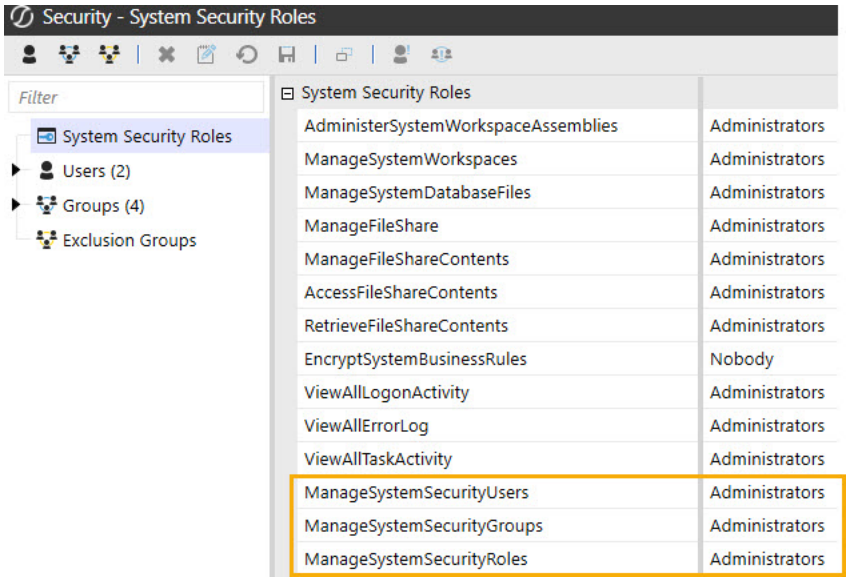
You can delete these security roles to non-administrators:

- **ManageSystemSecurityUsers**: Grants permission to manage users.
- **ManageSystemSecurityGroups**: Grants permission to manage groups, exclusion groups and group membership.
- **ManageSystemSecurityRoles**: Grants permission to manage system security role assignment.

Access System Security Roles

Follow the steps to access system security roles:

1. From the System tab, go to **Administration** > **Security**.
2. Select **System Security Roles**.



Manage System Security Users

This role enables you to:

- Create users
- Modify users
- Delete users
- Disable users

This role enables you to specify these user properties:

- General
- Authentication
- Preferences
- Custom Text

Limitations

Users with the Manage System Security role cannot create, modify, or delete administrators, directly or indirectly. Also, they cannot:

- Add or remove themselves to or from groups or roles.
- Delete themselves.
- Add other users to Manage System Security privileges.
- Add or remove groups they are members of from roles.

To manage group membership or copy users, the **ManageSystemSecurityGroup** is required.

Manage System Security Groups

This role lets you manage groups and exclusion groups. You can also:

- Add or remove members to or from groups and exclusion groups.
- Copy groups, except groups with administrator privileges.

Limitations

Users with this role cannot:

- Modify the Administrators group.
- Assign users to a group that establishes administrator privileges.
- Modify your membership in other groups.
- Modify the parent group of a group in which the user is a member.

Manage System Security Roles

This role lets you manage system security roles. However, you cannot:

- Modify the **ManageSystemSecurityRole** itself because it requires administrator level privileges.
- Assign the Everyone or Nobody groups that require administrator level privileges.
- Add a group to a role of which you are a member.

Load and Extract

Load and Extract functionality of Security requires a user to have permissions for all three of the Manage System Security roles, as well as the System User Interface Roles of **SystemLoadandExtractPage**.

The controls limiting Manage System Security user's capabilities is enforced during the Load and Extract process. Validation occurs by comparing the current state of security in the target environment to the changed state determined by the processing of the source file. Therefore, the validation of XML loads for Manage System Security users requires that security is pre-existing to determine the changed state.

For example, although Manage System Security users cannot create administrators, if the current Administrator Groups existed in the target environment prior to the XML load, then the XML will pass the validation and will be loaded. However, when an empty or new environment exists with no pre-existing users and groups, then an administrator would need to perform the load.

BRApi

You can manage user and group system security using BRApi functions such as CopyUser, DeleteUser and CopyGroup. These are controlled by the assigned Manage System Security role. See System Security Users and Groups.

> **Example:** If a dashboard is created to insert new users, and a dashboard button executed a BRApi to insert a user, the system validates that the user clicking the button is in the Administrators Group or has role permission to ManageSystemSecurityUsers.

Combined Roles

When you have access to more than one of these roles, you gain more functionality within the scope of the designed capabilities and restrictions. For example, if you have both the role of users and groups, you can copy a user or you can also can add a user to a group. Certain functionality requires assignment of combined roles, such as Load and Extract.

File Share Security Roles

The following are file share security roles:

ManageFileShareContents

- Exposes the Contents folder in File Explorer\FileShare under Application and System.
- Grants full rights to create, upload, download, and delete folders.

AccessFileShareContents

- Exposes the Contents folder in File Explorer\FileShare under Application and System.
- Only allows the ability to see the Contents folder and its sub-files, and allows download.

RetrieveFileShareContents

- The Contents Folder is not exposed to the user in the File Share for Application or System using the File Explorer.
- All files are accessible through the OneStream application, such as through dashboards and business rules.

See "Application Security Roles" in the *Application Tools Guide* for more information on application-based security roles.

Encrypt System Business Rules

This allows a user to encrypt or decrypt a rule from the Business Rule page in the System tab to hide the contents of the rule from all users. See "Business Rules" in the *Application Tools Guide* for more information on Business Rule Encrypt (Decrypt) functionality and use.

View All Logon Activity

If assigned the required access to view the System tab and the Logon Activity page, users in the assigned security group can see the login activity for all users in the environment.

View All Error Log

If assigned the required access to view the System tab and the Error Log page, users in the assigned security group can see the Error Log for all users in the environment.

View All Task Activity

Users in the assigned security group can view the tasks and detailed child steps through the Task Activity icon in the toolbar. If they have access to the System tab and page, they can also see this information in the Task Activity page.

System User Interface Roles

The following roles grant access to key features and tools.

SystemAdministrationLogon
This is for the System Administration application and set to Administration by default. When a security group is assigned to this role, it becomes available in the Application list during log in.

SystemPane
Based on the security group chosen, this role lets you access the System Tab found at the bottom left of the screen. By default, only administrators have access to this tab.

ApplicationAdminPage
Based on the security group chosen, this role lets you access the Application tab at the bottom left of the screen. By default, only administrators can access this tab.

SecurityAdminPage
Based on the selected security group, this role lets you view but not modify security artifacts and settings other than your password on **System** > **Administration**. By default, only administrators have access to this section.

DatabasePage
This role lets you access the Database Page on **System** > **Tools**. By default, only system administrators have access to this section.

FileExplorerPage

Based on the selected security group, this role lets you access the File Explorer on System >Tools. This section ties to the ManageSystemDatabaseFiles and ManageFileShare roles. By default, only administrators can access the File Explorer.

SystemLoadExtractPage

Based on the security group chosen, this role lets you access Load/Extract on **System** > **Tools**but you cannot actually import or extract items. By default, only administrators have access to this section.

ErrorLogPage

Based on the security group chosen, this role lets you access Error Log on **System** > **Logging**. By default, only administrators can access to this section.

LogonActivityPage

Based on the selected security group, this role lets you access to Logon Activity on **System** > **Logging**. You can view all users, but cannot log them off. By default, only administrators have access to this section.

TaskActvityPage

Based on the selected security group, this role lets you access Task Activity in **System** > **Logging**. By default, only administrators can access to this section.

TimeDimensionPage

Based on the security group chosen, this will allow a user access to the Time Dimension on **System** > **Tools**. By default, only administrators have access to this section.

System Security Users and Groups

Administrators go to **System** > **Administration** > **Security** to define and manage users, groups, and system security roles. Users, groups, and roles are not application-specific. See Create and Manage Groups and Create and Manage Users.

Every user must be assigned a user ID. Users can be added as native users or as references to users stored in external repositories such as Active Directory. Users can be externally authenticated with these standard providers:

- LDAP
- MSAD
- Okta
- PingFederate
- Azure AD (Microsoft Entra ID)
- SAML

For information about external authentication with standard providers, see the *Installation and Configuration Guide*.

Manage Users and Groups Using BRApi Functions

Administrators can manage users and groups with the following BRApi functions:

```
BRApi.Security.Admin.GetUsers

BRApi.Security.Admin.GetUser

BRApi.Security.Admin.GetUser

BRApi.Security.Admin.SaveUser

BRApi.Security.Admin.RenameUser

BRApi.Security.Admin.DeleteUser
```

BRApi.Security.Admin.CopyUser

BRApi.Security.Admin.GetGroupsAndExclusionGroups

BRApi.Security.Admin.GetGroups

BRApi.Security.Admin.GetGroup

BRApi.Security.Admin.GetGroupInfoEx

BRApi.Security.Admin.SaveGroup

BRApi.Security.Admin.RenameGroup

BRApi.Security.Admin.DeleteGroup

BRApi.Security.Admin.CopyGroup

BRApi.Security.Admin.GetExclusionGroups

BRApi.Security.Admin.GetExclusionGroup

BRApi.Security.Admin.SaveExclusionGroup

BRApi.Security.Admin.RenameExclusionGroup

BRApi.Security.Admin.DeleteExclusionGroup

BRApi.Security.Admin.CopyExclusionGroup

BRApi.Security.Admin.GetSystemRoles

BRApi.Security.Admin.GetApplicationRoles

BRApi.Security.Admin.GetRole

BRApi.Security.Admin.CopyExclusionGroup

Examples

```
Get a UserInfo object and change the User Description
    Dim objUserInfo As UserInfo = BRApi.Security.Admin.GetUser(si, "Administrator")
    If Not objUserInfo Is Nothing Then
        objUserInfo.User.Description = "New Description"
        BRApi.Security.Admin.SaveUser(si, objUserInfo.User, False, Nothing,
TriStateBool.Unknown)
    End If

Get a Group and UserInfo object and add the Group to the User's list of parent Groups
    Dim objGroupInfo As GroupInfo = BRApi.Security.Admin.GetGroup(si, "TestGroup")
    If Not objGroupInfo Is Nothing Then

        Dim objUserInfo As UserInfo = BRApi.Security.Admin.GetUser(si, "TestUser")
```

```
        If Not objUserInfo Is Nothing Then

            If (Not objUserInfo.ParentGroups.ContainsKey(objGroupInfo.Group.UniqueID)) Then
                Dim parentGroupIDs As List(Of Guid) = objUserInfo.ParentGroups.Keys.ToList()
                parentGroupIDs.Add(objGroupInfo.Group.UniqueID)

                BRApi.Security.Admin.SaveUser(si, objUserInfo.User, True, parentGroupIDs,
TriStateBool.Unknown)
            End If
        End If
    End If
```

Create a User

```
Dim objUser As User = New User()
    objUser.Name = "NewUser"
    objUser.Text1 = "Test Text 1"
    BRApi.Security.Admin.SaveUser(si, objUser, False, Nothing, TriStateBool.Unknown)
```

Create a Group

```
Dim objGroup As Group = New Group()
    objGroup.Name = "NewGroup"
    Dim objGroupInfo As GroupInfo = New GroupInfo()
    objGroupInfo.Group = objGroup
    BRApi.Security.Admin.SaveGroup(si, objGroupInfo, False, Nothing, TriStateBool.Unknown)
```

International Settings

Culture-related number and text formatting can be used with:

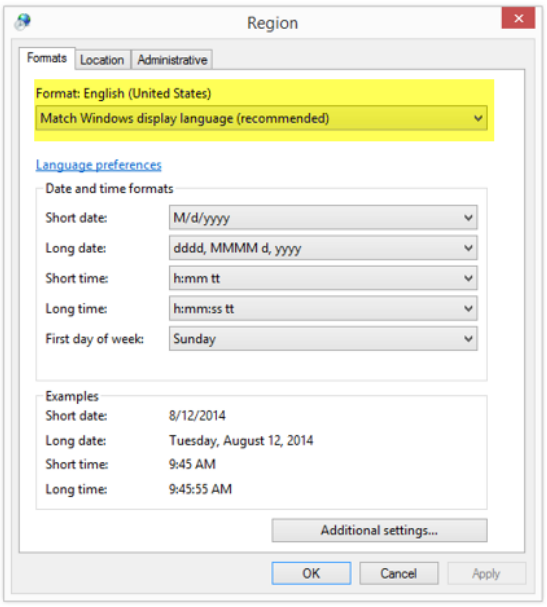
- Web-based client
- Excel Add-In
- Server components

For consistency, we recommend that each user's culture setting match the Windows Regional settings of their primary computer.

Specify Culture Settings on the Client Machine Operating System

Number and text formatting for Microsoft Excel is controlled by the client operating system's Windows Regional settings. To configure these settings:

1. Access the operating system **Control Panel**, and then select **Region**.
2. Select **Format**, and then set properties to reflect regional preferences. For example:



3. Select **Location**, and then set the **Home Location** to reflect the operating system's location, such as Canada, Germany or Australia.

Specifying Server Side User Culture Settings

For the web-based client and server components, specify culture settings for users by modifying user profiles in Security. The necessary culture codes must first be defined in the Application Server Configuration file.

Work with System Applications

After you log in as an administrator, you can open the System Administration application that enables you to create a new application based on existing or copied databases. For existing applications, go to **System** > **Administration** > **Applications**.

 **Create Application Reference**

Select to link an application and an existing database if they are from the same release version. Select a Database Server Connection, and then enter a Database Schema Name. The new application displays.

Allow Database Creation Via UI must be set to **True** in the Application Server Configuration.

 **Create Application Database**

Select to create a new database.

Application Name

Enter the name of the new application.

Description

(Optional) Enter a brief description.

Database Server Connection

Select the database server from the drop-down menu.

Database Schema Name

This is created by default and stored in SQL.

Time Dimension Definition

Select the ellipsis, and select the desired Time Dimension XML file. See System Tools.

The new application displays in the Application list when you log in.

> **NOTE:** Database Status indicates whether a selected application has an attached database. If there is an Error status, the database was deleted or detached and will not be available in the Application list.

 **Delete Selected Application Reference**

Select to remove an application's database link. Removing the link does not delete database files, only the references in the application.

 **Test Database Connection**

Select an existing application, and select the test checkbox to verify an active connection.

System Dashboards

System Dashboards are similar to Application Dashboards but they also enable you to use OneStream Framework database objects such as security and users. Application Dashboards use Application-level data stored in Cubes.

See "Dashboards" in the *Presentation Guide* for information about designing Dashboards.

Implementing Security

This section describes the four-pronged approach to managing security:

- Workflow security
- Entity security
- Account security
- Security roles

Security can be implemented on accounts or dimensions allowing you to control who can review specific dimension members. Security is determined through users and groups, with users given specific roles to determine what data can be accessed or edited.

Application Security

A four-prong approach to application security consists of:

- Workflow security
- Entity security
- Account security
- Security roles

Once you identify entities and assign them to workflow profiles, data loaders and certifiers can be determined for each entity. Data loaders load data into the system, therefore they need read/write access to entities. Data certifiers review and sign off on the loaded data, so they need read access to entities. Security can also be done on the account or any other dimension to control who can review specific dimension members.

Security is determined through users and groups. Users are given specific roles to determine what data is accessed or edited. For example, if a user is given the ModifyData role in an application, they will have write access to any data in it. Users are also put into security groups. Groups can support native groups, exclusion groups, or groups of groups. For example, a user can be put into an entity's read/write data group for read/write access to the entity's data.

Every object has access and maintenance security rights, with the exception of Task Scheduler. Access allows the security group to view the object, while maintenance allows the groups to edit the definition of the object. This system applies to most objects, such as cube views, dashboards, transformation rules, and workflow profiles.

Security Best Practices

This section details the best practices for using security.

Object Security

There needs to be different levels of access for object types and groups of objects, such as Cube Views, dashboards, or business rules. Application and System Roles can be granted to User Groups which create subject area administrators and by giving certain rights to a group, such as ManageCubeViews, pseudo-administrators are created for these actions. This provides the most power for a specific object type.

A Maintenance Group is the middle level of power for an object at the group level. For example, a Maintenance Group assigned to a specific Entity Transformation Rule Group allows the assigned users to create, edit, and delete rules within that Transformation Rule Group.

An Access Group is the lowest level of power for an object at the group level. This means the object can be used, but its definition cannot be edited.

Confirmation Rules

Confirmation Rule Groups are assigned to Confirmation Rule Profiles which are then assigned to Workflow Profiles. The run time access to these Confirmation Rules depends on to which Workflow Profile they have been assigned. If a user has Workflow Execution Access, they will be able to execute them.

The best way to control Confirmation Rules is to set Access to Everyone and Maintenance to Administrators for both Confirmation Rule Groups and Profiles.

Certification Questions

Certification Question Groups are assigned to Certification Question Profiles which are then assigned to Workflow Profiles. The run time access to these Certification Questions depends on to which Workflow Profile they have been assigned. If users have Workflow Execution Access, they will be able to execute them.

The best way to control Certification Questions is to set Access to Everyone and Maintenance to Administrators for both Certification Question Groups and Profiles.

Data Sources

Data Sources are assigned to Workflow Profiles. The run time access to these Data Sources depends on to which Workflow Profile they have been assigned. If a user has Workflow Execution Access, they will be able to execute them.

The best way to control Data Sources is to have to the ManageDataSources Application role, and no security settings at the object level.

Transformation Rules

Transformation Rule Groups are assigned to Transformation Rule Profiles which are then assigned to Workflow Profiles. In this case, an appropriate user group needs to be assigned to Access and Maintenance because users will be able to right-click on an Import Workflow Profile and view or edit their Transformation Rules. The user groups should include the users assigned to execute the Workflow Profiles to which the Transformation Rule Profile has been assigned.

The best way to control Transformation Rules is to set Access to Everyone and Maintenance to Administrators for most core, shared, or corporate Transformation Rule Groups For some specific Transformation Rule Groups, such as an Account Transformation Rule Group that applies to a specific location, assign the appropriate user groups to Access and Maintenance. Block access to the Maintenance screen for anyone except administrators because this could potentially allow users more access than they need.

Form and Journal Templates

Form or Journal Groups are assigned to Form or Journal Profiles which are then assigned to Workflow Profiles. The run time access to these Forms or Journals depends on to which Workflow Profile they have been assigned. If a user has Workflow Execution Access, they will be able to execute them.

The best way to control Form and Journal Templates is to set Access to Everyone and Maintenance to Administrators for both Form and Journal Groups and Profiles.

Cube Views

The best way to control Cube View Groups is to set Access to Everyone and Maintenance to Administrators and anyone else building a Cube View. To keep the assignment of Cube View Groups to multiple Cube View Profiles flexible, the Cube View Groups need to remain smaller in size. For Cube View Profiles, set Access to anyone who will need to see these Cube Views in OnePlace, Excel, or assign them to Workflow Profiles, Forms, or dashboards. Set Maintenance to anyone who needs to change the assignment of the Cube View Groups to Cube View Profiles.

OneStream recommends setting the Can Modify Data, Can Calculate, Can Translate, and Can Consolidate properties to False. This can be preset for all new Cube Views by creating an example or Cube View Template which can be copied to create new ones. Some examples of when this will not be needed is if the Cube Views are going to be read by administrators only, the Cube Views will be used as a data entry form or are only going to be visible in a formatted report or chart.

System and Application Dashboards

When assigning Dashboard Groups to Profiles, visibility is extremely important. For example, if a user has access to a Dashboard Profile in OnePlace, but not to a certain Dashboard Group in that Profile, the user will not be able see the dashboards in that group. Also, if a user has access to the Dashboard Groups, but not the Profiles, they will not be able to see the dashboards in OnePlace. If a Cube View is assigned to an Application dashboard, and the user only has access to the Cube View, they will not see the dashboard. Lastly, if a dashboard is pointing to an Entity, Scenario, or Cube Data to which the user does not have access, they will see one of the following: NoAccess in Data Explorer for the cells the user cannot see, a blank cell in the Data Explorer Report, or No Data Series if they are viewing a chart.

The best way to control Dashboard Groups is to set Access to Everyone and Maintenance to Administrators and anyone else building a dashboard. In order to keep the assignment of Dashboard Groups to multiple Dashboard Profiles flexible, the Dashboard Groups need to remain smaller in size. When assigning Maintenance for Dashboard Profiles, give access to anyone who needs to see the dashboard in OnePlace, assign it to a Workflow Profile, or change the assignments of Dashboard Groups to Dashboard Profiles.

Use multiple Dashboard Maintenance Units in order to keep them a reasonable size making it easier to manage multiple objects and access. Dashboard Parameters can also be used across all dashboards and do not need to be copied across all Maintenance Units. Security has no bearing on the use of Parameters.

Workflow Security

Security groups for Workflow Execution, which is the ability to process a Workflow for a specific Workflow Profile, Certification Signoff and the separate ability to process, approve and post journals, exist for all Workflow Profiles. In certain cases, the user simply needs the Access and Workflow Execution Group Access to run Workflow. For example, the user does not need Access or Maintenance Group access to Data Sources or Transformation Rules in order to run through the Import Workflow.

In some cases, having access to certain objects is necessary along with Workflow Execution Group Membership. The Manage App Role has to do with creating, reading, updating, and deleting Journal and Form Templates (metadata) themselves, not just instances of these objects at run time. It is expected that 90% of Workflow users will not have any of the Application Roles, but their access will be controlled by the Access Group for those Journal/Form Template Groups and Profiles. Workflow users also need Workflow Execution Group access in order to perform import, forms, and journal actions. The user does not have to be in the Manage Application role to create a Journal or enter data in the Form. Workflow security governs access to the forms. If the user is in the ManageJournalTemplates Application Role group, they can create any Journal needed for the Workflow Profiles to which they have proper execution access.

Users need to have at least Access Group privileges to the Cube Root Workflow Profile node to edit Workflow Profiles with having the ManageWorkflowProfiles role. Otherwise they will not be able to see any Workflow Profiles under the Cube Root Workflow Profile.

The order to follow when assigning access to Workflow Profiles and data is to first assign Read and Read/Write Groups to the Entities involved. Next, create an Access Group, Data Group, and Approver Group for each Workflow Profile and include the appropriate Entity groups.

Import

First, determine whether the users can load data to the Workflow for the assigned Entities and then determine whether they load both GL (BS and PL) and Supplemental data, or one or the other. Next, decide if the users for the assigned Entities can certify the loaded data as part of the Workflow.

Forms

Determine whether the users can manually input data into a form and certify it as part of the Workflow for the assigned Entities.

Adjustments

Determine whether the users can manually input data into a journal and certify it as part of the Workflow for the assigned Entities.

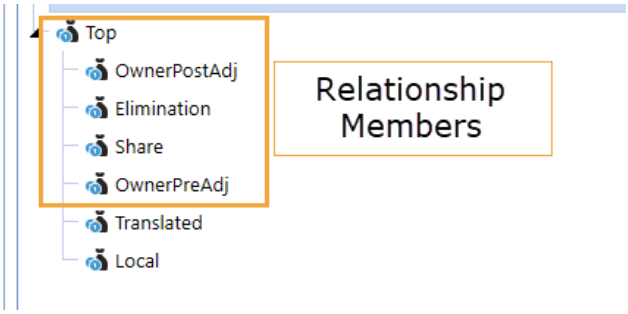
Entity Security

Entity Security controls the overall read/write access to Entity data and controls whether Cube Security should be used. When creating Entity security groups for the Read Data Group and the Read/Write Data Group, the groups should be named in a logical convention such as XXXX_View or XXXX_Mod. The Entity Read/Write Data Group should be designed first because it is needed for data loading in Workflows. The Workflow Execution Security Group should be assigned to all the Entities' Read/Write Security Group for the Workflow to gain loading access to the Entities.

When setting up View Security Groups for Entities, first consider how users need to view their data whether it is by segment or region. Determine whether it makes more sense to have one Entity View Group per Entity, or to create one Entity View Group per segment and apply one Entity View Security Group to many Entities' Read Data Group. All the Entities' View Groups below the Parent must be assigned to the Parent Level Entity View Group in order to gain access to data at the Parent Level Entity and View Entities below it. Try to minimize the amount of View Entity Security Groups where possible.

Relationship Security

You can change the security model to allow who controls viewing or modifying the relationship members in the consolidation dimension.



For the Use Parent for Relationship Consolidation dimension Members functionality:

- If set to False, the user entity rights control their rights to all members of the consolidation dimension. This is the default security model.
- If set to True, the user rights to the relationship members of the consolidation dimension are determined by their rights to the current entity's immediate parent.

Users have either read or read/write access to view or modify their entity so they can see their entire entity from all of the relationship members. You can allow the relationship security portion of the consolidation dimension to be controlled by the access to the parent entity in the immediate hierarchy.

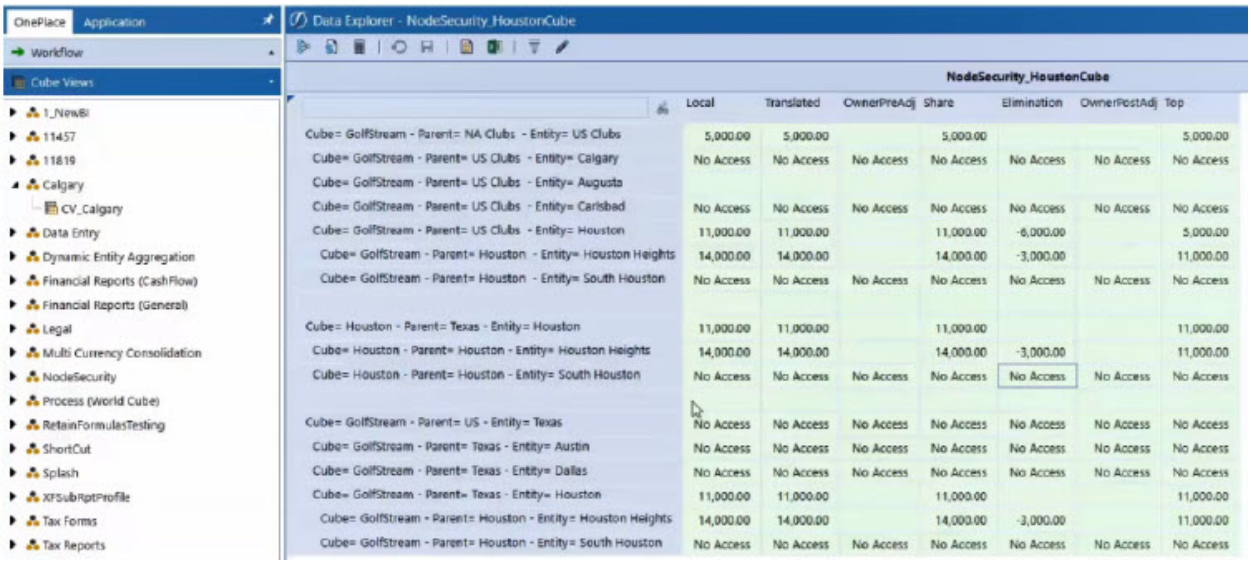
> **NOTE:** This is strictly a parent and child relationship.

Set this feature to True when:

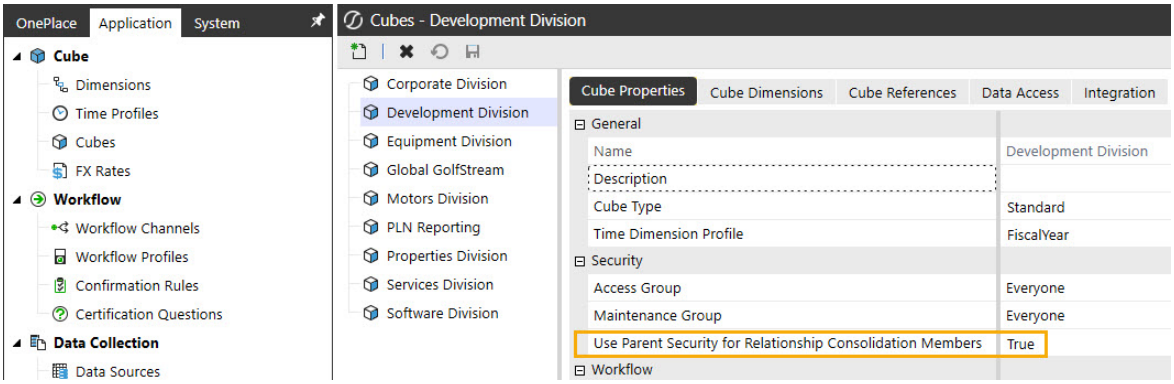
- A user's rights to the non-relationship consolidation dimension members (local and translated) are determined by the user's rights to the entity itself.
- A user's rights to the relationship consolidation dimension members is determined by the user's rights to the immediate parent entity.

Change the Relationship Security

To change relationship security, complete the following steps:

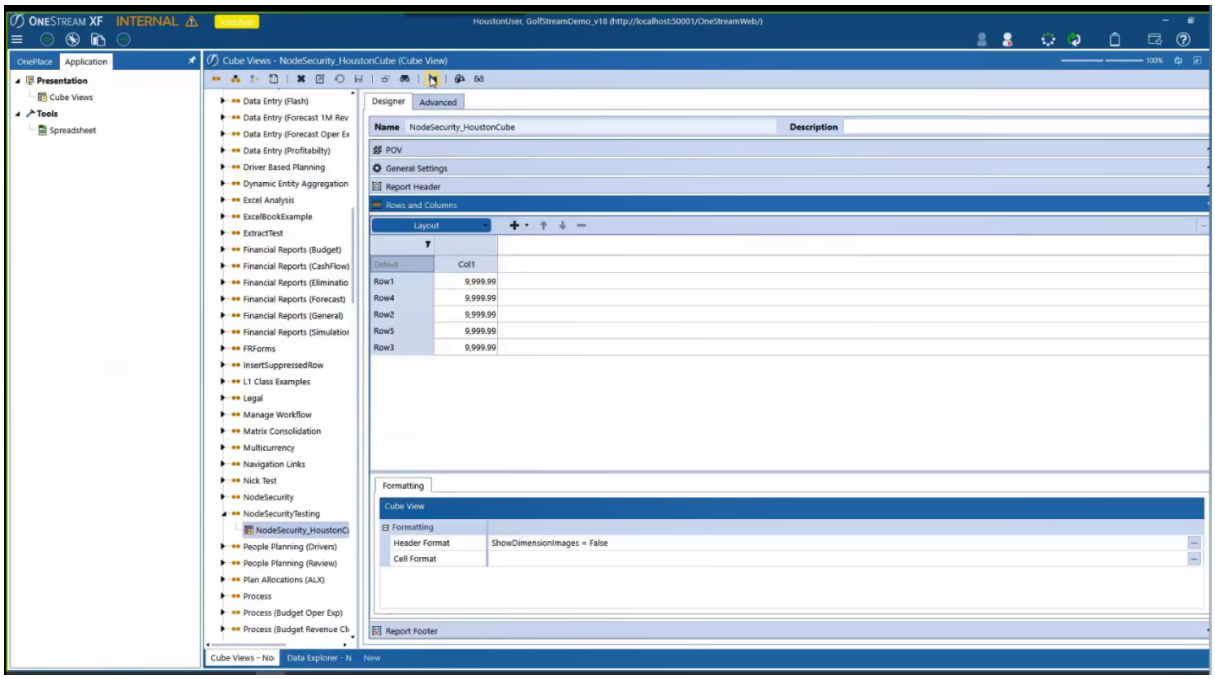


1. In the Application tab, under Cube, select **Cubes**.
2. Select a Cube.
3. In the Cube Properties tab, in **Use Parent Security for Relationship Consolidation Dimension Members**, select **True**.

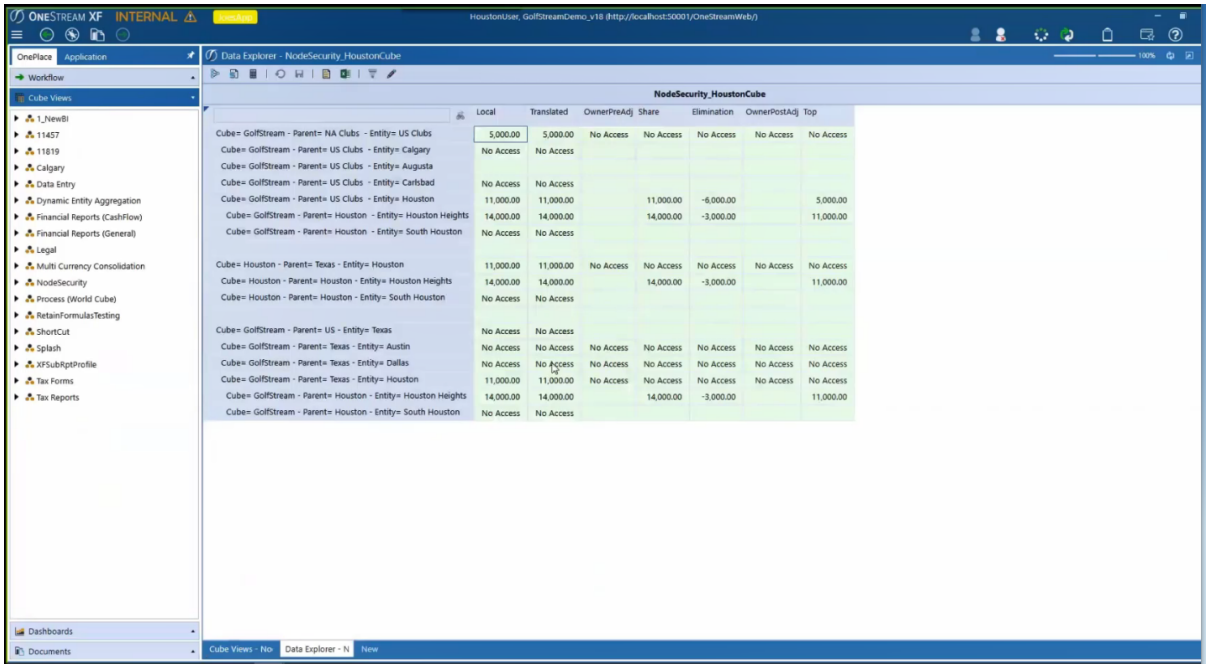


4. Select **Save** to save the cube properties. The security model is updated for the read or write relationship for the consolidation dimension members to be based on the security rights to the immediate parent entity.

5. Select **Refresh** to refresh the application.
6. In Cube Views, go to the Designer tab and select the **Open Data Explorer** icon.



All of the security is changed.



Notice the following changes to security:

- In the first image, all the consolidation dimension members are available across Houston.
- When you switch on the new security, the user has rights to `USClubs`, and all of the consolidation dimension members of the Houston member are available.
- In the last group, the user has no rights to Texas, based on the NoAccess to Local and Translated. In Houston, you can see the relationship members changed to NoAccess.
- The reason why USClubs turns to NoAccess is because the user has no rights to the parent NAClubs, which is not displayed on the report.

Data Security

Data security controls the overall read/write access to analytic models. There are several steps to see if you have access to data. First, it checks if you have the ModifyData role in the application, otherwise you do not have write access to data. Next, data security ensures you have either the access group or maintenance group for a cube, or you do not have access to any of the cube's data. It will then check the scenario and Entity's Read Data Group and Read Write Data Group to ensure access. Finally, it checks the Data Cell Access Security at the cube level. If you have access to the data and use Excel or any other method to import data, it ensures the entity being written to belongs to a workflow profile with an active forms channel that is not locked or certified. If any of these steps result in no access, the process stops.

- There are several ways to guarantee data is secure. Throughout the dimensions, different security groups are available, and an administrator can decide what users belong to each group.
- The scenario dimension has both Read Data Group and Read and Write Data Group.
- The entity dimension uses both security groups from the scenario and adds display member group and Use Cube Data Access.
- The display member group only refers to the member display access level, not the data access level. Use Cube Data Access is used if slice filters are being applied at the cube level to apply additional layers of security for specified security groups.
- The account, flow, and all user-defined dimensions also use display member group.

At the cube level, more security is put in place through groups, member filters, and complex layered security. A cube slice filters a data entry form to the right member set, such as choosing the cost center in which a user can enter data. For slice filters to take effect, the user must first be granted access to the cube, scenario, and entity. Slice security cannot increase access to data that was not administered first through Users and Groups. An administrator can also lock down more than one dimension by using cube data access and can control user visibility by only giving access to certain accounts. Finally, data cell conditional input and data management access security can be used. These are not security settings but can still control how a dimension can be used for input and how a cube is modified.

Application and System Security

Dimensions, cubes, business rules, data management, and File Explorer each have an access and maintenance group. OneStream recommends limiting access to these groups and assigning the screens to administrators. It is also recommended to give the ManageData role to administrators for data management and to give ManageTaskScheduler and TaskScheduler roles in Task Scheduler. The ManageFileShare role should also only be given to administrators. Anyone granted access to a folder in File Explorer has access to every file and folder through OnePlace. For FX rates, limit access by giving administrators the ManageFXRates role and selecting a set of power users.

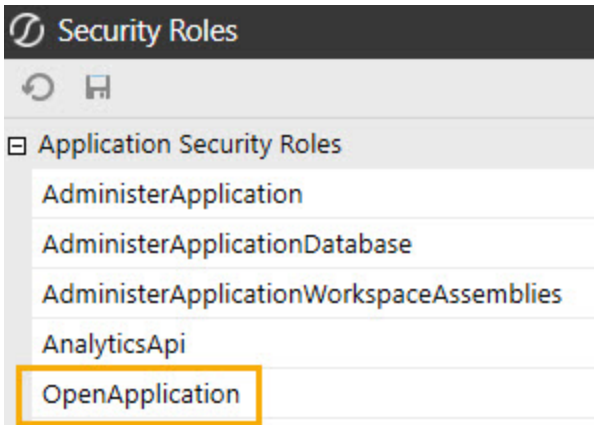
Security Configurations

Configure security settings to control access to applications and their features.

Restrict Users to an Application

Setting up access to an application can be done within the application security roles. When an application is first created, the OpenApplication defaults to `Everyone`. If specific people have access to log in to OneStream, but only need access to specific applications, then security groups can be assigned to the OpenApplication role. Once the security group is created, users can be assigned to it. This can be done by performing the following steps:

1. Go to **System** > **Administration** > **Security**.
2. Create a new security group.
3. Assign all users who should have access to the application to the new security group.
4. Refresh the application in order for this new security group to appear in all drop down menus.
5. Go to **Application** > **Tools** > **Security Roles** > **OpenApplication**.

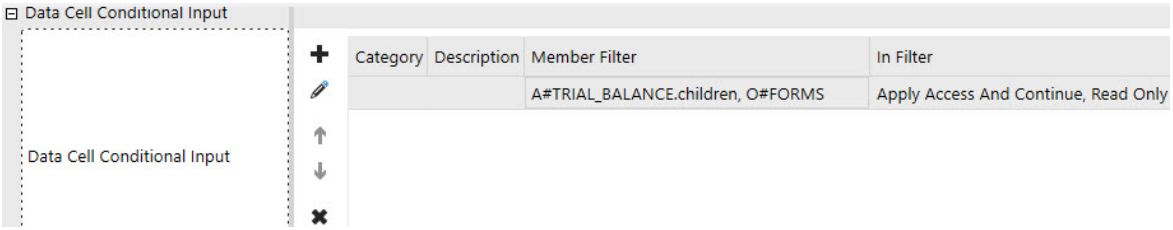


6. Select the drop-down menu and select the new security group.
7. Select the **Save** icon.

Restrict Data Input by Origin

There may be times where data should be loaded through the Import origin but should not be loaded using the Forms origin. This can be handled in the data cell conditional input. For example, users may be able to load trial balance data through the Import origin, but other users submit statistical data through the Forms origin. The data cell conditional input ensures the statistical data does not overwrite the Trial Balance data in Actual. Perform the following steps to do this:

1. Go to **Application** > **Cube** > **Cubes** > **Data Access**.
2. Go to **Data Cell Conditional Input**.
3. Select the ✚ icon to create a new line.
4. Select the  icon, or double-click on the cell to make changes to the member filter. Add the dimension intersection to restrict data loading. In this case, it restricts users from loading to the Trial Balance account through the Forms origin.
5. In the In Filter field, choose a behavior and choose the Read Only Access level.

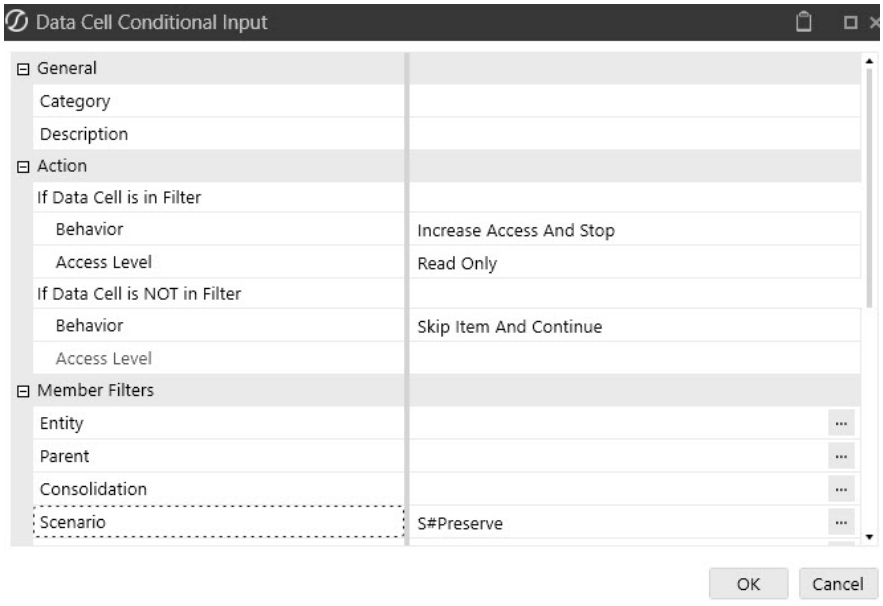


Omitting Data Cell Conditional Input by Scenario

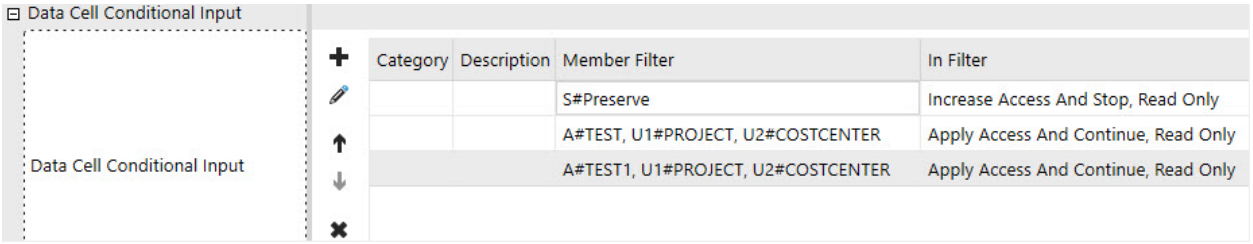
Data cell conditional input restricts access to certain intersections or slices of the cube. This behavior might not be desired for all scenarios, time periods or other elements, so this is a simple way to omit these rules for specific elements. The following method is useful when there are many data cell conditional input rules not defined by a scenario at the time of creation. After these rules are created, however, a scenario becomes a factor for historical data.

For example, there may be many read-only intersections in Actual to which users should not load data. These rules are set up in the data cell conditional input section in **Application** > **Cube** > **Cube** > **Data Access**. However, for historical purposes, there may be data in these intersections that existed before filter application. The scenario to which the data is being copied needs to allow access because the historical data in these intersections may need to be copied for analysis.

Create a new data cell conditional input rule for the entire scenario, set the behavior to Increase Access And Stop, and set the Access Level to Read Only.



Position this new rule at the top of the Data Cell Conditional Input for the scenario.



The behavior option Increases Access And Stop is being used because if the current cell matches the filter, access is being increased and all subsequent data access rules are being ignored below. In this case, the Preserve Scenario has access to everything, and the subsequent Data Cell Conditional access rules are ignored or not applied for Preserve.

System Security

System Security applies to the framework. There are some key assumptions around how the different roles or security groups work. First, it is important to understand the hierarchy of certain System Security Roles and Security Groups:

System Security Role

The System Role, such as ManageSystemDashboards, means the user has a higher privilege and does not need to be in any Maintenance Group or Access Group to see, edit, or delete all objects of that type. Having the ManageSystemDashboards System Security Role means the user can create, edit, and delete any System Dashboard, System Dashboard Group, or Profile.

Maintenance Group

The Maintenance Group means users cannot only see an object, but can create new objects in Groups, edit, and delete them. Users do not need to be in the Access Group for an object if they are in the Maintenance Group. The Maintenance Group can also control the contents of Profiles.

Access Group

The Access Group means users can see the object and read its contents.

Managing a OneStream Environment

Management of all changes to the system is recommended to follow best practice procedures. Whether the changes come from a OneStream software upgrade or through regular application maintenance, all changes are recommended to be first deployed and tested in a development environment. There are additional benefits to making a recent copy of the production Application database, renaming it, and using this as a base for these changes. See "Creating an Application Database" in the *Installation and Configuration Guide.*

Prior to deployment to a production environment, it is recommended to extract changes from the development environment and assess this deployment of changes in a separate test environment.

Deploying changes to a production environment should avoid times during high load and high application activity. Changes to these types of application artifacts especially should not be performed against a production environment experiencing heavy activity:

- Business rules, whether they contain Global functions or not
- Confirmation rules
- Metadata, especially when using member formulas

> **NOTE:** Applying changes while the production system is under a high level of activity may have a negative impact on servers and cause running processes to produce an error.

Standard environments are recommended to schedule production changes during slow periods or non-work hours. Large environments should consider using the Pause functionality in the Environment tab to allow activity to wind down. These large environment managers should also consider the OneStream Solution, Process Blocker, which allows a pause of critical processes to perform maintenance on the system, without having to shut down the entire application. Process Blocker allows current tasks to be completed, while any new requests are queued, allowing the changes to be applied safely and effectively. Once these changes are in place, it is recommended to significantly limit the ability for users to make such changes during high volume.

It is key that servers get a chance to recycle for good system memory health. IIS also has an Idle Time-Out setting for our OneStreamAppAppPool. This setting should be set to 0 since OneStream has other settings to recycle IIS. For active, global environments with Data Management Sequences regularly being executed, a recycle of IIS is recommended every 24 hours for these OneStream App Servers. Please discuss this situation with OneStream Support to find what is recommended, as each situation may vary.

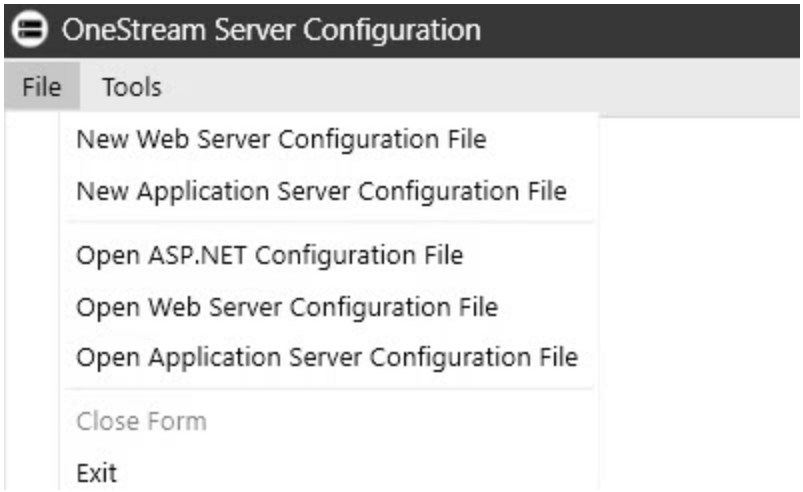
Disable Inactive Users

Use the disable inactive users feature to create an authorization policy that disables users after a specific period of login inactivity. Only active users remain in the system.

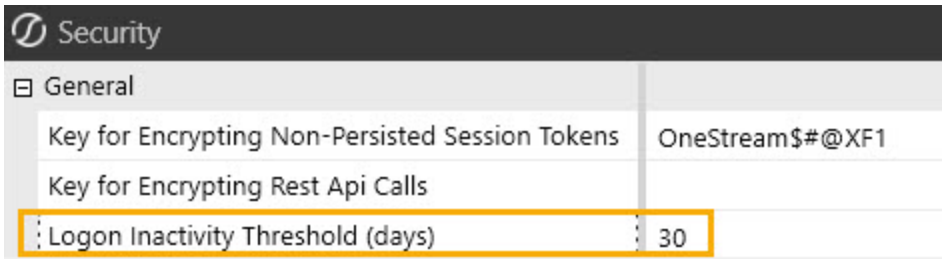
Set the Inactivity Threshold

Follow the steps to set the inactivity threshold:

1. In the OneStream Server Configuration Utility, select **File** > **Open Application Server Configuration File**.



2. Open the configuration file.
3. In the **Security** row, select the ellipses button.
4. Set the Logon Inactivity Threshold to the number of days of inactivity before the user can no longer access the system.

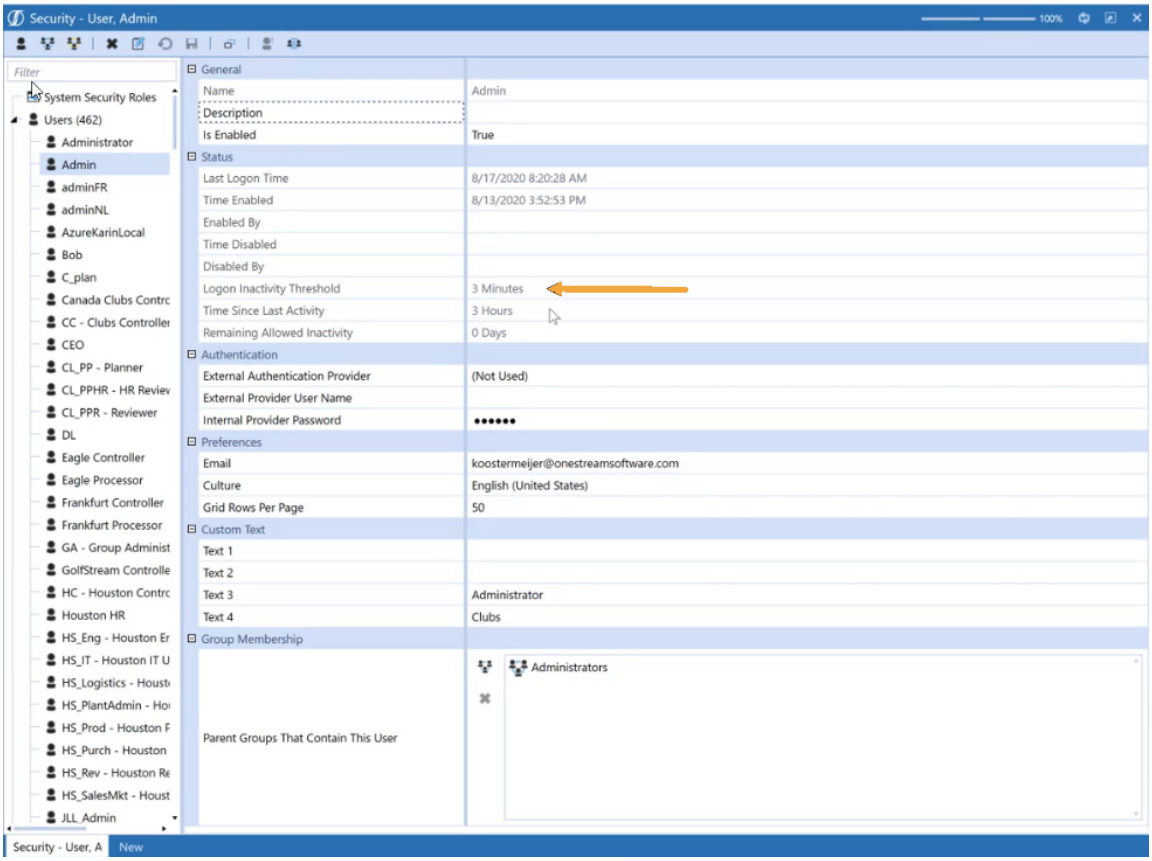


5. Select the **OK** button.
6. Select the **Save** icon.
7. Reset IIS to recognize the changes.

Review Settings

The administrator is the only role where the inactivity threshold does not apply.

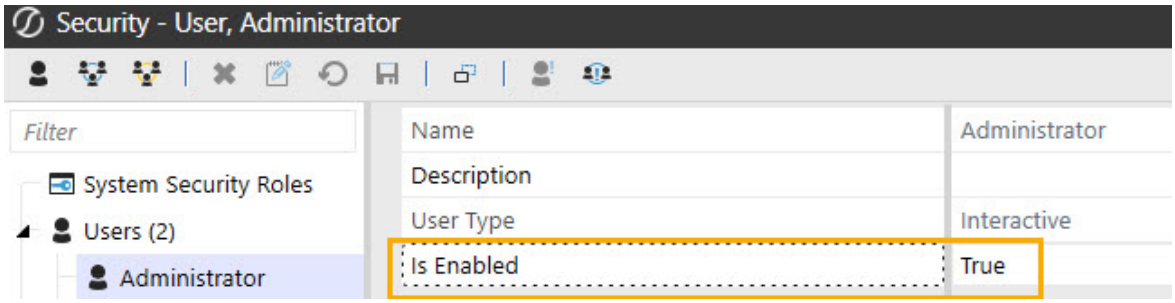
1. To review, go to **System** > **Security**.
2. Select **Users** and view the threshold setting.



> **IMPORTANT:** If the Remaining Allowed Inactivity is **0 Days**, that means the user no longer has access. That user gets a message stating they have been disabled if they try to log in.

To enable access:

1. Go to **System** > **Security**.



2. Select the user.
3. Select the **Is Enabled** drop-down menu.
4. Select **True**.
5. Select the **Save** icon.

   The Remaining Allowed Inactivity field updates allowing the user to log back in within the time frame specified.

Business Rules

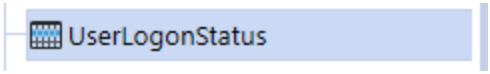
To access business rules:

1. Go to **Application** > **Business Rules** > **Extensibility Rules**.
2. The three new business rules are GetStatusByID, GetStatusByName, and LogoninactivityThresholdForAdmin.

System Table

To access the system table:

1. Go to **System** > **Database** > **System Database** > **Tables**.
2. There is a table name UserLogonStatus



How Users are Configured for Authentication

When an administrator creates users in **System** > **Security**, they specify authentication settings.

- For native authentication:
  - **External Authentication Provider**: In the drop-down menu, select **(Not Used)**.
  - **External Provider User Name**: Leave this field blank.
- For an external identity provider:
  - **External Authentication Provider**: In the drop-down menu, select the external identity provider.
  - **External Provider User Name**: Enter the user name configured in the external identity provider in this field.

See About Managing Users and Groups.

If you are in a OneStream-hosted environment, see the *Identity and Access Management Guide* for information about authentication with OneStream IdentityServer.

For instructions on configuring authentication in a self-hosted environment, see the *Installation and Configuration Guide*.

About Managing Users and Groups

See the following topics for help defining and managing users and groups:

- Ways to Add Users and Groups to an Application.
- Create and Manage Users.
- Create and Manage Groups.

For information about how group-based assignment to system security roles determines a user's access to artifacts and capabilities, see Manage System Security.

Ways to Add Users and Groups to an Application

You can add users and groups to an application in three ways:

- Define them manually in System Security. See Create and Manage Groups and Create and Manage Users.
- Load them in a bulk import using an XML load file that contains user and group properties and parameters. We suggest building this file using the sample security Excel template provided with the Sample Templates OneStream Solution. See Create and Manage Users and Create and Manage Groups.
- Use APIs. See Manage Users and Groups Using BRApi Functions.

Create and Manage Users

By default, only an administrator can complete the tasks described in the following topics. An administrator can enable other users to complete these tasks by giving them specific system security roles.

In this topic:

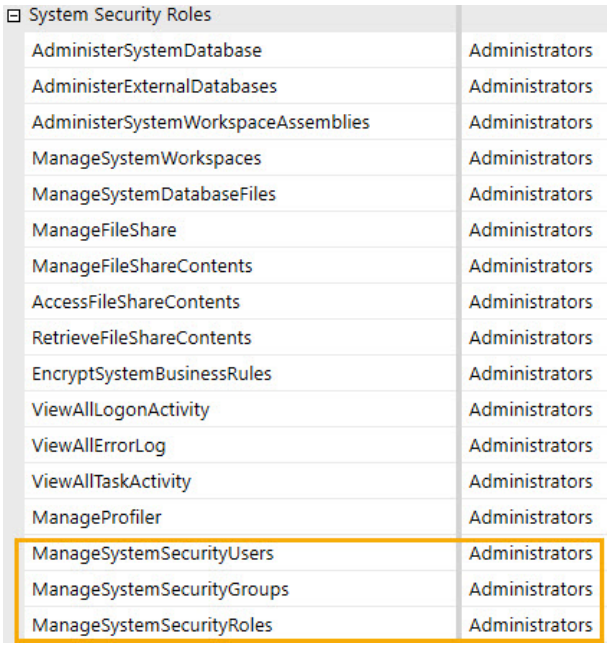
- Tips and Best Practices
- Create Users
- Manage Users
- Load and Extract Users

Requirements

To let non-administrators create and manage users and groups, grant them the required security roles. This involves assigning the group to which non-administrator belongs, to the required roles.

1. Go to **System** > **Security** > **System Security Roles**.
2. Select the ellipsis button by these roles to assign the group in which the user is a member:
    - **ManageSystemSecurityUsers**: Assignees can create, modify, and manage users.
    - **ManageSystemSecurityGroups**: Assignees can define, modify, and manage groups.
    - **ManageSystemSecurityRoles**: Assignees can manage roles to provide group-

based, function-specific access to artifacts and tools.



System Security Roles	
AdministerSystemDatabase	Administrators
AdministerExternalDatabases	Administrators
AdministerSystemWorkspaceAssemblies	Administrators
ManageSystemWorkspaces	Administrators
ManageSystemDatabaseFiles	Administrators
ManageFileShare	Administrators
ManageFileShareContents	Administrators
AccessFileShareContents	Administrators
RetrieveFileShareContents	Administrators
EncryptSystemBusinessRules	Administrators
ViewAllLogonActivity	Administrators
ViewAllErrorLog	Administrators
ViewAllTaskActivity	Administrators
ManageProfiler	Administrators
ManageSystemSecurityUsers	Administrators
ManageSystemSecurityGroups	Administrators
ManageSystemSecurityRoles	Administrators

To revoke the ability to manage users, groups, and roles, remove assignees from the relevant role. See Manage System Security.

Tips and Best Practices

- The administrator is assigned to all system security roles, so they can always manage application and system-wide users, groups, artifacts, data, and tools. Removing or reassigning the Administrator group or assigning other users and groups to roles does not revoke administrator access.
- The administrator cannot be disabled and is unaffected by inactivity thresholds that disable users who try to log in after a specific period of time elapses.

Create Users

Follow the steps to create users:

1. Go to **System** > **Security** > **Users**.
2. Select **Create User**.
3. Enter a name and description.
4. From **User Type**, select the purchased license type. This property does not control access to artifacts.
    - **Interactive**: They can use all features and tools.
    - **View**: They can access data, reports, and dashboards in a production environment and associated database, but cannot load, calculate, consolidate, certify, or change data.
    - **Restricted**: They cannot use some OneStream Solution features, such as Lease, Account Reconciliation, and more, due to contractual limitations.
    - **Third Party Access**: They can access applications with a third-party application by logging in using a named account. They cannot change data, modify artifacts, or access the Windows application or a browser-based application.
    - **Financial Close**: They can use Account Reconciliation and Transaction Matching OneStream Solutions.
5. Set **Is Enabled** to **True** to activate the user. Select **False** to deactivate the user.
6. The information in **Status** reflects user activity, such as the latest login. **Inactivity Threshold** displays the number of days a user can remain active in the system without a login. The user receives an error if they try to log in after the specified number of days elapses. See Set the Inactivity Threshold.
7. See About User Authentication, then Specify Authentication Settings.

About User Authentication

You can add and authenticate the following types of users:

- Native users that are managed locally in OneStream
- External users referenced by an external identity provider (IdP)

Specify Authentication Settings

Follow the steps to specify authentication settings:

1. From **External Authentication Provider**, indicate how to authenticate the user:
    - To use native authentication, select **Not Used** and enter the user password in **Internal Provider Password**. The first time the user logs in, they can change their password.
    - To use external authentication:
        a. Select the appropriate external IdP from **External Authentication Provider**.
        b. In **External Provider User Name**, enter the user name in the IdP. For example, if a user's name in Azure AD (Microsoft Entra ID) is Azure_LHall@azure.com, enter Azure_LHall@azure.com. This name must be unique and match the user name in the IdP.
2. See Specify Preferences and Group Membership.

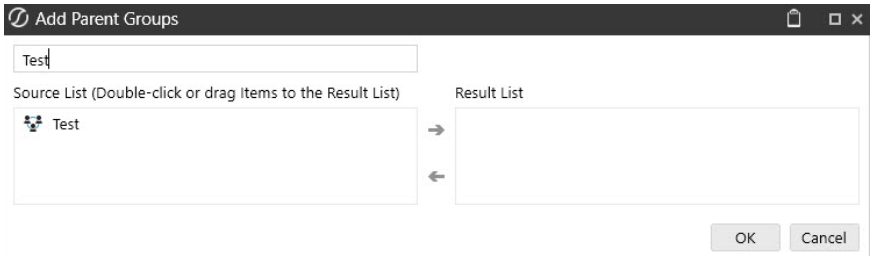
Specify Preferences and Group Membership

Follow the steps to specify any preferences or group membership settings:

1. In **Email**, enter the email address with which the user can receive alerts and messages, such as those generated with business rules.
2. In **Culture**, select the user's locale. Supported locales and languages are specified during OneStream server configuration. See International Settings.

3. In **Grid Rows Per Page**, specify how many rows to display on grids before a page break. Consider the rate of connectivity and screen resolution.
4. Use **Custom Text** to personalize aspects of functionality given the user's responsibilities. For example, you can define a text field to:
    - Act as a metadata tag, limiting who the user can email.
    - Filter a distribution list or provide text and images for the user's default Workflow Profile.
    - Launch a function-specific view of the user's workspace, such as reporting for controller or executive.

    See "Entity Dimension" in the *Understanding the Financial Model Guide.*
5. In **Group Membership**, select **Add Groups** to include the user in the groups that provide access to the features and tools that the user needs. If the appropriate group does not exist, create it. See Create and Manage Groups.



6. Select the **OK** button, select **Save**, and then select **Load**.

When processing finishes, review the user list and user settings to ensure the loaded users are correctly defined.

Manage Users

Complete the following tasks to edit, copy, delete and perform other management tasks. You can also manage users with API functions.

1. Ensure that you have the necessary security role. See Requirements.
2. Go to **System** > **Security** > **Users**.
3. Select a user, then an action to take. For example:
    - **Delete Selected Item**: Permanently delete the user.
    - **Copy Selected Item**: Create a new user based on the selected user's settings. See Copy Users.
    - **Show all parent groups for user**: See the groups in which the user is a member. Because group assignment to system security roles and user interface roles determines what a user can do, use this option to identify their access to artifacts.
4. Select **Save**.

Copy Users

Follow the steps to copy users:

1. Go to **System** > **Security** > **Users**.
2. Select the user, then select **Copy Selected Item**.
3. In **New Name**, enter a user name.
4. Select **Copy References made by parent groups** to add the user to the original user's groups except exclusion groups.
5. Select **OK** and modify other settings as needed. See Manage Users.
6. Select **Save**.

Disable Users

Administrators can disable users, preventing them from logging in by:

- Modifying a user's account to set **Is Enabled** to **False**. See Disable a User Manually.
- Specifying an inactivity threshold to deactivate all users, native and external, that try to log in after a particular amount of time elapses. This threshold applies to users in the Administrator group, but not the Administrator. Users that try to log in after the threshold expires receive an error. See Define an Inactivity Threshold.

Disable a User Manually

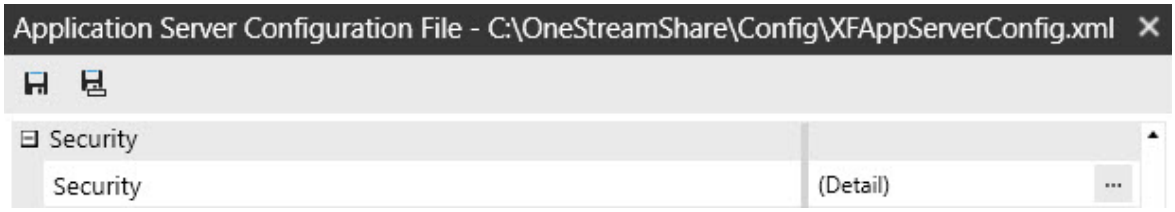
Follow the steps to disable a user manually:

1. Go to **System** > **Security**.
2. Expand **Users**, and select the user to disable.
3. From **Is Enabled**, select **False**.
4. Select **Save**.

Define an Inactivity Threshold

Follow the steps to define an inactivity threshold:

1. Launch the Server Configuration Utility.
2. Select **File** > **Open Application Server Configuration File** and browse to **OneStreamShare\Config\XSFAppServerConfig.xml**.
3. In **Authentication**, select **Security**.



4. In **Logon Inactivity Threshold**, enter the number of days after which inactive users who try to log in receive an error.
5. Select **OK**, then **Save**.
6. In a command prompt, reset IIS.
7. In the application, select **System** > **Security** > **Users**.
8. Select a user and review their **Logon Inactivity Threshold**.

Enable Users

Follow the steps to enable users:

1. Go to **System** > **Security**.
2. Expand **Users** and select the user.
3. In **General**, set **Is Enabled** to **True**.
4. Select **Save**.

Remove Users From Groups

Because group membership determines access to artifacts and tools, be sure that you want to remove a user from a group.

1. Select **System** > **Security**.
2. Expand **Users**, then click the user.

3. In **Group Membership**, select the group and click **Remove Selected Item**.
4. Select **Save**.

Manage Users With BRApi

You can complete some user and group management tasks using BRApi functions such as CopyUser, DeleteUser, and CopyGroup. The ability to use these functions is governed by your role as an administrator and may require a Manage System Security role. See Manage System Security.

For example, if a dashboard's design includes a button that uses a BRApi function to support adding users, users that select the button are validated to ensure they are in the Administrator group or associated with the **ManageSystemSecurityUsers** role.

Load and Extract Users

You can bulk load user accounts, groups, and security instead of defining them manually. You can load these artifacts in two ways:

- We recommend you use the **SecurityTemplate.xlsx** file provided by the Sample Templates OneStream Solution to generate an XML load file. See the *Sample Templates Guide*.
- Extract users in the sample GolfStream application, modify the XML export file to specify user and group properties, and then load the file. See Load Users.

Administrators must load users and groups into a new application or one without existing users and groups. If user accounts exist, loaded users are validated by comparing their current security settings to those in the XML load file.

Requirements

By default, only Administrators can load and extract users. To let other users load and extract users, grant them these system security roles:

- SystemLoadandExtractPage System. This is a User Interface role.
- ManageSystemSecurityUsers
- ManageSystemSecurityGroups
- ManageSystemSecurityRoles

Load Users

Follow the steps to load users:

1. Go to **System** > **Tools** > **Load/Extract**.
2. Select **Load**, and browse to an xml load file.
3. Select **Load**.
4. When processing finishes, review the user list and user settings to ensure the loaded users are correctly defined.

Extract Users

You can extract users, groups, and security roles to an XML export file.

1. Go to **System** > **Tools** > **Load/Extract**.
2. Select **Extract**, and then select **File Type** > **Security**.
3. In **Items to Extract**, select **Users**. Select **Export Unique IDs** to also extract each user's ID.

4. Take one of the following actions:
    - Select **Extract** to specify where to save the extract file.
    - Select **Extract and Edit** to view and modify the data in an XML Editor.

Create and Manage Groups

By default, only an administrator can perform the tasks described in the following topics. An administrator can enable other users to complete these tasks by assigning specific system security roles. See Requirements.

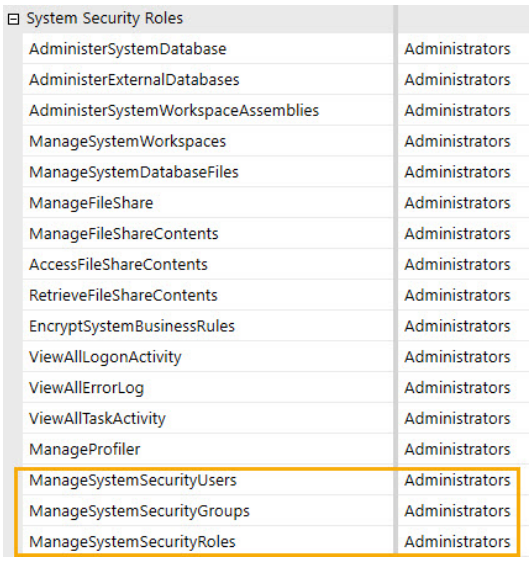
In this topic:

- About Groups and Inherited Security
- About Exclusion Groups
- Tips and Best Practices
- Create Groups
- Create Exclusion Groups
- Manage Groups
- Load and Extract Groups

Requirements

To let non-administrators create and manage users and groups, grant them group-based access to the required security roles.

1. Go to **System** > **Security** > **System Security Roles**.
2. Select **Edit** by these roles to assign the group in which the user is a member:
    - **ManageSystemSecurityUsers**: Assignees can create, modify, and manage users.
    - **ManageSystemSecurityGroups**: Assignees can define, modify, and manage groups.
    - **ManageSystemSecurityRoles**: Assignees can manage roles to provide group-based, function-specific access to artifacts and tools.



System Security Roles	
AdministerSystemDatabase	Administrators
AdministerExternalDatabases	Administrators
AdministerSystemWorkspaceAssemblies	Administrators
ManageSystemWorkspaces	Administrators
ManageSystemDatabaseFiles	Administrators
ManageFileShare	Administrators
ManageFileShareContents	Administrators
AccessFileShareContents	Administrators
RetrieveFileShareContents	Administrators
EncryptSystemBusinessRules	Administrators
ViewAllLogonActivity	Administrators
ViewAllErrorLog	Administrators
ViewAllTaskActivity	Administrators
ManageProfiler	Administrators
ManageSystemSecurityUsers	Administrators
ManageSystemSecurityGroups	Administrators
ManageSystemSecurityRoles	Administrators

To revoke the ability to manage users, groups and roles, remove assignees from the relevant role. See Manage System Security.

About Groups and Inherited Security

You cannot assign individual users access to tools and artifacts. System security roles to which you assign groups determine this access. Create groups to grant large numbers of users or other groups the function-specific access that they require.

You can define nested groups to best suit your organizational entities, workflows, and reporting structures. Nested groups contain lower-level child groups. In this case, child groups, and the users that they contain, inherit the access defined for the parent group.

> **NOTE:** Groups cannot be externally authenticated.

About Exclusion Groups

Use exclusion groups to grant almost everyone, except a particular group or a few users, access to a tool or artifact. For example, if everyone but User1 and User2 must create dashboards, define an exclusion group in which User1 and User2 are members set to Deny Access. All other members are set to Allow Access. To easily grant access to dashboards, assign the exclusion to which gives everyone access except User1 and User2.

Because groups providing access to data and artifacts may contain many groups, removing just a few users, to reflect a corporate reorganization for example, from the group hierarchy can be time-consuming. To reflect the reorganization, create an exclusion group with the users involved and apply it to the roles they no longer need.

Tips and Best Practices

- The administrator is assigned to all roles, so they can always manage artifacts, data, and tools. Assigning other groups to security roles does not revoke the administrator's access.
- Child groups, nested in higher-level parent groups, can access the tools and artifacts that the parent group can, given the parent group's assignment to system security roles. This access is inherited in group hierarchies, from a parent level downward to child groups.
- Removing child groups from parent groups revokes access to the tools and artifacts that the parent group provides, based on its assignments to roles.

- In an exclusion group, access to artifacts is determined based on the exclusion order you specify, regardless of a user's membership in a group. To ensure that users who are in several groups cannot access artifacts but everyone else can, set:
    - The groups to which the users belong at the top to **Allow Access**.
    - The individual users below the groups to **Deny Access**.

Create Groups

Follow the steps to create groups:

1. If you are not an administrator, verify that you meet the requirements. See Requirements.
2. Go to **System** > **Security**.
3. Select **Groups**, then select **Create Group**.
4. Enter a name and description.
5. In **Group Membership**, specify the users or child groups to add to the group you are defining, or select a parent group to which to add your new group. Take any of the following actions:

- To include users and groups in the new group, select **Add Users** or **Add Child Group**and select the user or group. Members can access the artifacts and tools for each system security role to which the group is assigned.
- To revoke group membership, select users and groups and select **Remove**. This revokes their access to the tools and artifacts group membership provides based on role assignments.
- To nest the group in a parent group, select **Add Groups** in **Parent Groups That Contain This Group** and select a higher-level group. Members in this parent group inherit its access and permissions based on role assignments.

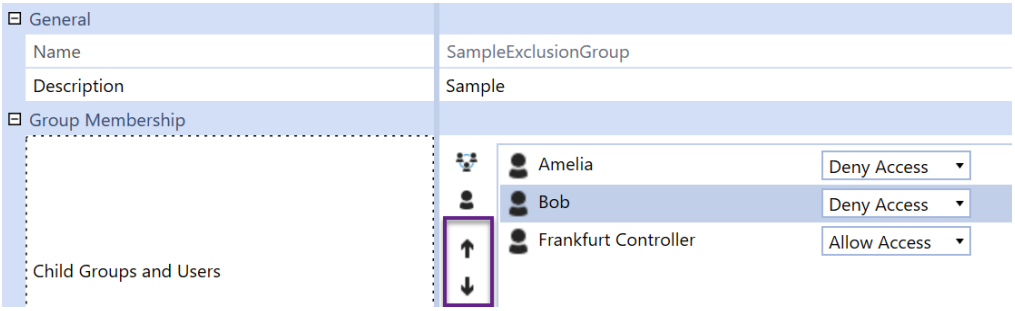
6. Select **Save**.

Create Exclusion Groups

Define an exclusion group to grant almost everyone, except a particular group or a few users, group access to a tool or artifact.

1. Go to **System** > **Administration** > **Security**.
2. Select **Groups**, then select **Create Exclusion Group**.
3. Enter a name and description that indicate who is being restricted by this group. For example, to exclude a department, use Everyone-But-<Department name>.
4. In **Group Membership**, select **Add Child Groups** or **Add Users** to specify who to include in the group.
5. To prevent members from accessing artifacts to which the group has role-based access, set particular users or groups to **Deny Access**. Otherwise, set members to **Allow Access**.
6. Use the arrows to order the exclusions carefully, because access is granted, regardless of a user's membership in a group, based on the order you specify.

   For example, if Amelia and Bob are in the Frankfurt Controller group, the order below does not restrict them from artifacts, even though they are listed first, because they are in the Frankfurt Controller group.



To ensure Amelia and Bob cannot access artifacts, put Frankfurt Controller first, set to **Allow Access**. Put Amelia and Bob below the group, set to **Deny Access**.

7. Select **Save**.

Manage Groups

Follow the steps to manage groups:

1. If you are not an administrator, meet the Manage Groups.
2. Go to **System** > **Security**.
3. Select **Groups** or **Exclusion Groups**, then select a group.
4. Click to perform any task:
    - **Delete Selected Item**: Permanently delete a group.
    - **Rename Selected Item**: Change a group's name.
    - **Copy Selected Item**: Create a group based on the existing group's settings. Select **Copy child user and group references** to add the same users or groups to the new group.
    - **Show All Users**: View the users in the group.
    - **Show All Groups**: View the lower level groups that are nested in the group.
5. In **Group Membership**, change who is in the current group and modify the parent groups associated with the current group. Take one of the following actions:
    - To withdraw users and groups, select them, and then select **Remove**. This revokes their access to artifacts and tools based on the system security roles to which the group is assigned.

- To add users and groups, select **Add User | Add Child Group**. This grants them access to the artifacts and tools the group provides based on role assignments.
- To withdraw the current group from a parent group, select the parent and select **Remove**. This revokes access to the artifacts and tools provided by the parent group based on role assignments.
- To include the current group in another parent group, select **Add Groups** and select the group.

Manage Group Membership

You can add groups and users to, and remove them from, other groups. This may create a hierarchy or impact system security role-based access to artifacts and tools. See Manage Groups.

1. Go to **System** > **Security**.

2. Expand **Groups**, and select the group.

3. In **Group Membership**, take any of the following actions:

- To include a user or group, select **Add User** or **Add Group** and select the user or group to add.
- To withdraw the current group from a parent group, select the parent and select **Remove**. This revokes access to the artifacts and tools provided by the parent group based on role assignments.
- To include the current group in a parent group, select **Add Groups** and select the group.

Load and Extract Groups

You can bulk load groups, users, and security roles instead of defining them manually. You can load groups in two ways:

- We recommend you use the **SecurityTemplate.xlsx** file provided by the SampleTemplates OneStream Solution to generate an XML load file. See the *Sample Templates Guide*..
- Extract the groups in the sample GolfStream application, modify the XML export file to specify your group properties, and then load the file. See Load Groups.

Administrators must complete the load for a new or empty application that does not contain users or groups. To enable other users to load and extract groups, assign them the required security roles. See Create and Manage Users.

Requirements

To enable other users to load and extract groups, administrators must assign the group in which these users are members access to the following roles:

- SystemLoadandExtractPage
- ManageSystemSecurityGroups
- ManageSystemSecurityUsers
- ManageSystemSecurityRoles

See Manage System Security.

Load Groups

Follow the steps to load groups:

1. If you are not an administrator, see Requirements.
2. Go to **System** > **Tools** > **Load/Extract**.
3. Select **Load**, and browse to an XML load file.
4. Select **Load**.

5. When processing finishes, review the **Groups** list and individual group settings to verify the loaded groups are correctly defined.

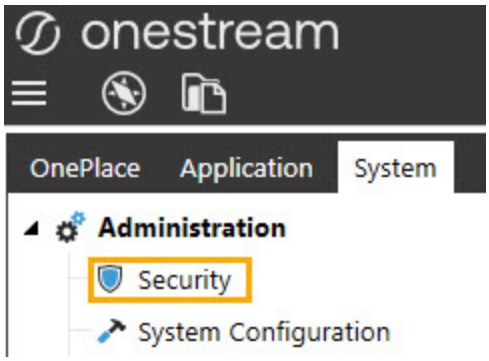
Extract Groups

Follow the steps to extract groups:

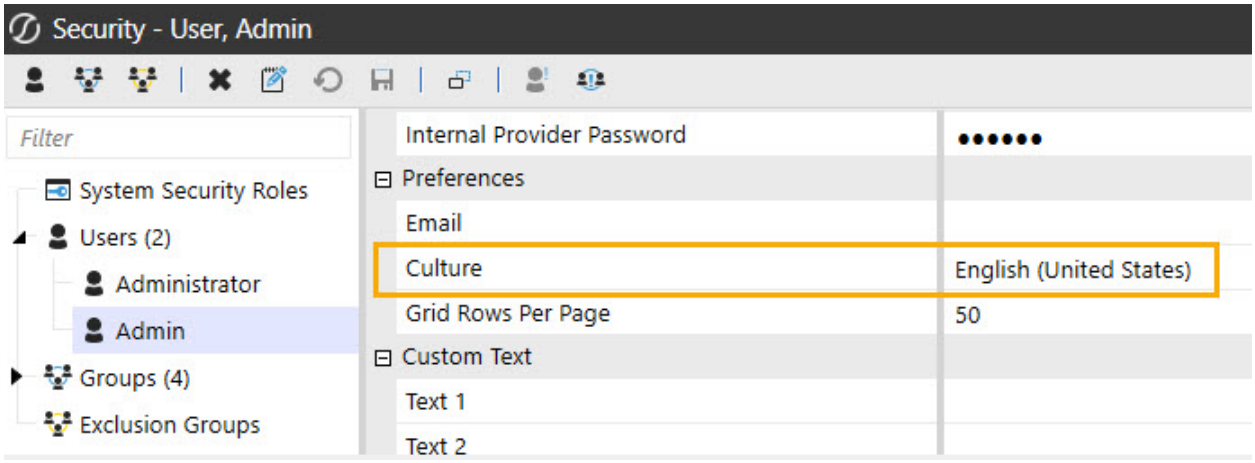
1. If you are not an administrator, see Requirements.
2. Go to **System** > **Tools** > **Load/Extract**.
3. Select **Extract**, and then select **File Type** > **Security**.
4. In **Items to Extract**, select **Security Groups**.
5. Take one of the following actions:
    - Select **Extract** to specify where to save the extract file.
    - Select **Extract and Edit** to modify the extracted data in an XML Editor.

User Culture

A User's culture is set in the Culture property field in each User's configuration. This is located within the Security section in the System tab under Administration.



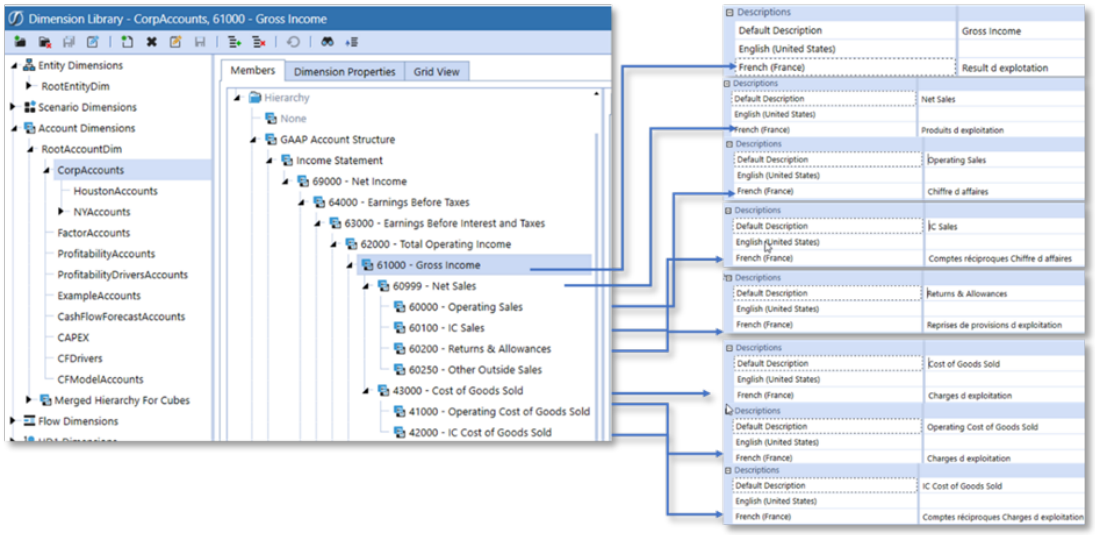
When the User is selected, a property grid will display. The Preferences tab within the property grid will contain an option for Culture which can be selected from the drop-down menu. These options are controlled in the OneStream Server Configuration Utility and additional languages can be added as needed.



Alias Dimension Member Descriptions

Dimension members can have more than one description to reflect other languages for that culture. The properties for the members will be reflected in Cube Views and Quick Views as related to the user's default or prompted culture settings.

In this example shown below, select the **Account Dimension** tab. Next, select the desired Dimension members, 61000 – Gross Income, to be updated. In the Descriptions field under the Member Properties tab, enter the translated description (Result d explotation) next to the language (French) being updated.



Alias Member Descriptions in Cube Views

Dimension members can have more than one description to reflect other languages for that culture. The properties for the members will be reflected in Cube Views and Quick Views as related to the user's default or prompted culture settings. This can be achieved by making certain changes to the Cube View's general settings.

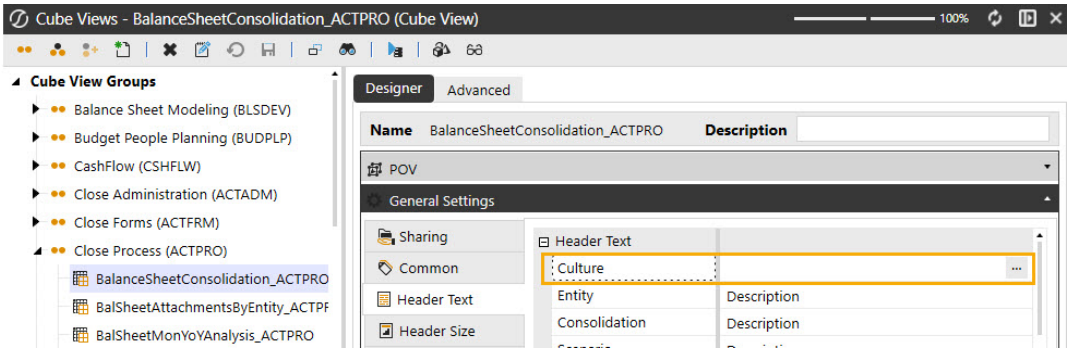
On the **Application** tab, select **Cube Views**, then select an existing Cube View from Cube View Groups or create a new one. On the **Designer** tab, select **General Settings**, and then select the Header Text box.

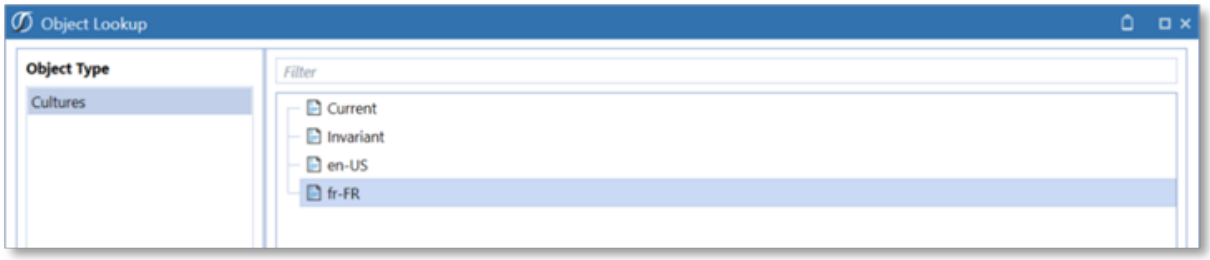
The Culture setting is associated with how the member description will be displayed in the Cube View. This setting can be set multiple ways to display in different languages associated with the application. Selecting the ellipsis at the end of the Culture field will provide options to define how the Members are displayed in the cube view:

Current: This is the default. When blank, it reacts the same as Current, which means the current User's Culture setting is used to apply a Report Alias during CubeVview rendering.

Invariant will display the members in their Default Description as defined in the item's member properties.

Selecting other cultures will display members in their respective languages for any User running the Cube View. In the example below, the Culture of fr-FR is selected and saved to display the members in French.



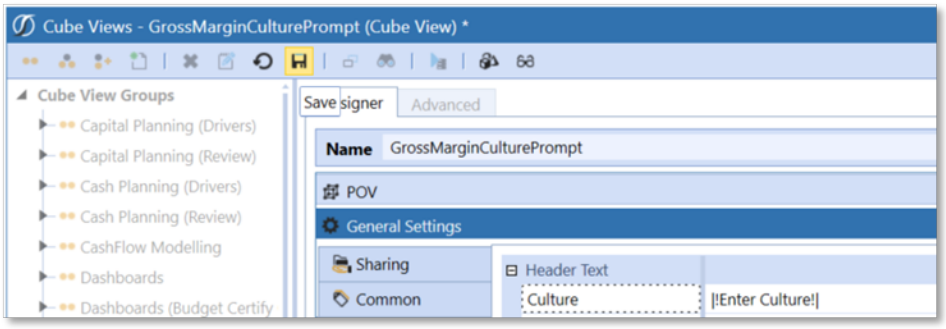


The results display the Account members in French for the given Cube View.

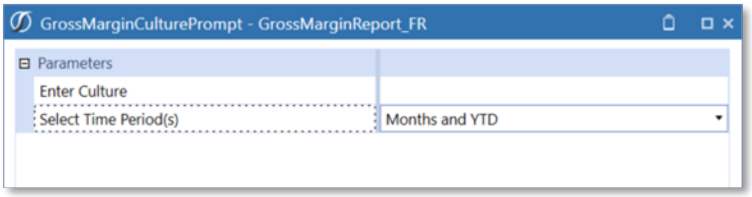
Modify the Culture Setting to Prompt the User for an Alternate Language

The Culture setting can also be set as a prompt to provide the option to change the language each time the Cube View renders. The user can type in a parameter to be used to prompt the user for a culture that will override the user's culture setting established in their security setup.

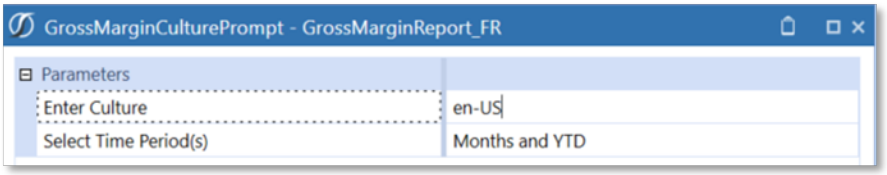
Below, the Parameter|!Enter Culture!| is entered in the Culture field.



To run the cube view, select the **Open Data Explorer** icon. You are prompted to enter the Culture, which you can type in. Alternatively, there could be a parameter set up under Application Dashboards which is a delimited list of applicable Cultures for this application.



You can modify the Culture to reflect English by typing in en-US.



This results in a Cube View display in English accounts.

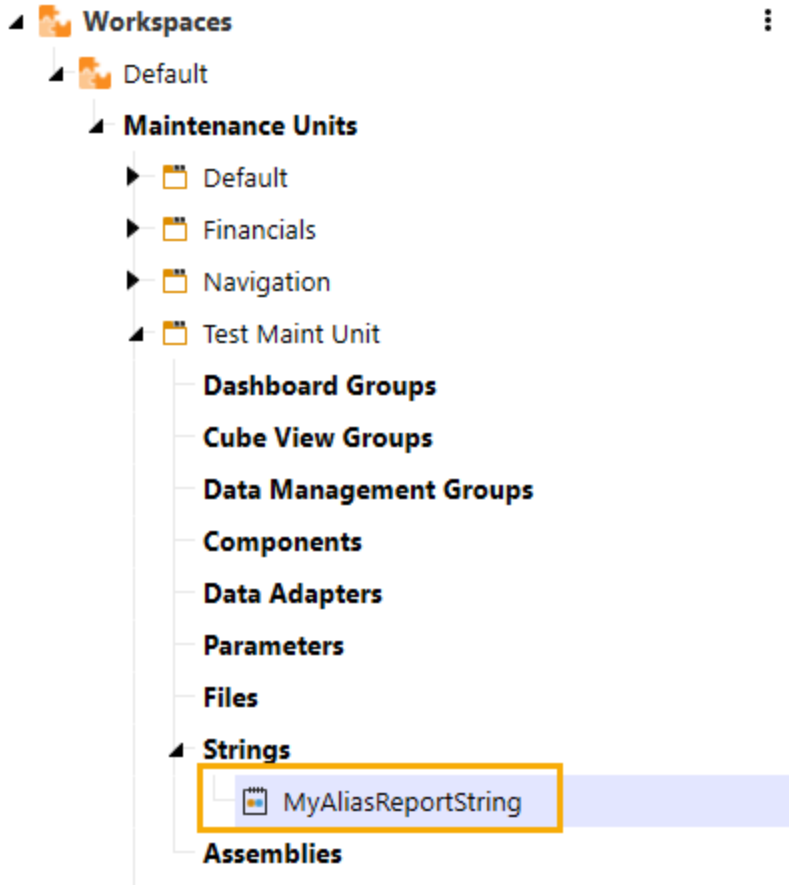
Alias for Headings: Strings within Dashboard Maintenance Unit

Strings are set up as an object type under a Dashboard Maintenance Unit. These strings can be used with XFString functionality and displayed in a Cube View as a caption or heading in a Cube View.

Reference Alias via XFString

You can use Alias strings with the XFString function to display page captions in another designated culture.

> **Example:** On the Application tab, select Workspaces under Presentation. In the Maintenance Units section, select Test Maint Unit group.



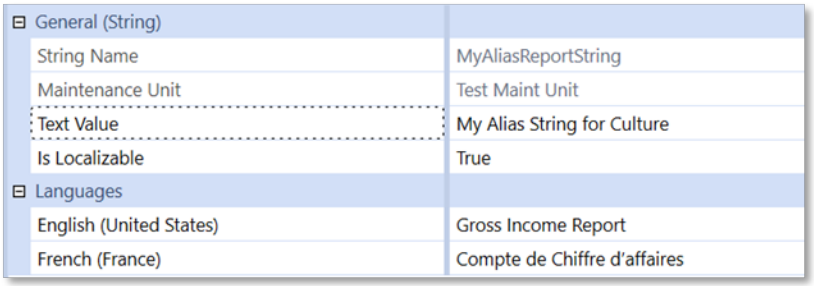
Select the **Strings** section, and then select the **Create String** icon on the toolbar.

This adds a new String called MyAliasReportingString. This will be used in the Cube View example to display the Page Caption of the Cube View report in multiple languages based on the User's default culture setting and througha parameter to prompt the user for a specific culture to render that respective language.

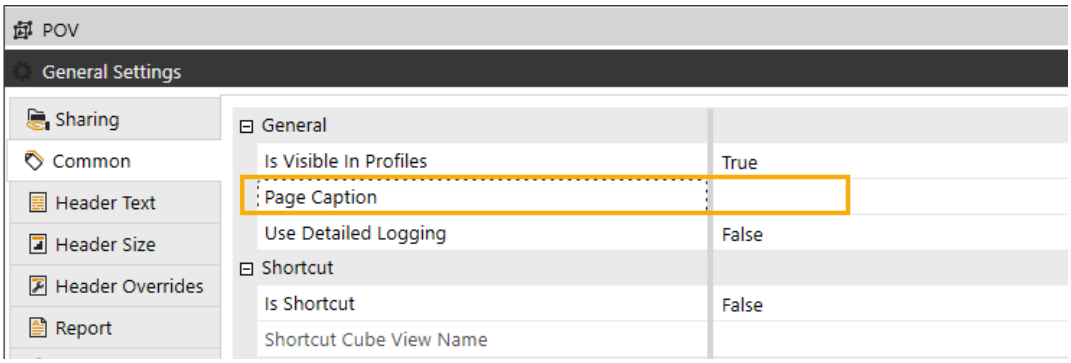
Here are the languages in the string:

- English (United States): Gross Income Report
- French (France): Compte de Chiffre d'affaires

From the General (String) menu, set the **Is Localizable** value to **True**

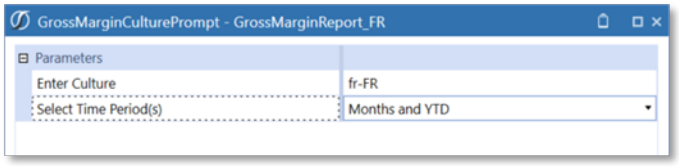


On the Designer tab in **Cube View** > **Common** > **General**, go to the Page Caption section. Update with an XFString function to call a string from the Dashboard Maintenance Units.

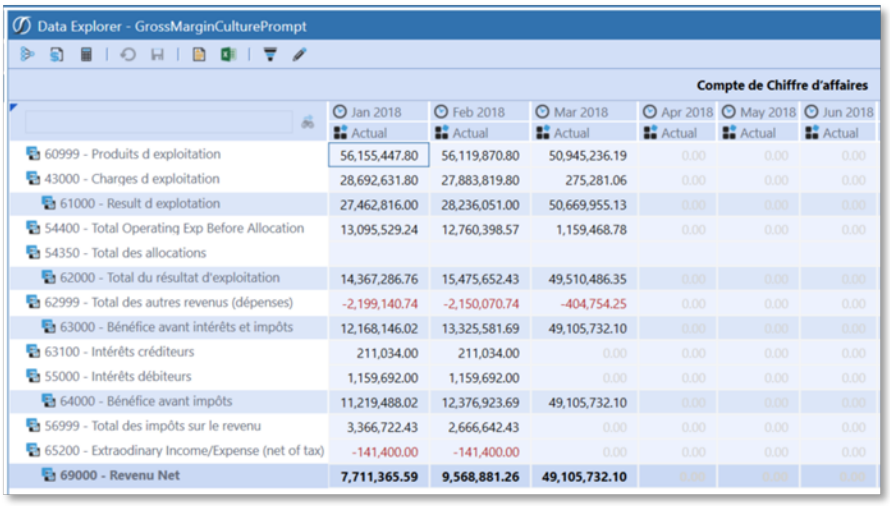


Type in XFString(MyAliasReportString, Culture=|!Enter Culture!|) to the Page Caption field and select the Save button. This formula will call the String, MyAliasReportString.

Using a parameter within the Page Caption in this instance will prompt the user to type in the culture of the language they wish the report caption to render.



The results shown below reflect the page caption of Gross Income Report in French:



	Jan 2018	Feb 2018	Mar 2018	Apr 2018	May 2018	Jun 2018
	Actual	Actual	Actual	Actual	Actual	Actual
60999 - Produits d exploitation	56,155,447.80	56,119,870.80	50,945,236.19	0.00	0.00	0.00
43000 - Charges d exploitation	28,692,631.80	27,883,819.80	275,281.06	0.00	0.00	0.00
61000 - Result d explotation	27,462,816.00	28,236,051.00	50,669,955.13	0.00	0.00	0.00
54400 - Total Operating Exp Before Allocation	13,095,529.24	12,760,398.57	1,159,468.78	0.00	0.00	0.00
54350 - Total des allocations						
62000 - Total du résultat d'exploitation	14,367,286.76	15,475,652.43	49,510,486.35	0.00	0.00	0.00
62999 - Total des autres revenus (dépenses)	-2,199,140.74	-2,150,070.74	-404,754.25	0.00	0.00	0.00
63000 - Bénéfice avant intérêts et impôts	12,168,146.02	13,325,581.69	49,105,732.10	0.00	0.00	0.00
63100 - Intérêts créditeurs	211,034.00	211,034.00	0.00	0.00	0.00	0.00
55000 - Intérêts débiteurs	1,159,692.00	1,159,692.00	0.00	0.00	0.00	0.00
64000 - Bénéfice avant impôts	11,219,488.02	12,376,923.69	49,105,732.10	0.00	0.00	0.00
56999 - Total des impôts sur le revenu	3,366,722.43	2,666,642.43	0.00	0.00	0.00	0.00
65200 - Extraodinary Income/Expense (net of tax)	-141,400.00	-141,400.00	0.00	0.00	0.00	0.00
69000 - Revenu Net	**7,711,365.59**	**9,568,881.26**	**49,105,732.10**	0.00	0.00	0.00

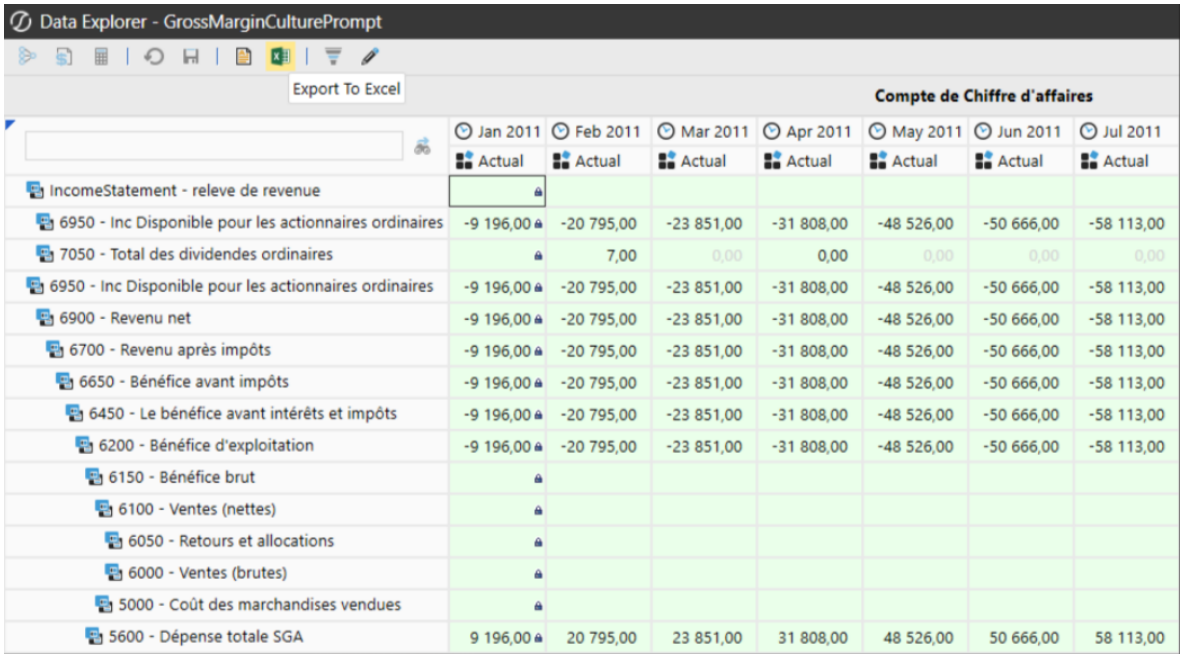
Report Alias (Displaying Alternate Descriptions for Members)

Report Alias functionality can make an end user's reporting analysis or forms entry easier by rendering headings and headers in other languages at runtime so that the user can see these objects in their respective language based on the user's Culture Property setting. Displaying alias descriptions for Members shown in the Headers of Cube Views as well as alias descriptions for Cube View and Report Headings is supported.

Report Alias with Spreadsheet and Excel

If alias properties are populated, the result is translated or alias member names are rendered in the Spreadsheet feature and Excel Add-in from Quick Views, exported Cube Views and using Cube View Connections.

For example, in the Cube View via Data Explorer, select the **Export To Excel** icon.



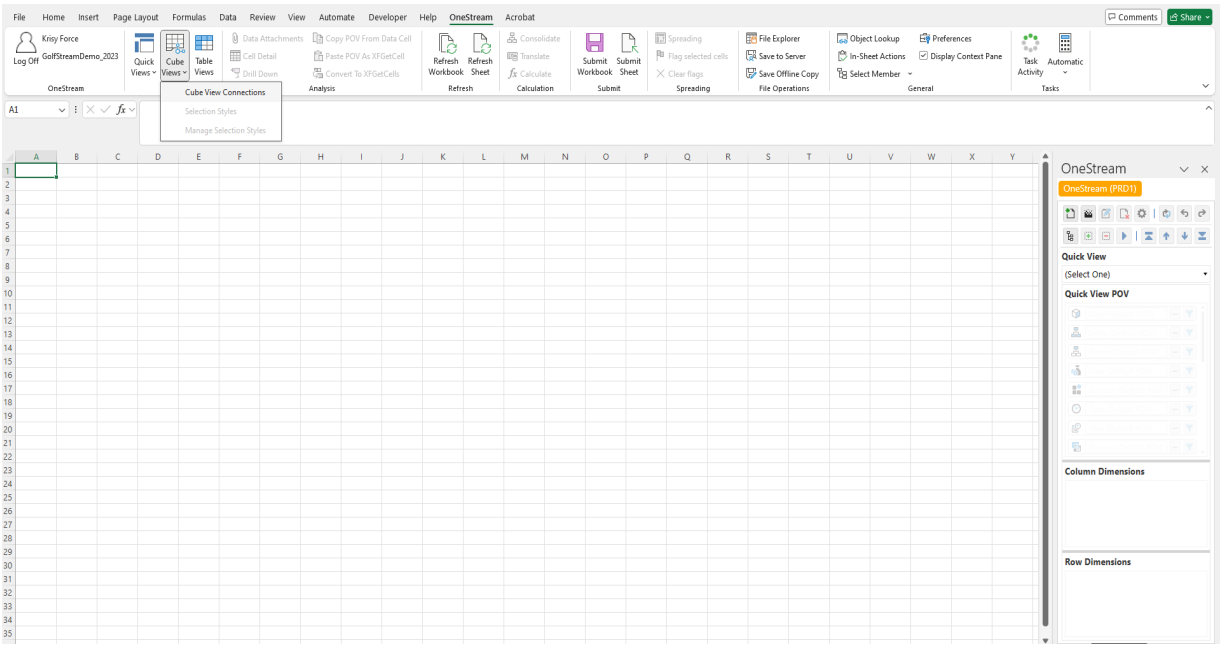
Compte de Chiffre d'affaires

	Jan 2011	Feb 2011	Mar 2011	Apr 2011	May 2011	Jun 2011	Jul 2011
	Actual	Actual	Actual	Actual	Actual	Actual	Actual
IncomeStatement - releve de revenue							
6950 - Inc Disponible pour les actionnaires ordinaires	-9 196,00	-20 795,00	-23 851,00	-31 808,00	-48 526,00	-50 666,00	-58 113,00
7050 - Total des dividendes ordinaires		7,00	0,00	0,00	0,00	0,00	0,00
6950 - Inc Disponible pour les actionnaires ordinaires	-9 196,00	-20 795,00	-23 851,00	-31 808,00	-48 526,00	-50 666,00	-58 113,00
6900 - Revenu net	-9 196,00	-20 795,00	-23 851,00	-31 808,00	-48 526,00	-50 666,00	-58 113,00
6700 - Revenu après impôts	-9 196,00	-20 795,00	-23 851,00	-31 808,00	-48 526,00	-50 666,00	-58 113,00
6650 - Bénéfice avant impôts	-9 196,00	-20 795,00	-23 851,00	-31 808,00	-48 526,00	-50 666,00	-58 113,00
6450 - Le bénéfice avant intérêts et impôts	-9 196,00	-20 795,00	-23 851,00	-31 808,00	-48 526,00	-50 666,00	-58 113,00
6200 - Bénéfice d'exploitation	-9 196,00	-20 795,00	-23 851,00	-31 808,00	-48 526,00	-50 666,00	-58 113,00
6150 - Bénéfice brut							
6100 - Ventes (nettes)							
6050 - Retours et allocations							
6000 - Ventes (brutes)							
5000 - Coût des marchandises vendues							
5600 - Dépense totale SGA	9 196,00	20 795,00	23 851,00	31 808,00	48 526,00	50 666,00	58 113,00

This will render the Cube View in Excel in the respective language.

	A	B	C	D	E	F	G	H
1							GrossMarginCultureReport_FR	
2								
3		Jan 2018	Feb 2018	Mar 2018	Apr 2018	May 2018	Jun 2018	Jul 2018
4		Actual	Actual	Actual	Actual	Actual	Actual	Actual
5	60999 - Produits d exploitation	56,155,447.80	56,119,870.80	50,945,236.19	0.00	0.00	0.00	
6	43000 - Charges d exploitation	28,692,631.80	27,883,819.80	275,281.06	0.00	0.00	0.00	
7	61000 - Result d explotation	27,462,816.00	28,236,051.00	50,669,955.13	0.00	0.00	0.00	
8	54400 - Total Operating Exp Before Allocation	13,095,529.24	12,760,398.57	1,159,468.78	0.00	0.00	0.00	
9	54350 - Total des allocations							
10	62000 - Total du résultat d'exploitation	14,367,286.76	15,475,652.43	49,510,486.35	0.00	0.00	0.00	
11	62999 - Total des autres revenus (dépenses)	-2,199,140.74	-2,150,070.74	-404,754.25	0.00	0.00	0.00	
12	63000 - Bénéfice avant intérêts et impôts	12,168,146.02	13,325,581.69	49,105,732.10	0.00	0.00	0.00	
13	63100 - Intérêts créditeurs	211,034.00	211,034.00	0.00	0.00	0.00	0.00	
14	55000 - Intérêts débiteurs	1,159,692.00	1,159,692.00	0.00	0.00	0.00	0.00	
15	64000 - Bénéfice avant impôts	11,219,488.02	12,376,923.69	49,105,732.10	0.00	0.00	0.00	
16	56999 - Total des impôts sur le revenu	3,366,722.43	2,666,642.43	0.00	0.00	0.00	0.00	
17	65200 - Extraodinary Income/Expense (net of tax)	-141,400.00	-141,400.00	0.00	0.00	0.00	0.00	
18	69000 - Revenu Net	7,711,365.59	9,568,881.26	49,105,732.10	0.00	0.00	0.00	

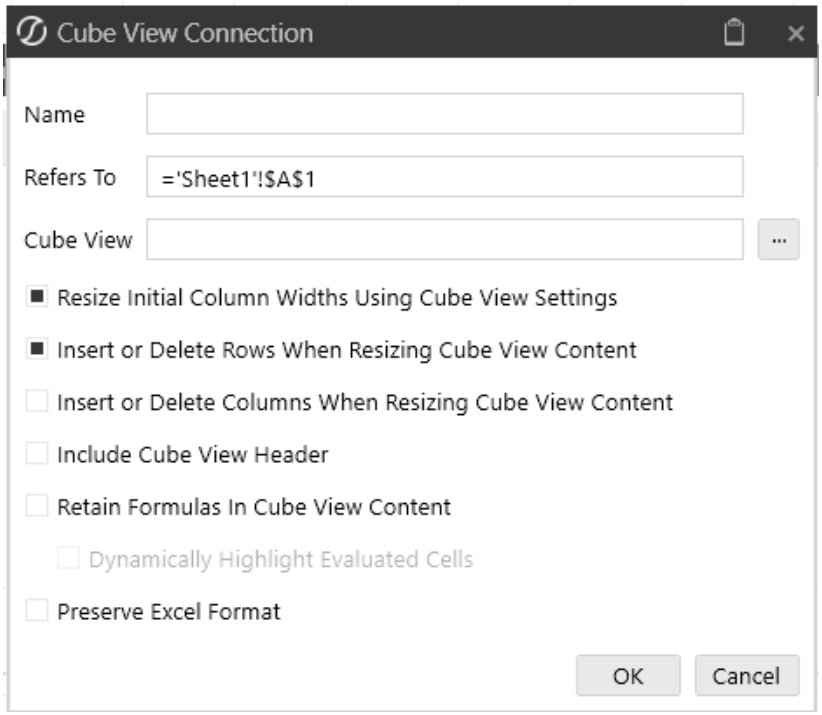
Using Cube View Connections in Spreadsheet and Excel Add-in will also render the Cube View in the language that is established. Open a new or existing Spreadsheet and select **Cube Views** > **Cube View Connections** in the OneStream menu.



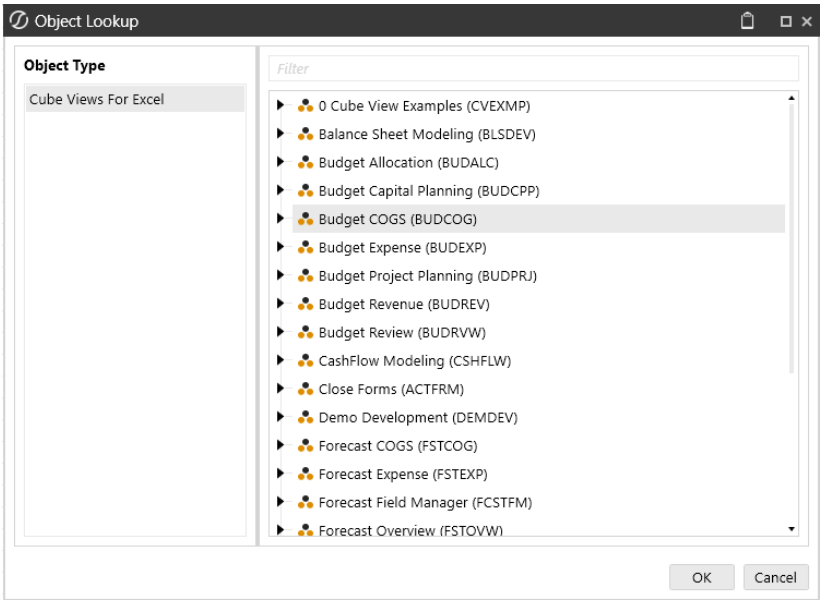
Select **Add** in the **Cube View Connections** dialog box.



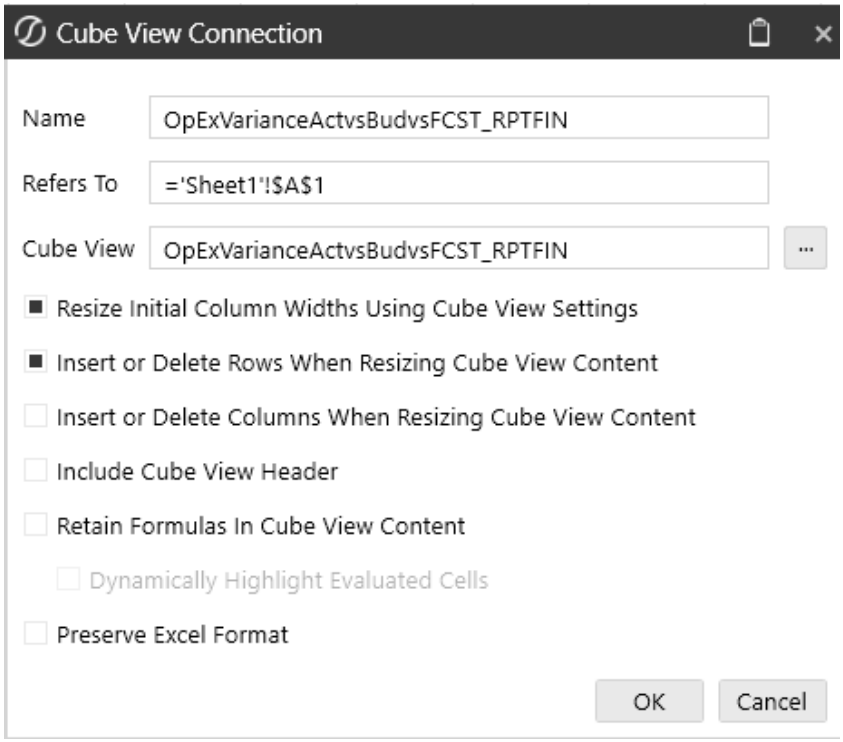
Select the ellipsis button in the next Cube View Connection dialog box.



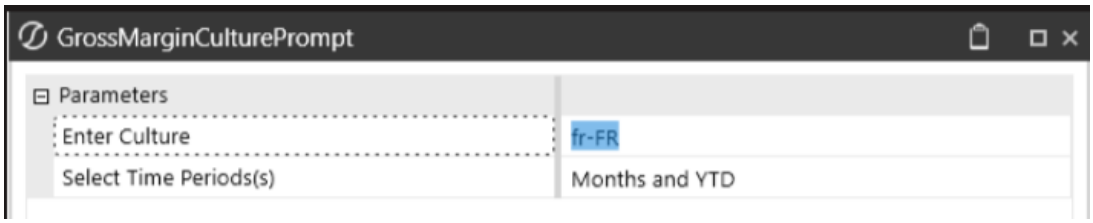
Search for your Cube View (Object Type) and then select the **OK** button.



In the Cube View Connection dialog box, check your settings and select **OK**.



The Cube View selected contains a prompt for Culture and Time Periods. Enter those accordingly and select **OK**.



This Cube View is now added. Select the **Close** button to view the results.

The results of the Cube View connection with the Language updates (Report Alias) in the Cube View.

B4 | IncomeStatement - releve de revenue

	A	B	C	D	E	F	G	H	I	J
1										
2			Jan 2011	Feb 2011	Mar 2011	Apr 2011	May 2011	Jun 2011	Jul 2011	Aug 2011
3			Actual	Actual	Actual	Actual	Actual	Actual	Actual	Actual
4		IncomeStatement - releve de revenue								
5		6950 - Inc Disponible pour les actionnaires ordinaires	-9196	-20795	-23851	-31808	-48526	-50666	-58113	-64203
6		7050 - Total des dividendes ordinaires		7	0	0	0	0	0	0
7		6950 - Inc Disponible pour les actionnaires ordinaires	-9196	-20795	-23851	-31808	-48526	-50666	-58113	-64203
8		6900 - Revenu net	-9196	-20795	-23851	-31808	-48526	-50666	-58113	-64203
9		6700 - Revenu après impôts	-9196	-20795	-23851	-31808	-48526	-50666	-58113	-64203
10		6650 - Bénéfice avant impôts	-9196	-20795	-23851	-31808	-48526	-50666	-58113	-64203
11		6450 - Le bénéfice avant intérêts et impôts	-9196	-20795	-23851	-31808	-48526	-50666	-58113	-64203
12		6200 - Bénéfice d'exploitation	-9196	-20795	-23851	-31808	-48526	-50666	-58113	-64203
13		6150 - Bénéfice brut								
14		6100 - Ventes (nettes)								
15		6050 - Retours et allocations								
16		6000 - Ventes (brutes)								
17		5000 - Coût des marchandises vendues								
18		5600 - Dépense totale SGA	9196	20795	23851	31808	48526	50666	58113	64203
19		5050 - Dépense horaire	10	4444	30	40	50	60	70	80
20		5100 - Dépense salariale	1000	2000	3000	4000	5000	6000	7000	8000
21		5150 - Dépense bonus	2138	5132	8553	12488	19136	22339	25731	27766
22		5200 - Frais de commissions	5000	6000	7000	8000	9000	10000	11000	12000
23		5250 - Avantages Dépense horaire	1000	2000	3000	4000	5000	6000	7000	8000
24		5300 - Avantages sociaux Dépenses salariales	10	20	30	40	50	60	70	80
25		5350 - Frais de déplacement et d'entraide	1	2	3	4	5123	6	7	8
26		5650 - Autres dépenses de fonctionnement								
27		5700 - Frais d'amortissement								
28		5750 - La charge d'amortissement								
29		6250 - Autres gains/pertes								
30		6300 - Divers autres gains/pertes								
31		6400 - Dividendes des investissements								
32		6500 - Revenu total d'intérêts								
33		6550 - Charges d'intérêt totales								

System Tools

There are a variety of system tools that can be used to manage the OneStream application. These tools include system business rules, database, tools that allow you to check the overall health of the application environment, and the File Explorer. In this section, you will learn how to use these and other tools to manage the application system.

System Business Rules

You can use System Extender business rules with Azure Server Sets for enhanced scalability at the Azure Database and Server Sets level. You can perform Server and eDTU scaling manually or using System business rules. If System business rules is selected as a Scaling Type, then a user-defined System Extender business rule determines if scaling is needed. You must implement the scaling function and return the proper scaling object by adding a System Extender business rule and assigning it appropriately.

Under each Case statement, use these rules and related Args and BRApis to check the current Server Set capacity, query metrics about a Server Set or Azure Database, and identify the impact of the Server Sets volume or level of Azure Database deployed. See "Azure Database Connection Settings" in the *Installation and Configuration Guide*.

Example starting point of empty System Extender business rule upon creation:

```
Namespace OneStream.BusinessRule.SystemExtender.ServerSet2
    Public Class MainClass
        Public Function Main(ByVal si As SessionInfo,
                             ByVal globals As BRGlobals,
                             ByVal api As Object,
```

```
                            ByVal args As SystemExtenderArgs) As Object
            Try
                Select Case args.FunctionType
                    Case SystemExtenderFunctionType.Unknown
                        ' Handle unknown function type

                    Case SystemExtenderFunctionType.GetDesiredServerSetCapacity
                        ' Handle desired server set capacity

                    Case SystemExtenderFunctionType.GetDesiredElasticDatabasePoolCapacity
                        ' Handle desired elastic database pool capacity

                    Case SystemExtenderFunctionType.GetDesiredExternalServerSetCapacity
                        ' Handle desired external server set capacity
                End Select

                Return Nothing
            Catch ex As Exception
                ' Log and throw exception
                Throw ErrorHandler.LogWrite(si, New XFException(si, ex))
            End Try
        End Function
    End Class
End Namespace
```

Sample System Business Rule

Metrics are passed to this function to help users determine if a server or database needs scaling. For server scaling, Environment metrics and Scale Set metrics are passed. For database scaling, Environment metrics and SQL Server Elastic Pool metrics are passed.

```
Select Case args.FunctionType

    Case SystemExtenderFunctionType.Unknown

    Case SystemExtenderFunctionType.GetDesiredScaleSetCapacity
        Dim systemExtenderScaleSetResult As New SystemExtenderScaleSetResult
        systemExtenderScaleSetResult.Capacity = args.ScaleSetArgs.CurrentScaleSetCapacity

        If args.ScaleSetArgs.ScaleSetMetricValues.AvgCPUUtilization > 50 Then
            systemExtenderScaleSetResult.Capacity =
args.ScaleSetArgs.CurrentScaleSetCapacity + 1
        End If

        Return systemExtenderScaleSetResult

    Case SystemExtenderFunctionType.GetDesiredElasticDatabasePoolCapacity
```

```
        Dim systemExtenderSQLServerElasticPoolResult As New
SystemExtenderSQLServerElasticPoolResult
        systemExtenderSQLServerElasticPoolResult.AzureElasticPoolDTU =
args.SQLServerElasticPoolArgs.DatabaseAndPoolDTU.AzureElasticPoolDTU

        If
args.SQLServerElasticPoolArgs.AzureElasticPoolLevelMetricValues.DTUConsumptionPercent > 90
Then
            systemExtenderSQLServerElasticPoolResult.AzureElasticPoolDTU = 1600
        End If

        Return systemExtenderSQLServerElasticPoolResult

    Case SystemExtenderFunctionType.GetDesiredExternalScaleSetCapacity

End Select
```

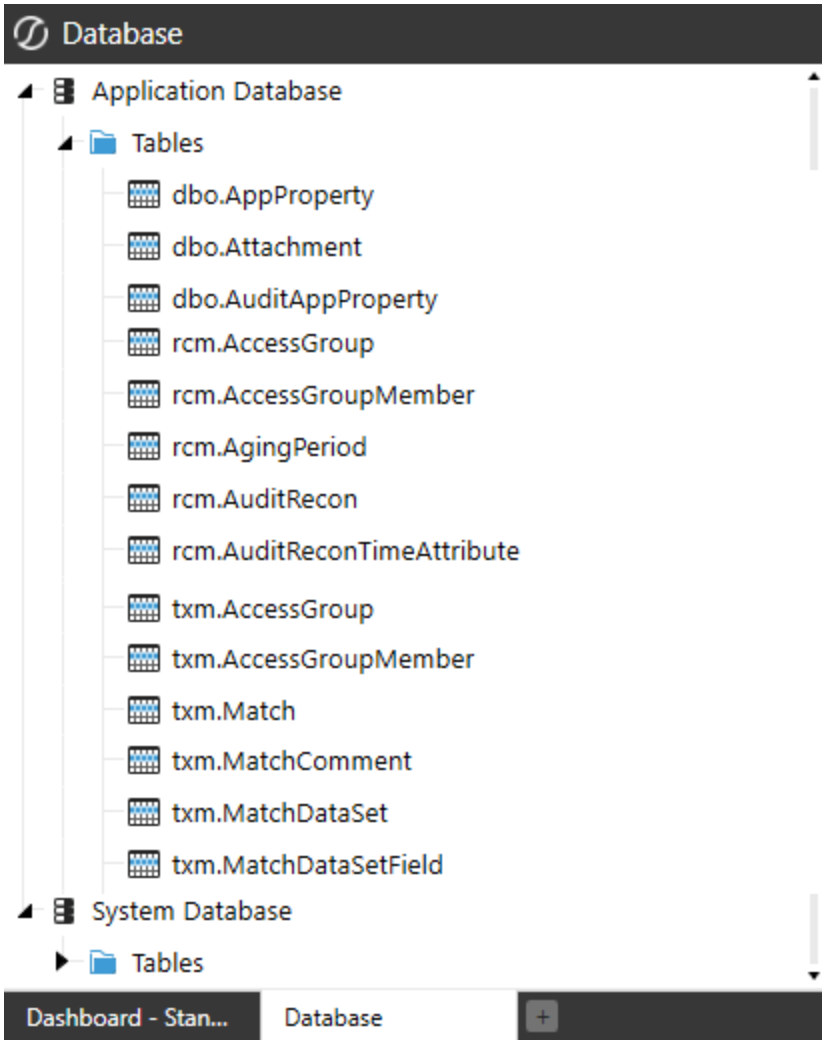
Database

The **Database** screen allows System Administrators to view database tables and provides tools for managing stored data and other information. To view the **Database** screen, go to **System** > **Tools** > **Database**.

Database Tables

Go to **Application Database** > **Tables** or **System Database** > **Tables** to view all tables in the Application Database or System Database. This view provides read-only access to the data tables that can be used for debugging tasks that do not affect the database or system logs.

Data tables that are imported through OneStream Solutions have their schema name added to the beginning of the database table name and replace dbo,for example, rcm.AccessGroup and txm.AccessGroup.



Tools

Database Tools enable System Administrators to manage the database.

Data Records

Go to **Application Database** > **Tools** > **Data Records** to view data for the entire system. Filter the data using the member filter.

Database Administration

The Database Administration feature enables you to copy database tables and edit views from the System Database Page in the OneStream Windows application. Administrators and solution designers can use it to maintain and deploy custom tables without direct SQL database access.

Database Administration tasks are advanced and intended for users with extensive database expertise.

Key Features

- Ability to copy database tables and views
- Modify view definition scripts to support environment migrations, database updates, and application name changes
- Rename and delete database tables and views
- Edit application references in the **StageBIBlendInformation** table to support environment migrations and application name changes

Configure Security

Administer Database requires **Enable Database Administration** to be enabled for the environment, as well as application-level and system-level provisioning. These roles allow administrators to limit access to only the required databases in a OneStream environment.

The Administer Database can be used in:

- Application Databases
- System Database
- External Databases

When using Database Administration:

- Application databases can be managed only within the currently logged-in application. Tables and views cannot be copied across environments or applications
- Deleting tables is allowed only on tables containing: **_Copy** or **_Delete**
- Application-level and system-level security roles apply only to databases where **Enable Database Administration = True** is set in the OneStream Application Server Configuration file

Enable Database Administration

Database Administration is intended for users with extensive database expertise and is available only by request through OneStream Support. To enable, ask OneStream Support to update the **Database Server Connections** collection by setting **Enable Database Administration = True** for each required database server connection in each environment.

With Database Administration enabled:

- When applied to the **OneStream Database Server**, this setting enables Database Administration for all OneStream applications and the System database, Framework, in the environment.
- Additional database connections are managed by OneStream Cloud Operations and must be enabled in each environment where Database Administration is required.
- **Enable Database Administration = True** makes the database available as a valid destination when copying tables and views.
- **Enable Database Administration = True** overrides Database Security settings configured on the **System Configuration Page**. When you access the Database Page, this setting grants full access, maintenance privileges, and permission to view data.

Application Security Roles

Administer Application Database: Default = Nobody: This application security role is set for each application and allows you to update the StageBIBlendInformation reference and copy, rename, or delete application database tables and views..

System Security Roles

- **Administer System Database**: Default = Nobody: This System Security Role enables the ability to copy, rename, and delete System Database Tables.
- **Administer External Databases**: Default = Nobody: This system security role allows you to copy, rename, and delete OneStream-managed external database tables. It does not apply to custom external database connections created on the System Configuration Page.

Database Access Group Security or System Configuration Page

Database Security provisioning on the System Configuration page grants limited permissions that allow tables to be used as copy sources.

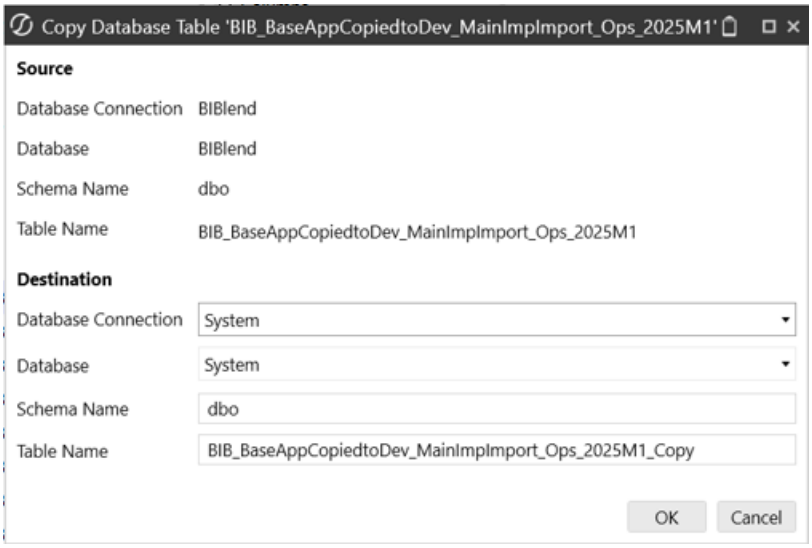
Users provisioned with **AdministerApplicationDatabase**, **AdministerSystemDatabase**, or **AdministerExternalDatabase** for a database with **Enable Database Administration** enabled can use other databases in the environment as copy sources when they also have the required source-database access roles, such as **Access Group for Platform Tables** or **Access Group for Ancillary Tables**.

Administer Database Tasks

These are tasks the administrator can perform.

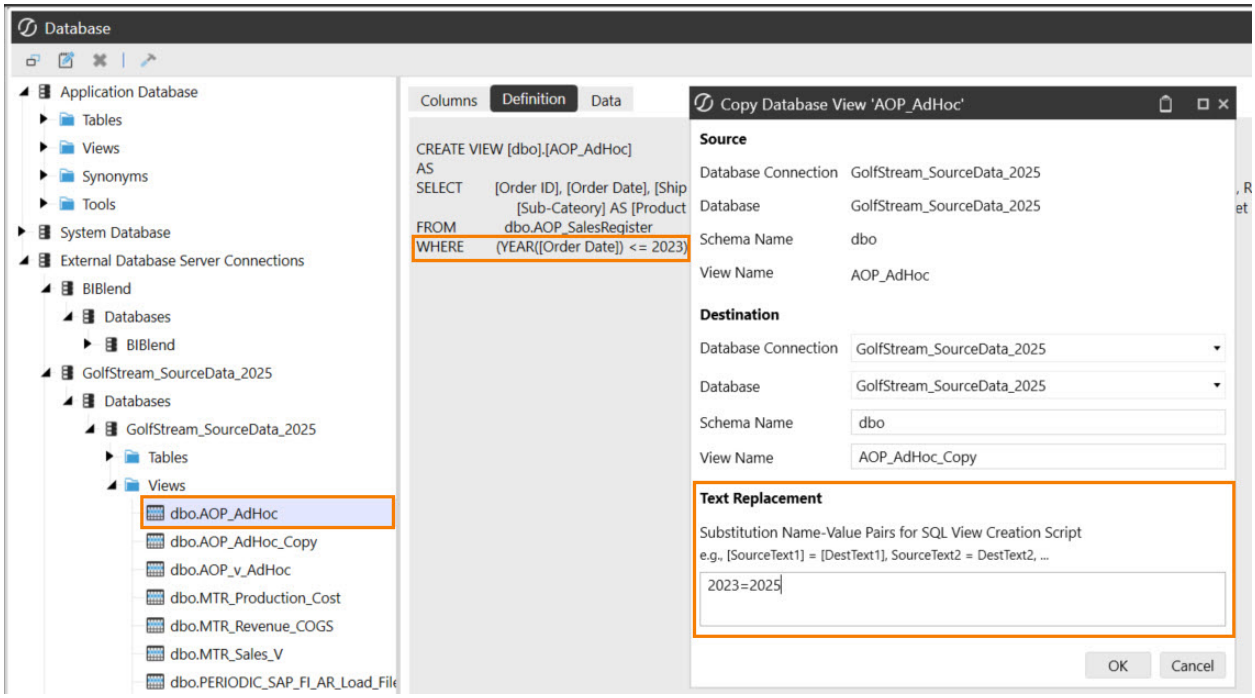
Copy Tables

You can copy tables from any database. Destination databases must be in the current environment and the active application session. Copying tables across environments or to other applications is not supported.



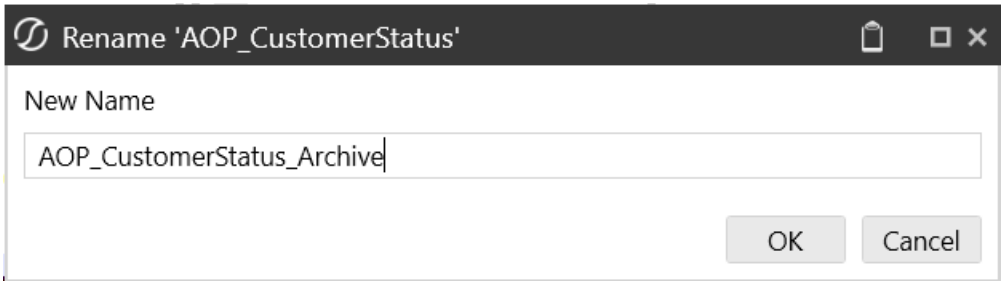
Copy Views and Modify Definitions

You can copy views from any database. Destination databases must be in the current environment and the active application session. Copying views across environments or to other applications is not supported. When a view definition requires a different reference, use the Text Replacement field to update the script without direct SQL database access.



Rename and Delete Tables and Views

You can rename tables and views. Only tables with names that include **_copy** or **_delete** can be deleted.

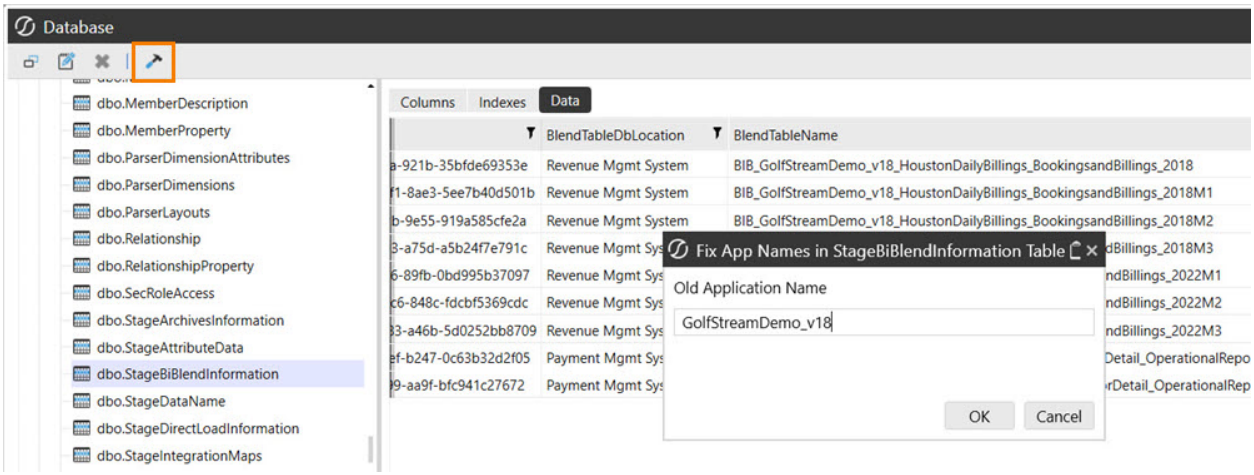


Fix App Names in StageBiBlendInformation

This task renames the application reference in the **StageBiBlendInformation** platform table and related BI Blend database tables. To use, select the **StageBiBlendInformation** table; then the rename option becomes available.

Use this task to reassign a BI Blend database to another application, such as when creating or managing application copies.

The **Fix App Names** text box replaces the entered text with the name of the current application.



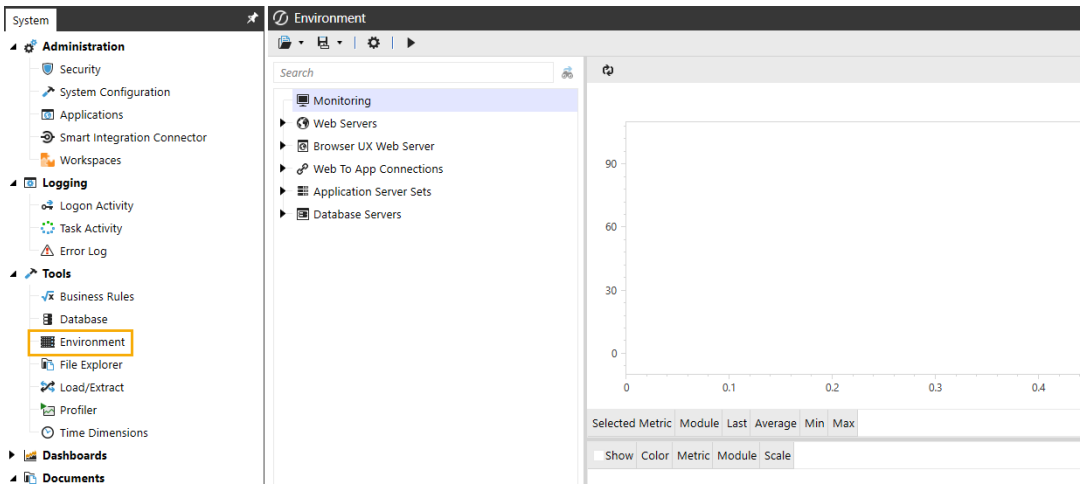
Environment

Use the Environment page to check the overall health of the environment, which contains Web Servers, Mobile Web Servers, Application Server Sets and Database Servers. This will check the connection status as well as the configuration.

The Environment page is designed to give both IT and power users a way to manage and optimize their applications and the environment that is running under. Using the Environment page, the user can monitor the environment, isolate bottlenecks, look at properties and configuration changes, and scale in or out application servers and database resources if needed. They can also customize what data to collect in log files, save collection metrics files, and replay collected performance data in many ways.

To access the Environment page, go to **System** > **Tools** > **Environment**.

> **NOTE:** The Environment page is only accessible in the Windows application.



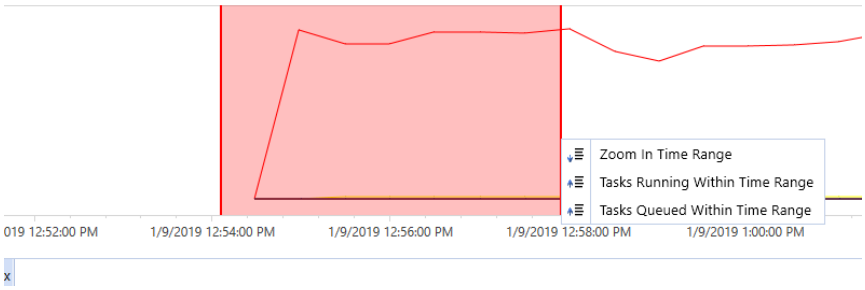
Monitoring Environments

Instead of logging onto the server to collect metrics, use the Monitoring page to access real time Key Performance Indicators (KPIs) across an environment. Go to **System** > **Tools** > **Environment** > **Monitoring** to:

- Access user activity and interactive KPI graphs.
- Track all system components that affect stability and performance.

You can perform these tasks:

- **Open**: Access a metrics and configuration setting file from the File System or a local folder.
- **Save As**: Save metrics and configurations locally or in the File System.
- **Settings**: Specify these types of KPI metrics to monitor and the monitor frequency:
  - Environment
  - Application Servers
  - Database Servers
  - Server Sets
- Zoom into part of the chart to see running or queued activities.



- **Refresh Automatically Using a Timer**: Retrieve metrics based on the Play Update Frequency interval setting.

Specifying General Settings

Set how often and how the Performance charts display data.

- **General Play Update Frequency (seconds):** How often to update Performance charts.
- **Metric and Task Time Range**: Indicate how much historical data to retrieve and depict on the Performance Chart. Applying a time range can help identify the cause of a server event or issue.
- **Y-Axis**: If Auto Range box is selected, the system sets the range for the Min and Max values on the Y-Axis. If cleared, you can set the Min and Max ranges on the Y-Axis.
- **Secondary Y-Axis**: Displays series of a different range of values, or different arguments or values in the same chart. Can be used when the numbers in a chart vary widely from data series to data series, or when there are mixed types of data.

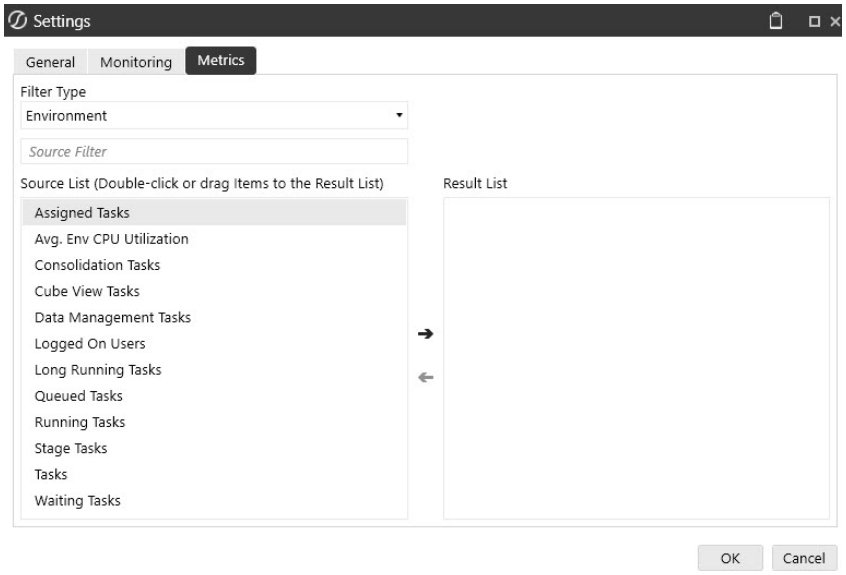
Specifying Monitoring Settings

Select the servers to monitor and the metrics to collect.

- **Monitoring(Server filter)**: Identify specific application or database servers to evaluate.
- **Filter Type**: Specify the type of servers for which to collect metrics.
- **Source Filter**: Use to filter the Source List.
- **Source List**: Displays the servers that meet your criteria.
- **Result List**: Displays selected **Source List** items for which to collect metrics.

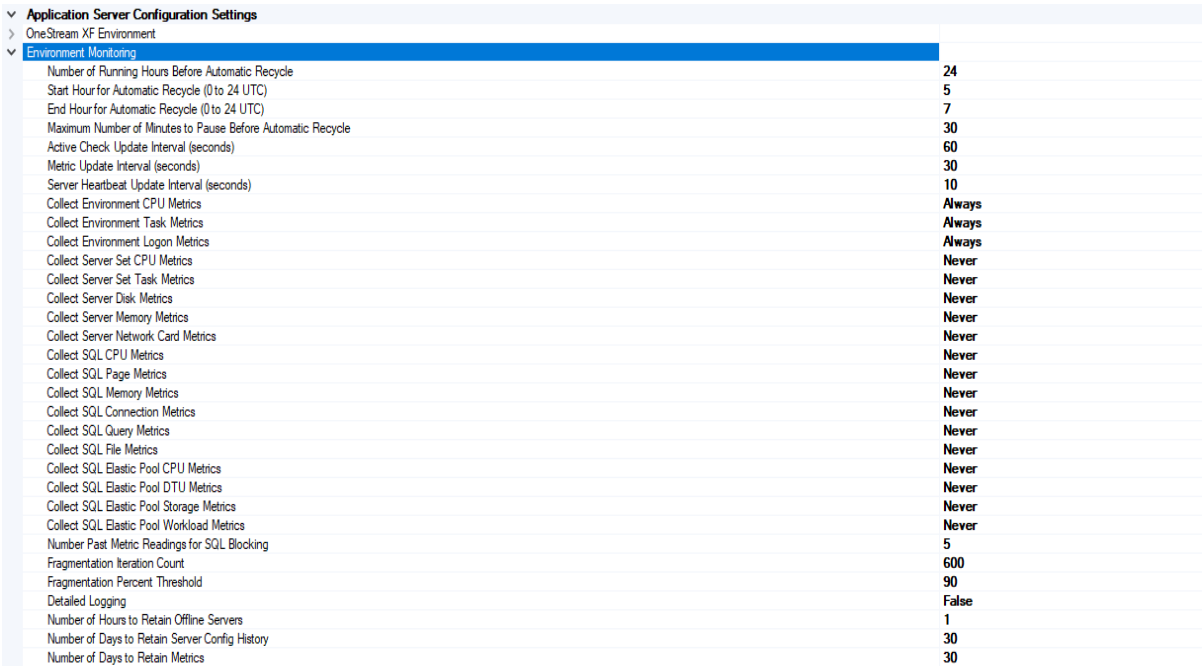
Specifying Metrics Settings

Metrics are collected based on the Metric Update Interval (seconds) setting in the Application Server Configuration utility. To minimize database access and maximize performance, some metrics are collected on every iteration, but some will skip iterations based on count settings defined for a metric.



- **Filter Type**: Refine the types of application servers, database servers or server sets for which to collect metrics.
- **Source Filter**: Use to filter the Source List.
- **Source List**: Displays the list of filtered application servers, database servers or server sets.
- **Result List**: Displays the items for which to collect metrics.

These settings shown below in the Application Server Configuration File in Environment Monitoring, determine which metrics are collected and how often.



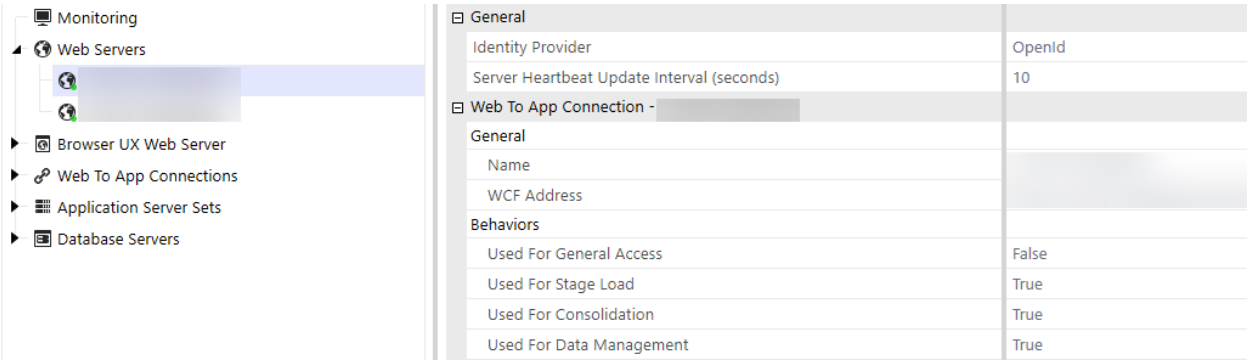
Application Server Configuration Settings	
OneStream XF Environment	
Environment Monitoring	
Number of Running Hours Before Automatic Recycle	24
Start Hour for Automatic Recycle (0 to 24 UTC)	5
End Hour for Automatic Recycle (0 to 24 UTC)	7
Maximum Number of Minutes to Pause Before Automatic Recycle	30
Active Check Update Interval (seconds)	60
Metric Update Interval (seconds)	30
Server Heartbeat Update Interval (seconds)	10
Collect Environment CPU Metrics	Always
Collect Environment Task Metrics	Always
Collect Environment Logon Metrics	Always
Collect Server Set CPU Metrics	Never
Collect Server Set Task Metrics	Never
Collect Server Disk Metrics	Never
Collect Server Memory Metrics	Never
Collect Server Network Card Metrics	Never
Collect SQL CPU Metrics	Never
Collect SQL Page Metrics	Never
Collect SQL Memory Metrics	Never
Collect SQL Connection Metrics	Never
Collect SQL Query Metrics	Never
Collect SQL File Metrics	Never
Collect SQL Elastic Pool CPU Metrics	Never
Collect SQL Elastic Pool DTU Metrics	Never
Collect SQL Elastic Pool Storage Metrics	Never
Collect SQL Elastic Pool Workload Metrics	Never
Number Past Metric Readings for SQL Blocking	5
Fragmentation Iteration Count	600
Fragmentation Percent Threshold	90
Detailed Logging	False
Number of Hours to Retain Offline Servers	1
Number of Days to Retain Server Config History	30
Number of Days to Retain Metrics	30

Web Servers

This section lists all the web servers that are participating in each environment. Each web server will display its configuration and its audited setting.

Configuration

Sample Web Server configuration settings:



Identity Provider

Displays the single sign-on identity provider, if used.

Server Heartbeat Update Interval (seconds)

Specifies how often each server updates its record that it is alive and responding to user input.

Name

Displays the name of the server as it is defined in the web configuration file.

WCF Address

Displays the full URL address of the server.

Used for General Access

Examines the web configuration file to see if it has this server configured as a general server. Settings are True or False.

Used for Stage Load

Examines the web configuration file to see if this server is configured as a Stage server. Settings are True or False.

Used for Consolidation

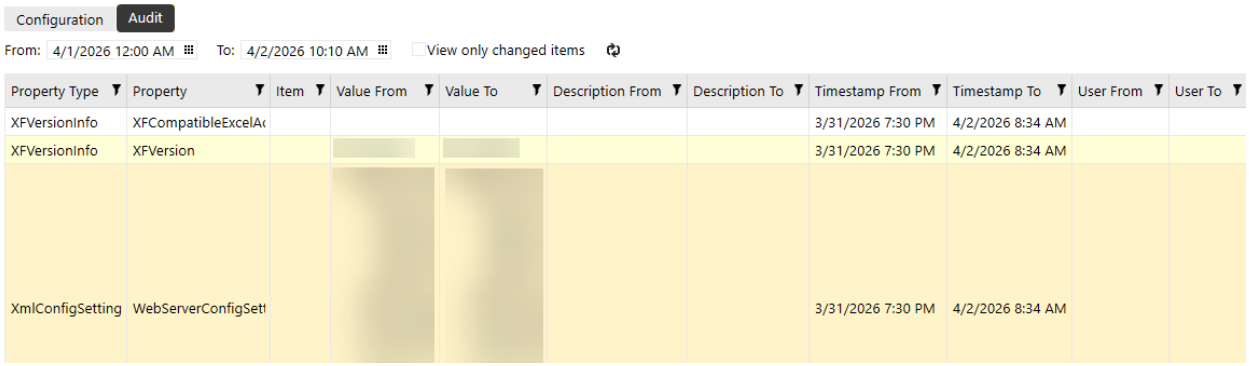
Examines the web configuration file to see if this server is configured as a consolidation server. Settings are True or False.

Used For Data Management

Examines the web configuration file to see if this server is configured as a Data Management server. Settings are True or False.

Audit

Sample Web Server audit setting:



Property Type

Displays the type of server property in the hardware or software that was changed.

Property

Displays the name of the property in the hardware or software that was changed.

Item

Displays the specific sub-setting that changed. If the entire property was updated, column is blank.

Value From

Displays the original value of the property.

Value To

Displays the new value of the property.

Description From

Displays the original description of the setting, if available.

Description To

Displays the new description of the setting, if available.

Timestamp From

Displays the original date and time of the setting, if available.

Timestamp To

Displays the new date and time of the setting.

User From

Displays the original user name, if available.

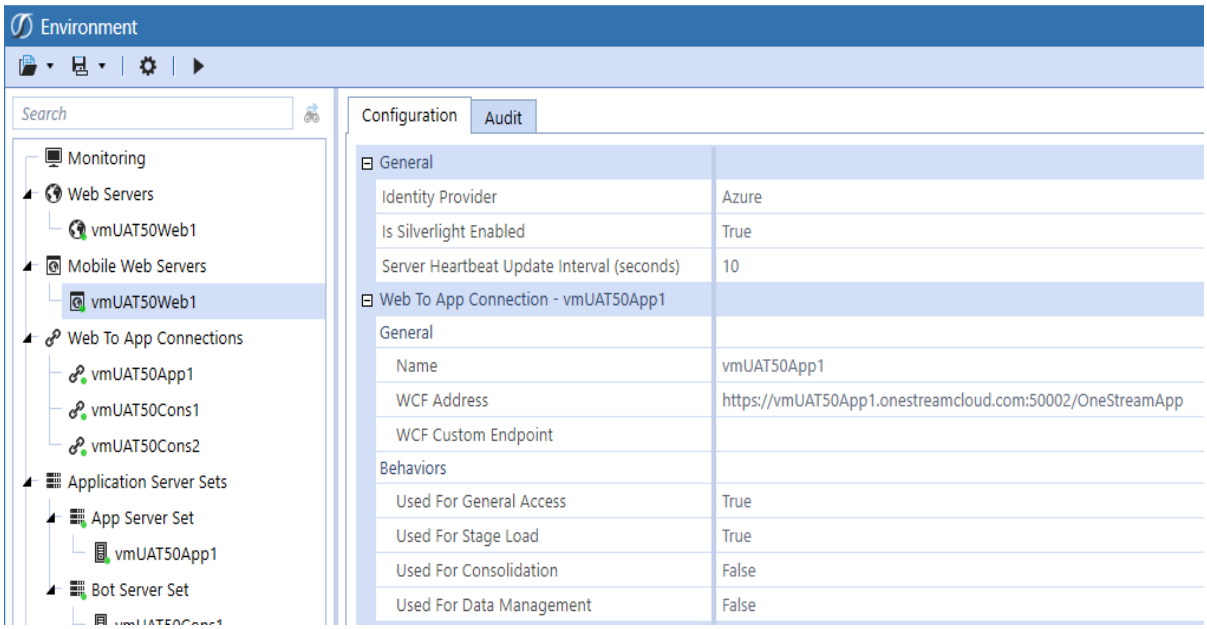
User To

Displays the user name of the person that made the change, if available.

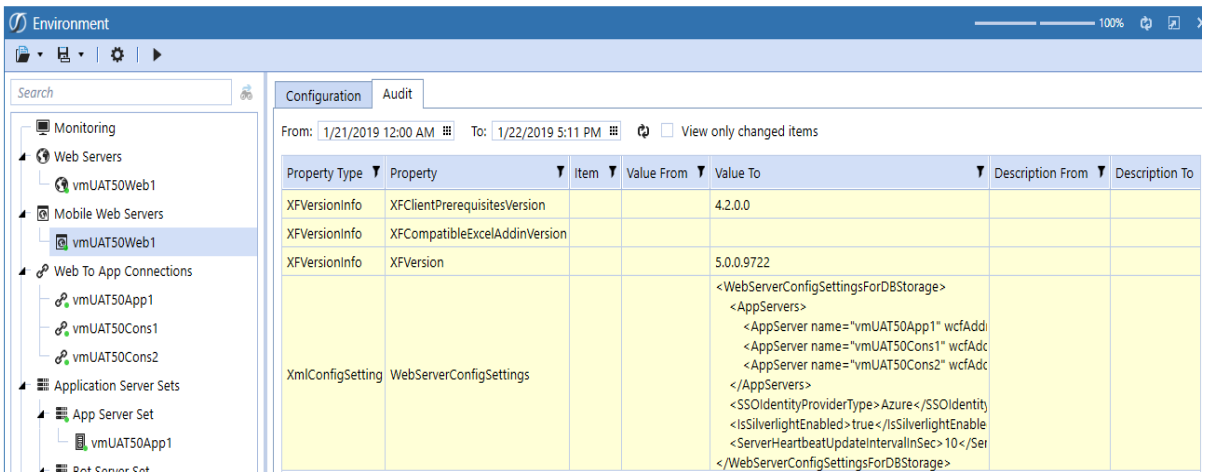
Mobile Web Servers

Similar to the web server, the mobile web servers list all the web servers that are included in that environment. It pulls the information from the ServerHeartBeat table in the Framework database.

Sample Mobile Web Server Configuration



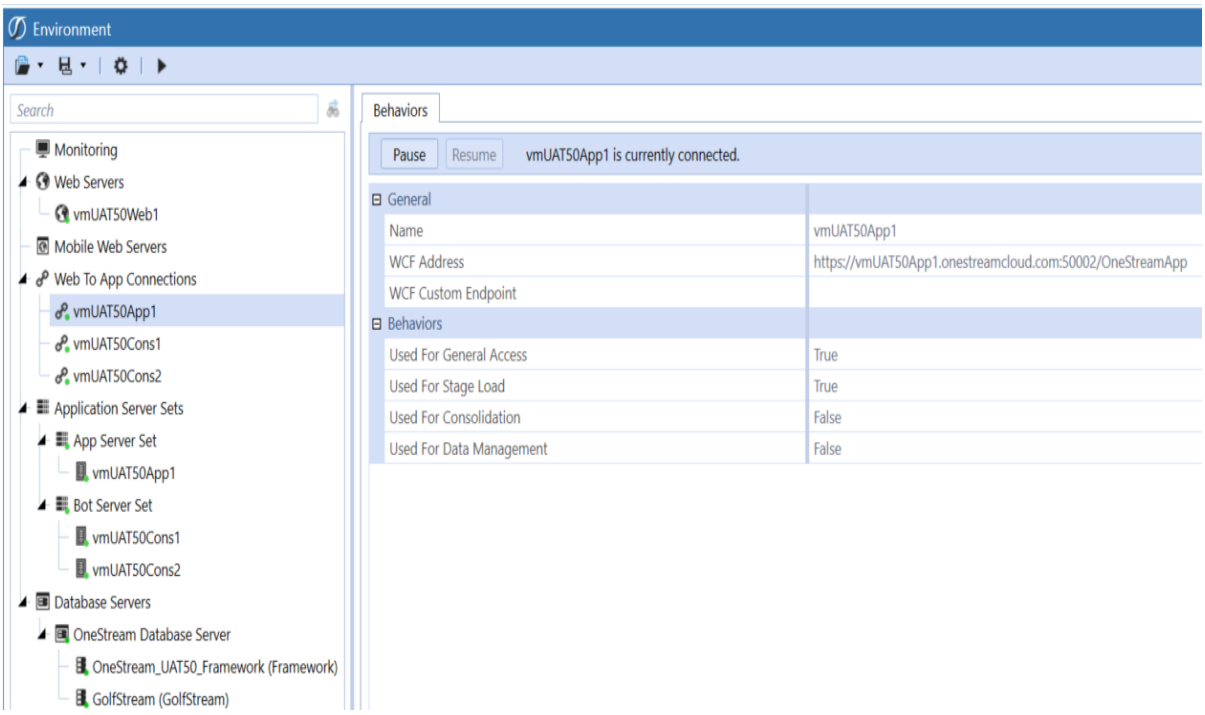
Sample Mobile Web Server Audit



Web To App Server Connections

This section lists all the combined connections from the web server configuration files to all the application servers. From here, the user can pause and then resume a specific connection to an application server or a load balancer which can point to multiple application servers. See the *Installation and Configuration Guide*.

Example Web to App connection configuration:



Pause

Pauses any request to a WCF Address connection. This connection could be either an Application Sever or a Load Balancer. This can be set in the web configuration file.

Resume

Resumes any request to a WCF Address connection. This connection could be either an Application Sever or a Load Balancer. This can be set in the web configuration file.

Name

Displays the name of the server as it is defined in the web configuration file.

WCF Address

Displays the full URL address of the server.

Used for General Access

Examines the web configuration file to see if it has this server configured as a general server. Settings are True or False.

Used for Stage Load

Examines the web configuration file to see if this server is configured as a Stage server. Settings are True or False.

Used for Consolidation

Examines the web configuration file to see if this server is configured as a consolidation server. Settings are True or False.

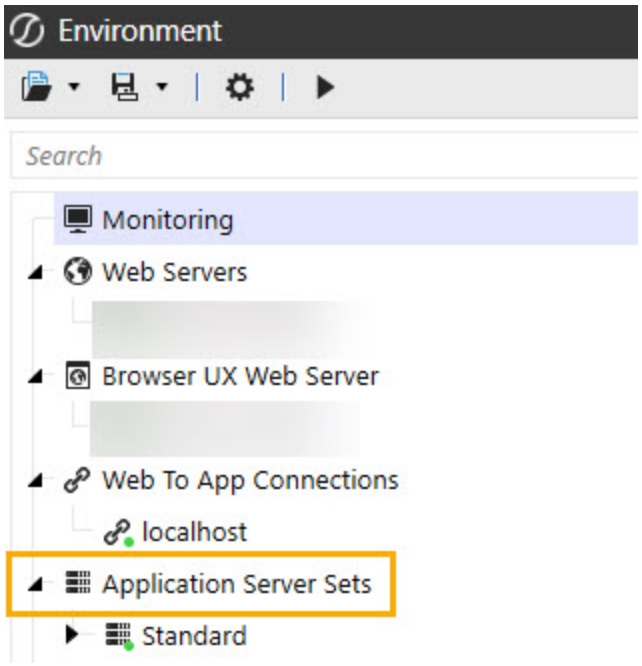
Used for Data Management

Examines the web configuration file to see if this server is configured as a Data Management server. Settings are True or False.

Work With Application Server Sets

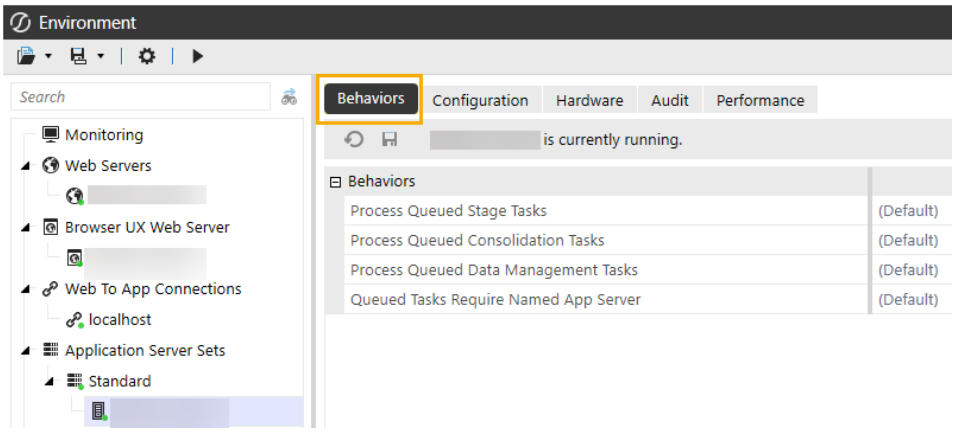
Select **Application Server Sets** to view the server sets participating in an environment. Sets display based on the Server Set configuration in the Application Server Configuration Utility. A red X indicates offline servers. You can access configurations for each server set and server in a server set. If a server is hosted on Azure, you can Scale Out and Scale In the Scale Set manually or by using a System Business Rule.

Sample Application Server Set:



Accessing Server Sets Behaviors

Use the **Behavior** tab to view the capability of a Server Set. You can Scale Out, or remove and Scale In, or add and configure, if the Scaling Type setting is set to Manual or you have ManualAndBusinessRule in the Server Configuration Utility file. This enables you to expand or contract server resources manually or automatically. For scaling with Azure, go to **Server Sets** > **Azure** > **Scaling Type**.

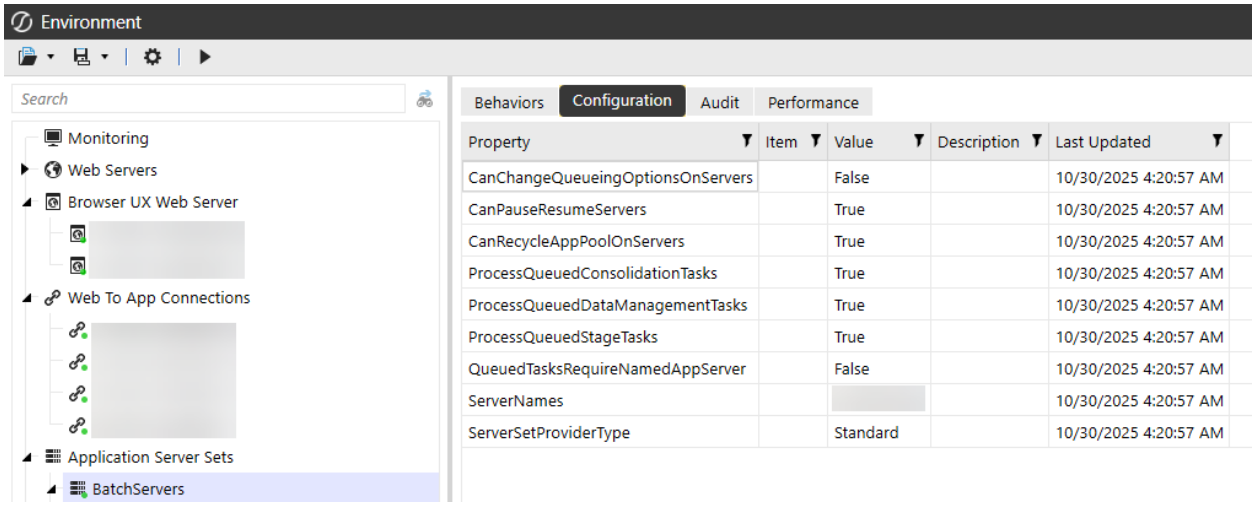


You can specify the following settings at the Server Set level using the Server Configuration Utility but override them at the individual Application Server level:

- **Process Queued Stage Tasks**: If true, the server can process stage tasks.
- **Process Queued Consolidation Tasks**: If true, the server can processes consolidation tasks.
- **Process Queued Data Management Tasks**: If true, the server can process data management tasks.
- **Queued Tasks Require Named App Server**: If true, the server only runs assigned tasks.

Server Sets Configuration

Use the **Configuration** tab to view Server Set configurations defined with the Application Server Configuration Utility. For example:



- **Azure Resource Group Name**: (Azure Scale Set Only) The resource group name for the set.
- **Azure Scale Set Name**: (Azure Scale Set Only) The scale set name in the resource group.
- **Can Change Queuing Options On Servers**: If true, administrators can change the queuing behavior, such as impacting stage, consolidation and data management tasks, of specific servers.
- **Can Pause or Resume Servers**: If set to true, then the user can pause or resume the server from the Environment page via the Pause and Resume buttons.
- **Can Stop or Start Servers**: (Azure Scale Set Only) If true, users can stop or restart the server on the Environment page.

- **Maximum | MinimumCapacity**: (Azure Scale Set Only) A fail-safe setting to identify the maximum and minimum number of servers.
- **Process Queued Consolidation Tasks**: If true, the server can process consolidation tasks.
- **Process Queued <feature> Tasks**: If true, the server can process tasks such as data management and state tasks.
- **Queued Tasks Require Named Application Server**: If true, the server only runs its assigned tasks.
- **Server Names for Standard Server Sets (Supports *? Wildcards)**: Specify server names if the standard server set type is used.
- **Server Set Provider Type**: Specify the external authentication provider used, such as Azure.
- **System Business Rule Name**: (Azure Scale Set Only) The name of the extender business rule for Azure scale set and database scaling.

Using Server Sets Audit

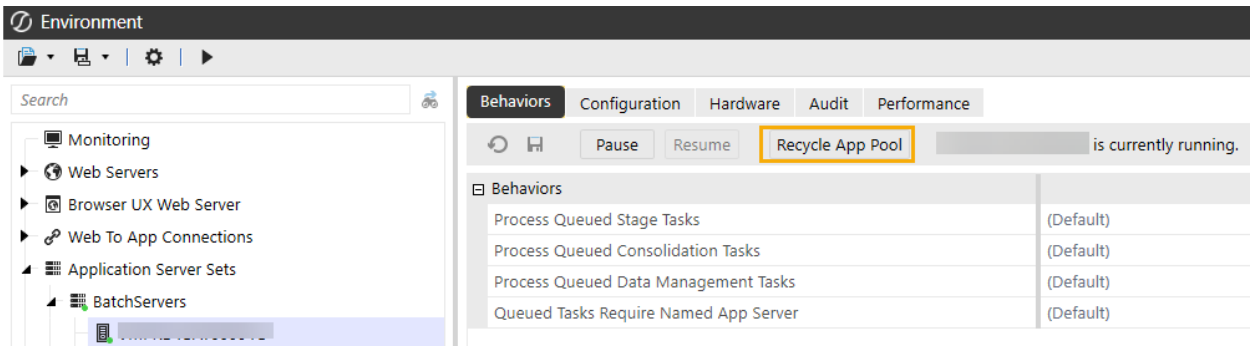
The **Audit** tab identifies all property changes made in **XFAppServerConfig.xml**. Changes display in yellow.

Monitoring Server Sets Performance

Use the **Performance** tab to view scale set and environment metrics, highlighting sections to drill down to time-specific records.

Application Server Behavior

When you select the Behaviors tab, you can pause and resume that server so that none of the long-duration tasks can be run on that particular server. IIS can be recycled by selecting the Recycle App Pool button. Whether these buttons appear or not is based on settings in the OneStream Server Configuration Utility.



Pause

Pause will stop the server from seeking more tasks to run from the queue but will finish tasks that have already started.

Resume

Server will resume accepting tasks from the queue.

Recycle App Pool

Used to recycle the specific server's application pool (reset IIS).

Stop - (Azure Scale Set Only)

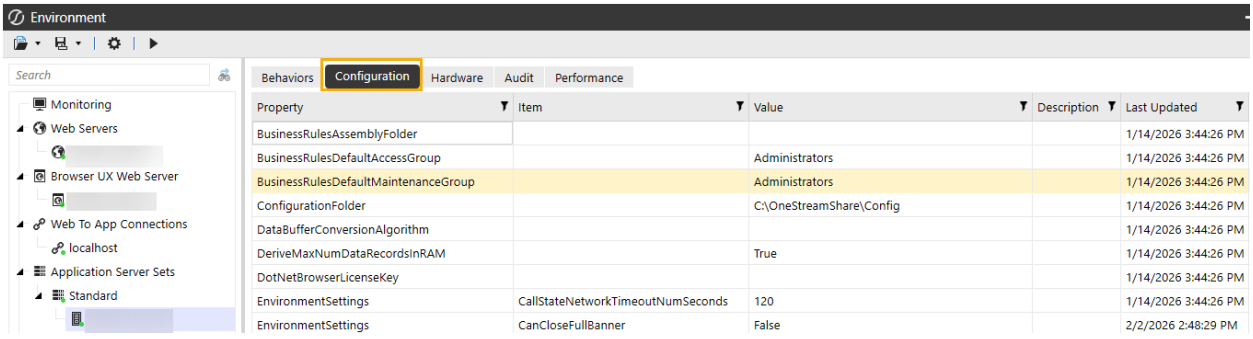
Stops the server, but while in this state will continue to incur Azure compute charges. The public and internal will be preserved.

Stop (Deallocate)- (Azure Scale Set Only)

Stopping this way will mean the cost of virtual machine will not be charged, but the public and internal IP will be deleted.

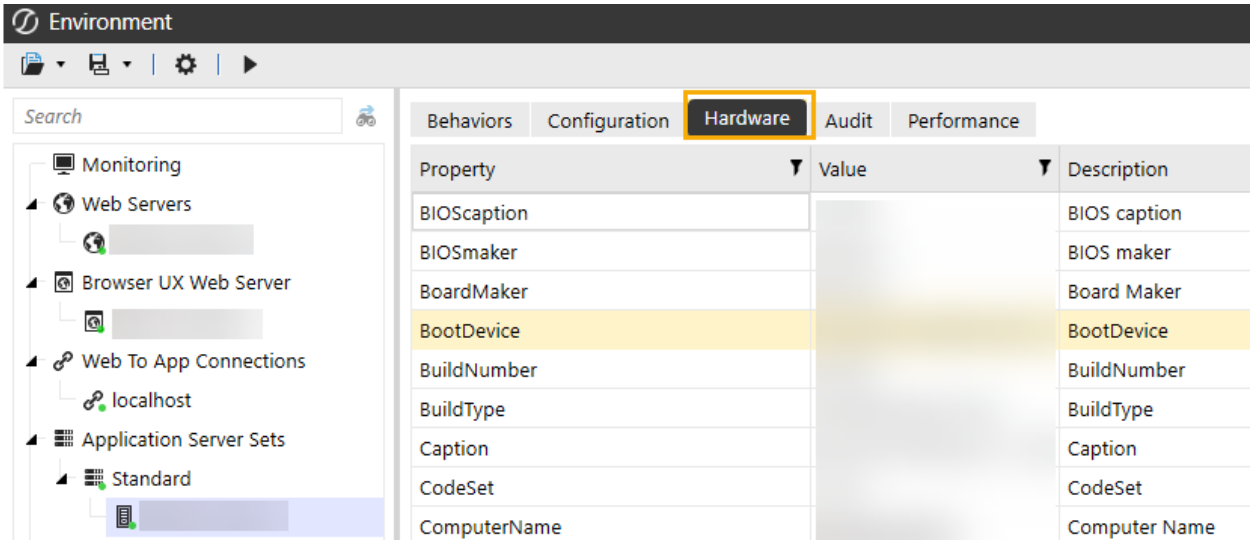
Application Server Configuration

The Configuration tab displays the server configurations from the OneStream Server Configuration Utility pertaining to that server.



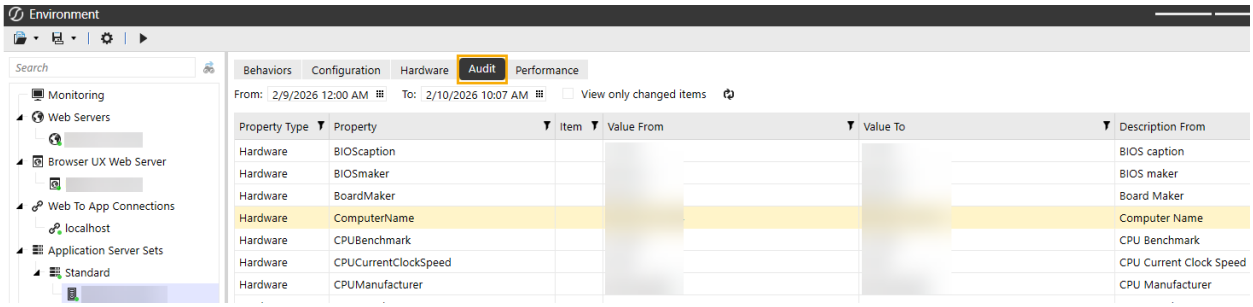
Application Server Hardware

The Hardware tab shows the machine hardware information based on settings in the OneStream Server Configuration Utility.



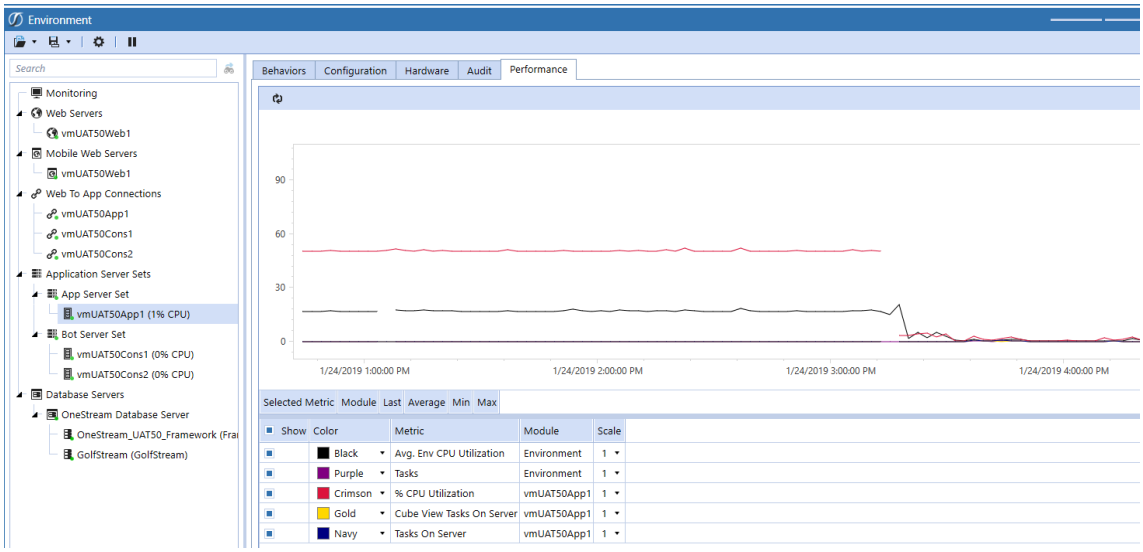
Application Server Audit

The Audit tab keeps track of and displays any hardware and configuration changes.



Application Server Performance

The Performance tab displays metric values pertaining to that server and the environment.



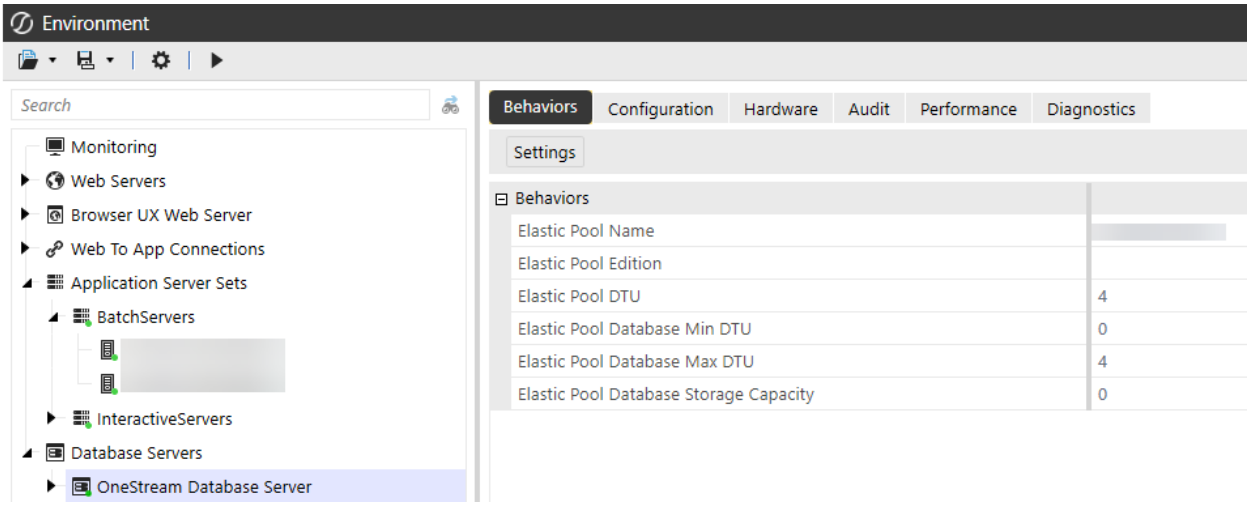
Database Servers

The Database Servers section will list all the database connections based on settings in the OneStream Server Configuration Utility and all the databases that each connection is pointing to.

From the database connection items, the user can expand the SQL server elastic pool if one is configured, view hardware and server properties, view audit info, look at SQL server metrics, and run diagnostic commands to track down performance issues.

Behaviors

Sample database connection Behaviors tab:

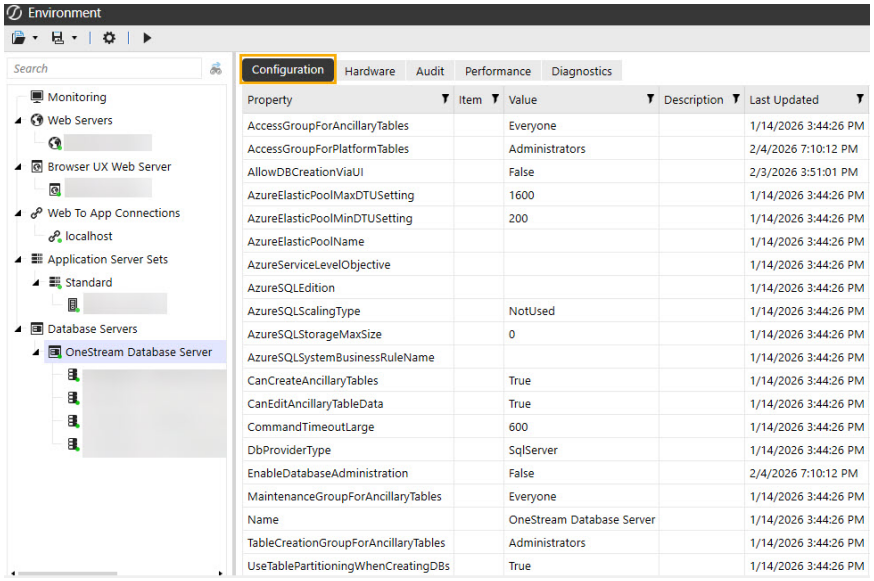


The behavior will show up if SQL server Azure and Elastic Pool are configured and used. Using the Behaviors tab, you can increase or decrease the resources available to an Elastic Pool based on resource needs. When rescaling Elastic Pool DTUs, database connections are briefly dropped. This is the same behavior that occurs when rescaling Elastic Pool DTUs for a single database not in a pool.

Configuration

The Configuration tab will display SQL server configuration properties.

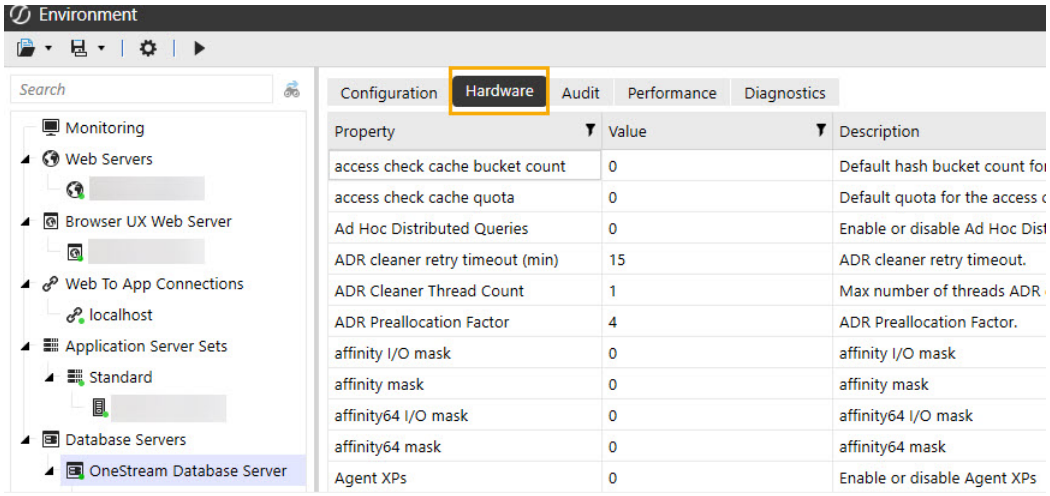
Sample configuration properties:



Hardware

The Hardware tab will display hardware related information pertaining to SQL server.

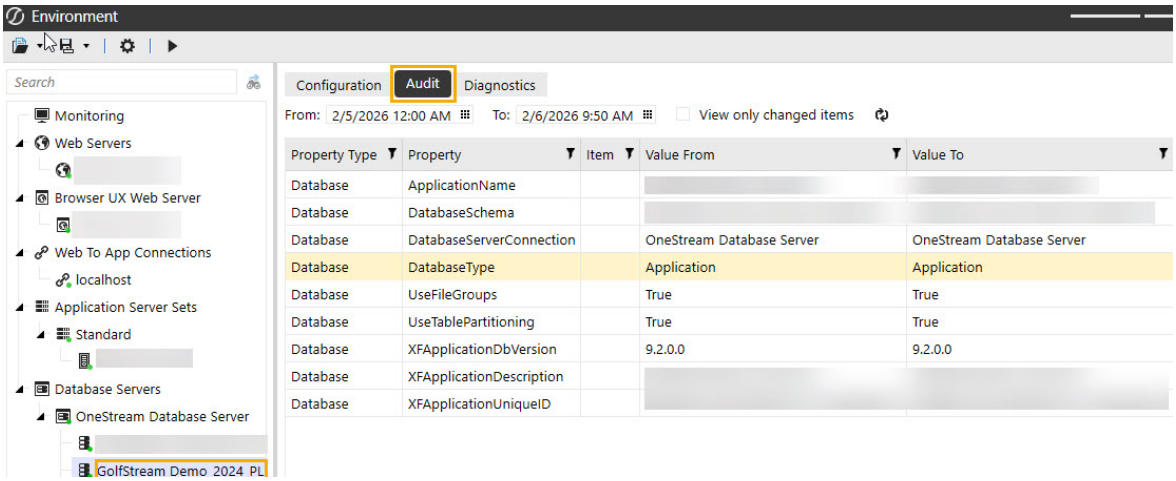
Sample hardware properties:



Audit

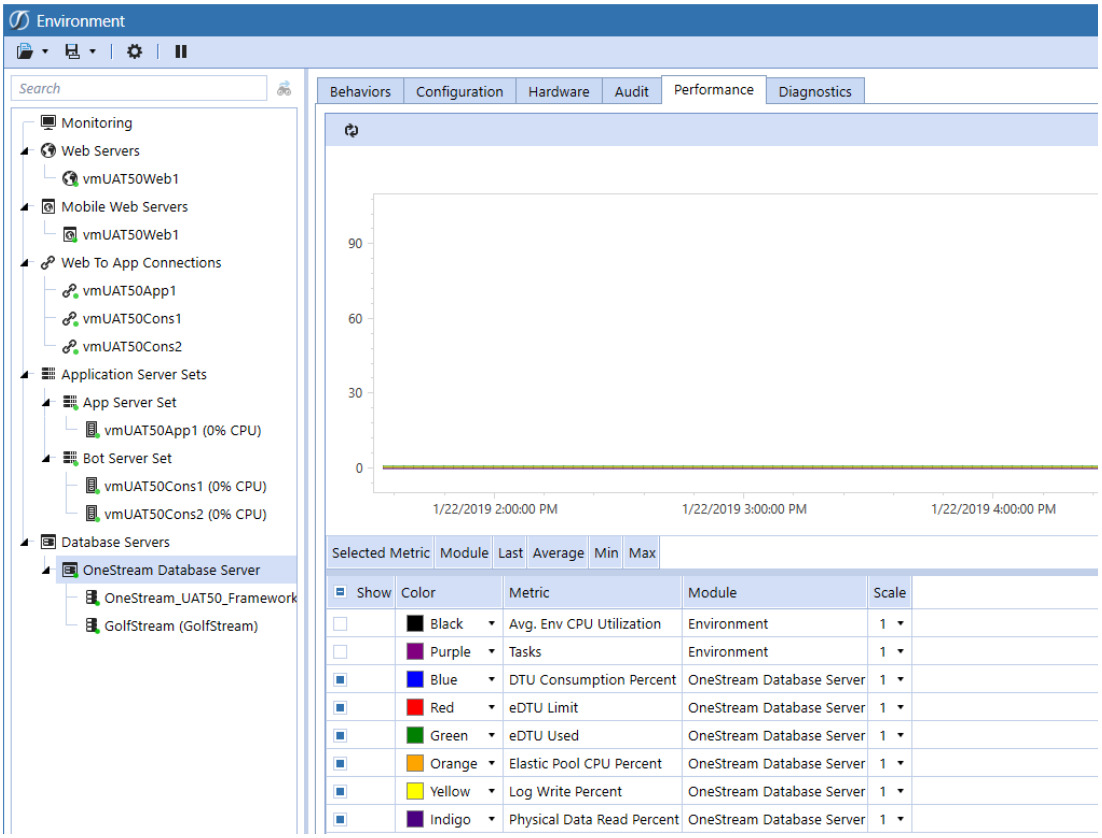
The Audit tab will display any changes to the SQL server properties.

Sample configuration audit report:



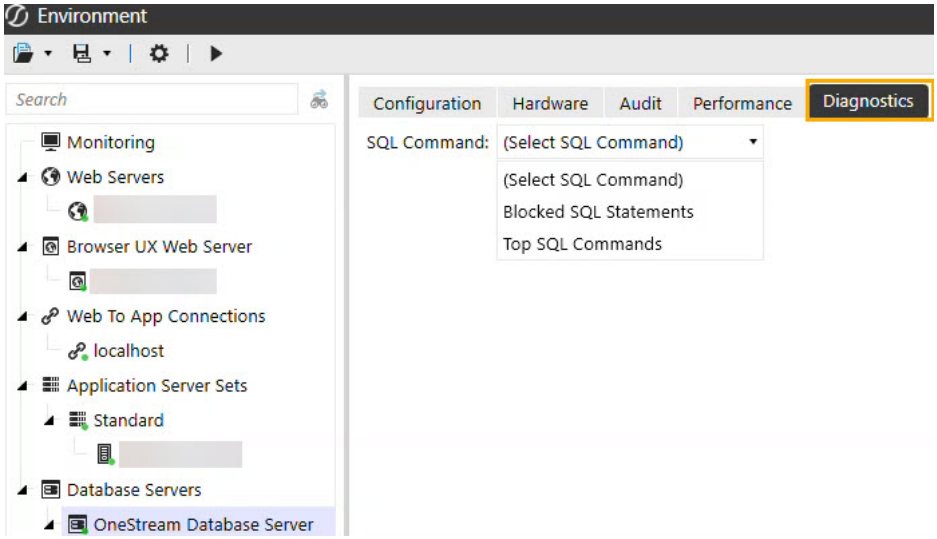
Performance

The Performance tab will display metrics pertaining to SQL server:



Diagnostics

The Diagnostics tab allows the user to run SQL diagnostic commands to determine performance issue on the database instance.



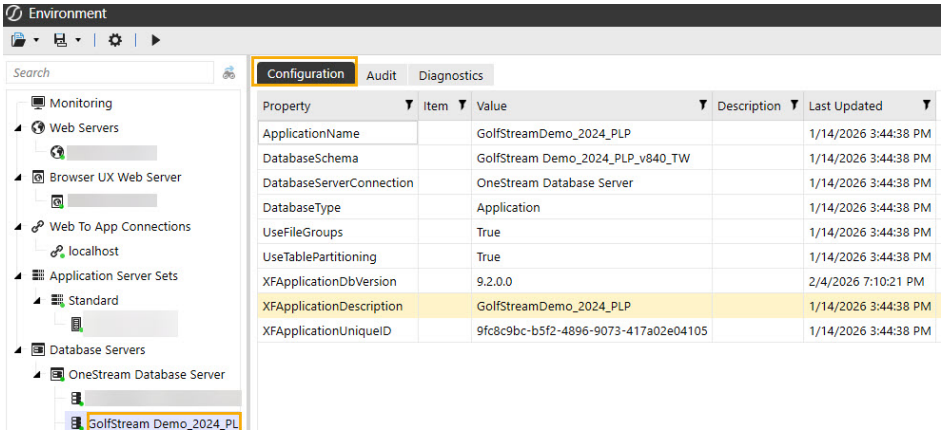
- SQL Deadlock information.
- The Deadlock SQL command will list out any deadlocks if any on the SQL server instance.
- Top SQL Commands will list out the top number of SQL using the order select by the user: Total Logical Reads, Total Logical Writes, Total Worker Time)

OneStream Database Servers (Schema Items)

This section lists all the database schemas that this connection is pointing to. Each schema has its own configurations, audit, and diagnostics tabs.

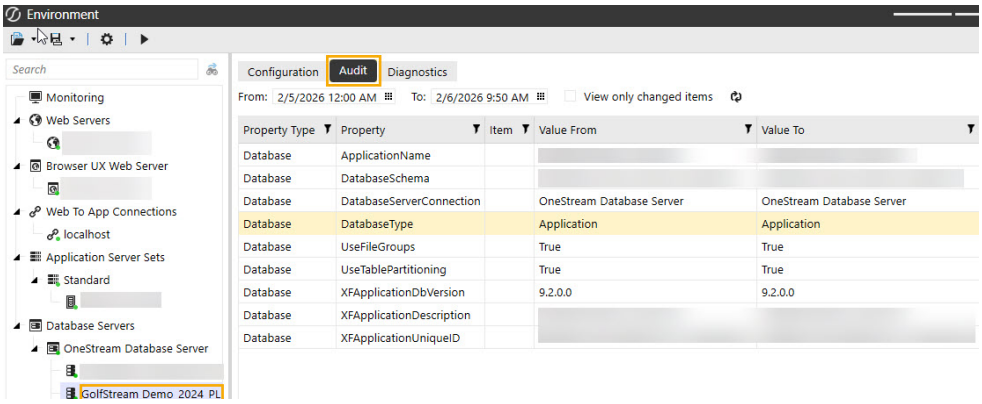
Configuration

The Configuration tab contains the application-specific information:



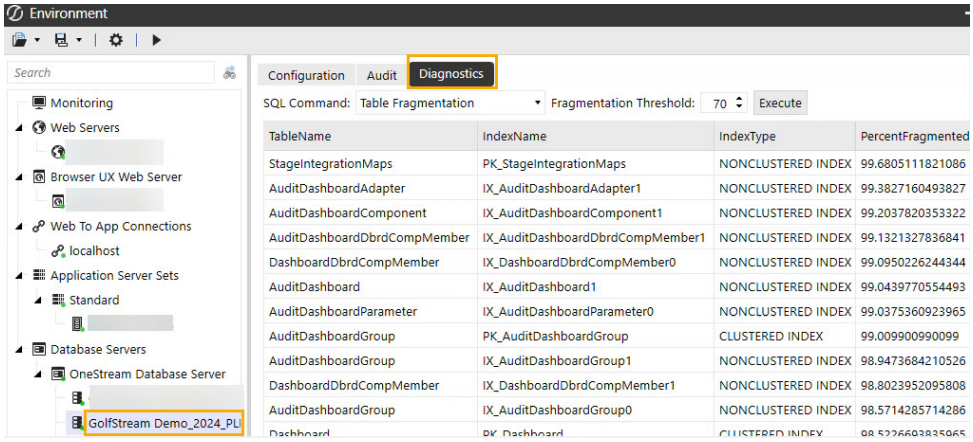
Audit

The Audit tab shows if any of the application configuration has been changed.



Diagnostics

The Diagnostics tab shows a report of current schema table fragmentation. Sample of table fragmentation on the framework DB showing all tables beyond 70% fragmented:

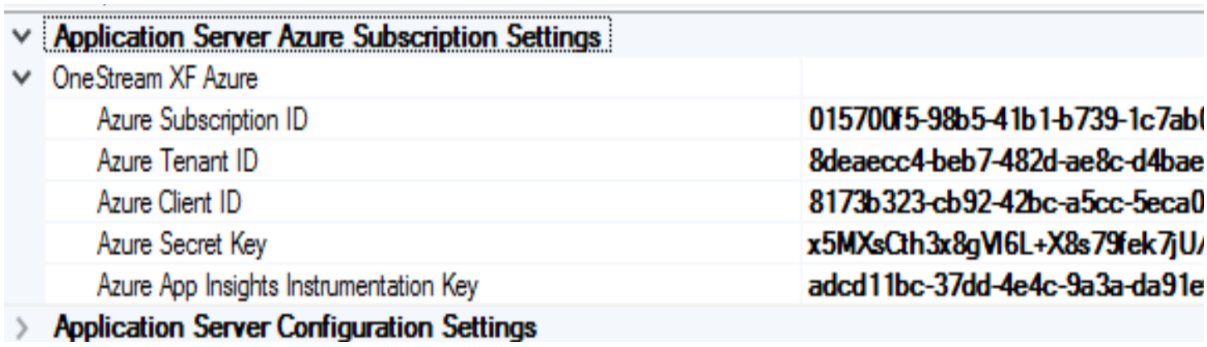


Azure Configurations

Complete these settings only if you use Azure or an Azure elastic pool.

Azure Subscription Settings

The Azure Subscription Settings must be completed because the system uses them to log in and retrieve Azure settings and data. This section must be completed when using Azure elastic pool or if using scale sets.



Environment Monitoring

The Environment Monitoring section configures how and how often metrics are collected. What is available for metrics or monitoring is based on configurations made in the OneStream Server Configuration Utility. See the *Installation and Configuration Guide*.

Environment Monitoring	
URL for the Automatic Recycle Service	**https://*:50002/OneStreamMgmt/MgmtService.svc**
Number of Running Hours Before Automatic Recycle	**24**
Start Hour for Automatic Recycle (0 to 24 UTC)	**5**
End Hour for Automatic Recycle (0 to 24 UTC)	**7**
Maximum Number of Minutes to Pause Before Automatic Recycle	**30**
Active Check Update Interval (seconds)	**60**
SQL Blocking Timeout Interval (minutes)	**5**
Metric Update Interval (seconds)	**30**
Server Heartbeat Update Interval (seconds)	**10**
Collect Environment CPU Metrics	**Always**
Collect Environment Task Metrics	**Always**
Collect Environment Logon Metrics	**Always**
Collect Server Set CPU Metrics	**Never**
Collect Server Set Task Metrics	**Never**
Collect Server Disk Metrics	**Never**
Collect Server Memory Metrics	**Never**
Collect Server Network Card Metrics	**Never**
Collect SQL CPU Metrics	**Never**
Collect SQL Page Metrics	**Never**
Collect SQL Memory Metrics	**Never**
Collect SQL Connection Metrics	**Never**
Collect SQL Query Metrics	**Never**
Collect SQL File Metrics	**Never**
Collect SQL Elastic Pool CPU Metrics	**Never**
Collect SQL Elastic Pool DTU Metrics	**Never**
Collect SQL Elastic Pool Storage Metrics	**Never**
Collect SQL Elastic Pool Workload Metrics	**Never**
Number Past Metric Readings for SQL Blocking	**5**
Fragmentation Iteration Count	**600**
Fragmentation Percent Threshold	**90**
Detailed Logging	**False**
Number of Hours to Retain Offline Servers	**1**
Number of Days to Retain Server Config History	**30**
Number of Days to Retain Metrics	**30**

URL for the Automatic Recycle Service

Used to specify the address of the recycle management service. Set the protocol to https or http, depending on how the service is deployed, and specify the port. The default value is 50002. The asterisk forces the service to use the fully qualified domain name of the executing server.

Number of Running Hours Before Automatic Recycle

Used to specify how often the application servers should be restarted. The default is 24.0. Use 0.0 to turn off automatic recycling. Fractional numbers may be used in this setting.

Start Hour for Automatic Recycle (0 to 24 UTC)

Used to specify the time period within each day that the server can be recycled. This setting is only used if Number of Running Hours Before Automatic Recycle is set to 24.0. The default setting is 5. With that value, the application servers are recycled between 5:00 AM UTC and the time set in End Hour for Automatic Recycle.

End Hour for Automatic Recycle (0 to 24 UTC)

Used to specify the time period within each day that the server can be recycled. This setting is only used if Number of Running Hours Before Automatic Recycle is set to 24.0. The default setting is 7. With that value, the application servers are recycled between 7:00 AM UTC and the time set in Start Hour for Automatic Recycle.

Maximum Number of Minutes to Pause Before Automatic Recycle

Used to specify the maximum number of minutes that the server should pause its ability to run newly queued tasks before recycling. The default setting is 30. This setting is the time period that the server will use to allow previously started tasks to finish. If there are no previously running tasks on the application server, the setting is ignored.

Active Check Update Interval (seconds)

How often system checks for system monitoring such as deadlocks.

Metric Update Interval (seconds)

How often system checks for metric updates.

Server Heartbeat Update Interval (seconds)

How often system updates that this server is alive.

Collect Environment CPU Metrics

How often to collect environment CPU metrics.

Collect Environment Task Metrics

How often to collect environment task metrics such as running tasks or Queued Tasks.

Collect Environment Login Metrics

How often to collect environment user login metrics.

Collect Server Set CPU Metrics

How often to collect server set CPU metrics.

Collect Server Set Task Metrics

How often to collect server set task metrics such as running tasks or Queued Tasks.

Collect Server Disk Metrics

How often to collect server disk metrics such as Average Disk read/write per sec.

Collect Server Memory Metrics

How often to collect server memory metrics such as Available MBytes.

Collect Server Network Card Metrics

How often to collect server network card metrics.

Collect SQL CPU Metrics

How often to collect SQL server CPU metrics.

Collect SQL Page Metrics

How often to collect SQL server Page caching metrics such as Page Life Expectancy.

Collect SQL Memory Metrics

How often to collect SQL server CPU metrics.

Collect SQL Connection Metrics

How often to collect SQL server connection metrics such as number of connections

Collect SQL Query Metrics

How often to collect SQL server Query metrics such as number of deletes and inserts.

Collect SQL File Metrics

How often to collect SQL server File growth metrics.

Collect SQL elastic pool CPU Metrics

How often to collect SQL server elastic pool CPU metrics such as number of connections.

Collect SQL elastic pool DTU Metrics

How often to collect SQL server elastic pool DTU metrics such as number of connections.

Collect SQL elastic pool Storage Metrics

How often to collect SQL server elastic pool Storage metrics such as disk storage usage.

Collect SQL elastic pool Workload Metrics

How often to collect SQL server elastic pool Workload metrics.

Number Past Metric Readings for SQL Blocking

Used to select the past number of metric values for blocking analysis.

Fragmentation Iteration Count

Used for fragmentation check, every 10 hours if the ActiveCheckUpdateIntervalInSec is set to 60.

Fragmentation Percent Threshold

Used for fragmentation threshold check in percent.

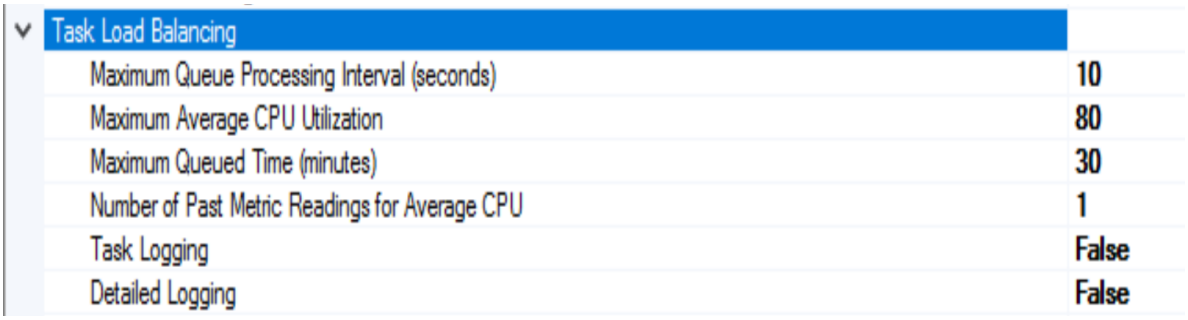
Detailed Logging

If true, then log whenever we enter and exit the metric collection and the Active System check.

Number Hours To Retain Offline Servers

Remove offline servers from the heartbeat table after certain number of hours.

Task Load Balancing



Maximum Queued Processing Interval (seconds)

How often the queuing thread checks for new tasks to be run.

Number Past Metric Reading For Analysis

How many metric readings to retrieve for analyzing server demand.

Maximum Queued Time (minutes)

Maximum time to wait for a task to run before it is canceled.

Maximum Average CPU Utilization

Maximum average CPU utilization before we determine that a server can't take a task.

Task Logging Only

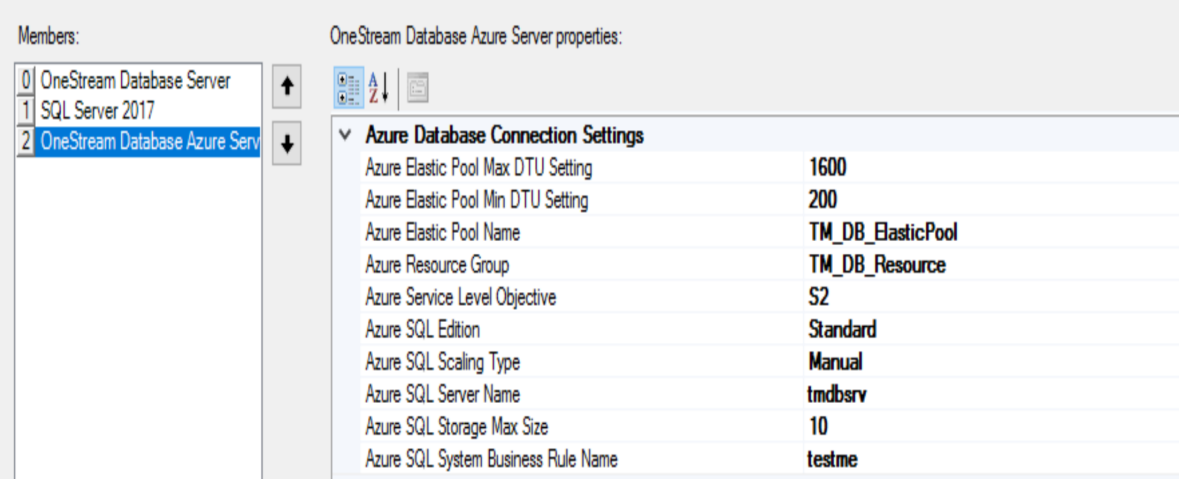
If true it only logs picked up tasks.

Detailed Logging

If true, then log whenever we enter and exit the Task Load Balancing function and what was run.

Database Server Connection

Complete the Azure section in the Database Connection Settings only if you use an Azure database or Azure elastic pool.



Sample Azure database connection settings:

Azure elastic pool Max DTU Setting

This is a fail-safe setting that the user can't set the DTU setting above this point.

Azure elastic pool Min DTU Setting

This is a fail-safe setting that the user can't set the DTU setting below this point.

elastic pool Name

The name of the elastic pool used with this database connection.

Azure Resource Group

The resource group name that the elastic pool is in.

Azure Service Level Objective

The service level used. This setting is used to create application on Azure.

Azure SQL Edition

The Azure SQL Server edition used.

Azure SQL Scaling Type

Manual, Business Rule, or ManualAndBusiness Rule. This is used to set the type of scaling that is used to Scale Out or Scale In the SQL Server eDTUs. The default setting should be set to Not Used.

Azure SQL Server Name

The name of the SQL Server. This setting is used to create application on Azure.

Azure SQL Storage Max Size

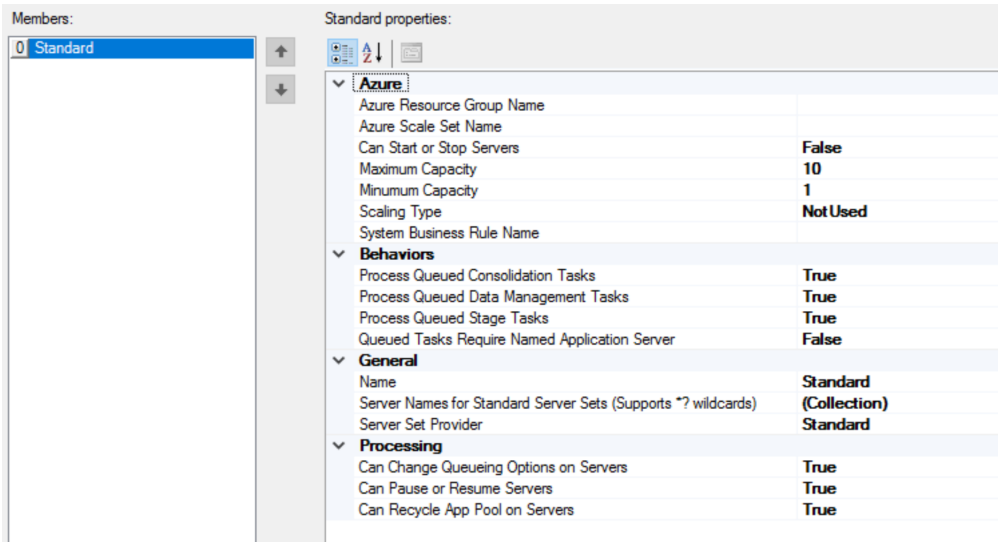
This is used to specify the database storage size when creating a database on Azure.

Azure SQL System Business Rule Name

If SQL Scaling Type is set to BusinessRule, this setting must be set to a business rule that is used to Scale In or Scale Out. The Environment metrics and the database metrics are passed to this rule to properly determine the eDTU scaling.

Azure Server Sets Settings

This setting is used to set up the used scale sets for the different application servers:



The **Azure** section is used to set the Azure resource group name and the scale set name as it exists on Azure. The Scaling options are used to set the scaling capacity and the Scaling Type such as Manual or BusinessRule. The System Business Rule Name must be set if the Scaling Type is set to Business Rule.

The **Behaviors** section is used determine how this scale set is used. Whether it can be called by the web server or it is used as a processing server for consolidations and Stage Load.

The **General** section is used to determine whether this scale set is used and who is its provider such as Azure or External.

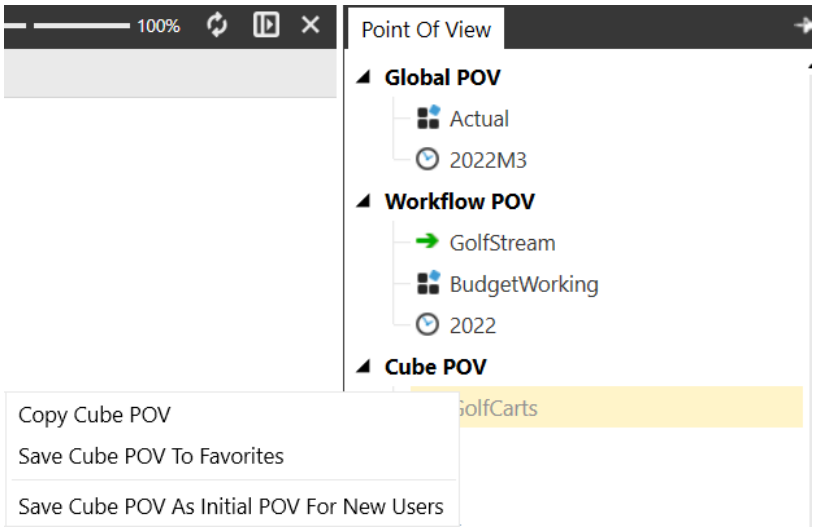
File Explorer

Documents and saved Point of View settings can be stored in the Application database.

 Create a new folder in the File Explorer.

 Upload a specific file into any folder. If a user has administrator rights or is in the ManageFileShare security role, they can upload and delete files in the Harvest folder.

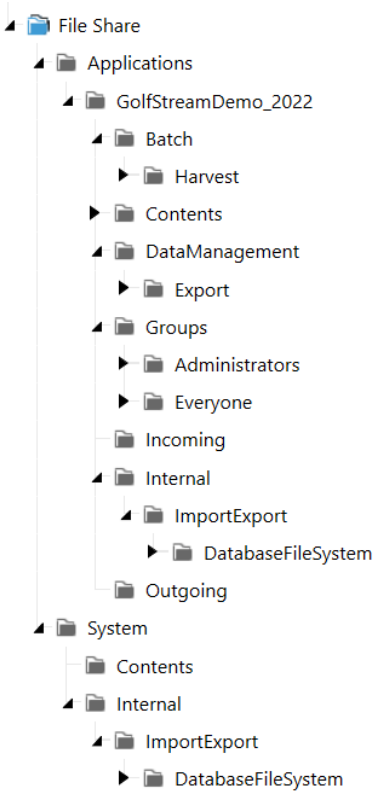
A common Cube Point of View can be stored for reuse by multiple users. The POV can be stored for all users in the Public area or for the specific user in the User directory. To create a saved, named POV, right-click the Cube POV node under Point of View within the Context Pane:



File Share

File Share is a self-service directory which supports file storage external from the OneStream Application and System Databases. Files stored in an Incoming folder are accessible only through that Workflow Profile.

 To access File Share, select the **File Explorer** button in the toolbar, or go to **System >Tools > File Explorer**.



Folders

Folders organize stored files and control access to them through the Application and System file areas.

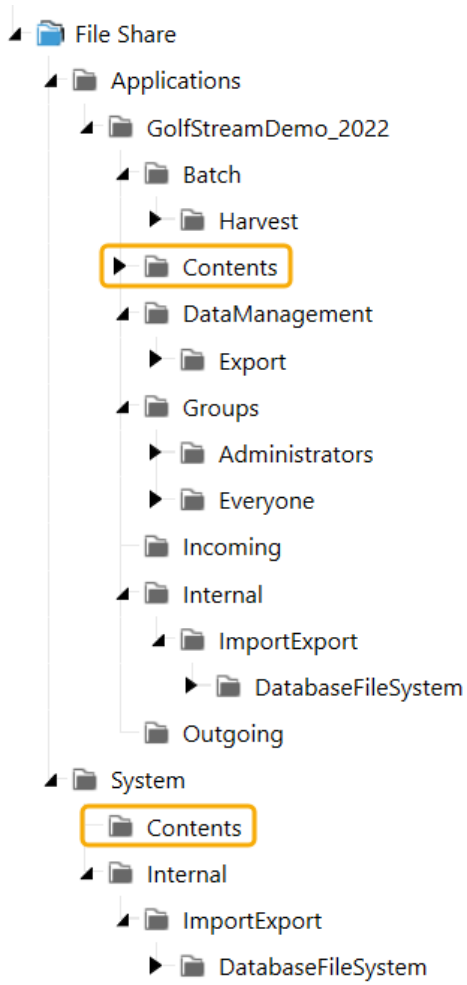
Contents Folders

Both the Application and System folders contain an auto-generated folder named Contents intended to store files larger than 300 MB. This folder is a secured storage area that can be used in place of the File Explorer application database.

Permissions

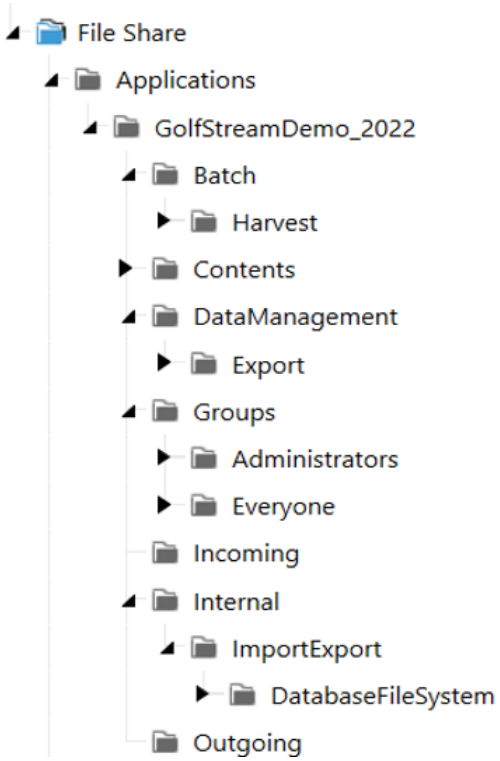
The Contents folders are managed and secured by System Security Roles. To set System Security Roles, go to **System** > **Security** > **System Security Roles**:

- Administrator and ManageFileShare Roles have full rights.
- Non-administrators can be assigned rights to modify, fully access, or have limited access to the Content folders.



Application Folders

This folder has application specific storage.



Batch and Harvest

These folders are used for automation of Connector Data Loads. When the Harvest folder loads a file, it is automatically cleared and an archive folder with a copy of the loaded file is created. To add or delete files from the Harvest folder, you must have administration rights or have the ManageFileShare security role.

> **NOTE:** The archive folder and the files within it can be cleared using Data Import Schedule Manager.

Content

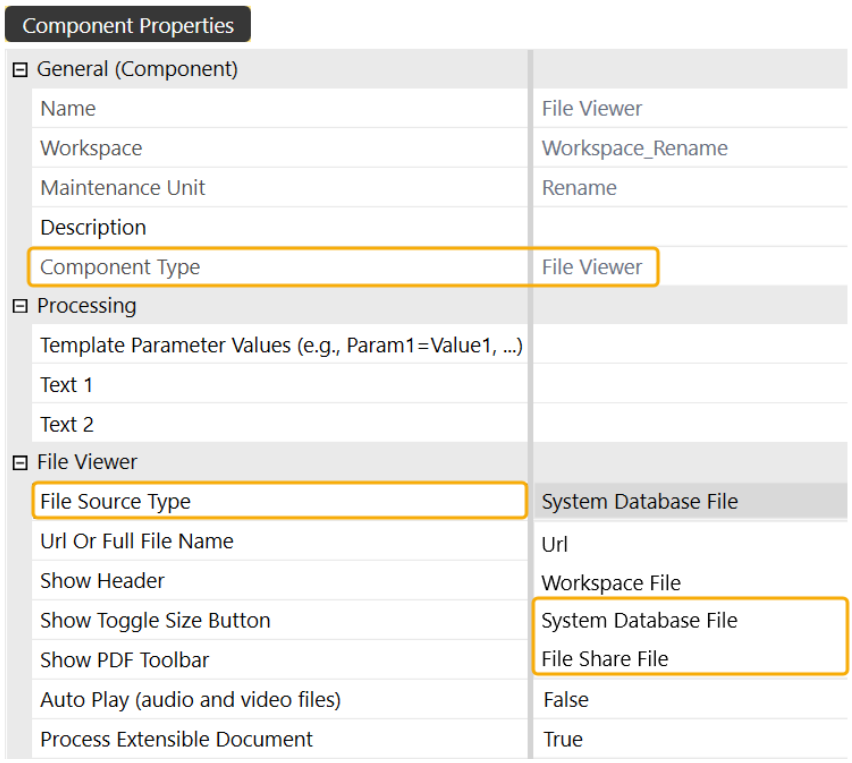
See Contents Folders.

Data Management

This is the default folder for the data management export process.

Groups

This folder is used for dashboard components with a File Source Type of File Share to allow viewing by Security. The file is placed in one of the folders under \\MyServerName\OneStreamShare\Applications\MyApplicationName\Groups and then placed into a folder with the same name as a User Group. The user must have permissions to that User Group to view the file.



Incoming

This folder is used as a location to place source files for import into Stage.

It is also used for the File Viewer Component. During an Import Load step, select **Load and Transform** > **Select Server File**. Select the ellipses to display source files placed in the Import folder. See "File Viewer" in the *Presentation Guide*.

Internal

This folder stores the contents of the Application Database files or System Database files. These icons enable users to export this content to File Share:



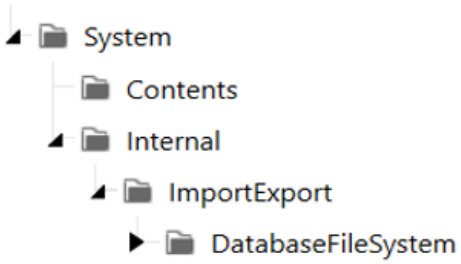
> **NOTE:** To access the File Share export and import options, the user must be granted rights to the SystemPane role and the FileExplorerPage role. When granted these rights, go to **System** > **Tools** > **File Explorer** and the icons display in the toolbar.

Outgoing

This folder is available for use in customized processes that require a defined folder location.

System Folders

This folder has system specific storage.



Content

See Contents Folders.

Internal

This folder exports from System Database.

Uploads

By default, authorized users can upload or edit files or folders in the File Share using the OneStream File Explorer and are required to use Content folder. To change this setting so no user has upload, edit file, or edit folder access to the File Share using the OneStream File Explorer, contact OneStream Support. Normal access rules apply for browsing files and folders in the File System section.

Users will receive a Security error when attempting to write or edit the files and folders while attempting to use API or non File Explorer methods.

Supported File Sizes

The OneStream File Explorer can be used as an application interface to the File Explorer Content folders. The supported file size varies by interface.

Windows application

- Uploads (Applications and System): Up to 300 MB
- Uploads (Content): Up to 2 GB
- Downloads (Application and System): Up to 2 GB
- Downloads (Content): Up to 2 GB

Whitelist File Extensions

Whitelist File Extensions provide a method of identifying which kinds of documents, according to their file extensions, are allowed to be saved into the OneStream application File Explorer. Whitelisting extensions helps alleviate the risk of uploading malicious file types into the application.

Overview

OneStream enables you save documents or upload documents from your device into the application. These documents are stored in one of three file storage root folders:

- Application Database: Displays stored documents for the current application only.
- System Database: Displays stored documents for the entire system without affecting the current application.
- File Share: This is a self-service directory that temporarily stores files before they are imported into the Application or System Database.

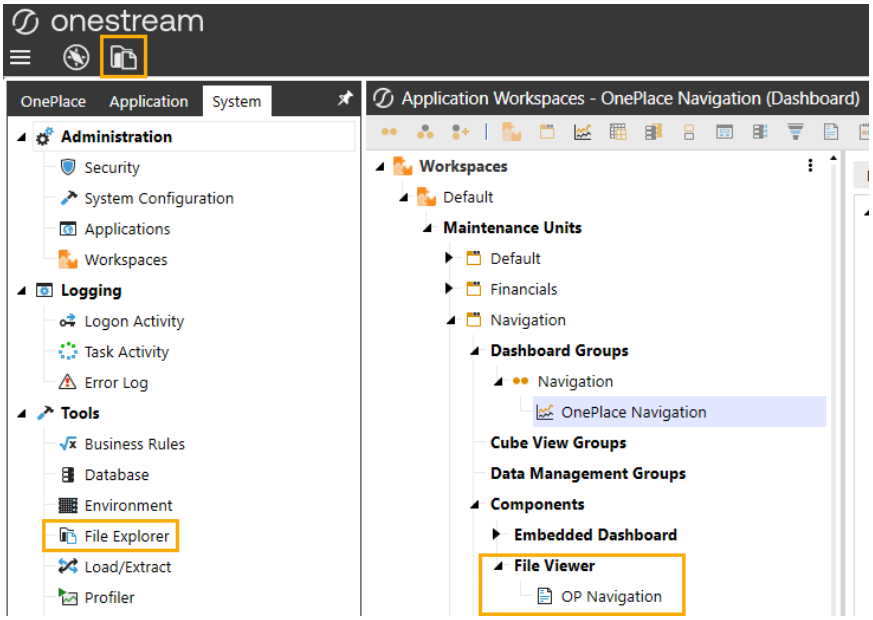
File Explorer is the product tool inside the Windows application that lets you browse saved documents or upload new ones.

Common use cases include:

- Saving a spreadsheet to any of the three root folders.
- Saving Cube POVs to the Application or System folders.

Access the File Explorer from:

- The main toolbar
- The System tab
- The File Viewer dashboard component, which launches the File Explorer.



Finally, there is a BRApi used by OneStream Solutions or custom-developed dashboards to upload documents.

Whitelist Files Extensions Prerequisites

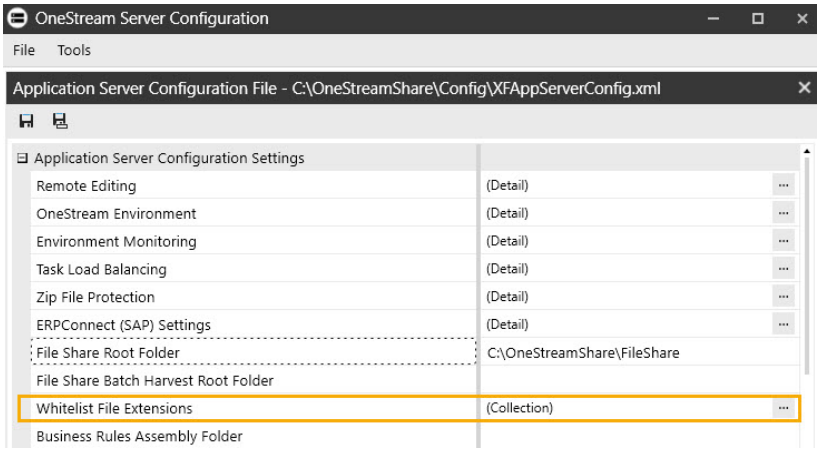
Standard File Explorer setup and security.

Define the List of File Extensions

Whilelisted file extensions must be specified in the OneStream Application Server Configuration file.

To enable the whitelist and define allowed file extensions:

1. Go to **Start** > **OneStream Software** > **OneStream Server Configuration Utility**, right-click and select **Run as Administrator**.
2. On the File menu, select **Open Application Server Configuration File**.
3. Browse to the location of your XFAppServerConfigFile, typically located at C:\OneStreamShare\Config, select the application config file, and select **Open**.
4. In the Application Server Configuration Settings section, locate Whitelist File Extensions and select the ellipss (**...**) on the far-right of the field.



5. In the dialog box, select the plus sign (**+**) then type the whitelisted file extension, for example, .txt.



6. Continue adding other whitelisted file extensions.
7. When you are finished, select the **OK** button.

8. Select **Save** to save the changes to the Application Server Configuration File.
9. Restart Internet Information Service (IIS).

> **NOTE:** Cloud customers should contact Support to have this configuration change made for them.

Also, if you enter any of the following characters, they will be automatically removed. For example, typing .txt (with a period) becomes txt.

/	^	=	'
(empty space)	&	\	[
!	*	?	]
@	(	<	.
#	)	>	
$	–	~	
%	+	`	

Add Documents using File Explorer

To add documents using File Explorer:

1. Navigate to any File Explorer component inside the Windows application.
2. Select **Upload File**.
3. Browse to the file you would like to upload and select **OK**.

   If the extension of the file is whitelisted, it will be uploaded. If not, you will receive an error message.

Troubleshooting

After a whitelist is defined, any new files with extensions not in the whitelist will be restricted from uploading.

> **IMPORTANT:** If you upload a file that contains an exploit, malware, or a malicious script or macro, other users can download the file and infect their machine.

Conclusion

Whitelisting a file extension provides a means of allowing only certain types of documents to be saved in the File Explorer. This helps alleviate the possibility of introducing malicious file types into the system.

Application Database and System Database

The Application Database displays stored documents for the current Application only. The System Database displays stored documents for the entire system without affecting the current application.

Documents

Documents can be stored with different access levels and in different locations.

Public

Files available to everyone with access.

Security Access

Enables a user to access an object and read the content.

Maintenance (Group)

Enables a user to view an object and create, modify and delete objects in Groups. If in a Maintenance Group, a user does not need to be in the Access Group. The Maintenance Group also controls user profile contents.

Users

Private documents only available to named users.

Internal

Files used internally that cannot be modified.

Load/Extract System Artifacts

You can import and export sections of the System using an XML Format.

> **TIP:** Only System Administrators have access to this portion of the tool.

Extract

Choose an item from the drop-down list, select the Extract icon to start the extract process, then name the output file.

Load

After browsing to the file, select the Load icon to initiate the process.

Extract and Edit

This option is available for all extracts and enables the end user to edit the XML file as needed.

The following items can be extracted:

Security

This covers System Roles, Users, Security Groups, and Exclusion Groups which can be found at **System Tab** > **Administration** > **Security**. The screen will display Extract Unique IDs. If this box is checked, the unique IDs OneStream assigns to each user will be extracted with the security. When moving security changes from one OneStream environment to another, trying to load the security with the unique IDs into the destination environment can result in an error if some of the records already exist. If this is the case, deselect this box and extract without the unique IDs. Items to Extract also displays and by default All is chosen. Choose specific items in each section or turn the sections on or off.

System Dashboards

This has multiple sections such as Maintenance Units and Profiles. Under Maintenance Units, the Groups, Dashboard Components, Dashboard Adapters, and Dashboard Parameters all go together. System Dashboards can be found under the System Tab| Administration| Dashboards. The screen will display Items To Extract and by default All is chosen. Choose specific items in each section or turn the sections on or off.

Error Log

This covers the Error Log found under **System Tab** > **Logging**> **Error Log**. The screen will display an Extract All Items check box along with a Start Time and End Time. If the check box is not checked, choose the Start and End Time by selecting  . Select the extract button and define where the file will be saved.

Task Activity

This covers the Task Activity found under **System Tab** > **Logging** > **Task Activity**. The screen will display an Extract All Items check box along with a Start Time and End Time. If the check box is not checked, choose the Start and End Time by selecting  . Select the extract button and define where the file will be saved.

Logon Activity

This covers the Logon Activity found under **System Tab** > **Logging** > **Logon Activity**. The screen will display an Extract All Items check box along with a Start Time and End Time. If the check box is not checked, choose the Start and End Time by selecting  . Select the extract button and define where the file will be saved.

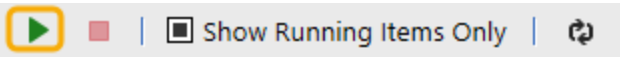
Profiler

> **IMPORTANT:** Profiler should be used by developers.

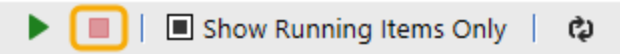
Profiler captures every event processed in a user session, such as business rules, formulas, and Workspace Assemblies. This enables you to view the input and output of a method or function to help troubleshoot performance issues. Any code processed inside OneStream is profiled during a session. Profiler is tied to user activity and does not capture activity at the application level.

System Security Role	
ManageProfiler	Users assigned to this role can run Profiler sessions and view Profiler Events. Without this role, users cannot start a Profiler session. The default role is Administrator.
System User Interface Role	
ProfilerPage	Users assigned to this role can view the Profiler page. They cannot run Profiler sessions or view Profiler Events. Without this role, users cannot view Profiler in the System tab, even if they are assigned to the ManageProfiler role. The default role is Administrator.

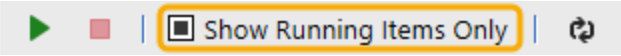
NOTE: Administrators can end any active Profiler session.



To start a Profiler session, select the **Start Profiler** button.



To end all active sessions, select the **Stop All Profiling for User** button.



To display only active Profiler sessions, select the **Show Running Items Only** checkbox.

To run a Profiler session, complete the following steps:

1. Select the **Start Profiler** button.
2. In the **Start Profiler** window, enter Profiler properties. None of the following fields are required to run a session:

Property	Description
General	
Description	Enter a session description to display on the Profiler page.
Number of Minutes to Run	This entry determines how long Profiler will run after a session has started. The session automatically ends after the allotted time. The default value is 20 and the max value is 60. Values over 60 will be reset to the default value.
Number of Hours to Retain Before Deletion	The Profiler session is deleted after the time entered has passed. The default value is 24 and the max value is 168. Values over 168 will be reset to the default value. **NOTE:** The Profiler session is deleted in the first server restart after the deletion time.
Filters	

Property	Description
Include Top Level Methods	This captures and displays high-level entry points, such as user actions, API calls, or workflow steps. When set to True, Profiler will log this activity. When set to False, no top-level methods display in the Profiler Events window. **NOTE:** Child Events are still visible when this filter is set to False. For example, if you have a data adapter that references a Workspace Assembly call, the Profiler Events will display the WSAS call as a child event within the Adapter event type.
Include Adapters	This includes any Data Adapter component calls to the Profiler output. When set to True, Profiler will log this activity. When set to False, no adapters display in the Profiler Events window, even when the Show All Child Events checkbox is selected.
Include Business Rules	This includes Business Rules in the Profiler output. When set to True, Profiler will log this activity. When set to False, no Business Rules display in the Profiler Events window, even when the Show All Child Events checkbox is selected.

Property	Description
Business Rule Filter	This entry determines what Business Rules are displayed in the Profiler Events window. See Filter Syntax.
Include Formulas	This includes formulas in the Profiler output. When set to True, Profiler will log this activity. When set to False, no formulas display even when the Show All Child Events checkbox is selected.
Formula Filter	This entry determines what Formulas are displayed in the Profiler Events window. See Filter Syntax.
Include Assembly Factory	This includes Assembly Method calls in the Profiler output. These are labeled as Factory to differentiate between Assembly Factory and Assembly Method calls. When set to True, Profiler will log this activity. When set to False, no Assembly Factories display even when the Show All Child Events checkbox is selected.

Property	Description
Include Assembly Methods	This includes Assembly Method calls in the Profiler output. These are labeled as WSAS to differentiate between Assembly Method and Assembly Factory calls. When set to True, Profiler will log this activity. When set to False, no Assembly Methods are listed even when the Show All Child Events checkbox is selected.
Assembly Method Filter	This entry determines what methods are displayed in the Profiler Events window. See Filter Syntax.

> **NOTE:** For the fields Number of Minutes to Run and Number of Hours to Retain Before Deletion, if the default values are deleted and no value is entered, Profiler will still default to these settings when a session is run. If a zero is entered for both fields, Number of Minutes to Run defaults to one minute, and Hours to Retain Before Deletion defaults to one hour.

3. Select the **Start** button. A new instance is displayed on the Profiler page.
4. Run the business rule, formula, or Workspace Assembly you want to profile. When finished, navigate back to the **Profiler** page. To end the session, find your session on the **Profiler** page and select the **Stop Profiler** button for that line item.

To delete a Profiler session, select the **Delete Selected Item** button. You cannot delete Profiler sessions that are actively running.



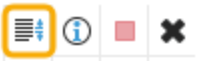
To end a singular session, select the **Stop Profiler** button.



To display all Profiler property settings for a session, select the **Instance Information** button. Profiler Settings are view-only and cannot be modified once you have started the session.



To display the Profiler Events window and view all child events, select the **Profiler Events** button.



> **IMPORTANT:** Application performance may be impacted if multiple users are running Profiler at the same time or performing long-running tasks while other users are running Profiler.

Filter Syntax

Use the Business Rule Filter, the Formula Filter, and the Assembly Method Filter to determine what displays in the Profiler Events window. For example, if you enter GetDataSet in the Assembly Method Filter, the filter only displays these methods.

The following wildcards are valid syntax:

- A question mark functions as a placeholder that accepts any character in its place.

  > **Example:** If you enter SS?B in the Business Rule Filter, only sources that match this filter are displayed, such as SSIB and SSVB.

> **Example:** If you enter A#????? in the Formula Filter, the filter only displays sources starting with A# followed by five characters.

- An asterisk indicates that any string can be added before or after the hard-coded string that is next to the asterisk.

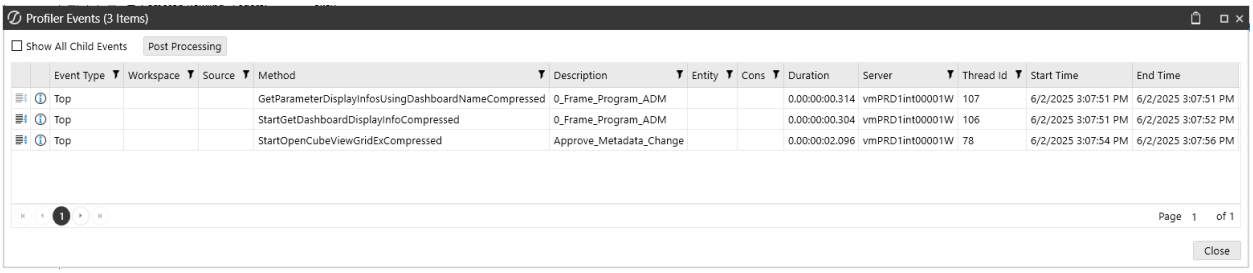
  > **Example:** If you enter *Validation in the Business Rule Filter, only rules ending with Validation are included.

  > **Example:** If you enter P* in the Assembly Method Filter, the filter only displays methods that start with P.

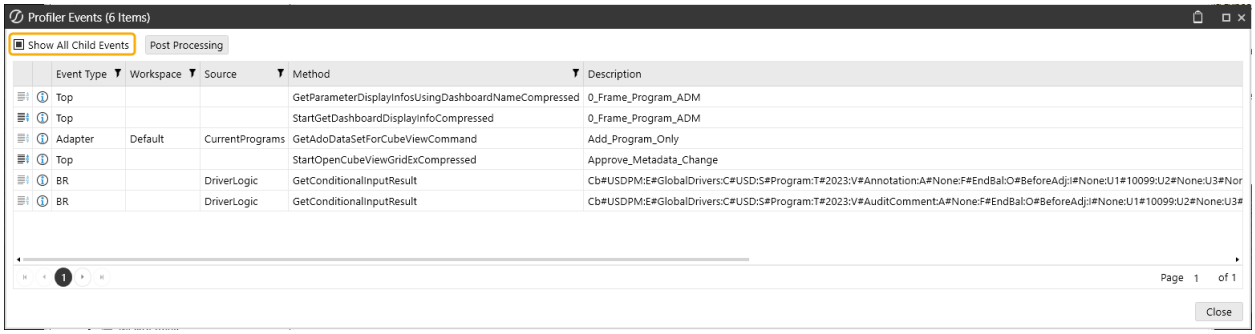
> **NOTE:** You can use multiple filters separated by a comma. For example, TableEditorTest* , Spreadsheet???????, IBM?nSave.

Profiler Events

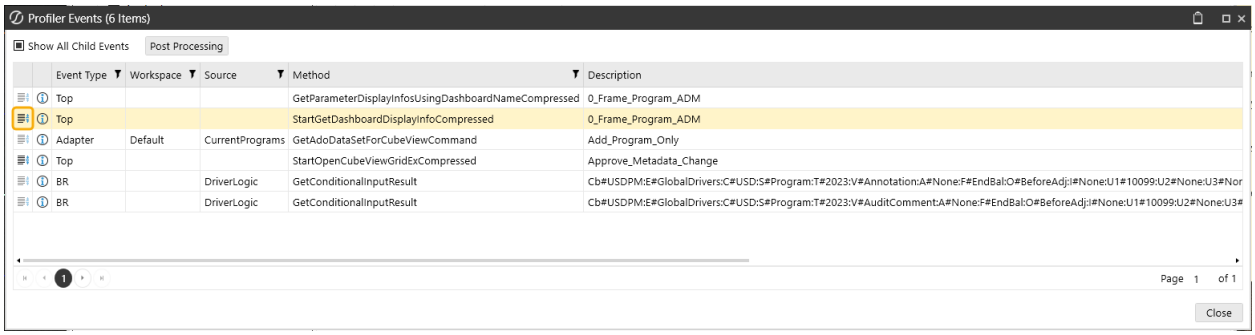
To display the **Profiler Events** window, navigate to the session you want to view and select the **Profiler Events** button. The Profiler Events window displays everything that occurred during the Profiler session with Top Level Events displayed as parents.

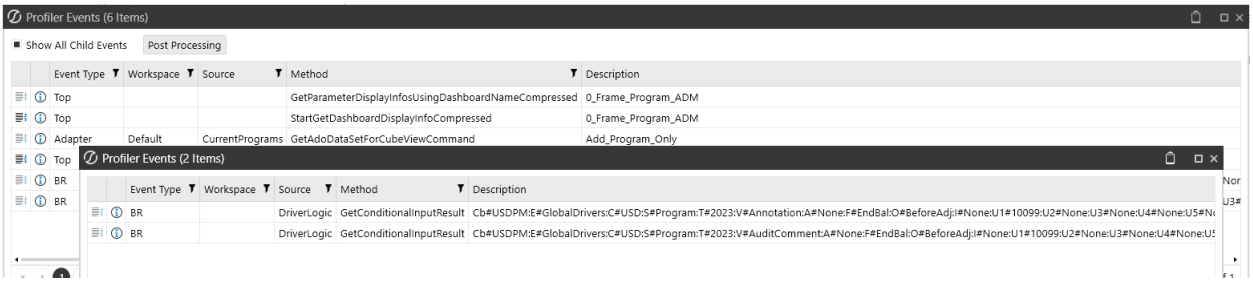


To display child events for all Top Level Events, select the **Show All Child Events** checkbox.



To drill down into a single Top Level event, select the **Child Events** button for that line item. This opens an additional Profiler Events window that only displays the child events for the selected Top Level event. If the Top Level event does not have any child events, the icon is grayed out for that item.





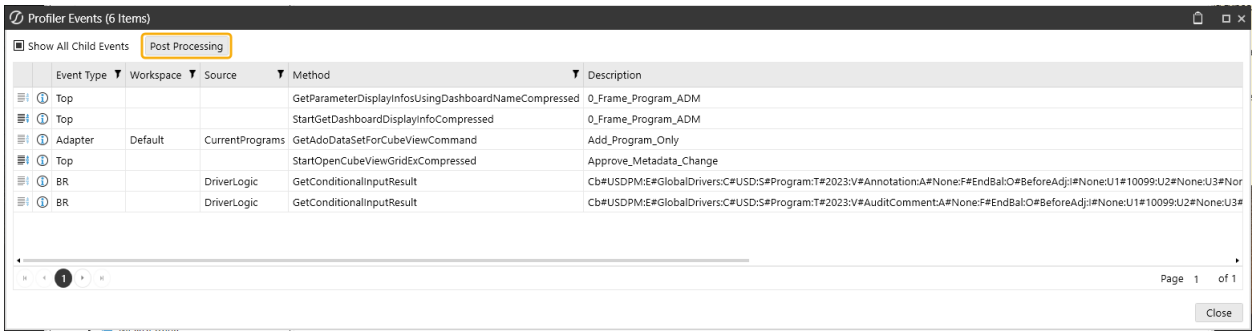
Review the following table for Profiler Events column descriptions:

Column	Description
Event Type	The following event types are displayed in this column: Top, Queue, Adapter, Formula, BR, Factory, WSAS, and Manual.
Workspace	This column displays the name of the Workspace containing the item that caused the event.
Source	This column identifies the origin of the profiled event. Its value varies depending on the event type being profiled. • For WSAS and Factory event types, the value is the workspace object that initiates the call, such as Dashboard, Component, or DataSet. • For Business Rule, Adapter, and Formula event types, the value is the specific name of the rule, adapter, or formula. • For Top Level events types, the value is the method name called by the top-level event. • Manual event types do not have an associated Source value.
Method	This column displays the method called.
Description	This column displays a description of the event type.
Entity	This column displays the name of the Entity dimension member associated with the event. This column is blank if the event is not tied to a specific entity.

Column	Description
Cons	This column displays the name of the Consolidation dimension member. This column is blank if the event is not related to a consolidation.
Duration	This column displays the duration of the event type.
Server	This column displays the server.
Thread ID	This column indicates the operating system thread identifier on which the event was run.

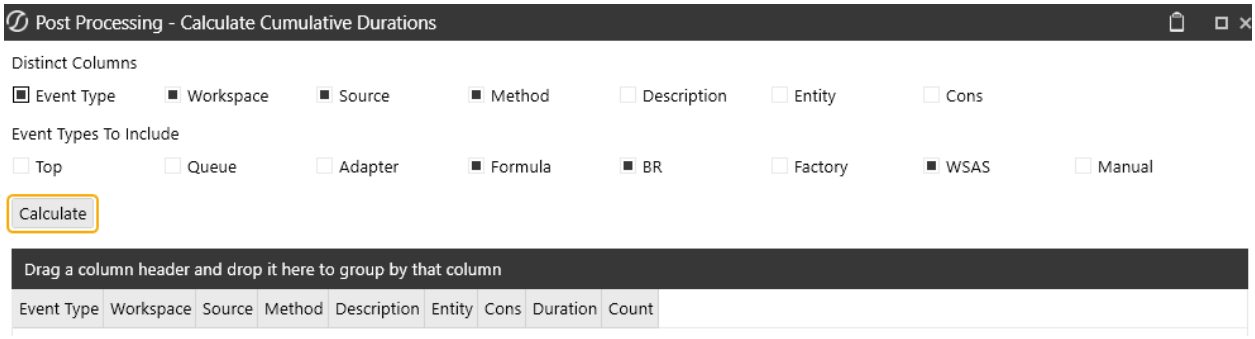
Post Processing

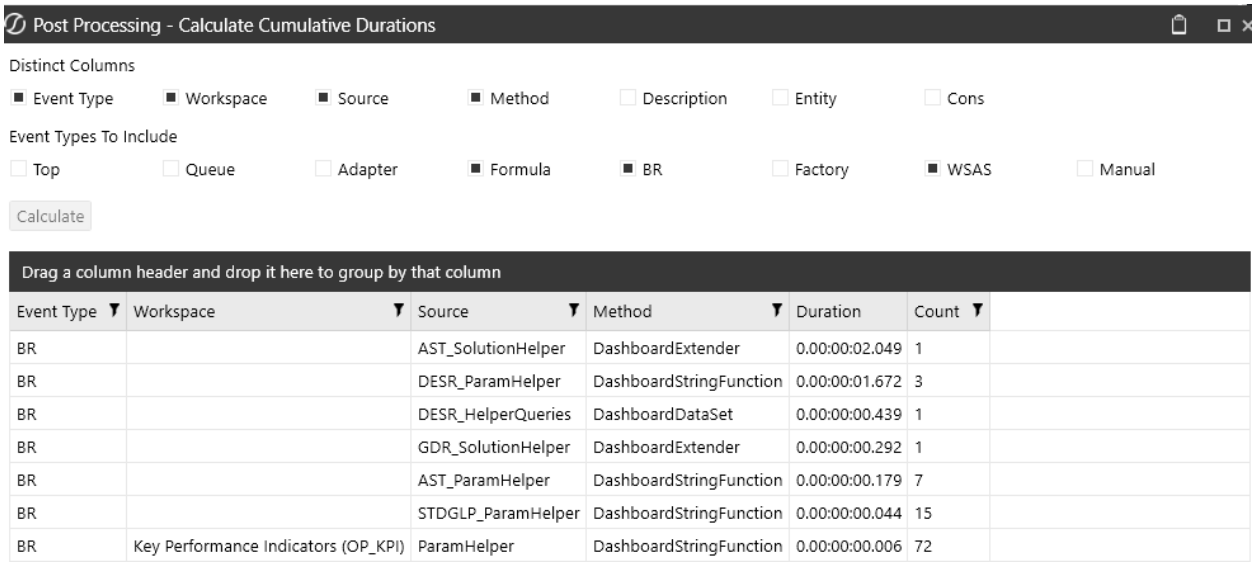
To display the **Post Processing - Calculate Cumulative Durations** window, select the **Post Processing** button.



You can use the Post Processing - Calculate Cumulative Durations window to view information on different groupings, total all filtered items, and see what was returned. This information can help improve performance queries. For example, if you are looking at performance time, you can filter by event types and have them grouped together. This enables you to view which methods or events are taking longer than others. When you run a calculate, the grid displays the duration and count for all Event Types selected in addition to selected Distinct Columns.

To run post processing, make selections from **Distinct Columns** and **Event Types To Include**, and then select the **Calculate** button. Distinct Column selections will display as columns in the grid, and Event Types To Include selections will display as rows in the grid. The following Distinct Columns and Event Types To Include are selected by default: Event Type, Workspace, Source, Method, Formula, BR, and WSAS.





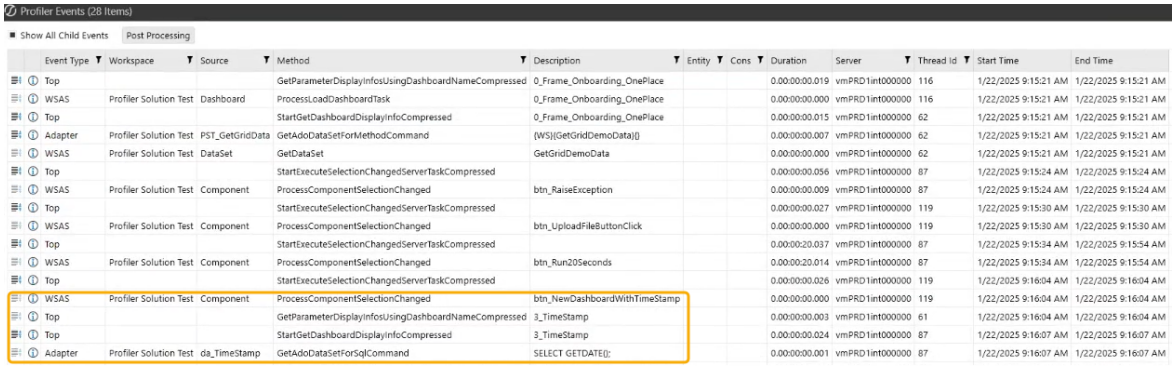
> **NOTE:** Updating the Distinct Column or Event Types To Include checkboxes after running a calculate will clear the results.

Event Information

To view Method Inputs, Method Results, and Method Errors for an event, select the **Event Information** button. The Events Information window contains the following tabs:

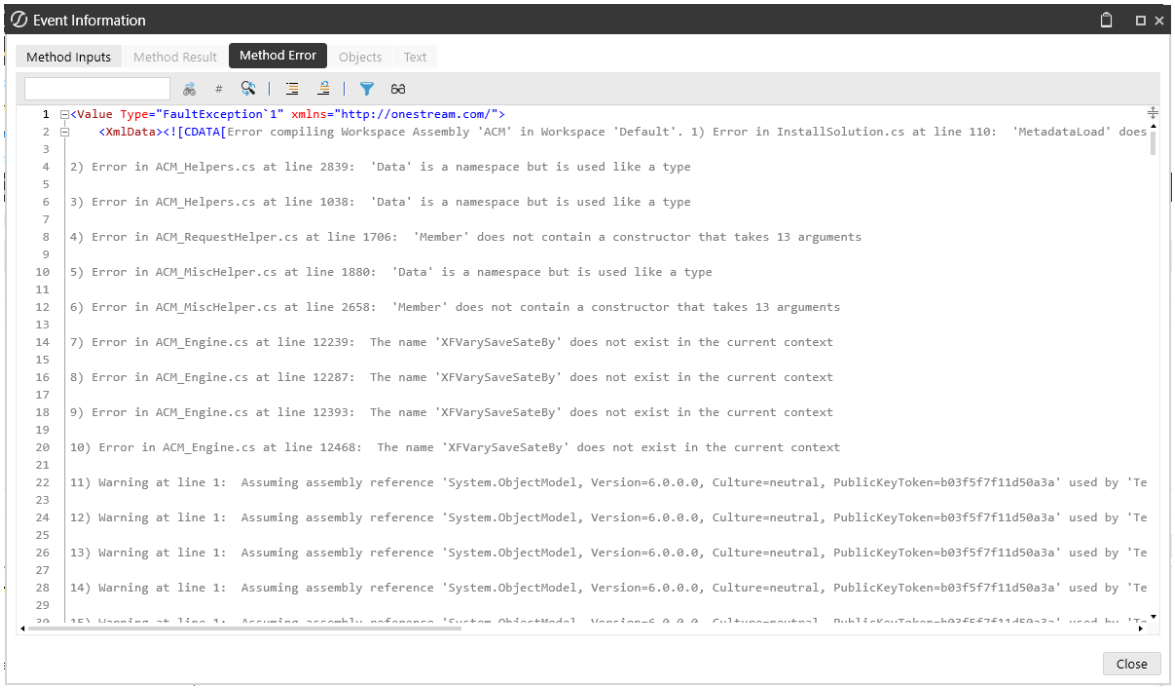
- **Method Inputs tab**: This displays the parameters or data passed into the method or event.
- **Method Result tab**: This displays the outcome or returned values of the method run.

  In the following example, the New Dashboard with Time Stamp button component was selected, which called the 3_TimeStamp dashboard and the GetAdoDataSetForSqlCommand method.



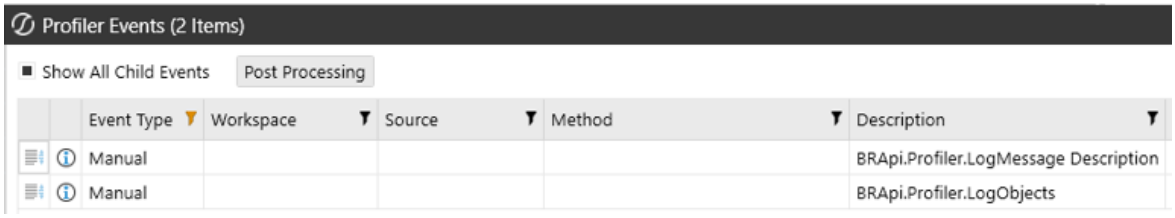
The Event Information window displays all method inputs, including the SQL Query and the date stamp submitted when the dashboard opened. The Method Result tab displays the time stamp that was returned to the dashboard.

- **Method Error tab**: This displays any errors encountered during the session, providing thorough troubleshooting potential.

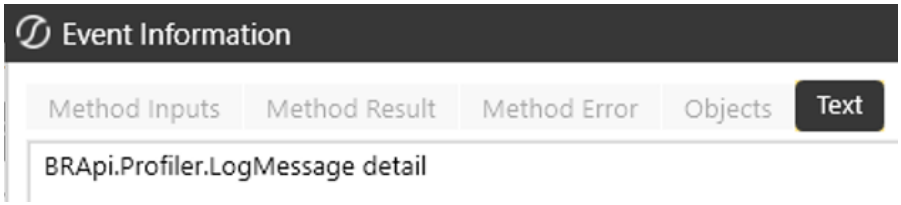


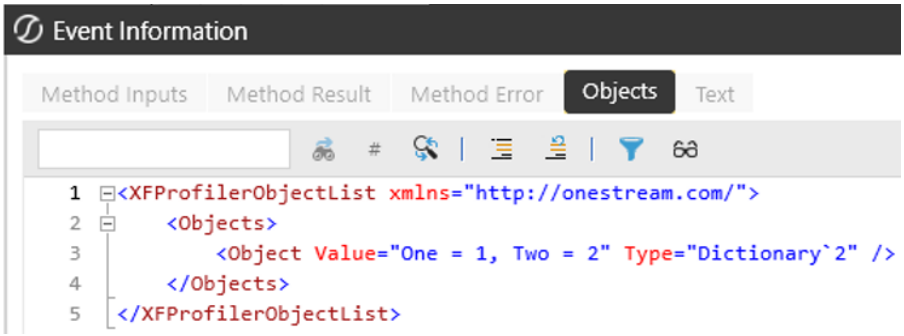
- **Objects and Text tabs**: These are enabled for Manual event types if objects or messages are logged through BRApi calls.

  In the following example, a user has the BRApi call attached to a button interaction to log the relevant information.



  In the Event Information window for Manual event types, the user can view the BRApi.Profiler.LogMessage description in the Text tab and the BRApi.Profiler.LogObjects in the Objects tab.





BRApi.Profiler Methods

Reference the following calls directly in your business rules or application logic using the BRApi.Profiler prefix.

IsProfiling
This call determines if profiling is currently enabled for the session. This is useful for checking whether to log additional profiling information or to skip profiling logic for performance.

Use BRApi.Profiler.IsProfiling(si). si is your current SessionInfo object.

LogMessage
This call records a custom message to the Profiler Events log. This can be used to log checkpoints, user actions, or important events during business rule processing.

Use BRApi.Profiler.LogMessage(si, brProfilerSettings, "Description", "Detail").

- **si**: This is your current SessionInfo object.
- **brProfilerSettings**: This is your Profiler settings object. Use null if not applicable.
- **"Description"**: This is a short description of the event.
- **"Detail" (Optional)**: This is any additional detail.

> **Example:** You can use the following API call to log a message when a button is selected: BRApi.Profiler.LogMessage(si, brProfilerSettings, "Button clicked", "User clicked the 'Process' button.")

LogObjects
This logs the state of one or more objects to the Profiler Events log. This is useful for capturing the values of key objects at specific points in your process for diagnostics or auditing.

Use BRApi.Profiler.LogObjects(si, brProfilerSettings, "Description", [object1, object2, ...]).

- **si**: This is your current SessionInfo object.
- **brProfilerSettings**: This is your Profiler settings object. Use null if not applicable.
- **"Description"**: This is a short description of the event.
- **[object1, object2, ...]**: These are the objects whose states you want to capture.

Time Dimensions

Applications can have a monthly or weekly Time Dimension. Time Dimension Types determine if an application uses a weekly, monthly or 12/13 period frequency, and the type of calendar, such as 445 or 454. In a new application, use a custom Time Dimension Type so users can specify the number of months in a quarter and the number of weeks in a month.

After you create a Time Dimension, an XML file is generated. New applications use this file to implement the desired Time Dimension. If a Time Dimension Type is not assigned to a new application database, the default Standard Type is used.

> **NOTE:** Applications created prior to 4.1.0 can convert a monthly application to weekly application using the Database Configuration Utility. Contact Support for assistance.

Time Dimension Types

The following are the time dimension types:

- **Time Dimension Type Standard**: Creates a Monthly Time Dimension and stores data by month in the data tables. Applications created prior to version 4.1.0 use this type.
- **StandardUsingBinaryData**: Creates a Monthly Time Dimension and stores data in a binary data table. Use this type if you may need to later convert an application to a Weekly Time Dimension.

- **M12_3333_W52_445**: Creates a 12 Month, 4 quarter, 52 Week, 445 calendar Time Dimension.
- **M12_3333_W52_454**: Creates a 12 Month, 4 quarter, 52 Week, 454 calendar Time Dimension.
- **M12_3333_W52_544**: Creates a 12 Month, 4 quarter, 52 Week, 544 calendar Time Dimension.
- **M12_3333_W53_445**: Creates a 12 Month, 4 quarter, 53 Week, 445 calendar Time Dimension.
- **M12_3333_W53_454**: Creates a 12 Month, 4 quarter, 53 Week, 454 calendar Time Dimension.
- **M12_3333_W53_544**: Creates a 12 Month, 4 quarter, 53 Week, 544 calendar Time Dimension.
- **Custom**: Creates a Time Dimension you can use to specify the months in a quarter and the in a month. This is only available for new applications.
- **Use Weeks**: If True, you can define a Custom Weekly Time Dimension. If False, you can create a Custom Monthly Time Dimension.
- **Vary Settings By Year**: If True, you can specify the number of weeks in a month for each year. If False, you can apply the number of weeks per month to each year.
- **M1- M16 Number of Weeks**: Specify the number of weeks per month. This coincides with the number of months per quarter, so any additional weeks required are enabled. If Vary Settings By Year property is True, select a year and customize the number of weeks in that year.