



Upgrade Guide for BrowserUX Early Access Programs

8.2.0 Release

Copyright © 2024 OneStream Software LLC. All rights reserved.

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

OneStream Software, OneStream, Extensible Dimensionality and the OneStream logo are trademarks of OneStream Software LLC in the United States and other countries. Microsoft, Microsoft Azure, Microsoft Office, Windows, Windows Server, Excel, .NET Framework, Internet Information Services, Windows Communication Foundation and SQL Server are registered trademarks or trademarks of Microsoft Corporation in the United States and/or other countries. DevExpress is a registered trademark of Developer Express, Inc. Cisco is a registered trademark of Cisco Systems, Inc. Intel is a trademark of Intel Corporation. AMD64 is a trademark of Advanced Micro Devices, Inc. Other names may be trademarks of their respective owners.

Table of Contents

Scheduling the Upgrade	1
Upgrading from Platform Releases pre-8.0	1
Upgrading from Platform Release 8.0	1
Requirements	2
Before Upgrading	4
Upgrade System Components	9
Uninstall OneStream Servers	9
Uninstall OneStream Client API	9
Re-Install OneStream Servers on an Application Server	9
Re-Install OneStream Servers on a Web Server	10
Re-Install OneStream for Desktop	11
Upgrade the Framework and Application Databases	12
Run the Upgrade Assistant Utility	12
Update the ASP.NET Configuration File	13
Update the Configuration Files	14
Update and Configure IIS	15
Test the Windows Client Login Using ClickOnce	15
Test the BrowserUX Login	16
Verify the Application	16

Table of Contents

Version 8.0 / .NET 6 Readiness	17
Business Rules	17
Custom DLLs	17
ERPConnect (SAP)	17
Smart Integration Connector	18
Authentication	18
.NET 6 Desktop Runtime and ASP.NET Runtime	18
VBA Changes	18
Client API Changes	18
Tiles Page	19
Help Documentation	19
Business Rule Groups	19
MarketPlace Solution Compatibility	19
Legacy Authentication	22
Native Authentication	23
Microsoft Active Directory (MSAD) and Lightweight Directory Access Protocol (LDAP) Authentication	24
OpenID Connect (OIDC) Authentication	24
Azure AD	24
Okta	27
PingFederate	30

Table of Contents

Security Assertion Markup Language (SAML) 2.0
Authentication 33

Enter External Provider Web SSO Key 36

Add Key for Encrypting Rest API Calls 37

User Profile Management 39

Third-Party Component Technology 40

Scheduling the Upgrade

Upgrading from Platform Releases pre-8.0

When upgrading from a Platform Release prior to 8.0 to Platform Release 8.0 or later, OneStream encourages customers to prepare for their upgrade by referencing content in the ONECommunity [Platform v8+ Upgrades](#) Group and by reaching out to their Customer Success representative.

OneStream Cloud customers may initiate Platform Release 8.0 or later upgrade interest by submitting a Software Upgrade request through the Service Catalog. Requests will be routed to the corresponding Customer Success representative who will reach out to discuss preparation activities required for upgrade readiness.

OneStream self-hosted customers may download Platform Release 8.0 or later from Solution Exchange, but are also encouraged to engage their Customer Success representative to review preparation activities to ensure a successful upgrade. Visit [Customer v8 Upgrade Summary & Readiness Checklist Documents](#) on OneCommunity for additional resources.

Upgrading from Platform Release 8.0

Upgrades from Platform Release 8.0 to 8.1 or later follow traditional OneStream best practices. Cloud customers can initiate and schedule upgrades through the Software Upgrade request on the Service Catalog, which will be followed by a scheduling request.

OneStream self-hosted customers may download Platform Release 8.2 directly from Solution Exchange and proceed with their upgrade.

Requirements

Information Technology professionals responsible for installing, maintaining and supporting OneStream, must satisfy the following requirements to best support an upgrade. They must also review the requirements and special notes in the *Installation and Configuration Guide* and *Release Notes*.

IMPORTANT: Platform Release 8.2 and later was developed using Microsoft .NET 8. As a result, all Business Rules must be tailored for .NET 8. For more information, see [Platform Release 8.0 or Later Readiness](#).

- OneStream Platform Release 8.2 or later requires Microsoft .NET 8.
 - App Server and Web Servers
 - Install the latest version of [ASP.NET Core Runtime \(Hosting Bundle\)](#) (minimum v8.0.2).
 - Install the latest version of [.NET Desktop Runtime \(x64\)](#) (minimum v8.0.2).
 - Client
 - Install the latest version of [.NET Desktop Runtime \(x64\)](#) (minimum v8.0.2).
- OneStream Servers requires IIS 7 or later.
- In each application, complete the **Compile all Business Rules and Formulas** to verify that business rules use the proper syntax.
- If your applications are referencing any 3rd party DLLs that are not provided by OneStream, verify these DLLs are .NET 8 compatible. Contact OneStream Support (<https://www.onestream.com/support/>) to discuss available upgrade options.
- When upgrading OneStream, ensure to update the database schema if an update is available. We recommend full database backups.
- Backup the Configuration files in your OneStream Share directory.
- For additional minimum system requirements, see Hardware and Software Requirements in the Installation and Configuration Guide.

Requirements

- When implementing SIC with the OneStream application, see [Requirements](#) in the Smart Integration Connector Guide.

IMPORTANT: Self-hosted customers must have a successful database connection prior to the Database Upgrade. See [Enable the Trust Server Certificate](#).

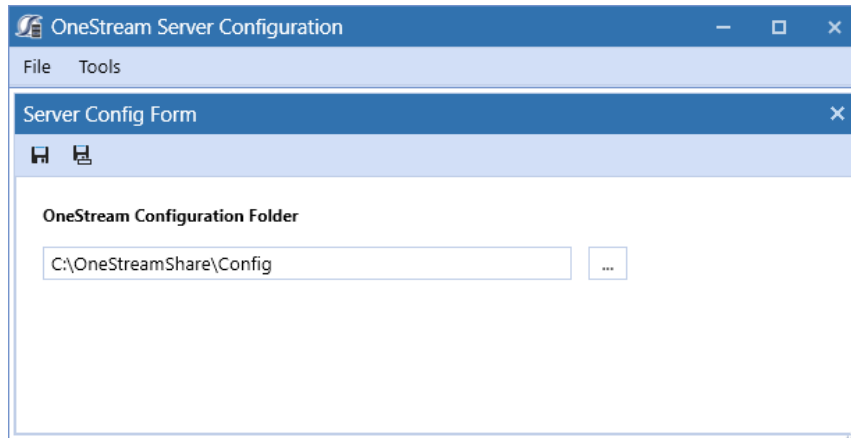
Before Upgrading

Perform these tasks before upgrading:

1. Perform a full backup of all OneStream databases.
2. Download the OneStream installation package from the [Solution Exchange](#):
 - a. Log in to the Solution Exchange and select **Platform** to get the latest version of OneStream.
 - b. Download the appropriate On-Premise package to get the appropriate setup files for the server installation.
3. Verify the location of the OneStream configuration files:
 - a. On a OneStream server, select **Start > Programs > OneStream Software > Server Configuration Utility**.
 - b. Right-click the utility and select **Run as Administrator**.
 - c. Select **File > Open ASP.NET Configuration File** and browse to the appropriate location.
 - **On web servers:** C:\Program Files\OneStream Software\OneStream WebRoot\OneStreamWeb and select **appsettings.json**.
 - **On application servers:** C:\Program Files\OneStreamSoftware\OneStreamAppRoot\OneStreamApp and select **appsettings.json**.

Before Upgrading

- d. The file opens and displays the path to the **XFAppServerConfig.xml** and **XFWebServerConfig.xml** configuration files.




- e. Copy and paste the path to the configuration file. You will specify this location during the upgrade.

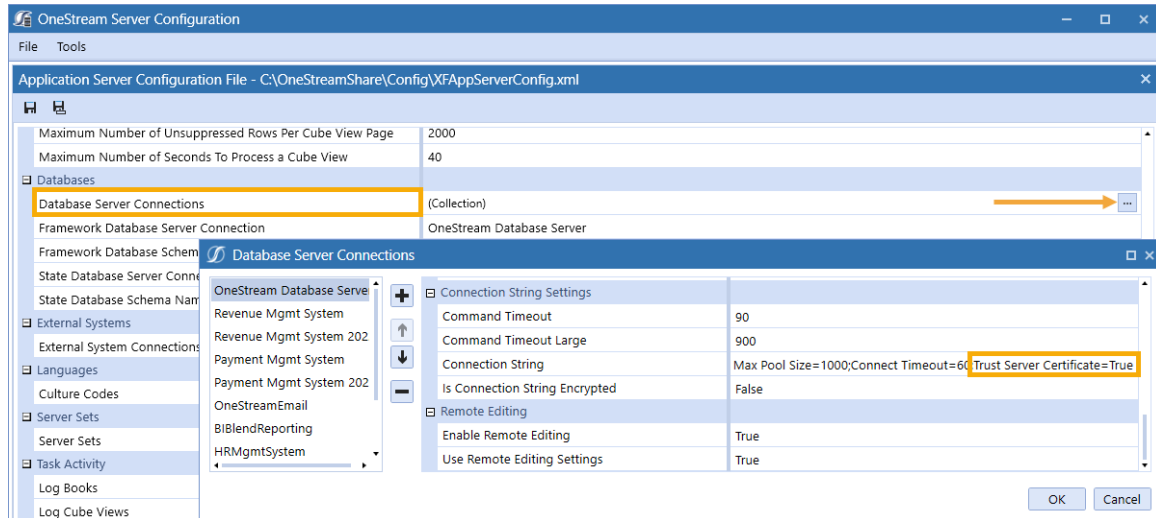
NOTE: This path is commonly set to **C:\OneStreamShare\Config**

4. For a backup, copy these configuration files.
5. Close the file without saving and exit the utility.
6. Verify the OneStream service account in Internet Information Services Manager:
 - a. The service account must be an Admin ID or in the IIS_IUSRS Group, Performance Log User and Performance Monitor Users group. The ID is required for queuing and CPU monitoring.
 - b. On each OneStream server, select **Start > Control Panel > Administrative Tools > Internet Information Services (IIS) Manager**.
 - c. Expand the server and select **Application Pools**. This displays application pools to the right. The OneStreamAppAppPool and OneStreamWebAppPool service accounts display in the Identity column. Note the Windows account and password as you will enter them in IIS after the upgrade.
7. Verify the availability of the OneStream Application Server where:

Before Upgrading

- The OneStream Database Configuration Utility is installed: On each OneStream application server, click **Start > Programs > OneStream Software** and verify that the OneStream Database Configuration Utility is installed.
 - OneStream is installed: On each OneStream application server, **Start > Programs > OneStream Software** to verify that OneStream is installed.
8. Install the following :
- **App Server and Web Servers**
 - Install the latest version of [ASP.NET Core Runtime \(Hosting Bundle\)](#) (minimum v8.0.2).
 - Install the latest version of [.NET Desktop Runtime \(x64\)](#) (minimum v8.0.2).
 - **Client**
 - Install the latest version of [.NET Desktop Runtime \(x64\)](#) (minimum v8.0.2).
9. On-prem customers must enable the **Trust Server Certificate** for the following:
- OneStream Database Server**
- From the OneStream Server Configuration Utility:
- a. Locate **Database Server Connections**.
 - b. Click  to open the Database Server Connections.
 - c. Add "Trust Server Certificate=True" to the end of the **Connection String**.
 - d. Click **OK**.

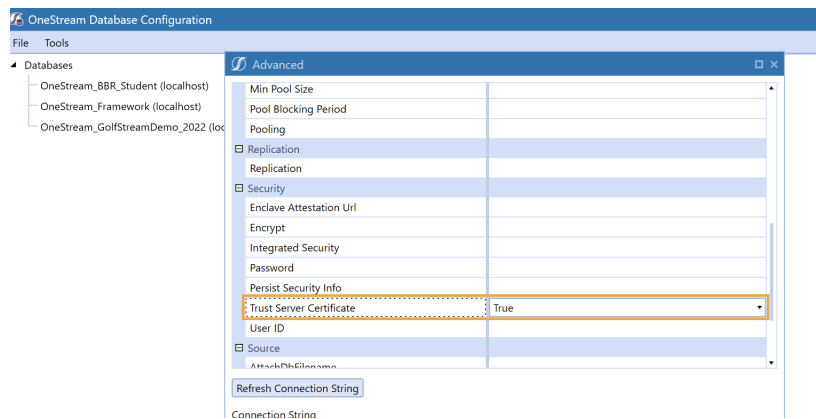
Before Upgrading



All Application Databases

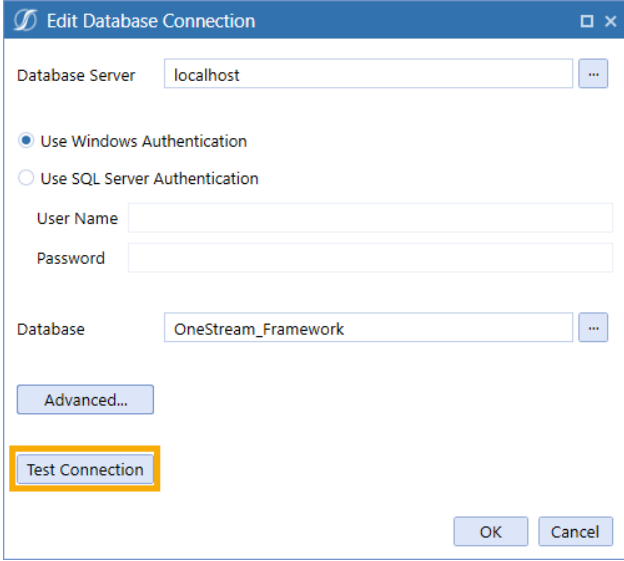
From the OneStream Database Configuration Utility:

- Right-click on a database, click **Edit the Database Configuration**.
- Select **Advanced**.
- Set **Trust Server Certificate** to **True**, then click **OK**.



Before Upgrading

- d. Select **Test Connection** to ensure a successful connection.



The screenshot shows a dialog box titled "Edit Database Connection". It contains the following fields and options:

- Database Server: localhost
- Use Windows Authentication (selected)
- Use SQL Server Authentication (unselected)
- User Name: (empty)
- Password: (empty)
- Database: OneStream_Framework
- Advanced... button
- Test Connection button (highlighted with an orange border)
- OK button
- Cancel button

NOTE: Alternatively, set the Trust Server Certificate to True directly in the XML.

```
];Max Pool Size=1000;Connect Timeout=60;TrustServerCertificate=True]]></ConnectionString>
```

Repeat these steps for all Application Databases.

Upgrade System Components

Perform the tasks in the following sections - in order, to upgrade the complete OneStream system.

Uninstall OneStream Servers

1. Select **Control Panel > Programs and Features > Uninstall a Program** and locate the OneStream Servers component.
2. Right-click **OneStream Servers** and select **Uninstall**.

Uninstall OneStream Client API

If installed, perform the following steps to uninstall the Client API:

1. Select **Control Panel > Programs and Features > Uninstall a Program** and locate the OneStream Client API component.
2. Right-click **OneStream Client API** and select **Uninstall**.

Re-Install OneStream Servers on an Application Server

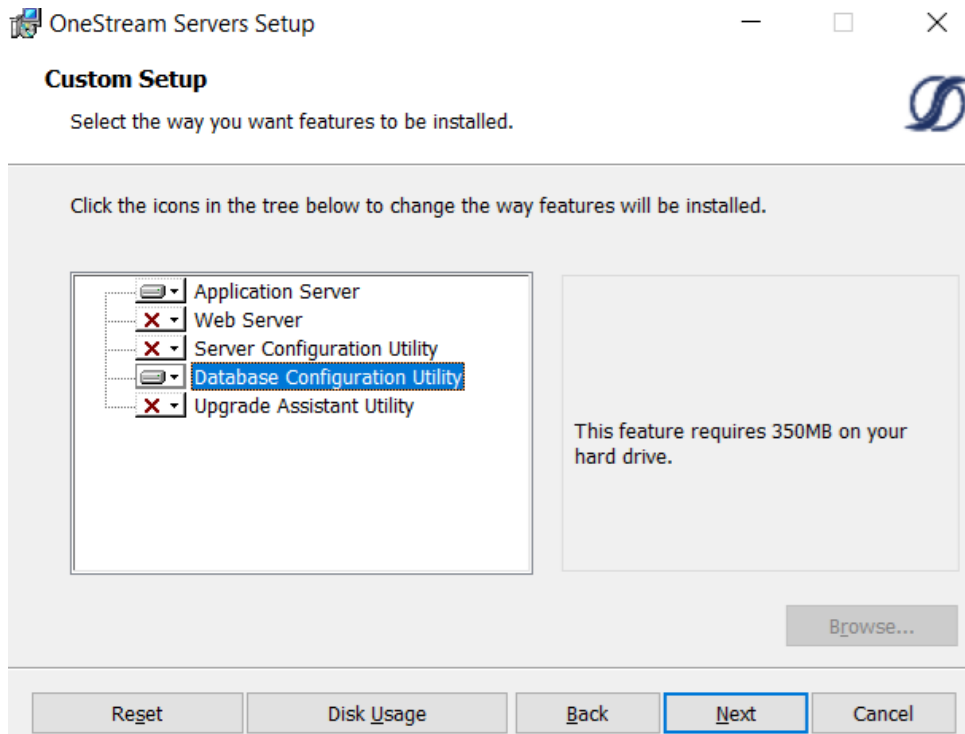
This is the primary installation package that performs a complete server setup, including the web server, application server and all utilities. You can perform a custom install to choose the appropriate server components.

1. Browse to the OneStream Servers package, right-click **OneStreamServers-WithBux-#.msi** and select **Install** to run the server installation.
2. Click **Next** on the landing page and accept the License Agreement.
3. Specify the directory where the software was previously installed and click **Next**.
4. Select **Custom**.

Upgrade System Components

5. On **Select Features**, choose **Application Server** and **Server Configuration Utility** and click **Next**.

NOTE: Choose the Database Configuration Utility and Upgrade Assistant Utility if the application server is the server where the Database Configuration Utility was previously installed.



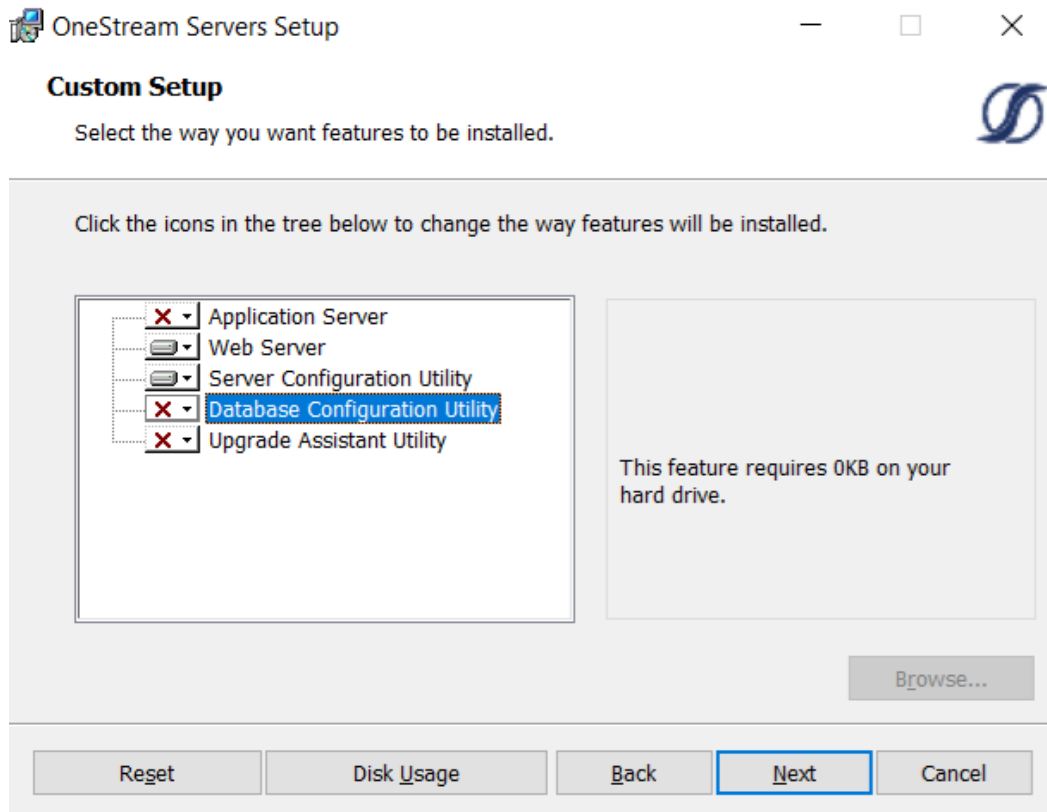
6. Click **Install** then **Finish**.

Re-Install OneStream Servers on a Web Server

1. Browse to the OneStream Servers package, right-click **OneStreamServers-WithBux-#.msi** and select **Install**.
2. Click **Next** and accept the **License Agreement**.
3. Specify the directory where the software was previously installed and click **Next**.

Upgrade System Components

4. Select **Custom**.
5. On **Select Features**, choose **Web Server** and **Server Configuration Utility** and click **Next**.



6. Click **Install** then **Finish**.

Re-Install OneStream for Desktop

1. Browse to the OneStream package, right-click **OneStreamDesktop-#.msi** and select **Install**.
2. Click **Next** and accept the License Agreement.
3. Select **Custom**.
4. Select the directory where the software was previously installed and click **Next**.

5. On **Select Features**, select all options and click **Next**.
6. Click **Install** then **Finish**.

Upgrade the Framework and Application Databases

Before performing these steps, have a database administrator back up all OneStream databases.

1. On the OneStream application server with the OneStream Database Configuration Utility installed, select **Start > Programs > OneStream Software > OneStream Database Configuration Utility**.
2. Right-click the utility and select **Run as Administrator**.
3. Right-click **OneStream Framework Database** and choose **Upgrade Database Version**.

NOTE: If this is disabled, an upgrade is not required.

NOTE: If you get an error, check the log for details: C:\Program Files\OneStream Software\XFDatabaseConfig\Log

4. Confirm the upgrade.
5. Repeat the upgrade for each **Application database** and the **Framework database** until the option is disabled. This will indicate you have updated to the current version.

Run the Upgrade Assistant Utility

Guidance for self-hosted environments

This is an additional step for when upgrading to Platform Release 8.0 or later and must be performed. Specifically, this version of the Upgrade Assistant Utility will convert any legacy reports that were stored in CodeDOM format to now be stored as XML.

1. On the OneStream application server with the OneStream Upgrade Assistant Utility installed, select **Start > Programs > OneStream Software > OneStream Upgrade Assistant Utility**.

Upgrade System Components

2. From the command line enter:

```
xfupgradeassistant -c C:\OneStreamShare\Config\XFAppServerConfig.xml -t  
ReportLayoutBytes -v -update
```

NOTE: C:\OneStreamShare\Config is the default path to the configuration file. You must update this path if it has been modified for your environment.

3. Enter exit to close the utility.
4. Restart IIS.

Update the ASP.NET Configuration File

The ASP.NET Configuration file (**appsettings.json**) must be updated on every server / folder as outlined below:

- Application server
 - C:\Program Files\OneStream Software\OneStreamAppRoot\OneStreamApp\appsettings.json
 - C:\Program Files\OneStream Software\OneStreamAppRoot\OneStreamMgmt\appsettings.json
 - Web servers:
 - C:\Program Files\OneStream Software\OneStreamWebRoot\OneStreamWeb\appsettings.json
 - C:\Program Files\OneStream Software\OneStreamWebApiRoot\OneStreamWebApi\appsettings.json
 - C:\Program Files\OneStream Software\OneStreamWebUIRoot\OneStreamWebUI\appsettings.json
1. On each OneStream server, launch the OneStream Server Configuration Utility by clicking **Start > Programs > OneStream Software > Server Configuration Utility**.
 2. Right-click the utility and select **Run as Administrator**.

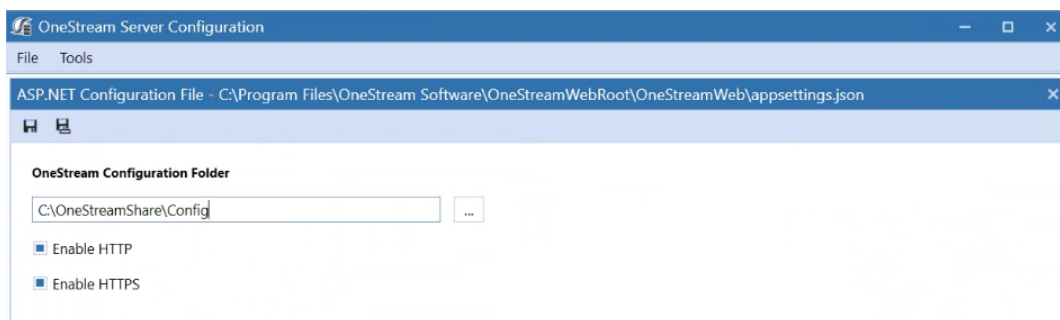
Upgrade System Components

3. Choose **File > Open ASP.NET Configuration File** and browse to the appropriate location from the folders above.
4. Select the **appsettings.json** file.
5. When the file opens, copy the directory path of the configuration files.

NOTE: This path is commonly set to C:\OneStreamShare\Config

6. **Enable HTTP** and **Enable HTTPS** are enabled by default.

NOTE: Clear **Enable HTTP** when SSL is enabled or clear **Enable HTTPS** when SSL is not enabled.



7. Save and close the file.
8. Repeat these steps on each web and app server in the environment.

Update the Configuration Files

1. Open the Application Server Configuration file from C:\OneStreamShare\Config in a text editor and select **Save**.
2. Open the OneStream Server Configuration Utility, Run as Administrator.
3. Select **File > Open** and select the file from C:\OneStreamShare\Config. In **Database Server Connections**, select the ellipsis and update the command time-outs for the OneStream Database Server connection:

Short = 90 *must do

Large =900 (minimum or 900)

4. Select **File > Save** and close the file.
5. Repeat these steps for the **Web Server Configuration** file.

Update and Configure IIS

1. On each OneStream server, open the OneStream Server Configuration Utility by clicking **Start > Programs > OneStream Software > Server Configuration Utility**.
2. Right-click the utility and select **Run as Administrator**.
3. Choose **Tools > Configure IIS**.
4. In **Configure IIS**, specify the following:
 - a. For Web Site Name, enter the name of the OneStream IIS Website to update.
 - b. The OneStream App Server, and Web Server sites.
5. Select **Update IIS Default Settings**.
6. Select options to update IIS for the appropriate websites:
 - a. **Use Web Server Settings**: Specify the Web Server site.
 - b. **Use App Server Settings**: Specify the App Server site.
 - c. **User Account Type**: Specify **Custom Account**, then enter the user name and password of the OneStream Service account.
7. Click **Update IIS Settings** then **OK**.
8. Repeat these steps to set the appropriate IIS settings for the application pools in IIS.
9. Click **Reset IIS**.

Test the Windows Client Login Using ClickOnce

1. Using the Microsoft Edge Web Browser, navigate to the OneStream Windows App URL:

Upgrade System Components

- **On Prem:** http://<webserver>:50001/OneStreamWeb
 - **Cloud:** https://<customer>.onestreamcloud.com/OneStreamWeb
2. Click **Open** to launch the ClickOnce Windows app.
 3. Confirm that you can log in.
 4. From **Application**, select **System Administration** then click **Connect**.
 5. Select **System > Tools > Environment** to identify the application servers and their status.
 6. Verify that each server is active.

Test the BrowserUX Login

1. Navigate to the OneStream BrowserUX URL:
 - **On Prem for BrowserUX:** http://<webserver>:50001
 - **Cloud for BrowserUX:** https://<customer>.onestreamcloud.com
2. Confirm that you can log in.

Verify the Application

1. Compile all business rules, ensure to:
 - Right-click the grid and export any errors for analysis using an Excel file format.
 - Apply updates as needed.
2. Download and import the Standard Application and Standard System Reports from the MarketPlace portal on the [Solution Exchange](#).

Version 8.0 / .NET 6 Readiness

Upgrading your OneStream Platform to version 8.0 or later requires .NET 6 for full compatibility.

This Platform release includes updates and enhancements to the Business Rules compiler to improve syntax detection. Administrators must resolve these errors to compile business rules fully. Warning messages identify line items that will function, but you should update them to support the latest compiler's requirements. Resolving these warnings varies. You may be able to use a provided replacement function or change a function's properties.

Business Rules

For more information, visit the [Platform v8+ Upgrades](#) page on ONECommunity.

Custom DLLs

If your implementation / business rules reference any custom DLLs that are not provided by OneStream, these DLLs must be .NET 6 compatible. Contact OneStream Support (<https://www.onestream.com/support/>) to discuss available upgrade options.

ERPConnect (SAP)

ERPConnect45.dll enabling connection to SAP systems is no longer available in Platform 8.0. A newer version ERPConnectStandard20.dll is available through the download "DLL Packages" from the Platform page of the [Solution Exchange](#).

On-Prem Customers:

1. Download ERPConnectStandard20.dll file to your integrations folder.
2. Install the required [Visual C++ 2013 Runtime](#).
3. Download and copy SAP NetWeaver RFC Library DLL (sapnwrfc.dll) to the integrations folder.
See [Theobald Software ERPConnect](#) Requirements for more information.
4. Modify your business rules to use the ERPConnectStandard20.dll.

Cloud/SaaS Customers: ERPConnect is available through the Smart Integration Connector (SIC). See ERPConnect section of the SIC Guide for installation details or contact OneStream Support (<https://www.onestream.com/support/>) to discuss more upgrade options.

Smart Integration Connector

[Smart Integration Connector](#) is required for OneStream Cloud integration with local customer data sources when using OneStream Platform version 8.0 or higher. VPN is no longer supported with version 8.0 or higher and will reach end of service for Platform versions prior to version 8 on August 31, 2024.

Authentication

Cloud Customers: [OneStream IdentityServer](#) is required for OneStream Platform 8.0.

Self-hosted Customers: Legacy Authentication support is the standard for self-hosted customers. See [Legacy Authentication](#) for more information.

.NET 6 Desktop Runtime and ASP.NET Runtime

To best align with Microsoft's long-term support strategy, OneStream Platform version 8.x is built using .NET 6. Platform 8.x users are required to use the latest versions of [.NET Desktop Runtime x64](#) and [ASP .NET Core Runtime Hosting Bundle \(6.0.14 minimum\)](#).

VBA Changes

ProcessSSOAuthenticationAndCreateToken is no longer supported as an authentication option from VBA scripts. See [Visual Basic for Applications \(VBA\) Procedures](#) for additional details. See Visual Basic for Applications (VBA) Procedures in the Design and Reference Guide for additional details.

Client API Changes

Client API is no longer provided with Platform version 8.0 or higher. OneStream recommends Task Scheduler or the REST API to replace existing Client API use cases.

Tiles Page

The ClickOnce journey is enhanced to launch the application with a single click of the **Open** button while eliminating the tiles page. For more information, see [Installation Using ClickOnce](#) in the Installation and Configuration Guide. For more information, see Installation Using ClickOnce in the Installation and Configuration Guide.

Help Documentation

Help documentation has moved from within the application to <https://documentation.onestream.com>. Clicking the in-app help icon routes you to this site.

Business Rule Groups

In version 8.0 the default for new Business Rule Access or Maintenance Groups is the Administrators group. This default can be changed by the Server Configuration Utility.

MarketPlace Solution Compatibility

The following MarketPlace Solutions are compatible with OneStream Platform version 8.0.

MarketPlace Solution	Version
Administrator Solution Tools	PV620 SV101
Application Control Manager	PV710 SV100
Capital Planning	PV620 SV102
Cash Planning	PV620 SV102
Cloud Administration Tools	PV600 SV100
Contract Compliance	PV620 SV102

MarketPlace Solution	Version
Dimension Comparison	PV600 SV100
Excel Add-in Installer	PV710 SV100
File Explorer Manager	PV650 SV102
Financial Close	PV710 SV201
Guided Reporting	PV600 SV102
Help Desk	PV640 SV100
Marketplace Solution Tools	PV720 SV100
Metadata Builder	PV520 SV101
Model Maker	PV680 SV201
Parcel Service	PV630 SV100
People Planning	PV620 SV103
Predictive Analytics 123	PV620 SV101
Provision Request Manager	PV440 SV104
Reporting Compliance	PV620 SV103
Sales Planning	PV620 SV102
Sample Templates	PV600 SV100
Scenario Analysis 123	PV530 SV100

MarketPlace Solution	Version
Security Audit Reports	PV620 SV100
Standard Application Reports	PV610 SV201
Standard Cube View Styles	PV410 SV100
Standard System Reports	PV430 SV102
System Diagnostics	PV620 SV202
Table Data Manager	PV620 SV100
Task Manager	PV660 SV102
Tax Provision	PV620 SV200
Thing Compliance	PV620 SV102
Thing Planning	PV620 SV101
XML Security Remover	PV410 SV100

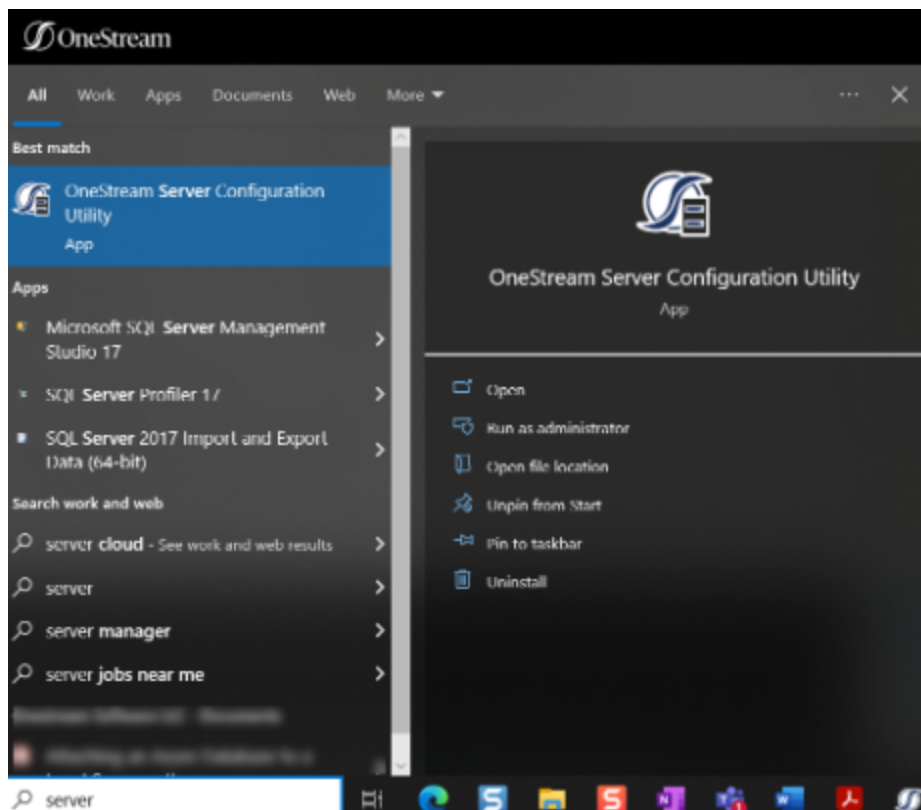
Legacy Authentication

If you are a customer in a self-hosted environment, you can choose between various authentication providers, but only one SSO authentication method can be used at a time. Before you configure your preferred method of authentication, ensure the following prerequisite steps have been completed:

- Download OneStream Platform v8.0.
- Perform the steps in [Installation and Configuration guide for SSO](#).

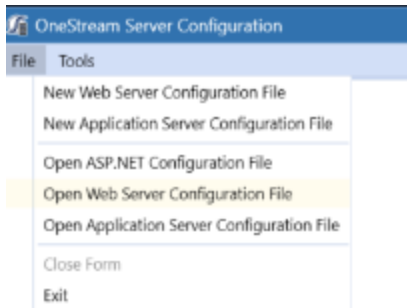
IMPORTANT: You must have these two items completed before you can proceed.

1. To begin, open the **OneStream Server Configuration Utility**.



Legacy Authentication

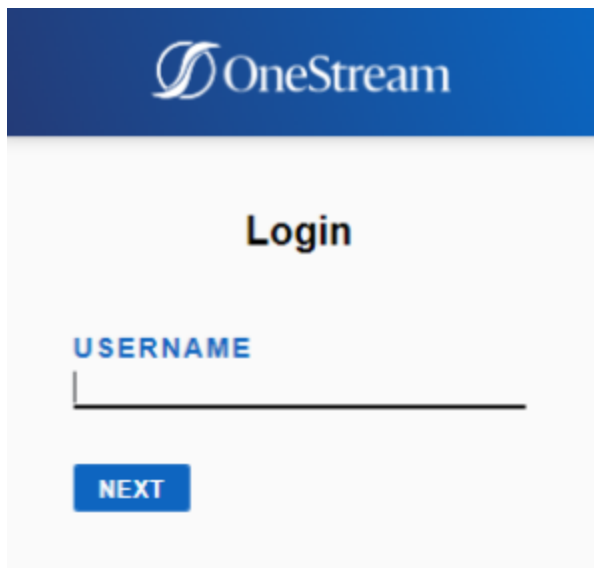
2. Select **File** to display the menu. Select **Open Web Server Configuration File**.



Native Authentication

Native authentication uses usernames and passwords saved in OneStream to authenticate BrowserUX users. To use native IDs for authentication, see the instructions provided in the Set Up for Native Authentication section of the Installation and Configuration Guide.

No additional configuration settings are required to enable Native authentication for BrowserUX.



Microsoft Active Directory (MSAD) and Lightweight Directory Access Protocol (LDAP) Authentication

BrowserUX supports MSAD and LDAP authentication. See Installation and Configuration Guide for configuration instructions.

No additional configuration settings are required to enable MSAD or LDAP authentication for BrowserUX.

OpenID Connect (OIDC) Authentication

For self-hosted customers, BrowserUX supports the following three OIDC IdPs:

- Azure AD
- Okta
- PingFederate

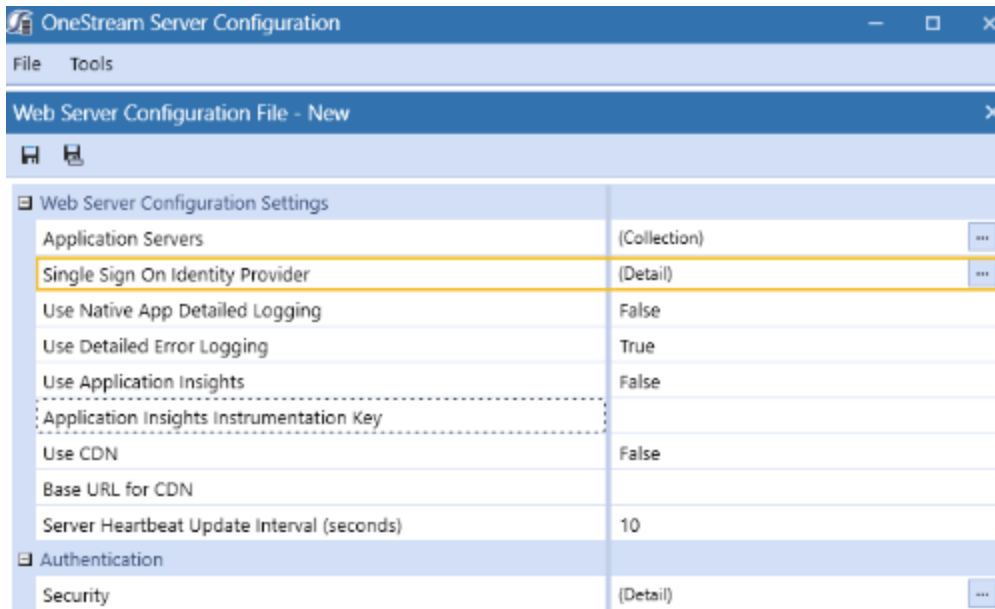
IMPORTANT: Once you have completed the configuration steps below for your IdP, we strongly recommend thoroughly testing your user authentication process.

Azure AD

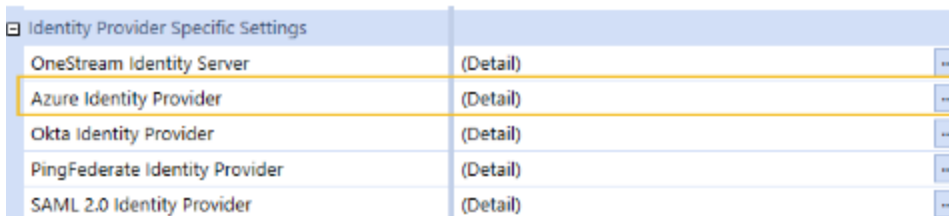
Follow these steps to enable Azure AD authentication for BrowserUX:

1. Log into your **Azure AD** account and complete the application registration.
2. Open the **OneStream Server Configuration Utility**.
3. Select **File > Open Web Server Configuration File**.
4. Open **Single Sign-On Identity Provider** settings.

Legacy Authentication



5. Open the **Azure Identity Provider** settings.

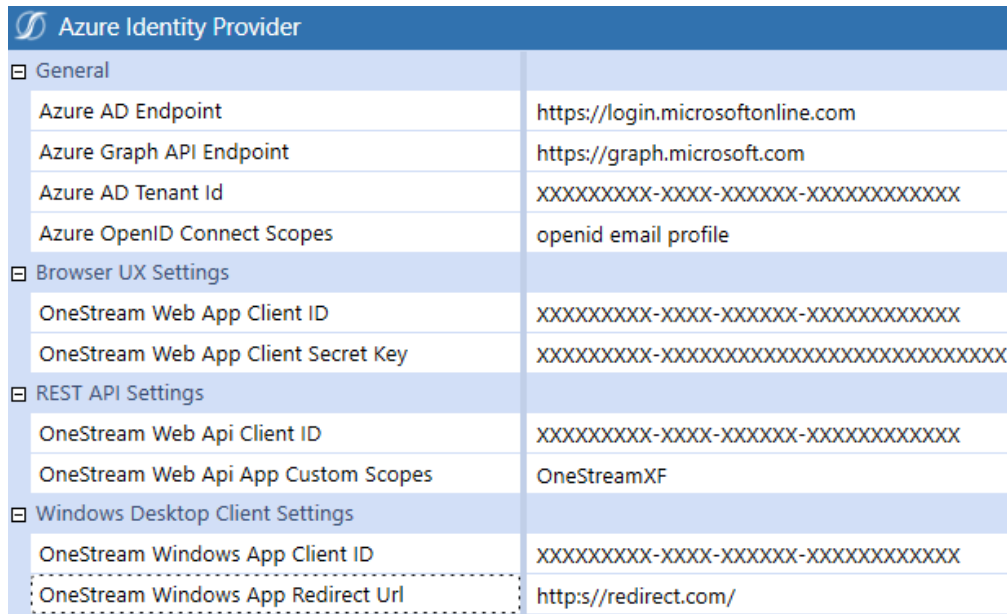


6. Collect the following **Azure Identity Provider** settings and enter:
 - a. **OneStream Web App Client ID** - Enter the Azure AD **Client ID**
 - b. **Azure Web App Client Secret Key** - Generate a random Secret Key from Azure.

NOTE: OneStream recommends using at least a thirty characters, alphanumeric, mixed case with symbols for a Secret Key. Copy your Client Secret Key. The value in your web server configuration must be the same in the application server configuration.

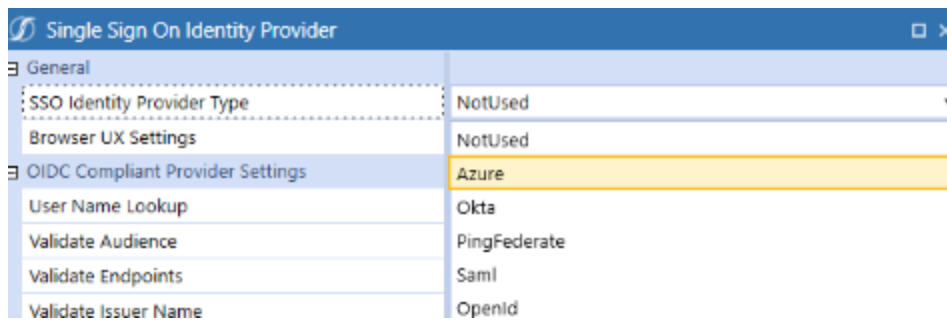
The settings should look like this:

Legacy Authentication



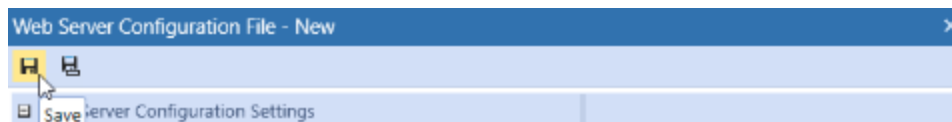
Azure Identity Provider	
General	
Azure AD Endpoint	https://login.microsoftonline.com
Azure Graph API Endpoint	https://graph.microsoft.com
Azure AD Tenant Id	XXXXXXXX-XXXX-XXXXXX-XXXXXXXXXXXX
Azure OpenID Connect Scopes	openid email profile
Browser UX Settings	
OneStream Web App Client ID	XXXXXXXX-XXXX-XXXXXX-XXXXXXXXXXXX
OneStream Web App Client Secret Key	XXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXX
REST API Settings	
OneStream Web Api Client ID	XXXXXXXX-XXXX-XXXXXX-XXXXXXXXXXXX
OneStream Web Api App Custom Scopes	OneStreamXF
Windows Desktop Client Settings	
OneStream Windows App Client ID	XXXXXXXX-XXXX-XXXXXX-XXXXXXXXXXXX
OneStream Windows App Redirect Url	https://redirect.com/

7. Select **OK**.
8. In the **Single Sign-On Identity Provider** window, set the **SSO Identity Provider Type** to **Azure**.



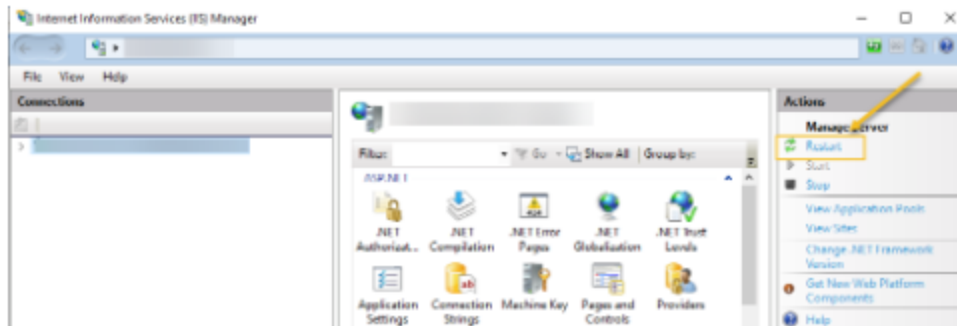
Single Sign On Identity Provider	
General	
SSO Identity Provider Type	NotUsed
Browser UX Settings	NotUsed
OIDC Compliant Provider Settings	
User Name Lookup	Okta
Validate Audience	PingFederate
Validate Endpoints	Saml
Validate Issuer Name	Openid

9. Select **OK**.
10. In the **Web Server Configuration File** window, select **Save**. Close the **OneStream Server Configuration Utility**.



Legacy Authentication

11. Open the **IIS Manager**. Run as an administrator.
12. Under **Manage Server**, click **Restart**.

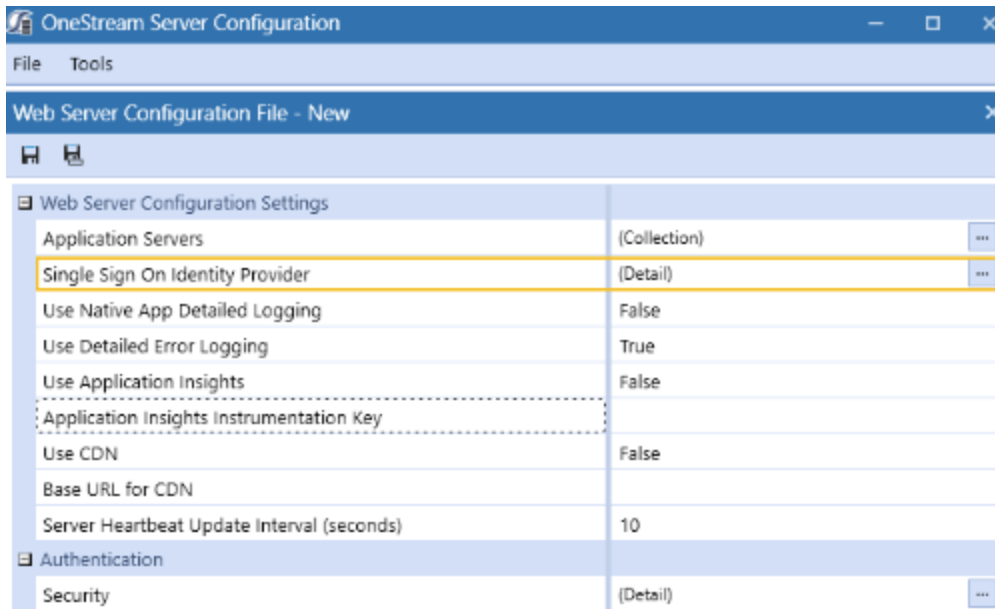


Okta

Follow these steps to enable **Okta** authentication for BrowserUX:

1. Log into your **Okta** account and complete the application registration.
2. Open the **OneStream Server Configuration Utility**.
3. Select **File > Open Web Server Configuration File**.
4. Open **Single Sign-On Identity Provider** settings.

Legacy Authentication



5. Open the **Okta Identity Provider** settings.
6. Collect the following from the **Okta Identity Provider** and enter the settings:
 - a. **OneStream Web App Client ID** - Enter the **Okta Client ID**
 - b. **Okta Web App Client Secret Key** - Generate a random Secret Key from Okta.

NOTE: OneStream recommends using at least a thirty characters, alphanumeric, mixed case with symbols for a Secret Key. Copy your Client Secret Key. The value in your web server configuration must be the same in the application server configuration.

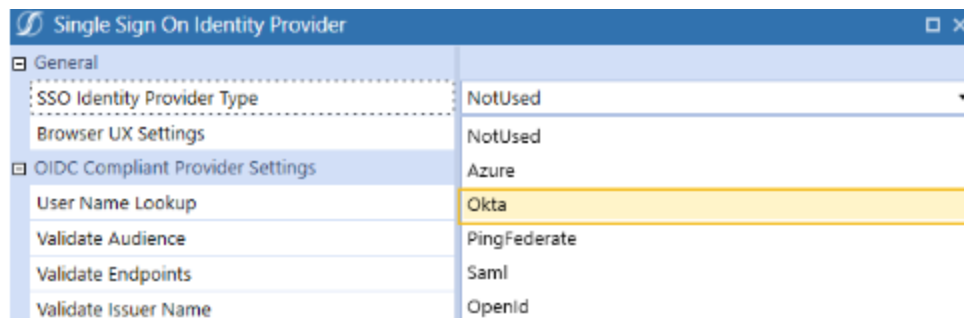
The settings should look like this:

Legacy Authentication



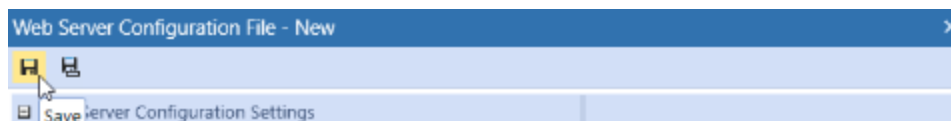
Okta Identity Provider	
General	
Okta Domain	https://onestreamsoftware.oktapreview.com/
Okta Scopes	openid email phone address profile
Okta Authorization Server ID	
Browser UX Settings	
OneStream Web App Client ID	XXXXXXXXXXXXXXXXXXXX
Okta Web App Client Secret Key	XXXXXX
REST API Settings	
Okta Web Api Client ID	XXXXXXXXXXXXXXXXXXXX
Okta Web Api Custom Scopes	
Okta Web Api Authorization Server ID	
Windows Desktop Client Settings	
OneStream Windows App Client ID	XXXXXXXXXXXXXXXXXXXX
OneStream Windows App Redirect Url	https://insights.onestreamcloud.com/OneStreamWeb/OneStreamLogonCallback.aspx

7. Click the **OK** button.
8. In the **Single Sign-On Identity Provider** window, set the **SSO Identity Provider Type** to **Okta**.



Single Sign On Identity Provider	
General	
SSO Identity Provider Type	NotUsed
Browser UX Settings	NotUsed
OIDC Compliant Provider Settings	
User Name Lookup	Okta
Validate Audience	PingFederate
Validate Endpoints	Saml
Validate Issuer Name	Openid

9. Select **OK**.
10. In the **Web Server Configuration File** window, select **Save**. Close the **OneStream Server Configuration Utility**.

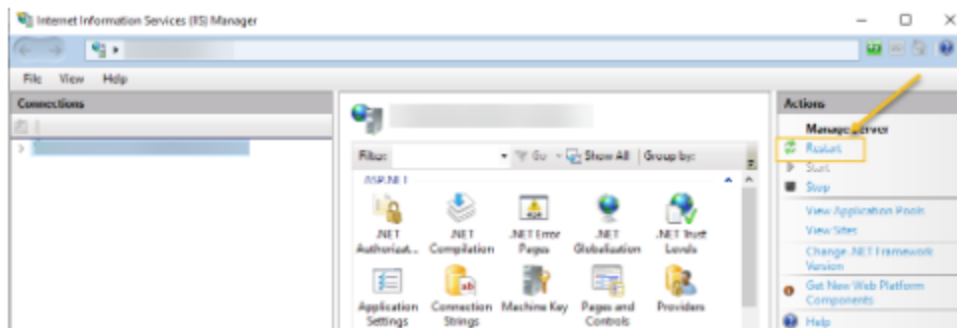


Web Server Configuration File - New	
Save	Server Configuration Settings

11. Open the **IIS Manager**. Run as an administrator.

Legacy Authentication

12. Under **Manage Server**, click **Restart**.

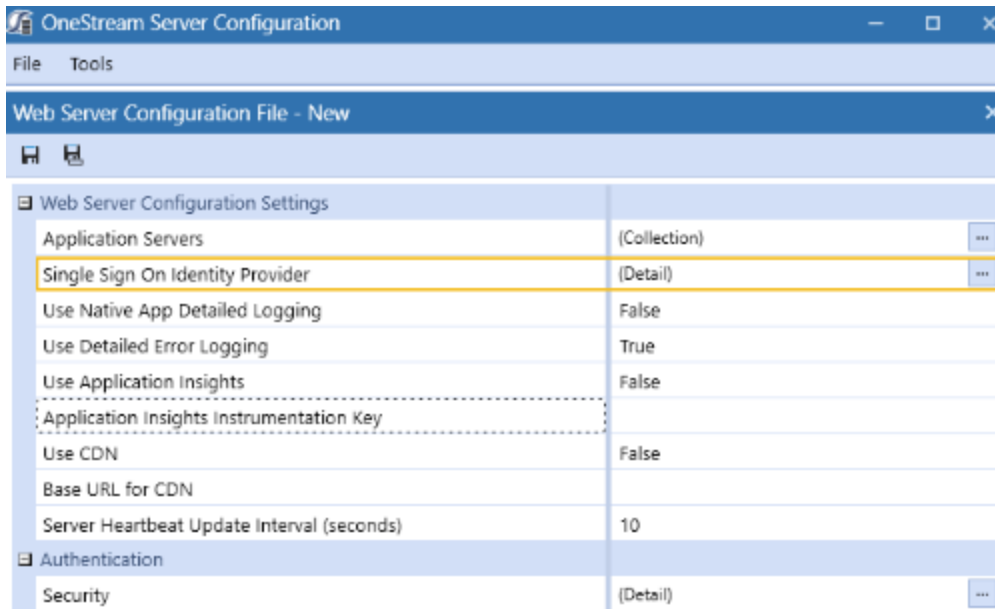


PingFederate

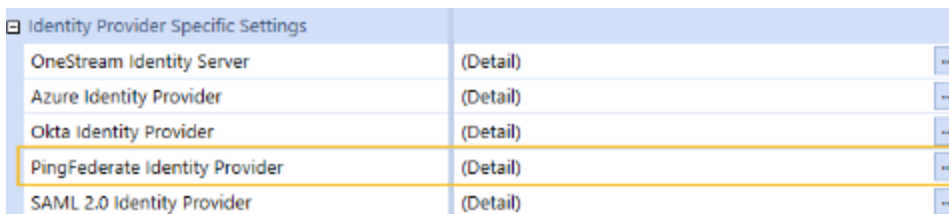
Follow these steps to enable PingFederate authentication for BrowserUX:

1. Log into your **PingFederate** account and complete the application registration.
2. Open the **OneStream Server Configuration Utility**.
3. Select **File > Open Web Server Configuration File**.
4. Open **Single Sign-On Identity Provider** settings.

Legacy Authentication



5. Open the **PingFederate Identity Provider** settings.



6. Collect the following **PingFederate Identity Provider** settings and enter:
 - a. **OneStream Web App Client ID** - Enter the PingFederate Client ID
 - b. **PingFederate Web App Client Secret Key** - Generate a random Secret Key from the PingFederate Administration utility.

NOTE: OneStream recommends using at least a thirty characters, alphanumeric, mixed case with symbols for a Secret Key. Copy your Client Secret Key. The value in your web server configuration must be the same in the application server configuration.

The settings should look like this:

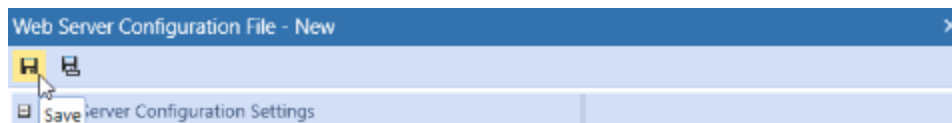
Legacy Authentication

PingFederate Identity Provider	
General	
PingFederate Domain	https://wmsso.pingfed.sso.onestreamdev.comXXXX
PingFederate Scopes	openid email phone address profile
Browser UX Settings	
OneStream Web App Client ID	TestBuxLegacy
OneStream Web App Client Secret Key	XX
REST API Settings	
OneStream Web Api Client ID	
OneStream Web Api Scopes	TestRestApi
OneStream Web Api JWKS Path	externalusername
Windows Desktop Client Settings	
OneStream Windows App Client ID	https://latest.onestreamdev.com/OneStreamWeb/OneStreamLogonCallback.aspx
OneStream Windows App Redirect Url	TestLocalDesktop

7. Select **OK**.
8. In the **Single Sign-On Identity Provider** window, set the **SSO Identity Provider Type** to **PingFederate**.

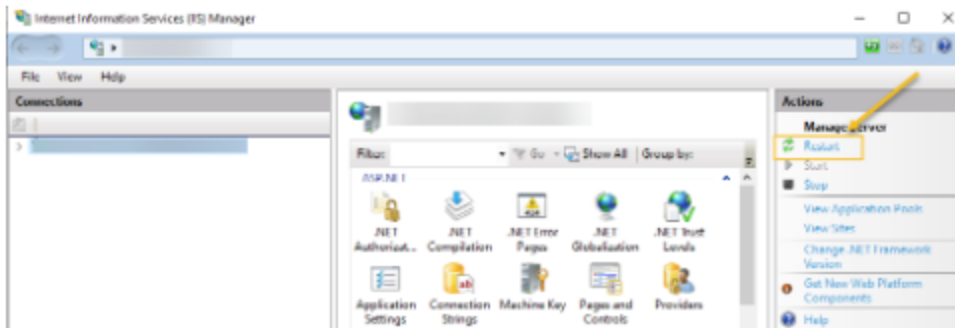
Single Sign On Identity Provider	
General	
SSO Identity Provider Type	NotUsed
Browser UX Settings	NotUsed
OIDC Compliant Provider Settings	
User Name Lookup	Okta
Validate Audience	PingFederate
Validate Endpoints	Saml
Validate Issuer Name	OpenId

9. Select **OK**.
10. On the **Web Server Configuration File** window, select **Save**. Close the **OneStream Server Configuration Utility**.



11. Open the **IIS Manager**. Run as an administrator.
12. Under **Manage Server**, click **Restart**.

Legacy Authentication

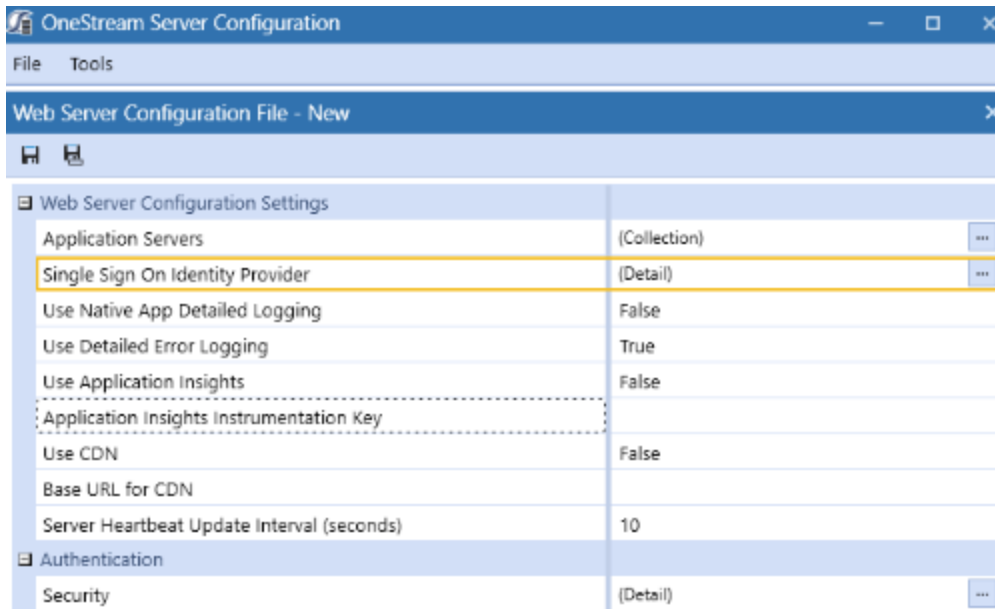


Security Assertion Markup Language (SAML) 2.0 Authentication

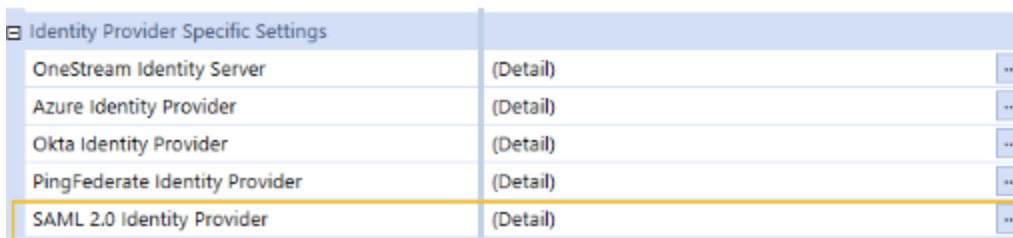
In BrowserUX, all SAML 2.0 Compliant IdPs are supported. Follow these steps to enable SAML support for BrowserUX:

1. Log into your **SAML 2.0 Identity Provider** account and complete the application registration.
2. Open the **OneStream Server Configuration Utility**.
3. Select **File > Open Web Server Configuration File**.
4. Open **Single Sign On Identity Provider** settings.

Legacy Authentication



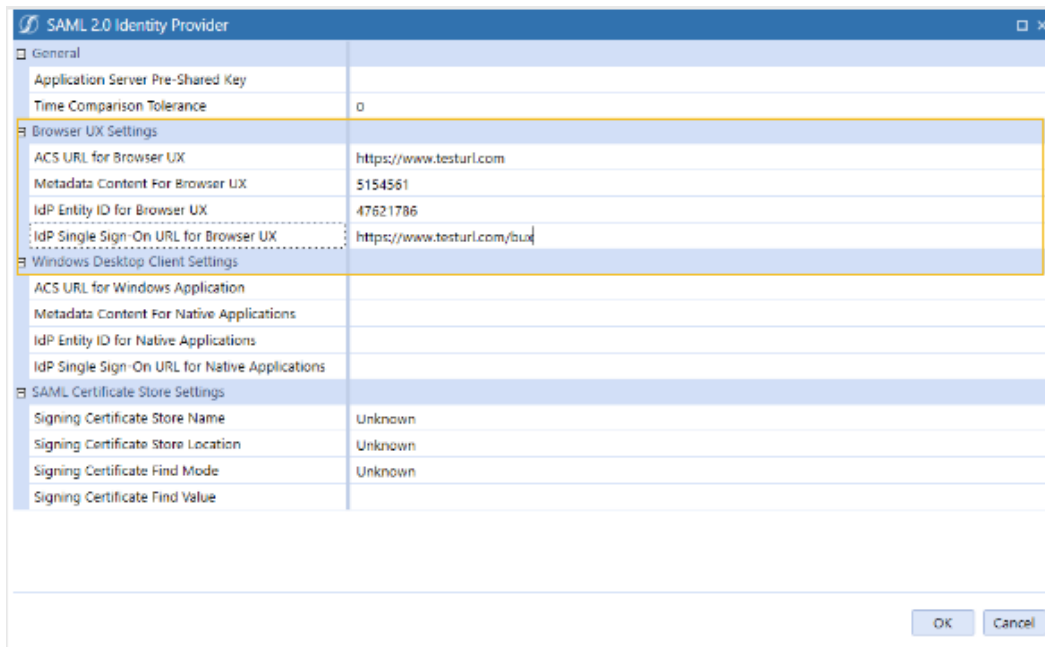
5. Open the **SAML 2.0 Identity Provider** settings.



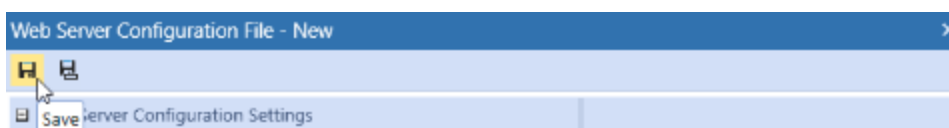
6. Enter the following BrowserUX settings:
 - a. **ACS URL for Browser** - Enter the Okta Client ID
 - b. **Metadata Content for BrowserUX**
 - c. **IdP Entity ID for BrowserUX**
 - d. **IdP Sign Sign-On URL for BrowserUX** - Create and enter the Secret Key from SAML.

The settings should look like this:

Legacy Authentication

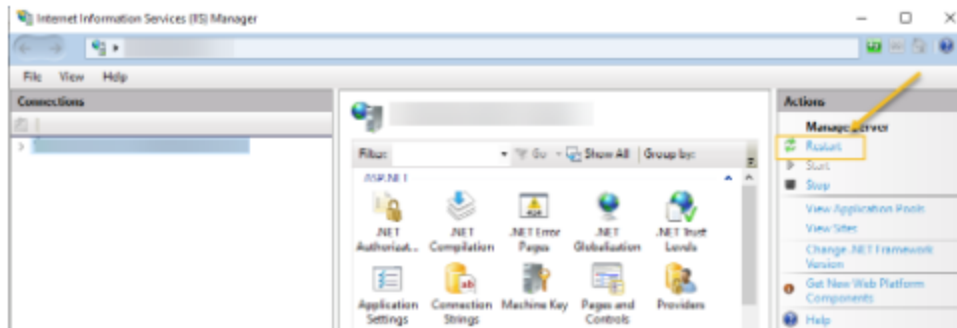


7. Select **OK**.
8. On the **Single Sign-On Identity Provider** window, set the **SSO Identity Provider Type** to **SAML**.
9. Select **OK**.
10. On the **Web Server Configuration File** window, select **Save**. Close the **OneStream Server Configuration Utility**.



11. Open your **Internet Information Services (IIS) Manager**. Run as an administrator.
12. Under **Manage Server**, click **Restart**.

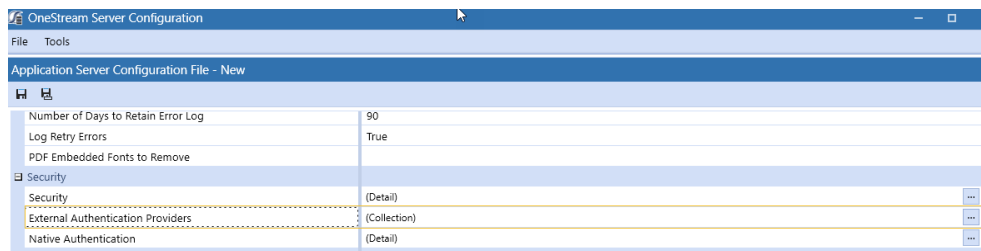
Legacy Authentication



Enter External Provider Web SSO Key

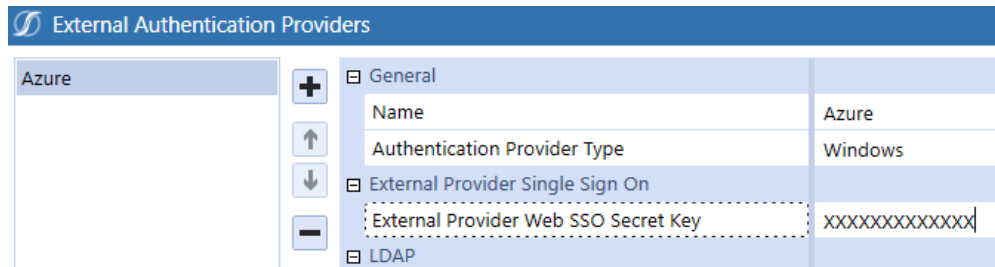
Next, you need to enter a unique value for **External Provider Web SSO Key**. This key is used in the OneStream Application Server Configuration and the OneStream Web Server Configuration. It enables your application server to communicate with the web server. This is the **Client Secret Key** you entered previously for your respective identity provider.

1. Copy your **Client Secret Key**.
2. Navigate to the **OneStream Server Configuration** utility.
3. Open **File > Open Application Server Configuration File > Security > External Authentication Providers**.



4. Click the ellipses and create a new **External Authentication Provider** for your respective identity provider.
5. Enter the **Client Secret Key** under **External Provider Web SSO Secret Key**.

Legacy Authentication



6. Click **OK**.
7. Save your **Application Configuration**.

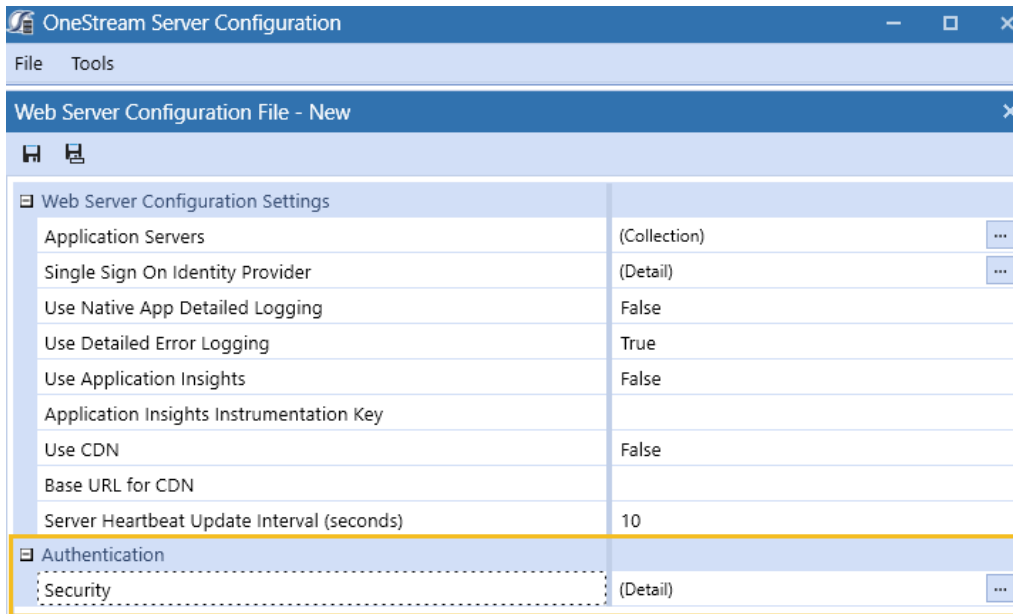
Add Key for Encrypting Rest API Calls

A Rest API key exists in both the OneStream Web Configuration and OneStream Application Configuration. If you do not enter a Rest API key, you will be unable to enter OneStream and BrowserUX clients.

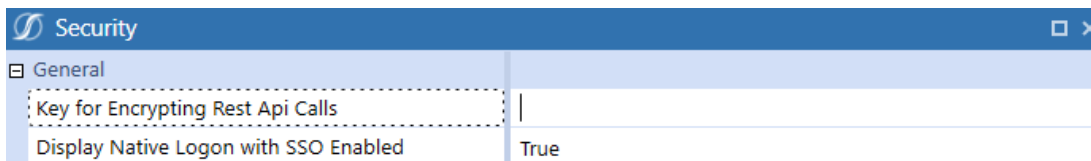
Web Server Configuration

1. Navigate to the **OneStream Server Configuration** utility.
2. Open **File > Open Web Server Configuration File > Authentication > Security**.

Legacy Authentication



3. Generate and enter a key in **Key for Encrypting Rest Api Calls**.



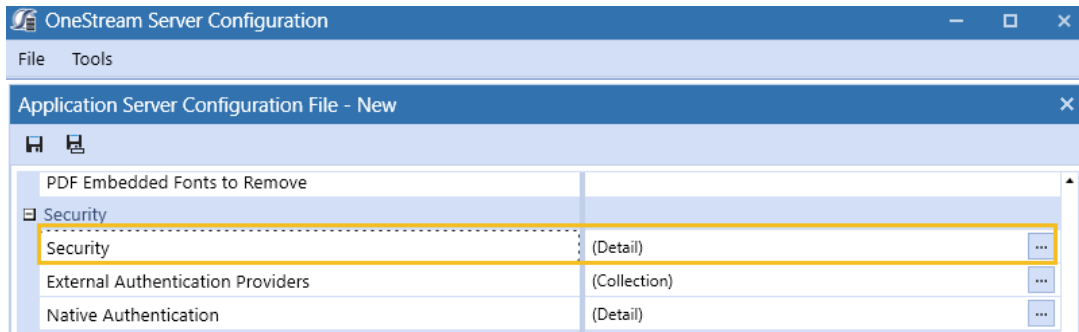
NOTE: OneStream recommends using at least a thirty characters, alphanumeric, mixed case with symbols for the **Key for Encrypting Rest Api Calls**.

4. Click **OK**.
5. Save your **Web Configuration**.

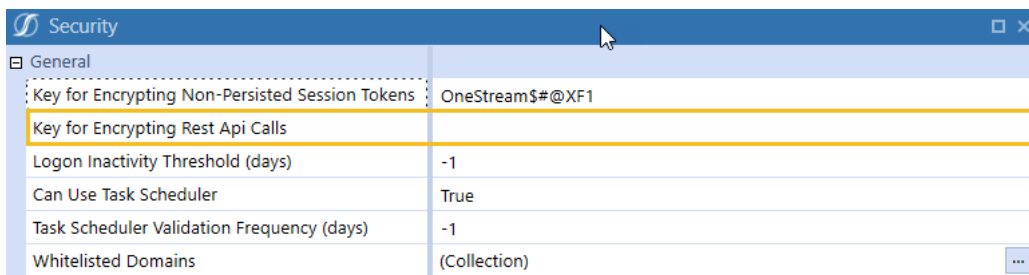
Application Server Configuration

1. Navigate to the **OneStream Server Configuration** utility.
2. Open **File > Open Application Server Configuration File > Security > Security**.

Legacy Authentication



3. Generate and enter a key in **Key for Encrypting Rest Api Calls**.



NOTE: OneStream recommends using at least a thirty characters, alphanumeric, mixed case with symbols for the **Key for Encrypting Rest Api Calls**.

4. Click **OK**.
5. Save your **Application Configuration**.

User Profile Management

OneStream has robust functionality for creating and managing users available in the Windows Client. For more information, see [Creating and Managing Users](#) in the Design and Reference Guide.

Once users have been configured, you can test IdP authentication configuration by logging into BrowserUX. See Log In and Log Out below.

Third-Party Component Technology

OneStream is created using both OneStream's own tools and third-party tools in the authoring, installation, and running of OneStream's supported products. OneStream BrowserUX third-party developer components include Syncfusion. OneStream customers are not required to purchase these developer tools.

The copyright notice with respect to these third parties is as follows:

- Syncfusion. (c) 2001-2023 Copyright Syncfusion Inc. All rights reserved.

For a comprehensive list of all third-party component tools throughout the OneStream Windows Client application, see [Third-Party Component Technology](#).