



Identity and Access Management Guide

8.2.3 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

About This Guide	1
OneStream IdentityServer	2
Benefits	2
Supported Authentication Configurations	3
Native Authentication	4
One External Identity Provider	4
Multiple External Identity Providers	4
How Users are Configured for Authentication	5
Load Authentication Properties by File	5
Authentication with an External Identity Provider	5
Native Authentication	6
Add New Users for Native Authentication	7
Onboarding Process and Considerations	8
About Environment Configuration	9
What to Expect	9
Best Practices	10
Verify User Accounts	11
Add an Email Address for Each User	11
Manage Native Accounts	11

Table of Contents

Resolve Common Errors	11
Global Errors	12
Common Errors	13
Logging	18
The End User Experience	18
About Login	19
Initial Login for Native Authentication	19
Login Flows	20
Change Applications and Log Off	26
Identity Providers	28
Requirements for Managing Identity Providers	28
OneStream IdentityServer Setup and System Configuration	28
Required System Security Role	29
Apply Security Role	29
Access the Manage Identity Providers Page	32
Manage OIDC Identity Providers	34
Add an OIDC Identity Provider	35
Test an OIDC Identity Provider	37
Resolve Common Issues when Testing OIDC Identity Providers	38
View Details of an OIDC Identity Provider	42

Table of Contents

Edit an OIDC Identity Provider	43
Remove an OIDC Identity Provider	44
Manage SAML 2.0 Identity Providers	44
Add a SAML 2.0 Identity Provider	45
Test a SAML 2.0 Identity Provider	50
Resolve Common Issues when Testing SAML 2.0 Identity Providers	51
View Details of a SAML 2.0 Identity Provider	56
Edit a SAML 2.0 Identity Provider	56
Remove a SAML 2.0 Identity Provider	58
Personal Access Tokens	59
Default Settings	60
Requirements for Using Personal Access Tokens	60
OneStream IdentityServer and Environment Setup	60
Required System Security Roles	60
Apply Security Roles	61
Access the Manage Personal Access Tokens Page	64
Manage Personal Access Tokens	67
Create a Personal Access Token	68
Revoke a Personal Access Token	68
About Using Personal Access Tokens in APIs	68

Table of Contents

Best Practices 69

Authentication Header Updates 69

API Call Comparison 70

Appendix: Example of Identity Provider Configuration 72

Okta OIDC Identity Provider 72

 Create an Okta Application 72

 Paste the Redirect URI in the Okta Application 78

About This Guide

This guide provides information about identity and access management, including:

- Benefits of OneStream IdentityServer (OIS) and high-level information about the supported authentication paths, end-user flows, best practices, and troubleshooting.
- Instructions to use the self-service feature to add, test, view, edit, and remove OIDC and SAML 2.0 compliant identity providers for authentication.
- Instructions to create, use, and revoke personal access tokens (PATs) generated by OneStream IdentityServer for authentication in OneStream REST API calls.

OneStream IdentityServer

OneStream IdentityServer is a single sign-on (SSO) service available for applications hosted in the OneStream Azure Cloud environment. OneStream IdentityServer supports multiple, concurrent OpenID Connect (OIDC) and SAML 2.0 protocol compliant external identity providers (IdPs) and native authentication, so you have more choice and flexibility implementing SSO.

OneStream IdentityServer is only available in the OneStream Hosted Cloud and is not intended for on-premises deployment. The Cloud Operations team deploys and configures OneStream IdentityServer.

The Cloud Operations team manages OneStream IdentityServer configuration properties in the IdentityServer database. Once an environment is enabled for OneStream IdentityServer:

- Native accounts are authenticated by OneStream IdentityServer.
- External provider user accounts are passed by OneStream IdentityServer to the configured IdP for authentication.
- You can generate and manage personal access tokens in the Identity & Access Management Portal to use in REST API calls. See [Personal Access Tokens](#).
- You can add and manage identity providers in the Identity & Access Management Portal. See [Identity Providers](#).

Users are defined in System Security, but their login flows vary depending on their configured authentication. See [Login Flows](#).

When implemented, OneStream IdentityServer governs authentication in the Windows Client application, the Excel Add-In, and BrowserUX.

Benefits

OneStream IdentityServer extends and optimizes user authentication by:

- Enabling real-time SSO with OIDC or SAML 2.0 compliant providers to best support an expanded user base.

- Simplifying the configuration of SAML 2.0-based IdPs, offering options for local certificate storage or the use of auto-discovery to eliminate certificate maintenance requirements.
- Providing for multiple IdP sources of authentication to be integrated to a single OneStream Cloud instance.
- Minimizing the end-user impact when adding and configuring external IdPs.
- Ensuring high system availability when adding or updating IdPs. Resetting IIS is not required during maintenance.
- Increasing security for OIS native authentication.
- Enabling OIS native authentication users to securely reset a forgotten password.
- Enabling you to independently manage OIDC and SAML 2.0 compliant identity providers. See [Identity Providers](#).
- Generating the personal access tokens you can use for seamless authentication in REST API calls. See [Personal Access Tokens](#).

Supported Authentication Configurations

OneStream IdentityServer provides a single source of authentication for the OneStream platform using OIDC protocol. This is beneficial because it ensures:

- Any OneStream application or process uses a well-defined standard authentication path.
- You can use and manage multiple authentication paths, such as native, external IdP using OIDC, and external IdP using SAML 2.0 protocol.

NOTE: OneStream IdentityServer does not support authentication using Microsoft Active Directory (MSAD) or Lightweight Directory Access Protocol (LDAP).

OneStream IdentityServer supports multiple configuration scenarios:

- Native authentication.
- Authentication with one external IdP. This can include native authentication.
- Authentication with multiple external IdPs. This can include native authentication.

Native Authentication

When used with native authentication, the OneStream IdentityServer acts as an identity provider. Usernames and passwords are validated against corresponding values in the OneStream framework database. In this authentication path, the OneStream platform performs all processing with no external dependencies.

To use this authentication path:

1. Submit a Support ticket requesting environment-specific support for native authentication. Environments must be initially configured for native authentication before you can use native login capabilities.
2. Enable user accounts for native authentication. See [How Users are Configured for Authentication](#) and [Native Authentication](#).

Similarly, contact the Support team if you later need to disable native authentication and native user accounts.

One External Identity Provider

If used with one external IdP, the OneStream IdentityServer acts as a service provider, passing authentication requests to a configured external IdP where users are challenged for their credentials. If a user has a valid SSO token, the request is processed without challenging the user for credentials. In this authentication path, processing depends on the OneStream platform and the external IdP. See [How Users are Configured for Authentication](#).

Multiple External Identity Providers

In this authentication path, you can configure the OneStream IdentityServer for:

- Native authentication with one or more external IdPs.
- Multiple external IdPs.

OneStream IdentityServer evaluates usernames at login using a "Home Realm Discovery" process where it determines the IdP configured to authenticate a user. The user is then challenged for their IdP credentials unless their SSO token is still valid. See [How Users are Configured for Authentication](#).

How Users are Configured for Authentication

To create users, go to **System > Security > Users > <user>**. Then, specify user authentication properties to authenticate users through an external IdP or using native authentication. In this example, a user is configured to authenticate through Okta.

General	
Status	
Authentication	
External Authentication Provider	Okta
External Provider User Name	OktaUser@okta.com
Internal Provider Password	•••••
Preferences	

TIP: You can load some authentication properties by file. See [Load Authentication Properties by File](#).

Load Authentication Properties by File

You can include the following external IdP properties in an XML load file that you import into System Security to configure users for authentication:

- External provider
- External provider user name

We suggest creating the load file using the security Excel templates provided with the Sample Templates MarketPlace solution. In the Security Template, on the Instructions tab, step 2 of User Security Design includes externalAuthProviderName and externalUserName.

Authentication with an External Identity Provider

To authenticate a user with an external IdP, complete the following fields:

- **External Authentication Provider** – The configured IdP provider, such as Salesforce or Okta. The selections available are determined by the security configuration and reflect the "Display Name" defined, during implementation, in the IdP's scheme.

- **External Provider User Name** – The username defined in the external IdP. This name must match and be used by only one user. For example, if a user's name for Okta is OktaUser@okta.com, specify OktaUser@okta.com as the External Provider User Name.

NOTE: Multiple users cannot have the same external provider user name.

NOTE: The default claims used to authenticate a user account with an external IdP are name identifier, email, and subject. Custom claims are also available. You can set up custom claims when you add or edit an identity provider in the Identity & Access Management Portal. See [Identity Providers](#). Contact Customer Support if needed.

General	
Status	
Authentication	
External Authentication Provider	Okta
External Provider User Name	OktaUser@okta.com
Internal Provider Password	••••••
Preferences	

Native Authentication

To configure users for native authentication and native login, modify user accounts in System Security, setting **External Authentication Provider** to **Not Used**, as shown in the following image. Note that you must first submit a Support ticket to request an environment be prepared for native authentication before you can configure user accounts.

General	
Status	
Authentication	
External Authentication Provider	(Not Used)
External Provider User Name	
Internal Provider Password	••••••
Preferences	

Similarly, work with Support to later disable native authentication and user accounts as needed.

Add New Users for Native Authentication




1. Go to **System > Security**.
2. Click **Create User**.
3. Enter information in the following fields.
 - **Name:** Enter a username.
 - **User Type:** Select a user type.
 - **External Authentication Provider:** Select **(Not Used)**.
 - **Internal Provider Password:** Enter a temporary password. The user will be prompted to reset the password the first time they log in.

NOTE: Default security settings are applied to OneStream passwords. Contact Customer Support for more information or to make a change to the security settings.

- **Email:** Enter the email associated with the account.

IMPORTANT: An email address is needed for the user to reset a forgotten password.

- **Group Membership:** Add the user to a group if needed. If no group is selected, the user will be added to the Everybody group.

[-] General	
Name	Jane
Description	
User Type	Interactive
Is Enabled	True
[-] Status	
[-] Authentication	
External Authentication Provider	(Not Used)
External Provider User Name	
Internal Provider Password	••••••
[-] Preferences	
Email	jane@email.com
Culture	English (United States)
Grid Rows Per Page	50
[-] Custom Text	
[-] Group Membership	
Parent Groups That Contain This User	  AccessAsNonInteractiveUserGroup 

4. Provide the user with the information that was entered in the **Name** and **Internal Provider Password** fields so that they can log in with their username and password.

Onboarding Process and Considerations

The Cloud Operations team installs OneStream IdentityServer and, if needed, will contact you with additional information about upgrading and the authentication configuration. To use OneStream IdentityServer, you must:

- Upgrade your OneStream Software environment to the latest version.
- Use OIDC or SAML 2.0 compliant external IdPs or OIS native authentication.

OneStream IdentityServer

- Partner closely with OneStream Software and the Cloud Operations team to integrate your identity providers, manage user data, and run tests.

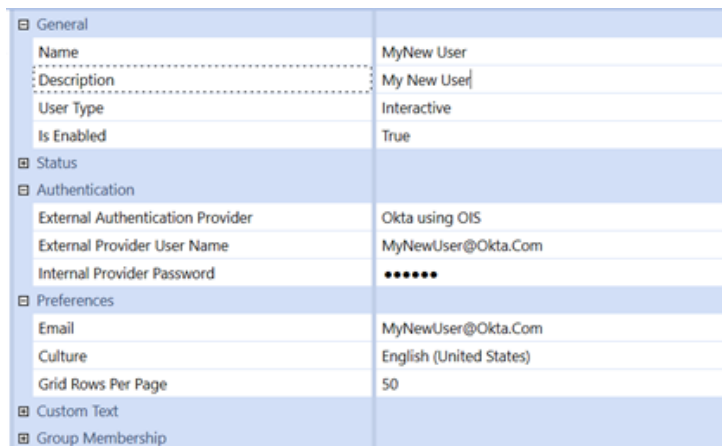
See [About Environment Configuration](#) and [What to Expect](#).

About Environment Configuration

Work with the Cloud Operations team to configure your environment and ensure all requirements are met.

Each OneStream environment can be uniquely configured for an SSO identity provider (IdP), with OneStream IdentityServer being one option. As a best practice, development, test, and production environments should have consistent configurations to simplify maintenance and migrations. When you deploy the OneStream IdentityServer, the first IdP is configured, as shown below, to seamlessly support OneStream IdentityServer for authentication. The IdP is configured:

- As the same type.
- So **OIS IdP Display Name** matches the existing **External Authentication Provider** label.



The screenshot shows a configuration interface for a new user. The configuration is organized into several sections, each with a collapse/expand icon (a square with a minus sign). The sections and their values are:

General	
Name	MyNew User
Description	My New User
User Type	Interactive
Is Enabled	True
Status	
Authentication	
External Authentication Provider	Okta using OIS
External Provider User Name	MyNewUser@Okta.Com
Internal Provider Password	*****
Preferences	
Email	MyNewUser@Okta.Com
Culture	English (United States)
Grid Rows Per Page	50
Custom Text	
Group Membership	

If the SSO IdP method differs between environments, ensure that the **OIS IdP Display Name** and the **External Authentication Provider** properties match. This ensures that you can migrate security between environments using the Load/Extract feature.

What to Expect

This section identifies what new and current customers can expect when adopting the OneStream IdentityServer.

New Customers

Cloud Operations installs OneStream IdentityServer and provides an External Identity Provider Request form that you complete to supply the configuration details required to set up IdPs for a OneStream environment. One of these properties is the **OIS IdP Display Name**, which:

- Is assigned as the external authentication provider to users created in OneStream.
- Dynamically determines the IdP with which users are associated. This determines the user login sequence. See [The End User Experience](#).

Add identity providers in the Identity & Access Management Portal. See [Identity Providers](#). Log a Support request if needed.

Existing Customers

When Cloud Operations convert an environment for OneStream IdentityServer:

- The current IdP is initially used as the first OneStream identity provider.
- Your environment is converted based on current legacy IdP configurations and current security settings.

You can authenticate users with OneStream IdentityServer when the **OIS IdP Display Name** matches the existing **External Authentication Provider** name. If these properties do not match, modify each user account to assign the appropriate IdP.

Work with the Cloud Operations team to ensure each identity provider has been migrated.

To use another external IdP, add an identity provider in the Identity & Access Management Portal. See [Identity Providers](#). Log a Support request if needed. You can also request to revert to your original configurations if needed.

If there are multiple identity providers with the same name in the **External Authentication Provider** drop-down menu, contact Support to remove the current legacy identity provider.

Best Practices

This section identifies best practices that will minimize login errors and streamline the login process.

Verify User Accounts

To avoid login errors, regardless of the authentication mode, confirm that:

- Users have valid, properly defined accounts in OneStream System Security. Ensure that their username in an external IdP is specified as their External Provider User Name.
- User accounts are active and were not disabled either in System Security or in the OneStream Framework database.

See "Creating and Managing Users" in the *Design and Reference Guide*.

Add an Email Address for Each User

To support all features of OneStream IdentityServer, add an email address for each user profile. An email address is needed to reset a forgotten password for OIS native authentication users.

General	
Status	
Authentication	
External Authentication Provider	(Not Used)
External Provider User Name	user@email.com
Internal Provider Password	••••••
Preferences	
Email	user@email.com
Culture	English (United States)
Grid Rows Per Page	50
Custom Text	
Group Membership	

Manage Native Accounts

Users you create in OneStream can be configured as native users. This means their accounts and passwords are managed in OneStream. Native authentication is treated as an additional identity provider, so using an external IdP with native authentication activates the Log In "Home Realm Discovery" dialog box.

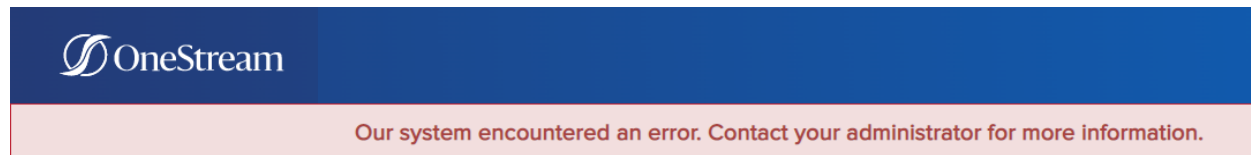
As a best practice, if you are not using OneStream IdentityServer native accounts, you should submit a Support ticket to disable native authentication. See [Native Authentication](#).

Resolve Common Errors

This section describes how errors display and how to resolve common issues.

Global Errors

When an environment is enabled for OneStream IdentityServer, generic messages about unrecoverable issues display on a Global Error Message page. For example: Our system encountered an error. Contact your administrator for more information.

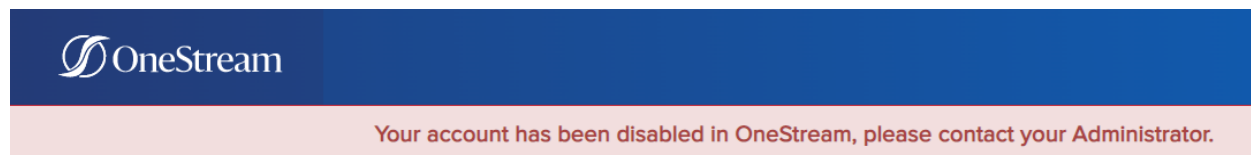


These issues can range from network and other communication problems to system configuration errors. Administrators resolve these issues. Other errors may display that are specific to how an environment is configured for user authentication, such as the number of external IdPs used.

For example, this error could indicate that the service provider entity ID URL is incorrect. The service provider entity ID URL both in the Identity & Access Management Portal and configured on the external identity provider must be an exact match, including capitalization.

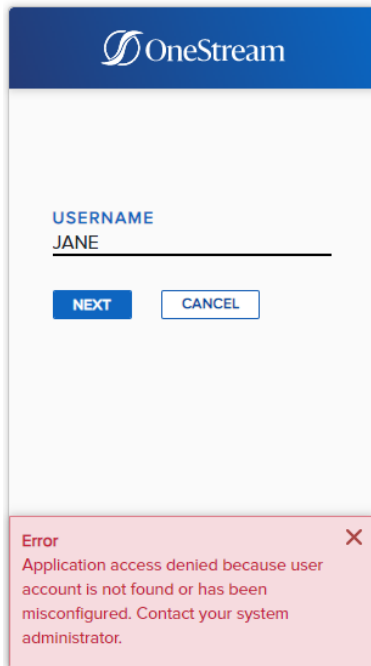
Single External IdP Configuration

If you use one IdP, the Global Error Message page may also display errors related to a user's authentication. For example, if a user authenticates through their IdP but is not a valid OneStream user or has a disabled user account, the following error displays: Your account has been disabled in OneStream, please contact your Administrator.



Multiple External IdP Configurations

If you use multiple IdPs, the Login dialog box may display errors and warning messages related to login and application access issues. For example: Application access denied because user account is not found or has been misconfigured. Contact your system administrator.

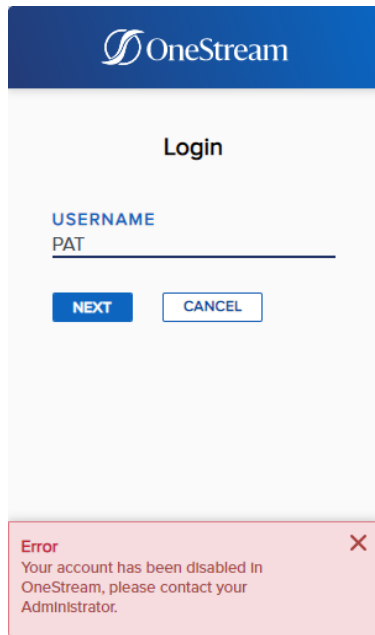


Common Errors

This section identifies how to resolve common errors you may encounter during OneStream IdentityServer and IdP configuration or at login.

Disabled Accounts

This error indicates that a user has valid IdP credentials or a token, but their user account in OneStream was manually disabled or disabled due to inactivity: Your account has been disabled in OneStream, please contact your system Administrator.

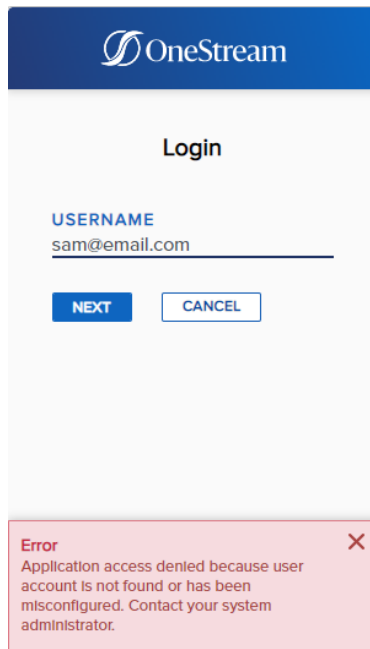


The screenshot shows the OneStream IdentityServer login interface. At the top is the OneStream logo. Below it is the title "Login". There is a label "USERNAME" above a text input field containing the text "PAT". Below the input field are two buttons: "NEXT" and "CANCEL". At the bottom of the form is a red error message box with a close button (X) in the top right corner. The error message text reads: "Error Your account has been disabled in OneStream, please contact your Administrator."

See "Managing Users" in the *Design and Reference Guide*.

User Account Does not Exist in OneStream

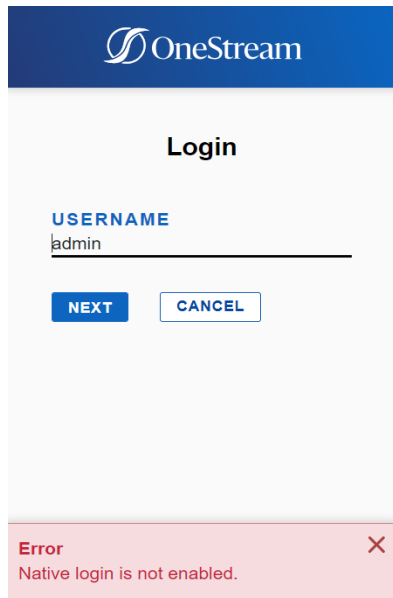
This error indicates that a corresponding user account must be created in OneStream and configured for OneStream IdentityServer: Application access denied because user account is not found or has been misconfigured. Contact your system administrator.



The screenshot shows the OneStream IdentityServer login interface. At the top is the OneStream logo. Below it is the title "Login". There is a label "USERNAME" above a text input field containing "sam@email.com". Below the input field are two buttons: "NEXT" (solid blue) and "CANCEL" (white with blue border). At the bottom of the form is a red error message box with a close button (X) in the top right corner. The error message reads: "Error Application access denied because user account is not found or has been misconfigured. Contact your system administrator."

Native Login not Enabled

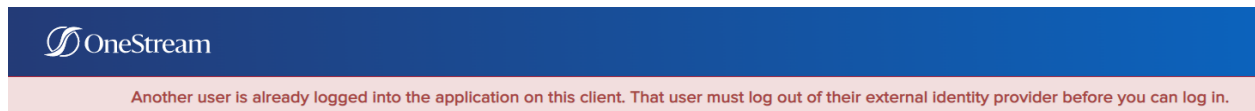
This error indicates that native login is not enabled for the user account: Native login is not enabled. To resolve this issue, submit a Support ticket requesting environment-specific support for native authentication. Environments must be initially configured for native authentication before you can use native login capabilities. Then, enable the user account for native authentication. See [How Users are Configured for Authentication](#) and [Native Authentication](#).



The screenshot shows the OneStream login interface. At the top is the OneStream logo. Below it is the title "Login". There is a "USERNAME" label and a text input field containing "admin". Below the input field are two buttons: "NEXT" and "CANCEL". At the bottom of the form, there is a red error message box with the text "Error Native login is not enabled." and a close button (X).

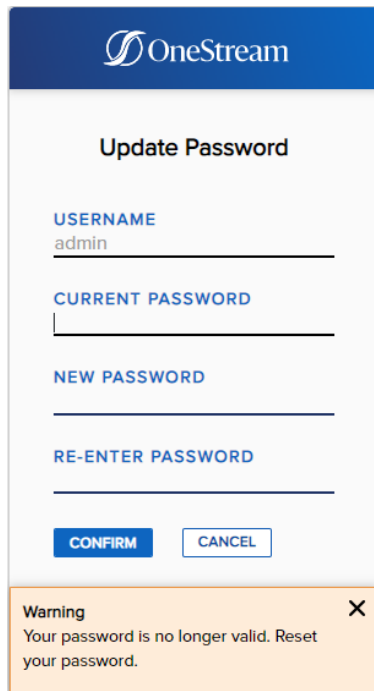
Another User is Logged In

This error indicates that a valid SSO token is being used by another user, which conflicts with the external username that you specified when logging in: Another user is already logged in the application on this client. That user must log out of their external identity provider before you can log in. To resolve this issue, the other user must log out of their IdP and clear cookies.



User Must Reset Password

This warning indicates that a password has expired or has updated security requirements: Your password is no longer valid. Reset your password. To resolve this issue, the user must reset their password.



OneStream

Update Password

USERNAME
admin

CURRENT PASSWORD

NEW PASSWORD

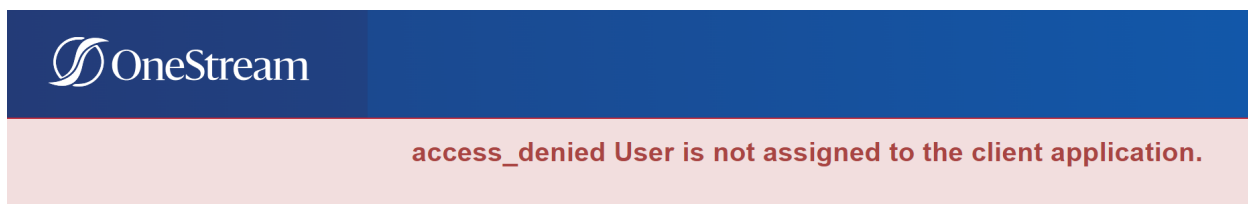
RE-ENTER PASSWORD

CONFIRM CANCEL

Warning X
Your password is no longer valid. Reset your password.

User is not Configured to the External IdP

This error indicates that the user attempting to log in with OIS is not configured to the external IdP. This error message is provided by the IdP, so it might be different for each IdP.



External IdP has an Expired Certificate

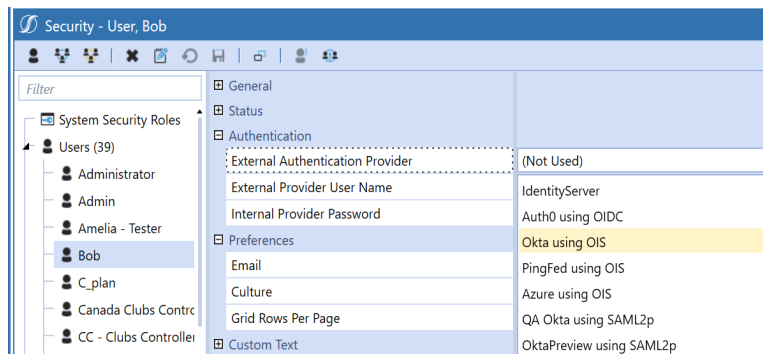
This error indicates that the encryption certificate or signing certificate for the external IdP is expired: An error has occurred with the authentication certificate(s). Please contact your System Administrator for support. To resolve this issue, upload a valid certificate for the external IdP in the Identity & Access Management Portal. See [Manage SAML 2.0 Identity Providers](#).



An error has occurred with the authentication certificate(s). Please contact your System Administrator for support.

An IdP is Unavailable in User Authentication Settings

All properly configured IdPs should be available in System Security as External Authentication Providers options, as shown below. You can customize External Authentication Provider labels to make them more intuitive. If an IdP does not display, check the configuration in the Identity & Access Management Portal. See [Identity Providers](#). Contact Support or the Cloud Operations team if needed.



Logging

During deployment, Customer Support enables logging to help diagnose configuration errors in OneStream IdentityServer. Logging is defined in the OneStream IdentityServer configuration files. These configuration items are updated by the Cloud Operations team and the Customer Support team. If you need support related to logging, contact Customer Support.

The End User Experience

How users log in and what happens when they switch applications or end a session depends on the authentication mode configured. See:

- [About Login](#).
- [Initial Login for Native Authentication](#).

- [Login Flows](#).
- [Change Applications and Log Off](#).

About Login

If you use one provider (native authentication or an external IdP), you are taken to the configured method to log in. Users with external IdPs enter their IdP username (specified in System Security as the External Provider User Name), then go to their IdP Login page on a new browser tab where they enter their username and password. For example, if you use an Okta identity provider, clicking **Logon** launches the Okta Login page. Users with native accounts enter their native account password and log in. See [Login for One External IdP](#) and [Login for OneStream IdentityServer Native Authentication](#).

If you use multiple IdPs, including native authentication with an external IdP, the Login dialog box (often called "Home Realm Discovery") displays. OneStream IdentityServer evaluates your user account authentication settings to identify your authentication mode, which determines the rest of your login with the appropriate IdP. See [Login for Multiple Authentication Methods](#).

SAML 2.0 users must re-enter their username, prefixed with their domain name if they use Active Directory Federation Services (ADFS). See [Login for SAML 2.0 and ADFS](#).

TIP: As a best practice, after you have configured an external IdP and are no longer using OneStream IdentityServer native accounts, you should submit a Support ticket to disable native authentication. See [Native Authentication](#).

Initial Login for Native Authentication

1. Navigate to the OneStream instance ClickOnce URL or launch OneStream from a previously created desktop shortcut.
2. If prompted, click **Run** to install the Windows Application.
3. On the **Login** dialog box, enter your username and click the **NEXT** button.
4. Enter your password and click the **LOG IN** button.
5. Change your password by entering your current and new passwords and clicking the **CONFIRM** button.

6. On the **Login** dialog box, enter your username and new password and click the **LOG IN** button.
7. In the OneStream application window, click the **Logon** button.
8. Select an application from the drop-down menu and click the **Open Application** button.

TIP: To save a shortcut to the application, click the **Create Windows Shortcut** icon, enter a name, and click the **OK** button.

Login Flows

See:

- [Login for One External IdP.](#)
- [Login for Multiple Authentication Methods.](#)
- [Login for the Excel Add-In.](#)
- [Login for SAML 2.0 and ADFS.](#)
- [Login for OneStream IdentityServer Native Authentication.](#)

Login for One External IdP

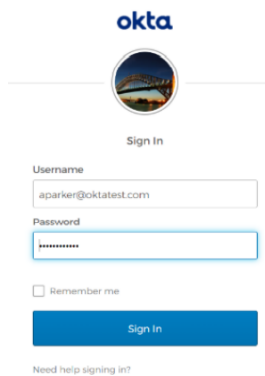
1. In **Server Address** on the **Logon** screen, specify the URL or a client connection and click the **Connect** button.

Authentication

Server Address

Application

2. Click the **Logon** button. If you already logged on and have an active login token, go to step 5 to open an application. Otherwise, you are taken to your IdP login page on a new browser tab. For example:



The image shows the Okta Sign In page. At the top is the Okta logo. Below it is a circular profile picture placeholder with the text "Sign In" underneath. The form includes a "Username" field with the value "aparker@oktatest.com", a "Password" field with masked characters, a "Remember me" checkbox, and a blue "Sign In" button. At the bottom, there is a link that says "Need help signing in?"

3. Enter your external username and password and click **Continue**.
4. **ADFS**: Enter your external username in this format <domain>\<username> and click the **Sign in** button.
5. On the OneStream Logon screen, open an application.

Login for Multiple Authentication Methods

Perform these steps if you use different IdPs or one IdP with native authentication.

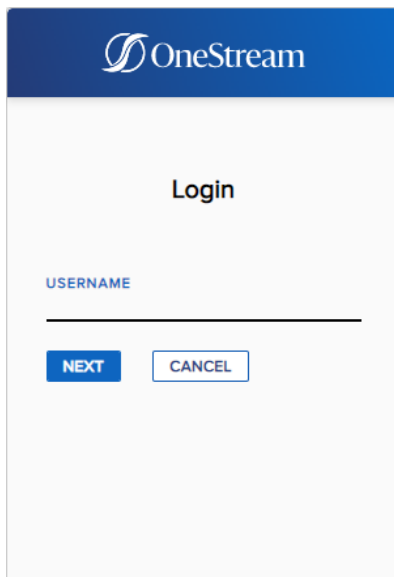
1. In **Server Address** on the **Logon** screen, specify the URL or a client connection and click the **Connect** button.

Authentication

Server Address

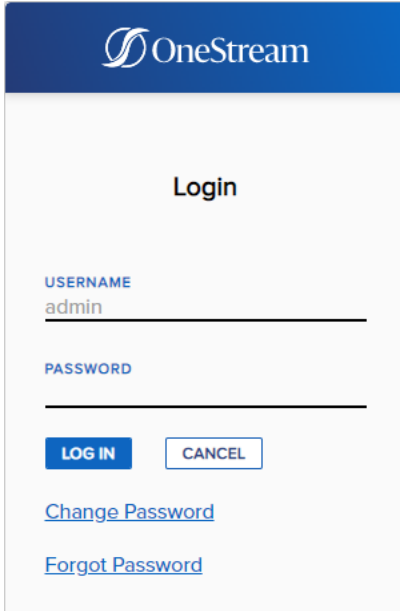
Application

2. Click **Logon**. The Login dialog box displays on a new browser tab. If the environment is configured for native authentication, you can log in with a native account.



3. Enter your username and click the **NEXT** button. Your username is evaluated to determine your authentication mode.
4. Follow the flow for the authentication mode:

- **OneStream IdentityServer Native Authentication:** Enter your native account password and click the **LOG IN** button.



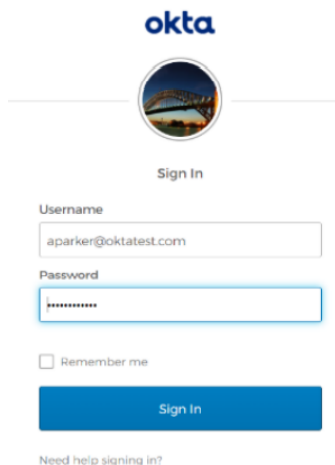
The screenshot shows the OneStream IdentityServer login interface. It features a blue header with the OneStream logo. The main content area is white and contains the following elements:

- Header:** OneStream logo.
- Title:** Login
- Username Field:** Labeled 'USERNAME', containing the text 'admin'.
- Password Field:** Labeled 'PASSWORD', currently empty.
- Buttons:** A blue 'LOG IN' button and a white 'CANCEL' button with a blue border.
- Links:** Two blue links: 'Change Password' and 'Forgot Password'.

NOTE: Click **Change Password** on the Login screen to change your password. Your username and current password are required to change your password.

NOTE: Click **Forgot Password** on the Login screen to reset your password. Your username and email address are required to reset your password. If you forgot your username, contact your administrator. This feature is only available for native authentication in OneStream IdentityServer.


- **External IdP:**
 - Enter your IdP username and click the **Next** button.
 - On the IdP login page that displays on a new tab, enter your password and click **Login** or **Sign In**. For example:



5. On the OneStream Logon screen, open an application.

Login for the Excel Add-In

The same login logic applies in Excel that is used in the Windows Application.

1. Click  **Logon**.
2. Specify a URL or client connection and connect.
3. Perform the task for your authentication flow:
 - If one IdP is configured and the token is active, you can open an application. Otherwise, log in using the IdP.
 - If multiple IdPs are configured, enter your username. If native authentication is enabled, enter your password. Otherwise, enter your IdP external username and password and sign in.
 - If you use native authentication, enter your native username and password.

Login for SAML 2.0 and ADFS

1. In **Server Address** on the **Logon** screen, specify the URL or a client connection and click the **Connect** button.
2. Click the **Logon** button. The Log In dialog box displays on a new browser tab.
3. Enter your username in SAML 2.0 and click **Next**.
4. On the IdP login page that displays on a new tab, enter your external username in SAML 2.0.
5. **For ADFS:** Enter your external username prefixed with your domain in this format: <domain>\<username>. For example, sso\jsmith.
6. Click the **Sign in** button.
7. On the OneStream Logon screen, open an application.

Login for OneStream IdentityServer Native Authentication

1. In **Server Address** on the **Logon** screen, specify the URL or a client connection and click the **Connect** button.

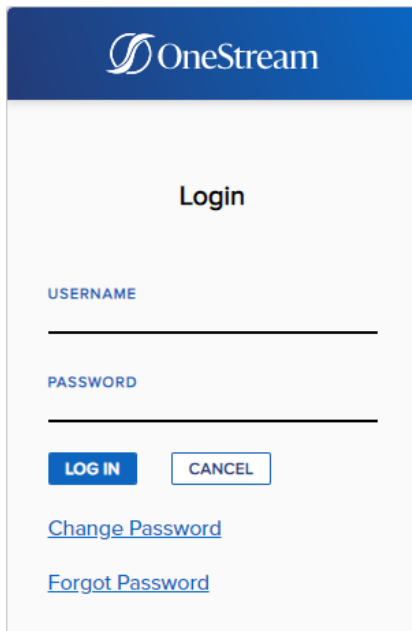
Authentication

Server Address

Application

2. Click the **Logon** button. The Login dialog box displays on a new browser tab.

3. Enter your username and password.



The screenshot shows the OneStream IdentityServer login interface. It has a blue header with the OneStream logo. Below the header, the word "Login" is centered. There are two input fields: "USERNAME" and "PASSWORD". Below the input fields are two buttons: "LOG IN" and "CANCEL". Below the buttons are two links: "Change Password" and "Forgot Password".

NOTE: Click **Change Password** on the Login screen to change your password. Your username and current password are required to change your password.


NOTE: Click **Forgot Password** on the Login screen to reset your password. Your username and email address are required to reset your password. If you forgot your username, contact your administrator. This feature is only available for native authentication in OneStream IdentityServer.

4. Click the **LOG IN** button.
5. On the OneStream Logon screen, open an application.

Change Applications and Log Off

When you change applications, your login is retained regardless of your authentication mode. You do not have to log in again.


Use either of the following options to change applications:

- Click **Logoff**  on any screen and then click the **Change Application** button.
- Select another application on the **Logon** screen and then click the **Change Application** button.

Ending a session:

- Logs you out of OneStream and disconnects you from the server.
- Does not log you out of their external IdP.

You can log back in without specifying credentials if your provider token is still valid. Use either of the following options to end a session:

- Click **Logoff**  on any screen and then click the **End Session** button.
- Click the **Logoff** button on the **Logon** page.

Identity Providers

Use the Identity & Access Management Portal to manage identity providers. This section includes requirements to manage identity providers and instructions to:

- Apply the required security role (ManageIdentityProviders).
- Access the Manage Identity Providers page.
- Add, test, view, edit, and remove OIDC and SAML 2.0 compliant identity providers.

See:

- [Requirements for Managing Identity Providers.](#)
- [Access the Manage Identity Providers Page.](#)
- [Manage OIDC Identity Providers.](#)
- [Manage SAML 2.0 Identity Providers.](#)

Requirements for Managing Identity Providers

OneStream IdentityServer Setup and System Configuration

To manage identity providers, you must:

- Work with the Cloud Operations team to configure users and environments for OneStream IdentityServer. See [Onboarding Process and Considerations](#) and [Best Practices](#).
- Have group-based access to the system security role to manage identity providers. See [Required System Security Role](#).

By default, the system configuration is enabled for the feature to manage identity providers. If you need support with the system configuration, submit a Support ticket.

Required System Security Role

You need group-based access to the ManageIdentityProviders system security role to manage identity providers. By default, the Administrators group is assigned to this role.

To assign the required role to a group, you must have the ManageSystemSecurityRoles role. To add users to an existing group, you must have the ManageSystemSecurityGroups role.

See:

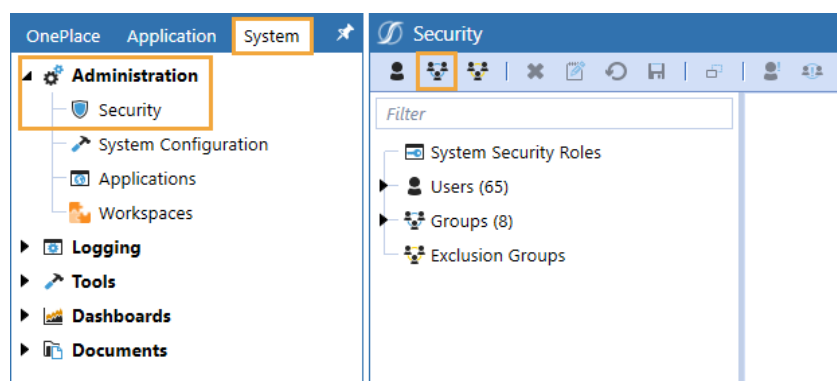
- [Apply Security Role](#).
- "Managing Users and Groups" in the *Design and Reference Guide*.

Apply Security Role

The following instructions provide an example of applying security roles. This may be configured differently depending on your security needs.

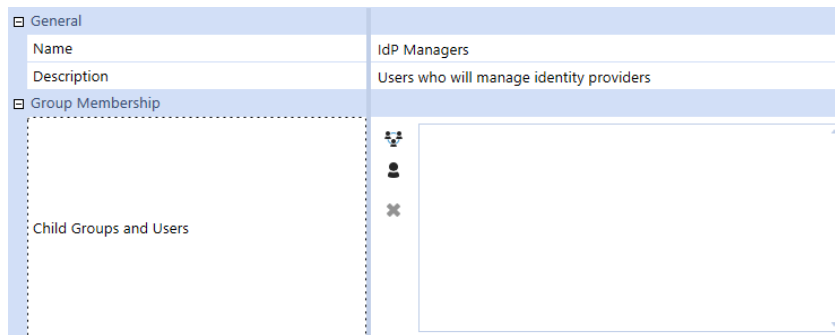
Assign the ManageIdentityProviders role to the users who will manage identity providers. Ensure the users are in the appropriate group, then assign the group to the role.

1. If one does not exist, create a group to which you will add all users who will work with identity providers. Otherwise, go to step 2.
 - a. Go to **System > Administration > Security**.
 - b. Click the **Create Group** icon.



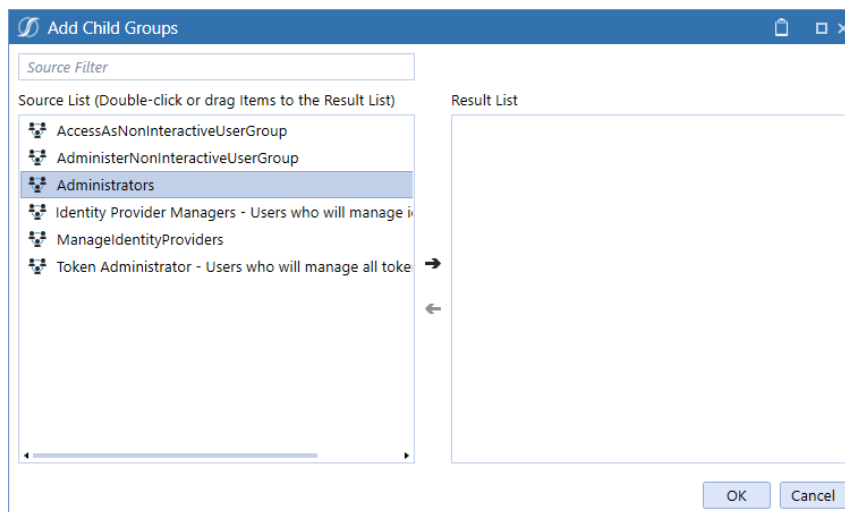
Identity Providers

- c. Enter a group name and description that reflects how users will work with identity providers. For example, use IdP Managers as the group name for users who will manage identity providers, and assign the ManageIdentityProviders role.



The screenshot shows the 'General' tab of a group configuration window. The 'Name' field contains 'IdP Managers' and the 'Description' field contains 'Users who will manage identity providers'. The 'Group Membership' tab is also visible, showing a 'Child Groups and Users' list area with icons for adding groups and users.

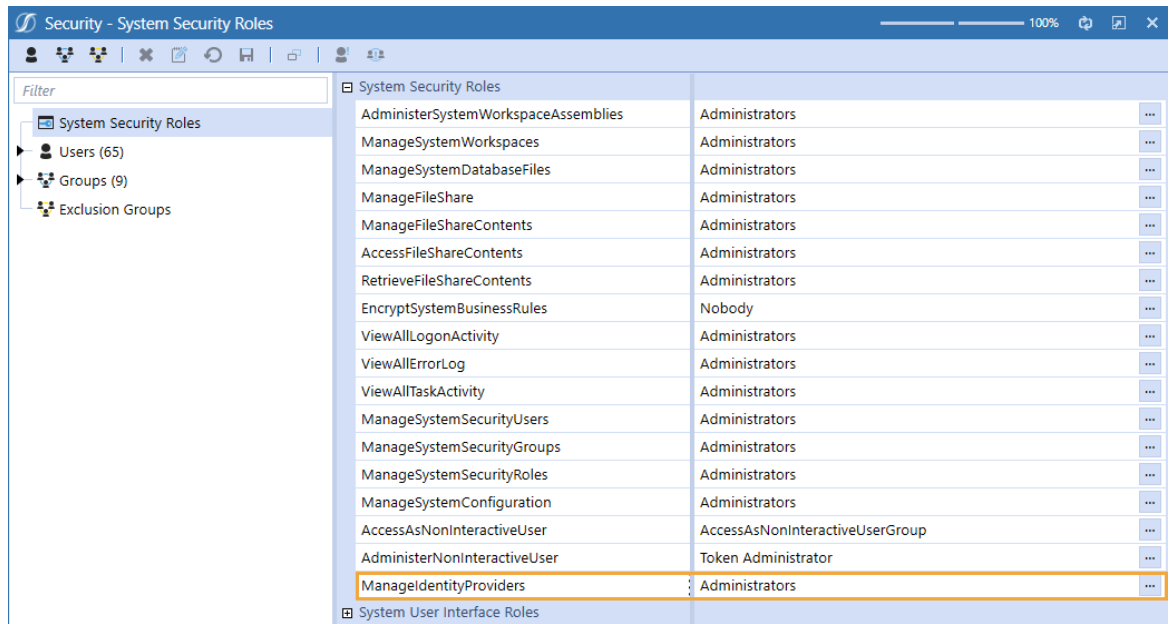
- d. In **Group Membership > Child Groups and Users**, click the **Add Child Groups** icon or the **Add Users** icon to include the users or groups of users who will manage identity providers.



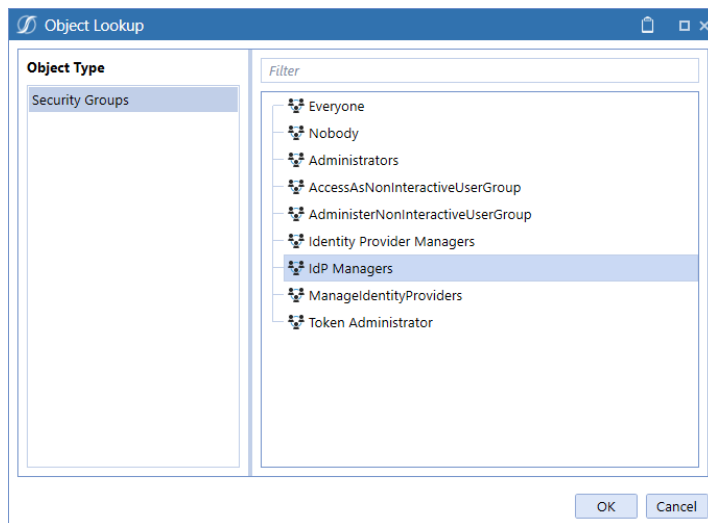
The screenshot shows the 'Add Child Groups' dialog box. It has a 'Source Filter' field at the top. Below it, there are two lists: 'Source List (Double-click or drag Items to the Result List)' and 'Result List'. The 'Source List' contains several groups, with 'Administrators' selected. There are right and left arrows between the lists. At the bottom right, there are 'OK' and 'Cancel' buttons.

- e. Click the **Save** icon.
2. Click **System Security Roles**, and then click the ellipsis next to **ManageIdentityProviders**.

Identity Providers




3. Select the group containing the users who will manage identity providers.



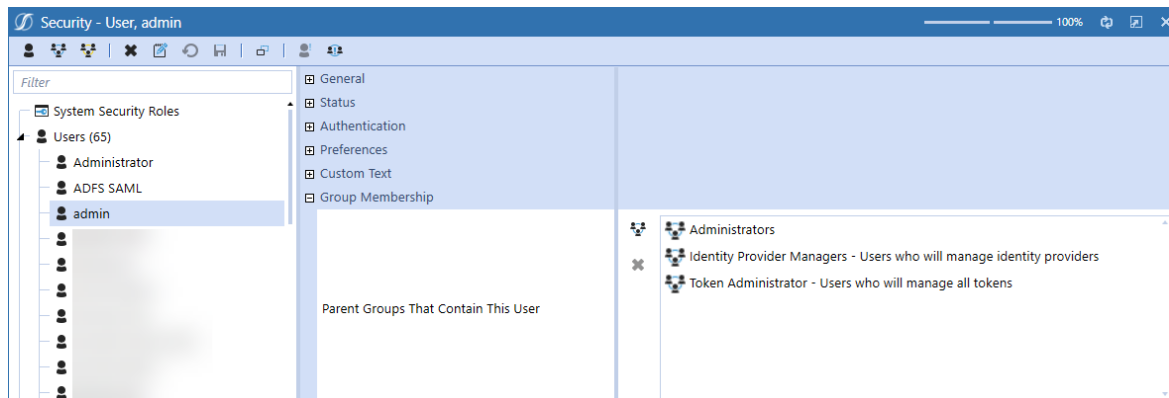
4. Click the **OK** button, then click the **Save** icon.

See "Managing Users and Groups" in the *Design and Reference Guide*.

Access the Manage Identity Providers Page

1. Log in to OneStream, following the flow for your configured IdP. See [Login Flows](#).
2. Click  **Identity Management & Access Portal**. This icon is only visible if you have a required security role.

TIP: To view your security roles, go to **System > Administration > Security > Users > <user>**. Your security groups will be listed under **Group Membership > Parent Groups That Contain This User**.



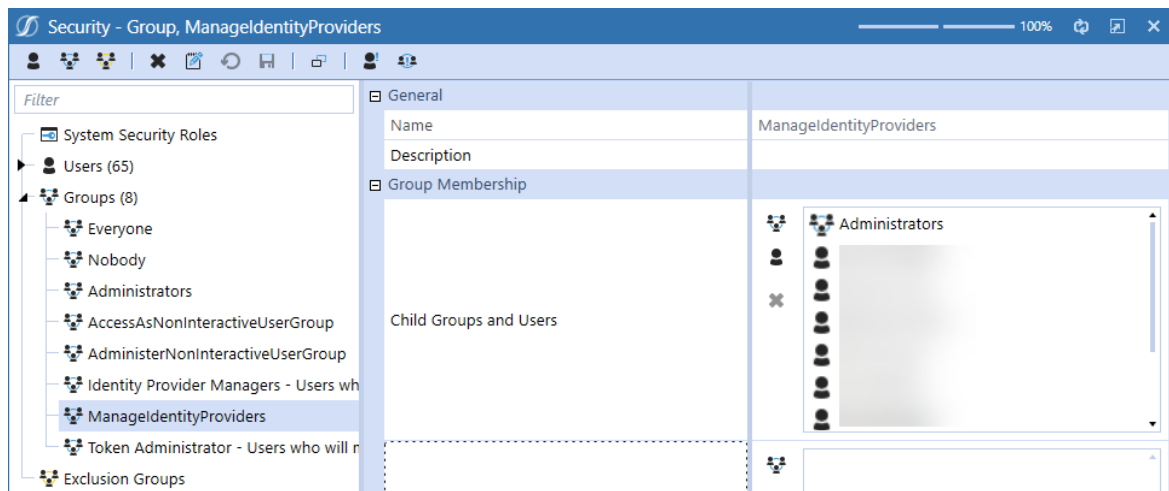
3. Click the **Manage Identity Providers** tile.



Identity Providers

This tile is only visible if you have the ManageIdentityProviders role. See [Required System Security Role](#).

TIP: To view the users and groups assigned to the ManageIdentityProviders role, go to **System > Administration > Security > Groups > ManageIdentityProviders**. The users and groups assigned to this role will be listed under **Group Membership > Child Groups and Users**.



On the Manage Identity Providers page, all identity providers are listed. Information is listed for each identity provider, including the name, type (OIDC or SAML), status (enabled or disabled), and created date. You can click the title of each column to sort the contents in alphabetical or numerical order.

Identity Providers

OneStream | Identity & Access Management

Home | **Manage Identity Providers**

[+ Add OIDC Provider](#) [+ Add SAML Provider](#)

Name ↑	Type	Status	Created On				
A test provider	OIDC	Disabled	01/10/2023	VIEW	EDIT	REMOVE	
ADFS using SAML2p	SAML	Enabled	03/31/2023	VIEW	EDIT	REMOVE	TEST
ADFS using SAML2p Auto	SAML	Enabled	01/01/0001			REMOVE	TEST
AS OKTA OIDC	OIDC	Enabled	02/07/2023	VIEW	EDIT	REMOVE	TEST
AS OKTA OIDC 2	OIDC	Enabled	02/08/2023	VIEW	EDIT	REMOVE	TEST
AzureSSO	OIDC	Enabled	09/28/2022	VIEW	EDIT	REMOVE	TEST
AzureSSO2	OIDC	Enabled	01/01/0001	VIEW	EDIT	REMOVE	TEST

K < 1 2 3 > >|

NOTE: If your environment is only configured for OIS native authentication, no identity providers will be displayed.

NOTE: The headings on the page include links to navigate through the Identity & Access Management Portal. For example, click Home to return to the Identity & Access Management Home.

To log out of the Identity & Access Management Portal:

1. Click .

2. Click **Log Out**.

Manage OIDC Identity Providers

This section includes instructions to manage OIDC identity providers.

See:

- [Add an OIDC Identity Provider](#).
- [Test an OIDC Identity Provider](#).

- [Resolve Common Issues when Testing OIDC Identity Providers.](#)
- [View Details of an OIDC Identity Provider.](#)
- [Edit an OIDC Identity Provider.](#)
- [Remove an OIDC Identity Provider.](#)
- [Appendix: Example of Identity Provider Configuration.](#)

Add an OIDC Identity Provider

1. On the **Manage Identity Providers** page, click the **Add OIDC Provider** button.
2. Complete the following fields. You can hover over the information icons ⓘ for instructions as you complete each field.
 - **Name** (required): Enter a name for the identity provider (for example, MY IDP US). This name will be displayed in the External Authentication Provider options in System > Security > Users > <user>. Each identity provider name must be unique.
 - **Scheme** (required): A scheme is automatically generated in OneStream, but you can edit it. The scheme is used in the redirect uniform resource identifier (URI) (for example, scheme: MYIDPUS; redirect URI: www.applicationname.com/federation/MYIDPUS/signin.com). Each identity provider scheme must be unique and use alphanumeric characters. The scheme cannot have spaces.

IMPORTANT: If you include special characters in the scheme, it may cause an issue in the redirect URI. Enter a scheme that is alphanumeric with no spaces.
 - **Issuer URL** (required): Enter the issuer URL, which is typically the address of the external IdP (for example, https://mycompanyname.identityprovider.com). The issuer URL is in the discovery document of the identity provider. Confirm the issuer URL with your identity provider.

The following examples show the issuer URL format for some OIDC identity providers:

Identity Providers

- **Azure AD (Microsoft Entra ID):**
<https://login.microsoftonline.com/AzureADTenantID/v2.0>
- **Okta:** <https://companyname.okta.com>
- **PingFederate:** <https://companyname.pf.com>
- **Client ID** (required): A client represents an application. Enter the client ID, which is a unique identifier for the application on the external IdP (for example, 00a73tc7yvXk93yT00rh2*****). If possible, copy and paste the client ID directly from the identity provider to ensure the value is an exact match.
- **Use PKCE** (optional): Select this option to use proof key for code exchange (PKCE) with authorization code flow. A one-time key is generated by the client to send with a request instead of the identity of a client to ensure that only the client that requested the key can redeem it. If you select this option, the Client Secret field is optional.
- **Client Secret** (required if Use PKCE is not selected): Enter the client secret from the identity provider. If possible, copy and paste the client secret directly from the identity provider to ensure the value is an exact match. A client secret is used by the client for an authorization code. A client secret is associated with a client and is sent with requests to prove the identity of a client. Characters entered in the field are masked for security.
- **Scopes** (required): Scopes identify information to be used for authentication. A scope is a request from the identity server for a group of properties about the user. Select one or more options from the list to use them as scope values.
 - **openid** (required)
 - **profile** (optional)
 - **email** (optional)
 - **address** (optional)
 - **phone** (optional)

- **Include Custom Scopes** (optional): Select this option to use a custom scope for authentication. If you select this option, enter the custom scopes in the field in a comma-separated value (CSV) format (for example, custom_profile,employee:details). Scopes in the list cannot be entered in the Custom Scopes field. Custom scopes can use letters, numbers, and special characters. Custom scopes cannot have spaces.
- **Include Custom Claims** (optional): Claims are properties about the user sent from the identity provider. Select this option to use a custom claim identifier for authentication. If you select this option, enter the custom claims in the field in a comma-separated value (CSV) format (for example, uniqueID,email). Custom claims can use letters, numbers, and special characters. Custom claims cannot have spaces. Claims are searched in the order they are entered in the field.

NOTE: The default response type for the identity provider is code. If needed, contact Customer Support to change the response type.

3. Click the **SAVE** button.
4. Click the **COPY** button to copy the redirect URI displayed in the message to configure on the external IdP.

The redirect URI is passed from OIS to the external IdP where it is saved. The external IdP verifies that the redirect URI from OIS matches its list of URIs. Then, the external IdP knows where to send the response.

5. Test the identity provider to ensure the authentication method is valid. See [Test an OIDC Identity Provider](#).

IMPORTANT: Test the identity provider configuration each time you add or edit an identity provider to ensure the authentication method is valid.

Test an OIDC Identity Provider

You can test an OIDC identity provider to ensure the authentication method is valid.

1. On the **Manage Identity Providers** page, find the identity provider to test.

NOTE: You can only test identity providers that are enabled.

Identity Providers

2. Click the **TEST** button in the row for the identity provider. If the test is successful, it will walk you through the login process. You will need to enter your credentials for the external IdP.
3. Return to the OneStream Identity Management tab in your browser to view the test results. The results indicate if the identity provider has been configured correctly, if the user profile exists in OneStream, and if the user profile is configured to this identity provider. If the test is not successful, resolve the issue. See [Resolve Common Issues when Testing OIDC Identity Providers](#). Contact Customer Support if needed.
4. Close the tab.

NOTE: After confirming the authentication method is valid, set up the authentication properties (external authentication provider and external provider user name) for each user in **System > Security > Users > <user>**. See [How Users are Configured for Authentication](#).

Resolve Common Issues when Testing OIDC Identity Providers

This section describes how errors display and how to resolve common issues that can occur when testing OIDC identity providers.

Incorrect Issuer URL

Identity Provider Test Details

Test Results

Authentication Result : Failed

- User claim : Not Found
- User claim name : Not Available
- User claim value : Not Available

IDX20804: Unable to retrieve document from: 'Http://dev-12345.octa.com/.well-known/openid-configuration'.

The test is complete. You may close this tab.

Identity Providers

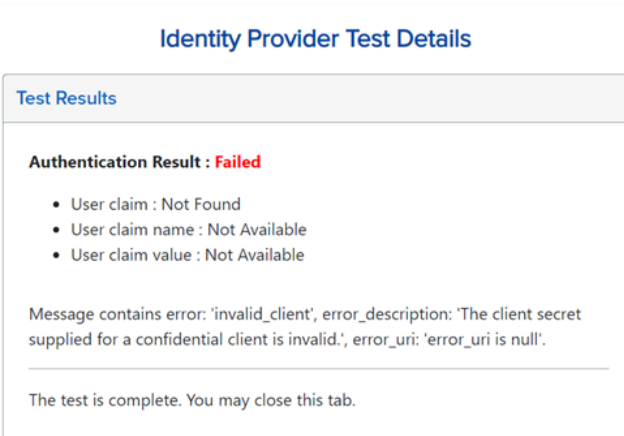
This error typically indicates that the issuer URL is set incorrectly for the identity provider. To resolve this issue, update the issuer URL in the Identity & Access Management Portal to match the issuer URL in the discovery document for the identity provider. See [Edit an OIDC Identity Provider](#).

The following examples show the issuer URL format for some OIDC identity providers:

- **Azure AD (Microsoft Entra ID):** <https://login.microsoftonline.com/AzureADTenantID/v2.0>
- **Okta:** <https://companyname.okta.com>
- **PingFederate:** <https://companyname.pf.com>

This error could also indicate a connection problem between OneStream IdentityServer and the identity provider. In some cases, the Internet Protocol (IP) address of the identity server may be blocked from accessing the identity provider.

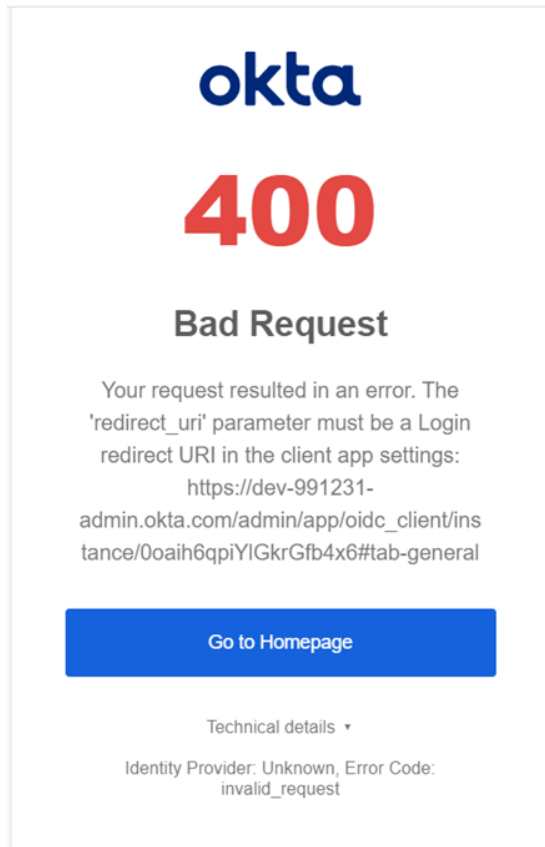
Incorrect Client Secret



The screenshot displays a window titled "Identity Provider Test Details". Inside, there is a section labeled "Test Results" with a sub-header "Authentication Result : Failed". Below this, a bulleted list shows three error details: "User claim : Not Found", "User claim name : Not Available", and "User claim value : Not Available". A message box contains the text: "Message contains error: 'invalid_client', error_description: 'The client secret supplied for a confidential client is invalid.', error_uri: 'error_uri is null'". At the bottom, a status message reads: "The test is complete. You may close this tab."

This error typically indicates that the client secret value entered in the Identity & Access Management Portal does not match what is configured on the identity provider. To resolve this issue, ensure the client secret entered in Identity & Access Management Portal matches the client secret from the identity provider. If possible, copy and paste the client secret directly from the identity provider to ensure the value is an exact match. See [Edit an OIDC Identity Provider](#).

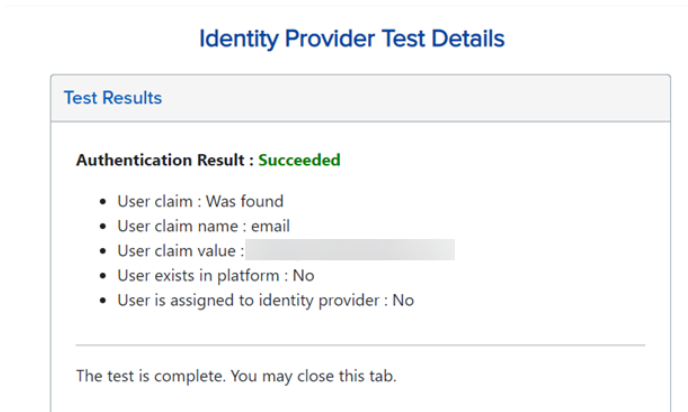
Redirect URI Not Valid



This is an example of an error that can occur when the redirect URI is not valid. Since this error comes from the identity provider, it can look different depending on which identity provider you use.

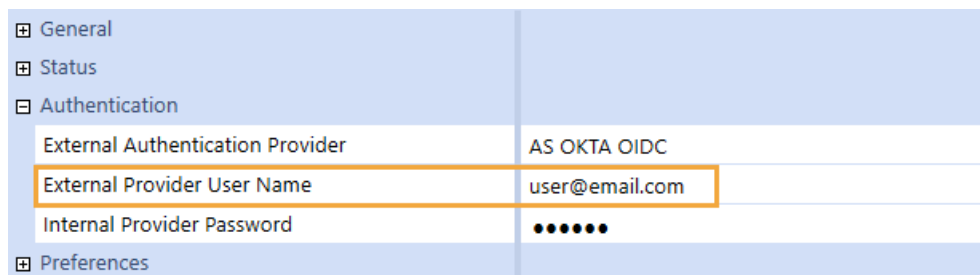
To resolve any errors related to the redirect URI, copy the redirect URI directly from the Identity & Access Management Portal when you add, view, or edit an OIDC identity provider and configure it on the external IdP. Remove any leading or trailing spaces when saving the redirect URI to the identity provider properties. See [Add an OIDC Identity Provider](#), [View Details of an OIDC Identity Provider](#), and [Edit an OIDC Identity Provider](#).

User Does not Exist in OneStream



This test result indicates that the authentication with the external identity provider was successful. However, there is no user in OneStream that matches the claim. Typically, this indicates that the user does not exist in OneStream. To resolve this issue, log in to OneStream and create the user. See [How Users are Configured for Authentication](#).

Another possibility is that the claim received from the identity provider does not match the External Provider User Name of the user in OneStream. If that is the case, either create a custom claim for the identity provider so that the correct user name is being used to look up the OneStream user (see [Edit an OIDC Identity Provider](#)) or change the External Provider User Name in the user profile in **System > Security > Users > <user>** (see [How Users are Configured for Authentication](#)).



User not Assigned to Identity Provider

Identity Provider Test Details

Test Results

Authentication Result : Succeeded

- User claim : Was found
- User claim name : email
- User claim value : [REDACTED]
- User exists in platform : Yes
- User is assigned to identity provider : No

The test is complete. You may close this tab.

This test result indicates that the authentication with the external identity provider was successful and that there is a user in OneStream that matches the claim value that was received from the identity provider. However, this user has not been assigned to the correct authentication provider in OneStream. To resolve this issue, assign the user to the correct External Authentication Provider in the user profile in **System > Security > Users > <user>**. See [How Users are Configured for Authentication](#).

General	
Status	
Authentication	
External Authentication Provider	AS OKTA OIDC
External Provider User Name	user@email.com
Internal Provider Password	••••••
Preferences	

View Details of an OIDC Identity Provider

1. On the **Manage Identity Providers** page, find the identity provider.
2. Click the **VIEW** button in the row for the identity provider.
3. You can click the **COPY** button to copy the redirect URI to configure on the external IdP. The redirect URI is passed from OIS to the external IdP where it is saved. The external IdP verifies that the redirect URI from OIS matches its list of URIs. Then, the external IdP knows where to send the response.

Identity Providers

- You can click the **EDIT** button to edit the identity provider. See [Edit an OIDC Identity Provider](#).

IMPORTANT: Editing identity provider information may affect the ability to log in for configured users.

- Click the **CANCEL** button to return to the **Manage Identity Providers** page.

Edit an OIDC Identity Provider

- On the **Manage Identity Providers** page, find the identity provider to edit.

NOTE: You cannot edit, test, or remove an identity provider if you are logged in with it.

Name	Type	Status	Created On	VIEW	EDIT	REMOVE	TEST
MY IDP US	SAML	Enabled	09/29/2023	VIEW	EDIT	REMOVE	TEST
SAML	SAML	Enabled	09/20/2023	VIEW	EDIT	REMOVE	TEST
OKTA OIDC UK	OIDC	Enabled	06/29/2023	VIEW	EDIT	REMOVE	TEST
PingFedSSO	OIDC	Enabled	06/28/2023	VIEW	EDIT	REMOVE	TEST

- Click the **EDIT** button in the row for the identity provider.

IMPORTANT: Editing identity provider information may affect the ability to log in for configured users.

- Edit the information. See [Add an OIDC Identity Provider](#).

NOTE: Select **Enable Identity Provider** to enable the identity provider. Clear the checkbox to disable the identity provider. If you disable an identity provider, it may affect the ability to log in for configured users. An identity provider cannot be disabled if a configured user is logged in with the identity provider.

NOTE: You can edit all fields except the redirect URI. The redirect URI can be copied but cannot be edited.

- Click the **SAVE** button.

Identity Providers

5. Click the **OK** button to confirm.
6. Click the **COPY** button to copy the updated redirect URI displayed in the message to configure on the external IdP. The redirect URI is passed from OIS to the external IdP where it is saved. The external IdP verifies that the redirect URI from OIS matches its list of URIs. Then, the external IdP knows where to send the response.

IMPORTANT: When changes are made to the configuration in OneStream, you must copy the updated redirect URI to configure on the external IdP.

7. Test the identity provider to ensure the authentication method is valid. See [Test an OIDC Identity Provider](#).

IMPORTANT: Test the identity provider configuration each time you add or edit an identity provider to ensure the authentication method is valid.

Remove an OIDC Identity Provider

1. On the **Manage Identity Providers** page, find the identity provider to remove.
2. Click the **REMOVE** button in the row for the identity provider.

IMPORTANT: An identity provider cannot be removed if users are configured to it. Remove the identity provider as an authentication method from any configured users before removing it.

3. Click the **OK** button to confirm. Once the identity provider is removed, it will no longer appear on the Manage Identity Providers page.

Manage SAML 2.0 Identity Providers

This section includes instructions to manage SAML 2.0 identity providers.

See:

- [Add a SAML 2.0 Identity Provider](#).
- [Test a SAML 2.0 Identity Provider](#).
- [Resolve Common Issues when Testing SAML 2.0 Identity Providers](#).

- [View Details of a SAML 2.0 Identity Provider.](#)
- [Edit a SAML 2.0 Identity Provider.](#)
- [Remove a SAML 2.0 Identity Provider.](#)

Add a SAML 2.0 Identity Provider

1. On the **Manage Identity Providers** page, click **Add SAML Provider**.
 2. Complete the following fields. You can hover over the information icons ⓘ for instructions as you complete each field.
 - **Name** (required): Enter a name for the identity provider (for example, MY IDP US). This name will be displayed in the External Authentication Provider options in System > Security > Users > <user>. Each identity provider name must be unique.
 - **Scheme** (required): A scheme is automatically generated in OneStream, but can be edited. Each identity provider scheme must be unique and should be alphanumeric with no spaces. The scheme is used in the assertion consumer service (ACS) URL and service provider entity ID URL. For example:
 - **Scheme:** MYIDPUS
 - **ACS URL:**
www.applicationname.com/OneStreamIS/federation/MYIDPUS/signin-saml
 - **Service provider entity ID URL:**
www.applicationname.com/OneStreamIS/federation/MYIDPUS/saml
- IMPORTANT:** If you include special characters in the scheme, it may cause an issue in the ACS URL and service provider entity ID URL. Enter a scheme that is alphanumeric with no spaces.
3. Select the **SAML Configuration Mode** you will use to add the identity provider:
 - **Metadata URL (recommended):** Select this option if you have a metadata URL (auto-discovery URL) from your identity provider. See [Metadata URL](#).

- **Manual Options:** If you do not have a metadata URL (auto-discovery URL) from your identity provider, select this option to upload an XML metadata file or manually complete the fields. See [Manual](#).

Metadata URL

1. Complete the following fields. You can hover over the information icons ⓘ for instructions as you complete each field.
 - **Metadata URL** (required): Enter the URL address to the identity provider metadata. This address is used to automatically retrieve identity provider metadata and configure the identity provider.
 - **Include Custom Claims** (optional): Claims are properties about the user sent from the identity provider. Select this option to use a custom claim identifier for authentication. If you select this option, enter the custom claims in the field in a comma-separated value (CSV) format (for example, uniqueID,email). Custom claims can use letters, numbers, and special characters. Custom claims cannot have spaces. Claims are searched in the order they are entered in the field.

Advanced Settings

- **Require Signed Assertion** (optional): This option indicates if assertions in an incoming sign-on response must be signed. When you select this option, the sign-on response validation will fail if the response does not contain signed assertions.
- **Require Encrypted Assertion** (optional): This option indicates if assertions in an incoming sign-on response must be encrypted. When you select this option, the sign-on response validation will fail if the response does not contain encrypted assertions. If selected, upload the certificate (a PFX file) used to encrypt assertions. Ensure the certificate is valid; an expired certificate will cause authentication to fail.
- **Encryption Certificate Password** (required if using an encryption certificate that is password protected): Enter the password for the encryption certificate. Characters entered in the field are masked for security.

Identity Providers

- **Sign Authentication Requests** (optional): When you select this option, the service provider will always sign generated requests. If selected, upload the signing certificate (a PFX file), which is used to sign generated requests. Ensure the certificate is valid; an expired certificate will cause authentication to fail.
- **Signing Certificate Password** (required if using a signing certificate that is password protected): Enter the password for the signing certificate. Characters entered in the field are masked for security.

2. Click the **SAVE** button.

IMPORTANT: After saving, you cannot edit the method to add the SAML 2.0 identity provider. To change the method, you must disable the identity provider and add a new identity provider.

NOTE: If you receive a validation error when attempting to save an IdP with a certificate, after resolving the error, you may need to upload the certificate again. For security purposes, certificates are not cached.

3. Click the **COPY** buttons to copy the ACS URL and the service provider entity ID URL displayed in the message to configure on the external IdP. Both of these values are case sensitive. So, the capitalization must match between the values configured in OneStream IdentityServer and the external identity provider.

The ACS URL directs the identity provider where to send its SAML response after authenticating a user. Some IdPs also refer to this URL as a recipient URL or destination URL. A service provider entity ID is typically a URL or URI that is assigned to the entity, and it is used to identify the entity in SAML messages and metadata. Some IdPs also refer to this URL as an audience URL.

4. Test the identity provider to ensure the authentication method is valid. See [Test a SAML 2.0 Identity Provider](#).

IMPORTANT: Test the identity provider configuration each time you add or edit an identity provider to ensure the authentication method is valid.

Manual

1. Complete the following fields. You can hover over the information icons ⓘ for instructions as you complete each field.

Either upload an XML metadata file or manually type data in the Identity Provider Entity ID, Single Sign-on Endpoint, and X509 Certificate fields.

- **Upload Metadata File** (optional): Upload an XML metadata file to automatically populate the Identity Provider Entity ID, Single Sign-on Endpoint, and X509 Certificate fields.
- **Identity Provider Entity ID** (required): Enter the entity ID from the identity provider. It is a unique identifier for the identity provider that is used to validate incoming SAML responses and assertions. It should be entered in a URI format (for example, <https://identityprovider.com/entityid>). If possible, copy and paste the identity provider entity ID directly from the identity provider to ensure the value is an exact match.
- **Single Sign-on Endpoint** (required): Enter the single sign-on endpoint from the identity provider (for example, <https://login.sso.example.com>). The single sign-on endpoint is a URL that is used by the service provider to initiate the login process. Authentication requests are sent to the single sign-on endpoint. If possible, copy and paste the single sign-on endpoint directly from the identity provider to ensure the value is an exact match.
- **X509 Certificate** (required): Enter the X509 certificate from the identity provider. It is a public key that is used to validate incoming SAML responses and assertions. If possible, copy and paste the X509 certificate directly from the identity provider to ensure the value is an exact match. Ensure the certificate is valid.
- **Include Custom Claims** (optional): Claims are properties about the user sent from the identity provider. Select this option to use a custom claim identifier for authentication. If you select this option, enter the custom claims in the field in a comma-separated value (CSV) format (for example, `uniqueID,email`). Custom claims can use letters, numbers, and special characters. Custom claims cannot have spaces. Claims are searched in the order they are entered in the field.

Advanced Settings

- **Require Signed Assertion** (optional): This option indicates if assertions in an incoming sign-on response must be signed. When you select this option, the sign-on response validation will fail if the response does not contain signed assertions.

Identity Providers

- **Require Encrypted Assertion** (optional): This option indicates if assertions in an incoming sign-on response must be encrypted. When you select this option, the sign-on response validation will fail if the response does not contain encrypted assertions. If selected, upload the certificate (a PFX file) used to encrypt assertions. Ensure the certificate is valid.
- **Encryption Certificate Password** (required if using an encryption certificate that is password protected): Enter the password for the encryption certificate. Characters entered in the field are masked for security.
- **Sign Authentication Requests** (optional): When you select this option, the service provider will always sign generated requests. If selected, upload the signing certificate (a PFX file), which is used to sign generated requests. Ensure the certificate is valid.
- **Signing Certificate Password** (required if using a signing certificate that is password protected): Enter the password for the signing certificate. Characters entered in the field are masked for security.

2. Click the **SAVE** button.

IMPORTANT: After saving, you cannot edit the method to add the SAML 2.0 identity provider. To change the method, you must disable the identity provider and add a new identity provider.

NOTE: If you receive a validation error when attempting to save an IdP with a certificate, after resolving the error, you may need to upload the certificate again. For security purposes, certificates are not cached.

3. Click the **COPY** buttons to copy the ACS URL and the service provider entity ID URL displayed in the message to configure on the external IdP. Both of these values are case sensitive. So, the capitalization has to match between the values configured in OneStream IdentityServer and the external identity provider.

The ACS URL directs the identity provider where to send its SAML response after authenticating a user. Some IdPs also refer to this URL as a recipient URL or destination URL. A service provider entity ID is typically a URL or URI that is assigned to the entity, and it is used to identify the entity in SAML messages and metadata. Some IdPs also refer to this URL as an audience URL.

4. Test the identity provider to ensure the authentication method is valid. See [Test a SAML 2.0 Identity Provider](#).

IMPORTANT: Test the identity provider configuration each time you add or edit an identity provider to ensure the authentication method is valid.

Test a SAML 2.0 Identity Provider

You can test a SAML 2.0 identity provider to ensure the authentication method is valid.

1. On the **Manage Identity Providers** page, find the identity provider to test.

NOTE: You can only test identity providers that are enabled.

2. Click the **TEST** button in the row for the identity provider. If the test is successful, it will walk you through the login process. You will need to enter your credentials for the external IdP.
3. Return to the OneStream Identity Management tab in your browser to view the test results. The results indicate if the:
 - Identity provider has been configured correctly.
 - User profile exists in OneStream.
 - User is assigned to the identity provider.
 - Authentication requests are signed.
 - Assertions are encrypted.
 - Assertions are signed.

If the test is not successful, resolve the issue. See [Resolve Common Issues when Testing SAML 2.0 Identity Providers](#). Contact Customer Support if needed.

4. Close the tab.

NOTE: After confirming the authentication method is valid, set up the authentication properties (external authentication provider and external provider user name) for each user in **System > Security > Users > <user>**. See [How Users are Configured for Authentication](#).

Resolve Common Issues when Testing SAML 2.0 Identity Providers

This section describes how errors display and how to resolve common issues that can occur when testing SAML 2.0 identity providers.

Incorrect Identity Provider Entity ID

Identity Provider Test Details

Test Results

Authentication Result : Failed

- User claim : Not Found
- User claim name : Not Available
- User claim value : Not Available

An error was encountered while handling the remote login. Invalid SAMLResponse issuer

The test is complete. You may close this tab.

This error typically indicates that the identity provider entity ID is set incorrectly for the identity provider. To resolve this issue, update the identity provider entity ID entered in the Identity & Access Management Portal to match the identity provider entity ID in the metadata file downloaded from the external identity provider. See [Edit a SAML 2.0 Identity Provider](#).

Incorrect Certificate

Identity Provider Test Details

Test Results

Authentication Result : Failed

- User claim : Not Found
- User claim name : Not Available
- User claim value : Not Available

An error was encountered while handling the remote login. Invalid SAML Request: SAML signature is valid but uses untrusted key

The test is complete. You may close this tab.

This error typically indicates that the certificate entered in the Identity & Access Management Portal does not match the certificate that is being used by the external identity provider. To resolve this issue, copy the certificate from the metadata file and paste it into the X509 Certificate field for the identity provider in the Identity & Access Management Portal to ensure the value is an exact match. See [Edit a SAML 2.0 Identity Provider](#).

Expired Certificate

Identity Provider Test Details

Test Results

Authentication Result : Failed

- User claim : Not Found
- User claim name : Not Available
- User claim value : Not Available

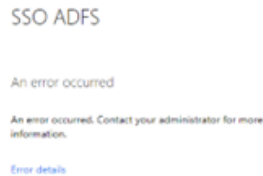
An error has occurred with the authentication certificate(s). Please contact your System Administrator for support.

The test is complete. You may close this tab.

Identity Providers

This error indicates that the encryption certificate or signing certificate in the Identity & Access Management Portal is expired. To resolve this issue, upload a valid certificate in the Identity & Access Management Portal. See [Edit a SAML 2.0 Identity Provider](#).

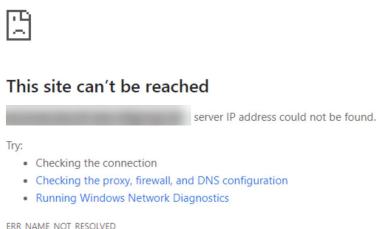
Incorrect ACS URL or Service Provider Entity ID URL



This is an example of an error that can occur if the ACS URL or the service provider entity ID URL is incorrect (for example, the capitalization is incorrect). Since this error comes from the identity provider, it can look different depending on which identity provider you use. For this type of error, more information can typically be found in the logs from the external identity provider.

To resolve any errors related to the ACS URL or the service provider entity ID URL, copy both values directly from the Identity & Access Management Portal and configure them inside the identity provider. Both of these values are case sensitive. So, the capitalization has to match between the values configured in OneStream IdentityServer and the external identity provider. Specifically, note the capitalization in the OneStreamIS part of the value. See [Add a SAML 2.0 Identity Provider](#) and [View Details of a SAML 2.0 Identity Provider](#).

Single Sign-on Endpoint Access Blocked



This is an example of an error that displays when a firewall prevents OneStream IdentityServer from accessing the single sign-on endpoint. To resolve this error, contact your IT department to ensure that OneStream IdentityServer can access this URL.

User Does not Exist in OneStream

Identity Provider Test Details

Test Results

Authentication Result : Succeeded

- User claim : Was found
- User claim name :
http://schemas.██████████/identity/claims/givenname
- User claim value : ADFS
- User exists in platform : No
- User is assigned to identity provider : No
- Authentication requests are signed : No
- Assertions are encrypted : Yes
- Assertions are signed : No

The test is complete. You may close this tab.

This test result indicates that the authentication with the external identity provider was successful. However, there is no user in OneStream that matches the claim. Typically, this indicates that the user does not exist in OneStream. To resolve this issue, log in to OneStream and create the user. See [How Users are Configured for Authentication](#).

Another possibility is that the claim received from the identity provider does not match the External Provider User Name of the user in OneStream. If that is the case, either create a custom claim for the identity provider so that the correct user name is being used to look up the OneStream user (see [Edit a SAML 2.0 Identity Provider](#)) or change the External Provider User Name in the user profile in **System > Security > Users > <user>** (see [How Users are Configured for Authentication](#)).

⊕ General	
⊕ Status	
⊖ Authentication	
External Authentication Provider	ADFS using SAML2p
External Provider User Name	user@email.com
Internal Provider Password	••••••
⊕ Preferences	

User not Assigned to Identity Provider

Identity Provider Test Details

Test Results

Authentication Result : Succeeded

- User claim : Was found
- User claim name :
http://schemas. /identity/claims/givenname
- User claim value : ADFS
- User exists in platform : Yes
- User is assigned to identity provider : No
- Authentication requests are signed : No
- Assertions are encrypted : Yes
- Assertions are signed : No

The test is complete. You may close this tab.

This test result indicates that the authentication with the external identity provider was successful and that there is a user in OneStream that matches the claim value that was received from the identity provider. However, this user has not been assigned to the correct authentication provider in OneStream. To resolve this issue, assign the user to the correct External Authentication Provider in the user profile in **System > Security > Users > <user>**. See [How Users are Configured for Authentication](#).

⊕ General	
⊕ Status	
⊖ Authentication	
External Authentication Provider	ADFS using SAML2p
External Provider User Name	user@email.com
Internal Provider Password	●●●●●●
⊕ Preferences	

View Details of a SAML 2.0 Identity Provider

1. On the **Manage Identity Providers** page, find the identity provider.
2. Click the **VIEW** button in the row for the identity provider.
3. You can click the **COPY** button to copy the ACS URL and service provider entity ID URL to configure on the external IdP.

The ACS URL directs the identity provider where to send its SAML response after authenticating a user. Some IdPs also refer to this URL as a recipient URL or destination URL. A service provider entity ID is typically a URL or URI that is assigned to the entity, and it is used to identify the entity in SAML messages and metadata. Some IdPs also refer to this URL as an audience URL.

4. You can click the **EDIT** button to edit the identity provider. See [Edit a SAML 2.0 Identity Provider](#).

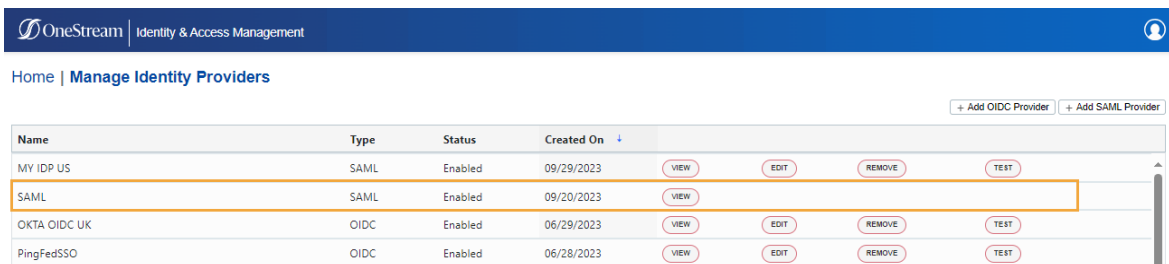
IMPORTANT: Editing identity provider information may affect the ability to log in for configured users.

5. Click the **CANCEL** button to return to the **Manage Identity Providers** page.

Edit a SAML 2.0 Identity Provider

1. On the **Manage Identity Providers** page, find the identity provider to edit.

NOTE: You cannot edit, test, or remove an identity provider if you are logged in with it.



OneStream | Identity & Access Management

Home | Manage Identity Providers

+ Add OIDC Provider + Add SAML Provider

Name	Type	Status	Created On	VIEW	EDIT	REMOVE	TEST
MY IDP US	SAML	Enabled	09/29/2023	VIEW	EDIT	REMOVE	TEST
SAML	SAML	Enabled	09/20/2023	VIEW	EDIT	REMOVE	TEST
OKTA OIDC UK	OIDC	Enabled	06/29/2023	VIEW	EDIT	REMOVE	TEST
PingFedSSO	OIDC	Enabled	06/28/2023	VIEW	EDIT	REMOVE	TEST

2. Click the **EDIT** button in the row for the identity provider.

Identity Providers

IMPORTANT: Editing identity provider information may affect the ability to log in for configured users.

3. Edit the information. See [Add a SAML 2.0 Identity Provider](#).

NOTE: Select **Enable Identity Provider** to enable the identity provider. Clear the checkbox to disable the identity provider. If you disable an identity provider, it may affect the ability to log in for configured users. An identity provider cannot be disabled if a configured user is logged in with the identity provider.

NOTE: You can edit all fields except the SAML Configuration Mode, ACS URL, and service provider entity ID URL. These fields can be copied but cannot be edited.

4. Click the **SAVE** button.

NOTE: If you receive a validation error when attempting to save an IdP with a certificate, after resolving the error, you may need to upload the certificate again. For security purposes, certificates are not cached.

5. Click the **OK** button to confirm.
6. Click the **COPY** buttons to copy the updated ACS URL and service provider entity ID URL displayed in the message to configure on the external IdP. Both of these values are case sensitive. So, the capitalization has to match between the values configured in OneStream IdentityServer and the external identity provider.

The ACS URL directs the identity provider where to send its SAML response after authenticating a user. Some IdPs also refer to this URL as a recipient URL or destination URL. A service provider entity ID is typically a URL or URI that is assigned to the entity, and it is used to identify the entity in SAML messages and metadata. Some IdPs also refer to this URL as an audience URL.

IMPORTANT: When changes are made to the configuration in OneStream, you must copy the updated ACS URL and service provider entity ID URL to configure on the external IdP.

7. Test the identity provider to ensure the authentication method is valid. See [Test a SAML 2.0 Identity Provider](#).

IMPORTANT: Test the identity provider configuration each time you add or edit an identity provider to ensure the authentication method is valid.

Remove a SAML 2.0 Identity Provider

1. On the **Manage Identity Providers** page, find the identity provider to remove.
2. Click the **REMOVE** button in the row for the identity provider.

IMPORTANT: An identity provider cannot be removed if users are configured to it. Remove the identity provider as an authentication method from any configured users before removing it.

3. Click the **OK** button to confirm. Once the identity provider is removed, it will no longer appear on the Manage Identity Providers page.

Personal Access Tokens

OneStream IdentityServer supports personal access tokens (PATs) for non-interactive authentication in REST API calls. Before OneStream IdentityServer, you had to issue a web request to your IdP to get a token that you included in API calls. This request is no longer necessary; use the PAT in place of that token.

NOTE: You cannot use JSON Web Tokens for non-interactive authentication in REST API calls with OneStream IdentityServer. Only reference tokens are supported.

Use the Identity & Access Management Portal to quickly generate a PAT identifier string for seamless authentication in REST API calls to:

- Schedule jobs.
- Perform batch processing.
- Use data connectors that support PATs.

A PAT takes on the identity and access rights of the creating user.

When you create a PAT in the Identity & Access Management Portal, the OneStream IdentityServer generates a unique identifier string, such as the following, that you can use in REST API calls.

```
664968BF50F90638D396A4C61075218CC135627101870E974623E9F8827D6A58-1
```

Copy and securely store these identifier strings as you would other sensitive credentials, possibly in a key vault. If you do not copy or you lose a PAT identifier string, revoke the PAT and create a new one. System security roles determine the tasks you can perform with PATs.

See:

- [Default Settings.](#)
- [Requirements for Using Personal Access Tokens.](#)
- [Access the Manage Personal Access Tokens Page.](#)

- [Manage Personal Access Tokens](#).
- [About Using Personal Access Tokens in APIs](#).

Default Settings

Each user can have 100 active PATs, which expire 365 days from creation. You cannot manually extend the default PAT lifetime or specify the number of active PATs that users can have. Contact OneStream Cloud Operations or Customer Support to change these defaults. The maximum lifetime that can be set for a PAT is 3650 days (10 years).

Requirements for Using Personal Access Tokens

OneStream IdentityServer and Environment Setup

To use PATs, you must:

- Work with the Cloud Operations team to configure users and environments for OneStream IdentityServer. See [Onboarding Process and Considerations](#) and [Best Practices](#).
- Have group-based access to the system security roles that determine the tasks you can perform with PATs. See [Required System Security Roles](#).

Required System Security Roles

Even if you are an administrator, you need group-based access to one or both of these required system security roles to create, manage, and use PATs in API calls:

- **AccessAsNonInteractiveUser**: Enables a user to:
 - Create PATs for their own use in API calls.
 - Revoke their own PATs.
 - Access details about their own PATs.

Personal Access Tokens

- **AdministerNonInteractiveUser:** Enables a user to revoke another user's PATs and access information about all PATs.

You do not need to be in the administrator group to be assigned either of these roles.

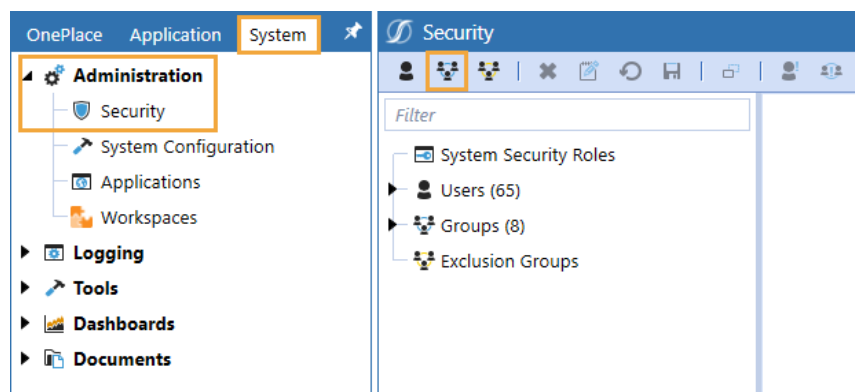
By default, the Nobody group that does not include administrators is assigned to both of these roles. To assign the required roles, you must have the `ManageSystemSecurityRoles` role. To add users to an existing group, you must have the `ManageSystemSecurityGroups` role. See:

- [Apply Security Roles](#).
- "Managing Users and Groups" in the *Design and Reference Guide*.

Apply Security Roles

The following instructions provide an example of applying security roles. This may be configured differently depending on your security needs.

1. If one does not exist, create a group to which you add all users who will work with PATs. Otherwise, go to step 2.
 - a. Go to **System > Administration > Security**.
 - b. Click the **Create Group** icon.



- c. Enter a group name and description that reflects how users will work with PATs. For example, use PATs Users as the group name for users who will create and revoke their own PATs, and assign the `AccessAsNonInteractiveUser` role.

Personal Access Tokens

The screenshot shows the configuration page for a group named 'PATs Users'. The 'General' tab is active, showing the group name and description. The 'Group Membership' tab is also visible, showing a list of child groups and users, which is currently empty. The 'Name' field contains 'PATs Users' and the 'Description' field contains 'Users who will create and revoke their own tokens'.

General	
Name	PATs Users
Description	Users who will create and revoke their own tokens

Group Membership

Child Groups and Users

Similarly, create a PATs Admin group for users who must access all PAT details and be able to revoke all PATs and assign the `AdministerNonInteractiveUser` role.

The screenshot shows the configuration page for a group named 'PATs Admin'. The 'General' tab is active, showing the group name and description. The 'Group Membership' tab is also visible, showing a list of child groups and users, which is currently empty. The 'Name' field contains 'PATs Admin' and the 'Description' field contains 'Users who access all PAT details and can revoke all PATs'.

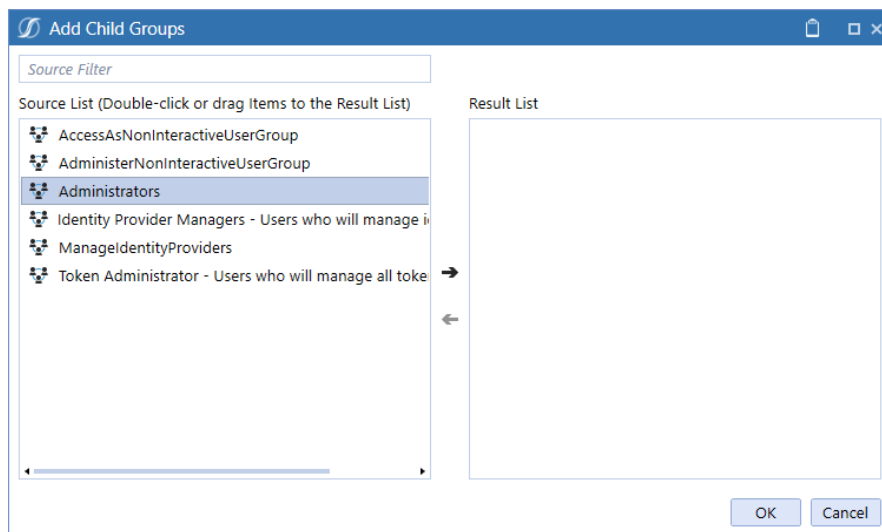
General	
Name	PATs Admin
Description	Users who access all PAT details and can revoke all PATs

Group Membership

Child Groups and Users

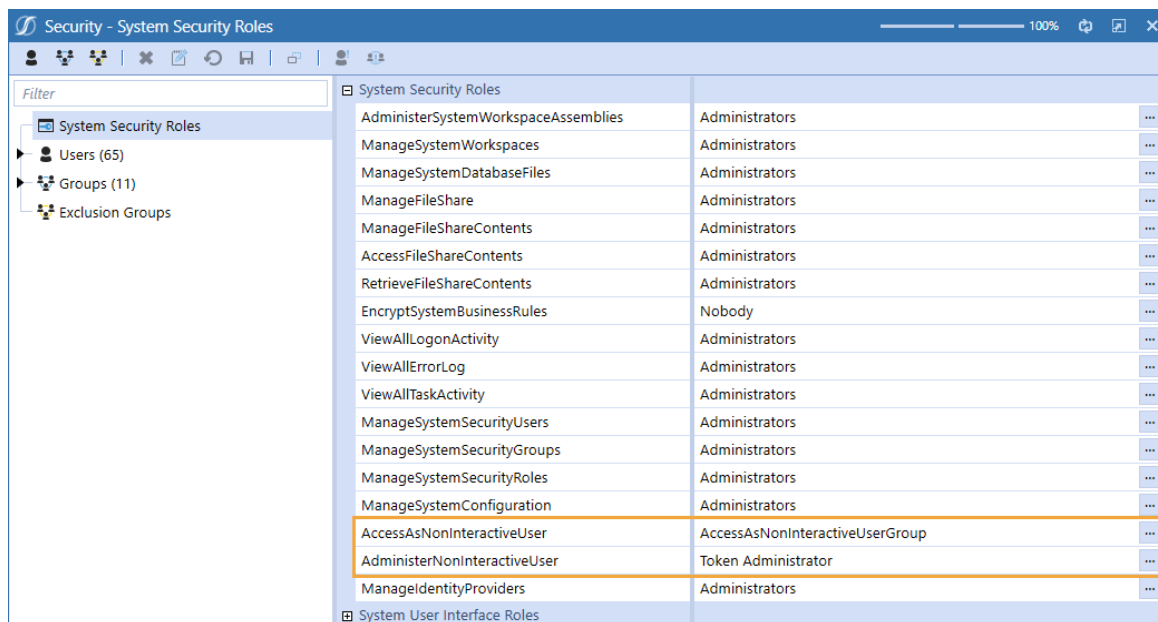
- d. In **Group Membership**, click the **Add Child Groups** icon or the **Add Users** icon to include the users or groups of users who will use PATs.

Personal Access Tokens



e. Click the **Save** icon.

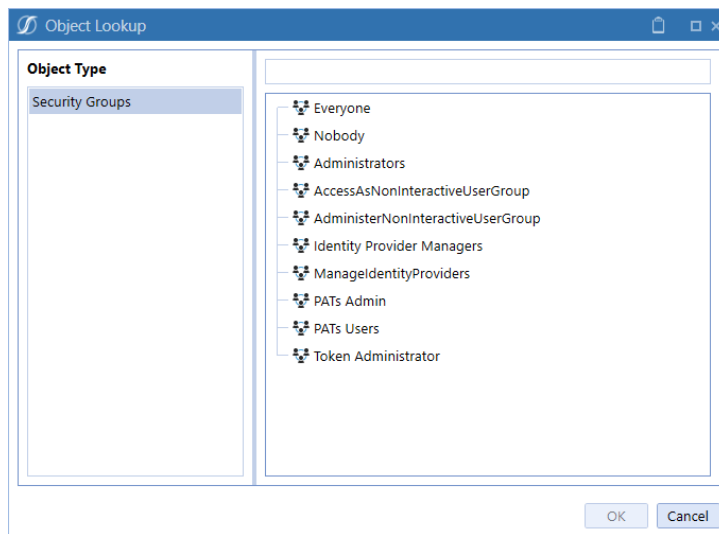
2. Click **System Security Roles**, and then click the ellipsis next to **AccessAsNonInteractiveUser** or **AdministerNonInteractiveUser**.



Personal Access Tokens

IMPORTANT: The **AccessAsNonInteractiveUser** role enables a user to create PATs for their own use in API calls, revoke their own PATs, and access details about their own PATs. The **AdministerNonInteractiveUser** role enables a user to revoke another user's PATs and access information about all PATs.


3. Select the group containing the users who will work with PATs.



4. Click the **OK** button, then the **Save** icon.

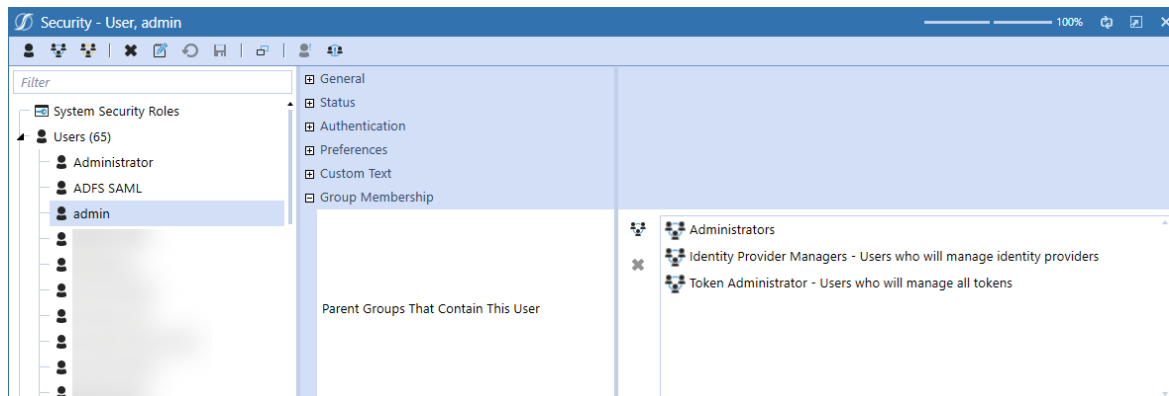
See "Managing Users and Groups" in the *Design and Reference Guide*.

Access the Manage Personal Access Tokens Page

1. Log in to OneStream, following the flow for your configured IdP. See [Login Flows](#).
2. Click  **Identity & Access Management Portal**. This icon is only visible if you have a required security role.

Personal Access Tokens

TIP: To view your security roles, go to **System > Administration > Security > Users > <user>**. Your security groups will be listed under **Group Membership > Parent Groups That Contain This User**.



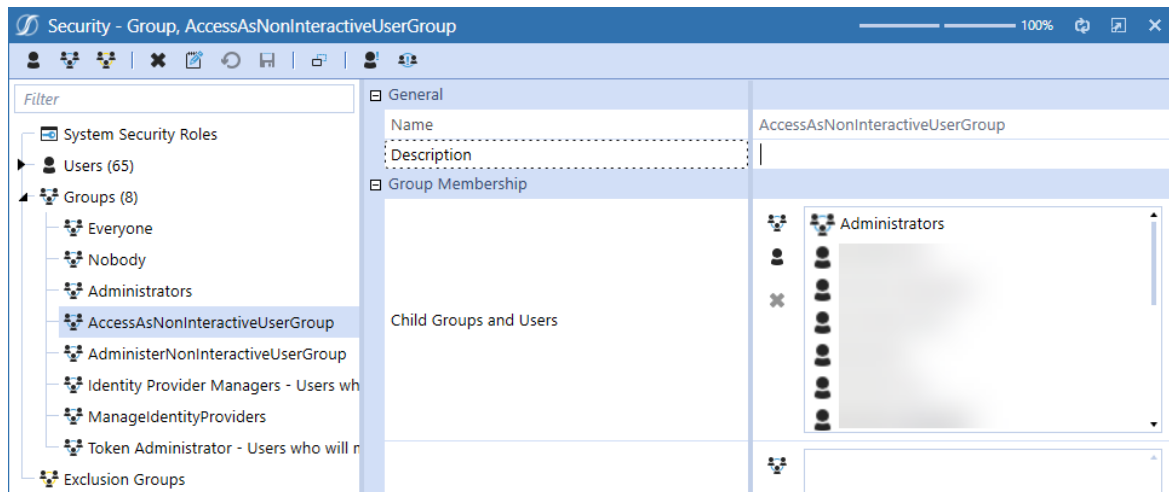
3. Click the **Manage Personal Access Tokens** tile.



This tile is only visible if you have the `AccessAsNonInteractiveUser` or `AdministerNonInteractiveUser` security role.

Personal Access Tokens

TIP: To view the users and groups assigned to these roles, go to **System > Administration > Security > Groups**. Select either **AccessAsNonInteractiveUserGroup** or **AdministerNonInteractiveUserGroup**. The users and groups assigned to the selected role will be listed under **Group Membership > Child Groups and Users**.



On the Manage Personal Access Tokens page, all PATs are listed. If you have the AccessAsNonInteractiveUser security role, you can access only information about your PATs. If you have the AdministerNonInteractiveUser security role, you can access information about all user PATs. See [Required System Security Roles](#). To see only your PATs, click the **View My Tokens** button. To return to the full list, click the **View All Tokens** button.

Information is listed for each PAT, including the username and status of the owner and the token status, expiration and created dates, and description.

The Token Status column indicates whether a PAT is Active, Revoked, or Expired. If the column displays Auto-revoked, it indicates that the PAT was expired and then automatically revoked when it was attempted to be used.

You can click on the title of each column to sort the contents in alphabetical or numerical order.

Personal Access Tokens

OneStream | Identity & Access Management

Home | **Manage Personal Access Tokens**

All Users View My Tokens + Create Token

Username	User Status	Token ID	Token ...	Days T...	Expiration	Created	Description
admin	Enabled	F661-1	REVOKE Active	6	06/08/2023	06/08/2022	
admin	Enabled	84C1-1	REVOKE Active	7	06/09/2023	06/09/2022	
admin	Enabled	65CE-1	REVOKE Active	28	06/30/2023	06/30/2022	
admin	Enabled	9335-1	REVOKE Active	42	07/14/2023	07/14/2022	
admin	Enabled	4640-1	REVOKE Active	42	07/14/2023	07/14/2022	
admin	Enabled	0301-1	REVOKE Active	42	07/14/2023	07/14/2022	
admin	Enabled	FD79-1	REVOKE Active	147	10/27/2023	10/27/2022	
admin	Enabled	79CB-1	REVOKE Active	147	10/27/2023	10/27/2022	Test 10.27.22

1 2 3 4 5 > >>

NOTE: The headings on the page include links to navigate through the Identity & Access Management Portal. For example, click Home to return to the Identity & Access Management Home.

To log out of the Identity & Access Management Portal:

1. Click .

2. Click **Log Out**.

Manage Personal Access Tokens

This section includes instructions to manage personal access tokens.

See:

- [Create a Personal Access Token](#).
- [Revoke a Personal Access Token](#).

Create a Personal Access Token

1. On the **Manage Personal Access Tokens** page, click the **Create Token** button.
2. Enter a description, which is optional, and click the **CREATE TOKEN** button.
3. Click the **COPY** button to copy the PAT to the clipboard so you can paste it into API call code.

IMPORTANT: Do not leave the page without copying the PAT. After you leave this page, you will not be able copy it again. Securely store the PAT the same way you would other sensitive credentials. If you do not copy the PAT or lose the PAT, revoke the PAT and have a new one issued.

4. Click the **BACK TO TOKENS** button.

See [About Using Personal Access Tokens in APIs](#).

Revoke a Personal Access Token

If you did not copy a PAT or lost a PAT, revoke it and create a new PAT.

If you try to use an expired PAT, it will be revoked automatically.

You cannot re-enable a revoked PAT. If you have the `AccessAsNonInteractiveUser` security role, you can revoke your own PATs. If you have the `AdministerNonInteractiveUser` security role, you can revoke the PATs of other users. See [Required System Security Roles](#).

1. On the **Manage Personal Access Tokens** page, find the PAT to revoke.
2. Click the **REVOKE** button in the row for the PAT to revoke.
3. Click the **YES, REVOKE TOKEN** button to confirm.

About Using Personal Access Tokens in APIs

With OneStream IdentityServer you can use PAT identifiers as strings in API authentication headers, reducing the amount of code required. Reference PAT identifiers stored in a file or key vault, or define global variables.

See:

- [Best Practices](#).
- [Authentication Header Updates](#).
- [API Call Comparison](#).

For information about OneStream APIs, see:

- The *API Overview Guide*.
- The *REST API Implementation Guide*.

Best Practices

While you can paste copied PAT identifiers in API scripts, we suggest you more securely reference them systematically to retrieve them from an external storage source such as file repository or key vault.

To avoid authentication errors, work as needed with an administrator to ensure that:

- Your user account is active in OneStream. Verify account status by clicking **System > Security > Users > <user>** and ensuring **Is Enabled** is **True**.
- You have not exceeded your log on inactivity threshold. See "Managing Users" in the *Design and Reference Guide*.
- You have group-based access to the `AccessAsNonInteractiveUser` security role. See [Required System Security Roles](#).
- Your PAT is not legacy, IdP-based. Use only PATs generated in the Identity & Access Management Portal.
- You use the complete PAT identifier string.
- A PAT did not expire and was not revoked.

Authentication Header Updates

In 7.0 legacy API calls, update authentication strings as the following to replace `clientId`, usernames, and passwords with a unique PAT identifier string.

For example, insert the following to reference a PAT identifier stored in an Azure key vault:

```
$token = Get-AzKeyVaultSecret -VaultName '<name>' -Name 'PATAdmin' -AsPlainText
```

Personal Access Tokens

While not recommended for security reasons, you could also replace the code below:

```
Get Authentication Token Dim authToken As String = GetClientCredentials AuthToken0S(si, methodType,
authorizationURL, clientId, ClientSecret, grantType, scope) ErrorHandler.LogMessage(si, authToken)
```

with a copied PAT identifier that you paste into the string:

```
Get Authentication Token Dim authToken As String = "<PAT identifier>" ErrorHandler.LogMessage
si,authToken)
```

Then save and run scripts against APIs.

API Call Comparison

To illustrate release-specific differences in portions of API call scripts, this section compares the same ExecuteSequence API call.

Legacy

The first 20 lines of code below request a token from an external IdP. The remaining lines use the returned token to authenticate and run a business rule to export data.

```
2 $clientId="myclientid"
3 $clientsecret="myclientsecret"
4 $clientcreds = [System.Text.Encoding]::UTF8.GetBytes("${clientId}:${clientsecret}");
5
6 $Header = @{ Authorization = "Basic $([System.Convert]::ToBase64String($clientcreds))"
7             Accept = "application/json" }
8 $body = "grant_type=client_credentials&scope=OneStreamXF"
9 $uri = "https://[redacted].com/oauth2/auspq8fsjcv51XQNT0h7/v1/token"
10 $type = "application/x-www-form-urlencoded"
11
12 $result = Invoke-WebRequest -ContentType $type -Method 'Post' -Uri $uri -Headers $header -Body $body
13 if ($result.StatusCode -ne 200)
14 {
15     Write-Warning "Couldn't get JWT"
16     $result
17 }
18 else
19 {
20     $jwt = (ConvertFrom-Json $result.Content).access_token
21 }
22
23 #Use the token in an API call. In this case we are calling ExecuteSequence in order to run a business rule to export some data.
24 $header = @{ Authorization = "Bearer $jwt" }
25 $body = "BaseWebServerUrl=https://[redacted].com/onestreamweb&ApplicationName=GolfStream&SequenceName=Export Stage Archives"
26 $uri = "https://[redacted].com/OneStreamApi/api/DataManagement/ExecuteSequence?api-version=5.2.0"
27
28 Invoke-WebRequest -ContentType $type -Method 'Post' -Uri $uri -Headers $header -Body $body
```

Current

Referencing a PAT generated in the Identity & Access Management Portal significantly reduces the code required. The following code references a PAT identifier from a key vault:

Personal Access Tokens

```
1 #Get the Personal Access Token. There is no programmatic way of generating a new token so an existing token must be used.
2
3 #The token can be specified directly in the script, but this is not recommended for security reasons.
4 #Its recommended to get the token from an external source, for example a text file or an Azure Key Vault
5 $Token = '[Your token]'
6
7 #Use the token in an API call. In this case we are calling ExecuteSequence in order to run a business rule to export some data.
8 $header = @{ Authorization = "Bearer $Token"}
9 $body = @"
10 {
11     "BaseWebServerUrl":"https:[Your Onestream domain]/onestreamweb",
12     "ApplicationName":"[Your Application Name]",
13     "SequenceName":"[Your Sequence Name]"
14 }
15 "@
16
17 $uri = "https://[Your Onestream domain]/OneStreamApi/api/DataManagement/ExecuteSequence?api-version=5.2.0"
18 $type = "application/json"
19 Invoke-WebRequest -ContentType $type -Method 'Post' -Uri $uri -Headers $header -Body $body
```

Appendix: Example of Identity Provider Configuration

This appendix includes an example of how to configure an Okta OIDC identity provider for OneStream IdentityServer (OIS). Depending on the identity provider and version, the steps you need to complete might be different.

To manage identity providers, you must:

- Work with the Cloud Operations team to configure users and environments for OneStream IdentityServer. See [Onboarding Process and Considerations](#) and [Best Practices](#).
- Have group-based access to the system security role to manage identity providers. See [Required System Security Role](#).

By default, the system configuration is enabled for the feature to manage identity providers. If you need support with the system configuration, submit a Support ticket.

Okta OIDC Identity Provider

The following sections show how to create an Okta application and copy the redirect URI from the OneStream Identity & Access Management Portal and paste it in the Okta application.

Create an Okta Application

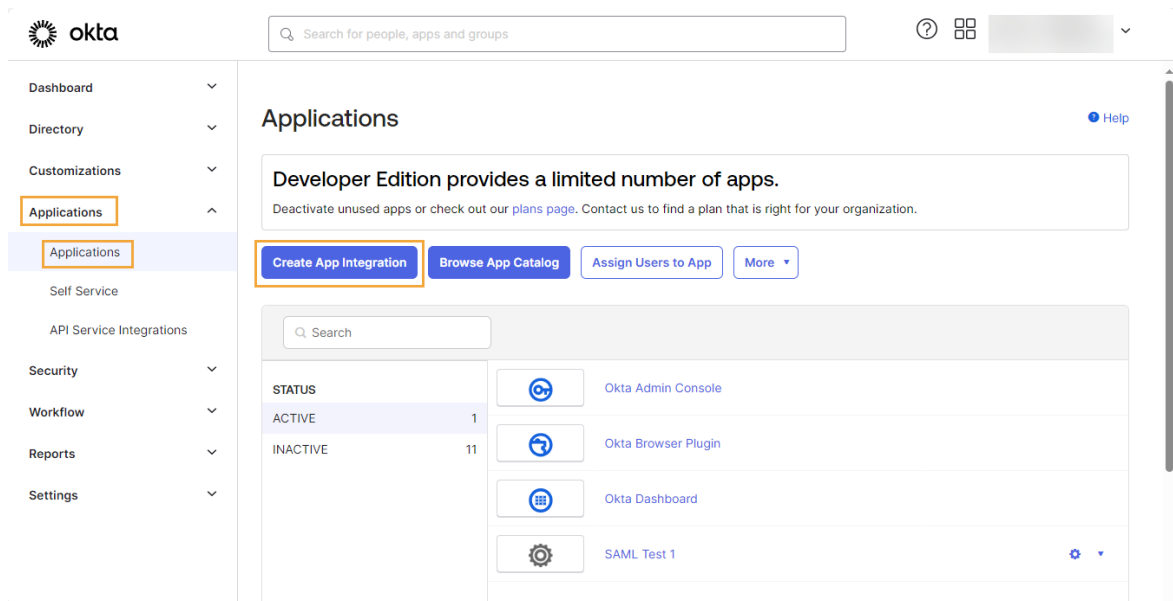
As you complete the steps in this section, you will copy the following information and paste it in the Identity & Access Management Portal:

- Okta server URL
- App integration name
- Client ID
- Client secret

See [Add an OIDC Identity Provider](#).

Appendix: Example of Identity Provider Configuration

1. Copy the Okta server URL (for example: <https://companyname.okta.com>). Paste this URL in the Identity & Access Management Portal in the **Issuer URL** field.
2. Sign in to Okta and go to **Applications > Applications**.
3. Click the **Create App Integration** button.



4. A **Create a new app integration** dialog box displays.
 - a. For **Sign-in method**, select **OIDC - OpenID Connect**.
 - b. For **Application type**, select **Web Application**.

Appendix: Example of Identity Provider Configuration

×

Create a new app integration

Sign-in method
[Learn More](#)

- OIDC - OpenID Connect**
Token-based OAuth 2.0 authentication for Single Sign-On (SSO) through API endpoints. Recommended if you intend to build a custom app integration with the Okta Sign-In Widget.
- SAML 2.0**
XML-based open standard for SSO. Use if the Identity Provider for your application only supports SAML.
- SWA - Secure Web Authentication**
Okta-specific SSO method. Use if your application doesn't support OIDC or SAML.
- API Services**
Interact with Okta APIs using the scoped OAuth 2.0 access tokens for machine-to-machine authentication.

Application type
What kind of application are you trying to integrate with Okta?

Specifying an application type customizes your experience and provides the best configuration, SDK, and sample recommendations.

- Web Application**
Server-side applications where authentication and tokens are handled on the server (for example, Go, Java, ASP.Net, Node.js, PHP)
- Single-Page Application**
Single-page web applications that run in the browser where the client receives tokens (for example, Javascript, Angular, React, Vue)
- Native Application**
Desktop or mobile applications that run natively on a device and redirect users to a non-HTTP callback (for example, iOS, Android, React Native)

[Cancel](#) [Next](#)

5. Click the **Next** button.

6. The **New Web App Integration** page displays.

- a. Enter an **App integration name** in the field. Copy and paste this name in the Identity & Access Management Portal in the **Name** field.
- b. For **Grant type > Client acting on behalf of a user**, verify that **Authorization Code** is selected.




Appendix: Example of Identity Provider Configuration


- c. For **Assignments**, select **Skip group assignment for now**.
- d. Click the **Save** button.

New Web App Integration

General Settings

App integration name

Logo (Optional)   

Grant type [Learn More](#) 

Client acting on behalf of itself

Client Credentials

Client acting on behalf of a user

Authorization Code


Refresh Token


Client-initiated backchannel authentication flow (CIBA)

Implicit (hybrid)

Sign-in redirect URIs Allow wildcard * in sign-in URI redirect.


Okta sends the authentication response and ID token for the user's sign-in request to these URIs



[Learn More](#) 

Sign-out redirect URIs (Optional)

After your application contacts Okta to close the user session, Okta redirects the user to one of these URIs.



Appendix: Example of Identity Provider Configuration

Trusted Origins

Base URIs (Optional)

Required if you plan to self-host the Okta Sign-In Widget. With a Trusted Origin set, the Sign-In Widget can make calls to the authentication API from this domain.

[Learn More](#)

Assignments

Controlled access

Select whether to assign the app integration to everyone in your org, only selected group(s), or skip assignment until after app creation.

Allow everyone in your organization to access

Limit access to selected groups

Skip group assignment for now

7. The application opens on a new page.
 - a. For **Client Credentials > Client ID**, click the **Copy to clipboard** icon. Paste it in the Identity & Access Management Portal in the **Client ID** field.
 - b. For **CLIENT SECRETS**, click the **Copy to clipboard** icon. Paste it in the Identity & Access Management Portal in the **Client Secret** field.

Appendix: Example of Identity Provider Configuration

My IDP US

Active ▾ View Logs

General Sign On Assignments Okta API Scopes Application Rate Limits

Client Credentials

Client ID: 0oaegzdeqy3BMOdmH5d7
Public identifier for the client that is required for all OAuth flows.

Client authentication: Client secret Public key / Private key

Proof Key for Code Exchange (PKCE): Require PKCE as additional verification

CLIENT SECRETS

Creation date	Secret	Actions
Jan 15, 2024	<input type="button" value="Generate new secret"/> <input type="button" value="Copy to clipboard"/> <input type="button" value="Active ▾"/>

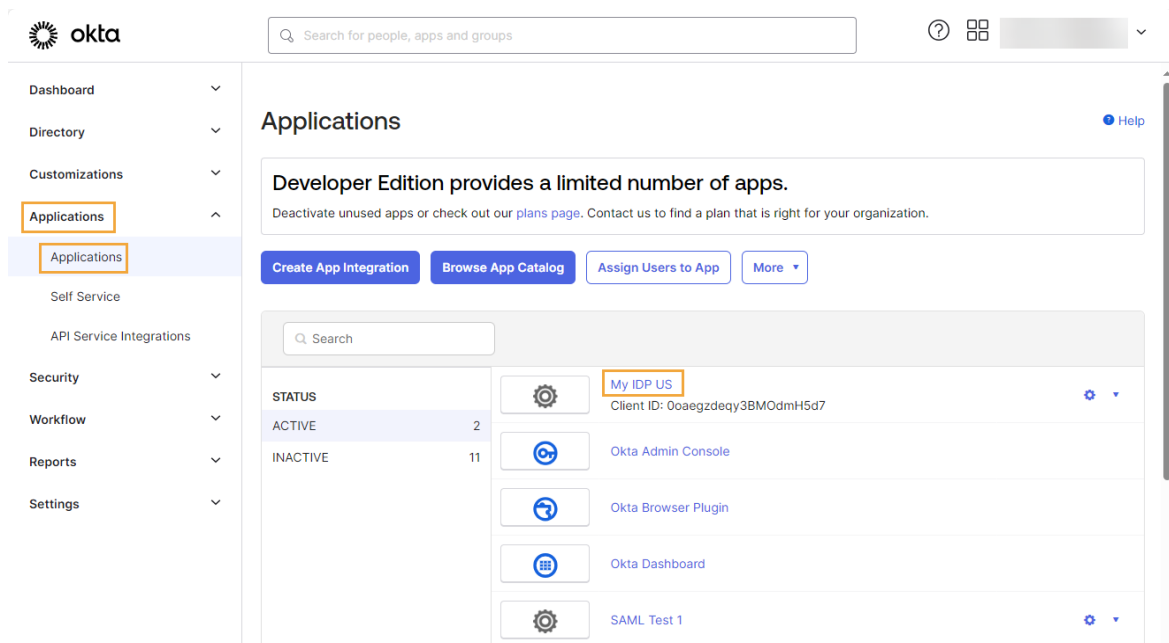
8. Select the **Assignments** tab and assign the application to any users who will use OneStream.

After you create the Okta application, go to the OneStream Identity & Access Management Portal and add the identity provider. See [Add an OIDC Identity Provider](#).

Paste the Redirect URI in the Okta Application

After you add the identity provider in the Identity & Access Management Portal, you must copy the redirect URI from OneStream and paste it in the Okta application.

1. Copy the redirect URI from the Identity & Access Management Portal in OneStream. See [Add an OIDC Identity Provider](#).
2. Sign in to Okta and go to **Applications > Applications** and select your identity provider.



3. Go to **General Settings** and click **Edit**.

Appendix: Example of Identity Provider Configuration

General Settings Edit

APPLICATION

App integration name	My IDP US
Application type	Web
Proof of possession	<input type="radio"/> Require Demonstrating Proof of Possession (DPoP) header in token requests
Grant type	<p>Client acting on behalf of itself</p> <p><input type="radio"/> Client Credentials</p> <p>Client acting on behalf of a user</p> <p><input checked="" type="radio"/> Authorization Code</p> <p><input type="radio"/> Refresh Token</p> <p><input type="radio"/> Client-initiated backchannel authentication flow (CIBA)</p> <p><input type="radio"/> Implicit (hybrid)</p>

4. Go to **LOGIN > Sign-in redirect URIs** and paste the redirect URI in the field.
5. Click the **Save** button.

Appendix: Example of Identity Provider Configuration

LOGIN

Sign-in redirect URIs ? Allow wildcard * in login URI redirect.

Sign-out redirect URIs ?

Login initiated by

Initiate login URI ?

EMAIL VERIFICATION EXPERIENCE

Callback URI ?

After you paste the redirect URI in the Okta application, go to the OneStream Identity & Access Management Portal and test the identity provider. See [Test an OIDC Identity Provider](#).

Then, configure users for authentication in OneStream. See [How Users are Configured for Authentication](#).