



Cloud Administration Tools Guide

PV6.0.0 SV200

Copyright © 2025 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, 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

Overview	1
User Management Console	1
Application Management	1
Key Management	2
Setup and Installation	3
Dependencies	3
Install Cloud Administration Tools	3
Set Up Cloud Administration Tools	4
Create Tables	5
Package Contents	5
Settings	6
Global Options	6
Email Connection	6
Domain	7
OneStream URL	7
Authentication Provider	7
Directory ID	7
Client ID	8
Client Secret	8

Table of Contents

Security Role	8
Uninstall	9
Home	10
User Management Console	12
User Details	13
Create User	14
Invite User	16
Send an Invitation	16
Import Users	17
Create Users Import Format	17
Invite Users Import Format	18
Import a Create/Invite User File	19
Delete User	20
Reset Password	21
Refresh	21
Security	21
Application Management	23
Application Details	23
Copy Application	25
Source	25

Table of Contents

Target	25
Application Properties	26
Database Properties	27
Confirm Summary	28
Remove Application	28
Confirmation Summary	29
Application History	30
Key Management	32
Bring Your Own Key	32
Enable Key Management	33
Key Information	33
Disable Key Management	34
Refresh	34
Certificates (Available Only with Platform 8.x)	34
Upload Certificates	35
Certificate Versions	36
Refresh	36
View Snippet	36
Remove Certificates	36
Secrets (Available Only with Platform 8.0)	37

Table of Contents

Upload Secrets	37
Secret Versions	38
Refresh	38
View Snippet	38
Remove Secrets	38
Help and Miscellaneous Information	39
Cloud Database Best Practices	39
Cloud Database Space	39
Cloud Services Team Updates	39
Display Settings	40
Package Contents and Naming Conventions	40
MarketPlace Solution Modification Considerations	41
Troubleshooting	41
Dashboard Rendering Errors	41

Overview

Cloud Administration Tools is a solution that contains access to multiple cloud service functions, each enabling OneStream Cloud Administrators to perform their role with greater efficiency.

User Management Console

The User Management Console manages the relationship between users hosted in the Microsoft Azure Active Directory (Azure AD) and OneStream Framework. With this console, a system administrator can self-manage their Azure AD users in OneStream by inviting, creating, deleting (disabling), and importing users and resetting passwords.

NOTE: User Management Console is only available with Azure AD hosted by OneStream Cloud Services and to members of the administrator's security group.

Application Management

Application Management maintains OneStream applications in a cloud environment. System administrators can copy existing applications, and create, replace, or remove new applications within OneStream. With Application Management, administrators can make changes for testing or archival purposes.

This functionality is only available to members of the administrator's security group.

Key Management

Key Management enables administrators to manage Azure Key Vaults by uploading .pfx encrypted files. Administrators on Platform 8.0 can manage secrets and certificates as well. The loss of service availability due to expired keys does not count against OneStream availability

Setup and Installation

This section contains important details related to the planning, configuring, and installation of your solution. Before you install the solution, familiarize yourself with these details.

See [MarketPlace Solution Modification Considerations](#).

IMPORTANT: If your environment Platform version is 8.0, or you use the User Management Console, the OneStream Cloud Support Team must perform all installation, setup, and configuration tasks. Contact OneStream Support for assistance. All others can install Cloud Administration Tools without assistance.

Dependencies

Component	Description
OneStream 8.0.0 or later	Minimum OneStream Platform version required to install this version of Cloud Administration Tools.

Install Cloud Administration Tools

1. On the OneStream MarketPlace Dashboard, go to **MarketPlace > Cloud Administration Tools**.



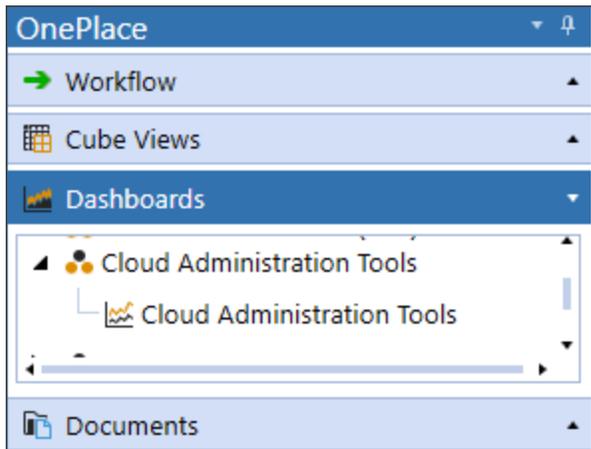
Cloud Administration Tools

2. On the **Cloud Administration Tools Solution** page, in the **Platform Version** drop-down list, select the appropriate OneStream Platform version.
3. In the **Solution Version** drop-down list, select the most recent version. Click **Download**.
4. Log into OneStream.
5. On the **Application** tab, go to **Tools > Load/Extract**.
6. On the **Load** tab, use the **Select File** icons to locate the solution package. Click **Open**.
7. When the solution file name appears, click **Load**.
8. Click **Close** to complete the installation.

Set Up Cloud Administration Tools

The first time Cloud Administration Tools is run, you are guided through the table setup process.

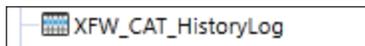
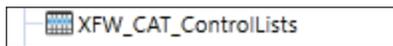
- In OneStream, go to **OnePlace > Dashboards > Cloud Administration Tools > Cloud Administration Tools**.



Create Tables

1. Click **Step 1: Create Tables**.

This step may be necessary when upgrading even if tables are already present. Cloud Administration Tools will not remove any tables that already exist but will modify table structures and add new ones if necessary.



2. When setup is complete, click **Step 2: Launch Solution** to open Cloud Administration Tools.

Package Contents

The Dashboard Maintenance Unit provides the user interface for Cloud Administration Tools and includes the required Dashboard Groups, Components, Data Adapters, Parameters, and files.

Settings

- The **Settings** page contains the **Global Options** tab in which key properties that guide administration are set as well as **Uninstall** options.

Global Options

The **Global Options** page contains key properties that guide global Cloud Administration Tools administration.

Global Options
Uninstall

Email Connection: OneStreamEmail

Domain:

OneStream URL:

Authentication Provider:

Directory ID:

Client ID:

Client Secret:

Security Role: Administrators

Save

Email Connection

Select an email connection from the drop-down list. The email connections are configured in the OneStream Application Server Configuration File and contain all the necessary

Settings

setup information for the local email provider, including the sending email address, server credentials, host, and port. The email connections list is pulled from the Database Server Connections list in the Application Server Configuration File.

For more details on email database connections, see the *Installation and Configuration Guide*. This setting can be changed by the administrator to send emails from a different connection.

Domain

The Azure Active Directory (Azure AD) domain name is @mydomain.onestreamcloud.com and should not be modified with the exception of a direction by Support.

OneStream URL

The Azure URL of the customer environment is https://xxxxxx.onestreamcloud.com/onestreamweb and should not be modified with the exception of a direction by Support.

Authentication Provider

The name of the authentication provider service for the OneStream Framework database in this server environment. Do not modify this setting unless directed to do so by Support.

Directory ID

This directory ID is the Azure Tenant ID.

Client ID

The client ID is configured by the OneStream Cloud Services Team. This encrypted key is masked and will display as a blank entry after the initial setup. Do not modify this setting unless directed to do so by Support.

Client Secret

The client secret is used to authenticate with the Azure Active Directory service.

Security Role

Since security is governed at the global level, it is the assignment of the user group to the Security Role that determines who will be global Cloud Administration Tools Administrators. This group is granted access to all areas of Cloud Administration Tools and are the only users who can see the Settings Page icon.

Uninstall

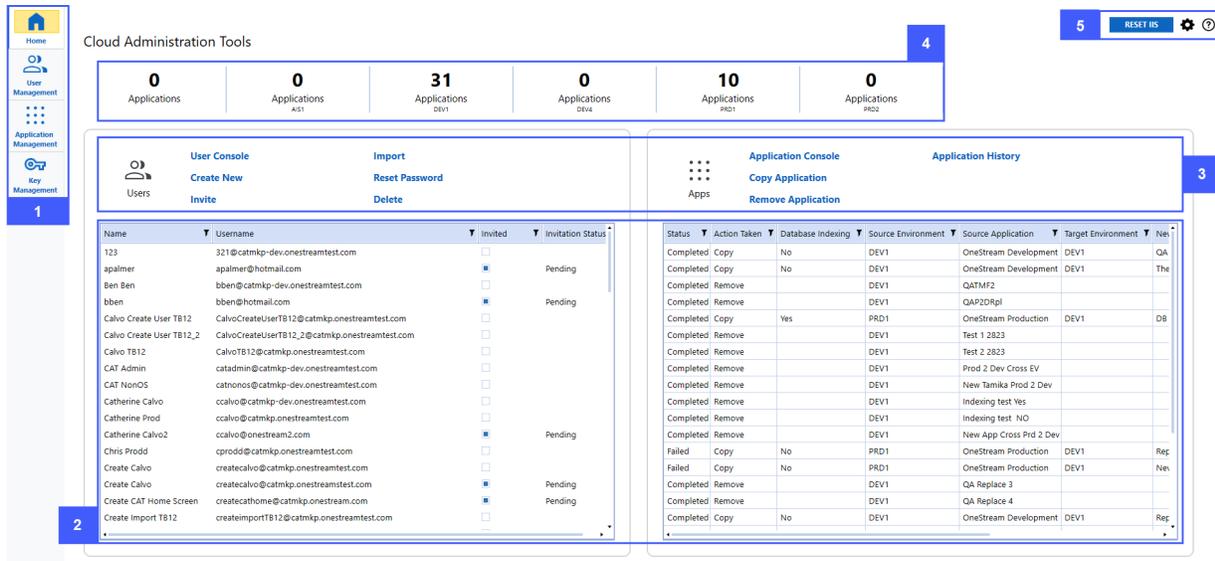
Use the Uninstall feature to remove the Cloud Administration Tools User Interface or the entire solution. If part of an upgrade, any modifications performed on standard Cloud Administration Tools objects are removed. These are the uninstall options:

- **Uninstall UI** removes Cloud Administration Tools, including related dashboards and business rules, but retains the database and related tables. For some releases, perform this step before accepting a new solution version as some of the dashboards or other objects may have changed. Choose this option to update Cloud Administration Tools without removing the data tables. The Release Notes indicate if an overinstall is supported.
- **Uninstall Full** removes all related data tables, data, and Cloud Administration Tools dashboards and business rules. Choose this option to completely remove Cloud Administration Tools or to perform an upgrade that is so significant in its changes to the data tables that this method is required.

CAUTION: Uninstall procedures are irreversible.

Home

The Home page displays the functionality enabled through Global Settings.



1. Navigational Tabs

- **Home:** Enables system administrators to monitor users, applications, and key performance metrics in one centralized location.
- **User Management:** Enables system administrators to perform all user account maintenance tasks in a single interface.
- **Application Management:** Enables system administrators to create, replace, or remove applications within the OneStream Azure environment.
- **Key Management:** Enables system administrators to manage the key vault and Bring Your Own Key (BYOK) settings.

2. Overviews

- **User Management Overview:** Displays a list of users, their type, and current status, such as active or inactive.
- **Application Management Overview:** Displays a list of applications, their type, and current status, such as active or inactive.

3. Quick Links

System administrators can use quick links to navigate through the solution to perform key tasks.

4. Key Performance Indicators (KPIs)

KPIs display an overview of the environment. Use the scroll bar to view additional metrics.

5. Settings

- **Reset IIS:** This button manually resets the environment.

IMPORTANT: Performing an IIS reset ends all tasks currently in progress.

- **Settings:** Icon that provides access to the Settings page.
- **Help:** Icon that links to solution documentation.

TIP: If the Home screen displays any errors or fails to render, see [Troubleshooting](#).

User Management Console

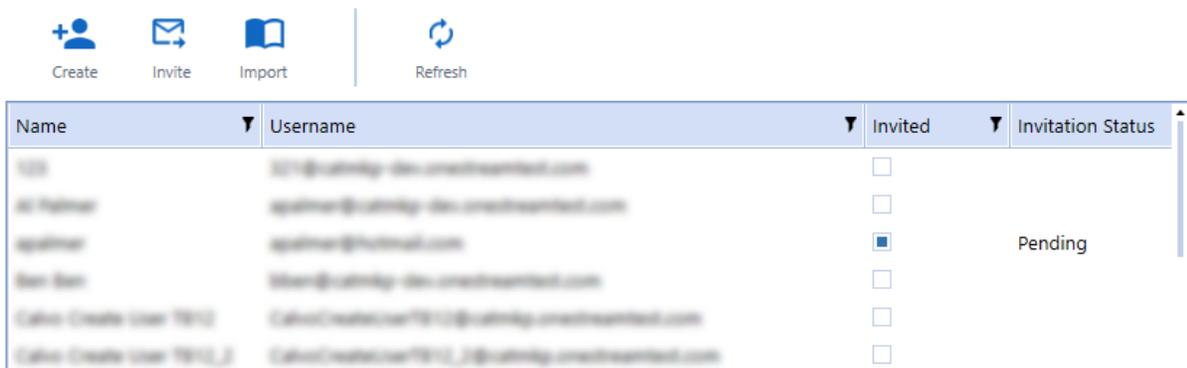
The User Management Console displays a grid containing all Azure AD users and their related actions.

Administrators running Platform 6.x and above, who currently have access to the User Management Console, can create, invite, import, and delete users and reset user passwords.

When launched, the User Management Console displays a user list in a grid view, which shows the following information about each user:

- **Name:** User's name in OneStream.
- **Username:** User's Azure AD username.
- **Invited:** Indicates if the user was invited from an external Azure AD tenant.
- **Invitation Status:** Indicates if the user responded to the invitation.

User Management Console



The screenshot shows the User Management Console interface. At the top, there are four action buttons: 'Create' (person icon), 'Invite' (envelope icon), 'Import' (book icon), and 'Refresh' (circular arrow icon). Below these buttons is a table with the following columns: Name, Username, Invited, and Invitation Status. The table contains six rows of user data.

Name	Username	Invited	Invitation Status
123	123@contoso.onestream.com	<input type="checkbox"/>	
456	456@contoso.onestream.com	<input type="checkbox"/>	
ap@contoso	ap@contoso.onestream.com	<input checked="" type="checkbox"/>	Pending
Bob Bob	Bob@contoso.onestream.com	<input type="checkbox"/>	
Calvin Create User 7812	CalvinCreateUser7812@contoso.onestream.com	<input type="checkbox"/>	
Calvin Create User 7812_2	CalvinCreateUser7812_2@contoso.onestream.com	<input type="checkbox"/>	

User Details

The following user details are displayed if the Azure AD member is a OneStream user:

User Info

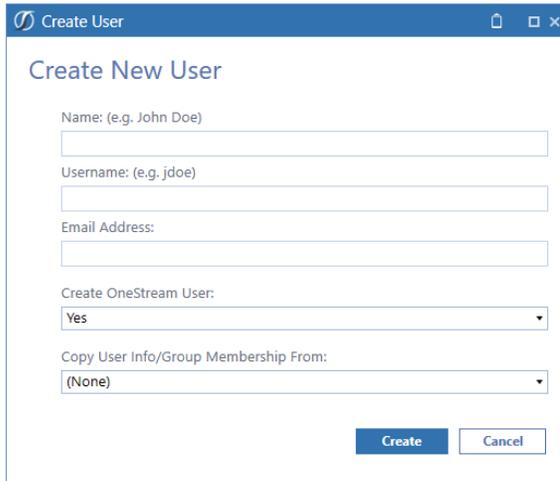
- Name
- Description
- Ext Auth Provider
- Ext UserName
- Email
- Is Enabled
- Culture Code

User Logon History

- Application Name
- Logon Type
- Logon Time
- Last Activity Time
- Logoff Time

User Groups

- Group Name
- Group Description



- **Name:** Enter the user's name.
 - **Username:** Enter the name used to log into Azure AD.
 - **Email Address:** Enter a valid email address.
 - **Create OneStream User:** Select **Yes** to add the user to the OneStream Framework database.
 - **Copy User Info/Group Membership From:** Select to copy an individual user's information or group information.
2. Click the **Create** button.
 3. Repeat the procedure for each user to add.
 4. Click close to exit the **Create User** dialog box.

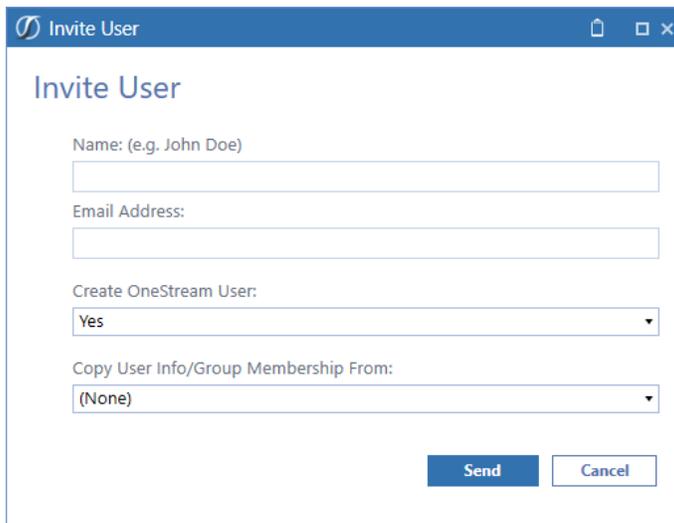
NOTE: Copied security groups can allow access to multiple applications in the OneStream Framework environment, requiring additional security group adjustments in OneStream **System > Administration > Security**.

Invite User

Invite User enables a system administrator to send an invitation to a user who has an existing Azure AD or Office 365 account not currently in the Azure AD tenant hosted by OneStreamCloud Services. After accepting the invitation, that existing account can access OneStream. This email also contains the company's OneStream environment URL.

Send an Invitation

1. On the **User Management Console** page, click **Invite** and complete the following fields:



The screenshot shows a web form titled "Invite User" with the following fields and controls:

- Name:** (e.g. John Doe) - Text input field.
- Email Address:** - Text input field.
- Create OneStream User:** - Dropdown menu with "Yes" selected.
- Copy User Info/Group Membership From:** - Dropdown menu with "(None)" selected.
- Buttons:** "Send" (blue) and "Cancel" (white).

- **Name:** Enter the user's name.
- **Email Address:** Enter a valid email address.

- **Create OneStream User:** Select **Yes** to add the user to the OneStream Framework database.
- **Copy User Info/Group Membership From:** Select to copy an individual user's information or group information from the security user information.

2. Click the **Send** button to send the invitation.

Import Users

Import Users enables a system administrator to perform a bulk create or invite by importing a valid comma-separated values (.csv) file of user properties.

The bulk import process creates users but does not assign a default security group in OneStream. Additional security group maintenance in the OneStream **System > Administration > Security** tab is necessary to finalize the new user's access.

Create Users Import Format

The format for **Create Users** is a 4-column, .csv file with the following fields:

- Name
- Username
- Email
- OneStream User

The OneStream User column determines if a user is added as a OneStream user or an Azure-only user.

User Management Console

- A **True** or **Yes** response designates them as a OneStream and Azure user.
- A **False** or **No** response designates them as an Azure-only user.

IMPORTANT: Do not add column headers to the .csv files. Headers will cause an import to fail.

Example Create User

OneStream and Azure User

```
Name,Username,Email,OneStream User
John Doe,jdoe,jdoe@mycompany.com,True
John Doe,jdoe,jdoe@mycompany.com,Yes
```

Azure-only User

```
Name,Username,Email,OneStream User
John Doe,jdoe,jdoe@mycompany.com,False
John Doe,jdoe,jdoe@mycompany.com,No
```

Invite Users Import Format

The format for Invite Users is a 3-column, .csv file with the following fields:

- Username
- Email
- OneStream User

The OneStream User column determines if a user is added as a OneStream user or an Azure-only user.

User Management Console

- A **True** or **Yes** response designates them as a OneStream and Azure user.
- A **False** or **No** response designates them as an Azure-only user.

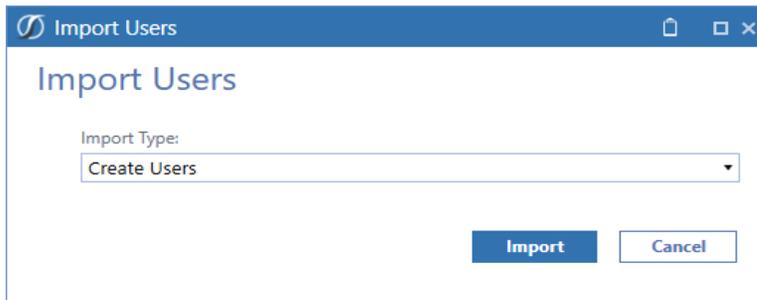
IMPORTANT: Do not add column headers to the .csv files. Headers will cause an import to fail.

Example Invite User

```
Username,Email,OneStream User
mdoe,mdoe@mycompany.com,True
mdoe,mdoe@mycompany.com,Yes
```

Import a Create/Invite User File

1. On the **User Management Console** page, click **Import**.
2. In the **Import Users** dialog box, use the **Import Type** drop-down list to select **Create Users** or **Invite Users**. Click the **Import** button.



3. Navigate to the location of the file and click **Open**. The Import Users process runs a data management job for the imported users. This job will run as a background task that can be monitored from the Task Activity screen.

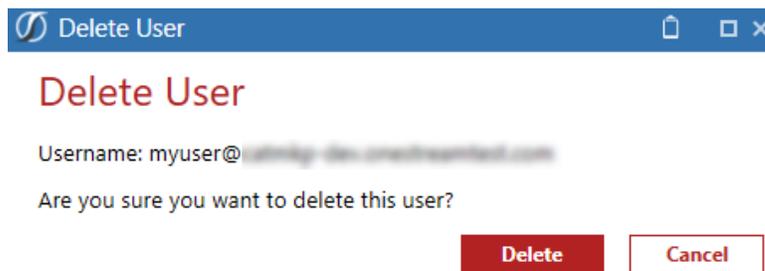
Delete User

The **Delete** button enables a system administrator to remove a user from Azure AD and disable them in the OneStream security.

When a user is deleted from the system, their user information remains in OneStream to preserve the integrity of the audit trail, which contains the activity history associated with the user ID.

To delete a user:

1. On the **User Management Console** page, select the user.
2. Under **User Information**, click **Delete**.
3. In the **Delete User** dialog box, click the **Delete** button to confirm.

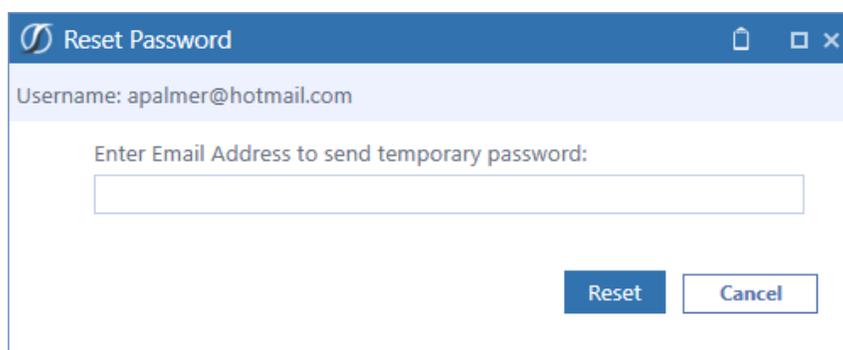


Reset Password

System administrators can use the **Reset Password** button to initiate the password reset process for a user.

To reset a user's password:

1. On the **User Management Console** page, select the name of the user.
2. Under **User Information**, click **Reset Password**.
3. In the **Reset Password** dialog box, enter the user's email address.
4. Click the **Reset** button to send the temporary password.



Refresh

- ° Click Refresh to update a page.

Refresh User Details updates the displayed information for changes in the security domain or the OneStream system security.

Security

- Security accesses the OneStream framework.

User Management Console

Security opens the **OneStream System > Administration > Security** page to manage the system security framework for OneStream users and groups.

Application Management

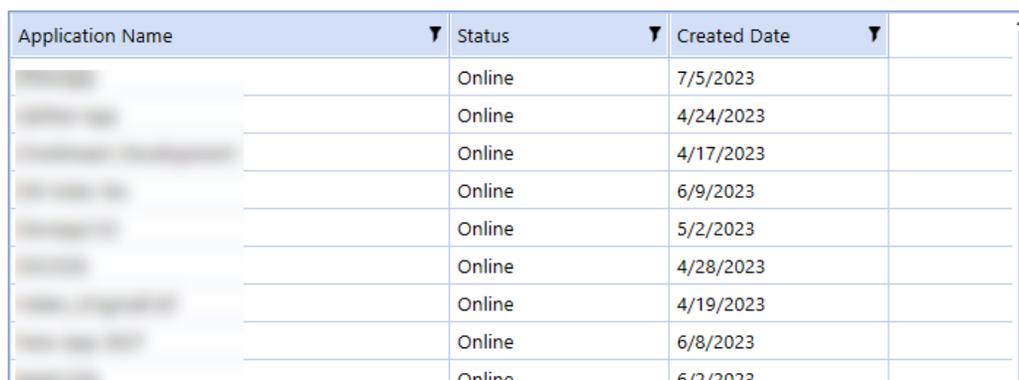
Application Management enables you to create or replace applications as a copy of existing applications or remove applications within your OneStream Azure environment.

Administrators running platform version 6.x can use Application Management to copy, replace, and remove applications and view historical activity on applications.

When you launch Application Management, the **Application Console** displays all applications in grid view and includes the following information:

- **Application Name:** Title of the application.
- **Status:** Indicates if the application is online or deleted.
- **Created Date:** Indicates when the application was created.

Application Console



Application Name	Status	Created Date	
[Blurred]	Online	7/5/2023	
[Blurred]	Online	4/24/2023	
[Blurred]	Online	4/17/2023	
[Blurred]	Online	6/9/2023	
[Blurred]	Online	5/2/2023	
[Blurred]	Online	4/28/2023	
[Blurred]	Online	4/19/2023	
[Blurred]	Online	6/8/2023	
[Blurred]	Online	6/2/2023	

Application Details

Select an application to view the following application details:

Application Management

Application Information

- Environment
- Owner
- Creation Date

Application History

- Action Taken
- User
- Start Time

Application Console

Application Name	Status	Created Date
...	Online	7/5/2023
...	Online	4/24/2023
...	Online	4/17/2023
...	Online	6/9/2023
...	Online	5/2/2023
...	Online	4/28/2023
...	Online	4/19/2023
...	Online	6/8/2023
...	Online	6/2/2023
...	Online	5/2/2023
...	Online	5/2/2023
...	Online	5/2/2023
...	Online	5/30/2023
...	Online	6/13/2023
...	Online	4/10/2023
...	Online	5/18/2023
...	Online	5/23/2023
...	Online	5/2/2023
...	Online	6/8/2023
...	Online	6/2/2023
...	Online	5/10/2023
...	Online	4/12/2023
...	Online	4/11/2023
...	Online	5/2/2023
...	Online	5/2/2023
...	Online	5/1/2023
...	Online	6/13/2023
...	Online	4/19/2023

Application Information

Environment: DEV1
Owner: @onestreamsoftware.com
Creation Date: 4/17/2023

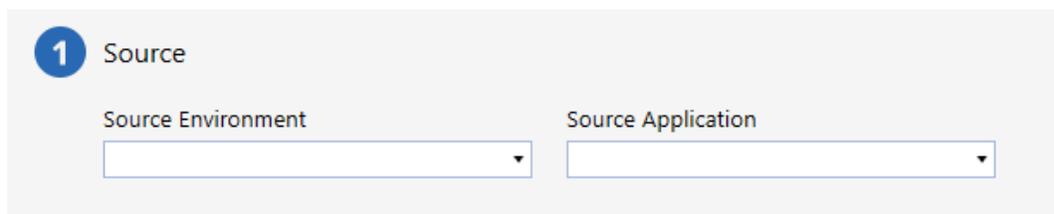
Application History

Action Taken	User	Start Time
Copy	...	6/13/2023 8:51:47 PM
Copy	...	6/13/2023 6:37:57 PM
Copy	...	6/8/2023 2:51:51 PM
Copy	...	6/8/2023 2:27:21 PM

Copy Application

Administrators can create or replace applications across environments using the **Copy Application** tab in the Application Management solution.

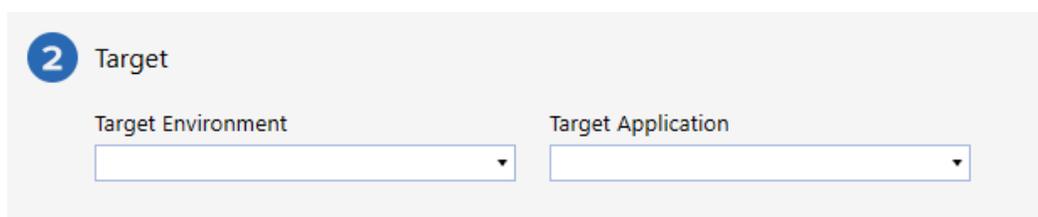
Source



The screenshot shows a light gray box with a blue circle containing the number '1' and the text 'Source'. Below this, there are two dropdown menus. The first is labeled 'Source Environment' and the second is labeled 'Source Application'. Both dropdown menus are currently empty.

1. Select a **Source Environment**, which is the environment of the application being copied or replaced. The Source Environment will display active OneStream environments.
2. Select a **Source Application**, which is the data that will be copied to create a new application or replace an existing application. The Source Application will display all active OneStream applications.

Target



The screenshot shows a light gray box with a blue circle containing the number '2' and the text 'Target'. Below this, there are two dropdown menus. The first is labeled 'Target Environment' and the second is labeled 'Target Application'. Both dropdown menus are currently empty.

1. Select a **Target Environment**, which is the environment where the source application data will be copied or replaced. Only the current environment can be

Application Management

selected from the drop-down list.

2. Select a **Target Application** to create a new application or replace an existing application. The drop-down list allows for a new application copy or displays all available applications that can be replaced.

IMPORTANT: Replacing the application removes all existing data and replaces it with a copy of the source application data.

Application Properties

Use **Application Properties** to configure options on the application being created or replaced.

3 Application Properties

Application Name: HoustonHeights

Enable Scheduled Tasks: Yes No

Application Name

Type a unique application name in the **Application Name** field.

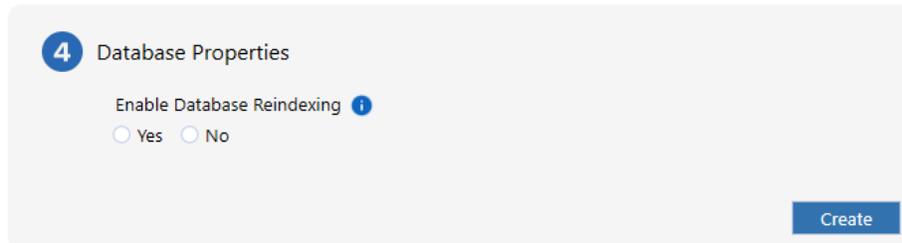
NOTE: Application names can be 4–128 characters in length and contain the following characters: period, space, underscore, alphanumeric characters, and hyphen.

Enable Scheduled Tasks

Select **Yes** to carry over scheduled tasks from the source application to the target application. Select **No** to disable all tasks in the the target application.

Database Properties

Enable Database Indexing rebuilds indexes during maintenance windows.



- Select **Yes** to enable.
- Select **No** to skip enabling.

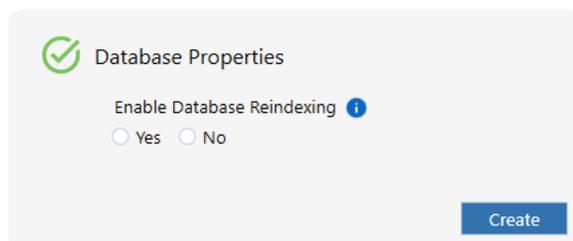
NOTE: Due to increased maintenance times, it is recommended to enable database indexing on only one business critical application.

Create or Replace Application

Depending on the selection made in the Target Application field, the button will display as **Create** or **Replace**.

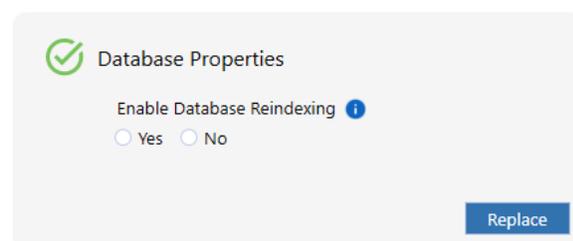
Create

If a new application is being created, a **Create** button displays.



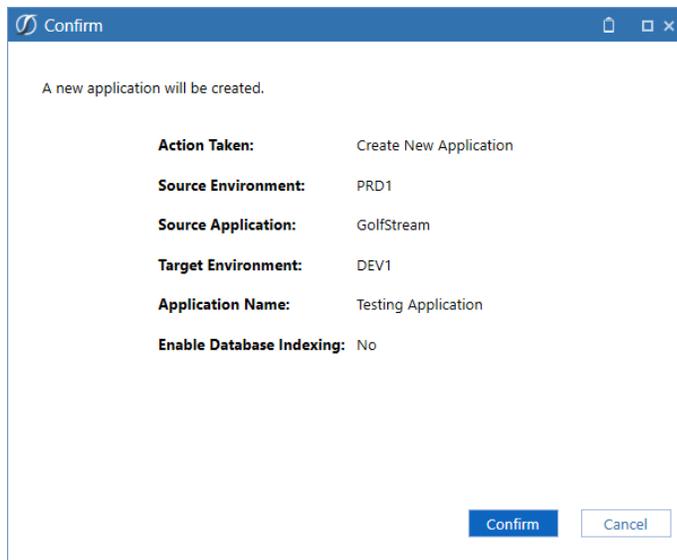
Replace

If an existing application was selected in the Target Application drop-down list, a **Replace** button displays.



Confirm Summary

The **Confirm** dialog box appears after the create or replace action runs. The **Confirm** dialog box displays the actions that must be confirmed. This confirmation also displays any warnings, such as if a production application is being created.



1. Review the confirmation summary.
2. Click the **Confirm** button to accept the actions.

NOTE: If you choose to cancel or close the dialog box, you can make your corrections.

Once you confirm, the **Application History** page displays.

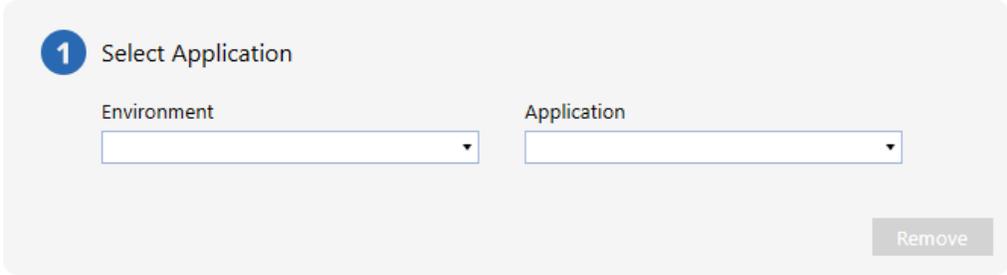
Remove Application

Administrators can remove applications using the **Remove Application** tab in Application Management.

Application Management

[Application Console](#) [Copy Application](#) [Remove Application](#) [Application History](#)

Remove Application



1 Select Application

Environment

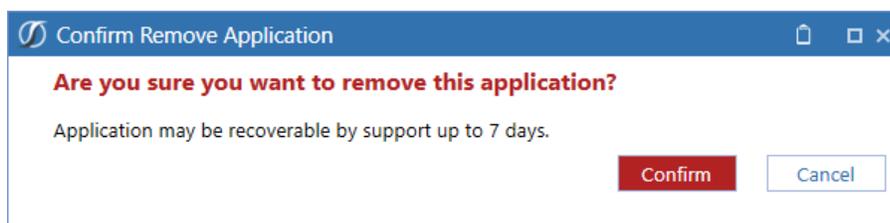
Application

Remove

1. Click **Remove Application**.
2. Select the **Environment**.
3. Select the **Application**.
4. Click the **Remove** button.

Confirmation Summary

The **Confirm Remove Application** dialog box displays after the remove action runs. Click the **Confirm** button to accept the actions.



After you confirm, you will be taken to the **Application History** page.

NOTE: If you choose to cancel or close the dialog box, you can make corrections.

Application History

The **Application History** page displays detailed information on the operations completed through Application Management. Click  to filter data in the table.

Application History

 Refresh

Status	Action Taken	Database Indexing	Source Environment	Source Application	Target Environment	New Application Name	Application Replaced	Start Time	End Time	User
Completed	Copy	No	DEV1	Cloudstream Development	DEV1	Old Test App	Replacement (APP ID) Prod 1.0.0	6/13/2023 8:51:47 PM	6/13/2023 9:02:31 PM	Service Manager
Completed	Copy	No	DEV1	Cloudstream Development	DEV1	New App		6/13/2023 6:37:57 PM	6/13/2023 6:46:14 PM	Service Manager
Completed	Remove		DEV1	App1234				6/13/2023 6:25:22 PM	6/13/2023 6:28:09 PM	Service Manager
Completed	Remove		DEV1	App123456				6/12/2023 1:41:24 PM	6/12/2023 1:44:03 PM	Service Manager

- **Status:** Shows the progression and results of all applications being created, replaced, or removed after the process starts. Application statuses include: **Running, Success, or Failed.**

NOTE: If the result is **Running**, click **Refresh** to see if the process has completed its action.

NOTE: If the result is **Failed**, navigate to the **Task Activity** dialog box to view a description of the error.

- **Action Taken:** Shows the action performed by the user. Displays **Copy** or **Remove** for all applications.
- **Enable Database Indexing:** Indicates whether the application will have indexes rebuilt during maintenance windows. Displays **Yes** or **No** for all applications.
- **Source Environment:** Displays the environment from which the Source Application is chosen.
- **Source Application:** Displays the data used to create a new application or to replace data in another application.

Application Management

- **Target Environment:** Displays the environment where the new or replaced application was placed.
- **New Application Name:** Displays the name given to the created or replaced application.
- **Application Replaced:** Displays the name of the replaced application. If a new application was created, this field is blank .
- **Start Time:** Indicates the start time of the copy, replace, or remove process.
- **End Time:** Indicates the end time of the copy, replace, or remove process.
- **User:** Indicates the user who created, replaced, or removed the application.

Key Management

 Key Management enables you to manage the OneStream Azure Key Vault and create keys, certificates, and secrets.

Bring Your Own Key

Our SaaS offering includes a robust key management service, ensuring the highest level of security for your data. Each client's key vault is uniquely deployed within our cloud infrastructure, enabling the Bring Your Own Key (BYOK) feature as part of our Cloud Administration Tools suite. This design guarantees that the lifecycle of your key vault is intrinsically linked to your specific instance, maintaining exclusivity and preventing access by other tenants.

You retain complete control over your keys through the Cloud Administration Tools interface, with keys securely stored in your private key vault, which is associated with a managed identity. Access to the key vault is stringently regulated; only the managed identity assigned to your OneStream instance's compute nodes and database server has the operational capability to manage keys, secrets, and certificates. This managed identity is granted specific roles—Certificates Officer, Crypto Officer, Service Encryption User, and Secrets Officer—to facilitate secure operations.

Network security measures are rigorously enforced to ensure that the key vault is accessible solely from your OneStream instance's network. Complementing these measures, we employ Azure policies and proactive alerting systems to safeguard against unauthorized changes to access policies. These policies are consistently reviewed in

Key Management

alignment with our SOC controls, further reinforcing our commitment to your data's security.

Bring Your Own Key

Refresh

Upload Key

Enter .pfx file password

Upload

Thumbprint	Status	Created Date
[Redacted]	Active	7/7/2023 2:09:56 PM
[Redacted]	Disabled	7/7/2023 2:09:28 PM
[Redacted]	Disabled	7/3/2023 6:44:16 PM
[Redacted]	Disabled	7/3/2023 5:27:10 PM
[Redacted]	Disabled	7/3/2023 5:26:58 PM
[Redacted]	Disabled	7/3/2023 5:26:41 PM

Key Information

Status: Active

Thumbprint: [Redacted]

Activation Date: 1/1/1970 12:00:00 AM

Expiration Date: 1/1/1970 12:00:00 AM

Disable BYOK

Enable Key Management

To enable BYOK:

1. Click **Upload**.
2. Select a .pfx file.

NOTE: Users on Platform 8.0 or above can choose to upload .pem files.

3. Click **Open**.
4. Your key is uploaded directly to the Azure Key Vault and the uploaded file is automatically deleted.

Key Information

Select a key to view its:

Key Management

- Name
- Status
- Azure thumbprint ID
- Activation Date
- Expiration Date

Disable Key Management

Disable key management by clicking the **Disable BYOK** button. BYOK will be disabled and your data will be managed by the service.

Refresh



This refreshes information in the grid.

Certificates (Available Only with Platform 8.x)

Certificates and their corresponding keys can be used for more secure authentication to APIs, FTP servers, and other integrations. Each certificate contains a thumbprint ID that can be used in the Azure configuration tiles to identify which key is in use. The certificate interface enables system administrators to securely store these for later use in business rules.

Key Management

Certificates

The screenshot displays the Certificates management interface. On the left, there is an 'Upload Certificate' form with fields for 'Certificate Name' and 'Password', and radio buttons for 'Key Type' (HSM or Non-HSM). Below the form is a table listing existing certificates. On the right, there are two tables: 'Certificate Versions' showing the 'Current Version' and 'Previous Versions'.

Name	Status	Created Date	Expiration Date
	Active	7/10/2023 3:41:36 PM	5/16/2024 9:25:55 PM
	Active	7/7/2023 2:11:28 PM	5/16/2024 9:25:55 PM
	Active	7/6/2023 6:18:24 PM	5/16/2024 9:25:55 PM
	Active	6/27/2023 2:48:51 PM	5/16/2024 9:25:55 PM
	Active	6/26/2023 4:21:44 PM	5/16/2024 9:25:55 PM
	Active	6/26/2023 4:20:31 PM	5/16/2024 9:25:55 PM
	Active	6/26/2023 4:19:53 PM	5/16/2024 9:25:55 PM
	Active	6/26/2023 3:56:58 PM	5/16/2024 9:25:55 PM
	Active	6/26/2023 3:56:33 PM	5/16/2024 9:25:55 PM
	Active	6/26/2023 3:55:01 PM	5/16/2024 9:25:55 PM
	Active	6/26/2023 3:54:25 PM	5/16/2024 9:25:55 PM
	Active	6/26/2023 3:53:38 PM	5/16/2024 9:25:55 PM

Version	Status	Created Date	Expiration
9335a9b64a1846daa1fe1cfd75214b83	Active	6/27/2023 2:48:51 PM	5/16/2024 9:25:55 PM

Version	Status	Created Date	Expiration Date
	Active	6/27/2023 2:48:15 PM	5/16/2024 9:25:55 P
	Active	6/27/2023 2:47:56 PM	5/16/2024 9:25:55 P
	Active	6/27/2023 2:47:10 PM	5/16/2024 9:25:55 P
	Active	6/27/2023 2:46:22 PM	5/16/2024 9:25:55 P
	Active	6/27/2023 2:46:09 PM	5/16/2024 9:25:55 P
	Active	6/27/2023 2:45:58 PM	5/16/2024 9:25:55 P
	Active	6/27/2023 2:45:46 PM	5/16/2024 9:25:55 P
	Active	6/27/2023 2:45:29 PM	5/16/2024 9:25:55 P
	Active	6/27/2023 2:45:16 PM	5/16/2024 9:25:55 P

Upload Certificates

To create a new certificate:

1. Enter a certificate name.

NOTE: Certificate names should be 127 characters or less.

2. Under **Key Type**, select **HSM** or **Non-HSM**.

NOTE: HSM is a physical device providing extra protection for sensitive keys. Using an HSM will permanently prevent exporting the private key in the future.

3. Enter a password.
4. Click the **Upload** button.
5. Select a .pfx file.
6. Click **Open**.

Certificate Versions

Select a certificate to view its status, creation and expiration dates, current version number, and previous versions.

Refresh



This refreshes information in the grid.

View Snippet

Click the **View Snippet** button to retrieve a sample BRAPI code of the certificate, which can be copied and used in your business rules.

Certificate X509Certificate2

```
BRApi.Utilities.GetCertificate(SessionInfo si, string certificateName)
```

This BRApi is used to access a certificate or key from within a business rule to load it into memory. It cannot be used with HSM backed keys.

Certificate Signature String

```
BRApi.Utilities.Sign(SessionInfo si, string keyName, string algorithm, byte[] digest)
```

This BRApi is used to generate a signature using a key stored in the key vault without extracting the key. This can be used with both HSM and non-HSM backed keys.

Remove Certificates

The **Delete Certificate** button enables you to delete a certificate.

NOTE: After you delete a certificate, you cannot reuse the same certificate name for 90 days.

Secrets (Available Only with Platform 8.0)

Secrets enable system administrators to securely store sensitive information like passwords, API keys, or connection strings for later use in business rules.

Secrets

The screenshot displays the 'Secrets' management interface. On the left, there is a 'Refresh' button and an 'Upload Secret' form. The form has two input fields: 'Name: *' and 'Secret value: *', followed by an 'Upload' button. Below the form is a list of existing secrets with a 'Name' column. On the right, there are 'View Snippet' and 'Delete Secret' buttons. Below these is the 'Secret Versions' section, which shows the 'Current Version' and a table of 'Previous Versions'.

Version	Created
	7/7/2023 2:13:12 PM
	7/6/2023 6:52:45 PM
	7/6/2023 5:51:36 PM
	6/14/2023 8:57:13 PM
	6/14/2023 8:56:52 PM
	6/14/2023 8:30:37 PM
	6/9/2023 12:51:35 PM
	6/9/2023 12:50:42 PM
	6/9/2023 12:49:58 PM

Upload Secrets

To create a new secret:

1. Enter a secret name.

NOTE: After you delete the name of a secret, you cannot reuse the same name for 90 days.

2. Enter a secret value.
3. Click the **Upload** button.

Secret Versions

Select a secret to view the current version number, previous version number, and creation dates.

Refresh



This refreshes information in the grid.

View Snippet

Click the **View Snippet** button to retrieve a sample BRAPI code of the secret, which can be copied and used in business rules.

Secret Value String

```
BRApi.Utilities.GetSecretValue(SessionInfo si, string secretName)
```

Remove Secrets

Click the **Delete Secret** button to delete a secret that is no longer in use.

Help and Miscellaneous Information



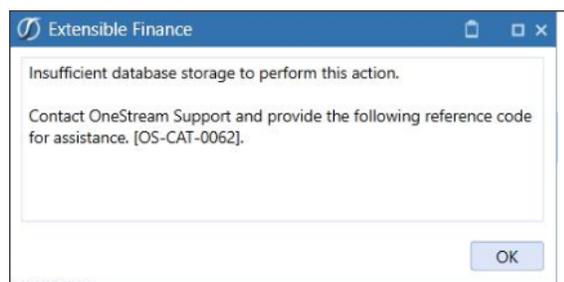
This page contains solution documentation.

Cloud Database Best Practices

Use the following best practices.

Cloud Database Space

When managing applications, if the Azure capacity is insufficient to copy an entire application, the copy process stops and an error message displays. OneStream Support may be able to increase your available storage at an additional cost or you may free up space by using **Remove Application** in **Application Management** to delete applications that are no longer needed.



Cloud Services Team Updates

OneStream may periodically release updates to Cloud Administration Tools to provide new functionality, address undesired behavior, or retire features that are no longer supported. These changes are displayed in Cloud Administration Tools. In addition, these

changes are reflected in the Dashboard Maintenance report, which can be run from OneStream's Navigation Center solution.

Display Settings

OneStream and MarketPlace solutions frequently require the display of multiple data elements for proper data entry and analysis. Therefore, the recommended screen resolution is a minimum of 1920 x 1080 for optimal rendering of forms and reports.

Package Contents and Naming Conventions

The package file name contains multiple identifiers that correspond with the platform. Renaming any of the elements contained in a package is discouraged in order to preserve the integrity of the naming conventions.

Example Package Name: CAT_PV6.0.0_SV200_PackageContents.zip

Identifier	Description
CAT	Solution ID
PV6.0.0	Minimum Platform version required to run solution
SV200	Solution version
PackageContents	File name

MarketPlace Solution Modification

Considerations

A few cautions and considerations regarding the modification of OneStream Solutions:

- Major changes to business rules or custom tables within a OneStream Solution will not be supported through normal channels as the resulting solution is significantly different from the core solution.
- If changes are made to any dashboard object or business rule, consider renaming it or copying it to a new object first. This is important because if there is an upgrade to the OneStream Solution in the future and the customer applies the upgrade, this will overlay and wipe out the changes. This also applies when updating any of the standard reports and dashboards.
- If modifications are made to a OneStream solution, upgrading to later versions will be more complex depending on the degree of customization. Simple changes such as changing a logo or colors on a dashboard do not impact upgrades significantly. Making changes to the custom database tables and business rules, which should be avoided, will make an upgrade even more complicated.

Troubleshooting

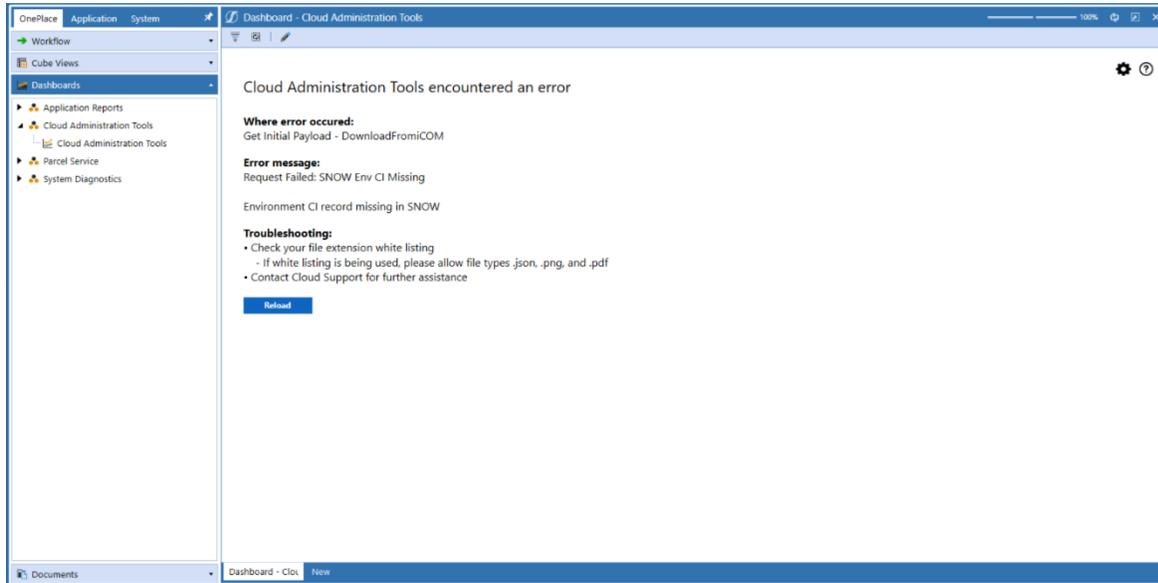
Dashboard Rendering Errors

When the Cloud Administration Tools encounters any dashboard rendering errors, a troubleshooting dashboard will be populated.

Help and Miscellaneous Information

On this dashboard, users can see where the error occurred, a brief error message, and steps for troubleshooting the error.

NOTE: Errors will still be tracked in the error log.



Reload: Use this button to reload the dashboard, during which time the application will clear out unused discover dashboard .json files. If this resolves the issue, users will be redirected to the Cloud Administration Tools homepage, otherwise the troubleshooting dashboard will populate again. The reload button can be used to reassess the issue twice before the button is taken away and users are prompted to contact Cloud Support.