

## Overview

This document describes the process of configuring remote URL authentication credentials within SOLV3D encompass (Encompass). It covers how to store credentials both Azure SAS URL and AWS STS authentication schemes.

## Assumptions

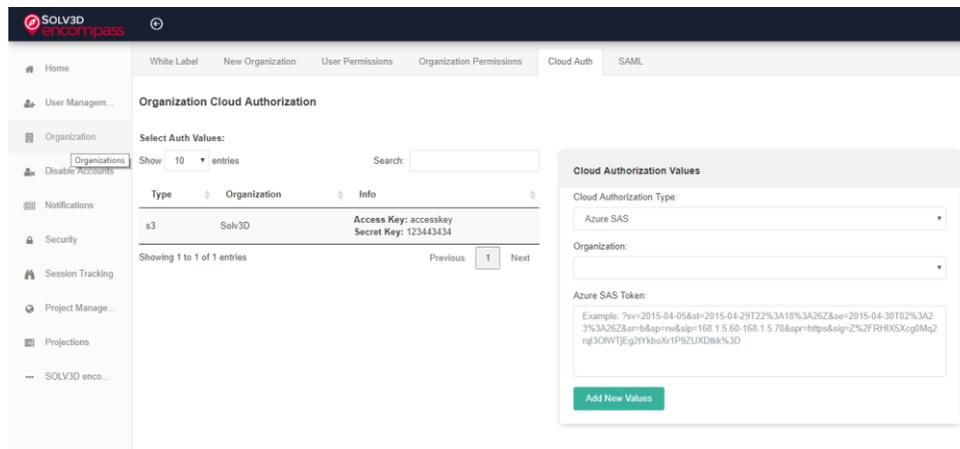
- Data is being hosted in either Azure or AWS.
- User has organization administrator privileges within Encompass.
- Organization administrator has knowledge or access/permissions to configure the cloud blob storage provider.
- Cloud storage credentials have been setup with Read Only access to the blob storage. This is the bare minimum level of permissions required.
- Data (points and images folder) has been uploaded to a location in the blob storage.

For all other authentication schemes and configuration, please contact [support@solv3d.com](mailto:support@solv3d.com) for more details.

## Viewing Existing Cloud Authorization

Access the Cloud Auth tab within the Organization configuration section

1. In the left-hand navigation, select **Management**.
2. Once Management loads, in the left-hand navigation select **Organization**.
3. On the Organization page, select the **Cloud Auth** tab.



The screenshot shows the SOLV3D encompass interface. The top navigation bar includes tabs for White Label, New Organization, User Permissions, Organization Permissions, Cloud Auth, and SAML. The left-hand navigation menu is expanded to show Organization, with sub-items for Organizations, Disable Accounts, Notifications, Security, Session Tracking, Project Manage..., and Projections. The main content area is titled "Organization Cloud Authorization" and features a "Select Auth Values:" section with a "Show 10 entries" dropdown and a search box. Below this is a table with columns for Type, Organization, and Info. The table contains one entry for "SolV3D" with "Access Key: accesskey" and "Secret Key: 123443434". A "Showing 1 to 1 of 1 entries" message and pagination controls are at the bottom of the table. To the right, a "Cloud Authorization Values" modal is open, showing a "Cloud Authorization Type:" dropdown set to "Azure SAS", an "Organization:" dropdown, and an "Azure SAS Token:" text area containing an example token. An "Add New Values" button is at the bottom of the modal.

## Adding New Cloud Authorization Credentials

1. Access the **Cloud Auth** tab as described above.
2. In the left-hand table, ensure no other existing cloud authorization records are selected.

3. On the right-hand side, within the **Cloud Authorizations Values** table, select the Cloud Authorization Type.
  - a. For Azure blob, select **Azure SAS** (Shared Access Signatures) select the organization and enter the SAS key query string. Note: Do not include blob information. Blob hostname and folder structure will be configured in project setup.

Example SAS key query string:

```
?sv=2015-04-05&st=2015-04-29T22%3A18%3A26Z&se=2015-04-30T02%3A23%3A26Z&sr=b&sp=rw&sip=168.1.5.60-168.1.5.70&spr=https&sig=Z%2FRHIX5Xcg0Mq2rql3OIWTjEg2tYkboXr1P9ZUXDtkk%3D
```

- b. For Amazon S3, choose **AWS S3 STS**, (Simple Token Service). Select the organization and enter the **Access Key** and **Secret Key** for the user.
4. Save the records by pressing **Add New Values**.

### **Modifying existing Cloud Authorization Credentials**

1. Access the **Cloud Auth** tab as described above.
2. In the left-hand table, select the existing cloud authorization record that you wish to modify.
3. Edit credentials as required in the **Cloud Authorizations Values** table.
4. Save the modifications by pressing **Update Values** button.

### **Delete existing Cloud Authorization Credentials**

1. Access the **Cloud Auth** tab as described above.
2. In the left-hand table, select the existing cloud authorization record that you wish to modify.
3. Delete the record by pressing **Delete** button.

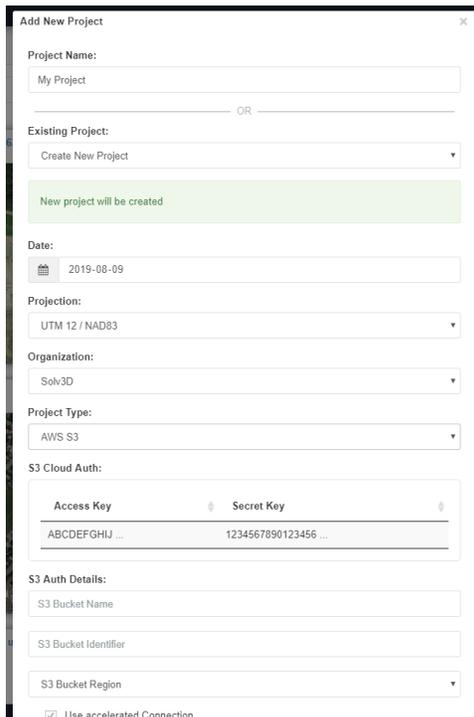
### **Assigning Cloud Authorization Credentials to Projects**

Assuming credentials have been set up by the Organization Administrator, upon creation of a project, the credentials can be assigned, along with additional bucket/URL information that points the location of where the data is hosted.

There are two methods described here, Azure Blob and AWS S3.

## Azure Blob

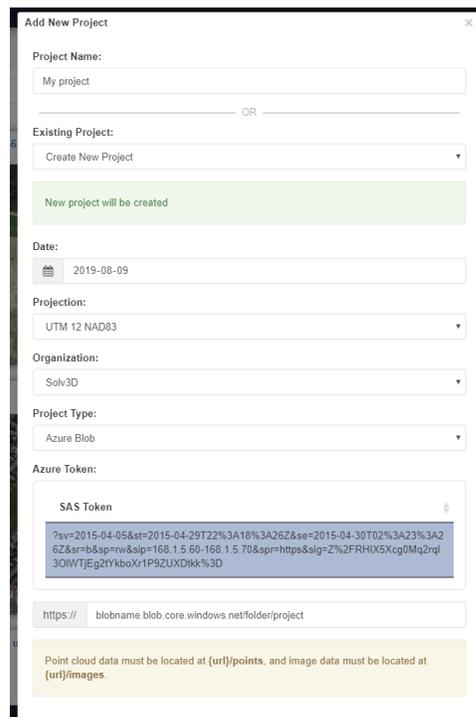
1. Fill in regular project details, including Project Name, Date, Projection and Organization.
2. Select **Azure Blob** as the **Project Type**.
3. Select the **SAS token** that was configured in the Cloud Auth entry above.
4. Supply the **URL** to the blob and include the folder/project path to the location where the **points** and **images** folder is located.
5. Save the project by pressing the **Add Project** button.



The screenshot shows the 'Add New Project' form with the following fields and values:

- Project Name:** My Project
- Existing Project:** Create New Project
- Date:** 2019-08-09
- Projection:** UTM 12 / NAD83
- Organization:** Solv3D
- Project Type:** AWS S3
- S3 Cloud Auth:** Access Key: ABCDEFGHIJ ...; Secret Key: 1234567890123456 ...
- S3 Auth Details:** S3 Bucket Name, S3 Bucket Identifier, S3 Bucket Region
- Use accelerated Connection

Azure  
AWS



The screenshot shows the 'Add New Project' form with the following fields and values:

- Project Name:** My project
- Existing Project:** Create New Project
- Date:** 2019-08-09
- Projection:** UTM 12 NAD83
- Organization:** Solv3D
- Project Type:** Azure Blob
- Azure Token:** SAS Token: ?sv=2015-04-05&st=2015-04-29T22%3A18%3A26Z&se=2015-04-30T02%3A23%3A26Z&sr=b&sp=rw&slp=168.1.5.60-168.1.5.70&spr=https&sig=Z%2FRHX5Xcg0Mq2rqI3OIWtJEg2YkboXr1P9ZUXDkk%3D
- URL:** https:// blobname.blob.core.windows.net/folder/project
- Note:** Point cloud data must be located at (url)/points, and image data must be located at (url)/images.

## AWS S3

1. Fill in regular project details, including Project Name, Date, Projection and Organization.
2. Select **AWS S3** as the **Project Type**.
3. Select the Access Key and Secret Key that was configured in the Cloud Auth entry above.
4. Supply the S3 Bucket Name, Bucket Identifier (folder/project path within the bucket to the location where the **points** and **images**), and Bucket Region that the bucket is configured in.
5. Choose **Use accelerated Connection** if the bucket has been configured for this.
6. Save the project by pressing the **Add Project** button.