

System Integrations | S3 | How to Reset Access Key

S3 - Customer Managed

Please work with your AWS team to change the keys and then update the new keys in S3 connector (Under Connectors 2.0 page).

1. Log in to the AWS Management Console.
 2. Navigate to IAM → **Users**, and pick the user whose key you want to reset.
 3. Go to the **Security credentials** tab → the **Access keys** section.
 4. Create a **new access key**: choose **Create access key**. The console will show you **Access Key ID + Secret Access Key. Make sure to copy / download them immediately** — the secret key can't be retrieved later.
 5. Update your applications/CLI scripts to start using the new key pair. For example, if using the AWS CLI, re-run `aws configure` or update your credentials file.
 6. After confirming everything works with the new key, **deactivate** the old key and then **delete** it. This avoids leaving redundant credentials lying around.
-

S3 - GS Managed

This article provides information on how admins can reset the Access Key for Gainsight S3 Managed Buckets.

Update Access Key

Amazon S3 bucket is a database used to store CSV/TSV data files. When a connection to your S3 bucket is established from your Gainsight org, you can fetch data from these files into Gainsight objects, using Rules Engine, Data Designer, and Adoption Explorer.

To avoid security risks, Gainsight recommends updating the Access Key every 180 days.

IMPORTANT:

- Only super admins can view and manage S3 keys for both Gainsight-managed and customer-managed S3 buckets.
- Non-super admins, even if they have access to the connector's page through permission bundles, can no longer view or rotate the S3 keys.
- Gainsight support teams can no longer have access to S3 keys, even when granted access through support channels. This further reduces the risk of unintended exposure to sensitive information.
- After resetting the credentials, you need to update all third-party systems that are either pushing data into this bucket or reading from it with the new credentials.

For more information on how to check all the rules and connectors reading from S3, refer to the [Identify Rules and Connector Jobs Reading from S3](#) article.

Note: You can identify the source system based on the file name configured in the rules. Make sure any source systems that drop data into S3 (as identified by the rules) are updated with the new keys so that there is no interruption in data flows.

To update the Access key:

1. Navigate to **Administration > Connectors**.
2. Click **View S3 Config**. The S3 Configuration page appears.

The screenshot shows the 'Connectors' page with a search bar at the top. Below the search bar, there are tabs for 'S3 CONNECTOR' and 'ZENDESK CONNECTOR'. The 'S3 Configuration' section is active, and a 'View S3 Config' button is highlighted in the top right corner. Below this, there is a table with the following columns: Data Ingest Job, Matrix Data-Object, Operation, Encryption, Schedule Freq., and Schedule Time. The table contains one row with the following values: 'Usage Data Ingest', 'Usage Data', 'Upsert', 'No', 'Not Set', and 'Not Set'. A '+ DATA INGEST JOB' link is also visible.

Data Ingest Job	Matrix Data-Object	Operation	Encryption	Schedule Freq.	Schedule Time
Usage Data Ingest	Usage Data	Upsert	No	Not Set	Not Set

3. Click the *Reset* icon next to the **Access Key**. Reset Access Key dialog appears.
4. Click **Proceed** to reset.

S3 CONNECTOR ZENDESK CONNECTOR

S3 Configuration Hide S3 Config

S3 bucket provider: Gainsight

Bucket Access Path: s3://gsext-us1tenantbucket/system-defined/12b152b0-b086-4cfc-bd39-3660b6222cbf

Access Key: Ⓢ

Security Token: Ⓢ

Click to Test TEST

Upload your files to
s3://gsext-us1tenantbucket/system-defined/12b152b0-b086-4cfc-bd39-3660b6222cbf/MDA-Data-Ingest/input

BACK

IMPORTANT: After resetting the credentials, you need to update all third-party systems that are either pushing data into this bucket or reading from it with the new credentials.

For more information on how to check all the rules and connectors reading from S3, refer to the [Identify Rules and Connector Jobs Reading from S3](#) article.

Note: You can identify the source system based on the file name configured in the rules. Make sure any source systems that drop data into S3 (as identified by the rules) are updated with the new keys so that there is no interruption in data flows.