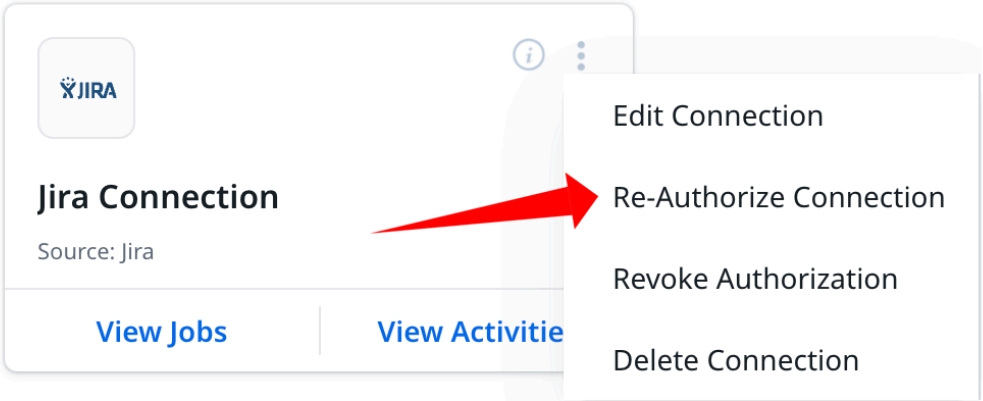
System Integrations | Rotating Keys & Reauthorization

Jira

- Click on the three dots on the Jira connection.
- Revoke Authorization: This option revokes the connection between Gainsight and Jira.
- Authorize Connection: After clicking "Authorize," the Jira OAuth page opens in a new tab. Complete the authorization by entering the Jira organization credentials.

For more information, please refer to the [JIRA support article](#).



Freshdesk

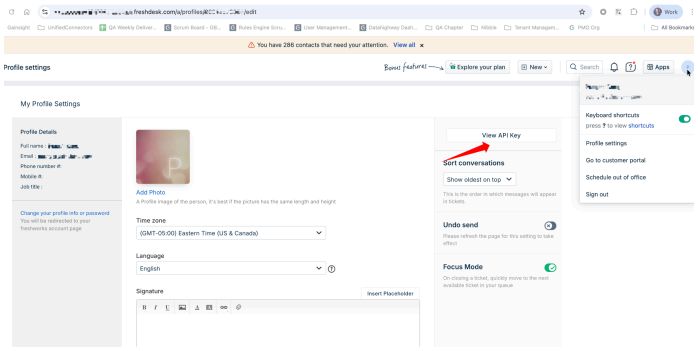
To update the Gainsight connection with Freshdesk, you must first log in to Freshdesk, reset the current ACCESS_KEY, and then use the newly generated ACCESS_KEY to configure the Gainsight connection.

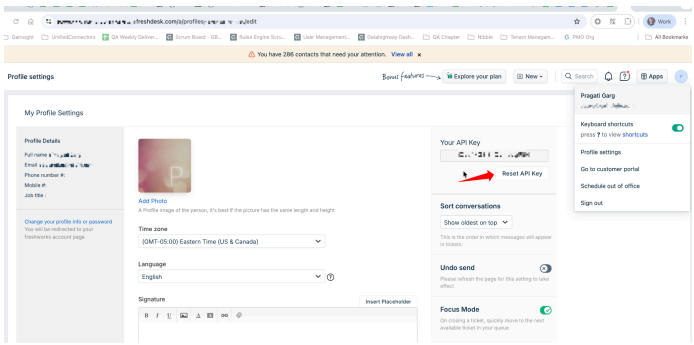
How to Reset and Update Your Freshdesk API Key

1. Log in to **Freshdesk**.
2. Click your Profile picture from the top-right corner.
3. Select **Profile Settings**.

In the API Key section on the right, click **View API Key** , and select **Reset API Key**.A new API key Is generated.

4. Copy the new key and update it on the Gainsight Connectors 2.0 page as follows.





For more information, please refer to the [Freshdesk Support Article](#).

Zuora

There is no Reauthorization option available from within Gainsight. You must reset your client ID and client secret in Zuora.

Snowflake

Prerequisites

Before you start, identify:

- **Which auth type your Gainsight and Snowflake connection use:**
  - Basic (username & password)
    Note: *Username and Password authentication will be deprecated, contact Snowflake Support for guidance if needed*
  - OAuth (through a Snowflake **SECURITY INTEGRATION**).
  - Key pair (RSA public key on a Snowflake user).
- **Which Snowflake principals are dedicated to Gainsight. Examples:**
  - **User**: `GS_GAINSIGHT_USER`
  - **Security Integration (OAuth)**: `GAINSIGHT`
  - Any dedicated Warehouse, Database, Schema, and Views used only by Gainsight.

Use these commands to discover relevant objects, with the patterns adjusted to match your naming:

```sql
SHOW USERS LIKE '%GAINSIGHT%';
SHOW SECURITY INTEGRATIONS LIKE '%GAINSIGHT%';
```

IMPORTANT: Replace the example names with your actual user, role, and integration names.

Rotate Credentials

Use this section if you want to improve security by rotating credentials, but keep Gainsight connected to Snowflake.

Basic (Username/Password)

If you are still on Basic auth, Gainsight recommends migrating to OAuth or key Pair. Please contact Snowflake Support for guidance if needed. While on Basic Auth, rotate the password regularly as follows:

1. **Set a new strong password on the Snowflake user**

```sql
ALTER USER "GS_GAINSIGHT_USER" SET PASSWORD =
'<NEW_STRONG_PASSWORD>';
```

   - Use a long, random password.
   - Do *not* disable the user.

2. **Update the password in Gainsight**

   1. Navigate to the **Connectors** page in Gainsight.
   2. Edit your Snowflake connection that uses Basic auth.
   3. Enter the new password and save.

3. **Validate**

   - Test the connection from Gainsight by creating a new job or running a job.
   - In Snowflake, you can check LOGIN_HISTORY for the Gainsight user if you need audit confirmation.

If you are ready to *deprecate* Basic auth (recommended), here are the steps to disconnect:

1. Rotate or invalidate the password, then disable the user:

```sql
ALTER USER "GS_GAINSIGHT_USER" SET PASSWORD =
'<NEW_RANDOM_PASSWORD>';
ALTER USER "GS_GAINSIGHT_USER" SET DISABLED = TRUE;
```

2. Drop the user if it is dedicated to Gainsight and no longer needed:

```sql
DROP USER IF EXISTS "GS_GAINSIGHT_USER";
```

OAuth / Security Integration

In this model, Gainsight connects to Snowflake using an OAuth **SECURITY INTEGRATION**.

Typical rotation actions:

1. Rotate secrets, or tokens, at your IdP or OAuth provider
    a. Follow your IdP or Snowflake OAuth provider's document to:
        - Rotate client secrets (if applicable), and/or
        - Revoke old refresh tokens.
2. Update the SECURITY INTEGRATION in Snowflake (if you changed any parameters)

    For example, to update properties on an existing integration:

```sql
ALTER SECURITY INTEGRATION "GAINSIGHT"
  SET <property> = <new_value>;
```

3. *(Optional)* Fill in the properties you changed, such as OAUTH_CLIENT_SECRET.
4. Update configuration in Gainsight
    1. In Gainsight Connectors, edit the Snowflake connection that uses OAuth.
    2. Ensure it points to the correct Security Integration and any rotated OAuth details.
    3. Re-authenticate if the UI prompts you to.

5. Validate

    1. Test the connection from Gainsight by creating a new job or running a job.
    2. Optionally verify in Snowflake that the integration is in the ENABLED status:

```
SQL
SHOW SECURITY INTEGRATIONS LIKE 'GAINSIGHT';
```

Note: Do not drop the Security Integration if your intent is only token and secret rotation.

Key Pair (RSA)

Snowflake supports having two public keys per user (`RSA_PUBLIC_KEY` and `RSA_PUBLIC_KEY_2`) to enable zero-downtime key rotation.

Recommended pattern:

1. Generate a new private key on your workstation.

```
Shell
openssl genrsa 2048 | openssl pkcs8 -topk8 -inform PEM -out
rsa_key_new.p8 -nocrypt
```

2. Generate the new public key.

```
Shell
openssl rsa -in rsa_key_new.p8 -pubout -out rsa_key_new.pub
```

3. Add the new public key to the Snowflake user.

    If you are currently using `RSA_PUBLIC_KEY`, attach the new one to `RSA_PUBLIC_KEY_2`:

```sql
ALTER USER "GS_GAINSIGHT_USER"
  SET RSA_PUBLIC_KEY_2 = '<NEW_PUBLIC_KEY_CONTENTS>';
```

4. Update Gainsight to use the new private key

    a. Navigate to the Gainsight Connectors page.
    b. Edit your Snowflake connection that uses key pair auth.
    c. Upload rsa_key_new.p8 as the private key.
    d. Save and test the connection.

5. Remove the old public key after successful cutover,nce you have confirmed successful connections using the new key:

```sql
ALTER USER "GS_GAINSIGHT_USER" UNSET RSA_PUBLIC_KEY;
```

6. Or, if you flipped which key is **active**, unset the unused one accordingly:

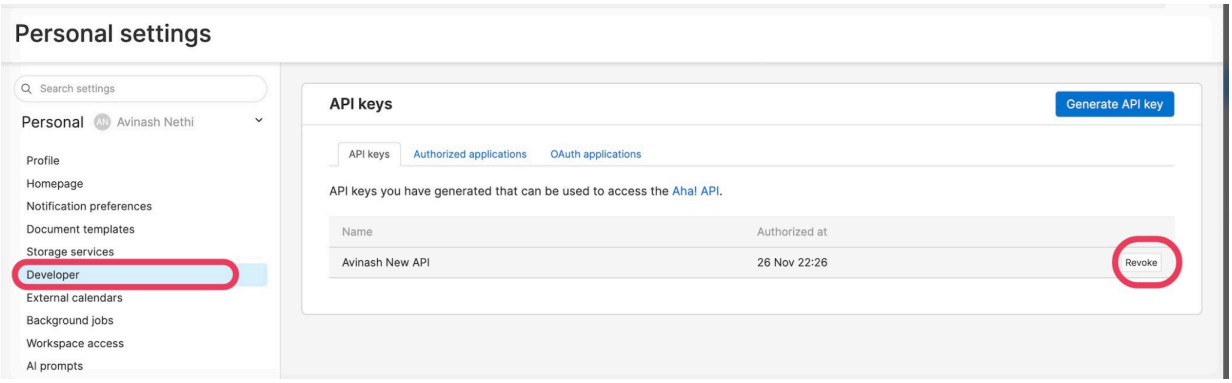
```sql
ALTER USER "GS_GAINSIGHT_USER" UNSET RSA_PUBLIC_KEY_2;
```

7. Validate - Test the connection from Gainsight by creating a new job or running a job.

IMPORTANT: Gainsight strongly recommends allow-listing Gainsight's IP addresses in your Snowflake account/network. Please raise a Gainsight support ticket to obtain the most up-to-date IP list. Ensure these IPs are allow-listed before creating or re-establishing the connection.

AHA

The AHA access key is provided by the AHA team. Reach out to the AHA administrator to revoke and create a new key within AHA and subsequently update the key in the AHA connection.



Product Board

The Product Board access key is provided by the Product Board team. Reach out to the Product Board administrator to reset the API key within the Product Board, and subsequently update the new key in the Product Board connection.

Ecosystem

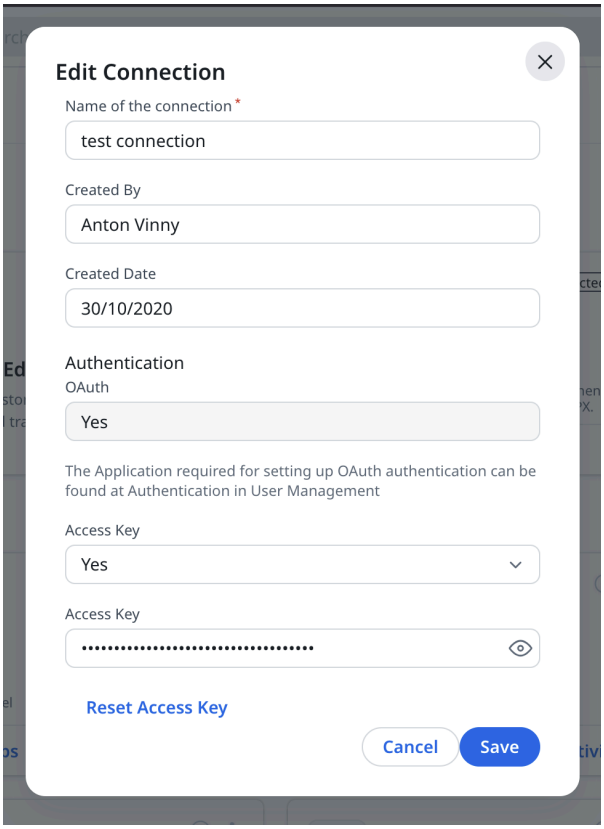
For more information on the Ecosystem integration, please refer to the [Ecosystem Connector support article](#).

Bulk API

For Bulk API integration:

1. Navigate to the Connectors 2.0 page,

2. Edit the connection and reset the access key.
3. Click **Save**.

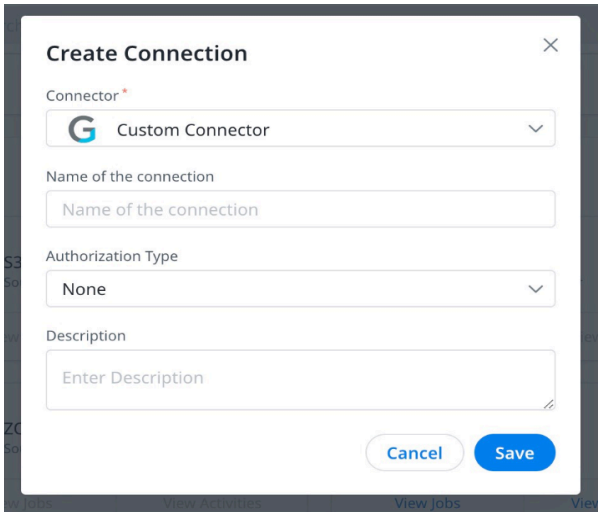


Bulk API (OAuth)

Delete the existing Auth Application and recreate it in User Management. To delete the existing Auth application, navigate to **User Management > Authentication > OAuth Application**.

Custom Connector (REST_API)

Since the custom connector's authentication is managed and generated within the external system you are connecting to, Gainsight advises obtaining new credentials directly from that external system and then updating the Custom Connectors with those new credentials.



For more information on custom connectors, please refer to the [Configure Custom Connectors support article](#).

SAP Datasphere

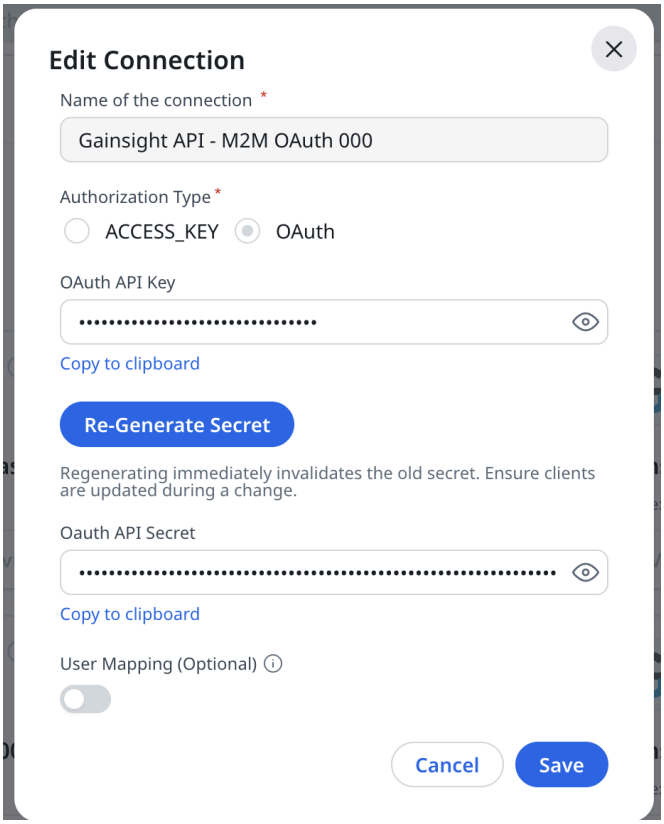
Reset the password in SAP Datasphere and update the new password in the connection.

Gainsight API (GS API) Access Key

The customer can reset the key from the Gainsight API Card. For more information on the Gainsight API access key, please refer to the [Generate REST API Key support article.](#)

Gainsight API (GS API) M2M

Customers will be able to resolve this either by regenerating the secret on the existing connector from January 9th onward, or by recreating the connection entirely.



EventStream

Delete the existing Auth Application and recreate it in User Management. To delete the existing Auth application, navigate to **User Management > Authentication > OAuth Application**.

BigQuery

Disconnecting Procedure

Connection auth type used in Gainsight:

- OAuth
- Service Account

Remove authentication surface OAuth, or Service Account.

A) If OAuth is used

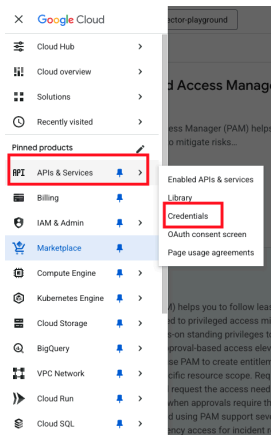
Permissions or IAM Roles Required for managing (or deleting) an OAuth Client.

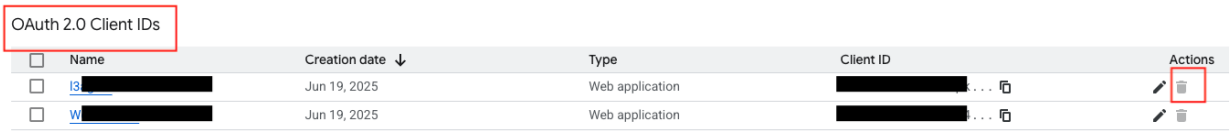
You need the roles/iam.oauthClientAdmin role on the project to create, update, or delete OAuth clients. For more information, please refer to the Manage OAuth application article.

Steps to Invalidate:

1. Open Google Cloud Console → APIs & Services → Credentials.
2. Under **OAuth 2.0 Client IDs**, locate the OAuth Client you want to turn off.
3. Ensure you have the 'roles/iam.oauthClientAdmin' permission (or equivalent).
4. Click the **OAuth Client** name.
5. Click DeleteDELETE to remove the OAuth Client ID or /Secret (there is no “disable” option).
6. Confirm deletion.

After deletion, any application using that Client ID or Secret stops working immediately.





B) If Service_Account is used (For disabling or deleting a Service Account)

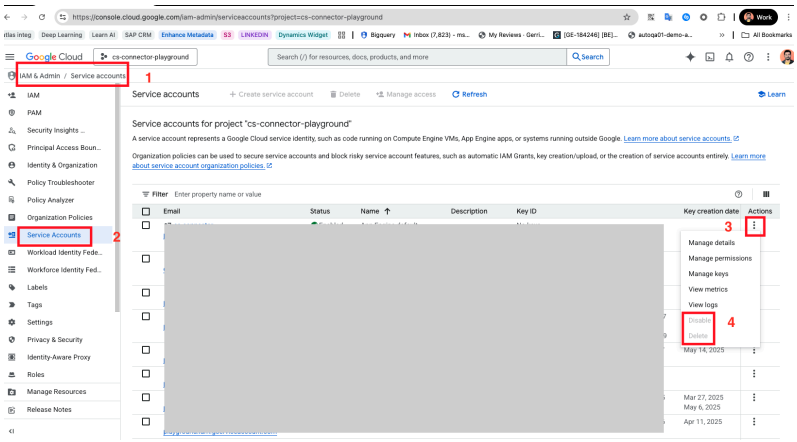
Permissions or IAM Roles Required

- You need the **roles/iam.serviceAccountAdmin** role on the project (or on the service account) to manage (disable/enable/edit) service accounts. Please refer to Google Cloud documentation.
- If you only need to disable or manage service account keys, you may need **roles/iam.serviceAccountKeyAdmin**. Please Refer to the Google Cloud Documentation for more information.

Steps to Invalidate (Delete Service Account)

1. Open **Google Cloud Console > IAM & Admin > Service accounts**.
2. Select the Project.
3. Find the service account to disable.
4. Ensure you have the 'roles/iam.serviceAccountAdmin' permission on the project (or account).
5. Under **Service account status,** click the service account name
6. Click Disable service account

Click **Confirm**. Once disabled, the service account cannot be used for authentication, and any workloads depending on it will fail.



Reconnecting Procedure

A) If OAuth was used

To reconnect BigQuery using OAuth, please refer to the BigQuery Connector support article.

B) If Service Account was used

To reconnect BigQuery using OAuth, refer to the [BigQuery Connector support article](#).

Dynamics

To re-authorize a Dynamics connection in Gainsight, follow these steps:

When a customer connects to Gainsight using an **M2M OAuth or Certificate flow**, they create credentials in their own Azure Entra ID tenant. Gainsight cannot modify or remove these credentials.

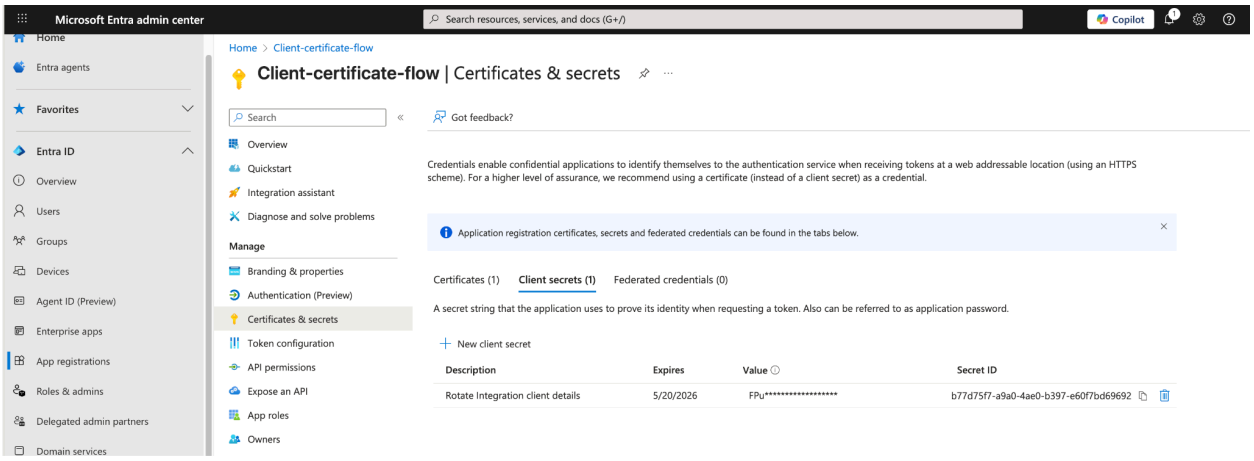
Therefore, the customer must perform the disconnection steps on their side.

If the customer created a *Client Secret*:

During initial M2M connection setup, customers generate a Client Secret in Azure Entra.

To disconnect:

1. Navigate to **Azure Portal >Entra ID > App Registrations.**
2. Open the App Registration used for Gainsight M2M.
3. Navigate to Certificates & Secrets.
4. Under Client Secrets, delete the secret that was created for Gainsight.



If the customer created a *Certificate*:

Some customers use certificate-based M2M authentication.

To disconnect:

1. Navigate to **Azure Portal > Entra ID > App Registrations.**
2. Open the relevant App Registration.
3. Navigate to Certificates & Secrets.
4. Under Certificates, delete the certificate used for Gainsight M2M.

Once the secret or certificate is removed, all M2M calls from Gainsight will immediately stop working.Gainsight does not need to perform any additional steps for disconnection.

Reconnecting Procedure (Customer Action Required)

If you want to reconnect after deleting the credential, you can follow the same steps they used during initial M2M setup.

Reconnection Steps

A. Create new credentials in Azure Entra

1. Navigate to **Azure Portal > Entra ID > App Registrations**
2. Open the same App Registration used earlier (or create a new one if they prefer).
3. Generate a new credential:
    a. Option 1: Add New Client Secret
       → Certificates & Secrets → New Client Secret
    b. Option 2: Upload New Certificate
       → Certificates & Secrets → Upload Certificate

B. Update the credentials in Gainsight

Once the new secret or certificate is created:

1. Log in to Gainsight.
2. Navigate to Connectors.
3. Select Edit Connection.
4. Replace the old credential with the new client secret or certificate.
5. Save and test the connection. Existing jobs should start working.

Databricks

We don't have re-authorization for this connection.

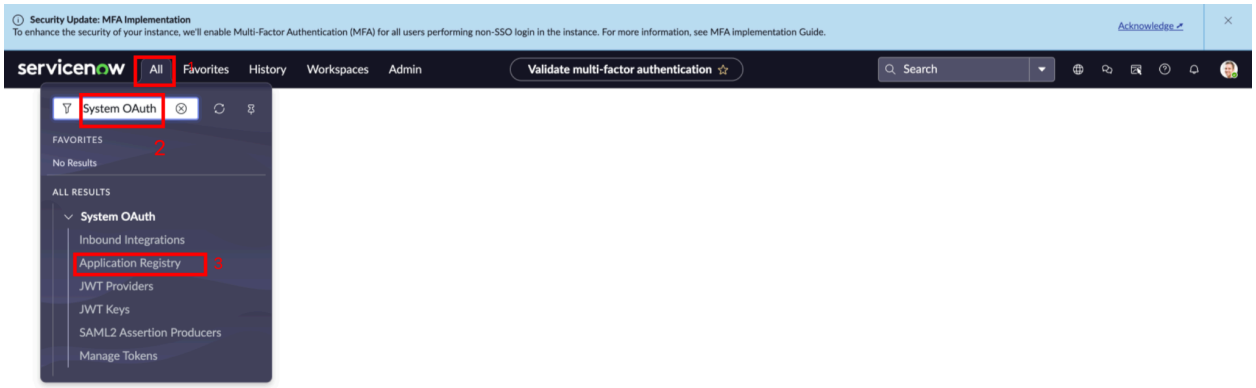
- For Username/Password: Request the user to update their password at the source.
- For OAuth: Need to reset their Client ID and Client Secret.

ServiceNow

Disconnecting Procedure

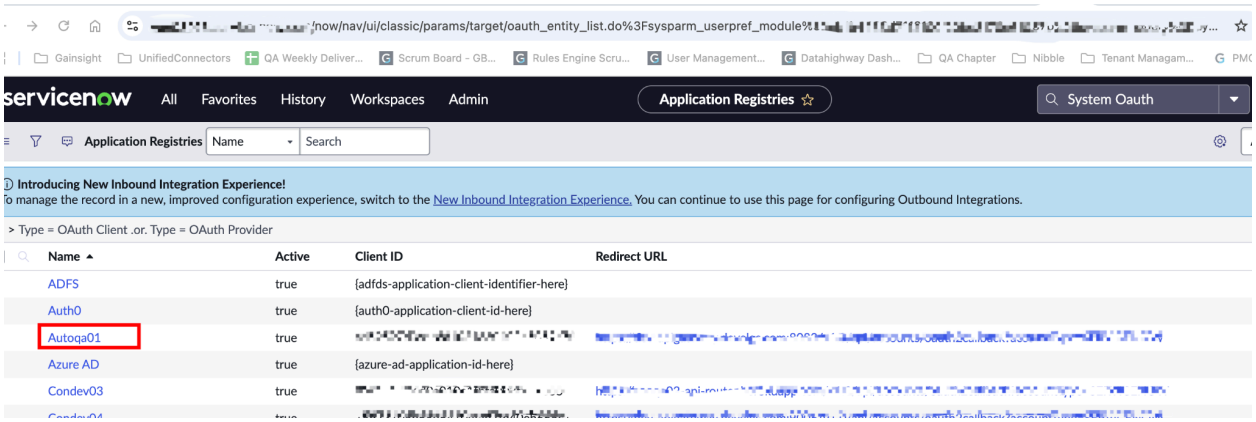
1. Navigate to the Application Registry

To find this in ServiceNow, use the left navigation menu to search for `System OAuth` → `Application Registry`, or type **Application Registry** in the filter.



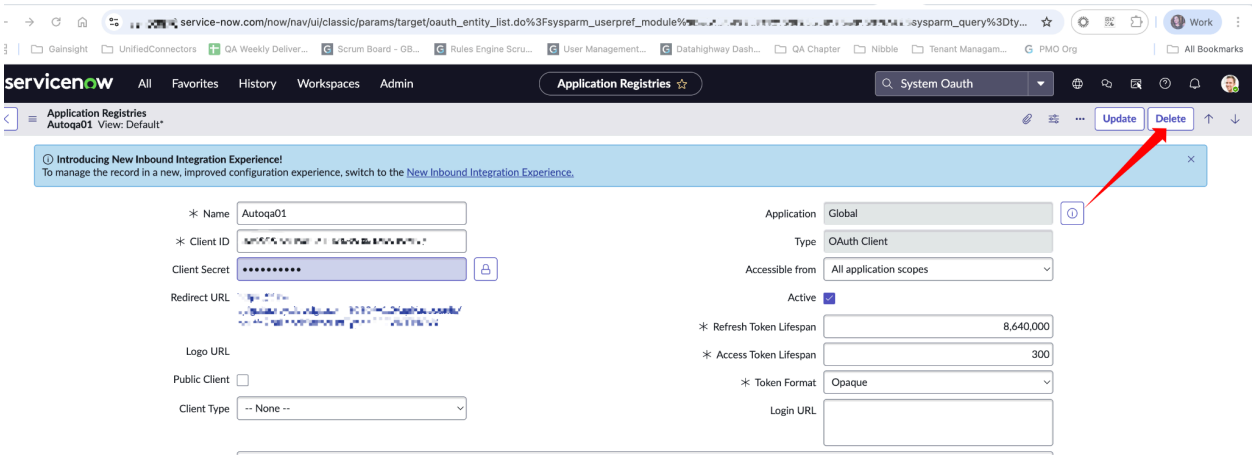
2. Open the OAuth App You Want to Delete

Click the application entry you want to remove.



3. Check for Related Tokens (Client ID)(Optional but recommended)

4. Click Delete.



Reconnecting Procedure

Please refer to the support article here.

S3 - Customer Managed

Please reach out to your AWS team to change the keys, as the custom bucket is owned by customers, and update the new keys in S3 connector (under the Connectors 2.0 page).

Log in to the AWS Management Console

1. Navigate to IAM → **Users**, and pick the user whose key you want to reset.
2. Go to the **Security credentials** tab → the **Access keys** section.
3. 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.
4. 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.
5. 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

Rotate S3 Keys - Please refer to the support article here.

Segment (only supported for US data centers)

The key needs to be reset, and the Segment team must be informed to update the key on their system. Please refer to the support article here.

Mixpanel

We are currently using the Mixpanel access key (generated by Mixpanel) in our connector. The Mixpanel admin can revoke the existing key, generate a new one, and update from the Connectors page in CS.

Google Analytics

1. Go to Adoption Explorer > Administration.
2. Click on your project name.
3. In the "Objects in Project" section, select the object where Google Analytics is configured.
4. Click the Edit Source icon next to the Google Analytics connection.
5. In the source connection settings, look for an option to remove or reauthorize the Google Analytics source.

6. Save your changes.

Postgres, MySQL, or Redshift

Please contact your database administrator to update the connection's username and password. Once updated, follow the instructions here to update the credentials in Adoption Explorer.