Reporting Api Credentials

Reporting Api Credentials

Purpose and when to use this record

Grant a named integration narrowly scoped, expiring access to reporting data, optionally restricted by source network.

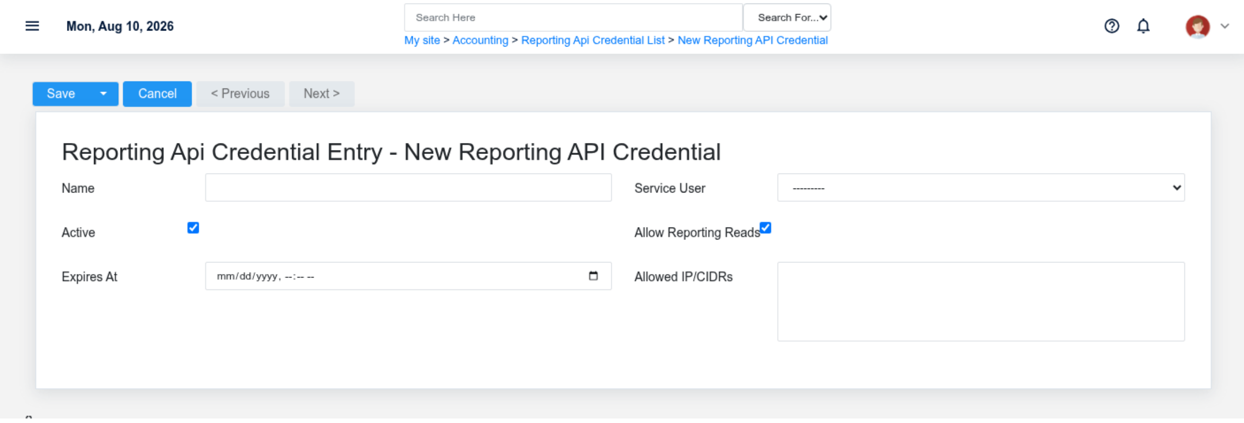
At a glance

- **Identify it by: Name**.
- **Check its business context: Service User**.
- **Why care:** Availability and publication flags affect future use without erasing history. Prefer disabling an obsolete setup record when existing transactions still refer to it.
- **Why care:** Grant the smallest capability and shortest practical lifetime. Treat any generated secret as confidential; copy it at creation time and never place it in notes or screenshots.

Before you begin

You need the Brisk permission for the action you are taking on reporting api credentials. If a Create, Edit, or Delete control is absent, do not work around it with another user’s account; ask an administrator to review your role.

Create a Reporting API Credential



The Reporting Api Credentials create screen in the Brisk documentation demo.

Create a Reporting API Credential for one identifiable integration or device. Do not share one credential across unrelated systems because revocation and audit history would become ambiguous.

1. Select the business context first: **Service User**.
2. Enter the required identifying and operational values: **Name**.
3. Review **Active**, and **Allow Reporting Reads** deliberately; these choices control availability or workflow rather than merely describing the record.
4. Save the Reporting API Credential, then confirm **Name** on its detail page before continuing.

After saving: Give the generated secret only to the named integration, test reporting access from an allowed network, and record the expiration/rotation plan outside the credential itself.

Delete a Reporting API Credential

Disable or revoke this Reporting API Credential when access must stop. Delete it only after its audit value is no longer needed and the integration has been moved to a replacement credential.

If the record is merely obsolete, use **Active** to remove it from future use while preserving existing references.

On the confirmation page, verify **Name**. After confirmation, return to the Reporting API Credentials list and make sure only the intended Reporting API Credential was removed.

Review Reporting API Credential details

Use the detail page as the shared record of what this Reporting API Credential currently means. Verify **Active** before relying on it for a decision.

Follow **Service User** to determine whether the issue is on this Reporting API Credential or on one of those linked records.

Next check: Give the generated secret only to the named integration, test reporting access from an allowed network, and record the expiration/rotation plan outside the credential itself.

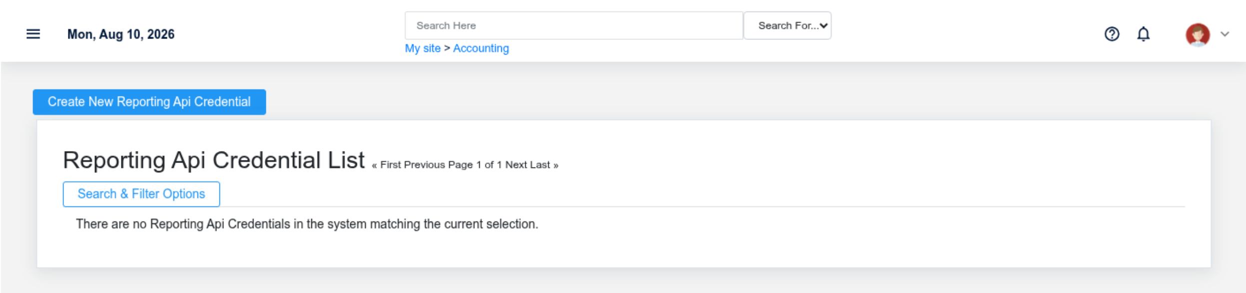
Edit an existing Reporting API Credential

Edit this Reporting API Credential to reduce access, rotate ownership, set an expiration, or disable the integration. Create a separate credential when the calling system changes.

1. Open the detail page. Compare **Service User** with the supporting document or approved request.
2. Recheck **Active**. These values are most likely to change account balances, financial periods, and statement results.
3. Save the change, return to the list, and confirm that the Reporting API Credential now appears under the expected **Active**.

After the change: Give the generated secret only to the named integration, test reporting access from an allowed network, and record the expiration/rotation plan outside the credential itself.

Find and review reporting api credentials



The Reporting Api Credentials list screen in the Brisk documentation demo.

Use the Reporting Api Credentials list to find the correct record before opening or changing it. Compare **Name**. Records with similar names or numbers can still belong to different **Service User**.

- Keyword search checks **Name**, and **Last Used Ip**.
- Narrow the list with **Service User** filters.
- The initial order emphasizes **Name**. Select a column heading when you need a different comparison.

Open the Reporting API Credential whose **Name** match the task. If it is missing, clear the list filters and recheck **Service User**, and **Active** rather than creating a replacement immediately.

Fields and business rules

Brisk stores 6 user-relevant fields for this Reporting API Credential, including 1 linked-record selection and 0 controlled-choice fields. Create and edit screens may hide calculated or workflow-managed values from this full reference.

Field	Required	What it controls
Name	Yes	Human-readable name for this reporting API credential.
Service User	No	Optional human owner for this credential.
Active	No	Whether this reporting API credential is active.
Allow Reporting Reads	No	Whether this reporting API credential allows read reporting.
Expires At	No	Date and time recorded for expires at on this reporting API credential.
Allowed Ip/Cidrs	No	Optional newline/comma-separated list of allowed IP or CIDR ranges.

What happens next

Give the generated secret only to the named integration, test reporting access from an allowed network, and record the expiration/rotation plan outside the credential itself.

Common mistakes and troubleshooting

- **The record will not save:** Recheck **Name** and any message beside the field. A required related record may also be inactive or unavailable to your role.
- **The record saved but is not available where expected:** Recheck **Active**, then clear the filters on the destination list. A saved record can still be inactive, unpublished, locked, unapproved, or in the wrong workflow state.
- **The values look right but the result is wrong:** Open **Service User** from the detail page. Correct the specific relationship that is wrong instead of forcing a total or status to compensate for it.

Revision #4
Created 2026-08-10 16:07:25 UTC by Brisk

Updated 2026-08-10 20:24:15 UTC by Brisk