



DATABLAU · DAM

Data service

Product module user manual

Version 9.1.2

Contents

- 01** Data services
 - 02** Data services quick start
 - 03** Develop and publish APIs
 - 04** Discover and request APIs
 - 05** Manage applications and authorization
 - 06** Review requests and monitor calls
-

Data services

Manage APIs and calling applications. Developers create, test, and publish APIs; consumers discover/request them; administrators review requests and monitor calls. This differs from marketplace product requests and offline delivery.

Choose a task

Task	Guide	Verify
Discover services	API marketplace	Endpoint, parameters, response
Develop/publish	API development	Tested and discoverable
Create/request an application	Applications	State, credentials, grants
Review/monitor	Approvals	Traceable decisions and calls

Start with [Quick start](#).

Understand objects

Object	Meaning	Relationship
API	Data access interface definition	Market entry after testing/publication
Application	Calling identity	Requests APIs and can be shared by approval
API request	Application's right to an API	Verify grant/validity after review
Application request	Use another owner's application	Separate approval
Call record	API/application monitoring	Not data delivery evidence

Before you begin

Administrators assign feature rights and development, application, request, and review responsibilities. Engineers prepare definitions, test sources, applications, and purposes. Visibility is not invocation authorization. Role names in source material describe responsibilities and can be customized.

Distinguish the marketplace

Data Marketplace discovers business assets/products and records requests with offline fulfillment. Data Services develops, publishes, authorizes, and invokes APIs. Their request objects and results differ.

Data services quick start

Develop, test, publish, request, and verify one approved API. Prepare source, owner, reviewer, and test account. Avoid sensitive production data for first tests.

1. Prepare an application

Create under My Created Applications, specify purpose, inspect state, and protect credentials. [Request another application](#) rather than borrowing keys.

2. Create and test

Create in My Developed APIs. Verify parameters, results, and errors. Passing one test is a publication prerequisite, not complete input/permission coverage.

3. Publish

Follow [API development](#), then inspect market parameters/responses. Use supported unpublish/edit workflows and notify consumers before contract changes.

4. Request use

Select API, application, and duration. After administrative review, inspect My Requested APIs and invoke as the authorized application. Approved status alone does not prove correct responses.

5. Verify

Run controlled calls and correlate monitoring. On failure check application/API states, validity, inputs, and logs.

Completion criteria

Discoverable API, matching approval/grants, successful controlled application call, traceable monitoring. Missing menus require license/role checks.

Develop and publish APIs

My Developed APIs manages owned interfaces. Manage APIs provides administration of published interfaces, users, and monitoring. Define source, scenario, parameters, response fields, and access boundaries first.

Create an API

1. Open **Data Services > My Developed APIs > Add**.
2. Complete configuration, purpose, parameters, and returned data.
3. Save and compare details with the intended source.
4. Test controlled inputs, empty results, and invalid inputs.

Use the current form and interface specification for authentication/fields, not other environments' URLs or credentials.

Test and publish

Select **Test** in details. Verify business content even after a success message; on failure check inputs, source, rights, and services. Only tested APIs can publish. Reopen market details afterward to check consumer-facing parameters and responses.

Change, unpublish, and delete

Check whether unpublishing is required before editing. Retest and republish. Existing requests may restrict unpublishing. Review authorizations, applications, current calls, and consumers before unpublishing or deletion. Record affected consumers and communicate contract changes; clickable actions do not establish low impact.

Administrator checks

Use Manage APIs for information, authorized users, and calls. Administrators can test/unpublish published APIs after checking requests. Management tests do not replace consumer acceptance.

Related: [Market](#), [Monitoring](#), [Applications](#).

Discover and request APIs

API Marketplace lists published interfaces. Requests authorize a specific calling application, not an offline data product.

Evaluate an API

1. Search by purpose in API Marketplace.
2. Open configuration, parameters, response fields, and examples.
3. Verify owner, purpose, inputs, and expected results rather than names alone.
4. Review sensitive access requirements and available applications.

Examples explain response structure; actual data depends on inputs, rights, and source state.

Request an API

1. Select **Request** in the list.
2. Choose application and duration.
3. Verify ownership, API, and validity; submit.
4. Administrators process API Review.
5. Check approval/grants in My Requested APIs.

Create an [Application](#) first, or request another owner's application separately.

Return and reapply

Use **Return** on an authorized request where available, then **Reapply** if needed. Check running calls before returning. Verify requested duration, review state, and actual calling eligibility separately.

Troubleshoot

Symptom	Check
Missing API	Tested/published state, visibility
Missing application	Created/requested and usable state
Approved but cannot call	App/API states, validity, inputs, logs
Response differs from example	Conditions, scope, definition changes

Manage applications and authorization

Applications identify API callers. Create your own or request another published application. Application approval and API approval are separate.

Create and enable

1. Open **My Created Applications > Add**.
2. Enter name, ownership, and purpose.
3. Save, inspect state, and enable as needed.
4. Request APIs through the [Marketplace](#).

Check enabled state and current dependencies before editing/deleting. Disablement affects visibility and calls.

Request another application

1. Verify owner/purpose in details.
2. Request review.
3. Administrators use Application Review.
4. Check My Requested Applications, return when finished, and reapply for later use.

Details show information, associated APIs, and access. Associated APIs are not automatically authorized to every applicant.

Administration and credentials

Manage Applications shows authorized users, APIs, and monitoring; administrators can add/remove users. Regenerating appSecret invalidates old client credentials; coordinate rotation first. Keep appKey/appSecret out of manuals, screenshots, repositories, and public tickets. Check calls and approvals before disabling, deleting, or rotating.

Verify results

Confirm application state, users, separate API authorization, and monitored real calls. Application approval alone does not establish API readiness.

Review requests and monitor calls

API and application requests are separate. Verify target, application, duration, and business purpose; applicants check the corresponding request list afterward.

Review API requests

1. Open API Review.
2. Inspect API, application, and period.
3. Approve/reject under policy and record comments.
4. Check state/grant scope; have applicants test calls.

Review application requests

1. Open Application Review.
2. Verify applicant, owner, purpose, and state.
3. Approve/reject and reconcile records with authorized users.
4. Check separate API grants.

Monitor access

Administrators use API/application management details; developers and owners inspect their own calls. Distinguish absent calls, technical failures, and successful calls with incorrect business results. Check identity/grants, configuration, and logs. Assess dependencies and notify owners before stopping applications or APIs.

Understand outcomes

Approval is an access decision; a test is one execution; monitoring proves calls occurred. Validate business content and definitions through controlled calls by the intended application and data-owner review.