



DATABLAU · DAM

System management

Product module user manual

Version 9.1.2

Contents

- 01** System administration
 - 02** System administration quick start
 - 03** Manage application systems and data source connections
 - 04** Configure approval forms, workflows, and monitoring
 - 05** Configure tags, email, and system parameters
 - 06** Manage system calls, drivers, and plugins
 - 07** Understand licenses and feature visibility
 - 08** Diagnose execution and operation issues with logs
 - 09** Manage organizations, users, roles, and groups
 - 10** Configure task schedules and time templates
-

System administration

Manage users, organizations, groups, roles, workflows, tasks, configuration, and licenses. Licensing, feature rights, and object rights are separate layers.

Choose a task

Start with [Quick start](#).

Goal	Guide
Systems and connections	Application systems/sources
Drivers and source plugins	Drivers/plugins
Organizations, users, roles	Access management
Forms, nodes, deployment	Approvals
Recurrence and execution	Scheduling
Tags, email, parameters	Configuration
Missing modules	Licenses
Failures and audit	Logs

Systems/sources are maintained in Metadata Management. Administration supplies calls, drivers, and plugins; business modules own rules/lifecycles.

Roles and rights

Configure roles, members, modules, features, and actions. Administrator, owner, steward, and module administrator are suggested responsibilities, not immutable built-in roles.

Workflows

Approvals use configurable Activiti-based models. Workflow Center, Monitoring, forms, deployment, and modeling support customer-specific nodes, participants, and fields.

Licensing

Licenses control top-level visibility/availability. Standards, metadata, and quality can be licensed separately. Assets, security, lineage, and agents depend on delivered combinations.

System administration quick start

Screenshot note: Screenshots are illustrative. Controls or labels may remain untranslated in the demo release, and pages without a faithful English capture retain the source illustration. Control names and layouts can vary by release.

Prepare organizations, rights, resources, and approvals for initial users. Start with limited scope and organization-defined roles.

Before you begin

Prepare hierarchy, people, responsibilities, systems, sources, and approvals. Obtain administration rights and licensed modules.

Step 1: Confirm features

Inspect Product License Management. Distinguish [Entitlements](#) for metadata/SQLink and Metric Standards/Management. Do not grant every administrator feature to new users.

Step 2: Configure identities and rights

Follow [Access management](#): create hierarchy, define roles, prepare systems and users, add groups for bulk grants/approvals, and test as users.

Configure [Schedules/templates](#) and [Email scenarios](#), including triggers, parameters, and recipients. Verify first outputs and history.

Completion checks

Area	Result
Identity	Correct organization and usable account
Rights	Intended user can perform responsibilities
Resources	Tested sources and drivers
Approvals	Deployed and routed to intended reviewers
Schedules	Correct recurrence/dates and traceable runs

Next: harvest initial objects in [Metadata management](#).

Manage application systems and data source connections

Systems describe business origin; sources hold connection information used by harvesting and quality tasks. Saving a connection does not harvest metadata. Systems/sources reside under Metadata > Harvesting Management; calls/drivers/plugins reside in administration.

Create a system

1. Open Application Systems > New.
2. Enter name, abbreviation, and required information.
3. Verify uniqueness of both name and abbreviation; save.
4. Find and inspect details.

Use Edit for changes and recheck afterward.

Import and export systems

1. Download the current template.
2. Complete new systems without changing columns/formats.
3. Import the saved file.
4. Inspect results and sample names, abbreviations, and properties.

Export uses template format. Check duplicates before importing existing systems as new entries.

Maintain business properties

Add/edit/delete custom text, number, or enumeration properties under Business Properties. Agree meanings and values first; avoid conflicting same-name properties.

Create a source

Prepare type, host, port, database/service identifier, authentication, and ownership. Forms vary by database.

1. Open Data Sources > New.
2. Select type/driver and enter connection information.
3. Use an account with task-appropriate permissions.

4. Test and resolve returned errors.
5. Save after success.
6. View Basic Information and Usage Information.

Basic Information describes connection; Usage Information lists module dependencies. Next configure [Harvesting](#) or [Quality](#).

Change connections and authentication

Edit, save, retest, and inspect affected harvesting/validation tasks after identifying dependencies.

Subscribe

Subscriptions notify supported metadata changes. Delivery also depends on [Email scenarios](#); no email does not establish no change.

Check before deletion

Referenced systems cannot be deleted. Source deletion can break tasks; inspect usage and resolve dependencies. Confirm deletion only for unused objects; do not recreate sources for ordinary credential updates.

Verify and troubleshoot

Symptom	Check
System creation fails	Duplicate names/abbreviations, required fields
Type missing	Source plugin
Connection fails	Network, port, authentication, identifier, driver
Connected but harvest fails	Object rights and scope
No tables/columns	Execute harvesting after registration

Related: [Drivers](#), [Quick start](#), [Scheduling](#).

Configure approval forms, workflows, and monitoring

Maintain definitions in Workflow Center and instances in Workflow Monitoring under System Management > Workflow Management. Marketplace approvals still require offline delivery.

Distinguish four concepts

Concept	Meaning
Scenario	Business approval category
Workflow	Nodes and participants; several can serve one scenario
Instance	One triggered approval
Form	Information collected/displayed

Built-in workflows cannot be deleted. Configurability does not imply identical nodes/approvers.

Edit forms

1. Select scenario/workflow.
2. Edit Form.
3. Inspect existing fields and add required properties.
4. Set unique codes and value types.
5. Save and test a request.

Types include text, number, date, and user. Approver expressions can resolve people dynamically; department-manager routing requires accurate organization/leadership data. Follow actual expression syntax.

Create and model

1. Select scenario and New Workflow.
2. Give it a distinct name.
3. Edit the model.
4. Configure nodes, participants, and conditions.

5. Verify all start/approval/end paths and save.

Activiti provides modeling. Administrators design; applicants use deployed workflows.

Deploy and verify

1. Deploy the saved definition.
2. Confirm deployment success.
3. Submit a controlled business request.
4. Inspect actual participants/path in Monitoring.
5. Test required approval/rejection paths and forms.

Saving is not deployment. Definition edits do not necessarily change running instances.

Inspect instances

Check name, initiator/department/time, state, and current reviewer. View historical nodes. Diagnose the stalled node and participants/organization/parameters before resubmitting duplicates.

Deletion restrictions

Built-in, business-referenced, or unfinished-instance workflows cannot be deleted. Resolve dependencies first.

Troubleshoot

- Old routing: deployment and actual selected workflow.
- Missing/wrong reviewer: form property, expression, organization.
- Missing tasks: current reviewer, account, rights.
- Evidence: retain instance/node history, not definition screenshots alone.

Configure tags, email, and system parameters

Shared settings affect multiple modules. Record original values and scope before changes.

Maintain tags

Tags follow group, folder, tag hierarchy.

1. Open Configuration Management > Tag Management.
2. Add a group above the tree.
3. Add a folder, then tags/properties.
4. Save and inspect details.
5. Tag business objects and verify references.

Recheck search/classification after edits. Referenced tags cannot be deleted. **Remove References disconnects every reference for the tag**, not one selected object. Inspect scope before using it.

Configure email servers

1. Edit server settings in Email Settings.
2. Enter organizational server/delivery information.
3. Verify configuration/account validity.
4. Enable each required business scenario and review templates.

A working server does not enable every scenario. Disabled scenarios send nothing despite triggers.

Edit templates

1. Select scenario and Email Template.
2. Edit subject/body.
3. Insert dynamic values from the parameter list at the cursor.
4. Verify meanings, such as recipient or changed source.
5. Decide attachments under policy and save.

Parameters resolve at send time; fixed text does not. Attachments vary by scenario.

Change control-panel parameters

Confirm module, purpose, valid values, and impacts; record old/new values and verify in the business module. Do not guess or copy another environment.

Troubleshoot

Symptom	Check
Cannot delete tag	References
Fewer tag results	Removed/changed associations
Missing notification	Scenario, trigger, server, recipient
Fixed/missing message values	Dynamic parameters
Unexpected behavior	Changed settings, documentation, restore original if needed

Related: [Users](#), [Workflows](#).

Manage system calls, drivers, and plugins

Under System Management > Data Source Management, calls record system relationships, drivers connect databases, and plugins provide integration, reverse engineering, and parsing. Plugins are direct harvesting prerequisites.

Register system calls

1. Open System Calls > New.
2. Enter caller, callee, and relationship information.
3. Verify source/database, resource, reference method, and function description.
4. Save, search, and check direction.

Search by source/database, resource, and description; lists show caller/callee and recording users. Manual relationships do not replace SQL/ETL lineage. Edit/delete after verification. For bulk registration, download the template, Import Calls, and sample direction afterward.

Add drivers

1. Select the database type in Driver Management.
2. Upload an approved compatible driver.
3. Verify it appears under the correct type.
4. Set the default driver.
5. Create/test a source and verify initialization.

Defaults initialize new sources; existing sources do not necessarily switch.

Replace or delete

Referenced drivers cannot be deleted. Migrate dependent sources and test first. Use approved packages and [Compatibility](#); supported types do not validate every driver combination.

Understand plugin types

Plug-in Manager				
Plugin type		DataSourcePlugin ^		
	Plugin type	Creation Time	Last Update	
>	HIVE	DataSourcePlugin	2026-04-29 17:53:42	2026-04-29 17:53:42
>	POSTGRES	DataSourcePlugin	2026-04-29 17:53:42	2026-04-29 17:53:42
>	ORACLE	DataSourcePlugin	2026-04-29 17:53:42	2026-04-29 17:53:42
>	IMPALA	DataSourcePlugin	2026-04-29 17:53:43	2026-04-29 17:53:43
>	MYSQL	DataSourcePlugin	2026-04-29 17:53:43	2026-04-29 17:53:43
>	METAMODELDEMO	DataSourcePlugin	2026-06-08 14:54:59	2026-06-08 14:54:59
>	OCEANBASEO	DataSourcePlugin	2026-07-09 10:56:16	2026-07-09 10:56:16
>	VERTICA	DataSourcePlugin	2026-08-18 18:16:41	2026-08-18 18:16:41
>	CUSTOMIZED	DataSourcePlugin	2026-08-24 16:32:52	2026-08-24 16:32:52
>	MAXCOMPUTE	DataSourcePlugin	2026-09-10 17:30:31	2026-09-10 17:30:31
>	DB2	DataSourcePlugin	2026-09-11 17:33:54	2026-09-11 17:33:54

Type	Responsibility
Source	Source types, forms, connections
Reverse engineering	Convert structures into tables, columns, views, routines, or metamodel objects
Lineage parser	Extract SQL/ETL/BI processing relationships

JDBC drivers do not add source types or complete reverse engineering/parsing.

Upload and validate

1. Open Plugin Management and choose type.
2. Upload the matching file.
3. Verify name/type/state.
4. Test source creation/connections for source plugins.
5. Test limited harvesting and properties for reverse engineering plugins.
6. Test known parsing, node matching, and dependencies for parsers.

Source packages may contain multiple components, but source/reverse engineering types remain separate. Reupload can replace a plugin; installed plugins normally cannot be deleted directly. Have delivery/development teams retain previous versions, dependency lists, and verification records.

Troubleshoot

Symptom	Check
Driver exists, type missing	Source plugin
Connected, objects missing	Reverse engineering compatibility, rights, schemas, logs
Metadata exists, parsing fails	Parser, format, engine, namespace
Driver deletion blocked	Source references
Calls differ from lineage	Separate manual relationship and parsed evidence/history

Understand licenses and feature visibility

Licenses control top-level modules; roles control functions, and objects can have separate rights.

Review entitlements

- 1. Administrators open Configuration Management > Product License Management.
- 2. Inspect licensed modules.
- 3. Compare with user roles and menus.
- 4. Distinguish unlicensed features, missing grants, and object scope.

Actual entitlements determine combinations; this is not a fixed button-level matrix.

Distinguish capabilities

Capability	Boundary
Basic modules	Standards, metadata, quality separately licensable
Metadata lineage	Basic/end-to-end inspection from metadata objects
Data lineage	SQLink maps/scenarios and advanced features; separately entitled
Metric Standards	Basic data-standard metrics
Metric Management	Definitions, mapping, applications; Data Metrics license
Governance agents	Optional AI assistance; without entitlement, chat and related AI features are hidden

DDC includes catalog/marketplace; DDS includes security/gateway. Documentation organization does not imply purchase/deployment bundles.

Diagnose missing menus

Check environment, license, roles, object rights, and enabled deployment. Administrator visibility does not establish all-user rights.

Related: [Organizations](#), [Product structure](#).

Diagnose execution and operation issues with logs

Identify time, object, account, and task before choosing evidence.

Choose logs

Purpose	Log	Entry
Task failure	Execution log	Scheduling history > Log
Backend failure	Service log	Log Management where provided
Business audit	Operation log	Log Management where provided

Deployments may provide separate operational tools. Task logs do not replace full service/audit logs; check permissions/entry points.

Query service logs

1. Filter service, level, and time.
2. View full records.
3. Copy contextual errors or export for analysis.
4. Correlate business/task times.

Retain context beyond the final error and mask credentials, connections, and business data before sharing.

Query operation logs

Filter description, user, module, action, and time. Compare objects/history. Operation records do not prove approval or task success.

Provide operations with

- Entry, object, time, expected result.
- Actual message, task state, failure scope.
- Relevant execution/log evidence.

- Preceding connection, permission, rule, or schedule changes.

Related: [Scheduling](#), [Connections](#).

Manage organizations, users, roles, and groups

Use System Management > Organization Management for manual maintenance. Integrated identities follow enterprise integration agreements.

Distinguish objects

Object	Purpose
Organization	Formal hierarchy and membership
User	Login identity, profile, enablement
Role	Feature/action rights
Group	Virtual teams, bulk grants, multi-person approval

Feature rights do not automatically grant all business objects.

Create organizations

1. Select a parent in Organization Management.
2. Add a child and complete information.
3. Verify the unique, immutable code; save.
4. Inspect hierarchy/users.

Edit supported fields. Resolve children/users before deletion.

Move personnel

Add existing users in organization membership lists. Users require an organization. Transfer through user organization fields or supported add-to-target actions, then verify final membership rather than simply removing membership.

Define roles

1. Create a role.
2. Select module, feature, and action rights.

3. Save/reopen to verify.
4. Add/remove members.
5. Test as the target user.

Default roles exist and can be adapted. Suggested responsibilities include platform administration, data ownership, stewardship, module administration, and consumption. Inspect actual grants rather than names.

Create users

Prepare roles, systems, and organizations first.

1. Open User Management > New.
2. Complete profile and role/system/organization associations.
3. Save.
4. Check organization/role membership.
5. Have the user verify modules and object access.

Edit profiles and enable/disable as needed. Disabled users cannot log in; separately transfer tasks, approvals, and ownership for departures.

Maintain groups

Create/save a group, add users in Members, remove users where needed, edit group details, and check approval/grant dependencies before deletion.

Troubleshoot

Issue	Checks
Missing creation options	Roles, systems, organizations
Login failure	Enablement/authentication
Missing menu	License and feature grants
Missing objects	Module object scope
Cannot delete organization	Children/users
Wrong approver	Organization, groups, participants

Related: [Workflows](#), [Licenses](#), [Quick start](#).

Configure task schedules and time templates

Administration schedules recurring tasks and exposes execution evidence. Business rules/scope remain in their modules.

Before configuration

Create the business task and agree interval, dates, and maintenance windows. Prepare templates for restricted dates first.

Create templates

1. Open Task Management > Time Templates > New.
2. Enter information and allowed dates, importing through the provided template if needed.
3. Check month/year boundaries and holidays.
4. Reference it in scheduling.

Templates support editing, enabling, disabling, and deletion. **Referenced templates can still be disabled/deleted; tasks then lose those restrictions.** Review affected tasks first.

Set recurrence

1. Find the task and select Schedule.
2. Enable/disable scheduling. Disablement does not terminate a current process.
3. Set repeat interval.
4. Choose time filters and verify allowed dates.
5. Save/reopen and inspect the next eligible execution.

Allowed dates must satisfy templates and recurrence. Multiple templates use their **intersection**. For example, weekday and trading-day templates permit only dates in both sets; these are illustrative, not built-in templates.

Inspect execution

Review time/status and open the run's Log. Return to the business module to verify actual harvested objects or quality reports after scheduling success.

Monitor services

Task Monitoring shows nodes, memory, processes, tasks, and logs. Operations should assess impacts before force-terminating a process. Task Files registers files for task services; check dependencies and actual use after uploading.

Troubleshoot

Symptom	Check
Did not run	Enablement, interval, allowed dates/intersection
Ran on unexpected dates	Disabled/deleted/changed templates
Failed	Logs, connections, files, business settings
Runs indefinitely	Service/process evidence; operations decides termination
Success, incomplete output	Business scope and per-object failures

Related: [Sources](#), [Logs](#).