



DATABLAU · DAM

Data security

Product module user manual

Version 9.1.2

Contents

01	Data security
02	Data security quick start
03	Configure access, row filters, and masking policies
04	Manage recognition algorithms
05	Design security classifications, levels, and information items
06	Process classification results in the workbench
07	Collaborate on classification and review
08	Maintain legal provisions and classification evidence
09	Maintain masking rules and security configuration
10	Manage policy folders and security operation logs
11	Configure recognition algorithms, rules, and tasks

Data security

Data Security (DDS) covers classification, sensitivity levels, recognition algorithms/tasks, review/publication, access policies, authorization, and masking. Classification, reviewer confirmation, and data access controls are related but separate tasks.

Understand the objects

Object	Purpose	Follow-up
Security classification	Organize by business meaning	Design hierarchy, create nodes, assign objects
Classification information item	Reusable recognition concept	Not a specific database column
Security level and rationale	Requirements and evidence	Same-class objects can have different levels
Algorithms, rules, tasks	Bulk candidate recognition	Review results before publication
Access policy	Identities, scope, controls	Direct access, rows, table/column masking
Masking rule	Presentation of sensitive values	Reference in policies and verify actual access

Before you begin

Harvest metadata, confirm meanings, and agree classifications, levels, and evidence. Prepare real test identities and approved samples for gateway verification.

Recommended responsibilities: business owners explain meaning, security stewards maintain controls, reviewers confirm classification, and administrators configure enforcement. Actual roles/permissions are organization-defined. Start with a few manually classified objects using [Quick start](#), then expand recognition.

Understand the gateway boundary

This module governs rules and results. [Security Gateway](#) is the separate DDS dynamic masking component, including server, JDBC clients, and audit.

Find a task

Goal	Guide
First governance cycle	Quick start
Framework, concepts, levels	Classification design
Legal evidence	Legal basis
Manual classification/review	Collaboration, Workbench
Bulk recognition	Recognition
Algorithm library	Algorithms
Access, rows, masking	Policies
Folders and evidence	Policy folders/logs
Masking and operation	Rules/configuration

Read the security overview

Published here means reviewed associations between assets, classes, and levels, not catalog publication or verified access policies.

Chart	Meaning
Asset levels	Proportions of published assets; exclude unconfirmed candidates
Classification and levels	Level counts within top-level classes
Levels by system	Published assets by their business system
Levels by department	Business department of the table/column's system, not the operator

Align objects, hierarchy, review states, and department properties before reconciling counts. Coverage does not replace access/masking tests.

Data security quick start

Screenshot note: Captured from the English interface. Some controls are still untranslated in this release; demo data names retain their original language.

Classify a few harvested tables/columns, then verify one access or masking requirement with business/security owners.

Before you begin

Requirement	Check
Harvested objects	Correct source, names, meaning
Classification evidence	Owners can explain categories/levels
Stewards/reviewers	Rights and approval responsibilities
Test identities	Expected data scope for access tests

Reuse approved frameworks rather than duplicating them.

1. Establish the framework

Use [Classification design](#) to configure levels/types, create nodes, define sensitivity and evidence, and associate legal provisions. Interface names may use Security Classification instead of Data Classification.

Verify target-type support and actual nodes/levels. Existing nodes restrict reductions in levels/types.

2. Classify a few objects

1. Find To Classify objects under Collaborative Classification.
2. Verify source/meaning and associate the right category.
3. Review Pending Confirmation classes/levels.
4. Edit incorrect values or Reclassify.

Check selections and individual levels. All pilot objects need explainable results; deferred objects stay distinct. See [Collaboration](#).

3. Review and publish

1. Submit confirmed results.
2. Authorized reviewers open Review and Publish.
3. Verify object/class/level/evidence; approve or reject for correction.
4. Inspect success/failure counts and publication.
5. Compare objects with the [Overview](#).

Track unresolved/partial failures. Submission is not approval.

4. Verify access and masking as needed

Define one user's expected scope, create [Policies](#), and follow [Gateway quick start](#) for JDBC masking. Query as the actual identity and check logs. Verify classification and enforcement separately.

Expand scope

Use [Recognition](#) after the pilot. Test positives/negatives, execute, review, publish. Scores are not final decisions. Begin with the [Synthetic expression test](#); it saves no algorithm or classification.

Configure access, row filters, and masking policies

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.

Policies control access to data values, unlike documentation or catalog browsing rights.

Choose a policy

Type	Purpose
Access	Allow/deny object scopes
Row-level access	Restrict records in accessible tables
Table masking	Configure column rules from a table/view
Column masking	Configure rules per identity from a column

Create named/described folders first. Resolve contained policies before deletion.

Before you begin

Confirm objects, identities, purpose, row criteria, and [Masking rules](#). Users/groups/organizations come from [Organization management](#); objects come from harvested metadata. Test approved limited scopes first. Denying selected objects differs from allowing everything except selected objects.

Create an access policy

1. Open **Security Policies > Access Policies > New > Access Policy**.
2. Set name, description, folder, and validity.
3. Select execution operation, allow/deny action, and scope.
4. Verify Include, Exclude, or All at each level.
5. Select users/groups/organizations; use a denylist to remove identities from an allowlist if needed.
6. Save and verify actual effective access as target identities.

Basic Information

Access Data Config

Data Execution

SELECT

Action

Data Access Action

☒ Allow
☐ Refuse

Collection Name

Select

Data Source

The screenshot has no selected harvesting scope and is not an effective policy example.

Setting	Check
Name/folder	Required; clear purpose
Validity	Available only for allow policies as described by the form; expiry revokes access, empty means permanent
Execution	SELECT, INSERT, UPDATE, DELETE; grant only approved operations
Action	Allow/deny, checked with operation and scope
Harvesting name	Correct source before lower-level scope
Scope	All, Include, Exclude at source/table/view/column levels
Identities	User/group/organization and final allowlist minus denylist

Verify expiry on the actual enforcement path. It does not establish marketplace delivery or offline account revocation.

Create row-level access

1. Select New Row-level Access Policy and complete basics.
2. Add tables/views and identities.
3. Add row data conditions for each identity.
4. Define groups and inspect generated SQL.
5. Test known visible and excluded rows as that identity.

行级数据 | 数据表: pty_conp

新增条件组

数据行数限制100

det_addr_desc(详细地址)

=

北京

+

🗑️

取消

添加

Use fields, comparisons, values, and available group controls. Locations and row limits shown are examples. After **Add**, inspect the identity list's SQL before saving the policy. One user's conditions do not cover all others; verify multi-condition logic.

Create table masking

1. Select New Table Masking Policy and complete basics.
2. Add tables/views and inspect columns.
3. Associate masking rules.
4. Select applicable users/groups/organizations.
5. Verify target and untargeted columns.

Create column masking

1. Select New Column Masking Policy.
2. Add columns and identities.
3. Set a masking rule for each identity row.
4. Verify the same column under different identities.

Verify and maintain

Search by name, view effective scope/rules, and recheck prefilled settings when editing. Use [Gateway verification](#); saving does not establish correct client routing. Test overlapping policies instead of assuming precedence. Record original scope/identities before changes/deletion.

Symptom	Checks
Saved but unrestricted	Gateway route, identity, object scope, operation/action
Users in same group differ	Direct/group/organization grants, denylist, overlaps
Row filter returns nothing	Field/value/logic, matching source records, query scope
Some columns unmasked	Policy type, selected columns, rules, identity
Unexpected expiry behavior	Allow policy, validity, routing, processing logs

Manage recognition algorithms

Algorithms, rules, and tasks produce candidate classifications; accountable reviewers confirm and publish them.

Choose an algorithm

Type	Use	Management focus
Algorithm library	Text, column, pattern recognition	Folders, expressions, samples, descriptions
Lineage cascade	Propagate candidates from confirmed objects	Lineage quality and scope
Machine learning	Model-based suggestions	Applicability and review sampling

Availability depends on deployment/license. Check features and rights if absent.

Create an algorithm

1. Open **Data Security > Recognition Algorithms > Algorithm Library**.
2. Create a clear-purpose folder.
3. Select **New Algorithm** and enter name, code, description, and applicable types.
4. Configure expressions/parameters and test matches/nonmatches.
5. Verify status, folder, and rule availability after saving.

Use synthetic samples, including nulls, boundaries, Chinese characters, and invalid formats.

Import, export, and maintain

Use system templates, unique codes, existing folders, and valid parameters. Inspect failed rows; task creation does not prove every algorithm is effective. Exports support review/backup, not version history. Resolve rule dependencies or create replacements before retirement/deletion and monitor subsequent results.

Check before publication

- Names/codes match business meaning.

- Positive, negative, and null tests pass.
- Results explain evidence and proposed classification.
- Rules reference intended algorithms.
- Task scope and owner are clear.

Next: [Rules and tasks](#).

Design security classifications, levels, and information items

Classification describes business categories; levels describe sensitivity. Classification information items are reusable semantic concepts, not physical columns. Associate actual objects after recognition or manual review. Establish policy and framework first.

Design the hierarchy

1. Open **Data Security > System Settings > Data Classification Design**, also labeled Security Classification Design.
2. Set levels, names, and supported types. Data item support also supports information items.
3. Configure custom properties/icons and save.
4. Create nodes in **Data Classification and Levels > Data Classification**.

Once nodes exist, levels and supported types can increase, not decrease. Changing a property type clears values; making it required requires completion. Assess impacts first.

Reuse catalog structures

If approved, select one enabled catalog space and immediate or real-time synchronization. Its depth must be at least the security hierarchy depth. Existing attached assets/information items block synchronization. Enabling it prevents independent hierarchy edits.

Synchronization mainly copies names/descriptions, not all properties. Set default levels/importance or complete them afterward. Verify supported types:

Catalog support	Security support
Folders only	Folders
Folders/tables	Folders/tables
Folders/data items	Folders/data items
Standards, services, metrics, files, reports	Security table/data-item/view scope; those business types are not copied

Later synchronization follows changed source folder types. Verify hierarchy and eligible objects, not names alone.

Maintain information items

1. Create a named/described folder in **Classification Information Items**.
2. Create the item and save its properties.
3. Define custom properties through **More > Custom Properties** as needed.
4. Download import templates; choose automatic codes or provide codes.
5. Inspect progress, successes/failures, and search by name/code.

Attached items cannot be deleted; nonempty folders cannot be deleted. Export without selections covers all; with selections it covers selected items.

Maintain classifications

Create/edit nodes, add information items, and import/export templates in Data Classification, also called Security Classification. Existing items, assets, or approvals block deletion. Structure exports differ from asset exports, which include the current class and descendants.

Define levels and evidence

Maintain levels, importance references, and decision criteria in **Data Levels**. Built-in values are editable; referenced levels cannot be deleted. Upload legal files in **Legal Provisions** and verify downloads. Referenced provisions cannot be deleted. Uploading evidence alone does not establish compliance.

Next: [Collaborative classification](#) or [Recognition](#).

Process classification results in the workbench

States include To Classify, Pending Confirmation, Under Review, Published, and Deferred. They describe governance progress, not database modifications.

Classify collaboratively

1. Open **Data Security > Classification Tools > Collaborative Classification**.
2. Filter To Classify by system, folder, type, and name.
3. Select assets, category, and level; verify count before submitting.
4. Defer out-of-scope objects with reasons.
5. Check classification, level, evidence, and owner in Pending Confirmation; edit and submit for review.

Same-class assets can have different levels. Recheck batch selections to avoid applying one level to different meanings.

Review and publish

Reviewers inspect details, hierarchy, evidence, and recognition source. Approval publishes; rejection returns results for correction with reasons. Follow the current workflow's return state. Publication does not verify access/masking. Before reclassifying published objects, assess policy and marketplace impacts.

Import and export

1. Download the template and preserve columns, codes, and states.
2. Asset Review requires confirmation; Direct Publication requires authorization.
3. Correct identifiers, classification codes, and levels in failed rows.
4. No selection exports all objects in the current state; selections restrict scope.

Handle asset names, columns, and sensitivity levels through approved storage/transfer channels.

Troubleshoot states

Symptom	Check
Missing unclassified object	Harvesting, filters, folder rights
Submission failure	Class, level, evidence, required owner
Hidden after review	Publication, catalog rights, license
Reclassify unavailable	State, role, active review

Collaborate on classification and review

Screenshot note: Captured from the English interface. Some controls are still untranslated in this release; demo data names retain their original language.

Use manual classification for tables, views, and data items requiring individual judgment. Prepare categories, levels, evidence, and reviewer responsibilities.

Move from unclassified to pending confirmation

1. Open **Classification Tools > Collaborative Classification**.
2. Select objects in **To Classify** and verify source/meaning.
3. Select the security class on the right and confirm association.
4. Inspect class/level in **Pending Confirmation**.
5. Use **Edit Classification** or **Edit Security Level** as needed. Same-class assets can have different levels.
6. **Submit for Review**.

Classification & Grading Workbench

Asset Inventory Progress 0 %

Data Asset Name	Table	Collection Name	Data Source	schema	Data Classification	Security Level	Inventory Status	Inventory Time	Operation
frozen	db_trashed_model	反洗钱-采集	反洗钱-采集-data...	datablau_ddm	01-银行业/监管/数据服...	新等级	To Be Co...	2026-10-14 16:09:27	
description	db_trashed_model	反洗钱-采集	反洗钱-采集-data...	datablau_ddm	02-证券业/公司管理/办...	普通数据	To Be Co...	2026-10-12 16:14:20	
is_dw_model	db_trashed_model	反洗钱-采集	反洗钱-采集-data...	datablau_ddm	02-证券业/公司管理/办...	普通数据	To Be Co...	2026-10-12 16:14:20	

Data Classification 01-银行业 02-证券业 03-期货业 04-保险业 05-制造业 06-零售业 其他行业

Verify count/scope before batch actions. Mark excluded objects **Defer Classification**. **Reclassify** returns objects to To Classify; published/deferred objects can also be revisited.

Import existing classifications

Download the Import Assets template. **Asset Review** imports into Pending Confirmation and still requires submission. **Publish Directly** bypasses this review page and requires organizational authorization. Correct failures. Exports cover the current state unless rows are selected.

Review and publish

1. Open **Classification Tools > Review and Publish**.
2. Filter asset, system, source, harvesting name, inventory mode, and classification time.
3. Inspect objects, classes, levels, and evidence rather than scores alone.
4. Approve correct results to publish.
5. Reject incorrect results for reclassification.
6. Inspect success/failure counts; deleted metadata can cause partial failure.

Verify results

Check actual object classifications and published overview distributions. Publication does not configure access. Use [Policies](#) and [Gateway](#) separately.

Maintain legal provisions and classification evidence

Legal provisions provide traceable evidence for classification, levels, and review. They do not automatically classify data.

Upload provisions

1. Open **Data Security > Legal Provisions**.
2. Upload an organization-approved file.
3. Enter name, issuer, scope, effective information, and description.
4. Verify complete metadata and download access.

Use identifiable subjects/dates in filenames. Do not upload temporary private or unpublished materials into production.

Associate evidence

Select uploaded provisions in classification/level rationale fields. Add clauses, interpretations, and internal decisions. Multiple references may apply; record why and who confirmed the decision. Preserve new files/clauses for changes rather than overwriting history. Review object, level, evidence, and reviewer together.

Download, replace, and delete

- Download original evidence for retention.
- Check references and document impacts before replacement.
- Referenced provisions normally cannot be deleted; resolve references or follow archival procedures.

Verify results

Open a referencing classification and compare evidence names, clauses, and downloads. If absent, check saving and viewing rights before concluding no evidence exists.

Maintain masking rules and security configuration

Rules define presentation; policies define applicable objects and identities. Creating a rule alone does not enforce it.

Create and reuse rules

- 1. Open **Security Policies > Masking Rules** and create a folder.
- 2. Create a rule using available types/properties.
- 3. Verify purpose and expected presentation.
- 4. Reference it in table/column policies and test actual access.

Referenced rules cannot be edited/deleted. Plan replacement against affected policies first.

Choose masking behavior

Data	Verify
Identifiers	Required prefixes/suffixes and re-identification risk
Contact details	Minimum visibility for display/support/analysis
Amounts/dates	Statistical precision and ordering requirements
Fully hidden fields	No leakage through queries, exports, errors

Use current algorithm names/parameters. Test null, Chinese, long, and invalid values on nonproduction data before policy use.

Maintain folders and references

Assign maintenance responsibilities. Use reference information for impact. Folder renames do not change execution but affect management/audit searches; record changes.

Understand Ranger synchronization

Enablement attempts policy synchronization, not guaranteed enforcement. Verify target objects, contents, failures, timing, and source mappings in Ranger before retrying.

Maintain in bulk

Import through More Actions. Export from All Masking Rules for all content, or select rows for partial export. Search by name. Nonempty folders cannot be deleted.

Configure codes and synchronization

In **System Settings > Parameters**, also labeled Parameter Settings, set information-item code generation or manual coding. Configure Ranger per source and verify target outcomes independently of the switch.

Read overviews and logs

Security overview covers published classifications, levels, systems, and departments, excluding unconfirmed/pending results. Operation logs trace administration; gateway audit traces SQL. See [Gateway verification](#).

Manage policy folders and security operation logs

Folders organize policy/masking maintenance and searches without automatically changing enforcement scope.

Create policy folders

Open **Data Security > Access Policies > Folder Management**, organize by system/domain/department, assign viewing/maintenance rights, then create policies. Check references before deletion.

Inspect policies

- Direct access, row access, table masking, or column masking type.
- Systems, sources, databases, tables, columns, or tags.
- Users, groups, or roles.
- Effective/expiration times and priority.
- Masking rules and conflict handling.

Test allowed and denied paths with real test accounts. Viewing details does not prove enforcement.

Read security operation logs

Open Log Audit or Security Operation Logs. Filter time, user, object, action, and result. Retain query criteria, time, identifier, and error for correlation with [Gateway audit](#). Platform operations and data query records differ. Align time zones, proxy identities, and routing before comparing.

Configure recognition algorithms, rules, and tasks

Follow algorithms, rules, tasks, confirmation, then review/publication. General rules can use library expressions. Cascade/ML options depend on deployed features.

Maintain the algorithm library

1. Open **System Settings > Recognition Algorithms > Algorithm Library** and prepare a folder.
2. Select **New** in the algorithm list, not the folder tree. Enter name, folder, and expression.
3. Test one input, then positive/negative cases.
4. Save and search by name/description; edit as needed.

Editing referenced algorithms warns of impacts. Referenced algorithms and parent algorithms with children cannot be deleted. Import/export templates through More Actions and inspect task progress. No selection exports all; selection restricts scope. Nonempty folders cannot be deleted.

If available, **Machine Learning Algorithms > Try It** shows candidate categories/scores. On a 0–1 scale, higher scores indicate relative match likelihood, not compliance or published levels. Otherwise use general rules and tests.

Test a regular expression with synthetic codes

This tests text only without querying business data or saving an algorithm.

1. Enter a test name and accessible folder; required fields are validated before testing.
2. Choose Regular Expression and enter `^[A-Z]{2}[0-9]{4}$`.
3. Test AB1234 and expect a match.
4. Test AB12 and expect no matching content.
5. Cancel afterward. For production, use business-approved expressions and samples before saving.

* Algorithm Name

Code test

9/12

Parent Algorithm

Select

* Select Catalog

默认目录

Description

Please enter

Recognition Algorithm Type

☒ Regular Expression

* Recognition Algorithm

^[A-Z]{2}[0-9]{4}\$

Content

Test

AB1234

Test

Test Result

☒ Matches Rule

Input	Result	Reason
AB1234	Matches	Two uppercase letters and four digits
AB12	No match	Too few digits

This illustrates matching direction, not an enterprise code policy. Test object-level conditions and task results before classification confirmation.

Configure recognition rules

Open **Classification Tools > Intelligent Classification > Recognition Rules**. The verified creation menu offers General Rule. Use other types only where available.

Type	Focus
General	Information-item or classification target; AND/OR conditions; small-sample tests
Lineage cascade	Downstream recommendations; unlike inventory's two-direction cascade
Machine learning	Table, table-dependent column, independent column, or information-item target; category, priority, threshold, count

Referenced rules cannot be deleted. Review affected scope after changes.

Test general rule conditions

1. Select **New > General Rule**.
2. Choose Information Item or Data Classification. For classification, choose table/view/entity or data-item granularity and the category.
3. Enter name, folder, description, priority, and AND/OR groups.
4. **Test Conditions** on a few known metadata objects.
5. Compare expected matches/nonmatches before saving.

Include negative examples; large tests take longer.

Basic Information

* Rule Name

Please enter

0/40

* Identification Target

☐ Info Item

☒ Data Classification

* Identification Asset Type

☒ Table/View/Entity

☐ Data Item

* Select Data Classification

+ Select Data Classification

0 selected

* Select Catalog

Please select

Description

Please enter

* Priority

☒ P3

☐ P2

☐ P1

Some interfaces label security classifications Data Classification. Recheck selected categories/conditions after changing target/type.

Control	Check
Name	Purpose and length limits
Target	Determines category/information-item selection
Asset type	Table/view/entity versus data item
Target object	Select an existing object, not just descriptive text
Folder/description	Ownership, scope, evidence
Priority	P1/P2/P3; do not infer conflict outcomes from labels
Groups/test	Compose conditions, test known positives/negatives

Configure machine learning

Choose the table category, a classified parent for dependent columns, an independent column category, or an information item as appropriate. Record folder, description, and priority and check overlapping rules. Threshold constrains candidate scores, not final sensitivity. Recommendation count limits classifications, not sampled rows. Table classification is not every column's final level.

Create and run tasks

1. Prepare a task folder.
2. Create a task and add rules.
3. Save, check scope, and enable if needed.
4. Run and inspect completion; submission success is not completion.
5. Copy to reuse, rename, and recheck rules/scope.

Enablement and execution differ. Search names fuzzily. Nonempty task folders cannot be deleted. Preserve required run/review evidence before deletion.

Confirm results

In Recognition Result Confirmation, also called Recognition Results, filter by asset, system, source, harvesting name, table, or level. Verify identity/class/level and edit where needed.

Action	When	Verify
Edit classification/level	Correct object, wrong suggestion	Both associations independently
Submit for Review	Reviewed candidates	Pending workflow, not publication
Reclassify	Rework evidence	Returns to To Classify and can join later runs
Defer	Exclude this round	Deferred state and reason

Reviewers [Approve and publish](#); rejected objects require reclassification. Deleted metadata can produce partial failures; inspect rows. With no results check execution, scope, tests, and conditions. Fix mass false positives instead of publishing for coverage.