ART

AIR-GAP REGULATED TRANSFER

2U RACK-MOUNT APPLIANCE

Sending a file: the experience of the user, approver and administrator

Three simple steps for the user, complete evidence for the administrator and approver. ART never buys simplicity by bypassing security.

For: IT managers and administrators rolling ART out to users

In this catalog: Sending a file as the user, the approver and the administrator see it, the console, policy, delivery at the destination, and retention

https://www.bardin.tech/en/bardingate-art/

To send a file the user does three things: picks the file and destination, confirms with the operating system's own means, and waits. Everything else, from assurance to delivery, is the appliance's job.

Safe network — Unsafe network

Your two networks stay separate and are never physically connected to each other; the 2U rack-mount appliance is attached to only one of them at any moment.

1. **Select**
Choose “Send via Bardin Gate” in the file menu. Only authorized destinations appear; a path cannot be typed.

2. **Confirm presence**
The operating system's own prompt, showing the file and destination. The Agent has no password box.

3. **Protected custody**
The Agent keeps an encrypted copy and a durable request, and waits for the appliance's next visit.

4. **Follow**
An activity window and native notifications in plain states; no invented percentage or time.

The path of a transfer

Preparing → Waiting for Bardin Gate → Sending → Received → Under security review → Waiting for approval → Waiting for destination → Delivering → Delivered

Rejected · Expired · Cancelled · Failed: action required

Each state is a stable, plain concept; technical detail sits behind a Details control, with a correlation code.

> **You can cancel until the durable receipt**
>
> After the receipt the file is in Bardin Gate's custody and cancelling is an administrative act. The Agent explains that handover plainly; removing local history deletes nothing from the audit trail.

The Agent is deliberately small

The file action · A compact Send window · A compact Activity window · Native notifications

Enrolment and access without a password in the Agent

1 Request access
The user selects Request access in the Agent and sees a code to read to the administrator.

2 Administrator approves
The administrator identifies the person by their own means, types the code and selects role and scope.

3 Set a password
A Safe-side Agent offers Complete registration and opens the console, where the user sets their password.

The Agent never receives the user's password and never stands in for a console session. No username, long token, QR code or typed URL is needed.

Administrators

- **Sign-in with a local username and password.** High-risk actions ask for the password again.
- **No vendor password, hidden account or email reset.** An authorized administrator resets a forgotten password with a one-time one; recovering the last administrator happens at the unit.

The console: five groups, filtered by permission

Group	Pages
Work	Dashboard, transfers, approvals, quarantine
File assurance	Validation, schemas, trusted signers, inspection engines
Directory and access	Agent hosts, destinations, users, groups, identity mappings, roles
Configuration	Policies, configuration, versions, export and import, licence, updates, security settings
Operations	System health, runtime, switching, jobs, audit, metrics

Each person's menu shows only what they may use, but hiding is never authorization: a deep link calls the same REST route with the same permission check.

Policy is structured data, not code

Policy is built from rules that carry a condition and give defined, registered effects. Scripts, SQL, general regular expressions, expression languages and plugins are not allowed in policy.

Effect	What it decides
Admission	Whether the transfer may be registered
Disposition	Deny or quarantine, after validation, after inspection or before delivery
Approval requirement	Who must approve and how many
Destinations and limits	Allowed destinations, maximum size, deadlines and retry ceiling
Priority and notification	Queue order (never weakens security) and which notifications go out
Preview and download	Closed by default; open only when one effect allows and none forbids

- **Default deny.** Without an explicit allow the transfer is refused, and an explicit deny beats everything: priority, scope specificity, approval and every allow.
- **The policy is snapshotted at registration.** Publishing or rolling back affects only later transfers; revocation, host disablement, licence, time and storage integrity always stay current.
- **Rule order does not matter.** Effects aggregate commutatively, so moving a rule cannot tighten or loosen a decision.

Human approval

- **Several independent approvers.** Each requirement names who and how many; a partial approval grants nothing and the first rejection ends the transfer.
- **Every decision re-enters the password** and is recorded with a snapshot of the exact evidence.
- **A security override is bounded:** exact permission, an eligible verdict and state, a bounded reason, the password again and immutable audit. Approval never releases confirmed malware.

Delivery at the destination

- Delivery is automatic, to the fixed path the administrator defined; the destination user does not need to accept the file.
- The final name is `<TransferId>_<SafeFilename>`. A partial file is never visible; publication is atomic and the final file is reopened and hashed.
- A hash mismatch at the destination is shown as a security failure, not as success.

Retention defaults

Content or data	Default retention
Delivered content	Deleted immediately after verified delivery
Rejected or failed content	7 days
Quarantined content	30 days
Transfer metadata	One year

All are configurable. An authorized Hold prevents deletion until an audited release; there is no hidden or automatic extension.

A dashboard that names no file

The dashboard is live and says whether the appliance is working now, what crossed and which way, what was stopped and why, and who has to act. The Now band refreshes every five seconds; the chosen window (hour, day, 7 or 30 days) is compared with the period before, and if the appliance has not answered for 15 seconds the live mark turns red.

Simple for the user, strict with the file, and clear to the auditor.

More about this product

CATALOG 1
Product overview

CATALOG 3
Content assurance

CATALOG 4
Security and operations

For advice, a demonstration and contact details:
https://www.bardin.tech/en/bardingate-art/

Specifications may change without notice.