Kinspeed Connect

Kinspeed Connect User Guide

Kinspeed Connect helps organizations run workflows, review operational results, and keep process activity visible in one customer-facing platform.

This guide is intended for customers, prospects, sales teams, and account teams who need a clear overview of what users can do in Connect and how the platform is used day to day.

What Connect is used for

Connect is used to:

- Run configured business workflows on demand or on a schedule
- Preview workflow data before processing where the workflow supports preview
- Monitor workflow activity, progress, history, and logs
- Run reports and export report results
- Schedule report delivery where access is granted
- Review worker availability when workflow work is delayed
- Manage customer users, roles, and audit logs through Manager permissions
- Protect accounts with password controls, MFA, trusted devices, and auditability

Customer access

Each customer uses their own Connect URL. Users sign in with their Connect username and password, then complete any required verification step such as an email code or authenticator app code.

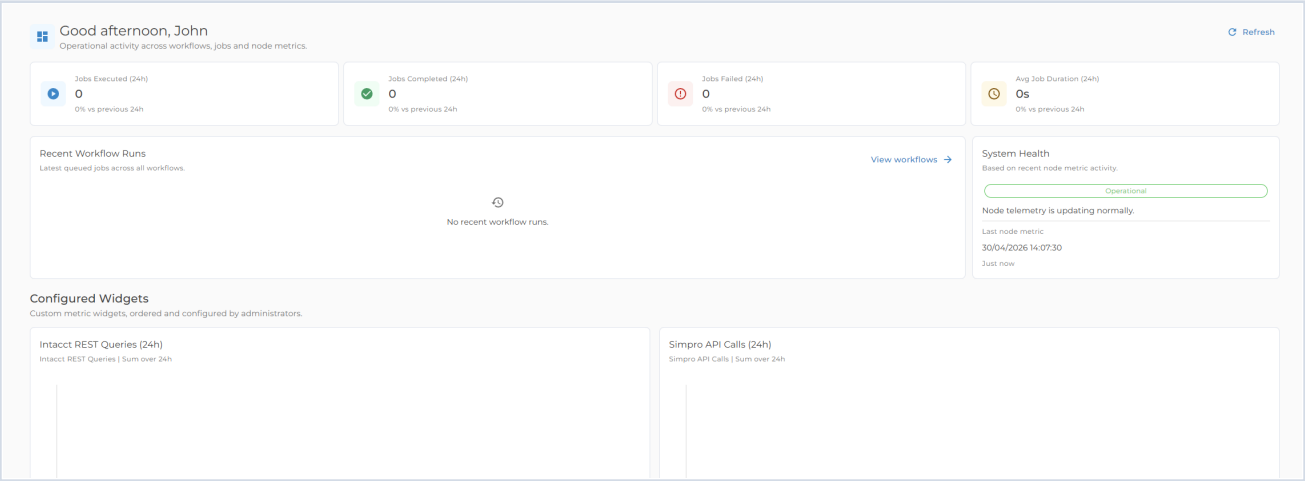
The pages and actions visible to each user depend on their role and customer configuration. This keeps the interface focused on the workflows, reports, and management tools relevant to that user.

Main areas

Connect is organized around a small set of day-to-day areas:

- Dashboard: a summary of current workload and recent workflow activity
- Workflows: the place to run workflows, preview data, review history, and inspect logs
- Reports: the place to run reports, view results, export data, and manage schedules where permitted
- Nodes: worker status for background workflow processing
- Account: profile, password, email, MFA, recovery codes, and trusted devices
- Users and Roles: Manager tools for customer user and access management
- Audits: Manager visibility into user, security, and workflow activity

Kinspeed Connect dashboard overview



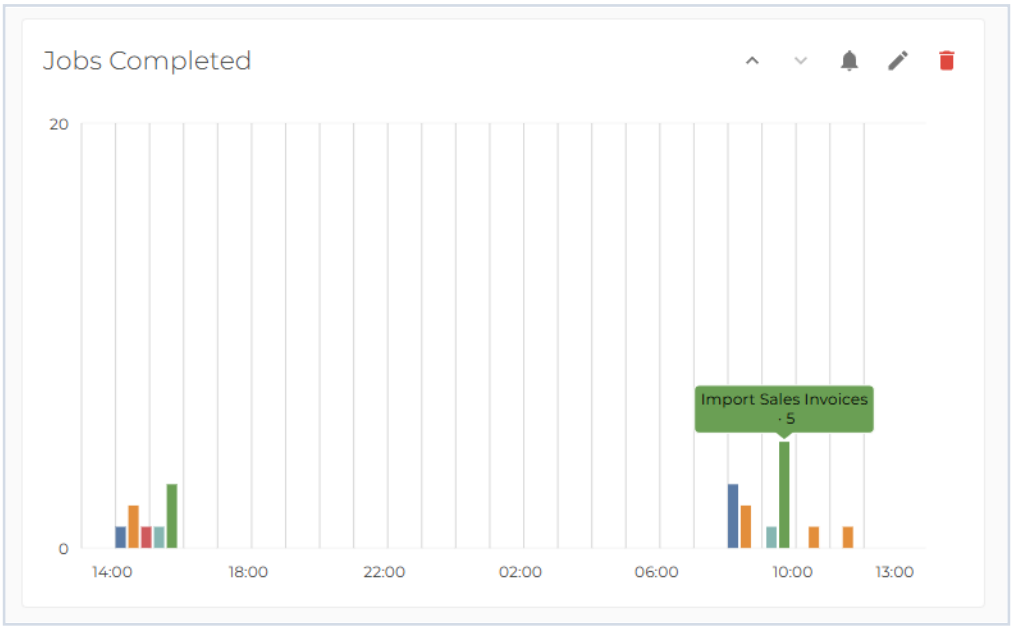
Dashboard

The dashboard gives users a fast view of the current workload across their Connect instance.

It highlights scheduled workflows, queued work, running jobs, completed jobs, and success or failure trends. Users can use the dashboard at the start of the day, after scheduled processing windows, or before investigating a support issue.

The dashboard is a summary view. Detailed investigation happens in workflow history and job logs.

Dashboard cards and charts

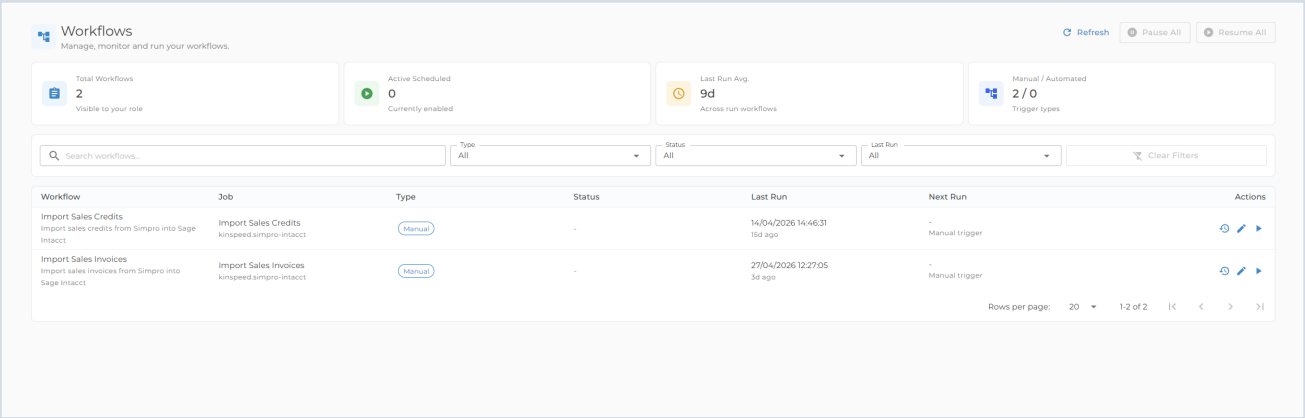


Workflows

Workflows are configured business processes. Depending on customer setup and user permissions, workflows can be run manually, run on a schedule, or triggered by external systems.

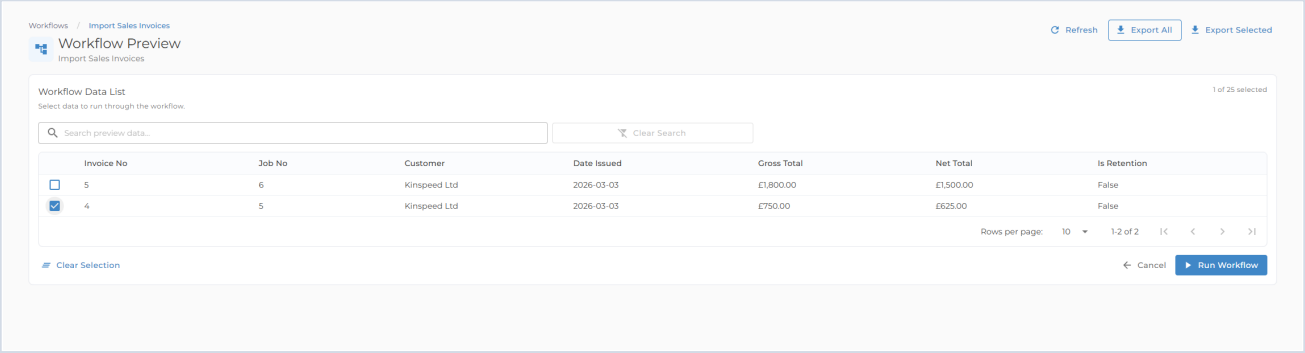
Users can search and filter workflows, review next and last run details, start allowed workflows, and open run history or logs when they need more detail.

Workflows list



Some workflows are previewable. A previewable workflow shows a data list before the workflow runs, allowing users to search, filter, select rows, export preview data, and run only the selected records. Some workflows automatically hide records that have already been processed, so the preview focuses on records still eligible for action.

Workflow preview table



Managers and administrators may be able to edit published workflow settings. Draft workflow setup and publishing remain administrator-only. The workflow editor provides configuration, role restrictions, schedule settings, connection profile settings, secrets, and template-backed workflow configuration in one full-page setup experience.

New workflows created by administrators start as drafts. Drafts are visible only to administrators and cannot be previewed, run, externally triggered, or scheduled until they are published. Published workflows are visible and runnable according to their role restrictions.

Scheduled workflows use local wall-clock time. A workflow scheduled for midnight runs at midnight in the configured scheduling timezone, including when clocks move forward or back.

Template-backed workflows may include guided configuration steps, query filter builders, mapping-rule drawers, lookup scope options, mapping dictionary drawers, and custom-field rule lists. These controls keep connector configuration structured while preserving the saved workflow settings behind the scenes.

Workflow history and logs

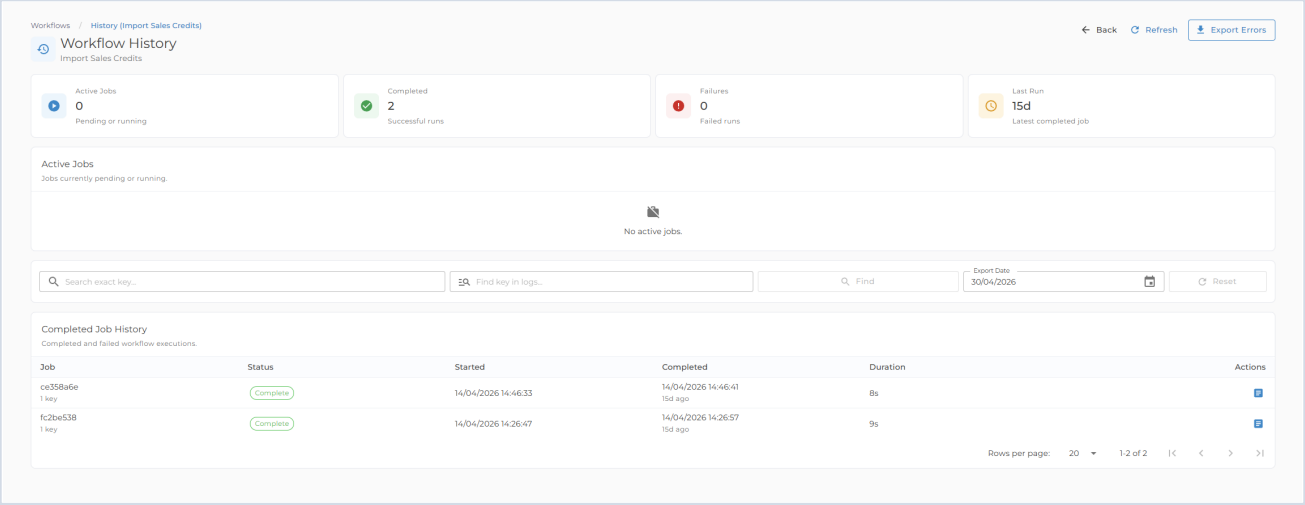
Workflow history shows active and completed runs. Users can search for a run, review status, find logs containing a key value, and export relevant logs when support needs them.

Job logs show live and historical log entries for a run. Logs can be filtered by level and searched by metadata where available. Some technical details may be visible only to Kinspeed support or approved platform operators.

Completed or failed jobs can be replayed where the user's access allows it. Replay creates a new queued run using the original selected keys and runtime values from the historical job. The new run still waits for normal worker capacity, workflow status, permissions, and node availability. Replay uses the current published workflow configuration rather than restoring an old copy of the workflow setup.

Replayed jobs are marked in workflow history and link back to the original source job. If the replay action is not available, the job may still be pending or running, the workflow may no longer be published, or the signed-in user may not have access to replay that workflow.

Workflow history



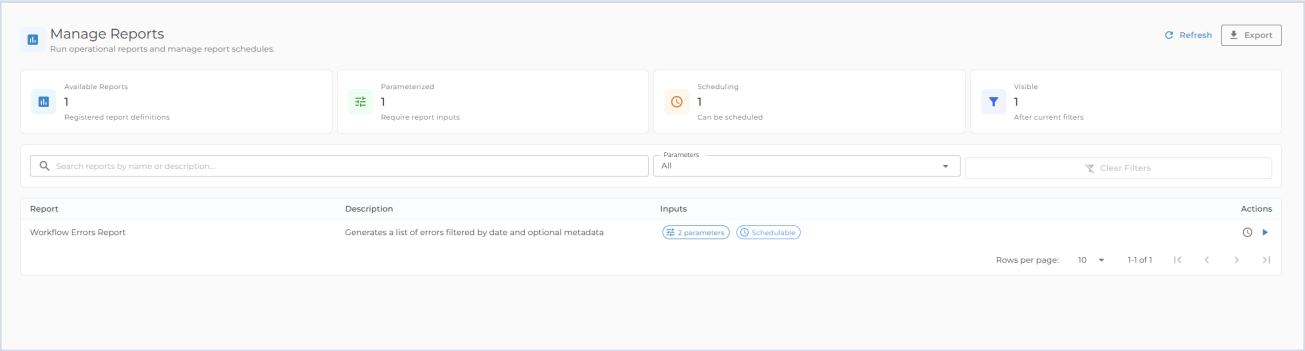
Reports

Reports summarize workflow and operational data. Users can run allowed reports on demand, enter required parameters, view report sections, and export table results to CSV where available.

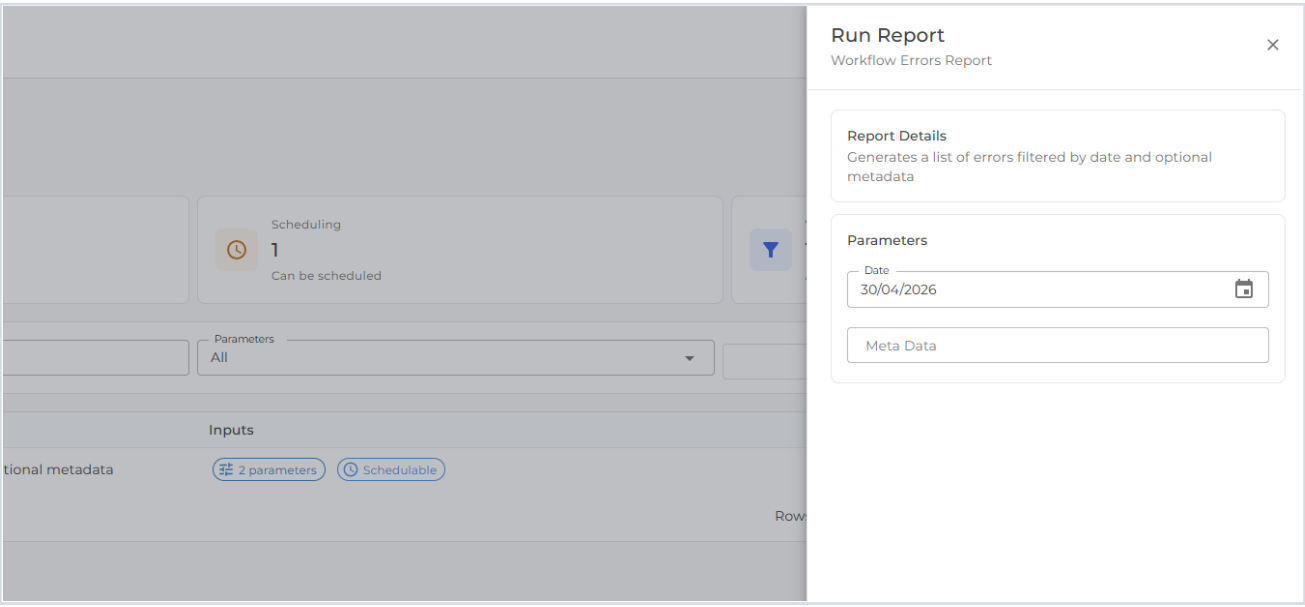
Managers may also be able to manage report schedules. Scheduled reports send configured report output by email according to the schedule set for that report. The schedule drawer includes a cron expression, a simple schedule builder, and a readable preview of the schedule.

Report schedules use the same local wall-clock scheduling behavior as workflows. For example, a report scheduled for midnight is sent at midnight in the configured scheduling timezone across daylight-saving changes.

Reports list



Report results

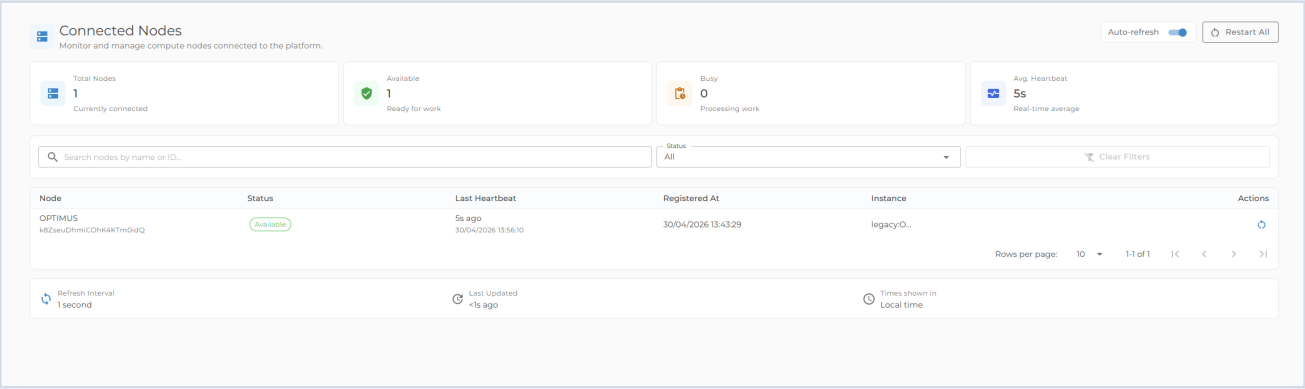


Nodes

Nodes are workers that execute workflows in the background. Most users only need the Nodes page when workflow preview or processing is waiting for an available worker, jobs are queued longer than expected, or Kinspeed support asks for worker status.

If a worker appears unavailable for longer than expected, users should contact Kinspeed rather than repeatedly starting the same workflow.

Nodes list



Account and MFA

Users manage their own profile and security settings from Account.

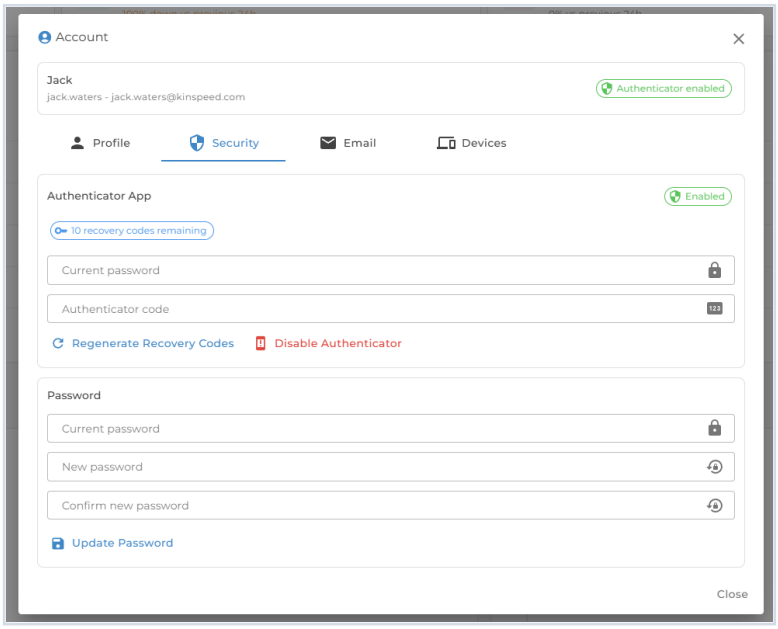
Account settings include:

- Display name and username review
- Password change
- Email address and email verification
- Authenticator app setup
- One-time authenticator recovery codes
- Trusted browser or device review and revocation

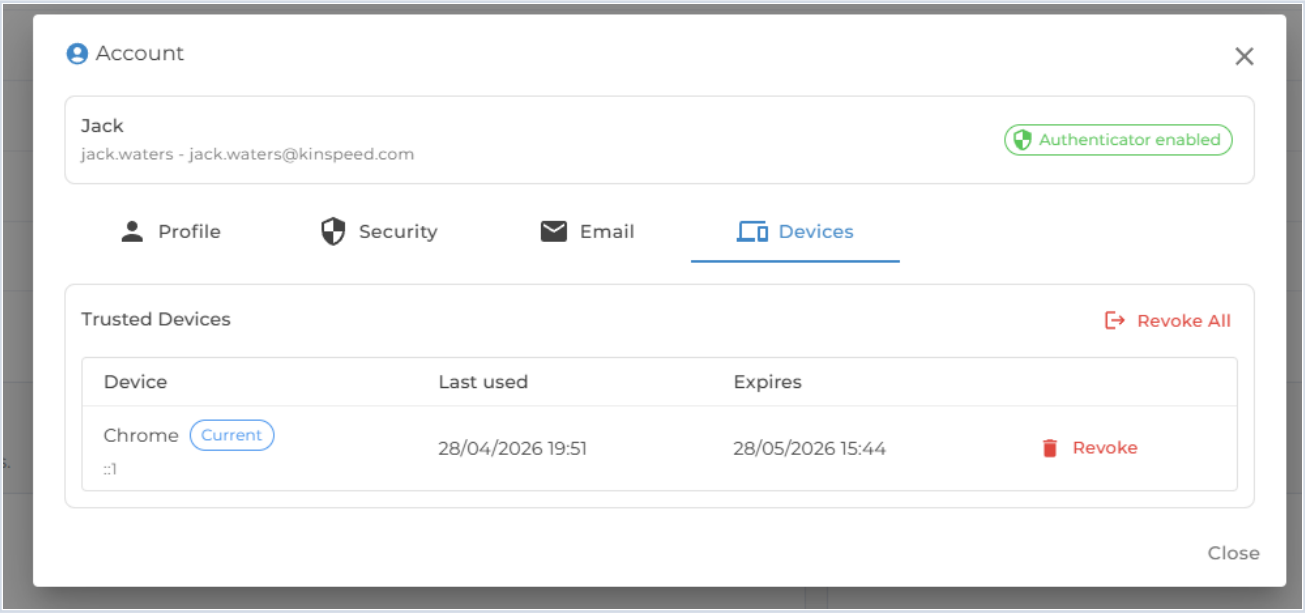
Authenticator app MFA adds an extra sign-in step. Recovery codes provide one-time backup access if the authenticator app is unavailable.

Trusted devices allow a browser or device to skip MFA until the configured trusted-device period expires or the trusted-device record is revoked.

Account security settings



Trusted devices



Roles and access

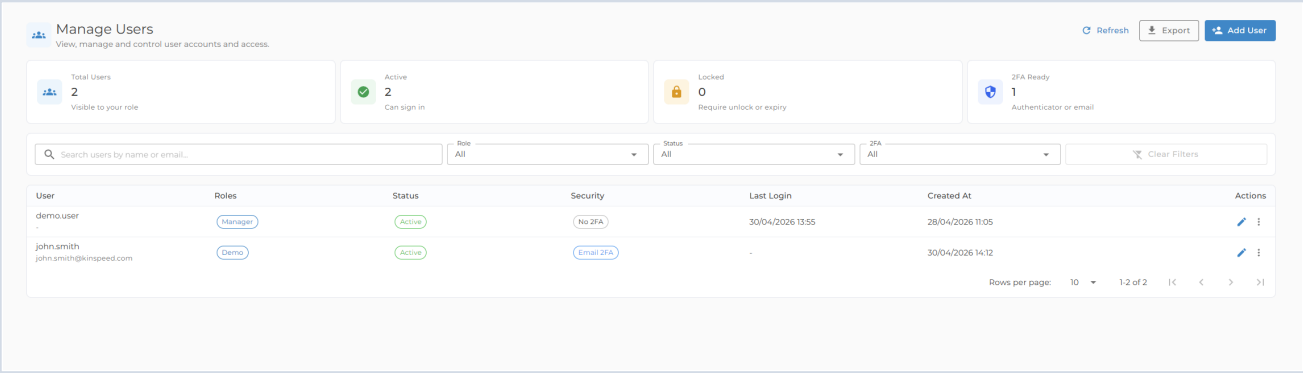
Connect uses role-based access. Standard users typically access dashboard, workflows, reports, nodes, and their own account settings.

Managers can manage customer users, customer roles, audits, report schedules where enabled, published workflow settings where enabled, and selected account recovery tasks such as unlocking customer users or disabling authenticator MFA when recovery is required.

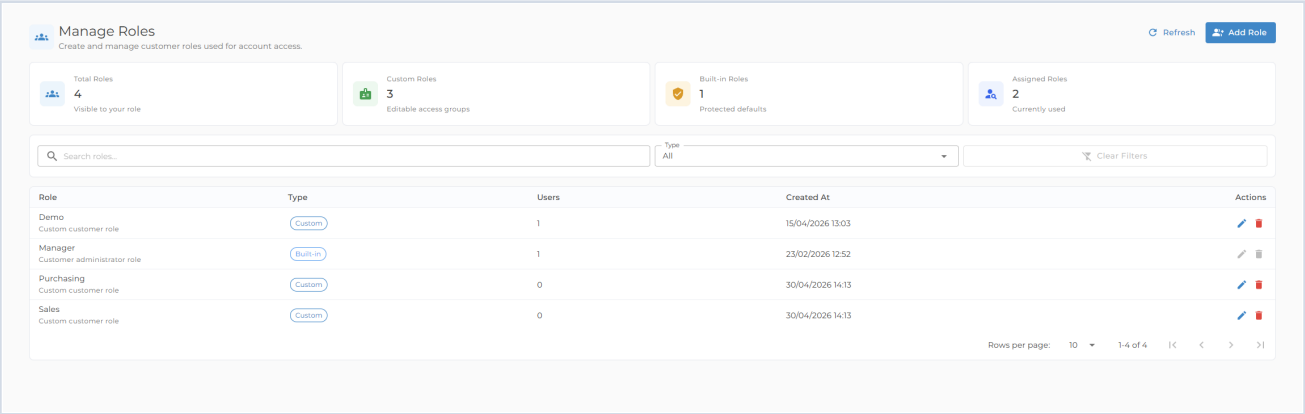
Custom roles can tailor workflow and report access for the customer's organization.

Platform-level access is reserved for Kinspeed support or approved platform operators. Customer Managers cannot assign platform-level privileges or publish draft workflows.

Users list



Roles list



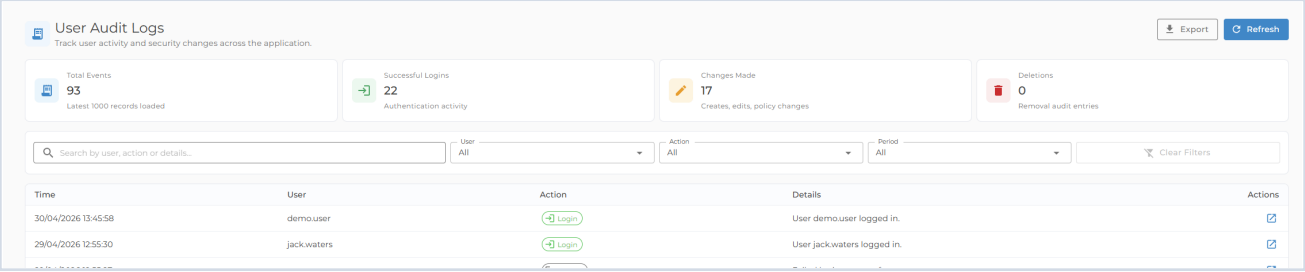
Auditability

Audit logs help Managers understand user, security, and workflow activity.

Audit records can include sign-in and sign-out activity, failed sign-in attempts, account lockouts, user and role changes, workflow changes, account security changes, workflow activity, timestamps, and request metadata where available.

Audit logs are useful when reviewing access changes, investigating workflow activity, or preparing information for Kinspeed support.

Audit logs



Notifications

Connect can show in-app notifications and send email notifications where email delivery is configured.

Email notifications may include report schedules, password reset, email verification, email MFA, and workflow-specific notifications depending on customer setup.

In-app notifications can include active system messages, worker connectivity warnings, session messages, or access messages.

Security overview

Connect is designed to protect customer data and accounts with separated customer environments, role-based access controls, configurable authentication policies, secure sessions, MFA options, trusted-device controls, audit logging, and careful handling of credentials and tokens.

Each customer instance has its own customer data boundary and separate database.

Protected application secrets use instance-specific encryption material.

Security policies that are exposed as platform settings are configured per customer instance and can be adjusted by Kinspeed where applicable to meet customer requirements.

A separate Security Overview PDF is available for teams that need a focused security summary.

Kinspeed-managed areas

Some capabilities are managed with Kinspeed support rather than directly through the customer-facing pages.

Examples include:

- New workflow setup
- Workflow script changes
- Plugin and customisation changes
- Platform policy changes
- Customer-specific configuration
- Secure integration or workflow trigger setup
- Advanced troubleshooting or operational review

When requesting a managed change, include the customer Connect URL, affected workflow or report, business reason, and timing requirements. Do not send passwords, MFA codes, recovery codes, integration keys, or other secrets.

Getting support

For faster support, customers should include:

- Customer Connect URL
- Username or display name
- Workflow, report, or page being used
- Date and time of the issue
- Visible error message
- Run ID or workflow history entry, if available
- Exported logs for workflow run failures
- Screenshot for visual or permission-related issues

For suspected account misuse, unexpected MFA prompts, unknown trusted devices, or unexplained role changes, customers should contact their Manager or Kinspeed promptly and include the approximate time of the event.

Scope

This document is a customer-facing overview of Kinspeed Connect user functionality. It does not replace customer-specific onboarding, configured workflow documentation, contractual terms, or separately confirmed security and infrastructure statements.