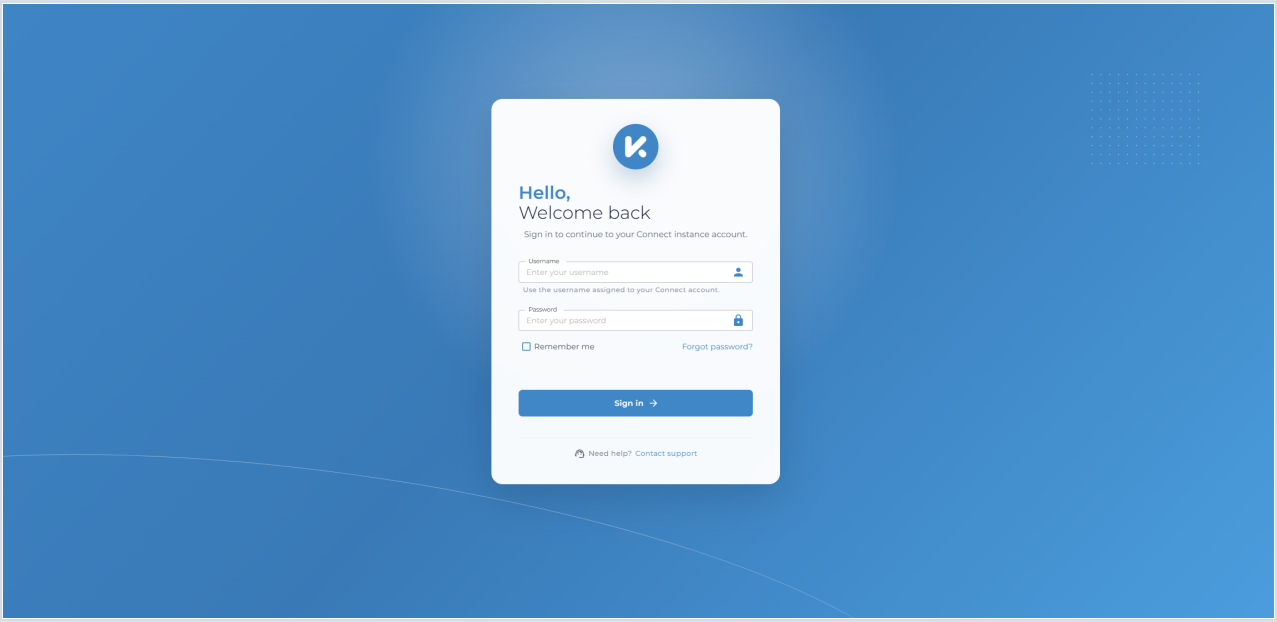
Kinspeed Connect

Security Overview

Kinspeed Connect is designed to protect customer data, user accounts, and workflow operations with separated customer environments, role-based access controls, configurable authentication policies, and audit logging.

Connect sign-in screen



Customer data separation

Each customer instance is separated from other customers. This means each customer has:

- A dedicated customer URL
- A separate customer database
- Unique encryption material for that instance

Customer operational data is stored in that customer's database. This includes users, roles, workflows, workflow settings, job history, audit logs, integration access records, two-factor authentication records, trusted-device records, and password reset records.

Instance-specific encryption material is used for protected application secrets, including authenticator app secrets. This gives each customer instance its own encryption boundary for these protected values.

Adjustable policies

Security policies that are exposed as platform settings are configured per customer instance. Kinspeed can adjust applicable policies for customer requirements without

changing other customer instances.

Current configurable authentication policies include:

- Failed password attempts before the first temporary lockout
- Failed password attempts after an expired lockout
- First and second lockout durations
- Permanent lockout threshold
- Email two-factor authentication enabled or disabled
- Email two-factor code expiry
- Trusted-device duration
- Email two-factor resend cooldown
- Maximum incorrect email two-factor code attempts

Default login protection settings are:

- 5 failed password attempts before the first temporary lockout
- 15-minute first temporary lockout
- 1 failed password attempt after an expired lockout before the next lockout
- 60-minute second temporary lockout
- Permanent lockout on the third lockout, until manually unlocked
- 10-minute email two-factor code expiry
- 30-day trusted-device duration
- 60-second email two-factor resend cooldown
- 5 incorrect email two-factor code attempts before the challenge is blocked

These values are defaults and may be adjusted where policy controls are available.

Authentication and account protection

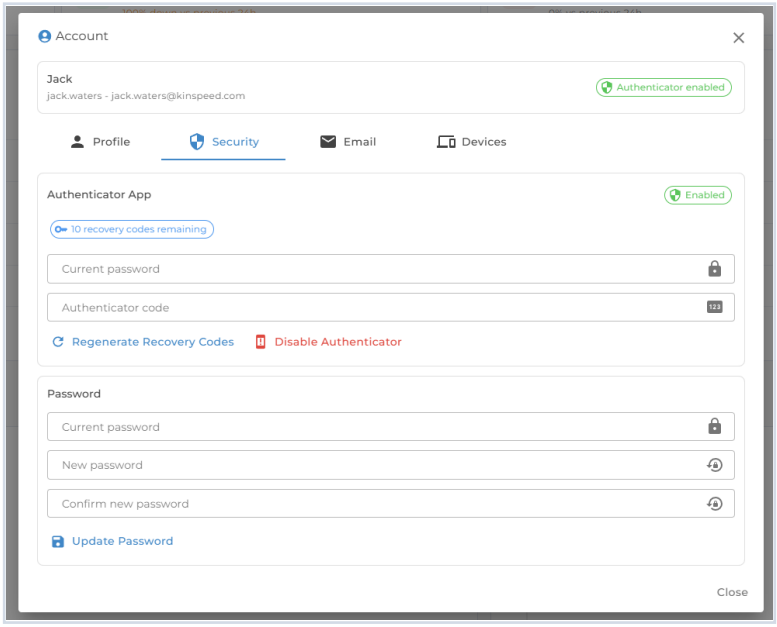
Users sign in with a username and password. The platform also supports additional account protections:

- Email verification code two-factor authentication when email is configured and the user has a confirmed email address
- Authenticator app two-factor authentication
- One-time authenticator recovery codes
- Trusted browser/device recognition
- Password reset through a confirmed email address

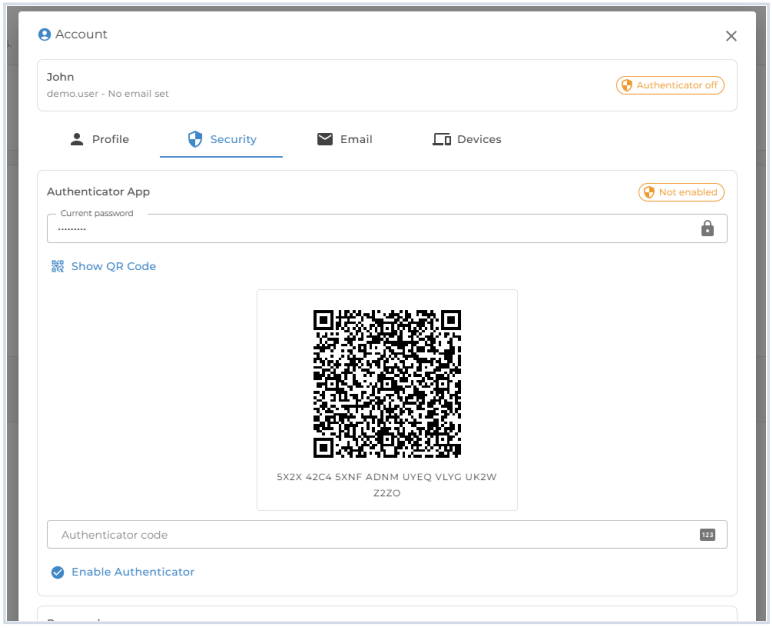
Authenticator app verification is checked before email two-factor authentication. Users with trusted browsers or devices can skip the second factor until the trusted-device record expires or is revoked.

Suspended or inactive accounts cannot sign in.

Account security settings



Authenticator app setup



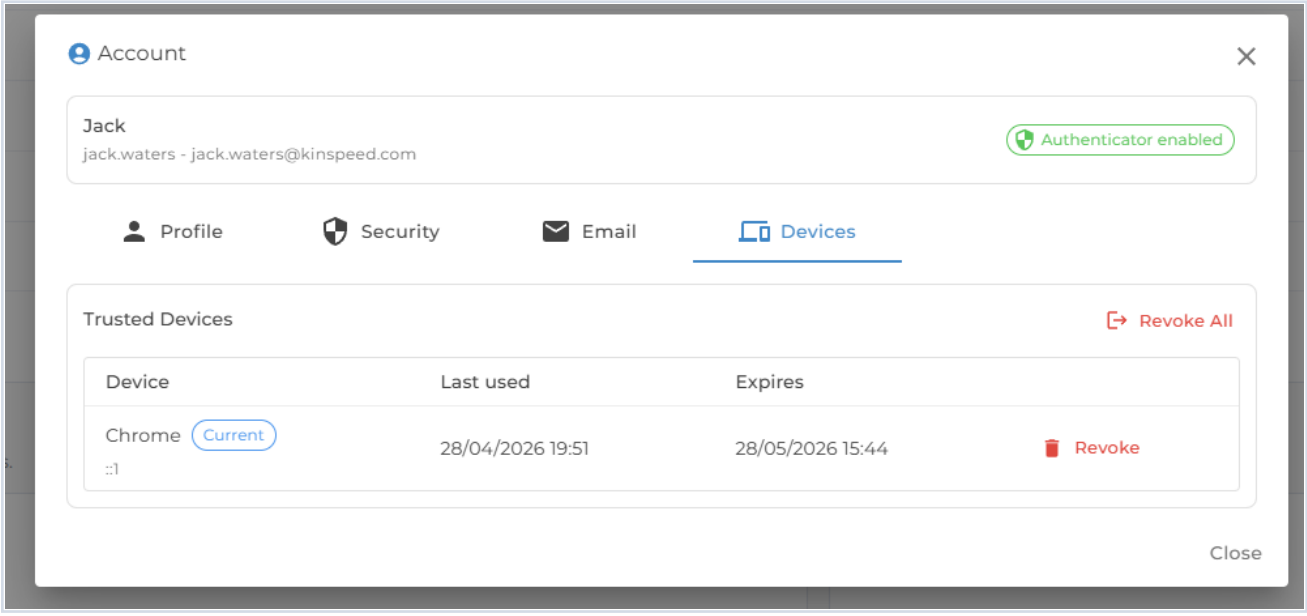
Session protection

Connect uses secure browser sessions with protections that help reduce account and session misuse:

- Session cookies are protected from normal browser script access
- Session cookies are only sent over secure connections
- Session cookies are restricted to the Connect site
- 30-minute sliding session expiry by default
- 30-day remembered sessions when Remember me is selected

Sensitive account changes invalidate older sessions in other browsers or devices.

Trusted devices



Credential and token storage

Connect does not store raw passwords. Passwords are protected with one-way hashing before storage.

The platform also avoids storing raw secrets for security-sensitive flows:

- Integration access keys are stored as hashes and are shown only once when created
- Password reset links and login tokens are not stored as raw reusable secrets
- Trusted-device tokens are stored as hashes
- Email two-factor codes and authenticator recovery codes are protected before storage
- Authenticator recovery codes are one-time use
- Authenticator app secrets are encrypted using instance-specific encryption material

Where external workflow trigger access is configured, keys can be scoped to specific workflows, given an expiry date, revoked, and deleted by authorized operators.

Data and secret encryption

Connect uses several protection methods depending on the type of information being protected:

- Customer data is kept in the customer's separate database, so each customer instance has its own data boundary.
- Customer access to Connect is protected over HTTPS, helping protect data while it moves between the user's browser and the platform.
- Sensitive application secrets are encrypted at rest using AES symmetric encryption with instance-specific encryption material.
- Encrypted secret values use a unique initialization value for each encrypted item, so the same secret is not encrypted into the same stored value each time.
- Passwords, integration access keys, reset links, login tokens, trusted-device

tokens, and verification codes are protected with one-way hashing rather than reversible encryption.

In practical terms, passwords and security tokens are designed not to be recoverable from storage, while secrets that the platform must use later, such as authenticator app secrets, are encrypted using the customer's instance-specific encryption material.

Request protection

The web application applies common request and browser protections:

- HTTPS is enforced for customer access
- Browser protections are enabled for production access
- Anti-forgery protection
- Login and workflow trigger authentication throttling, with a default of 5 attempts per minute per IP address
- Content-type sniffing protection
- Frame restrictions
- Referrer policy
- Permissions policy for browser features such as geolocation, microphone, and camera

Access control and auditability

Access is role-based. Managers can manage customer users, roles, audits, and other manager-level areas. Platform-level access is reserved for Kinspeed support or approved platform operators.

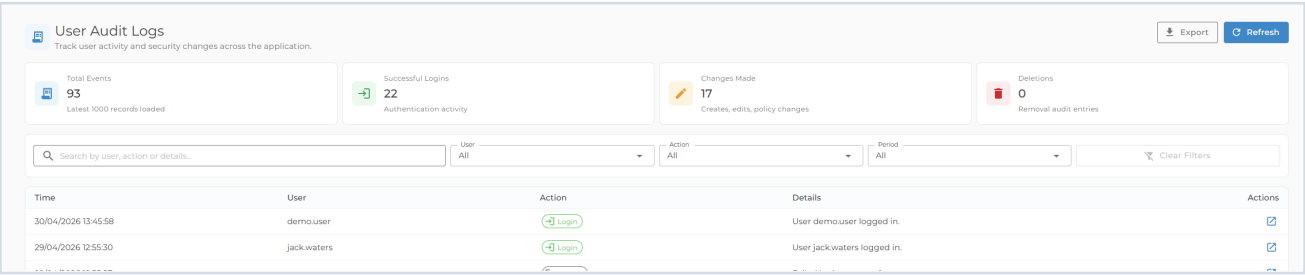
Customer managers cannot manage protected platform operator accounts or assign platform-level privileges.

Audit logs record security and operational activity, including:

- Login and logout
- Failed login attempts
- Account lockouts and blocked login attempts
- User, role, workflow, and integration access changes
- Password reset and account security changes
- Workflow activity

Audit entries include timestamps and, where available, request metadata such as IP address and user agent.

Audit logs



Scope

This document describes platform controls implemented in Connect. It does not make claims about external compliance certifications, backup retention, disaster recovery targets, or customer-specific infrastructure arrangements unless those are separately confirmed by Kinspeed.