Identity & Access Management (IAM) Overview

Version: 2.0
Last Updated: 1st September 2026
Classification: Public

Identity & Access Management (IAM) Overview

This document describes the Identity and Access Management controls protecting customer accounts, platform resources, and administrative systems. Read together with the Security Overview, Infrastructure & Architecture Overview, and the Information Security Schedule.

Identity Security Principles

Least privilege, need-to-know access, defense in depth, strong authentication, separation of duties, and accountability through audit logging. Access is granted only where necessary to perform an authorized business function.

Identity Architecture

Identity services govern authentication and authorization for customer users and administrators, Concord support and operations personnel, APIs, and service accounts — each under authentication and authorization controls appropriate to that identity type.

Authentication

Concord supports username/password authentication, multi-factor authentication, Single Sign-On, federated identity, session management, and password reset workflows. Available methods depend on a customer's subscription and configuration.

Multi-Factor Authentication (MFA)

MFA is mandatory for internal privileged accounts in Concord's production environment — enrollment is enforced at login, not optional, and login genuinely withholds access until a valid code is verified. Where a tenant is configured to require Single Sign-On, MFA is satisfied through the customer's own identity provider instead of Concord's native check. Customers are encouraged to enable MFA for their own users wherever it's available to them.

Single Sign-On (SSO)

Customers may integrate Concord with an enterprise identity provider using SAML 2.0 or OAuth 2.0/ OpenID Connect (Okta, Google, or Microsoft as the OIDC provider). SSO can be required exclusively for a tenant, centralizing authentication and access-policy enforcement in the customer's own IdP.

Authorization

Following authentication, access is granted according to role-based access control (RBAC), considering assigned role, tenant boundary, application context, and administrative privilege. Users receive only the permissions necessary for their responsibilities.

Role-Based Access Control (RBAC)

Concord ships with a defined set of system roles spanning administrative, legal/compliance, development, and external-collaborator functions, plus support for custom roles built from a fixed permission set. Customers assign roles appropriate to their own governance requirements.

Privileged Access Management

Administrative access carries enhanced controls: restricted accounts, mandatory MFA in production, least-privilege assignment, activity logging, and periodic access review.

User Lifecycle Management

Joiners — provisioning, initial role assignment, access approval.

Movers — role and permission updates, access review.

Leavers — account deactivation, access removal, privileged-access revocation, and credential invalidation. Customers remain responsible for managing the lifecycle of their own user accounts.

Password Management

Where password authentication is used: complexity requirements, secure hashing, secure reset procedures, and protection against common/breached passwords.

Session Management

Session expiration, secure session tokens, and re-authentication for sensitive administrative actions where appropriate, reduce the risk of unauthorized use of an active session.

Service Accounts & API Credentials

API credentials support least-privilege scoping, rotation, secure storage, and activity monitoring, with revocation when no longer required. Customers are responsible for securely managing API credentials issued to their organization.

Access Reviews

Concord periodically reviews privileged access to internal systems, and encourages customers to review user access within their own organizations on a similar cadence to catch excessive privilege, dormant accounts, or role drift.

Audit Logging

Authentication, failed login attempts, MFA events, password resets, role changes, and administrative activity are logged to support security monitoring, incident investigation, and compliance activity.

Monitoring & Detection

Suspicious authentication attempts, repeated login failures, privilege escalation, and unusual access patterns are monitored as part of Concord's broader security monitoring program.

Shared Responsibility

Concord is responsible for: platform authentication and authorization, identity security controls, administrative access governance, and audit logging.

Customers are responsible for: managing their own user accounts and role assignments, promptly removing access for departing personnel, protecting credentials, and enabling MFA or SSO where available to them.

Additional Information

Available on request, subject to confidentiality obligations: Security Overview, Infrastructure & Architecture Overview, Information Security Schedule, and Secure SDLC & Vulnerability Management Overview.
