

IDENTITY & INTELLIGENCE

i2i Identity & Access

Control who can sign in, what they can do and who touched production

OVERVIEW

i2i Identity & Access is the central identity service for i2iCore. It holds organisations, users, roles and permissions, issues the signed tokens that the other services verify, and keeps an audit trail of sign-ins and administrative actions. Staff, partner staff and machine accounts are all managed in one console.

Alongside it, a separate production access service lets support staff launch a production application without ever seeing its password and open a browser-based SSH terminal to a server. Grants have a time window, administrators can watch and end live sessions, and every launch is audited, whether it was allowed or denied.

THE CHALLENGE

Operators give many people access to sensitive systems: their own staff, partner staff and automated integrations. Access is often granted in a hurry, is rarely reviewed and is hard to prove to an auditor. Support engineers who need production access are given shared passwords, and nobody can say afterwards who opened which system and when.

AT A GLANCE

- ✓ One-time-code sign-in hand-off between i2i consoles
- ✓ Roles and permissions grouped by application and module
- ✓ Time-boxed and emergency access with mandatory review
- ✓ Passwordless production launches, every one audited

Capabilities

Organisations and users

Each organisation is a tenant with its own users, and usernames are unique within it. Staff, partner and machine accounts follow different rules, and machine clients use client credentials with secrets shown once. A new tenant and its first administrator are created in one step.

Sign-in hand-off

A signed-in user moves between registered i2i consoles through a one-time code that is stored as a hash, is short-lived and is checked against the redirect address registered for the organisation. The redeemed session shares its identity for single sign-out.

Multi-factor codes and credential hardening

Users can be required to enter a code sent by SMS or email. Guess limits, rate limits and code expiry are settings. Password policy, session limits and per-user IP ranges add further control.

- Non-revealing forgotten password and username flows
- Session directory with revoke

Roles, risk tiers and entitlements

Roles bundle permissions organised by application, module and action. Each permission has a risk tier, and organisation entitlements cap the permissions that can take effect. Partner accounts are limited by an access profile.

Governance workflows

Access requests, break-glass emergency access, certification campaigns and segregation-of-duties rules cover the lifecycle of a grant. Every grant records where it came from: manual, profile, just-in-time or emergency.

Policy decisions

A decision service applies deny-first rules, requires fresh on-duty presence for higher-risk permissions and a just-in-time grant for the highest tier. Enforcement is an organisation setting.

Audit and compliance reports

An append-only audit log records the user, module, action, status, IP address and user agent. Views show privileged activity and observations such as repeated denials, login failures, off-shift activity and dormant privileged accounts.

- Five downloadable compliance reports
- Retention purge by policy

Production access

A separate service registers applications and SSH servers. A launch is validated against a grant, the target returns a one-time handle instead of a password, and the browser opens the target. SSH secrets are encrypted and write-only.

- Watch and end live sessions
- Audit with CSV download

Technical summary

TOKENS	Signed tokens verified by other services through a public key set; refresh and service tokens supported
SIGN-IN HAND-OFF	Proprietary one-time code between registered i2i consoles; not a federation standard
SECOND FACTOR	One-time code by SMS or email, per user or organisation default
POLICY ENGINE	Deny-first decisions; enforcement set per organisation
AUDIT	Append-only log with search, CSV download and retention purge
PRODUCTION ACCESS	One-time handle launch, browser SSH terminal, time-boxed grants, live session watch and end, audit
TENANCY	Multi-tenant; the platform operator organisation administers the rest
DATABASE	PostgreSQL for both the identity service and production access

Related modules

Modules operators often run alongside i2i Identity & Access. Each is a separate module; the integrations that exist are listed in the technical summary above.



Where it is used

Give a support engineer time-boxed elevated access

An engineer needs a higher-risk permission for one maintenance window. They raise an access request, an approver grants it for a set period, and it expires by itself. If it is an emergency, break-glass access is available and another person must review it afterwards.

Limit what a partner's staff can do

A distributor creates accounts for its own staff. Each partner account is capped by an access profile set by the operator, so the distributor can pass on only permissions inside that ceiling and cannot pass on more than the operator allows.

Review access every quarter

A security officer starts an access certification campaign. Reviewers keep or revoke each grant, segregation-of-duties rules flag conflicting roles, and the compliance reports list user access and emergency access for the auditors.

See i2i Identity & Access on your network

Talk to our team about your operator type, your network and where to start. We will show you the module and answer the technical questions.

i2icore.com/products/i2i-iam/

EMAIL

info@i2icore.com

PHONE

+91 7946033677 · +91 9925019774

AHMEDABAD (HQ)

507, Shivalik Shilp II, Opp ITC Narmada Hotel,
Satellite, Ahmedabad - 380 015, Gujarat

MUMBAI

91-92 Powai Plaza, Central Avenue Road, Hiranandani
Gardens, Powai, Mumbai - 400 076, Maharashtra

Specifications are subject to change as the product develops; confirm details for your deployment with i2iCore. Screens shown are illustrative. i2iCore, i2i AAA, i2i CRM, i2i BNG, i2i 360 and related names are marks of i2iCore Technologies. © 2026 i2iCore Technologies. All rights reserved.