

CORE ACCESS & NETWORK

i2i AAA

A RADIUS AAA server with a policy engine and operator console

Live sessions					ILLUSTRATIVE
SUBSCRIBER	ACCESS	GATEWAY	IP	STATUS	
FTTH-44120	PPPoE	bng-01	100.64.18.23	Authorised	
FTTH-51877	PPPoE	bng-02	100.64.22.140	Authorised	
ENT-2209	IPoE	bng-01	203.0.113.14	Authorised	
WIFI-GUEST-88	Hotspot	ap-lobby	10.20.4.77	Captive portal	
FTTH-39002	PPPoE	bng-02	–	Rejected: expired plan	
4 authorised · 1 rejected					IP logs retained · Trace

ILLUSTRATIVE SCREEN

OVERVIEW

i2i AAA is a RADIUS AAA server for ISPs and operators. It authenticates each subscriber, authorises what the session may use and records the accounting stream. The same node can also disconnect or re-shape a live session on request, so the network follows the plan the subscriber has bought.

Behaviour is set in a web console rather than in code. You define workflows made of steps, route each request to a workflow by source or condition, attach policies written in a compiled expression language and keep subscriber data in the database you already run. Nodes pull their configuration from a central control service and keep the last good copy on disk. It works with i2i BNG and i2i Hotspot as RADIUS clients and writes usage into the i2i billing schema, so accounting feeds invoicing directly.

THE CHALLENGE

Every subscriber login, Wi-Fi association and session record passes through the AAA layer. If it is slow to change, plans need code changes. If it is opaque, support teams cannot see why a user was rejected or dropped. If accounting is lost, revenue is lost. Operators need a server whose rules they can edit, whose sessions they can see and control, and whose records reach billing intact.

AT A GLANCE

- ✓ Access decided by plan, status and policy
- ✓ Live disconnect and speed change from the console
- ✓ Enterprise Wi-Fi with a managed certificate store
- ✓ Accounting written straight to billing

Capabilities

Workflow-driven request handling

Each request follows a workflow of steps. The engine routes it by source peer, peer group or a condition expression, so one node can serve broadband, Wi-Fi and enterprise access with different rules.

- Identify, profile lookup, authenticate, authorise
- Assign IP, response attributes, conditional response
- Framed route, bandwidth policy, capture MAC

EAP with a managed trust store

EAP-TLS checks client certificates against trust anchors that operators manage in the console. EAP-TTLS and EAP-PEAP run inside a server TLS tunnel. EAP messages are reassembled and correlated by state, and the Message-Authenticator is verified.

Policy expression language

Policies are written in a compiled expression language and evaluated per request. Items can reply, reject, set or add attributes. Vendor-specific attributes are addressed by number or by name through an editable dictionary.

Bandwidth and time-based QoS

QoS profiles, bandwidth policy, peer overrides by VLAN or plan and access-time schedules define what each subscriber gets. An agent enforces schedule changes on live sessions with CoA.

Accounting and billing feed

Start, Interim and Stop records are processed with gigawords support. CDRs go to the i2i billing database through a fallback chain, and a daily usage roll-up supports quota metering. Writes are queued and drained on shutdown.

Sessions and dynamic authorisation

Session managers apply concurrency limits and clear stale sessions, using in-memory, Redis or PostgreSQL stores. The console can disconnect a session, batch-disconnect a set or send CoA from a template.

Operator console

A web console covers nodes, peers, workflows, policies, datasources, sessions, request logs and analytics such as drop and disconnect analysis. Menus are permission-gated, and an audit log records administrative actions.

Deployment and tenancy

Nodes install as a systemd service from a tar package with upgrade and rollback scripts. Peers, nodes and datasources carry an organisation identifier for multi-tenant use.

Technical summary

RADIUS	Access on UDP 1812, accounting on 1813; RFC 2865, 2866, 2868, 2869, 3162, 3579, 4818 and 5176 (sender)
AUTHENTICATION	PAP, CHAP, MS-CHAPv2, EAP-TLS, EAP-TTLS (inner PAP), EAP-PEAP (inner GTC)
SUBSCRIBER DATA	JDBC lookup, i2i billing schema, LDAP (search and compare), external subscriber API, datasource groups
SESSION STORES	In-memory, Redis, PostgreSQL and i2i billing schema
MONITORING	SNMP v2c agent with RADIUS MIBs (RFC 4668 to 4672 series), HTTP-JSON exporter, live node telemetry
INTEGRATIONS	i2i billing database, i2i BNG and i2i Hotspot as clients, Redis, Mikrotik RouterOS API
CONTROL PLANE	Spring Boot service on PostgreSQL; node pulls configuration at start-up and on reload
DEPLOYMENT	Java service under systemd on Linux from a tar package; upgrade and rollback scripts; Dockerfile provided

Standards and interfaces

RADIUS

- RFC 2865 and 2866
- RFC 2868 tunnel attributes
- RFC 3162 and 4818 IPv6 attributes
- RFC 3579 EAP over RADIUS
- RFC 5176 dynamic authorisation (client)

SNMP

- RADIUS authentication and accounting MIBs, RFC 4669 to 4672 series

Related modules

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



Where it is used

Broadband ISP with PPPoE

A regional ISP points its gateways at i2i AAA. Each login is checked against the subscriber record in the billing database, the plan sets the speed through vendor attributes and the accounting stream lands in the billing schema. Support can then disconnect a subscriber from the console.

Enterprise and campus Wi-Fi

An operator serving business customers runs 802.1X with EAP-TLS, EAP-TTLS or EAP-PEAP. The team loads the issuing certificate authorities into the Trust Anchors screen, so only clients whose certificates chain to a trusted root are admitted.

Fair-use by time of day

A plan gives full speed overnight and a reduced speed in the evening peak. The access-time policy and its agent send CoA to running sessions when a schedule changes, so subscribers do not need to log in again for the new speed to apply.

See i2i AAA 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-aaa/

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.