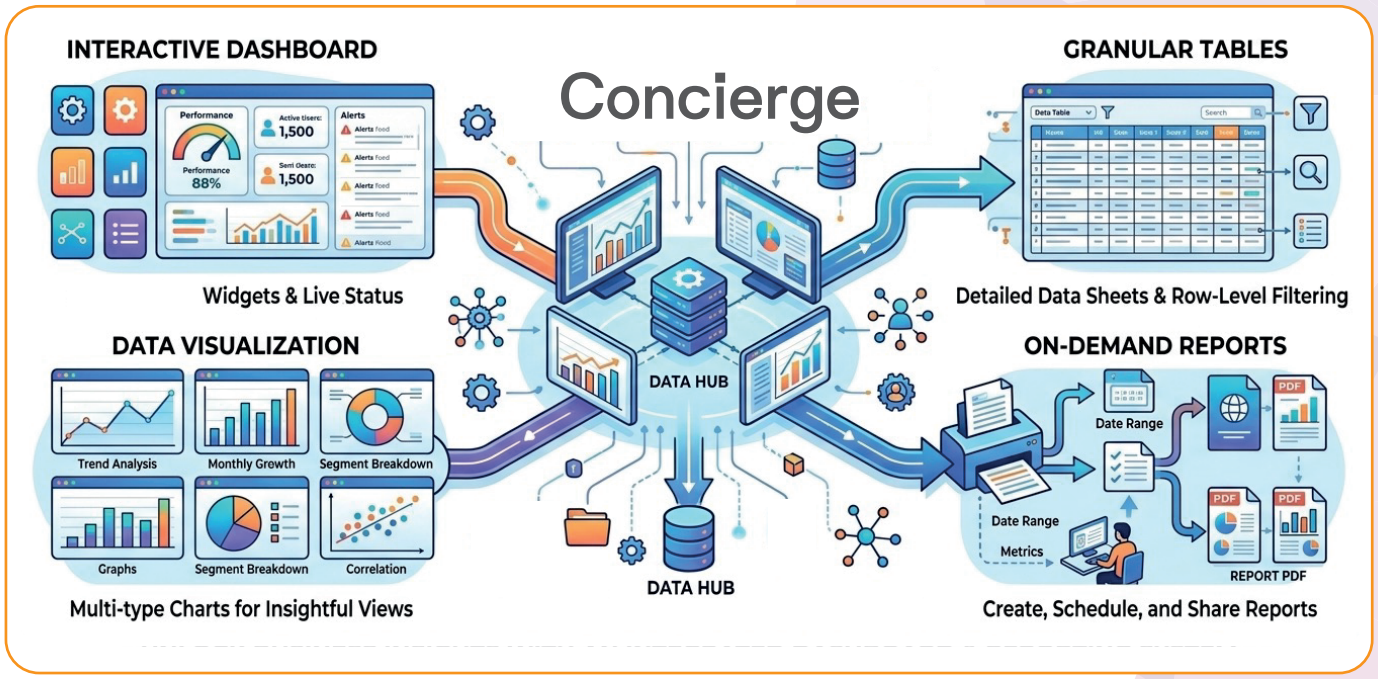
Concierge

INSIGHTS & MONITORING

Complete Visibility & Intelligence for Your Salt mSign Fleet

Concierge is a comprehensive data dashboard and reporting platform designed for organizations managing field-deployed fleets of Salt mSign MFA tokens. Moving beyond basic token status, Concierge transforms raw telemetry into actionable intelligence across five core pillars:

- **Reporting** – Deep insights into token usage, adoption rates, feature preferences, and operational metrics.
- **Planning** – Proactive tracking of token versions, forced updates, impacted users, and OS patches.
- **Performance** – Fleet-wide optimization for peak load handling and superior user experience.
- **Troubleshooting** – Real-time visibility into tokens operating in the field.
- **Fraud Detection** – Granular forensic views of historic token activity, multi-profile tracking, and host device profiles.



By centralizing telemetry from every deployed token into a unified data hub, Concierge bridges the gap between raw field activity and enterprise decision-making. The platform continuously ingests, processes, and structures distributed mobile data—translating complex device interactions, app permissions, and authentication sessions into intuitive interactive dashboards, granular tables, multi-type data visualizations, and on-demand reports that empower administrators to monitor performance, plan updates, and secure their entire ecosystem at a glance.

The Mobile MFA Blind Spot

Historically, mobile tokens like Salt mSign replaced hardware tokens (Vasco, RSA, Smartcards). However, management frameworks built for hardware tokens are fundamentally broken for mobile. Hardware tokens were uniform, self-contained devices tracked simply by serial number, server-side OTPs, and internal clocks. **All hardware tokens are identical.**

Mobile tokens are entirely different. They rely on user-owned (BYO) devices subject to varying manufacturer OS builds, biometrics, cameras, screen sizes, and secure storage environments. Your MFA app lives in a complex, potentially hostile ecosystem.

Without specialized oversight, organizations face total operational darkness:

- **The MFA Black Box**: Operating without visibility into what your mobile MFA fleet is actually doing.
- **Blind Flight**: Managing a mission-critical security layer with zero real-time device telemetry.

Unmasking the Unknowns in the Field

Concierge captures, aggregates, and visualizes critical telemetry from every active Salt mSign token, giving you direct visibility into:

- **Device Architecture**: Model, OS versions, hardware specs, and device "time" offsets with the server.
- **App Permissions**: Push notification status, camera access, and biometric capabilities.
- **Security & Integrity**: RASP (Runtime Application Self-Protection) errors and security flags.
- **Authentication Flow**: Sign-in method (PIN vs. Biometric), launch vectors (Icon, Notification Center, Inter-App), and screen-time duration.
- **Lifecycle & History**: Token profiles, serial numbers, activation dates, and status (Active, Menu-Reset, Blocked).

Precision Intelligence & Forensic Depth

1. Multi-Token & Multi-Profile Mapping
   - **Tokens on Device**: View all token serial numbers and profile names residing on a single device, including status and last usage dates.
   - **Cross-Device Traceability**: Track a profile name as a user migrates across multiple phones and token serial numbers over time.
2. Granular Session Forensics
   - **Authentication Session Depth**: Gain frame-by-frame visibility into completed authentication sessions, including app launch methods, authentication types used (Push, QR, OTP, Inter-App), and exact time spent reviewing transaction summaries (including scroll behavior).
   - **Diagnostic Insight**: Leverage session data to isolate why users fail to receive Push notifications.
   - **Surgical Blocking**: Isolate and block vulnerable device OS, hardware, and app version combinations with precision.

Operational Governance & Surgical Mitigation

Raw telemetry is only valuable when it empowers action. Beyond passive monitoring, Concierge equips security administrators with the operational leverage required to secure mobile fleets dynamically:

- **Targeted Enforcement & OS Patching**: When critical vulnerabilities emerge in specific mobile OS builds or device hardware combinations, Concierge allows you to instantly identify precisely which users are impacted. Deploy forced updates or surgical restrictions with precision rather than blanket, disruptive blocks.
- **Proactive Helpdesk Empowerment**: Enable support teams with a complete historical timeline of user profiles, token serial numbers, and device switches. When a user is locked out or experiencing authentication failures, support agents can instantly verify past device contexts and resolve issues without compromising security protocols.
- **Lifecycle Anomaly Detection**: Track behavioral drift across multi-device migrations. Spot unusual patterns—such as rapid re-activations or overlapping profile states—before they escalate into credential compromise or identity fraud.
- **Audit-Ready Compliance Reporting**: Generate point-in-time snapshots and compliance logs tracking token distribution, app version parity, and operating system adoption across your entire organizational footprint for regulatory audits.
- **Push-Notification Diagnostics**: Instantly pinpoint permission block settings that cause silent push-delivery failures for individual remote users.
- **Adoption and Feature Analytics**: Measure real-world feature uptake—such as biometric sign-in preferences versus PIN entry or Inter-App launching workflows—to drive product planning and future mSign rollout milestones.

Purpose-Built for MFA — Not Just System Health

mSign Concierge is **not** an Application Performance Monitoring (APM) tool like Dynatrace, Datadog, or New Relic.

While APM tools focus on general infrastructure health (bottlenecks, server crashes, and network latency), **Concierge operates a layer above network telemetry**:

- **Zero Configuration**: Day-one, out-of-the-box dashboards tailored specifically for Salt mSign—no weeks of custom system telemetry setup required.
- **Contextual Security Data**: Specialized information tailored entirely for product management, security teams, and administrators tracking the real-world user experience of mobile MFA tokens.

Salt Group Pty Ltd
Level 30, 459 Collins Street
Melbourne VIC 3000
Australia

Australia & Asia Pacific
T: +61-3-9614-4416
F: +61-3-9614-2992
E: sales@saltgroup.com.au