# One of the Defence Establishments in India Achieves Unified Identity Control and Mission-Ready SSO Across Classified Systems with eMudhra SecurePass IAM

## Client Overview

The One of the Defence Establishments in India (One of the Defence Establishments in India) is one of the world's largest air forces, operating a complex, technology-intensive estate of mission-critical systems across airbases, command headquarters, maintenance depots, training establishments, and forward operational locations nationwide. As part of India's ongoing defence modernisation programme, One of the Defence Establishments in India has progressively digitised its operational, administrative, and logistics functions — deploying a broad portfolio of classified applications and secure networks spanning flight operations, mission planning, maintenance management, personnel systems, intelligence platforms, and inter-service communication infrastructure. The delivery partner for a significant portion of this digital estate is the defence electronics implementation partner, India's premier defence electronics public sector undertaking, which implements and supports the integrated implementation environment. Securing access to this environment — across a large, geographically dispersed user base interacting with multiple classified systems simultaneously — is a security and operational imperative that directly determines One of the Defence Establishments in India's ability to sustain mission readiness.

## The Challenge

Across the the implementation environment, One of the Defence Establishments in India personnel — from aircrew and operations officers to ground crew, logistics managers, and administrative staff — were required to authenticate separately into each of the classified applications and secure networks they used in the course of their duties. With multiple systems in daily operational use across departments and locations, the cumulative authentication burden was substantial: personnel managing separate credentials for each application faced repeated login cycles that consumed operational time, introduced friction at exactly the moments when speed and focus matter most, and created a proliferating credential landscape that was difficult for both users and security administrators to manage securely.

"In an air force environment, every second of operational friction has a cost. Our personnel were managing multiple credentials across dozens of classified systems, and our security team had no unified view of who was accessing what. SecurePass SSO addressed both — simplifying access without compromising the security controls our environment demands."

**— Air Vice Marshal, Information Management & Communication, One of the Defence Establishments in India**

The security consequences of this fragmented access environment were equally significant. Multiple credential sets per user create multiple attack surfaces: each additional password represents a potential point of credential compromise, phishing exposure, or weak-password risk. Without a centralised identity governance framework, enforcing consistent security policies — password complexity, credential rotation, access scope alignment with current role and clearance — across all systems was operationally impractical, resulting in security standards that varied by system and by administrative unit. Multi-factor authentication, essential for access to systems of One of the Defence Establishments in India's classification sensitivity, was either absent or inconsistently applied across the the implementation environment application estate, leaving a significant proportion of classified system access points protected by password authentication alone.

Access management across the the implementation environment environment was administered manually and in isolation per system — with no centralised provisioning platform, no automated deprovisioning workflows, and no unified oversight of access rights across the full application estate. Personnel postings — a routine and high-frequency event in a military organisation — required access changes to be manually executed across each affected system individually, creating delays during which personnel either lacked access they needed for their new role or retained access that should have been revoked from their previous posting. The latter created a persistent, unacceptable insider threat exposure in an environment where classified system access carries direct national security implications. Privileged access — held by the implementation partner system administrators and One of the Defence Establishments in India IT officers — was similarly ungoverned, with no session monitoring, no time-bound access controls, and no mechanism to detect anomalous privileged activity before it escalated.

## The Solution

The One of the Defence Establishments in India, working with the implementation partner as the implementation partner, deployed eMudhra's SecurePass IAM platform — with Single Sign-On (SSO) as the centrepiece capability — to unify identity governance, eliminate authentication friction, and establish centralised, defence-grade access control across the the implementation environment classified system environment.

SecurePass SSO was deployed across the the implementation environment application portfolio, enabling One of the Defence Establishments in India personnel to authenticate once — through a single, secured login event — and access all authorised classified applications and systems within their session, without re-authenticating per system. SSO was implemented using federated identity protocols that allow SecurePass IAM to act as the central identity broker across the implementation environment's heterogeneous application landscape — including legacy and modern systems — providing a consistent, governed authentication experience regardless of the underlying application architecture. The authentication event itself was strengthened: Multi-Factor Authentication (MFA) was enforced at the SSO gateway for all users, with step-up authentication controls requiring enhanced verification for access to the most sensitive classified systems. This combination — single authentication point, but with MFA enforced — achieved the dual objective of reducing authentication friction for users while simultaneously raising the security standard above what individual application-level password authentication had previously delivered.

A centralised identity repository was established as the authoritative source for all One of the Defence Establishments in India user identities across the the implementation environment environment. Role-Based Access Control (RBAC) policies were designed in alignment with One of the Defence Establishments in India's rank, role, and clearance framework: access entitlements to classified applications are defined by the combination of an individual's current posting, functional role, and authorised clearance level — automatically provisioned when assignments are made and consistently enforced across all integrated systems. This policy-driven approach replaced the system-by-system, manually maintained access configurations that had varied across the implementation environment's application estate, and established the consistent, auditable access control framework that classified defence systems require.

Automated user lifecycle management was deployed to govern the access implications of One of the Defence Establishments in India's high-frequency personnel posting cycle. When an officer or airman is posted to a new assignment, SecurePass IAM automatically updates their access entitlements across all the implementation environment systems to reflect their new role and clearance — provisioning required access and simultaneously revoking entitlements from their previous posting — eliminating both the access gaps and the residual access risks that manual administration had produced. Privileged Access Management (PAM) was implemented as a dedicated governance layer, bringing the implementation partner system administrators and One of the Defence Establishments in India IT officers' privileged access under structured control: approval workflows, time-bound access grants, full session recording, and real-time anomaly alerting ensure that the most sensitive access rights within the the implementation environment environment are exercised under continuous oversight. The unified audit trail spanning SSO authentication events, access changes, privileged sessions, and policy exceptions provides One of the Defence Establishments in India's security leadership and defence auditors with the complete, on-demand accountability record required for classified environment governance.

## Results

The deployment of eMudhra SecurePass IAM — with SSO at its core — delivered a measurable transformation across all four dimensions One of the Defence Establishments in India had identified as strategic objectives: security posture, operational efficiency, centralised identity control, and mission readiness.

| Metric | Before | After |
|---|---|---|
| **Authentication Experience** | Separate login per classified application | Single Sign-On across all the implementation environment systems |
| **Identity Governance** | Fragmented; no centralised control | Unified identity management across all departments and networks |
| **Access Control Framework** | Inconsistent; manually administered per system | Centralised RBAC enforced across all classified applications |
| **Multi-Factor Authentication (MFA)** | Absent or inconsistently applied | MFA enforced at all access points; step-up for classified systems |
| **Privileged Access Governance** | Uncontrolled; no session monitoring | PAM with session recording, time-bound grants, anomaly alerting |
| **User Provisioning & Deprovisioning** | Manual; delayed across multiple systems | Automated lifecycle; simultaneous revocation across all systems |
| **Operational Efficiency & Mission Readiness** | Impaired by authentication friction and admin overhead | Streamlined access; reduced admin burden; enhanced readiness |

SecurePass SSO eliminated the per-application authentication overhead that had consumed operational time and degraded focus across One of the Defence Establishments in India's personnel, replacing multiple credential management burdens with a single, MFA-secured session spanning all authorised classified applications. The concentration of authentication into a single governed gateway — with MFA enforced and step-up controls for the most sensitive systems — materially strengthened One of the Defence Establishments in India's

authentication security posture above what distributed, application-level password controls had previously delivered. Centralised RBAC and automated lifecycle management aligned access entitlements precisely to current role and clearance in real time, closing the residual access window created by manual posting-cycle administration and eliminating the insider threat exposure it had sustained. Privileged access governance brought the highest-risk access rights in the the implementation environment environment under continuous, auditable oversight — providing One of the Defence Establishments in India's security leadership and defence auditors with the accountability visibility that classified system governance demands. Taken together, the reduction in authentication friction, elimination of access management overhead, and strengthened security controls directly contributed to the enhanced mission readiness that the the implementation environment programme had set as its defining measure of success.

## About eMudhra

eMudhra is a globally trusted provider of digital trust services, offering eSignatures, PKI, Certificate Lifecycle Management, Multi-Factor Authentication, and Identity & Access Management solutions. Licensed by the Controller of Certifying Authorities (CCA), India, eMudhra serves 1000+ enterprises across 40+ countries, helping organisations build secure, compliant, and paperless digital ecosystems.