SECUREPASS · DEFENCE · INDIA

A Defence organisation in India Strengthens Security Posture and Mission Readiness Across Its Research Establishment with eMudhra SecurePass IAM

SECTOR	REGION	SOLUTION
Defence	India	SecurePass

CLIENT OVERVIEW

The A Defence Organisation in India (A Defence Organisation in India) is India's premier defence research and development agency, operating under the Ministry of Defence. With a network of over 50 specialised laboratories and establishments distributed across the country — spanning aerospace, armaments, electronics, combat vehicles, naval systems, life sciences, and advanced materials — A Defence Organisation in India employs tens of thousands of scientists, engineers, technicians, and administrative personnel engaged in classified research and the development of cutting-edge defence technologies for the national armed forces. The organisation operates some of India's most sensitive information systems: classified research databases, design repositories, inter-laboratory collaboration platforms, testing and evaluation infrastructure, and inter-agency communications systems that collectively represent critical national security assets requiring the highest standards of identity assurance, access governance, and operational security.

THE CHALLENGE

Across A Defence Organisation in India's vast, geographically distributed network of laboratories and establishments, identity and access management had evolved organically rather than strategically — each lab and establishment developing its own user directory, access control mechanisms, and authentication procedures in accordance with local administrative practices rather than an overarching, organisation-wide security framework. The result was a deeply fragmented identity landscape: a large user base spread across dozens of sites, each operating with different systems, different credential management practices, and no unified view of who held access to which systems across the organisation. For an agency whose information assets are classified at the highest levels of national sensitivity, this fragmentation represented a systemic security vulnerability.

The access management challenges this created were multi-dimensional. Privileged access — held by system administrators, senior scientists, laboratory directors, and personnel with rights to

> *"A Defence Organisation in India's systems contain some of India's most sensitive defence research. With a large, distributed user base and no centralised identity control, we faced real security risks — from insider threats to access sprawl across classified systems. We needed a platform built for the security standards that a defence research organisation demands. "*
>
> **Chief Information Security Officer, A Defence Organisation in India**

classified research repositories and sensitive operational systems — was managed without centralised oversight, session monitoring, or enforced least-privilege controls. In a defence research environment where the unauthorised access or exfiltration of a single classified project's data could have strategic national security consequences, the absence of privileged access governance was a material and unacceptable risk. Personnel movements — transfers between laboratories, promotions to new roles, secondments to joint programmes, and exits from the organisation — were handled through manual access change requests that were slow to execute and inconsistently tracked, leaving residual access entitlements active across sensitive systems long after they should have been revoked.

Multi-factor authentication — an essential control for access to classified systems — was either absent or inconsistently applied across A Defence Organisation in India's application and system estate, leaving authentication security dependent on passwords alone at many access points. Without a unified access monitoring and anomaly detection capability, A Defence Organisation in India's security operations team had no reliable mechanism to detect unusual access patterns, identify potential insider threat indicators, or respond to access anomalies before they escalated. The combination of fragmented identity governance, uncontrolled privileged access, delayed deprovisioning, and limited authentication security created a threat surface that was directly at odds with A Defence Organisation in India's mission-critical security obligations — and with the access governance standards increasingly expected of defence establishments under India's national cybersecurity framework.

THE SOLUTION

A Defence Organisation in India deployed eMudhra's SecurePass IAM platform to establish a centralised, defence-grade identity and access management framework across its laboratories and establishments — consolidating fragmented identity governance into a unified, policy-driven system designed to meet the exacting security requirements of India's foremost defence research

organisation.

SecurePass IAM was deployed as the authoritative identity platform for A Defence Organisation in India's organisation-wide user base — scientists, engineers, technicians, administrators, and contracted personnel across all laboratories and establishments. A centralised identity repository was established, integrating with A Defence Organisation in India's existing directory infrastructure to create a single, governed identity store from which access rights across all connected systems are administered. Role-Based Access Control (RBAC) policies were designed in alignment with A Defence Organisation in India's organisational hierarchy, security classification levels, and project-based access requirements: access entitlements are defined by role and clearance level, automatically provisioned when assignments are made, and consistently enforced across all integrated systems — replacing the inconsistent, manually administered access controls that had varied by laboratory and system.

Multi-Factor Authentication (MFA) was enforced across all access points to A Defence Organisation in India's high-security and classified systems — implementing a layered authentication approach that combines credentials with additional verification factors appropriate to the sensitivity of the systems being accessed. MFA enforcement eliminated the password-only authentication vulnerability that had persisted across significant portions of A Defence Organisation in India's system estate, substantially raising the bar against both external intrusion and insider credential misuse. For the most sensitive access scenarios — classified research repositories, privileged administrative functions, and inter-laboratory data exchange platforms — step-up authentication controls were configured to require enhanced verification commensurate with the access being requested.

Privileged Access Management (PAM) was implemented as a dedicated governance layer within SecurePass IAM, bringing A Defence Organisation in India's most sensitive access rights under structured, auditable control for the first time. Privileged accounts — including system administrators, database custodians, and senior research personnel with broad access rights — are managed under enhanced approval workflows, time-bound access grants, and session recording. Every privileged session is logged in full, with real-time monitoring alerts configured to flag anomalous activity patterns for immediate review by A Defence Organisation in India's security operations team. Automated user lifecycle management was deployed end-to-end: onboarding provisions identities and assigns roles through governed workflows; transfers automatically update access entitlements across all systems to reflect the new role and clearance; and exits trigger immediate, simultaneous revocation across every connected system — closing the residual access window that manual deprovisioning had left open across the distributed laboratory estate.

RESULTS

The deployment of eMudhra SecurePass IAM delivered a comprehensive transformation of A Defence Organisation in India's security posture, operational efficiency, and identity governance capability — establishing the centralised, defence-grade access control framework that an organisation of A Defence Organisation in India's scale, sensitivity, and national strategic importance demands.

METRIC	BEFORE	AFTER
Identity Management	Fragmented across labs and establishments	Centralised identity governance across all A Defence Organisation in India entities

METRIC	BEFORE	AFTER
Access Control Framework	Inconsistent; manually administered per system	Unified RBAC enforced across all sensitive systems
Privileged Access Governance	Uncontrolled; no oversight or session monitoring	Full privileged access management with session recording
User Provisioning & Deprovisioning	Manual; delayed revocation on exits and transfers	Automated lifecycle; immediate access revocation on exit
Multi-Factor Authentication (MFA)	Absent or inconsistently applied	MFA enforced across all high-security system access points
Insider Threat Detection	No unified access monitoring capability	Real-time anomaly detection and unified access audit trail
Mission Readiness & Operational Efficiency	Impaired by access friction and admin overhead	Streamlined access; reduced admin burden; enhanced readiness

Centralised identity management replaced the fragmented, laboratory-by-laboratory access landscape with a unified governance framework spanning A Defence Organisation in India's entire distributed estate — giving security leadership, for the first time, a single authoritative view of identity and access across the organisation. MFA enforcement across high-security systems closed the authentication gaps that had left classified access points reliant on password-only controls, materially strengthening A Defence Organisation in India's defence against both external and insider threats. Privileged access governance — with session recording, time-bound grants, and real-time anomaly alerts — brought A Defence Organisation in India's most sensitive access rights under the structured oversight that the national security stakes of its research mandate require. Automated deprovisioning eliminated the residual access risk endemic to manual, siloed administration, while streamlined access workflows reduced the operational friction that had impeded scientist and engineer productivity across the laboratory network — directly contributing to the enhanced mission readiness that A Defence Organisation in India's leadership had identified as a strategic objective of the IAM programme.

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 1,000+ enterprises across 40+ countries, helping organisations build secure, compliant and paperless digital ecosystems.

Customer name withheld for confidentiality.