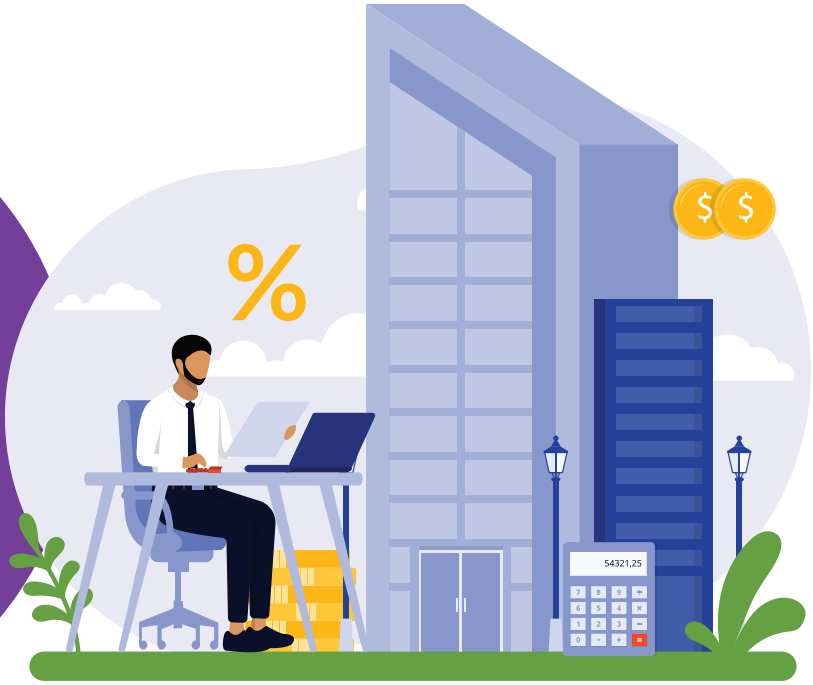
one of the Revenue Departments in India Unifies Identity and Access Governance Applications with eMudhra SecurePass IAM



Client Overview

The One of the Revenue Departments in India, operating under India's a national government ministry, is one of the country's largest and most operationally complex government organisations — responsible for the administration, assessment, and enforcement of direct taxation across India's vast and diverse economy. With a national footprint spanning thousands of officers, officials, and support personnel across regional offices, assessment units, investigation wings, and central headquarters, the Department operates a broad portfolio of government applications and information systems: from taxpayer-facing portals and e-filing platforms to internal assessment management systems, investigation databases, and inter-agency data exchange infrastructure. Securing access to these systems — and ensuring that the right personnel have precisely the right access, with full accountability — is a governance imperative that directly affects both the integrity of India's tax administration and the security of sensitive taxpayer data.

The Challenge

Across the One of the Revenue Departments in India's application landscape, identity management had evolved in parallel with each system rather than as a unified, centrally governed capability. Individual applications — assessment platforms, investigation systems, filing portals, internal workflow tools, and interagency interfaces — each maintained their own user directories, authentication mechanisms, and access control configurations. The result was a deeply fragmented identity ecosystem: officers and officials held separate credentials for each application, with no single authoritative identity store, no consistent access policy framework, and no unified view of who had access to what across the Department's entire system estate.

The operational consequences were significant and compounding. User provisioning — the process of granting, modifying, and revoking access as personnel join, transfer, or leave the Department — was handled manually by application administrators working in isolation across each system. Access changes were slow, inconsistent, and prone to error: personnel transfers and exits frequently left residual access entitlements active across systems long after they should have been revoked, creating a persistent insider threat exposure in an environment

> "Our officers were managing separate credentials for every system they used, and our administrators were manually maintaining access across dozens of applications with no central oversight. We had no reliable way to know, at any given moment, exactly who had access to which systems — and that was an unacceptable risk for an organisation handling the volume and sensitivity of data that the One of the Revenue Departments in India does."
>
> **Director General, Systems, One of the Revenue Departments in India**

handling highly sensitive taxpayer and investigation data. The absence of centralised deprovisioning meant that the Department could not guarantee timely access revocation — a control failure with serious information security and compliance implications.

The fragmented identity landscape also created an audit and compliance gap that grew in urgency as India's data protection and government IT security frameworks tightened. Without a unified access log spanning all applications, the Department could not produce a complete, reliable picture of user access activity for internal reviews, investigation support, or regulatory compliance assessments. Privileged access — held by system administrators, senior investigators, and personnel with access to sensitive databases — was similarly ungoverned: there was no centralised mechanism to enforce least-privilege principles, monitor privileged account usage, or demonstrate privileged access controls to government IT auditors. Meeting the identity governance standards increasingly mandated by the national technology ministry and the national IT standards body for government information systems required a fundamentally different approach to identity and access management.

The Solution

The One of the Revenue Departments in India deployed eMudhra's SecurePass IAM platform to replace its fragmented, application-siloed identity management with a centralised, policy-governed identity and access management framework spanning its full portfolio of government applications and systems.

At the foundation, SecurePass IAM established a single, authoritative identity store for the Department — consolidating the previously dispersed user directories from individual applications into a unified identity repository from which access rights across all connected systems are governed. Every officer, official, and support personnel across the Department's national footprint

is represented by a single, managed digital identity, with attributes, roles, and entitlements maintained centrally and propagated consistently across all integrated applications. This unified identity foundation eliminated the credential fragmentation that had required personnel to maintain separate logins per system, and provided administrators with the single-pane-of-glass visibility into user access that the Department had previously lacked entirely.

Single Sign-On (SSO) was implemented across the Department's government application portfolio, enabling officers to authenticate once and access all authorised systems within their working session — removing the friction of repeated logins across assessment tools, investigation systems, filing platforms, and internal workflow applications, while concentrating authentication events into a single, auditable entry point under SecurePass IAM's governance. Role-Based Access Control (RBAC) policies were designed in alignment with the Department's functional hierarchy and information classification requirements: access entitlements are defined by role, automatically provisioned when roles are assigned, and consistently enforced across all integrated applications — replacing the inconsistent, manually maintained access configurations that had previously varied per system.

Automated user lifecycle management was deployed end-to-end: when personnel join the Department, their identity is provisioned and roles assigned through a governed onboarding workflow; when they transfer, access entitlements are updated to reflect their new role and location; and when they exit, access across all connected systems is revoked immediately and simultaneously — eliminating the residual access risk that manual, siloed deprovisioning had made endemic. Privileged access governance was implemented as a distinct control layer within SecurePass IAM: privileged accounts are managed under enhanced approval and monitoring controls, with session activity logging and time-bound access grants enforcing least-privilege principles across the Department's most sensitive systems. The unified access audit trail — spanning authentication events, access changes, privileged sessions, and policy violations across all connected applications — provides the Department's CISO, compliance team, and government IT auditors with the complete, on-demand accountability record required under the national technology ministry and the national IT standards body identity governance standards.

Results

The deployment of eMudhra SecurePass IAM transformed the One of the Revenue Departments in India's identity and access management posture from a fragmented, manually administered patchwork into a centralised, policy-governed, and fully auditable framework — closing the governance gaps that had exposed the Department to insider threat risk and compliance vulnerability across its government application estate.

Metric	Before	After
Identity Management	Fragmented; siloed per application	Centralised identity store across all systems via SecurePass IAM
User Access Control	Inconsistent; manually administered	Unified, policy-driven RBAC enforced across all applications

Metric	Before	After
Single Sign-On (SSO)	Absent; separate login per system	SSO enabled; one authenticated session across all govt applications
User Provisioning & Deprovisioning	Manual; delayed and error-prone	Automated lifecycle management with immediate access revocation
Privileged Access Governance	Uncontrolled; no oversight mechanism	Privileged access managed and audited via SecurePass IAM
Insider Threat & Audit Visibility	Limited; no unified access log	Complete, real-time access audit trail across all systems
Compliance with Govt IT Standards	Partial; siloed controls insufficient	Fully aligned with the national technology ministry and the national IT standards body identity governance mandates

Centralised identity management eliminated the credential fragmentation that had burdened officers with multiple logins and denied administrators unified visibility across systems. SSO compressed the authentication experience for thousands of Department personnel while concentrating identity governance into a single, auditable platform. Automated provisioning and — critically — immediate, simultaneous deprovisioning across all connected systems closed the residual access exposure that manual, siloed administration had made endemic; personnel exits and transfers are now reflected across the Department's entire application estate in real time. The unified access audit trail and privileged access governance controls provide the Department's security and compliance leadership with the accountability visibility needed to satisfy government IT audit requirements and demonstrate alignment with India's evolving data protection and information security standards.

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.