CASE STUDY

SECUREPASS · MANUFACTURING · INDIA

A Specialty Chemicals Manufacturer in India Secures Plant and Office Access for a Dispersed Workforce with eMudhra SecurePass

SECTOR	REGION	SOLUTION
Manufacturing	India	SecurePass

CLIENT OVERVIEW

The organisation is a specialty chemicals manufacturer based in western India with two production facilities and a corporate office employing a combined workforce of around 1,600. The company produces formulations for the agriculture, textile, and construction sectors and has been investing in digitising its plant operations, including deploying a manufacturing execution system and an ERP platform that are accessible by both plant supervisors and corporate finance and procurement teams.

THE CHALLENGE

The company's IT team was managing access to the ERP, manufacturing execution system, HR portal, and several departmental tools using a mixture of local application accounts and Active Directory credentials — with no unified access management platform. Access provisioning happened through email requests to the IT team, and there was no systematic deprovisioning process when staff left. An HR audit found that 47 accounts for former employees remained active across various systems, including two accounts with ERP access that had not been reviewed since the staff members departed nearly a year earlier. The company's cybersecurity insurance provider had also asked for evidence of MFA on systems holding financial and operational data as part of the annual policy renewal — a requirement the company could not meet with its existing setup.

> *"Our insurance provider asked for evidence of MFA on financial systems and we couldn't provide it. That was the moment we realised our access management setup had fallen behind where it needed to be."*
>
> **Finance and Operations Director**

THE SOLUTION

eMudhra deployed SecurePass across the company's plant and corporate workforce. A centralised identity directory was established integrating with Active Directory and the HR system, and the 47 stale accounts were deactivated during the initial reconciliation. Automated joiner-mover-leaver workflows were configured to provision and deprovision access based on HR system triggers. MFA was enabled using OTP via authenticator app and SMS backup, applied to ERP and financial system logins — meeting the cybersecurity insurance requirement. SSO was configured for the ERP, MES, HR portal, and departmental tools, giving employees a single authenticated session. Role-based access profiles were defined for the main workforce categories — plant supervisors, production operators, finance staff, and procurement — with access scoped to the systems each role required.

RESULTS

All 47 stale accounts were deactivated within the first week. The company submitted MFA evidence to its cybersecurity insurer and successfully renewed the policy. In the year since deployment, no access-related security issues have been identified in either the plant or corporate environment.

METRIC	BEFORE	AFTER
Stale accounts deactivated	47 former employee accounts still active	All deactivated in initial reconciliation
MFA coverage — financial systems	Not in place; insurance requirement unmet	OTP MFA on ERP and financial systems
Account lifecycle process	Manual email requests; no deprovisioning process	Automated HR-integrated provisioning
SSO coverage	Separate credentials per application	ERP, MES, HR, departmental tools under SSO
Cybersecurity insurance	MFA evidence requested; could not provide	Evidence submitted; policy successfully renewed

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.