A Telecom Operator in India Strengthens Remote Access Security and Reduces Insider Risk Across a Field and NOC Workforce with eMudhra SecurePass

Client Overview

The organisation is a regional telecom operator in India offering mobile and broadband services with a combined workforce of around 2,800 employees — including network operations centre staff, field engineers, retail channel teams, and back-office functions. The company has been expanding its use of cloud-hosted management and business applications over the past two years, which has increased the importance of securing access for a workforce that is both distributed and regularly working outside the office.

The Challenge

Network operations centre staff and field engineers were accessing network management platforms, configuration tools, and ticketing systems using password-only authentication. Several of these systems held sensitive network configuration data, and the IT security team had raised the absence of MFA as a risk given the value of that data to external threat actors. An internal access review found that 38 accounts for former employees and contractors — several from a field force restructuring 18 months earlier — were still active across various network and business systems. There was also no consistent joiner-mover-leaver process, with provisioning requests handled through informal channels that varied by department and team manager.

> "Network management systems with password-only authentication are a risk we were aware of but hadn't fixed. Combined with dozens of active accounts for people who had left, it was a situation we needed to address properly."
>
> **Head of Network Security**

The Solution

eMudhra deployed SecurePass to manage identity and access for all 2,800 employees and the active contractor population. Integration with the HR system automated provisioning and deactivation, and the 38 stale accounts were deactivated during the initial reconciliation. MFA was enforced for all network management platform access using TOTP — suitable for NOC staff at workstations and for field engineers using mobile devices on-site. SSO was configured across the network management platform, ticketing system, HR portal, and key business applications, giving employees a single login for all authorised systems. Role-based access profiles were defined for NOC engineers, field engineers, retail staff, and back-office functions, with network management access scoped to the roles that required it. Remote access for field engineers was secured through MFA-gated VPN access rather than direct application exposure.

Results

All stale accounts were deactivated in the first week. MFA coverage on network management systems was achieved within six weeks of deployment. The IT security team closed the MFA risk item at the next quarterly review and reported the access management improvement to the company's technology committee.

Metric	Before	After
Stale accounts deactivated	38 former employee and contractor accounts active	All deactivated in initial reconciliation
MFA coverage — network management	Password only; risk item open	TOTP MFA enforced; risk item closed
Joiner-mover-leaver process	Informal; inconsistent across teams	Automated HR-integrated lifecycle management
SSO coverage	Separate credentials per system	Network, ticketing, HR, business apps under SSO
Remote access security	Direct application access; no MFA gate	MFA-gated VPN for all field engineer remote access

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.