CASE STUDY

SECUREPASS · BANKING & FINANCIAL SERVICES · EAST AFRICA

A Commercial Bank in East Africa Unifies Staff Access Across a Multi-Branch Network with eMudhra SecurePass

SECTOR	REGION	SOLUTION
Banking & financial services	East Africa	SecurePass

CLIENT OVERVIEW

The organisation is a commercial bank operating in two East African countries with 65 branches and around 1,800 employees. The bank has been investing in digital banking services, including a mobile banking platform and an internet banking portal, and has been upgrading its internal IT infrastructure to support a more connected and secure operating environment.

THE CHALLENGE

Branch staff across the network accessed the core banking system, loan management platform, and internal reporting tools using separate login credentials, with no single sign-on in place. Password resets were a frequent source of IT help desk calls, consuming staff time and occasionally delaying branch operations during busy periods. An internal security review found that a number of accounts belonging to former employees — primarily from a staff reorganisation 18 months earlier — were still active in the core banking system. The bank's central bank regulator had also raised access management as a point of improvement during its most recent IT inspection, citing the absence of MFA for core banking access as a specific gap.

> *"Handling password resets for branch staff was taking up a disproportionate share of our IT team's time. And when we found active accounts for people who left over a year ago, we knew we had a more serious problem to address."*
>
> **Head of IT and Digital Services**

THE SOLUTION

eMudhra deployed SecurePass across the bank's branch network and head office, covering all 1,800 employees. A centralised identity store was set up, integrating with the bank's HR system to automate account provisioning and deactivation. Stale accounts from the previous staff reorganisation were identified and deactivated during the initial reconciliation exercise. MFA was enabled using SMS OTP — suited to the branch environment where staff use shared workstations and personal smartphones are not always available. SSO was configured for core banking, loan management, and the internal reporting tool, reducing the number of credentials branch staff needed to manage. A self-service password reset portal was deployed, allowing staff to reset their own passwords after verifying their identity — without needing to call the IT help desk.

RESULTS

All stale accounts were deactivated during the initial reconciliation. Help desk calls related to password resets dropped by around 50% in the three months following the self-service portal launch. The central bank regulator reviewed the deployment during its next inspection and closed the MFA finding. The bank's IT team reported that the joiner-mover-leaver process, previously handled through email-based requests, was now consistent and auditable.

METRIC	BEFORE	AFTER
Stale accounts deactivated	Several dozen from prior reorganisation	All deactivated during initial reconciliation
Password reset help desk calls	Frequent; significant IT team overhead	~50% reduction via self-service portal
MFA coverage — core banking	Not in place; regulator finding raised	SMS OTP enforced; finding closed
Account lifecycle process	Manual email-based requests; inconsistent	Automated HR-integrated provisioning
SSO coverage	Separate credentials per system	SSO across core banking and key platforms

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.