SECUREPASS · TELECOMMUNICATIONS · MIDDLE EAST

A Broadband and Managed Services Provider in the Middle East Enforces Zero-Trust Access for Its Technical and Support Workforce with eMudhra SecurePass

SECTOR	REGION	SOLUTION
Telecommunications	Middle East	SecurePass

CLIENT OVERVIEW

The organisation is a broadband and managed services provider in the GCC, offering fixed internet, enterprise connectivity, and managed IT services to residential and corporate customers. The company employs around 950 staff across network operations, technical support, customer care, sales, and administration. As the company's managed services business has grown, it has taken on responsibility for managing customer IT environments — which has made the security of its own internal access controls a more prominent concern.

THE CHALLENGE

The company's technical support and managed services teams accessed internal management tools, customer management portals, and — through privileged connections — elements of customer network environments. These teams were using password-based authentication with no MFA, and the IT security manager had identified this as an exposure given that a compromised managed services account could potentially be used to access customer environments. A prospective enterprise customer raised the absence of MFA for the company's managed services staff as a condition they wanted addressed before signing a service agreement. The company also had no formal privileged access management for the accounts used by network engineers to access customer network devices.

> *"A prospective customer made MFA for our managed services team a condition of signing. It was a reasonable ask, and it pushed us to fix something we should have addressed earlier."*
>
> **Chief Operating Officer**

THE SOLUTION

eMudhra deployed SecurePass to enforce MFA and manage access for the company's full workforce, with a particular focus on the managed services and technical support teams. MFA was enforced using push notification and TOTP, applied to all internal system logins. For managed services staff accessing customer environments, a Privileged Access Management layer was configured within SecurePass, requiring additional authentication for privileged sessions and logging all privileged session activity for audit purposes. SSO was deployed across the internal customer management portal, ticketing system, HR platform, and managed services tooling. Role-based access profiles were defined for each team, with managed services accounts explicitly scoped to the customer environments each team member was authorised to access. An automated joiner-mover-leaver workflow was integrated with the HR system.

RESULTS

MFA was deployed for all staff within four weeks. The prospective enterprise customer reviewed the deployment and signed the service agreement. Privileged session logging for managed services access has been in place since go-live and has been referenced in two subsequent customer security reviews as a positive control.

METRIC	BEFORE	AFTER
MFA coverage — all staff	Not enforced; managed services teams at risk	Push and TOTP MFA for all 950 staff
Customer contract outcome	MFA condition blocking enterprise contract	Condition met; contract signed
Privileged access model	No PAM; no session recording for cust. access	PAM with full session logging for managed services
SSO coverage	Separate credentials per internal system	All key internal applications under SSO
Customer security reviews	MFA absence noted as concern	PAM controls cited positively in 2 reviews

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.