SECUREPASS · GOVERNMENT & PUBLIC SECTOR · MIDDLE EAST

A Government Ministry in Middle East Strengthens Internal Access Controls Ahead of a National Cybersecurity Audit with eMudhra SecurePass

SECTOR	REGION	SOLUTION
Government & public sector	Middle East	SecurePass

CLIENT OVERVIEW

The organisation is a government ministry in a GCC nation with around 2,200 employees across a central office and several field offices. The ministry operates a mix of on-premises and cloud-hosted systems, including a case management platform, a document management system, HR and finance applications, and interfaces with national government portals. In preparation for a national cybersecurity audit, the ministry's IT team reviewed its access management practices and identified a number of gaps requiring attention.

THE CHALLENGE

The ministry's employees used separate credentials for each system, with no MFA enforced for internal application access. An access review conducted ahead of the audit found that a number of accounts had access rights that did not align with current job roles — a result of promotions, internal transfers, and project assignments that had been handled without corresponding access updates. The national cybersecurity audit framework required ministries to demonstrate MFA enforcement, formal access review processes, and documented role-based access controls. The ministry had a limited window before the audit and needed a solution that could be deployed quickly and would produce the documentation required by the audit team.

> *"The audit framework was clear about what was needed — MFA, access reviews, role-based controls. We needed a platform that would let us meet those requirements in time and keep meeting them going forward."*
>
> **Head of Information Security**

THE SOLUTION

eMudhra deployed SecurePass within the ministry's available preparation window. A centralised identity directory was set up, consolidating user accounts from the ministry's various application stores. Role-based access profiles were defined for each job function within the ministry, and an access reconciliation exercise aligned existing accounts to the new role profiles — removing access that was no longer appropriate. MFA was enabled using TOTP and push notification options, applied to all internal system logins. An automated quarterly access review workflow was configured to generate reports for the IT security team and ministry leadership, fulfilling the audit framework's access review requirement. SSO was deployed across the ministry's key internal applications, reducing the number of separate credentials employees needed to manage.

RESULTS

The ministry completed its access remediation and MFA deployment ahead of the national cybersecurity audit. The audit team reviewed the SecurePass deployment and confirmed that the ministry's access controls met the framework requirements. The quarterly access review process has continued to run without manual intervention since deployment.

METRIC	BEFORE	AFTER
MFA enforcement	Not in place for internal systems	TOTP and push MFA across all application logins
Role-based access alignment	Access misaligned due to role changes	All accounts aligned to current role profiles
National cybersecurity audit outcome	Gaps identified ahead of audit	Access control requirements met; audit passed
Quarterly access reviews	No formal access review process	Automated quarterly reports for IT and leadership
SSO coverage	Separate credentials per system	Key internal applications under unified SSO

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.