



How **Access360 Helix** balances
autonomy and governance across 26
Agricultural Bank of Egypt branches

Agricultural Bank of Egypt is a wholly state-owned public sector bank headquartered in Giza, Greater Cairo. Founded in 1930, it is one of the largest agricultural banks in the Arab world and the most widely distributed bank in Egypt, with more than 1,200 branches and village banks across the country's governorates. Alongside agricultural and rural development finance, the bank provides retail, corporate, SME, and microfinance services.

IDCUBE implemented Access360 Helix across 26 main and regional branches. The deployment uses a federated architecture combining central governance with independent branch-level operations.

The Challenges

The major concerns faced by ICICI Lombard were:

- Access administration was distributed across branches, with each site managed independently.
- Policy and configuration changes had to be repeated branch by branch, increasing administrative effort and the risk of inconsistent settings.
- There was no common point for observing access activity or reporting across all 26 branches.
- Branch operations could not depend entirely on continuous connectivity to the center because the bank's network extends into remote and rural governorates.
- Independently administered branches created the possibility of configuration drift between locations.
- The deployment also had to satisfy the bank's cybersecurity compliance requirements.

The Requirements

Agricultural Bank of Egypt required the solution to:

- Bring the 26 branches in scope under a common access management framework.
- Provide central governance through a master configuration managed from one command center.
- Define user roles and policies once and apply them consistently across branches.
- Allow each branch to continue operating locally if connectivity to the center is interrupted.
- Consolidate events and reporting from all branches at the master level.
- Support future branch onboarding without rebuilding access policies from scratch.
- Meet the bank's cybersecurity and compliance expectations.

The Solution

IDCUBE deployed Access360 Helix using a federated architecture designed to combine central governance with local branch autonomy. Each of the 26 branches operates its own dedicated on-premises Access360 Helix server. The local server maintains the branch population, enforces access policies, and continues operating independently if communication with the center is unavailable. When connectivity returns, the branch server reconciles with the master server.

A master server provides the central control layer for the federation. Access templates and role definitions are created once at the master level and distributed to branch servers, allowing policies to be applied consistently across the estate without rebuilding them independently at each location.

The data flow works in both directions. Policy and configuration authority move outward from the master to individual branches, while access events and site data flow back to the master. This gives the central environment both the authoritative configuration and a consolidated record of activity across all 26 branches.

The deployment also addressed the bank's cybersecurity compliance requirements through IDCUBE's SOC 2 Type II, ISO 27001, and ISO 27018 certifications, GDPR compliance, and the vulnerability assessment and penetration testing (VAPT) performed on the platform.

The Results

The implementation delivered the following benefits to Agricultural Bank of Egypt:

- **Consistent Policy Across Branches:** Access roles and policies are defined once at the master level and inherited by branch servers, reducing configuration differences between locations.
- **Lower Administrative Effort:** Central templates remove the need to recreate the same access policies separately at each branch.
- **Consolidated Estate-Wide Reporting:** Events from all 26 branches are available at the master, allowing network-wide reporting without collecting and reconciling individual branch reports.
- **Operational Continuity at Branch Level:** Each branch continues enforcing access policies through its local server even when connectivity to the center is interrupted.
- **Improved Security Oversight:** Centralised event visibility allows access activity from any branch to be reviewed and investigated from the master environment.
- **Simpler Expansion:** New branches can be added to the federation and inherit existing templates rather than being configured as entirely independent systems.
- **Simplified Operator Experience:** Security teams can work from one federated environment instead of managing separate systems for each site.

Scan to explore more



USA

IDCUBE Corporation
20, Corporate Place South,
2nd Floor, Piscataway,
New Jersey – 08854 USA

691 S Milpitas Blvd
Ste 217 Milpitas
CA 95035 USA

Toll-free number:
+1 (833) 703-1765

UAE

IDCUBE FZE
Techno Hub 1 – Office
F 144 Dubai Silicon
Oasis Dubai, UAE

+971 4 388 7900

INDIA

IDCUBE Identification Systems
(P) Ltd.
B-19, Sector-2, Noida-201301
Uttar Pradesh, INDIA

+91 76761 10110