

GateKeeper & FFIEC Compliance

Proximity-Based MFA for Financial Institutions & Banking Environments

Why It Matters:

The Federal Financial Institutions Examination Council (FFIEC) establishes cybersecurity, risk management, and data protection standards for banks, credit unions, and other financial institutions. GateKeeper delivers proximity-based MFA, automatic session locking, and detailed audit trails that help financial institutions meet FFIEC expectations while improving daily workflow efficiency.

FFIEC Domain	FFIEC Requirement	How GateKeeper Meets It
1. Cyber Risk Management & Oversight	Institutions must maintain governance and oversight of cybersecurity risk, defining accountability and roles for access management.	GateKeeper enforces individual user accountability through proximity tokens + PINs, ensuring every access event is uniquely tied to a verified user. Administrators can centrally manage policies and monitor compliance through the Hub.
2. Threat Intelligence & Collaboration	Organizations must identify, assess, and respond to potential cyber threats and share relevant threat information internally.	GateKeeper logs all user activity, which can be integrated with SIEM systems for monitoring and reporting. Audit data enhances visibility and supports proactive threat analysis and collaboration across departments.
3. Cybersecurity Controls	Institutions must implement layered security controls—such as strong authentication, endpoint protection, and data safeguards—to prevent unauthorized access.	GateKeeper provides MFA using proximity tokens + PIN, auto-locks unattended computers, manages passwords securely, and integrates with Active Directory for centralized security control. This satisfies access control, data protection, and secure configuration guidelines.

4. External Dependency Management	<p>Institutions must oversee third-party vendors and external service providers to ensure security controls meet FFIEC standards.</p>	<p>GateKeeper offers both on-premises and cloud deployment options with secure communication between all components. GateKeeper never has access to organizational data or credentials. Both the client and hub applications use end-to-end encryption and device-level authentication to protect information. Organizations can document access boundaries, vendor dependencies, and use GateKeeper logs as evidence of third-party compliance control.</p>
5. Cyber Incident Management & Resilience	<p>Financial institutions must have plans for detecting, responding to, and recovering from cybersecurity incidents.</p>	<p>GateKeeper enables immediate workstation lockdown upon token removal or user departure, preventing data exposure during incidents. Authentication operates entirely offline, ensuring continued protection even if internet access is disabled during a cyber incident. For on-premises deployments, GateKeeper Hub provides automated daily backups to maintain data integrity and support recovery. Detailed audit logs assist in forensic analysis and incident investigations.</p>

Benefits for FFIEC-Regulated Institutions

- **FFIEC-Aligned MFA:** Provides workstation-level MFA that satisfies FFIEC cybersecurity expectations for strong authentication.
- **Automatic Session Lock:** Instantly secures systems when users leave, reducing insider and unattended access risks.
- **Data Protection:** Prevents unauthorized access and credential misuse while maintaining compliance with encryption and session control standards.



240-547-5446
info@gkaccess.com
gkaccess.com

- **Zero Password Sharing:** Each login is user-specific—ideal for shared computers in teller, back-office, or customer-service environments.
- **Audit-Ready Reporting:** Generates user-specific access logs for examiners and IT auditors to review quickly.
- **Improved Workflow Efficiency:** Staff log in and out in seconds using tokens and PINs, without retyping passwords.