GATEKEEPER

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

CMMC Level 3 Compliance with GateKeeper

“This is perfect for fulfilling the DoD requirements”

“This is perfect for fulfilling the DoD CMMC and SPRS requirements for 2FA, audit logs, … This product has worked flawlessly since it was installed and fully setup. The GateKeeper team was extremely helpful during the setup process (they will walk you through all of the required steps to get the system operational which helped tremendously).”

W. Faller
Owner

Automating CMMC compliance is the best way to enforce it. Automatically enforce strong 2FA without interrupting users’ workflows. The token automatically locks workstations when users leave – automatically securing computers from unauthorized access. Continuous authentication means significantly more secure sessions compared to “one-time” 2FA.

Control Family	Control ID	Description	CMMC Level	GateKeeper Proximity Enterprise
ACCESS CONTROL (AC)	AC.1.001	Limit information system access to authorized users, processes acting on behalf of authorized users, or devices (including other information systems). • FAR Clause 52.204-21 b.1.i • NIST SP 800-171 Rev 1 3.1.1 • CIS Controls v7.1 1.4, 1.6, 5.1, 14.6, 15.10, 16.8, 16.9, 16.11 • NIST CSF v1.1 PR.AC-1, PR.AC-3, PR.AC-4, PR.AC-6, PR.PT-3, PR.PT-4 • CERT RMM v1.2 TM:SG4.SP1 • NIST SP 800-53 Rev 4 AC-2, AC- 3, AC-17 • AU ACSC Essential Eight	1	**GateKeeper Enterprise provides proximity-based authentication and authorization to workstations. Using GateKeeper Enterprise, organizations can granularly assign access permissions to individuals/groups on a per workstation basis. GateKeeper automatically locks a user’s computer when they are no longer in proximity to their workstation, immediately protecting unauthorized users from accessing a system.**

ACCESS CONTROL (AC)	AC.1.002	Limit information system access to the types of transactions and functions that authorized users are permitted to execute. • FAR Clause 52.204-21 b.1.ii • NIST SP 800-171 Rev 1 3.1.2 • CIS Controls v7.1 1.4, 1.6, 5.1, 8.5, 14.6, 15.10, 16.8, 16.9, 16.11 • NIST CSF v1.1 PR.AC-1, PR.AC-3, PR.AC-4, PR.AC-6, PR.PT-3, PR.PT-4 • CERT RMM v1.2 TM:SG4.SP1 • NIST SP 800-53 Rev 4 AC-2, AC- 3, AC-17	1	**GateKeeper Enterprise provides proximity-based authentication and authorization to workstations. Using GateKeeper Enterprise, organizations can granularly assign access permissions to individuals/groups on a per workstation basis. GateKeeper automatically locks a user's computer when they are no longer in proximity to their workstation, immediately protecting unauthorized users from accessing a system.**
ACCESS CONTROL (AC)	AC.1.003	Verify and control/limit connections to and use of external information systems. • FAR Clause 52.204-21 b.1.iii • NIST SP 800-171 Rev 1 3.1.20 • CIS Controls v7.1 12.1, 12.4 • NIST CSF v1.1 ID.AM-4, PR.AC-3 • CERT RMM v1.2 EXD:SG3.SP1 • NIST SP 800-53 Rev 4 AC-20, AC-20(1)	1	**GateKeeper Enterprise provides proximity-based authentication and authorization to workstations. Using GateKeeper Enterprise, organizations can granularly assign access permissions to individuals/groups on a per workstation basis. GateKeeper automatically locks a user's computer when they are no longer in proximity to their workstation, immediately protecting unauthorized users from accessing a system.**
ACCESS CONTROL (AC)	AC.2.007	Employ the principle of least privilege, including for specific security functions and privileged accounts. • NIST SP 800-171 Rev 1 3.1.5 • CIS Controls v7.1 14.6 • NIST CSF v1.1 PR.AC-4 • CERT RMM v1.2 KIM:SG4.SP1 • NIST SP 800-53 Rev 4 AC-6, AC- 6(1), AC-6(5) • UK NCSC Cyber Essentials	2	**GateKeeper Enterprise provides proximity-based authentication and authorization to workstations. Using GateKeeper, organizations can granularly assign access permissions to individuals/groups on a per workstation basis. This helps enforce the concept of least privilege on a system level.**

ACCESS CONTROL (AC)	AC.2.009	Limit unsuccessful logon attempts. • NIST SP 800-171 Rev 1 3.1.8 • NIST CSF v1.1 PR.AC-7 • NIST SP 800-53 Rev 4 AC-7	2	**GateKeeper has the ability to lock a user's account after an administrator-defined number of unsuccessful login attempts.**
ACCESS CONTROL (AC)	AC.2.010	Use session lock with pattern-hiding displays to prevent access and viewing of data after a period of inactivity. • NIST SP 800-171 Rev 1 3.1.10 • CIS Controls v7.1 16.11 • NIST SP 800-53 Rev 4 AC-11, AC-11(1)	2	**GateKeeper automatically locks a user's workstation when they are no longer in proximity to their workstation - preventing access/viewing of data.**
ACCESS CONTROL (AC)	AC.2.013	Monitor and control remote access sessions. • NIST SP 800-171 Rev 1 3.1.12 • CIS Controls v7.1 12.11, 12.12 • NIST CSF v1.1 PR.AC-3, PR.PT-4 • CERT RMM v1.2 TM:SG2.SP2 • NIST SP 800-53 Rev 4 AC-17(1)	2	**GateKeeper Enterprise provides proximity-based authentication and authorization to workstations. Using GateKeeper Enterprise, organizations can granularly assign access permissions to individuals/groups on a per workstation basis. GateKeeper automatically locks a user's computer when they are no longer in proximity to their workstation, immediately protecting unauthorized users from accessing a system.**

ACCESS CONTROL (AC)	AC.3.017	Separate the duties of individuals to reduce the risk of malevolent activity without collusion. • NIST SP 800-171 Rev 1 3.1.4 • NIST CSF v1.1 PR.AC-4 • NIST SP 800-53 Rev 4 AC-5	3	**GateKeeper Enterprise provides proximity-based authentication and authorization to workstations. Using GateKeeper Enterprise, organizations can granularly assign access permissions to individuals/groups on a per workstation basis. GateKeeper automatically locks a user's computer when they are no longer in proximity to their workstation, immediately protecting unauthorized users from accessing a system.**
ACCESS CONTROL (AC)	AC.3.018	Prevent non-privileged users from executing privileged functions and capture the execution of such functions in audit logs. • NIST SP 800-171 Rev 1 3.1.7 • NIST CSF v1.1 PR.AC-4 • CERT RMM v1.2 KIM:SG4.SP1 • NIST SP 800-53 Rev 4 AC-6(9), AC-6(10)	3	**GateKeeper Enterprise provides proximity-based authentication and authorization to workstations. Using GateKeeper Enterprise, organizations can granularly assign access permissions to individuals/groups on a per workstation basis. This helps enforce the concept of least privilege on a system level.**
ACCESS CONTROL (AC)	AC.3.019	Terminate (automatically) user sessions after a defined condition. • NIST SP 800-171 Rev 1 3.1.11 • CIS Controls v7.1 16.7, 16.11 • NIST SP 800-53 Rev 4 AC-12	3	**GateKeeper automatically locks a user's workstation when they are no longer in proximity to their workstation - preventing access/viewing of data.**
AUDIT AND ACCOUNTABILITY (AA)	AU.2.041	Ensure that the actions of individual system users can be uniquely traced to those users so they can be held accountable for their actions. • NIST SP 800-171 Rev 1 3.3.2 • CIS Controls v7.1 16.8, 16.9 • NIST CSF v1.1 DE.CM-1, DE.CM- 3, DE.CM-7 • CERT RMM v1.2 MON:SG1.SP3 • NIST SP 800-53 Rev 4 AU-2, AU- 3, AU-3(1), AU-6, AU-11, AU-12	2	**GateKeeper Enterprise provides robust auditing capabilities that identifies when an individual user was in proximity to a workstation and successfully locked/unlocked it, even on shared accounts.**

AUDIT AND ACCOUNTABILITY (AA)	AU.2.042	Create and retain system audit logs and records to the extent needed to enable the monitoring, analysis, investigation, and reporting of unlawful or unauthorized system activity. • NIST SP 800-171 Rev 1 3.3.1 • CIS Controls v7.1 6.2 • NIST CSF v1.1. DE.CM-1, DE.CM- 3, DE.CM-7 • CERT RMM v1.2 MON:SG2.SP3 • NIST SP 800-53 Rev 4 AU-2, AU- 3, AU-3(1), AU-6, AU-11, AU-12	2	**GateKeeper Enterprise provides robust auditing capabilities that identifies when an individual user was in proximity to a workstation and successfully locked/unlocked it, even on shared accounts. These audit logs are retained indefinitely and can be on on-premise.**
AUDIT AND ACCOUNTABILITY (AA)	AU.2.044	Review audit logs. • CMMC • CIS Controls v7.1 6.7 • NIST CSF v1.1 PR.PT-1 • CERT RMM v1.2 COMP:SG3.SP1 • NIST SP 800-53 Rev 4 AU-6	2	**GateKeeper Enterprise provides robust auditing capabilities that identifies when an individual user was in proximity to a workstation and successfully locked/unlocked it. These audit logs are retained indefinitely.**
AUDIT AND ACCOUNTABILITY (AA)	AU.3.045	Review and update logged events. • NIST SP 800-171 Rev 1 3.3.3 • CIS Controls v7.1 6.7 • CERT RMM v1.2 IMC:SG2.SP2 • NIST SP 800-53 Rev 4 AU-2(3)	3	**GateKeeper Enterprise provides robust auditing capabilities that identifies when an individual user was in proximity to a workstation and successfully locked/unlocked it. These audit logs are retained indefinitely.**
AUDIT AND ACCOUNTABILITY (AA)	AU.3.049	Protect audit information and audit logging tools from unauthorized access, modification, and deletion. • NIST SP 800-171 Rev 1 3.3.8 • CERT RMM v1.2 MON:SG2.SP3 • NIST SP 800-53 Rev 4 AU-6(7), AU-9	3	**GateKeeper Enterprise provides robust auditing capabilities that identifies when an individual user was in proximity to a workstation and successfully locked/unlocked it. GateKeeper can connect to a syslog server and integrate with an enterprise security architecture. Authorized admins have the ability to export audit logs to further enable audit review, analysis, and reporting processes.**

AUDIT AND ACCOUNTABILITY (AA)	AU.3.050	Limit management of audit logging functionality to a subset of privileged users. • NIST SP 800-171 Rev 1 3.3.9 • CERT RMM v1.2 MON:SG2.SP2 • NIST SP 800-53 Rev 4 AU-6(7), AU-9(4)	3	**GateKeeper Enterprise provides robust auditing capabilities that identifies when an individual user was in proximity to a workstation and successfully locked/unlocked it. GateKeeper can connect to a syslog server and integrate with an enterprise security architecture. Authorized admins have the ability to export audit logs to further enable audit review, analysis, and reporting processes.**
AUDIT AND ACCOUNTABILITY (AA)	AU.3.051	Correlate audit record review, analysis, and reporting processes for investigation and response to indications of unlawful, unauthorized, suspicious, or unusual activity. • NIST SP 800-171 Rev 1 3.3.5 • CIS Controls v7.1 6.6, 6.7 • NIST CSF v1.1 DE.AE-3 • CERT RMM v1.2 COMP: SG3.SP1 • NIST SP 800-53 Rev 4 AU-6(3)	3	**GateKeeper Enterprise provides robust auditing capabilities that identifies when an individual user was in proximity to a workstation and successfully locked/unlocked it. GateKeeper can connect to a syslog server and integrate with an enterprise security architecture. Authorized admins have the ability to export audit logs to further enable audit review, analysis, and reporting processes.**
AUDIT AND ACCOUNTABILITY (AA)	AU.3.052	Provide audit record reduction and report generation to support on-demand analysis and reporting. • NIST SP 800-171 Rev 1 3.3.6 • NIST CSF v1.1 RS.AN-3 • CERT RMM v1.2 COMP:SG3.SP2 • NIST SP 800-53 Rev 4 AU-7	3	**GateKeeper Enterprise provides robust auditing capabilities that identifies when an individual user was in proximity to a workstation and successfully locked/unlocked it. GateKeeper can connect to a syslog server and integrate with an enterprise security architecture. Authorized admins have the ability to export audit logs to further enable audit review, analysis, and reporting processes.**

AUDIT AND ACCOUNTABILITY (AA)	AU.4.053	Automate analysis of audit logs to identify and act on critical indicators (TTPs) and/or organizationally defined suspicious activity. • CMMC • CIS Controls v7.1 6.6 • NIST CSF v1.1 DE.AE-3 • NIST SP 800-53 Rev 4 SI-4(2)	4	**GateKeeper Enterprise provides robust auditing capabilities that identifies when an individual user was in proximity to a workstation and successfully locked/unlocked it. These audit logs are retained indefinitely and can be sent automatically to administrators.**
AUDIT AND ACCOUNTABILITY (AA)	AU.4.054	Review audit information for broad activity in addition to per-machine activity. • CMMC • NIST CSF v1.1 PR.PT-1 • NIST SP 800-53 Rev 4 RA-5(6), RA-5(8), RA-5(10)	4	**GateKeeper Enterprise provides robust auditing capabilities that identifies when an individual user was in proximity to a workstation and successfully locked/unlocked it. These audit logs are retained indefinitely and can be sent automatically to administrators.**
AUDIT AND ACCOUNTABILITY (AA)	AU.5.055	Identify assets not reporting audit logs and assure appropriate organizationally defined systems are logging. • CMMC • CIS Controls v7.1 6.2 • NIST SP 800-53 Rev 4 AU-12	5	**GateKeeper Enterprise provides robust auditing capabilities that identifies when an individual user was in proximity to a workstation and successfully locked/unlocked it. These audit logs are retained indefinitely and can be sent automatically to administrators.**

IDENTIFICATION AND AUTHENTICATION (IDA)	IA.1.076	Identify information system users, processes acting on behalf of users, or devices. • FAR Clause 52.204-21 b.1.v • NIST SP 800-171 Rev 1 3.5.1 • CIS Controls v7.1 4.2, 4.3, 16.8, 16.9 • NIST CSF v1.1 PR.AC-1, PR.AC-6, PR.AC-7 • CERT RMM v1.2 ID:SG1.SP1 • NIST SP 800-53 Rev 4 IA-2, IA-3, IA-5	1	**GateKeeper Enterprise provides robust auditing capabilities that identifies when an individual user was in proximity to a workstation and successfully locked/unlocked it, even on shared computers. GateKeeper can connect to a syslog server and integrate with an enterprise security architecture. Authorized admins have the ability to export audit logs to further enable audit review, analysis, and reporting processes.**
IDENTIFICATION AND AUTHENTICATION (IDA)	IA.1.077	Authenticate (or verify) the identities of those users, processes, or devices, as a prerequisite to allowing access to organizational information systems. • FAR Clause 52.204-21 b.1.vi • NIST SP 800-171 Rev 1 3.5.2 • CIS Controls v7.1 4.2, 4.3, 16.8, 16.9 • NIST CSF v1.1 PR.AC-1, PR.AC-6, PR.AC-7 • CERT RMM v1.2 TM:SG4.SP1 • NIST SP 800-53 Rev 4 IA-2, IA-3, IA-5 • UK NCSC Cyber Essentials	1	**GateKeeper Enterprise provides proximity-based identification, authentication, and authorization to workstations. Using GateKeeper Enterprise, an organization can granularly assign access permissions to individuals/groups on a per workstation basis.**
IDENTIFICATION AND AUTHENTICATION (IDA)	IA.2.078	Enforce a minimum password complexity and change of characters when new passwords are created. • NIST SP 800-171 Rev 1 3.5.7 • CIS Controls v7.1 4.2, 4.4 • NIST CSF v1.1 PR.AC-1, PR.AC-6, PR.AC-7 • NIST SP 800-53 Rev 4 IA-5(1) • UK NCSC Cyber Essentials	2	**GateKeeper can integrate with an organization's Active Directory to enforce this control.**

IDENTIFICATION AND AUTHENTICATION (IDA)	IA.2.079	Prohibit password reuse for a specified number of generations. • NIST SP 800-171 Rev 1 3.5.8 • CIS Controls v7.1 4.2, 4.4 • NIST CSF v1.1 PR.AC-1, PR.AC-6, PR.AC-7 • NIST SP 800-53 Rev 4 IA-5(1)	2	**GateKeeper can integrate with an organization's Active Directory to enforce this control.**
IDENTIFICATION AND AUTHENTICATION (IDA)	IA.2.080	Allow temporary password use for system logons with an immediate change to a permanent password. • NIST SP 800-171 Rev 1 3.5.9 • NIST CSF v1.1 PR.AC-1, PR.AC-6, PR.AC-7 • NIST SP 800-53 Rev 4 IA-5(1)	2	**GateKeeper can integrate with an organization's Active Directory to enforce this control.**
IDENTIFICATION AND AUTHENTICATION (IDA)	IA.2.081	Store and transmit only cryptographically-protected passwords. • NIST SP 800-171 Rev 1 3.5.10 • CIS Controls v7.1 16.4, 16.5 • NIST CSF v1.1 PR.AC-1, PR.AC-6, PR.AC-7 • CERT RMM v1.2 KIM:SG4.SP1 • NIST SP 800-53 Rev 4 IA-5(1)	2	**GateKeeper utilizes military-grade AES-256 encryption to securely store and transmit passwords.**
IDENTIFICATION AND AUTHENTICATION (IDA)	IA.2.082	Obscure feedback of authentication information. • NIST SP 800-171 Rev 1 3.5.11 • NIST CSF v1.1 PR.AC-1 • NIST SP 800-53 Rev 4 IA-6	2	**GateKeeper PIN login is obscured and all authentication information is obscured.**

IDENTIFICATION AND AUTHENTICATION (IDA)	IA.3.083	Use multifactor authentication for local and network access to privileged accounts and for network access to nonprivileged accounts. • NIST SP 800-171 Rev 1 3.5.3 • CIS Controls v7.1 4.5, 11.5, 12.11 • NIST CSF v1.1 PR.AC-1, PR.AC-6, PR.AC-7 • CERT RMM v1.2 TM:SG4.SP1 • NIST SP 800-53 Rev 4 IA-2(1), IA-2(2), IA-2(3) • AU ACSC Essential Eight	3	**GateKeeper Enterprise has the capability to enforce multifactor authentication (MFA) for all access to a workstation.**
IDENTIFICATION AND AUTHENTICATION (IDA)	IA.3.084	Employ replay-resistant authentication mechanisms for network access to privileged and non-privileged accounts. • NIST SP 800-171 Rev 1 3.5.4 • NIST CSF v1.1 PR.AC-1, PR.AC-6, PR.AC-7 • NIST SP 800-53 Rev 4 IA-2(8), IA-2(9)	3	**GateKeeper is a proximity-based identification and authentication solution. A user must be present with their physical token to unlock their workstation, making it inherently replay-resistant.**
IDENTIFICATION AND AUTHENTICATION (IDA)	IA.3.085	Prevent the reuse of identifiers for a defined period. • NIST SP 800-171 Rev 1 3.5.5 • CIS Controls v7.1 16.7, 16.10, 16.12 • NIST CSF v1.1 PR.AC-1, PR.AC-6, PR.AC-7 • NIST SP 800-53 Rev 4 IA-4	3	**GateKeeper can integrate with an organization's Active Directory to enforce this control.**
IDENTIFICATION AND AUTHENTICATION (IDA)	IA.3.086	Disable identifiers after a defined period of inactivity. • NIST SP 800-171 Rev 1 3.5.6 • CIS Controls v7.1 16.9, 16.10, 16.11 • NIST CSF v1.1 PR.AC-1, PR.AC-6, PR.AC-7 • NIST SP 800-53 Rev 4 IA-4	3	**GateKeeper Proximity can integrate with an organization's Active Directory to enforce this control.**

"IT loves the fact we can put more secure passwords on all of our systems. Password resets have gone down while security has gone up."

David C.
Director of IT
Hospital & Health Care