

WINMAGIC[®] and CMMC

FIPS validated

WinMagic's SecureDoc Full Disk Encryption and MagicEndpoint Authentication are FIPS validated and can support Defense Industrial Base (DIB) contractors in achieving Cybersecurity Maturity Model Certification (CMMC) compliance. WinMagic solutions provide increased assurance that contractors and subcontractors are meeting the most stringent cybersecurity requirements that apply to acquisition programs and systems that process controlled, unclassified information.

Summary of CMMC Requirements Compliance for WinMagic

As an introduction, our passwordless authentication and laptop encryption solutions align with CMMC requirements, offering robust security measures to protect Controlled Unclassified Information and ensuring compliance with relevant regulations.

Overview: Our products, SecureDoc Encryption and MagicEndpoint Authentication, provide comprehensive solutions to meet various requirements outlined in the Capability Maturity Model Certification (CMMC). Our offerings ensure robust access control, audit and accountability, identification and authentication, maintenance, media protection, physical protection, and system & communications protection.

Access Control: SecureDoc & MagicEndpoint offer a suite of security features including group and role management, encryption key management, and robust authentication mechanisms. Administrators have centralized control over privileges and encryption keys, ensuring system access is restricted to authorized transactions and functions.

Audit & Accountability: Our software diligently monitors and documents various system events, maintaining audit logs with unique identifiers and timestamps. Access to audit logs is regulated, and cryptographic measures ensure data integrity. Management of audit logging functionality is restricted to privileged users.

Identification & Authentication: SecureDoc employs unique identifiers and multifactor authentication methods to verify user identities. It enforces password complexity requirements, prohibits password reuse, and secures authentication information cryptographically. MagicEndpoint introduces "no user action" authentication and aims to comply with NIST SP800-63C standards for federated authentication assurance.

Maintenance: Our solutions feature robust crypto-erase operations and mandate multifactor authentication for maintenance activities conducted via external network connections, enhancing data security during off-site maintenance.

Media Protection: SecureDoc ensures the confidentiality of Controlled Unclassified Information (CUI) through encryption techniques and rigorous sanitization processes. Access to CUI is restricted, and cryptographic mechanisms safeguard data during transport. Disk Access Control feature enables precise control over removable media usage.

Value added notes:

- Our products are FIPS Validated
- Our products are offering as an on-premise and cloud solution
- Our products offer Windows Login with the most comprehensive MFA including CAC / PIV card authentication.
- For the DIB community, the FedRamp option is a fairly expensive solution making it prohibitive or profitably unacceptable.
- Purchasing our solution is a more cost effective without compromising security or ease of use. In fact, we have the most secure solution with the best possible user experience – no user action for secure online authentication.
- Our solutions allow our customers to control access and storage of the keys. Therefore the data encrypted is no longer considered CUI.



Authenticate. Encrypt. Achieve.

US & Canada
+1 888 879 5879

EMEA
+49 69 175 370 530

Japan
+03 5403 6950

For more information, [click here](#) or contact WinMagic



Encryption and Authentication Solutions for Governments

To have industry-leading government cybersecurity solutions that protect intellectual property.

By employing robust multi-factor authentication access to data is restricted to authorized users and endpoints ensuring security for CUI with our advanced File and Folder encryption solution. Whether deployed on premise or through a Cloud Service Provider (CSP), our encryption solution offers versatile protection for both static and removable media, guaranteeing comprehensive coverage across your entire infrastructure. Our cost-effective approach compared to other solutions for Data at Rest and Data in Transit, allows you to achieve regulatory compliance while staying in budget and not eroding profitability. Safeguard your data efficiently, effectively and affordably with our authenticated encryption solution today.

WinMagic CMMC Level 2

SecureDoc

MagicEndpoint

Access Control

Authorized Access Control	AC.L2-3.1.1		✓
Transaction & Function Control	AC.L1-3.1.2	✓	
Least Privilege	AC.L2-3.1.5	✓	✓
Non-privileged Accounts	AC.L2-3.1.6		✓
Privileged Functions	AC.L2-3.1.7	✓	
Unsuccessful login attempts	AC.L2-3.1.8	✓	✓
Privacy and security notices	AC.L2-3.1.9	✓	
Session lock	AC.L2-3.1.10	✓	
Remote Access Control	AC.L2-3.1.12		✓
Wireless access protection	AC.L2-3.1.17		✓
Mobile device connection	AC.L2-3.1.18	✓	
Encrypt CUI on mobile	AC.L2-3.1.19	✓	
Portable storage use	AC.L2-3.1.21	✓	

Audit and Accountability

System auditing	AU.L2-3.3.1	✓	✓
User accountability	AU.L2-3.3.2	✓	✓
Audit failure alerting	AU.L2-3.3.4	✓	
Authoritative time source	AU.L2-3.3.7	✓	✓
Audit protection	AU.L2-3.3.8	✓	✓
Audit management	AU.L2-3.3.9	✓	

Identification and Authentication

Identification	IA.L1-3.5.1	✓	✓
Authentication	IA.L1-3.5.2	✓	✓
Multifactor authentication	IA.L2-3.5.3	✓	✓
Replay-resistant authentication	IA.L2-3.5.4		✓
Password complexity	IA.L2-3.5.7	✓	✓
Password reuse	IA.L2-3.5.8	✓	✓
Temporary passwords	IA.L2-3.5.9	✓	
Cryptographically protected passwords	IA.L2-3.5.10	✓	
Obscure feedback	IA.L2-3.5.11	✓	✓

Maintenance

Equipment sanitization	MA.L2-3.7.3	✓	
Nonlocal Maintenance	MA.L2-3.7.5		✓

Media Protection

Media Access	MP.L2-3.8.2	✓	
Media disposal	MP.L1-3.8.3	✓	
Media Markings	MP.L2-3.8.4	✓	
Portable storage encryption	MP.L2-3.8.6	✓	
Removable media	MP.L2-3.8.7	✓	
Protect Backups	MP.L2-3.8.9	✓	

Physical Protection

Alternative Work Sites	PE.L2-3.10.6	✓	✓
------------------------	--------------	---	---

System and Communications Protection

Role Separation	SC.L2-3.13.3	✓	
Data in Transit	SC.L2-3.13.8	✓	
Key Management	SC.L2-3.13.10	✓	✓
CUI Encryption	SC.L2-3.13.11	✓	✓
Communications Authenticity	SC.L2-3.13.15		✓
Data at Rest	SC.L2-3.13.16	✓	