

CMMC Level 2 Requirements Guide

NIST SP 800-171 Rev 2 Controls Mapped to ForteFide Scanner

Version	1.4.2
Controls	110
Families	14

DenseDefense | Confidential

What is CMMC Level 2?

The Cybersecurity Maturity Model Certification (CMMC) Level 2 requires organizations handling Controlled Unclassified Information (CUI) to implement 110 security practices from NIST SP 800-171 Rev 2 across 14 families.

ForteFide scans all 110 controls across Windows and Linux, providing automated assessment with evidence collection.

Control Families

ID	Family	Qty	Scope
AC	Access Control	22	Limit access, control flow, enforce least privilege
AT	Awareness & Training	3	Security awareness and role-based training
AU	Audit & Accountability	9	Create, protect, and retain audit logs
CM	Configuration Management	9	Security configs, change control
IA	Identification & Auth	11	MFA, password policy, device auth
IR	Incident Response	3	Detect, report, respond to incidents
MA	Maintenance	6	Timely maintenance, control tools/personnel
MP	Media Protection	9	Protect and sanitize media with CUI
PE	Physical Protection	6	Physical access controls (policy-based)
PS	Personnel Security	2	Personnel screening, access termination
RA	Risk Assessment	3	Risk assessment, vulnerability scanning
CA	Security Assessment	4	Assess controls, plans of action
SC	System & Comm Protection	16	Comms monitoring, crypto, boundary defense
SI	System & Info Integrity	7	Flaw remediation, malware protection, monitoring

Automated vs Manual Controls

ForteFide automates assessment of all 110 controls. 11 require manual attestation:

Family	Count	Scope
AT -- Awareness & Training	3	Security awareness training programs
PE -- Physical Protection	6	Physical access controls, visitor logs
PS -- Personnel Security	2	Personnel screening, access termination

7-Step Compliance Workflow

ForteFide's 7-step workflow takes you from initial scan to assessment-ready evidence:

- Steps 1-3: Discover, prepare, and scan your environment
- Step 4: Baseline evidence auto-collected (pre-remediation state)
- Step 5: Review findings, attest manual controls, document exceptions
- Step 6: Automated remediation with safety engine, then rescan
- Step 7: Collect final evidence and tear down service accounts

Evidence Package

ForteFide generates a 23-document signed evidence package for C3PAO assessment:

- System Security Plan (SSP)
- Plan of Action & Milestones (POA&M)
- SPRS Scorecard
- Per-control evidence with command output and timestamps
- 14 policy documents (one per applicable family)
- Verification manifest (SHA-256 + Ed25519 digital signature)

SPRS Scoring

- Start at 110 points (perfect)
- Each NOT MET deducts 1, 3, or 5 points by severity
- Document all gaps in POA&M