CMMC(TM) Level 2 Compliance Readiness Guide

From Zero to C3PAO Evidence Submission

Product	ForteFide by DenseDefense
Version	1.4.2
Date	March 2026
Framework	NIST SP 800-171 Rev 2 (110 controls, 14 families)
Regulation	32 CFR Part 170 (CMMC 2.0 Final Rule)
Audience	OSAs, ISSMs, IT Directors, Compliance Officers

Table of Contents

PART 1

Customer Journey: Zero to Evidence

This section walks you through the complete ForteFide workflow from installation to delivering a signed evidence package to your C3PAO. The workflow follows a definitive 7-step process with two pre-workflow prerequisites (Install and License Activation). Each step includes the exact actions to take, what ForteFide does behind the scenes, and what artifacts are produced for your assessment.

> **Session Persistence**
> ForteFide maintains full session state in an AES-256-GCM encrypted SQLite database. You can close your browser, restart the service, or even reboot the machine -- pressing F5 restores your exact position in the workflow, including scan results, credential profiles, remediation progress, and attestation state. No work is ever lost.

Pre-Workflow: Install ForteFide

Windows Installation

Download ForteFide_Setup_1.4.2_Windows.exe from the DenseDefense download portal or your partner distribution package. Right-click the installer and select Run as Administrator. Follow the setup wizard -- default options are recommended. ForteFide installs to C:\Program Files\ForteFide\.

```
Silent install (GPO/SCCM):
ForteFide_Setup_1.4.2_Windows.exe /VERYSILENT /SUPPRESSMSGBOXES /NORESTART
```

Linux Installation (Ubuntu/Debian)

```
sudo dpkg -i ForteFide_Setup_1.4.2_linux.deb
sudo systemctl enable fortefide
sudo systemctl start fortefide
```

System Requirements

Requirement	Minimum	Recommended
OS	Windows 10 / Server 2016 / Ubuntu 20.04	Windows 11 / Server 2022 / Ubuntu 22.04
RAM	512 MB	2 GB
Disk	200 MB	500 MB (scan history)
Network	TCP 5000 (dashboard)	TCP 5000
Privileges	Administrator / root	Dedicated service account

Verify Installation

Open your browser to http://localhost:5000. The ForteFide Risk Operations Center (ROC) dashboard loads automatically. No login is required. Verify the version number in the top-left corner matches 1.4.2.

Pre-Workflow: Import License

ForteFide ships as a free scanner. To unlock remediation, evidence packaging, and scheduled scans, you need a license key. Three methods are available:

- **Drag and Drop:** Drag your .key file onto the license panel in the left sidebar. ForteFide auto-imports and reloads.
- **Dashboard Import:** Navigate to the License page, click Import License, and select your license.key file.
- **API Import:** POST /api/import-license with the key file for headless or automated deployments.
- **File Drop:** Place license.key in C:\ProgramData\ForteFide\ (Windows) or /etc/fortefide/ (Linux). Detected on next startup.

License Tiers

Feature	Free	Starter	Professional	Enterprise
Price (Monthly)	$0	$599/mo	$1,799/mo	$4,999/mo
Price (Annual)	$0	$499/mo	$1,499/mo	$4,166/mo
Scanning (110 controls)	Yes	Yes	Yes	Yes

Max Endpoints	Unlimited	25	100	Unlimited
Auto Remediation	No	Single-host	Batch	Batch
Evidence Package	No	Basic	Full (signed ZIP)	Full (signed ZIP)
Scheduled Scans	No	No	Yes	Yes
API Access	Read-only	Full	Full	Full
Priority Support	Community	Email	Email + Phone	Dedicated

License Validation
ForteFide uses Ed25519 cryptographic signatures for license validation. Licenses are machine-bound, tamper-proof, and verified entirely offline. No internet connection or phone-home is required.

Step 1: Network Recon

The workflow begins with CIDR-based network discovery. ForteFide's reconnaissance engine scans your network range and identifies every live endpoint, its OS type, and available management protocols. This step establishes the complete asset inventory that your C3PAO will require for the assessment.

How to Run Discovery

- Enter a CIDR range in the Discovery panel (e.g., 192.168.1.0/24)
- Click Discover -- ForteFide probes WinRM (5985) and SSH (22) to auto-detect OS type
- Results populate with IP, hostname, OS, and open ports
- Select which hosts are in-scope for your CUI boundary
- After discovery, the scan configuration panel auto-appears for the selected hosts
- API: POST /api/discover with {"targets": "192.168.1.0/24"}

Why Discovery Matters for CMMC

CMMC assessors require a complete asset inventory of all systems that process, store, or transmit CUI. Missing a single endpoint from your scope can result in a NOT MET finding for multiple controls. The discovery step produces the authoritative scope that flows through every subsequent step -- scan, remediation, and evidence collection.

C3PAO Scoping Tip
Only include endpoints within your CUI boundary. Systems that never touch CUI (guest WiFi, personal devices, non-CUI printers) should be excluded. Document your boundary decisions -- the C3PAO will ask exactly how you determined scope during the assessment.

Step 2: Prepare Endpoints

The Prepare step is where ForteFide configures your endpoints for authenticated scanning. This panel contains resource group management, service account creation, and authentication method selection -- all in a single unified flow. ForteFide automates what it can and guides you through what it cannot.

Resource Groups

Discovered hosts are organized into resource groups inside the Prepare panel. Resource groups let you apply shared credential profiles to sets of similar machines (e.g., all domain workstations, all Linux servers). Per-host credential overrides remain available for mixed environments.

- Create resource groups by OS type, role, or network segment
- Assign shared credential profiles at the group level
- Override individual host credentials where needed (common in mixed Windows/Linux environments)
- Groups persist across sessions for repeat scans

Authentication Method Dropdown

Each resource group or individual host has an auth method dropdown with three options:

Auth Method	How It Works	Best For
SSH Key (Default)	ForteFide auto-generates an Ed25519 keypair and deploys the public key to targets during preparation	Linux hosts, highest security, zero-password scanning
Certificate	Uses X.509 certificates for WinRM or SSH certificate-based auth	Enterprise PKI environments, domain-joined Windows

Password	Traditional username/password over WinRM (NTLM) or SSH	Quick setup, legacy systems, environments without key infrastructure

Automated Key Generation

When SSH Key auth is selected (the default), ForteFide automatically generates a unique Ed25519 keypair for the scan session. The public key is deployed to each target during preparation, and the private key never leaves the scanner host. After teardown (Step 7), the keys and service accounts are removed -- leaving no persistent credentials on the endpoints.

Service Account Creation

ForteFide creates a dedicated service account on each target during preparation. This account is used exclusively for scanning and remediation, then removed during teardown.

- **Windows:** Creates fortefide-svc with local admin rights. Enables WinRM if not already active. Opens TCP 5985 inbound.
- **Linux:** Creates fortefide-svc with sudo group membership. Deploys SSH key to authorized_keys. Configures passwordless sudo for the scan user.

```
# What ForteFide does automatically on Windows targets:
winrm quickconfig -q
net user fortefide-svc <generated> /add
net localgroup Administrators fortefide-svc /add

# What ForteFide does automatically on Linux targets:
sudo adduser --disabled-password fortefide-svc
sudo usermod -aG sudo fortefide-svc
# Deploys Ed25519 public key to ~fortefide-svc/.ssh/authorized_keys
```

> **C3PAO Assessment Note: Service Account Lifecycle**
> The automated service account creation and teardown addresses multiple CMMC controls: AC.L2-3.1.1 (authorized access), AC.L2-3.1.5 (least privilege), IA.L2-3.5.1 (identify system users), and IA.L2-3.5.2 (authenticate users). The full lifecycle is captured in the remediation log and evidence package for assessor review.

Step 3: Configure & Execute Scan

After endpoint preparation, ForteFide auto-detects all prepared hosts and presents the scan configuration panel. For endpoints prepared with SSH key or certificate auth, no additional credentials are needed -- scanning is truly zero-credential from the operator's perspective. The full scan assesses all 110 NIST SP 800-171 Rev 2 security requirements across 14 control families using actual system interrogation -- not questionnaires.

Zero-Credential Scanning

Endpoints prepared in Step 2 with key-based or certificate auth require no credential entry at scan time. ForteFide uses the deployed keys to authenticate automatically. This eliminates credential exposure in the UI, reduces operator error, and strengthens the audit trail for C3PAO review.

What Happens During a Scan

- ForteFide auto-detects prepared hosts and populates the target list
- ForteFide connects to each target via WinRM (Windows) or SSH (Linux)
- 110 check functions execute against the live system configuration
- Each check returns MET or NOT MET with a technical detail string
- Evidence is captured: the command executed, raw output, timestamp, and hostname
- Progress updates stream to the dashboard in real-time
- Typical scan time: 2-5 minutes per host depending on network speed

14 Control Families Assessed

Family	Name	Controls	Description
AC	Access Control	22	User access, least privilege, session controls
AT	Awareness & Training	3	Security training, role-based awareness
AU	Audit & Accountability	9	Audit logging, review, protection
CA	Security Assessment	4	Continuous monitoring, system connections
CM	Configuration Mgmt	9	Baselines, change control, least functionality

IA	Identification & Auth	11	Passwords, MFA, authenticator management
IR	Incident Response	3	Detection, reporting, response testing
MA	Maintenance	6	System maintenance, remote maintenance
MP	Media Protection	9	Media access, storage, transport, sanitization
PE	Physical Protection	6	Physical access, monitoring, visitor control
PS	Personnel Security	2	Screening, personnel actions
RA	Risk Assessment	3	Vulnerability scanning, risk management
SC	System & Comm Protection	16	Boundary protection, encryption, session auth
SI	System & Info Integrity	7	Flaw remediation, malware, monitoring, alerts

Scan Output

Each scan produces a complete result set containing: per-control determination (MET/NOT MET), technical evidence string, SPRS score calculation, per-host breakdown, and family-level compliance percentages. All results are stored in the AES-256-GCM encrypted SQLite database and persist across browser refreshes, service restarts, and system reboots.

Step 4: Baseline Evidence (Auto-Collected)

Immediately after a scan completes, ForteFide silently collects baseline evidence and generates a signed ZIP package. There is no button to click and no prompt to dismiss -- baseline evidence collection is automatic. A green checkmark appears in the workflow indicator confirming that baseline evidence has been captured.

What Gets Collected Automatically

- Per-control determination (MET/NOT MET) with technical evidence strings
- Per-host scan results with command output and timestamps
- SPRS score calculation and per-family compliance breakdown
- Asset inventory of all scanned endpoints
- Configuration baseline snapshot at time of scan
- SHA-256 hashes and Ed25519 cryptographic signature over the manifest

Chain of Custody

The signed evidence package includes a verification manifest with SHA-256 hashes for every document. The manifest itself is signed with the license key's Ed25519 signature, creating an unbroken chain of custody from scan execution to evidence delivery. Each artifact is timestamped and fingerprinted at the moment of collection. This proves to the C3PAO that no evidence has been tampered with between generation and review.

> **C3PAO Assessment Note: Evidence Integrity**
> The auto-collected baseline establishes the 'before remediation' snapshot. Assessors can compare this to the post-remediation evidence (Step 7) to verify exactly which controls improved and how. The cryptographic chain of custody ensures both snapshots are authentic and unmodified.

Step 5: Review, Attest & Override

This step is where you review scan findings, complete manual attestations for the 11 controls that require them, document control overrides and exceptions, and plan your remediation strategy. Take as long as needed -- there is no timer. Session state persists across browser refreshes.

Review Findings

- Total score: X/110 controls MET across all hosts with SPRS estimate
- Family breakdown: bar chart of compliance percentage per family
- Findings list: every NOT MET control with technical detail and severity
- Host filter dropdown: isolate findings for a specific IP address
- Severity indicators: High (5-point), Medium (3-point), Low (1-point)

Prioritization Strategy

Focus remediation in this order: (1) 5-point controls (highest SPRS impact), (2) 3-point controls, (3) 1-point controls that are NOT eligible for POA&M, (4) remaining 1-point controls. This maximizes your SPRS score improvement per remediation effort.

Critical: Non-POA&M-Eligible Controls

Six 1-point controls CANNOT be placed on a POA&M and must be fully implemented before your assessment: AC.L2-3.1.20 (External Connections), AC.L2-3.1.22 (Control Public Info), CA.L2-3.12.4 (SSP), PE.L2-3.10.3 (Escort Visitors), PE.L2-3.10.4 (Access Logs), PE.L2-3.10.5 (Physical Access). Additionally, ALL 3-point and 5-point controls must be MET -- they cannot appear on a POA&M.

Manual Attestations (11 Controls)

Eleven controls across three families require manual attestation. These represent organizational processes that cannot be verified by scanning a system configuration.

Family	Count	Controls	Evidence Needed
AT (Training)	3	AT.2.056, AT.2.057, AT.3.058	Training records, LMS exports, phishing simulation results
PE (Physical)	6	PE.1.131-PE.3.136	Badge logs, visitor escorts, access logs, camera footage, remote work policy
PS (Personnel)	2	PS.2.127, PS.2.128	Background check policy, termination checklists, access revocation records

For each attestation, check the box and acknowledge the confirmation: "By checking this control, I attest that this requirement has been implemented, is actively maintained, and can be evidenced upon request during a CMMC assessment." Attestation status syncs with the overall compliance score immediately.

Control Overrides & Documented Exceptions

Not every control applies to every environment in the same way. ForteFide supports documented control overrides for situations where an alternative implementation satisfies the requirement or where a control is genuinely not applicable.

- **Alternative Implementation:** The control is satisfied by a different mechanism than what ForteFide checks (e.g., third-party EDR instead of Windows Defender for SI.1.211-213).
- **Compensating Control:** A different control mitigates the same risk (e.g., network segmentation compensating for missing host-based firewall).
- **Not Applicable:** The control does not apply to this system (e.g., BitLocker on a virtual machine without removable media). Must be documented and justified.
- **Risk Acceptance:** Leadership formally accepts the risk. Documented in the POA&M with a timeline for future implementation.

Every override must include: (1) the control ID, (2) the reason, (3) the alternative or compensating measure, (4) the risk assessment, and (5) the authorizing official's signature and date. ForteFide captures these in the evidence package as part of the SSP.

Step 6: Remediate & Rescan

Remediation and rescanning happen in a single unified panel. ForteFide's bulletproof remediation engine can automatically fix 68+ controls across Windows and Linux. After remediation completes, rescan from the same panel to verify improvements. Plan for 2-4 remediate-rescan cycles -- each typically improves the score by 10-15 points.

Bulletproof Remediation Engine

The remediation engine is designed for air-gapped, unattended operation where no support access is available. Every aspect is hardened against failure:

- Smart ordering: safe controls (audit policies, passwords, USB) run first; connectivity-affecting controls (CM.3.067 AllowGroups, SC.1.175 firewall, sshd changes) run last
- Per-command SSH timeout (90s) -- hung commands are killed and skipped automatically
- Lockout detection: if 3 consecutive auth failures occur, auto-rollback the last connectivity-affecting change and resume
- CM.3.067 pre-check: verifies scan user is in sudo group before applying AllowGroups
- Pre-flight connectivity check before each host -- unreachable hosts skip immediately
- Every change logged with rollback point for instant undo

Remediation Categories

Category	Count	Examples
Registry/GPO	~20	Audit policies, password policies, USB restrictions
Service Config	~15	Enable Windows Defender, EventLog, WinRM hardening
Firewall	~8	Enable firewall with WinRM/RDP allow rules

File System	~10	NTFS permissions, share restrictions, encryption
SSH/PAM (Linux)	~10	sshd_config hardening, PAM complexity, sudo config

DANGER MODE

Some NOT MET controls cannot be auto-remediated because they require hardware changes, organizational processes, or physical actions. DANGER MODE provides a manual remediation interface for these controls, allowing operators to execute custom commands against endpoints directly from the Remediate & Rescan panel.

- Multi-Factor Authentication (IA.3.083, IA.3.084) -- requires MFA hardware/software
- BitLocker/LUKS encryption (AC.3.019, MP.2.119, MP.3.124, SC.3.190) -- requires TPM or manual setup
- Training controls (AT family) -- requires documented training program
- Physical controls (PE family) -- requires physical access controls, logs, escorts
- Personnel controls (PS family) -- requires screening and termination procedures

DANGER MODE Warning

DANGER MODE bypasses the safety checks that protect automation-safe remediation. Commands entered in DANGER MODE execute exactly as typed with full administrative privileges. Use only for controls that have no automated remediation path. All DANGER MODE actions are logged in the remediation record for C3PAO review.

Rescan in the Same Panel

After remediation (automated or manual), click Rescan without leaving the panel. The rescan produces a delta report comparing before/after scores. Each control shows its previous and current status. Newly MET controls are highlighted with the remediation that fixed them.

Safe Remediation Design

ForteFide is designed to never execute an automated remediation command that could lock you out. Firewall rules always create WinRM and RDP allow rules before enabling the firewall. SSH hardening preserves the scan user's access. Smart ordering ensures CM.3.067 (AllowGroups sudo) runs last. Every change is logged and reversible.

Target Score

Aim for 110/110 (SPRS = 110). While conditional certification is available at 88/110 (80%), a perfect score eliminates POA&M risk, simplifies your assessment, and demonstrates mature security posture. ForteFide customers typically reach readiness scores of 95-105/110 within 3 scan cycles.

Step 7: Final Evidence & Teardown

When you are satisfied with your compliance posture, this final step collects post-remediation evidence and cleans up all artifacts ForteFide created on your endpoints.

Post-Remediation Evidence Package

ForteFide generates a comprehensive signed evidence package suitable for C3PAO review. The package is a signed ZIP file containing 23 PDF documents covering every aspect of your CMMC Level 2 compliance.

- Dashboard: Click 'Collect Final Evidence' when your score is satisfactory
- API: POST /api/scan/<id>/signed-evidence-package (includes cryptographic manifest)
- The post-remediation ZIP is the definitive evidence package for your C3PAO
- Includes delta report comparing baseline (Step 4) to final state

Evidence Package Contents (23 Documents)

Doc ID	Document	Description
00	Verification Manifest	Document inventory, hashes, chain of custody
01	System Security Plan (SSP)	Complete SSP with per-control status and system description
02	Plan of Action & Milestones	POA&M for all NOT MET controls with remediation timelines
03	SPRS Scorecard	Official SPRS score calculation with per-control point values
04	Scan Report	Full scan results: per-host, per-control, per-family breakdown
05	Remediation Log	Timestamped record of all remediations (auto + DANGER MODE)
06	Asset Inventory	Complete inventory of all scanned endpoints with OS and role
07	Incident Response Plan	IRP template aligned to IR family requirements
08	Training Records	Attestation records for AT family controls

09	Control Evidence Summaries	Per-control evidence narratives for assessor review
10-19	Policy Documents (10)	AC, AT, AU, CA, CM, IA, IR, MA, MP, SC/SI policies
20	Delta Report	Before/after comparison showing remediation improvements
21	Configuration Baseline	Baseline system configurations at time of scan
22	Audit Log Extract	Audit log evidence supporting AU family controls

Teardown

After evidence collection, ForteFide's teardown process removes all artifacts created during preparation:

- Removes service accounts (fortefide-svc on Windows, fortefide-svc on Linux)
- Removes deployed SSH keys from authorized_keys
- Cleans up temporary files created during scanning and remediation
- The teardown is logged as part of the evidence record
- Endpoints are returned to their pre-ForteFide state

C3PAO Assessment Note: Clean Teardown

The teardown process demonstrates compliance with AC.L2-3.1.1 (authorized access control) and IA.L2-3.5.1 (identify system users) by showing that temporary scan credentials are properly revoked after use. The full lifecycle -- creation, use, and removal -- is captured in the evidence package.

Submitting to Your C3PAO

- Visit the Cyber AB Marketplace at https://cyberab.org/marketplace
- Filter for C3PAOs authorized for Level 2 assessments
- Request quotes from 2-3 C3PAOs (typical cost: $30,000-$120,000)
- C3PAO lead times are currently 3-6 months; book early

What to Send the C3PAO

- Complete ForteFide evidence ZIP (signed, from this step)
- Your System Security Plan (included in evidence package)
- Network diagrams showing CUI data flow and system boundaries
- Organizational chart with security roles identified
- Any additional policies not auto-generated by ForteFide

Pre-Assessment Readiness Checklist

Item	Status	Notes
SPRS score >= 88	Required	Minimum for conditional certification
All 5-point controls MET	Required	Cannot be on POA&M
All 3-point controls MET	Required	Cannot be on POA&M
6 critical 1-point controls MET	Required	AC.L2-3.1.20/22, CA.L2-3.12.4, PE.L2-3.10.3/4/5
SSP completed and signed	Required	Authorizing official must sign
POA&M current (if needed)	If applicable	Only for eligible 1-point controls
Asset inventory complete	Required	Every CUI-touching system listed
Network diagrams current	Required	Show CUI boundaries and data flow
Policy documents signed	Required	14 policy documents covering all families
Training records available	Required	Current fiscal year training evidence
Physical security evidence	Required	Access logs, camera footage, badge records
Incident Response Plan tested	Required	Annual IRP test documentation

PART 2

C3PAO Assessment Process: Expert Deep Dive

This section explains what happens after you submit your evidence package to a C3PAO. Understanding the assessment process helps you prepare effectively and avoid common pitfalls that delay certification.

8. Pre-Assessment Requirements

Selecting a C3PAO

C3PAOs are third-party assessment organizations authorized by the Cyber AB (formerly CMMC-AB) to conduct Level 2 assessments. As of 2026, there are approximately 50+ authorized C3PAOs, with capacity projected to reach 500+ by 2027. Each C3PAO must maintain ISO 17020 accreditation and employ Certified CMMC Assessors (CCAs).

Pre-Assessment Consultation

Before the formal assessment begins, the C3PAO conducts a pre-assessment consultation (sometimes called a gap assessment or readiness review). This is NOT the official assessment -- it is advisory only and does not affect your certification.

- The C3PAO reviews your SSP and POA&M for completeness
- Scope boundaries are defined: which systems, enclaves, and locations are in scope
- Assessment team composition is determined (typically 2-4 CCAs)
- Assessment schedule is agreed upon (typically 3-5 business days)
- Logistics are arranged: on-site dates, remote access, interview scheduling

System Security Plan (SSP) Requirements

The SSP is the single most important document in your assessment. Per NIST SP 800-171 requirement CA.L2-3.12.4, you MUST have an SSP. This is one of the six 1-point controls that cannot be placed on a POA&M. No SSP = automatic assessment failure.

- System description: purpose, architecture, data flow
- CUI boundary definition: what systems process/store/transmit CUI
- Security controls: status of all 110 requirements (MET, NOT MET, N/A)
- Roles and responsibilities: ISSO, ISSM, system administrators
- Interconnections: external systems, cloud services, subcontractors
- ForteFide auto-generates the SSP technical sections from scan data

Scope of Assessment

The assessment scope encompasses all information systems that process, store, or transmit CUI, plus any systems that provide security protection for those CUI systems. This includes:

- Servers, workstations, and laptops in the CUI enclave
- Network devices (firewalls, switches, routers) protecting CUI
- Cloud services used for CUI (e.g., GCC High, AWS GovCloud)
- Mobile devices if they access CUI
- Subcontractor systems if they process CUI (flow-down requirement)

> **Scope Minimization**
> Reducing your CUI boundary reduces assessment complexity and cost. Consider CUI enclaves: isolate CUI-processing systems in a dedicated VLAN or network segment. Fewer in-scope systems = fewer controls to demonstrate = faster, cheaper assessment.

9. Assessment Execution

Assessment Team

The C3PAO assessment team consists of a Lead Certified CMMC Assessor (Lead CCA) and one or more supporting CCAs. The Lead CCA has overall responsibility for the assessment methodology, findings, and final report. At least one team member must be on-site.

Three Assessment Methods

Per NIST SP 800-171A, assessors use three methods to evaluate each of the 320 assessment objectives across all 110 controls:

Method	Description	Examples
EXAMINE	Review documents, configurations, and artifacts	SSP review, firewall rule inspection, GPO screenshots, ForteFide scan reports
INTERVIEW	Discuss processes with personnel who implement or manage controls	System admin interviews, ISSO discussions, end-user awareness verification
TEST	Exercise controls under specified conditions to compare actual vs expected	Attempt unauthorized access, verify audit log generation, test account lockout

320 Assessment Objectives

Each of the 110 controls has multiple assessment objectives defined in NIST SP 800-171A. In total, there are 320 assessment objectives. A control is MET only when ALL of its assessment objectives are satisfied. For example, AC.L2-3.1.1 (Authorized Access Control) has multiple objectives covering account types, access enforcement, and privilege restrictions.

Evidence Types Accepted

Evidence Type	Description	ForteFide Provides
Technical Artifacts	System configurations, screenshots, log exports	Yes -- scan reports, remediation logs, config baselines
Documentation	Policies, procedures, plans, inventories	Yes -- SSP, POA&M, policies, asset inventory, IRP
Interview Notes	Verbal confirmation from personnel	No -- conducted live by assessor
Test Results	Output from assessor-executed tests	Partial -- scan results serve as technical tests

On-Site vs. Remote Assessment

CMMC Level 2 assessments require at least partial on-site presence. The Lead CCA determines the assessment approach based on the organization's environment:

- Physical security controls (PE family, 6 controls) typically require on-site verification
- Technical controls can often be assessed remotely via screen-sharing and artifact review
- Interviews may be conducted remotely for geographically distributed staff
- The 18 PE/PS assessment objectives generally require physical presence
- Hybrid assessments (2-3 days on-site, remainder remote) are common

Sampling for Multi-Site Organizations

For organizations with multiple physical locations processing CUI, assessors use a sampling methodology:

- Primary site: assessed in full (100% of controls)
- Additional sites: representative sampling based on risk and similarity
- If sites have materially different configurations, each requires full assessment
- The Lead CCA documents the sampling rationale in the assessment report
- Cloud-hosted environments are assessed as a separate enclave

Assessment Timeline (Typical)

Day	Activity	Your Role
Day 1	Opening meeting, scope confirmation, document review	Present SSP, network diagrams, key personnel introductions
Day 2-3	Technical assessment: examine artifacts, test controls	Provide access to systems, answer technical questions, produce evidence
Day 3-4	Interviews with key personnel (ISSO, admins, users)	Make staff available, ensure they understand their security responsibilities
Day 4-5	Physical security verification, remaining controls	Tour facilities, demonstrate physical access controls, camera systems
Day 5	Preliminary findings debrief, next steps discussion	Ask clarifying questions, understand any NOT MET findings

10. Assessment Results & Scoring

Control Determinations

Each of the 110 controls receives one of three determinations:

Determination	Meaning	Impact
MET	All assessment objectives for the control are satisfied	Full points retained in SPRS score
NOT MET	One or more assessment objectives are not satisfied	Points deducted from SPRS score (1, 3, or 5 points)
NOT APPLICABLE	The control does not apply to the assessed system	Not counted in scoring; requires documented justification

SPRS Score Calculation

The Supplier Performance Risk System (SPRS) score starts at 110 (perfect compliance) and deducts points for each NOT MET control. Point values are assigned based on security impact:

Point Value	Criteria	Count	Impact if NOT MET
5 points	Could lead to significant exploitation or CUI exfiltration	~22 controls	Severe: these CANNOT be on a POA&M
3 points	Specific and confined effect on network security	~41 controls	Major: these CANNOT be on a POA&M
1 point	Limited or indirect effect on security	~47 controls	Minor: most can be on a POA&M (except 6)

The SPRS score range is 110 (perfect) to -203 (worst possible). No partial credit is awarded -- a control is either fully MET or NOT MET. The only exceptions are controls 3.5.3 and 3.13.11, which have official partial credit provisions in the DoD Assessment Methodology.

Conditional Certification (POA&M) Rules

If you do not achieve a perfect 110, you may still obtain conditional certification under strict rules defined in 32 CFR Part 170:

Rule	Requirement
Minimum Score	SPRS score must be >= 88 (80% of 110)
POA&M Eligibility	Only 1-point controls may be on a POA&M (with 6 exceptions)
3-Point Controls	ALL must be MET -- cannot appear on POA&M
5-Point Controls	ALL must be MET -- cannot appear on POA&M
6 Critical 1-Pointers	AC.L2-3.1.20, AC.L2-3.1.22, CA.L2-3.12.4, PE.L2-3.10.3/4/5 -- must be MET
Maximum NOT MET	At most ~22 eligible 1-point controls (SPRS >= 88)
POA&M Closeout	All POA&M items must be remediated within 180 days
Closeout Assessment	C3PAO must verify POA&M closure (assesses only unmet requirements)
Failure to Close	Conditional certification revoked; full re-assessment required

Six 1-Point Controls NOT Eligible for POA&M

Control ID	NIST 800-171 Ref	Requirement
AC.L2-3.1.20	3.1.20	Verify and control connections to external information systems
AC.L2-3.1.22	3.1.22	Control information posted on publicly accessible information systems
CA.L2-3.12.4	3.12.4	Develop, document, and periodically update system security plans
PE.L2-3.10.3	3.10.3	Escort visitors and monitor visitor activity
PE.L2-3.10.4	3.10.4	Maintain audit logs of physical access
PE.L2-3.10.5	3.10.5	Control and manage physical access devices

POA&M Is Not a Free Pass

A Plan of Action & Milestones is a commitment to fix -- not permission to ignore. You have exactly 180 days from the assessment date to close every POA&M item. The C3PAO must verify closure in a follow-up assessment. If you fail to close, your conditional certification is revoked and you must undergo a complete new assessment.

11. Post-Assessment & Certification

Assessment Report Submission

After completing the assessment, the C3PAO submits its findings to the CMMC enterprise Mission Assurance Support Service (eMASS). The Cyber AB reviews the submission for procedural compliance (not re-assessing your controls). This process takes approximately 10-20 business days.

Certification Outcomes

Outcome	SPRS Score	What Happens Next
Final Level 2 (C3PAO)	110	Full certification issued. Valid for 3 years.
Conditional Level 2 (C3PAO)	>= 88	POA&M required. 180-day closeout window.
Assessment Failed	< 88	No certification. Must remediate and re-assess.

Annual Affirmation Requirements

CMMC certification is valid for 3 years, but annual affirmation is required. Each year after certification, a senior official must affirm in SPRS that the organization continues to meet all CMMC Level 2 requirements. This is a declaration -- not a new assessment.

- Year 1: Affirmation due within 12 months of assessment date
- Year 2: Second annual affirmation
- Year 3: Full re-assessment required before certification expires
- Affirmation must be submitted by a senior official with authority
- False affirmation carries False Claims Act liability

Re-Assessment Triggers

Beyond the 3-year cycle, certain events may trigger an earlier re-assessment:

- Significant security incident involving CUI
- Major system architecture changes (new enclave, cloud migration)
- Merger, acquisition, or significant organizational restructuring
- DIBCAC (Defense Contract Management Agency) surveillance finding
- Failure to submit annual affirmation on time
- Subcontractor compliance issues that affect your CUI handling

Appeals Process

If you disagree with a C3PAO's findings, the CMMC dispute resolution process provides recourse:

- Step 1: Discuss the finding directly with the Lead CCA during the debrief
- Step 2: Submit additional evidence to the C3PAO within the assessment window
- Step 3: File a formal appeal with the Cyber AB within 30 days of the final report
- Step 4: The Cyber AB reviews the appeal and may assign an independent review team
- The appeals process does not guarantee a different outcome

12. ForteFide Evidence Mapping

This section maps every ForteFide output to the specific C3PAO evidence requirements it satisfies. Understanding this mapping helps you identify what ForteFide covers automatically and what you need to supplement.

ForteFide Outputs vs. C3PAO Evidence Requirements

ForteFide Output	Assessment Method	Controls Covered	Sufficiency
Scan Report (Doc 04)	EXAMINE	All 110 technical controls	Primary evidence for technical controls
SSP (Doc 01)	EXAMINE	CA.L2-3.12.4 + all control narratives	Satisfies SSP requirement; may need org-specific additions
POA&M (Doc 02)	EXAMINE	CA.L2-3.12.2	Complete POA&M; needs authorizing official signature
SPRS Scorecard (Doc 03)	EXAMINE	Scoring validation	Matches DoD Assessment Methodology calculation
Remediation Log (Doc 05)	EXAMINE/TEST	All remediated controls	Proves remediation actions with timestamps
Asset Inventory (Doc 06)	EXAMINE	CM.L2-3.4.1, AC.L2-3.1.1	Lists all scanned endpoints; may need non-IT assets
IRP (Doc 07)	EXAMINE	IR.L2-3.6.1, IR.L2-3.6.2, IR.L2-3.6.3	Template; customize with org-specific contacts and procedures
Training Records (Doc 08)	EXAMINE	AT.L2-3.2.1, AT.L2-3.2.2, AT.L2-3.2.3	Attestation records; supplement with LMS exports
Policy Documents (Docs 10-19)	EXAMINE	All 14 families	Policy templates; need executive signature
Delta Report (Doc 20)	EXAMINE	Remediation verification	Shows score improvement over time

Config Baseline (Doc 21)	EXAMINE	CM.L2-3.4.1, CM.L2-3.4.2	Baseline at time of scan
Audit Log Extract (Doc 22)	EXAMINE	AU family (9 controls)	Proves audit logging is active and configured

What ForteFide Does NOT Provide

While ForteFide covers the majority of technical evidence requirements, some artifacts must come from your organization:

Missing Artifact	Required For	How to Obtain
Network Diagrams	SSP, CA family	Create using Visio, draw.io, or Lucidchart
Organizational Chart	PS family, SSP	HR department with security roles annotated
Physical Access Logs	PE.L2-3.10.3/4/5	Badge system exports, visitor sign-in sheets
Background Check Records	PS.L2-3.9.1, PS.L2-3.9.2	HR department (redacted per PII requirements)
MFA Configuration Evidence	IA.L2-3.5.3, IA.L2-3.5.4	Screenshots of MFA setup, enrollment records
Encryption Certificates	SC.L2-3.13.8,	Certificate authority exports, FIPS validation docs
Subcontractor Flow-Down	Multiple	Signed subcontractor compliance agreements
Business Continuity Plan	IR family supplements	Organizational BCP/DRP documents
Risk Assessment Report	RA.L2-3.11.1	Formal risk assessment per NIST 800-30
Continuous Monitoring Plan	CA.L2-3.12.3	Document describing ongoing monitoring activities

Evidence Completeness Rule

A single missing document will not fail your assessment, but assessors need sufficient evidence to determine a MET finding. ForteFide provides the technical evidence foundation. Your organizational policies and procedures complete the picture. Start preparing supplemental documents at least 90 days before your assessment.

PART 3

Evidence Package Contents

This section provides detailed descriptions of every document in the ForteFide evidence package. Each document is designed to satisfy specific C3PAO assessment objectives.

13. Complete Evidence Package Reference

Document 00: Verification Manifest

The manifest is the master index of the evidence package. It contains SHA-256 hashes of every document, generation timestamps, the scan ID that produced the evidence, and the overall SPRS score at time of generation. The signed variant includes a cryptographic signature over the manifest, creating an unbroken chain of custody.

- Purpose: Package integrity verification and document inventory
- C3PAO use: Verify no artifacts have been modified post-generation
- Includes: Document count, per-doc SHA-256 hash, generation timestamp

Document 01: System Security Plan (SSP)

The SSP is the cornerstone document of any CMMC assessment. ForteFide generates a technical SSP that includes system description, asset inventory, per-control status (MET/NOT MET), and family-level compliance summaries. The SSP maps directly to NIST SP 800-171 requirement CA.L2-3.12.4.

- System description: Purpose, architecture, boundaries
- CUI scope: What data is CUI, where it lives, how it flows
- Per-control status: All 110 controls with determination and evidence
- Family summary: Compliance percentage per family with pass/fail counts
- Host inventory: IP, hostname, OS, role, per-host score
- Action required: Add organizational context (mission, org chart, data flow diagrams)

Document 02: Plan of Action & Milestones (POA&M)

The POA&M lists every NOT MET control with a planned remediation timeline. ForteFide auto-generates the POA&M from scan results, including the control ID, description, current status, planned remediation action, responsible party, and target completion date.

- Only 1-point controls (except the 6 critical ones) may appear on a POA&M
- Each entry includes: control ID, deficiency, milestone, resources, completion date
- POA&M closeout must occur within 180 days of assessment
- C3PAO conducts a closeout assessment to verify POA&M items are resolved
- Action required: Assign responsible parties and realistic completion dates

Document 03: SPRS Scorecard

The SPRS scorecard shows the official score calculation: starting from 110, each NOT MET control deducts 1, 3, or 5 points based on the DoD Assessment Methodology. The scorecard lists every control, its point value, determination, and running total.

- Score range: 110 (perfect) to -203 (worst possible)
- Minimum for conditional certification: 88
- Each control shows: ID, point value (1/3/5), MET/NOT MET, deduction
- Summary shows: total score, controls MET, controls NOT MET, POA&M eligibility
- Action required: Submit score to SPRS (https://www.sprs.csd.disa.mil/)

Document 04: Scan Report

The full scan report contains per-host, per-control results with technical evidence strings. This is the primary technical artifact for the assessment. Each control entry shows the check that was performed, the raw output, and the determination.

- Per-host breakdown: Each target IP with its individual score
- Per-control detail: Command executed, output received, determination logic
- Family heatmap: Visual compliance percentage per family

- Evidence capture: Command, raw output, timestamp, hostname per check
- Supports the EXAMINE assessment method for all technical controls

Document 05: Remediation Log

A timestamped, immutable record of every automated remediation action ForteFide performed. Each entry includes the control ID, the command executed, the target host, the timestamp, the result (success/failure), and the pre-remediation state.

- Proves when and how each deficiency was addressed
- Supports delta analysis (before/after remediation)
- Includes rollback information for each action
- Demonstrates due diligence in remediation efforts

Document 06: Asset Inventory

A complete inventory of all endpoints scanned by ForteFide, including IP address, hostname, operating system, open ports, system role, and compliance score. This satisfies the CM.L2-3.4.1 (system component inventory) requirement.

Document 07: Incident Response Plan (IRP)

A template IRP aligned to the IR family requirements (IR.L2-3.6.1, IR.L2-3.6.2, IR.L2-3.6.3). The template covers incident categories, severity levels, escalation procedures, communication plans, evidence preservation, and post-incident review. Customize with your organization's specific contacts and procedures.

Document 08: Training Records

Attestation records for the AT family controls. When a user attests to training completion in the ForteFide dashboard, this document records the attestation date, the attesting official, and the specific controls attested (AT.2.056, AT.2.057, AT.3.058). Supplement with LMS exports and completion certificates.

Documents 09: Control Evidence Summaries

Narrative evidence summaries for each of the 110 controls. Each summary explains how the control is implemented, what evidence supports the MET determination, and any relevant configuration details. These narratives directly support the EXAMINE assessment method.

14. Policy Documents

ForteFide generates 14 policy document templates aligned to the 14 CMMC Level 2 control families. Each policy covers the organizational requirements that complement the technical controls verified by scanning.

Doc #	Policy	Families Covered	Key Contents
10	Access Control Policy	AC	Account management, least privilege, remote access, session controls
11	Awareness & Training Policy	AT	Training requirements, frequency, role-based training, social engineering
12	Audit & Accountability Policy	AU	Audit events, log retention, log protection, review frequency
13	Security Assessment Policy	CA	Continuous monitoring, system connections, POA&M management
14	Configuration Management Policy	CM	Baselines, change control, least functionality, software restrictions
15	Identification & Authentication	IA	Password policy, MFA requirements, authenticator management
16	Incident Response Policy	IR	Incident categories, response procedures, reporting, testing
17	Maintenance Policy	MA	Maintenance authorization, remote maintenance, maintenance records
18	Media Protection Policy	MP	Media access, storage, transport, sanitization, CUI marking
19	SC/SI Combined Policy	SC, SI	Boundary protection, encryption, flaw remediation, malware, monitoring

Policy Customization

ForteFide-generated policies are professional templates that require organizational customization before your assessment. At minimum, you must:

- Replace placeholder organization name with your company name
- Add your organization's specific procedures and contacts
- Have each policy signed by the appropriate executive (CISO, CTO, etc.)
- Set review dates (policies must be reviewed at least annually)
- Distribute policies to all personnel and document acknowledgment

15. Verification & Chain of Custody

Cryptographic Verification

The signed evidence package uses SHA-256 hashing and Ed25519 digital signatures to ensure integrity. Every document in the package has its hash recorded in the verification manifest. The manifest itself is signed, preventing any modification to the package after generation.

Chain of Custody

The chain of custody documents the lifecycle of the evidence package from generation to C3PAO delivery:

- Generation: ForteFide creates the package, records scan ID, timestamp, and hashes
- Storage: Package stored in AES-256-GCM encrypted local database
- Transfer: Deliver to C3PAO via encrypted email, secure file transfer, or physical media
- Verification: C3PAO verifies manifest hashes match delivered documents
- Retention: Both you and the C3PAO retain copies for the certification period (3 years)

Evidence Integrity Verification Command

```
# Verify evidence package integrity:
python -c "
import hashlib, json, zipfile, sys
with zipfile.ZipFile(sys.argv[1]) as z:
    manifest = json.loads(z.read('manifest.json'))
    for doc in manifest['documents']:
        h = hashlib.sha256(z.read(doc['filename'])).hexdigest()
        status = 'OK' if h == doc['sha256'] else 'MISMATCH'
        print(f'{status}: {doc["filename"]}')
" ForteFide_Signed_Evidence_123.zip
```

APPENDICES

Appendix A: SPRS Score Calculation Reference

The SPRS (Supplier Performance Risk System) score is the official metric used by the DoD to evaluate your cybersecurity posture. The scoring methodology is defined in the DoD Assessment Methodology and implemented by ForteFide's SPRS Scorecard (Document 03).

Scoring Formula

```
SPRS Score = 110 - SUM(point deductions for NOT MET controls)

Point values per control:
  5 points: Significant exploitation risk (e.g., no encryption, no access control)
  3 points: Confined security effect (e.g., weak passwords, missing audit)
  1 point:  Limited/indirect effect (e.g., policy gaps, training)

Examples:
  110/110 MET = SPRS 110 (perfect)
  105/110 MET (5 x 1-point failures) = SPRS 105
  100/110 MET (2 x 5-point failures) = SPRS 100
  All NOT MET = SPRS -203
```

Score Thresholds

SPRS Score	Meaning	Assessment Result
110	Perfect compliance -- all 110 controls MET	Final Level 2 (C3PAO)
88 - 109	Minor gaps in 1-point controls only	Conditional Level 2 (POA&M required)
0 - 87	Significant gaps -- POA&M not available	Assessment failed
Negative	Critical gaps in high-value controls	Assessment failed -- major remediation needed

Partial Credit (Two Controls Only)

The DoD Assessment Methodology provides official partial credit for exactly two controls:

- **3.5.3 (IA.L2-3.5.3):** MFA -- if MFA is implemented for remote access but not for privileged access (or vice versa), a 3-point deduction applies instead of 5.
- **3.13.11 (SC.L2-3.13.11):** CUI Encryption -- if encryption is implemented but not FIPS-validated, a 3-point deduction applies instead of 5.

Appendix B: POA&M Eligibility by Control

This reference shows which controls may appear on a Plan of Action & Milestones for conditional certification. Only 1-point controls (minus the 6 critical exclusions) are eligible. All 3-point and 5-point controls must be fully MET.

Category	Count	POA&M Eligible	Notes
5-point controls	~22	NO	Must be MET. No exceptions.
3-point controls	~41	NO	Must be MET. No exceptions.
1-point controls (eligible)	~41	YES	Can be on POA&M. 180-day closeout.
1-point controls (excluded)	6	NO	AC.L2-3.1.20/22, CA.L2-3.12.4, PE.L2-3.10.3/4/5
Total	110	~41 eligible	Maximum ~22 can be NOT MET (SPRS >= 88)

POA&M Strategy

Even though up to ~22 controls can theoretically be on a POA&M, best practice is to have zero. Every POA&M item: (1) requires a closeout assessment (additional C3PAO cost), (2) creates a 180-day countdown clock, (3) carries the risk of conditional certification revocation if not closed. Use ForteFide's automated remediation to eliminate as many findings as possible before the assessment.

Appendix C: CMMC Enforcement Timeline

The CMMC 2.0 enforcement rollout follows a phased approach defined in 32 CFR Part 170 (effective December 16, 2024) and the DFARS acquisition clause 252.204-7021.

Phase	Date	What Happens	Who Is Affected
Phase 1	Dec 16, 2024	Self-assessment for Level 1 and some Level 2 contracts. CMMC clauses appear in new solicitations.	All DIB contractors handling FCI (L1) or CUI (L2 self-assessment)
Phase 2	Nov 10, 2026	C3PAO assessments required for Level 2 contracts. Mandatory third-party certification.	All contractors handling CUI on new contracts after this date
Phase 3	Est. late 2027	Full Level 2 and Level 3 enforcement. All applicable contracts require certification.	All DIB contractors at Levels 2 and 3
Phase 4	Est. 2028	Full implementation across all DoD contracts. No new contracts without CMMC.	Entire Defense Industrial Base (~220,000 organizations)

Act Now

Phase 2 begins November 10, 2026. C3PAO lead times are currently 3-6 months, and achieving compliance readiness takes 6-18 months. Organizations that have not started their CMMC journey are at serious risk of missing contract deadlines. Start with ForteFide today to establish your baseline and begin remediation.

Capacity Projections

DoD projections from the 32 CFR rule show C3PAO assessment capacity growing significantly but lagging demand:

Year	Projected C3PAOs	Assessment Capacity	Estimated Demand
Year 1 (2025)	~50	~500 assessments	High (early adopters)
Year 2 (2026)	~250	~2,500 assessments	Very high (Phase 2 deadline)
Year 3 (2027)	~500+	~8,500 assessments	Peak demand

Appendix D: 14 Control Family Reference

Complete reference of all 14 NIST SP 800-171 control families with control counts, point value ranges, and automation coverage in ForteFide.

Family	Name	Ctrls	Points	Auto	Coverage
AC	Access Control	22	1-5	~18	User access, least privilege, remote access, session lock, mobile device, external connections
AT	Awareness & Training	3	1	0 (manual)	Security awareness, role-based training, social engineering awareness
AU	Audit & Accountability	9	1-5	~7	Audit events, content, capacity, review, reduction, generation, protection, correlation
CA	Security Assessment	4	1-3	~3	Security assessments, POA&M, continuous monitoring, system connections
CM	Configuration Mgmt	9	1-5	~7	Baselines, change control, security settings, least functionality, software restrictions
IA	Identification & Auth	11	1-5	~6	User identification, MFA, authenticator management, password complexity, replay resistance
IR	Incident Response	3	1-3	~2	Incident handling, reporting, response testing
MA	Maintenance	6	1-3	~4	System maintenance, remote maintenance tools, maintenance personnel
MP	Media Protection	9	1-5	~5	Media access, CUI marking, storage, transport, sanitization, accountability
PE	Physical & Environ	6	1	0 (manual)	Physical access, escorts, access logs, access devices, facility monitoring, alt
PS	Personnel Security	2	1	0 (manual)	Personnel screening, personnel actions (termination/transfer)
RA	Risk Assessment	3	1-5	~3	Risk assessment, vulnerability scanning, vulnerability remediation
SC	System & Comm Prot	16	1-5	~11	Boundary protection, architectural design, encryption, session auth, CUI at rest/transit
SI	System & Info Integrity	7	1-5	~5	Flaw remediation, malware protection, security alerts, system monitoring, advanced threats

Total Coverage Summary

Metric	Value
Total Controls	110
Assessment Objectives (NIST 800-171A)	320
Control Families	14
ForteFide Auto-Remediable (Windows)	~68
ForteFide Auto-Remediable (Linux)	~42
Manual/Attestation Controls	11 (AT: 3, PE: 6, PS: 2)
Hardware-Dependent Controls	~7 (MFA: 3, Encryption: 4)
SPRS Score Range	110 to -203
Minimum for Conditional Cert	88 (80%)
POA&M Closeout Window	180 days
Certification Validity	3 years (annual affirmation)

About This Guide

This guide was prepared by DenseDefense as a comprehensive reference for organizations pursuing CMMC Level 2 certification using ForteFide. While every effort has been made to ensure accuracy, the CMMC program is actively evolving. Always consult the authoritative sources:

- 32 CFR Part 170 (CMMC Final Rule): https://www.ecfr.gov/current/title-32/part-170
- NIST SP 800-171 Rev 2: https://csrc.nist.gov/publications/detail/sp/800-171/rev-2/final
- NIST SP 800-171A: https://csrc.nist.gov/publications/detail/sp/800-171a/final
- DoD CIO CMMC Page: https://dodcio.defense.gov/CMMC/
- Cyber AB Marketplace: https://cyberab.org/marketplace
- SPRS Portal: https://www.sprs.csd.disa.mil/

DenseDefense | ForteFide v1.4.2 | CMMC Level 2 Compliance Platform

densedefense.com | Confidential | March 2026