ForteFide Quick Start & Evaluation Guide

From Zero to Evidence Collection in 7 Steps

Product	ForteFide CMMC L2 Scanner & Remediation Platform
Version	1.4.2
Framework	NIST SP 800-171 Rev 2 / CMMC Level 2
Controls	110 across 14 families
Platforms	Windows (.exe) & Linux (.deb)
Publisher	DenseDefense -- DFW, Texas
Website	densedefense.com

Installation

ForteFide installs in under a minute and requires no external dependencies. Choose the package that matches your scanner host operating system.

Windows (.exe)

- Download ForteFide_Setup_1.4.2_Windows.exe from your DenseDefense representative or densedefense.com
- Right-click the installer and select Run as Administrator
- Follow the setup wizard -- default install path: C:\Program Files\ForteFide\
- Select the dashboard port during installation (default: 5000)
- ForteFide starts automatically and opens http://localhost:5000 in your default browser

Linux (.deb)

```
sudo dpkg -i ForteFide_Setup_1.4.2_linux.deb
```

- Native ELF binary (Nuitka-compiled) -- no Python runtime or pip packages required
- Only dependency: libc6 >= 2.28 (standard on Debian 11+ / Ubuntu 22.04+)
- Service starts automatically on install and opens your default browser
- Dashboard available at http://localhost:5000

> **Air-Gap Ready**
> Both the Windows .exe and Linux .deb are fully self-contained. No internet connectivity is required for installation, scanning, remediation, or evidence collection. The entire product operates offline.

License Activation

ForteFide supports three methods to activate your license. Without a license, ForteFide operates in Free tier mode -- scanning all 110 controls with no time limit, but automated remediation, evidence collection, and scheduling are disabled.

Option A: Drag & Drop

- Drag and drop your .key license file directly onto the license panel in the lower-left sidebar

Option B: Manage License

- Click "Manage License" in the sidebar and use the file import dialog to select your .key file

Option C: API Import

```
curl -X POST http://localhost:5000/api/import-license \
  -H "Content-Type: application/json" \
  -d '{"content": "<base64-encoded .key content>"}'
```

When a valid license is active, the sidebar shows PRO LICENSED with the number of days remaining. License verification uses Ed25519 digital signatures and is fully offline -- no phone-home or network calls.

Machine-Bound Licensing

- Run fortefide --request-code on the target machine to generate a hardware-bound request code
- Send the request code to DenseDefense (email, USB, or any offline channel)
- Receive a license.key cryptographically tied to that machine's fingerprint
- The raw hardware identifiers never leave the machine -- only a SHA-256 hash is transmitted

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
Priority Support	Community	Email	Email + Phone	Dedicated

Trial License
A 10-day trial license provides Professional-equivalent features so you can evaluate remediation and evidence collection before purchasing. Trial is a license type, not a pricing tier.

Step 1: Network Recon

Network discovery is the first step in the ForteFide workflow. It identifies all live hosts on your subnet so you can select which endpoints to include in the compliance scan. No credentials are required for discovery.

How to Run Discovery

- Enter your network CIDR (e.g., 192.168.1.0/24) in the Discovery panel
- Click "Start Discovery" -- ForteFide probes all addresses for live hosts
- Discovery typically completes in 2-5 minutes for a /24 network (254 addresses)

What Discovery Detects

- IP address of each live host
- Hostname (via reverse DNS lookup)
- Open ports (TCP probe across common service ports)
- Operating system type (Windows vs. Linux, based on port signatures)
- Running services inferred from open ports

Selecting Targets

- Review the discovered hosts table -- filter by OS type if needed
- Select hosts to include in the scan using checkboxes
- Deselect hosts that should NOT be scanned: network devices, ESXi hosts, printers, IoT devices, etc.
- Click "Scan Selected" to populate the scan targets -- discovery flows directly into scan configuration

Tip: OS Detection
Discovery uses TCP port probing on ports 22, 135, 445, 3389, and 5985. Hosts with ports 135/445/5985 open are classified as Windows; hosts with port 22 open are classified as Linux. ICMP and reverse DNS supplement the detection.

Step 2: Prepare Endpoints

After discovery, ForteFide shows the Prepare Endpoints panel. This step creates a dedicated fortefide-svc service account on each target to ensure safe scanning and remediation without using shared admin credentials.

Resource Groups

- Targets are organized into resource groups -- each group can have its own credentials
- Per-group credentials allow mixed environments: domain admin for Windows, root for Linux, etc.
- Groups are defined automatically based on OS detection or can be customized manually

Authentication Method Dropdown

For each resource group, select the authentication method from the dropdown:

Method	Use Case	Notes
Password	Standard username/password	DOMAIN\User for Windows, root or admin for Linux
SSH Key	Key-based authentication	Auto-generates Ed25519 keypair if none exists
Certificate	Certificate-based auth	For environments using PKI/certificate auth

Walkthrough A: Password Auth (Simplest)

- Select "Password" from the Auth Method dropdown
- Enter admin credentials: DOMAIN\Administrator for Windows, root or admin for Linux
- Click "PREPARE SELECTED ENDPOINTS"
- ForteFide creates the fortefide-svc account with a strong random password on each target
- In Step 3, enter the same admin credentials -- or let ForteFide use the stored service account

Walkthrough B: SSH Key Auth (Recommended)

- Select "SSH Key" from the Auth Method dropdown
- Enter admin credentials (needed once to deploy the key)
- Click "PREPARE SELECTED ENDPOINTS" -- ForteFide auto-generates an Ed25519 keypair
- The public key is deployed to each Linux target's ~/.ssh/authorized_keys for fortefide-svc
- The private key stays on the scanner host in the keys/ directory and never leaves the machine
- In Step 3, no credentials are needed -- the banner shows "All endpoints using key-based auth"
- Scan, remediation, and rescan all use the deployed key automatically

Walkthrough C: Certificate Auth (Zero Trust)

- Select "Certificate" from the Auth Method dropdown
- Enter admin credentials (needed once to deploy the certificate)
- Click "PREPARE SELECTED ENDPOINTS" -- ForteFide generates a client certificate
- Linux targets: certificate is added to authorized principals for fortefide-svc
- Windows targets: WinRM HTTPS is configured with the client certificate
- In Step 3, no credentials are needed -- certificate auth is used automatically
- Ideal for environments that require PKI-based authentication or certificate-only policies

> **Recommendation: Use SSH Key or Certificate Auth**
> Key and certificate auth eliminate passwords from the scan and remediation workflow. Admin credentials are entered once during preparation and never again. The deployed keys are rotatable, auditable, and do not expose passwords in memory. Password auth is provided for environments where key deployment is not possible.

Deploy to Targets

- Click "PREPARE SELECTED ENDPOINTS" to deploy service accounts to all selected targets
- ForteFide connects to each target using the provided admin credentials
- A dedicated fortefide-svc account is created with a strong random password

What Gets Created

Component	Linux	Windows
Service account	fortefide-svc local user	fortefide-svc local user
Password	Strong random, never expires	Strong random, never expires
Privileges	sudo group + /etc/sudoers.d/ entry	Administrators + Remote Mgmt Users
Access restriction	SSH only (key or password)	WinRM only (deny interactive + deny RDP)
SSH key (optional)	~/.ssh/authorized_keys	N/A

Warning: CM.3.067 Lockout Risk
Do NOT skip endpoint preparation. CM.3.067 remediation enforces AllowGroups sudo in sshd_config. If your scanning account is not in the sudo group, SSH access will be permanently severed. The fortefide-svc account is always in the sudo group, preventing this lockout scenario.

Step 3: Configure & Execute Scan

After endpoint preparation, ForteFide transitions to the scan configuration panel. It auto-detects which endpoints have been prepared and adjusts its behavior accordingly.

Auto-Detection of Prepared Endpoints

- Prepared endpoints display a "Using service accounts" banner in the scan configuration
- ForteFide automatically uses the fortefide-svc credentials for prepared hosts
- No manual credential entry is needed for prepared endpoints

Manual Credential Override

- For hosts that were NOT prepared (or where you want to use different credentials), enter credentials manually in the inline scan configuration
- Per-host credential overrides: use the dropdown to assign different credentials to specific hosts
- Supports dual credential profiles: separate Windows and Linux credential sets

Scan Execution

- ForteFide scans each host against all 110 NIST 800-171 / CMMC Level 2 controls
- Auto OS detection: ForteFide detects the target OS and selects the appropriate check set
- Credential profiles: Windows hosts use WinRM (port 5985), Linux hosts use SSH (port 22)
- Progress is shown per-host, per-control in the Activity Log

Platform	Transport	Approx. Time	Controls
Windows	WinRM (TCP 5985)	~30s per host	110
Linux	SSH (TCP 22)	~15s per host	110

Tip: Mixed-OS Environments
ForteFide handles mixed Windows/Linux environments in a single scan. Auto OS detection eliminates the need to run separate scans for each platform. Credential profiles are matched to each host's detected OS automatically.

Step 4: Baseline Evidence

Immediately after the first scan completes, ForteFide automatically collects baseline evidence to capture the pre-remediation state of your environment. This is critical for demonstrating improvement to your C3PAO assessor.

Automatic Collection

- Baseline evidence is auto-collected after the scan -- no manual trigger required
- Evidence is packaged as a cryptographically signed ZIP with full chain of custody

Chain of Custody

- Every file is hashed with SHA-256
- Machine fingerprint is embedded in the manifest (ties evidence to the scanning host)
- The verification manifest is signed with Ed25519 digital signatures
- Timestamps are recorded for every artifact

Verification Manifest

- A standalone verify_evidence.py script is included in every evidence package
- The verifier requires only Python 3 -- no ForteFide installation needed
- Assessors can independently confirm that no documents have been tampered with

Evidence Package Contents

Document	Description
Scan Report PDF	Complete scan results with per-control detail
System Security Plan (SSP)	Comprehensive security plan mapped to 110 controls

POA&M	Plan of Action & Milestones for unmet controls
SPRS Scorecard	Supplier Performance Risk System score calculation
Asset Inventory	All scanned endpoints with OS, IP, hostname, services
Remediation Log	Timestamped record of every remediation action
Control Evidence Summaries	Per-control evidence with command output and timestamps
Incident Response Plan	Template IRP aligned to NIST 800-171 IR family
Training Records Template	Blank template for documenting security training
14 Policy Documents	One policy per applicable CMMC family
Verification Manifest	SHA-256 hashes + Ed25519 digital signature
verify_evidence.py	Standalone verification script for assessors

Why Baseline Evidence Matters
The baseline package establishes your starting point. When paired with the final (post-remediation) package, the delta between the two scans shows your C3PAO exactly what improved and by how much.

Step 5: Review, Attest & Override

After the baseline evidence is captured, review your scan results, complete manual attestations, and document any overrides before proceeding to automated remediation. Take as long as needed at this step.

Findings Review

Review your scan results across multiple views:

- Score Cards: overall compliance percentage, passed/failed counts, severity breakdown
- Overview tab: executive summary with family-level scores and risk distribution
- Family Breakdown: per-family compliance across all 14 CMMC families
- Findings tab: every failed control with severity, description, remediation guidance, and impact
- Delta tab: before/after comparison showing which controls changed status
- Host Filter: filter findings by specific host IP to focus on one endpoint at a time

Manual Attestations (11 Controls)

11 controls require manual attestation because they cover organizational processes that cannot be verified through technical scanning.

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

- Open the Attestations tab in the results view
- Check each control that your organization has implemented
- A confirmation modal appears: "By checking this control, I attest that this requirement has been implemented..."
- Attestations are recorded with timestamp and included in the evidence package

Control Overrides

For controls that cannot be met through automation or attestation, ForteFide supports documented overrides aligned with the CMMC assessment process.

- Open any finding detail view and click "OVERRIDE"
- Select the override type:
- **Documented Exception** -- the control requirement does not apply to this environment
- **Alternative Implementation** -- the requirement is met through a different mechanism
- Enter a justification (minimum 20 characters)
- Optionally reference supporting evidence or documentation
- All overrides are tracked with full audit trail and included in the evidence package

Step 6: Remediate & Rescan

With a Starter, Professional, or Enterprise license active, ForteFide can automatically remediate failing controls. This is where the platform delivers its greatest value -- turning a failing score into a passing one in minutes.

Batch Remediation

- Click "REMEDIATE ALL AUTO CONTROLS" in the Step 6 panel
- ForteFide executes safe auto-remediable controls across all hosts
- Smart ordering: safe controls first, connectivity-affecting controls last
- Progress is shown per-host, per-control in the Activity Log

DANGER MODE

For controls that require manual intervention or carry higher risk, ForteFide provides DANGER MODE -- a separate remediation path with additional safeguards.

- DANGER MODE handles controls marked as MANUAL INTERVENTION (unsafe for auto-remediation)
- A confirmation overlay requires explicit acknowledgment before execution
- Every DANGER MODE action includes automatic rollback capability
- Rollback restores the previous configuration if the remediation causes connectivity loss

Bulletproof Remediation Engine

ForteFide's remediation engine includes multiple safety layers to prevent lockouts and service disruption:

Safety Feature	Description
Smart Ordering	Safe controls execute first; connectivity-affecting controls run last
Preflight Check	Connectivity verification before each host remediation begins
90-Second Timeout	Per-control timeout prevents hangs on unresponsive endpoints
Lockout Detection	3 consecutive auth failures trigger automatic rollback
Auto-Rollback	Reverts changes if post-remediation connectivity check fails
Post-Verification	Connectivity re-verified after firewall and sshd changes
CM.3.067 Last	AllowGroups sudo always executes absolutely last to prevent lockout

Rescan to Verify

- After remediation completes, click "RESCAN NOW" in the same panel
- ForteFide re-evaluates all 110 controls against the remediated state
- The Delta tab compares before/after scores to quantify improvement
- Any remaining failures can be addressed with additional remediation or overrides

Safety First
ForteFide never remediates Critical/High controls without explicit selection. Connectivity-affecting controls (firewall rules, sshd config, AllowGroups) include post-change verification to ensure the endpoint remains reachable. CM.3.067 runs last in every batch to prevent SSH lockout.

Step 7: Final Evidence & Teardown

Collect Final Evidence Package

- Click "COLLECT & SIGN EVIDENCE" in the sidebar after the rescan confirms improved posture
- This generates the post-remediation evidence package with the same chain of custody as baseline
- Both baseline (Step 4) and final (Step 7) ZIPs are submitted to your C3PAO
- The delta between scans shows the assessor exactly what improved and by how much

Evidence Integrity

- Every file: SHA-256 hash
- Manifest: Ed25519 digital signature
- Machine fingerprint embedded for provenance
- Standalone verify_evidence.py included -- requires only Python 3

Teardown: Remove All Artifacts

After evidence collection is complete, tear down the service accounts. This ensures zero ForteFide artifacts remain on target systems.

- Navigate to the Teardown panel and click "TEARDOWN SELECTED ENDPOINTS"

Component	Linux Teardown	Windows Teardown
Service account	Deletes fortefide-svc user	Deletes fortefide-svc local user
Sudo/admin access	Removes /etc/sudoers.d/ entry	Removes WinRM access config
Group membership	Removes from sudo group	Removes deny-logon policies
SSH keys	Cleans authorized_keys entries	N/A

Verify Clean Teardown

- Use the standalone verification script to confirm all artifacts have been removed
- The script checks for residual accounts, sudoers entries, and SSH keys on each target

Important: Always Teardown After Assessment

The fortefide-svc account has elevated privileges by design. Leaving it in place after an assessment is a security risk. Teardown removes the account, sudoers configuration, and all access grants -- leaving zero artifacts on target systems.

Session Persistence (F5 Safe)

ForteFide v1.4.2 persists all scan results in an encrypted SQLite database. You can refresh the browser (F5), close and reopen, or restart the service without losing any data.

- Auto-save: every completed scan is persisted immediately upon completion
- Auto-restore: on startup, all previously saved scans are loaded into the dashboard
- Encryption: AES-256-GCM with HKDF-SHA256 key derived from machine hardware fingerprint
- Device-bound: copying scans.db to another machine renders it unreadable
- Crash recovery: partial scans are not persisted; only completed scans are saved

Platform	Database Path
Windows	C:\ProgramData\ForteFide\scans.db
Linux	/var/lib/fortefide/scans.db

HallMonitor Security Advisor

HallMonitor is ForteFide's built-in security advisor. It provides proactive threat analysis and scheduled scanning to maintain continuous compliance posture.

- Scheduled threat scanning: configure automated scans on daily, weekly, biweekly, or monthly cadences
- Continuous monitoring: HallMonitor tracks compliance drift between scheduled scans
- Alert notifications: dashboard alerts when compliance score drops below threshold
- Definition updates: automatically pulls latest scanner definitions before each scheduled scan (connected environments)
- Air-gap support: displays staleness reminder when definitions are older than 7 days
- Audit trail: every scheduled scan event is logged with timestamps, trigger source, and results

CMMC Continuous Monitoring

HallMonitor's scheduled scanning directly satisfies NIST 800-171 controls RA.L2-3.11.2 (Vulnerability Scanning), CA.L2-3.12.1 (Security Assessment), CA.L2-3.12.3 (Continuous Monitoring), and SI.L2-3.14.5 (Security Alerts).

Evaluation Checklist

Use this checklist to track your evaluation progress from installation through evidence submission.

#	Step	Reference	Done
1.	Install ForteFide (Windows .exe or Linux .deb)	Installation	[ ]
2.	Import and activate license (drag-drop, Manage License, or API)	License Activation	[ ]
3.	Run network discovery -- enter CIDR, select in-scope hosts	Step 1	[ ]
4.	Prepare endpoints -- create fortefide-svc service accounts	Step 2	[ ]

5.	Configure and execute full 110-control scan	Step 3	[ ]
6.	Verify baseline evidence package was auto-collected	Step 4	[ ]
7.	Review findings and complete manual attestations (AT=3, PE=6, PS=2)	Step 5	[ ]
8.	Add control overrides for documented exceptions	Step 5	[ ]
9.	Run batch remediation -- select severity levels	Step 6	[ ]
10.	Rescan to verify remediation improvements	Step 6	[ ]
11.	Collect final evidence package (post-remediation)	Step 7	[ ]
12.	Teardown endpoints -- remove fortefide-svc from all targets	Step 7	[ ]
13.	Verify evidence integrity with verify_evidence.py	Step 7	[ ]
14.	Submit both evidence ZIPs (baseline + final) to C3PAO	Submission	[ ]

Once all 14 steps are complete, your organization is ready for CMMC Level 2 third-party assessment. Provide both evidence packages to your C3PAO -- the assessor uses verify_evidence.py to confirm package integrity and the delta between baseline and final scans demonstrates your compliance journey.