ForteFide Administration Guide

CMMC(TM) Level 2 / NIST 800-171 Compliance Readiness Platform

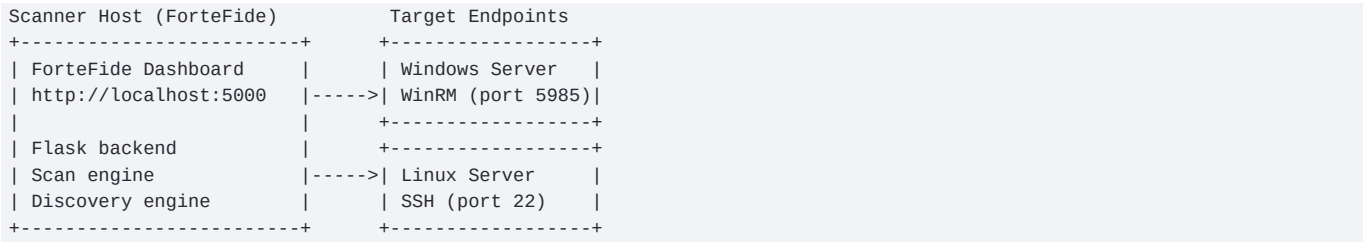
Version	1.4.9.2
Date	April 2026
Product	ForteFide by DenseDefense
Framework	NIST SP 800-171 Rev 2 / CMMC(TM) Level 2 (110 controls, 14 families)
Platforms	Windows (.exe) + Linux (.deb)
Publisher	DenseDefense -- DFW, Texas
Website	densedefense.com

Table of Contents

1. Product Overview

ForteFide is a CMMC(TM) Level 2 compliance readiness scanner and remediation platform that helps organizations prepare for CMMC assessment by scanning Windows and Linux endpoints against all 110 NIST SP 800-171 Rev 2 controls across 14 families. It provides automated compliance readiness scanning via WinRM (Windows) and SSH (Linux), network discovery, a Risk Operations Center (ROC) dashboard, PDF compliance reports, batch remediation, cryptographically signed evidence packages, and scheduled scanning. All deployments are fully air-gap ready with no internet connectivity required.

Architec



Control Families

ForteFide assesses 110 controls across 14 NIST 800-171 families:

Family	Name	Controls
AC	Access Control	22
AT	Awareness & Training	3
AU	Audit & Accountability	9
CA	Assessment & Authorization	4
CM	Configuration Management	9
IA	Identification & Authentication	11
IR	Incident Response	3
MA	Maintenance	6
MP	Media Protection	9
PE	Physical & Environmental Protection	6
PS	Personnel Security	2
RA	Risk Assessment	3
SC	System & Communications Protection	16
SI	System & Information Integrity	7

Key Capabilities

- 110-control NIST 800-171 compliance readiness scanning (Windows + Linux) via WinRM and SSH
- Network discovery: CIDR sweep, Active Directory LDAP, jump host/proxy
- Endpoint preparation: automated fortefide-svc service account creation and teardown
- Batch remediation with bulletproof safety engine (smart ordering, rollback)
- Danger Mode for manual/risky controls with rollback
- Cryptographically signed evidence packages (SHA-256, Ed25519, machine fingerprint)
- Encrypted scan persistence (AES-256-GCM, device-bound SQLite)
- Scheduled scanning with definition updates (connected) or offline import (air-gap)
- HallMonitor security advisor with continuous monitoring
- 55-route REST API for automation and integration
- Per-host credentials with dual credential profiles (Windows/Linux)
- Auto OS detection for mixed-OS environments

2. System Requirements

Scanner Host (where ForteFide is installed)

Windows:

- Windows 10/11 or Windows Server 2019+
- 4 GB RAM minimum, 500 MB disk space
- Administrator privileges for installation
- Network access to target endpoints (TCP 5985 for WinRM, TCP 22 for SSH)

Linux (Debian/Ubuntu):

- Debian 11+ or Ubuntu 22.04+, x86_64 (amd64)
- libc6 >= 2.28 (standard on all supported releases)
- 4 GB RAM minimum, 500 MB disk space
- Root or sudo access for installation and service management
- No Python runtime required -- native ELF binary (Nuitka-compiled)
- No internet access required -- fully self-contained

Target Endpoints

Platform	Minimum OS	Required Service	Port
Windows	Windows 10/Server 2016+	WinRM enabled	TCP 5985
Linux	Any modern distribution	SSH enabled	TCP 22

3. Installation

Windows (.exe)

- Download ForteFide_Setup_1.4.2_Windows.exe
- Right-click and select Run as Administrator
- Follow the setup wizard -- default path: C:\Program Files\ForteFide\
- Select dashboard port during installation (default: 5000)
- ForteFide launches automatically and opens http://localhost:5000

What the installer does:

- Installs application files to C:\Program Files\ForteFide\
- Creates Start Menu shortcuts (ForteFide + Uninstall)
- Registers in Add/Remove Programs (HKLM\SOFTWARE\ForteFide)
- Creates Windows Firewall rule for the dashboard port
- Uses runasoriginaluser flag to launch browser in user context (FIX-058)

Linux (.deb)

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

The .deb contains a native ELF binary (Nuitka-compiled). No Python runtime, virtual environment, or pip packages are required.

Path	Purpose
/opt/fortefide/	Native ELF binary and support files
/opt/fortefide/fortefide	Main executable (Nuitka ELF)
/usr/lib/systemd/system/fortefide.service	Systemd unit (LimitSTACK=infinity)
/usr/local/bin/fortefide	CLI launcher
/usr/local/bin/fortefide-setup	First-run setup wizard
/etc/fortefide/fortefide.conf	Configuration file
/var/lib/fortefide/	Runtime data directory

Air-Gap Deployment

Both the Windows .exe and Linux .deb are fully self-contained. Transfer the installer to the air-gapped network via USB drive or approved media. No internet connectivity is required at any point: installation, scanning, remediation, evidence collection, and license verification all operate entirely offline.

- Windows: copy .exe to USB, run on target machine
- Linux: copy .deb to USB, install with dpkg -i
- License: transfer .key file via USB; verification is Ed25519 offline
- Definitions: transfer .ddef file via USB; import through dashboard or API

Linux First-Run Setup

```
sudo fortefide-setup
```

- Dashboard configuration: bind address (default: 0.0.0.0) and port (default: 5000)
- SSH key generation (optional): generates Ed25519 keypair for key-based auth
- Firewall configuration: opens dashboard port using ufw or firewalld
- Service start: optionally starts ForteFide service immediately

4. License Management

Import Methods

ForteFide supports three methods to import a license:

- **Drag & Drop:** drag the .key file onto the license panel in the lower-left sidebar
- **Manage License:** click the button in the sidebar and use the file import dialog
- **API:** POST /api/import-license with base64-encoded license content

```
POST /api/import-license
{"content": "<base64-encoded license.key content>"}
```

Activation Code (Split-Key Unlock)

ForteFide uses a two-phase delivery model. The license.key file enables scanner features. If the license contains key_material, a separate activation code is required to unlock the split-key remediation engine.

- Activation code format: FIDE-XXXX-XXXX-XXXX-XXXX-XXXX-XXXX (base32, AES-256-GCM encrypted)
- Enter the code in the dashboard activation panel or via API:

```
POST /api/activate
{"activation_code": "FIDE-XXXX-XXXX-XXXX-XXXX-XXXX-XXXX"}
```

- Dual-bound: activation code is cryptographically bound to both the build binary and license_id
- Device-locked: triple binding (device hardware + license + binary) prevents transfer
- Fully offline: no network traffic, no phone-home -- entirely air-gap compatible
- One-time entry: activation state is persisted locally; code is not needed after restarts

Machine-Bound Licensing

- Step 1: Run fortefide --request-code on the target machine -- generates SHA-256 hash of hardware fingerprint
- Step 2: Send the request code to DenseDefense (email, USB, or any offline channel)
- Step 3: Receive a license.key tied to that machine's fingerprint, signed with Ed25519
- Step 4: Install the .key file -- ForteFide verifies fingerprint match before accepting

Fingerprint factors:

Platform	Fingerprint Sources
Windows	HKLM\SOFTWARE\Microsoft\Cryptography\MachineGuid + hostname + disk serial + OS platform
Linux	/etc/machine-id + hostname + disk serial + OS platform

Drag-and-Drop Import

The license panel in the lower-left sidebar accepts drag-and-drop file import. Drag a .key file from your file manager directly onto the panel. The license is validated immediately and licensed features unlock without restart.

License Tiers

Feature	Free	Starter	Professional	Enterprise
Price (Monthly)	$0	$599/mo	$1,799/mo	From $4,999/mo
Price (Annual)	$0	$499/mo	$1,499/mo	From $4,166/mo
Scanning (110 controls)	Yes	Yes	Yes	Yes
Max Endpoints	Unlimited	25	100	500+
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.

License Hot-Reload

ForteFide supports license hot-reload. Import a license and activate paid features without restarting the application. All in-memory scan results, score history, and delta comparisons are preserved across license changes.

Air-Gap License Activation

DenseDefense products are fully designed for air-gapped environments. The licensing system does not require an internet connection at any point during activation or ongoing use.

- 1. Export Request Code: On the air-gapped machine, run 'fortefide --request-code' or click 'Save to File' next to the Request Code in the UI. Save to a USB drive.
- 2. Transfer to connected machine: Move the USB drive to a machine with network or email access.
- 3. Submit Request Code: Send the file to DenseDefense via email (sales@densedefense.com) or the customer portal.
- 4. Receive license file: DenseDefense sends back a .key file bound to your air-gapped machine's hardware fingerprint.

- 5. Transfer license to USB: Save the .key file to a USB drive.
- 6. Import on air-gapped machine: Import the .key file via drag-and-drop, file dialog, or API.
- 7. Enter activation code (if applicable): Type the activation code manually. The code is short enough to transcribe by hand if necessary.

SECURITY NOTE
The license file and activation code contain no sensitive information about your network, infrastructure, or scan results. They are safe to transfer through unclassified channels. Treat the activation code as confidential since it unlocks licensed features.

Machine Transfers

If you need to move your license to a different machine (hardware upgrade, OS reinstall, or workstation replacement), you can request a license transfer.

You NEED a transfer if you:

- Replaced the machine's primary hard drive
- Reinstalled the operating system (regenerates the machine ID)
- Renamed the machine's hostname
- Are migrating to entirely new hardware

You do NOT need a transfer if you:

- Upgraded RAM or added a network adapter
- Applied OS patches or updates (not a reinstall)
- Migrated a virtual machine to a different host (guest OS unchanged)

To request a transfer:

- 1. Generate a Request Code on the NEW machine
- 2. Contact DenseDefense support with your existing license ID and the new Request Code
- 3. DenseDefense revokes the old license and issues a new .key file for the new machine
- 4. Import the new .key file on the new machine

License transfers do not consume an additional seat. The old license is deactivated and replaced by the new one. Each order includes 2 free transfers. Additional transfers require admin approval. Enterprise customers with priority support receive emergency transfer processing.

License Expiration & Renewal

When your license expires, previously collected scan results and evidence remain accessible, but you cannot run new scans or perform remediation. The dashboard displays a clear expiration notification.

To renew:

- Contact your DenseDefense account representative or sales team
- A new .key file is generated with the updated expiration date
- If hardware has not changed, no new Request Code is needed
- Import the new .key file to replace the expired one -- features restore immediately

Billing Cycle	Duration	Renewal
Monthly	30 days from order	Automatic (if payment on file) or manual
Annual	365 days from order	Contact sales or account representative
Trial	10 days from activation	Convert to paid subscription to continue

We recommend renewing at least 14 days before expiration to ensure uninterrupted service. Renewal reminders are sent as the expiration date approaches.

Contact & Support

- Technical Support: support@densedefense.com
- Sales & Licensing: sales@densedefense.com
- Web: densedefense.com/pricing

Response times: within 1 business day (Starter/Professional), 4 hours (Enterprise). When contacting support, include your license ID, order reference, product version, OS version, and any error messages or log files.

5. 7-Step Compliance Readiness Workflow

ForteFide follows a structured 7-step workflow from initial reconnaissance through final evidence collection and teardown. Each step builds on the previous one.

Step	Name	Description
1	Network Recon	CIDR discovery, host detection, target selection
2	Prepare Endpoints	Resource groups, service account creation, key deployment
3	Configure & Execute Scan	Auto-detect prepared hosts, 110-control scan
4	Baseline Evidence	Auto-collect signed evidence package after scan
5	Review, Attest & Override	Findings review, 11 attestations, documented overrides
6	Remediate & Rescan	Batch remediation, DANGER MODE, rescan to verify
7	Final Evidence & Teardown	Collect final package, remove all artifacts

6. Step 1: Network Recon (Discovery)

Discovery finds scan targets on your network. Access it from the collapsible Network Discovery panel in the center of the dashboard.

Method 1: CIDR Network Scan

- Enter a CIDR range (e.g., 192.168.1.0/24)
- TCP port probe across all addresses to find live hosts
- OS detection based on open ports: 135/445/5985 = Windows, 22 = Linux
- Results: IP, hostname (reverse DNS), OS guess, open ports
- Duration: 2-5 minutes for a /24 (254 addresses)
- No credentials required

Method 2: Active Directory (LDAP)

- Enter DC IP, domain name, and domain credentials
- Single LDAP query enumerates all computer objects
- Results: hostname, OS version, OU, last logon, enabled/disabled status
- Uses NTLM authentication via ldap3 (pure Python, air-gap safe)
- Duration: seconds regardless of network size

Method 3: Jump Host / Proxy

- Discover hosts through an SSH bastion/jump host for isolated network segments
- Enter proxy host details and remote network CIDR or AD connection details
- Scanner creates SSH tunnel and runs discovery on the remote network

Discovery Comparison

Criteria	CIDR Sweep	AD Discovery
Credentials	None	DC IP + domain creds
Protocol	TCP port probe (per IP)	Single LDAP query
Speed (/24)	2-5 minutes	Seconds
Scope	All devices on subnet	Domain-joined only
Finds unmanaged	Yes	No
Best for CMMC	Secondary	Primary

Using Discovery Results

- Review discovered hosts table -- filter by OS type if needed
- Select hosts using checkboxes; deselect non-scannable devices
- Click "Scan Selected" to populate scan targets
- Use "Merge" to combine with previously discovered hosts
- Discovery flows directly into the scan configuration panel

7. Step 2: Prepare Endpoints (Resource Groups)

Resource Groups

Targets are organized into resource groups. Each group has its own credential set, allowing mixed environments with different admin credentials per group.

- Groups are auto-created based on OS detection (Windows group, Linux group)
- Custom groups can be created for specific subnets or organizational units
- Per-group credentials: DOMAIN\Admin for Windows, root for Linux, etc.

API Endpoints for Resource Groups

Method	Endpoint	Description
GET	/api/resource-groups	List all resource groups
POST	/api/resource-groups	Create a resource group
PUT	/api/resource-groups/<id>	Update group credentials
DELETE	/api/resource-groups/<id>	Delete a resource group
POST	/api/prepare-endpoint	Create service account on target
POST	/api/teardown-endpoint	Remove service account from target

Authentication Methods

Method	Use Case	Configuration
Password	Standard username/password	Enter creds in UI or API
SSH Key	Key-based auth (Linux)	Auto-generate Ed25519 or provide existing key
Certificate	PKI/cert-based auth	Import certificate and key pair

Service Account Creation

When you click "PREPARE SELECTED ENDPOINTS", ForteFide creates a fortefide-svc account on each target:

Component	Linux	Windows
Account name	fortefide-svc	fortefide-svc
Password	Strong random, never expires	Strong random, never expires
Admin access	sudo group + /etc/sudoers.d/	Administrators + Remote Mgmt Users
Access restriction	SSH only	WinRM only (deny interactive + RDP)
SSH key (optional)	~/.ssh/authorized_keys	N/A

CM.3.067 Warning

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. Always use the fortefide-svc account (which is always in sudo) or ensure your custom account has sudo group membership before enabling CM.3.067 remediation.

8. Step 3: Configure & Execute Scan

Auto-Detection of Prepared Endpoints

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

Dual Credential Profiles

ForteFide supports two simultaneous credential profiles -- one for Windows targets and one for Linux targets. When scanning a mixed-OS environment, each host is matched to the appropriate profile based on auto OS detection.

Profile	Transport	Port	Auth Methods
Windows	WinRM / SSH / PSRP	5985 / 22	NTLM, password, key, cert
Linux	SSH	22	Password, SSH key, certificate

Auto OS Detection

- ForteFide probes each target's open ports before scanning
- Ports 135/445/5985 indicate Windows; port 22 indicates Linux
- The correct credential profile and check set are selected automatically
- Override available: manually set OS type per host if auto-detection is incorrect

Manual Credential Override (Per-Host)

- For unprepared hosts, enter credentials manually in the inline scan configuration
- Use the per-host credential dropdown to assign different credentials to specific hosts
- Credential profiles are stored in credential_profiles._hosts[ip] in the session

Certificate-Based Authentication

- Upload client certificate and private key through the scan configuration UI
- Certificate auth is supported for both SSH (Linux) and WinRM (Windows with HTTPS)
- Certificates are used for the scan session only and are not persisted to disk

Scan Execution

- Click "EXECUTE SCAN" to begin the assessment
- 110 NIST 800-171 controls are evaluated per host
- Progress is shown per-host, per-control in the Activity Log
- Windows: ~30s per host via WinRM; Linux: ~15s per host via SSH
- Results are auto-saved to encrypted SQLite on completion

9. Step 4: Baseline Evidence Collection

Baseline evidence is auto-collected after the first scan completes. The evidence package captures the pre-remediation compliance posture and establishes the starting point for your CMMC assessment.

Chain of Custody

- Every file in the package is hashed with SHA-256
- Machine fingerprint is embedded in the manifest (ties evidence to the scanning host)
- Verification manifest is signed with Ed25519 digital signatures
- Timestamps recorded for every artifact
- Downloaded as a cryptographically signed ZIP

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
Incident Response Plan	Template IRP aligned to NIST 800-171 IR family
Training Records Template	Blank template for security training documentation
14 Policy Documents	One policy per applicable CMMC family
Verification Manifest	SHA-256 hashes + Ed25519 signature
verify_evidence.py	Standalone verification script (Python 3 only)

Standalone Verifier

Every evidence package includes verify_evidence.py. The assessor runs this script to independently confirm that no documents have been tampered with. It requires only Python 3 -- no ForteFide installation needed.

```
python verify_evidence.py ForteFide_Evidence_2026-03-30.zip
```

10. Step 5: Review, Attest & Override

After 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.

Results Views

- Score Cards: compliance %, passed/failed, severity counts (Critical/High/Medium/Low)
- Overview tab: executive summary, family-level scores, risk distribution chart
- Family Breakdown: per-family compliance across all 14 CMMC families
- Findings tab: filterable list with severity, control ID, description, remediation steps
- Delta tab: before/after comparison showing controls that changed status
- Host Filter: filter by specific host IP to focus on one endpoint

Attestations (11 Controls)

See Section 18 for complete attestation details.

Family	Count	Controls
AT -- Awareness & Training	3	AT.L2-3.2.1, AT.L2-3.2.2, AT.L2-3.2.3
PE -- Physical Protection	6	PE.L2-3.10.1 through PE.L2-3.10.6
PS -- Personnel Security	2	PS.L2-3.9.1, PS.L2-3.9.2

Control Overrides

See Section 17 for complete override documentation.

- Documented Exception: the control requirement does not apply
- Alternative Implementation: the requirement is met through a different mechanism
- Minimum 20-character justification required
- All overrides tracked with audit trail in evidence package
- Click "PROCEED TO REMEDIATION" when ready for Step 6

11. Step 6: Remediate & Rescan

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
- Activity Log shows real-time progress with OK/FAIL status per control

Bulletproof Remediation Engine

ForteFide's remediation engine includes multiple safety layers designed to prevent lockouts and service disruption. See Section 14 for full technical details.

Feature	Description
Smart Ordering	Safe controls first; connectivity-affecting controls last
Preflight Check	Connectivity verification before each host
90s Timeout	Per-control timeout prevents hangs
Lockout Detection	3 consecutive auth failures trigger auto-rollback
Auto-Rollback	Reverts if post-remediation connectivity check fails
CM.3.067 Last	AllowGroups sudo always runs absolutely last

DANGER MODE

- For controls marked MANUAL INTERVENTION (higher risk)
- Confirmation overlay requires explicit acknowledgment
- Automatic rollback capability for every action
- See Section 15 for full Danger Mode documentation

Rescan

- After remediation, click "RESCAN NOW" in the same panel
- Delta tab shows before/after comparison
- Remaining failures can be addressed with additional remediation or overrides

12. Step 7: Final Evidence & Teardown

Final Evidence Package

- Click "COLLECT & SIGN EVIDENCE" after rescan confirms improved posture
- Generates post-remediation evidence package with same chain of custody as baseline
- Both baseline (Step 4) and final (Step 7) ZIPs submitted to C3PAO
- Delta between scans demonstrates compliance improvement

Teardown

- Click "TEARDOWN SELECTED ENDPOINTS" to remove all artifacts from targets

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

Verification

- Use standalone verification script to confirm all artifacts removed
- Checks for residual accounts, sudoers entries, SSH keys on each target

Always Teardown
The fortefide-svc account has elevated privileges. Leaving it after assessment is a security risk. Teardown removes everything -- zero artifacts remain.

13. Scan Persistence (Encrypted SQLite)

ForteFide v1.4.2 automatically persists scan results across application restarts in an encrypted SQLite database. No configuration required.

How It Works

- On scan completion: results serialized and written to encrypted SQLite
- On startup: previous scan results restored into dashboard
- Browser refresh (F5): safe -- all data persists
- Service restart: safe -- all data persists

Database Location

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

Encryption Details

Property	Value
Cipher	AES-256-GCM (authenticated encryption)
Key derivation	HKDF-SHA256 from machine hardware fingerprint
Device binding	Yes -- unreadable on a different machine
Key management	Fully automatic (no user interaction)
Backup	Files can be backed up but only restored to same machine

Operational Behavior

- Auto-save: every completed scan persisted immediately
- Auto-restore: all saved scans loaded on startup

- Crash recovery: partial scans not persisted; only completed scans saved
- Disk usage: ~10-50 KB per host per scan
- Reset: delete scans.db to clear all history; recreated on next scan

Security

Encrypted scan data satisfies NIST 800-171 controls SC.L2-3.13.16 (protection of CUI at rest) and MP.L2-3.8.9 (media protection). Even if scans.db is exfiltrated, it cannot be decrypted without the original machine's hardware fingerprint.

14. Remediation Engine (Bulletproof)

ForteFide's bulletproof remediation engine is designed to prevent lockouts and minimize service disruption during automated compliance remediation.

Smart Control Ordering

Controls are executed in a safety-prioritized order:

- Phase 1: Safe controls -- audit policies, password settings, USB disable, registry hardening
- Phase 2: Medium-risk controls -- service configuration, account policies
- Phase 3: Connectivity-affecting controls -- firewall rules, sshd configuration
- Phase 4 (LAST): CM.3.067 (AllowGroups sudo) -- always runs absolutely last

CONNECTIVITY_CONTROLS List

The following controls are flagged as connectivity-affecting and receive special treatment during remediation (post-change verification, auto-rollback on failure):

- SC.L2-3.13.1: Boundary protection (firewall rules)
- SC.L2-3.13.6: Network communication by exception (deny-all firewall)
- CM.3.067: AllowGroups sudo (SSH access restriction)
- AC.L2-3.1.12: Remote access session control

Preflight Check

- Before remediating each host, ForteFide verifies connectivity (WinRM or SSH)
- If the host is unreachable, it is skipped and flagged in the activity log
- No remediation is attempted on unreachable hosts

90-Second Timeout

- Each control has a 90-second execution timeout
- Prevents hangs on unresponsive endpoints or long-running commands
- Timed-out controls are marked FAIL and the engine moves to the next control

Lockout Detection

- ForteFide tracks consecutive authentication failures per host
- 3 consecutive failures trigger automatic rollback of all changes on that host
- The host is flagged as LOCKOUT DETECTED in the activity log
- Remediation continues on other hosts

Auto-Rollback

- After connectivity-affecting controls, ForteFide re-verifies connectivity
- If connectivity is lost, the last change is automatically rolled back
- Rollback restores the previous configuration for that specific control
- The control is marked ROLLED BACK in the activity log

15. Danger Mode

Danger Mode provides remediation for controls that are too risky for fully automated execution. These controls are marked MANUAL INTERVENTION in the findings view.

How Danger Mode Works

- Select a MANUAL INTERVENTION control in the findings view
- Click "Remediate (DANGER MODE)"
- A confirmation overlay appears explaining the risk and expected impact

- You must explicitly acknowledge the risk before execution proceeds
- The remediation executes with the same bulletproof safety features (timeout, rollback)

Rollback Capability

- Every Danger Mode remediation records the pre-change state
- If the change causes connectivity loss, it is automatically rolled back
- Manual rollback is also available via the activity log

> **Danger Mode Safety**
> Danger Mode controls are never included in batch remediation. They must be executed individually with explicit confirmation. This prevents accidental execution of high-risk changes during automated batch runs.

16. Evidence Chain of Custody

Cryptographic Integrity

Component	Algorithm	Purpose
File hashes	SHA-256	Tamper detection for every file in the package
Manifest signature	Ed25519	Non-repudiation -- proves who generated the evidence
Machine fingerprint	SHA-256 of HW IDs	Provenance -- ties evidence to specific scanner host
Timestamps	ISO 8601 UTC	Temporal ordering of all evidence artifacts

Verification Manifest

The verification manifest (manifest.json) is the cornerstone of evidence integrity. It contains SHA-256 hashes for every file in the package, the machine fingerprint, generation timestamp, and an Ed25519 signature covering the entire manifest.

Standalone Verifier

Every evidence package includes verify_evidence.py, a standalone script that validates the entire package without requiring ForteFide. The script:

- Verifies the Ed25519 signature on the manifest
- Recalculates SHA-256 hashes for every file and compares against manifest
- Reports any tampered, missing, or extra files
- Requires only Python 3 standard library (no pip packages)

17. Control Overrides

Control overrides allow organizations to document exceptions and alternative implementations for controls that cannot be met through technical remediation.

Override Types

Type	When to Use	Example
Documented Exception	Control does not apply to this environment	Air-gapped network has no wireless -- AC.L2-3.1.16 N/A
Alternative Implementation	Requirement met through different mechanism	Smart card used instead of password complexity

Creating an Override

- Open any finding detail view in the Findings tab
- Click the "OVERRIDE" button
- Select override type: Documented Exception or Alternative Implementation
- Enter justification (minimum 20 characters)
- Optionally reference supporting evidence or documentation
- Click "Save Override" to apply

Audit Trail

- Overrides are recorded with timestamp, user context, type, and justification
- All overrides are included in the evidence package for assessor review
- Overrides can be edited or removed before final evidence collection

18. Attestations (11 Manual Controls)

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

Attestation Controls

Control ID	Family	Description
AT.L2-3.2.1	AT	Security awareness training for all users
AT.L2-3.2.2	AT	Role-based security training
AT.L2-3.2.3	AT	Insider threat awareness training
PE.L2-3.10.1	PE	Physical access authorizations
PE.L2-3.10.2	PE	Physical access control at entry/exit points
PE.L2-3.10.3	PE	Escort visitors and monitor activity
PE.L2-3.10.4	PE	Physical access audit logs
PE.L2-3.10.5	PE	Physical access to output devices
PE.L2-3.10.6	PE	Alternative work site physical controls
PS.L2-3.9.1	PS	Screen individuals prior to granting access
PS.L2-3.9.2	PS	Protect CUI during personnel actions

How to Attest

- Open the Attestations tab in the results view
- Check each control that your organization has implemented
- Confirmation modal: "By checking this control, I attest that this requirement has been implemented..."
- Attestations are recorded with timestamp and included in evidence package
- Uncheck a previously attested control to remove the attestation

19. Scheduler & Definitions

Scan Scheduler Configuration

Access the scheduler from Settings -> Scheduler. Requires Professional or Enterprise license.

Interval	Description
Daily	Runs once every 24 hours at configured time
Weekly	Runs once per week on configured day and time
Biweekly	Runs once every two weeks
Monthly	Runs on the same day each month

Scheduler Behavior

- Checks whether scanner is idle (concurrent scans are queued)
- Connected: auto-pulls latest definitions before scanning
- Air-gapped: runs on schedule, shows reminder if definitions >7 days old
- Writes audit log entry with schedule ID, trigger time, scan ID, results

Starting and Stopping

```
# Start scheduler
POST /api/scheduler/start

# Stop scheduler
POST /api/scheduler/stop

# Check status
GET /api/scheduler/status

# View history
GET /api/scheduler/history
```

Definition Updates

- Connected: automatic pull from definitions.densedefense.com before each scheduled scan
- Air-gapped: download .ddef file on internet-connected machine, transfer via USB
- Import via dashboard (Settings -> Definitions -> Import) or API:

```
POST /api/definitions/import
Content-Type: multipart/form-data
(attach .ddef file)
```

- Every definition package is Ed25519 signed; tampered packages are rejected
- Staleness reminder appears when definitions >7 days old (non-blocking banner)
- Dismiss for 7 days via button or POST /api/definitions/dismiss-reminder

CMMC Compliance Mapping

Control ID	Name	How Scheduler Satisfies
RA.L2-3.11.2	Vulnerability Scanning	Recurring scans on defined cadence
CA.L2-3.12.1	Security Assessment	Automated periodic assessment
CA.L2-3.12.3	Continuous Monitoring	Ongoing compliance monitoring
SI.L2-3.14.5	Security Alerts	Definition updates keep checks current

20. API Reference (55 Routes)

ForteFide exposes a REST API on the dashboard port (default: 5000) for integration and automation. All endpoints accept and return JSON.

Scanning (6 routes)

Method	Endpoint	Description
POST	/api/scan	Start a new scan
GET	/api/scans	List all completed scans
GET	/api/scan/<id>	Get scan details by ID
GET	/api/scan/<id>/pdf	Download PDF report for scan
GET	/api/scan/<id>/delta/<prev>	Compare two scans (delta)
GET	/api/scan/history	Score history for trending

Discovery (3 routes)

Method	Endpoint	Description
POST	/api/discover	Start network or AD discovery
GET	/api/discover/<id>	Get discovery results
POST	/api/discover/merge	Merge discovery result sets

Remediation (4 routes)

Method	Endpoint	Description
POST	/api/remediate	Remediate a single control
POST	/api/remediate-batch	Batch remediate controls
POST	/api/remediate-danger	Danger Mode remediation
POST	/api/remediate-rollback	Rollback a remediation

Endpoint Preparation (4 routes)

Method	Endpoint	Description
POST	/api/prepare-endpoint	Create service account on target
GET	/api/prepare-endpoint/<id>	Check preparation status
POST	/api/teardown-endpoint	Remove service account
GET	/api/teardown-endpoint/<id>	Check teardown status

Resource Groups (4 routes)

Method	Endpoint	Description
GET	/api/resource-groups	List all resource groups
POST	/api/resource-groups	Create a resource group
PUT	/api/resource-groups/<id>	Update group credentials
DELETE	/api/resource-groups/<id>	Delete a resource group

Evidence (4 routes)

Method	Endpoint	Description
POST	/api/evidence/collect	Collect and sign evidence package
GET	/api/evidence/<id>	Download evidence ZIP
GET	/api/evidence/list	List all evidence packages
POST	/api/evidence/verify	Verify evidence package integrity

License & Activation (4 routes)

Method	Endpoint	Description
POST	/api/import-license	Import license (base64 content)
POST	/api/activate	Activate with activation code
GET	/api/license-status	License state, tier, expiry, features
GET	/api/capabilities	Feature flags and version info

Scheduler (6 routes)

Method	Endpoint	Description
GET	/api/scheduler/status	Current state and next run time
GET	/api/scheduler/config	Retrieve all schedule configs
POST	/api/scheduler/config	Create or update schedule
POST	/api/scheduler/start	Start (enable) scheduler
POST	/api/scheduler/stop	Stop (pause) scheduler
GET	/api/scheduler/history	Audit log of scheduler events

Definitions (4 routes)

Method	Endpoint	Description
GET	/api/definitions/status	Current version, date, staleness
POST	/api/definitions/import	Import .ddef definition package
GET	/api/definitions/history	History of definition updates
POST	/api/definitions/dismiss-reminder	Dismiss staleness reminder

Attestations & Overrides (6 routes)

Method	Endpoint	Description
GET	/api/attestations	List all attestations
POST	/api/attestations	Create or update an attestation
DELETE	/api/attestations/<id>	Remove an attestation
GET	/api/overrides	List all control overrides
POST	/api/overrides	Create a control override
DELETE	/api/overrides/<id>	Remove an override

Other (9 routes)

Method	Endpoint	Description
GET	/api/matrix	Full CMMC control matrix (110 controls)
GET	/api/matrix/<id>	Single control details
GET	/api/logs	Activity log (?since=N for filtering)
GET	/api/status	System health and uptime
GET	/api/config	Current configuration
POST	/api/config	Update configuration
GET	/api/hallmonitor/status	HallMonitor security advisor state
POST	/api/hallmonitor/scan	Trigger HallMonitor threat scan
GET	/api/hallmonitor/findings	HallMonitor findings and alerts

Total: 55 documented routes across 10 categories.

21. Security Architecture

ForteFide v1.4.2 includes eight layers of binary protection, intellectual property security, and anti-reverse-engineering measures.

Layer 1: Binary Compilation (Nuitka)

The application is compiled from Python to native C code using Nuitka. The resulting binary is not reversible with standard Python decompilers (pyinstxtractor, uncompyle6, etc.).

Layer 2: Split-Key Architecture

Cryptographic keys are never stored as single values. Each key is split into multiple XOR-masked fragments distributed across separate compiled modules. Fragments are recombined in memory only when needed and zeroed after use.

Layer 3: Command Generation Engine

Remediation commands are generated at runtime from parameterized templates and control-specific logic. Commands are never stored as static strings, eliminating the attack surface of encrypted command stores.

Layer 4: AES-256-GCM Encryption

All remediation commands are encrypted at rest using AES-256-GCM with HKDF-SHA256 per-command key derivation. Commands are decrypted one at a time in memory during execution and never cached in plaintext.

Layer 5: Activation Code Security

Activation codes use AES-256-GCM with HKDF key derivation. The payload is bound to the build binary hash and license_id. Device-locked activation uses triple binding (device HW fingerprint + license + binary).

Layer 6: Ed25519 License Verification

License validation uses Ed25519 digital signatures. The public key is embedded in the compiled binary at build time. Verification is fully offline.

Layer 7: Integrity Self-Checks

At startup, ForteFide verifies integrity of critical files using SHA-256 hashes, control dictionary counts, encrypted store counts, and module canary attributes.

Layer 8: Anti-Forensic Properties

- No network traffic: all operations local -- no telemetry, no phone-home
- Encrypted I/O: remediation commands exist only encrypted on disk
- Memory zeroing: sensitive values overwritten after use

PIPpro (Proprietary IP Protection)

ForteFide uses PIPpro, the DenseDefense proprietary IP protection layer, which combines all eight layers into a unified anti-tampering and anti-extraction system.

Security Layer Summary

Layer	Protection	Mechanism
1	Binary compilation	Nuitka C compilation
2	Split-key architecture	XOR-masked fragments across modules
3	Command generation	Runtime assembly from templates
4	Command encryption	AES-256-GCM + HKDF per-command keys
5	Activation codes	AES-256-GCM, device-locked triple binding
6	License signing	Ed25519 asymmetric signatures
7	Integrity checks	SHA-256 hashes, canary attributes
8	Anti-forensic	No network, encrypted I/O, memory zeroing

22. HallMonitor Security Advisor

HallMonitor is ForteFide's built-in security advisor that provides continuous monitoring, threat analysis, and proactive compliance management.

Capabilities

- Scheduled threat scanning: daily, weekly, biweekly, or monthly cadences
- Continuous monitoring: tracks compliance drift between scheduled scans
- Alert notifications: dashboard alerts when score drops below threshold
- Definition management: auto-updates in connected environments
- Compliance trending: historical score tracking with trend analysis
- Audit trail: every event logged with timestamps and results

API Endpoints

Method	Endpoint	Description
GET	/api/hallmonitor/status	Current HallMonitor state
POST	/api/hallmonitor/scan	Trigger threat scan
GET	/api/hallmonitor/findings	HallMonitor findings and alerts

CMMC Compliance Mapping

HallMonitor directly supports continuous monitoring requirements: 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).

23. Troubleshooting

Dashboard Not Loading

- Check service: sudo systemctl status fortefide (Linux)
- Check port: ss -tlnp | grep 5000 (Linux) or netstat -ano | findstr 5000 (Windows)
- Check firewall: sudo ufw status or Windows Firewall settings
- View errors: sudo journalctl -u fortefide -n 50 (Linux) or fortefide.log (Windows)

Windows Target Scan Fails

- Connection refused on 5985: enable WinRM on target (enable-winrm-scan.ps1)
- Access denied: verify local admin creds, check LocalAccountTokenFilterPolicy = 1
- Timeout: check target responsiveness and network connectivity
- Command truncation: switch transport to SSH or PSRP (no 8KB limit)

Linux Target Scan Fails

- Connection refused on 22: start SSH service (sudo systemctl start ssh)
- Authentication failed: verify credentials, check PasswordAuthentication in sshd_config
- Permission denied (sudo): verify sudoers config for scan account
- CM.3.067 lockout: use fortefide-svc account (always in sudo group)

Scan Shows 0% Compliance

- Verify credentials are correct (test manually with ssh/winrm)
- Verify OS type selection matches the target (or use auto-detect)
- Check Activity Terminal for specific error messages
- Ensure WinRM/SSH is reachable from the scanner host

License Issues

- Invalid/corrupt license: ensure the .key file was not modified after receipt. Even a blank line breaks the Ed25519 signature. Re-download the original file.
- Machine mismatch: license was generated for a different machine. If you changed hostname, reinstalled OS, or replaced hardware, request a transfer (see Section 4).
- Activation code rejected: the code is bound to a specific build + license_id. Verify you are on the correct machine. Copy-paste rather than typing manually.
- Expired: check expiry date via /api/license-status. Contact sales to renew.
- Seat limit reached: your order has a max number of concurrent licenses. Revoke an unused license to free a seat, or contact sales to upgrade.
- Application won't start: check fortefide.log for errors. Ensure license.key is in one of the expected locations (app dir, home dir, or system config dir). On Windows, try running as Administrator for initial setup.

Evidence Collection Fails

- No scan data: run a scan first -- evidence requires at least one completed scan
- Permission denied: ensure write access to installer_output directory
- ZIP creation error: check disk space

Browser Shows Old Dashboard

- Hard refresh: Ctrl+Shift+R
- Clear browser cache or use incognito/private window

Service Management (Linux)

```
# Start / Stop / Restart
sudo systemctl start fortefide
sudo systemctl stop fortefide
sudo systemctl restart fortefide

# Status and logs
sudo systemctl status fortefide
sudo journalctl -u fortefide -f

# Run interactively (debugging)
sudo /opt/fortefide/fortefide
```