ForteFide Quickstart Guide

Get scanning in 5 minutes

Version	1.4.2
Product	ForteFide CMMC L2 Scanner
Platform	Windows & Linux

1. Download & Install

Windows

- Download ForteFide_Setup_1.4.2_Windows.exe from densedefense.com
- Run the installer as Administrator
- Follow the setup wizard (default options are recommended)
- ForteFide installs to C:\Program Files\ForteFide\

Linux (Ubuntu/Debian)

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

- Native ELF binary -- no Python runtime required. Only dependency: libc6 >= 2.28
- Service starts automatically and opens your browser to http://localhost:5000

2. First Launch

Open your browser to http://localhost:5000

The ForteFide dashboard loads automatically. No login required for scanning.

> **Free Tier**
> Without a license, ForteFide operates in the Free tier -- scan all 110 controls with no time limit. Remediation requires a Starter license or above. Evidence collection and scheduled scans require a Professional license or above.

3. The 7-Step Workflow

ForteFide follows a structured 7-step workflow from network discovery through final evidence collection. See the full Quick Start & Evaluation Guide for detailed walkthroughs of each step.

Step	Name	What Happens
1	Network Recon	CIDR discovery -- find and select target hosts
2	Prepare Endpoints	Create service accounts, deploy SSH keys/certs
3	Configure & Execute	Auto-detect prepared hosts, run 110-control scan
4	Baseline Evidence	Auto-collected after scan (signed ZIP)
5	Review, Attest & Override	Review findings, attest 11 manual controls, document exceptions
6	Remediate & Rescan	Batch auto-remediation, then rescan to verify
7	Final Evidence & Teardown	Collect final evidence, remove service accounts

4. Authentication Options

Step 2 offers three authentication methods for endpoint preparation:

Method	Use Case	Step 3 Behavior
Password	Standard username/password	Enter credentials manually
SSH Key (Recommended)	Auto-generated Ed25519 keypair	Zero credentials needed
Certificate	PKI/certificate-based auth	Zero credentials needed

Recommendation
Use SSH Key or Certificate auth. Admin credentials are entered once during preparation and never again. All subsequent scanning and remediation uses the deployed keys automatically.

5. Activate a License

- Drag and drop your .key file onto the license panel in the lower-left sidebar
- Or click "Manage License" and use the file import dialog
- License verification is fully offline -- no phone-home or network calls
- Without a license, scanning works but remediation and evidence are locked

6. Next Steps

- Read the Quick Start & Evaluation Guide for full 7-step walkthroughs
- Read the Administration Guide for advanced configuration
- Review the API Reference for automation and integration
- Set up HallMonitor scheduled scans for continuous monitoring