ForteFide

Linux Installation Guide

Version	1.4.2
Platform	Ubuntu 20.04+, Debian 10+, RHEL 8+
Package	ForteFide_Setup_1.4.2_linux.deb
Binary	Native ELF (Nuitka-compiled). No Python required.
Size	~87 MB (self-contained, air-gap ready)

1. System Requirements

Component	Requirement
Operating System	Ubuntu 20.04+, Debian 10+, RHEL 8+ (or compatible derivative)
Architecture	x86_64 (amd64)
RAM	512 MB minimum (1 GB recommended for large scans)
Disk	200 MB for installation + space for scan data
Runtime	None -- native ELF binary, no Python or pip required
Dependencies	libc6 >= 2.28 (standard on all supported OS)
Network	Not required. Fully self-contained and air-gap ready.
Privileges	Root or sudo access for installation

2. Installation

Transfer the .deb package

Copy ForteFide_Setup_1.4.2_linux.deb to the target system via USB drive, SCP, or any secure transfer method.

```
scp ForteFide_Setup_1.4.2_linux.deb user@target:/tmp/
```

Install

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

The package has no dependencies beyond libc6. If dpkg reports missing dependencies, resolve with:

```
sudo apt-get install -f
```

What happens during installation

- Native ELF binary and templates installed to /opt/fortefide/
- Systemd service (fortefide.service) installed with LimitSTACK=infinity
- CLI launcher installed at /usr/local/bin/fortefide
- Keys directory created at /opt/fortefide/keys/
- Runtime data directory created at /var/lib/fortefide/ (chmod 755)
- Service starts automatically after install
- Browser opens automatically (Chrome > Chromium > xdg-open, as desktop user)

3. Accessing the Dashboard

After installation, the ForteFide dashboard is immediately available at:

http://<server-ip>:5000

The dashboard binds to 0.0.0.0:5000 by default. If accessing from the same machine, use http://localhost:5000.

4. The 7-Step Workflow

ForteFide guides you through a structured 7-step compliance workflow:

Step	Name	Description
1	Discovery	CIDR network scan to find endpoints
2	Prepare	Deploy SSH keys or certificates to targets
3	Scan Config	Configure credentials (if not using key auth)
4	Baseline Evidence	Auto-collect evidence after initial scan
5	Review & Attest	Review findings, attest controls, set overrides
6	Remediate & Rescan	Fix findings and verify with rescan
7	Final Evidence	Collect final evidence package and teardown

The dashboard tracks your progress through each step. Session state persists across browser refreshes and service restarts.

5. License Activation

ForteFide scanning works without a license (Scanner Only mode). To unlock Pro features (remediation, evidence packages, scheduling), import a license key:

- Drag and drop the .key file onto the license panel in the dashboard
- Or use the API: base64 license.key | curl -X POST -d @- http://localhost:5000/api/import-license

License file location after import: /var/lib/fortefide/license.key

Tier	Scanning	Remediation	Evidence	Scheduling
Scanner Only	All 110 controls	No	No	No
Pro	All 110 controls	Yes	Yes	Yes
Trial (10-day)	All 110 controls	Yes	Yes	Yes

6. Authentication Options

ForteFide supports three authentication methods for connecting to target endpoints. Key-based auth is the default and recommended method.

Method	Setup	Recommended For
SSH Key (default)	Step 2 deploys keys automatically	All environments
Certificate	Step 2 deploys certs automatically	High-security / PKI environments
Password	Enter in Step 3 scan config	Legacy / quick evaluation

When using key or certificate auth, admin credentials are entered once during Step 2 (Prepare). All subsequent scanning and remediation uses the deployed credentials automatically -- no passwords on the wire.

7. Service Management

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

# Check status
sudo systemctl status fortefide

# View logs
sudo journalctl -u fortefide -f

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

8. Firewall Configuration

Port	Direction	Purpose
5000/tcp	Inbound	ForteFide web dashboard
22/tcp	Outbound	SSH to Linux targets
5985/tcp	Outbound	WinRM to Windows targets

UFW (Ubuntu/Debian)

```
sudo ufw allow 5000/tcp
```

firewalld (RHEL/CentOS)

```
sudo firewall-cmd --add-port=5000/tcp --permanent
sudo firewall-cmd --reload
```

9. Installed File Locations

Path	Contents
/opt/fortefide/fortefide	Main ELF executable (Nuitka-compiled)
/opt/fortefide/templates/	Web dashboard HTML/CSS/JS
/opt/fortefide/keys/	Generated SSH keys and certificates
/var/lib/fortefide/	Runtime data, scan results, license
/var/lib/fortefide/license.key	License file (after import)
/usr/lib/systemd/system/fortefide.service	Systemd service unit
/usr/local/bin/fortefide	CLI launcher

10. Uninstall

Remove (keeps data and license)

```
sudo dpkg --remove fortefide-scanner
```

Purge (removes everything)

```
sudo dpkg --purge fortefide-scanner
```

Purging removes /opt/fortefide/, /var/lib/fortefide/, and the systemd service. Back up /var/lib/fortefide/license.key before purging if you plan to reinstall.

11. Troubleshooting

Service fails to start

- Check logs: sudo journalctl -u fortefide -e
- Verify binary exists: ls -la /opt/fortefide/fortefide
- Verify LimitSTACK=infinity in fortefide.service (required for Nuitka ELF)

Port 5000 already in use

- Check: sudo ss -tlnp | grep 5000
- Kill conflicting process or change ForteFide port

Browser does not open after install

- Manual access: http://localhost:5000
- Auto-open requires a desktop session (X11/Wayland)

Reinstall

```
sudo dpkg --purge fortefide-scanner
sudo dpkg -i ForteFide_Setup_1.4.2_linux.deb
```