



NetFortress

Dashboard User Manual

Every page explained in plain English

Version 3.1 - September 2026

Contents

1. Getting started
2. Dashboard
3. Devices
4. Device blocking
5. Web Control
6. Firewall
7. Security modules
8. Users, groups and permissions
9. Network
10. Operations
11. Reports
12. Licensing
13. Audit log
14. Safety rails (quick reference)

1. Getting started

Opening the dashboard for the first time, the setup wizard, and how the safety design works.

Sign in

Open the dashboard in a browser (for example <http://192.168.50.2/> - the Operations page lets you move it to another port later). The first account you create is the administrator. Sessions last 8 hours; the Log out button always asks first so a stray tap never signs you out. If a session does end while you work, sign back in and you return to the page you were on.

The setup wizard (5 steps)

The wizard runs once per appliance. It walks through: architecture (how the appliance sits in your network - two-NIC routed gateway, transparent bridge, or one-NIC VLAN trunk), adapters (which network card faces the internet and which faces your devices), the client network and DHCP range, and activation.

The golden rule: nothing risky is ever applied silently. The final step shows an activation phrase you must type exactly. The new configuration goes live with a countdown - if you do not confirm that everything works before the countdown ends, the previous configuration restores itself automatically.

2. Dashboard

Live status at a glance: is the firewall enforcing, is DNS protecting clients, what happened recently.

The dashboard shows protection cards with honest state colours: green (up) means enforced, amber (partial) means some of it is active, red (down) means it is off or not working. Clicking a card drills into the matching page. Recent devices, event counts and licence state are shown as metrics. The dashboard never hides a problem - a failed service shows as failed.

3. Devices

Every client the appliance has seen, with one-click blocking.

The Devices page lists observed client devices with hostname, IP address, MAC address, interface and state. States come from live observation, not guesswork: **Online** means the appliance just verified the device, **Recently seen** means it was talking moments ago or has gone quiet but is still in the network tables, and **Offline** means it was seen before but is missing from the latest sweep - switched off or left the network. A device that disappears is marked offline at the next scan; nothing keeps showing as online after it is gone.

- **Block button** - blocks that device by every identity it has (name, IP and MAC together), so a new DHCP address does not sneak past it.
- **Unblock** - removes the blocking rules and restores access.
- **Search** - filter by any part of the hostname, IP or MAC.

Blocking a device compiles into the guarded firewall flow: the rule appears in the next candidate and goes live only through the apply-and-confirm steps.

4. Device blocking

Blocking rules, device groups, group members, and time-based schedules.

Blocking rules

A blocking rule stops one client from reaching the network. Create one with New blocking rule and choose:

- **Rule name** - what you will recognise later, e.g. 'Block office laptop'.
- **Target type** - MAC address, IP address, hostname, or a device group.
- **Target value** - the address or hostname, or the group selector.
- **Reason** - stored with the rule and shown in the audit log.
- **Schedule** - Always, or one of your time windows.

Device groups and members

A device group applies one rule to many identities - useful for 'guests', 'printers' or 'the warehouse PCs'. Type a name and Add group, then add members (MACs, IPs or hostnames) to it. Create a blocking rule with Target type: Device group and the whole group is blocked together. Remove a member and it stops being covered by the group's rules.

Time-based schedules

A schedule is a named time window, for example 'Evening block' from 20:00 to 22:00 in your chosen time zone. A blocking rule with a schedule only applies inside that window - the same rule can be harmless by day and enforced by night. Schedules are listed with their windows so you can double-check them at a glance.

5. Web Control

Site and application blocking: category groups, services, DNS enforcement, blocklists, the block page, proxy and the policy portal.

Category and application groups

Categories are cards - Social media, Ads, Streaming and so on. Click a card to open it and see every service inside (Facebook, Instagram, TikTok...), the feed covering it, and any custom domains you added. The card's switch blocks or unblocks the whole group; inside, each service has its own tick - untick Facebook and Facebook alone stays reachable while the rest of the group stays blocked.

Related domains: services often sit on shared infrastructure - threads.com uses the same static.cdninstagram.com addresses as Instagram. The domain scan finds every related address before a service is added, so a 'blocked' brand is really blocked, not just its front door. You can extend an existing service with more domains at any time.

Custom domains and blocklists

Add any single domain with Block or Allow override. Blocklists download curated feeds (StevenBlack and category feeds), validate them and stage them safely - a broken feed never takes enforcement down; the last good list keeps running.

DNS enforcement and resolver

The compiled domain set is served by the local resolver. Apply DNS now pushes it live; the status row shows whether enforcement is active and how many domains are compiled. The resolver form sets upstream servers, whether blocked names go to the block page or NXDOMAIN, and DNSSEC validation.

Block page

Three ways to serve it, in priority order: (1) forward blocked visits to your own URL, (2) upload your own HTML design, or (3) use the generated branded page (logo, colours, contact, policy link). With Allow access requests on, the page shows a request form - submissions land in Reports → Access requests, and approving creates the allow rule automatically.

HTTPS sites: browsers encrypt traffic before any page can be shown, so the appliance serves the branded page over its own HTTPS with an appliance certificate. Show the branded block page on HTTPS sites too requires the client to trust the appliance certificate - once installed, blocked HTTPS sites show the branded page instead of a browser error.

Web proxy and cache

Optional explicit proxy with disk and memory caching. Enable it, set the listen port and cache sizes. HTTPS inspection stays off until a managed certificate authority is provisioned.

Policy acceptance (new devices)

When on, every new device must open a web page, read your policy and press accept before it gets internet. On acceptance the device can also install the network certificate. The Accepted devices list shows who accepted and lets you revoke - a revoked device must accept again.

6. Firewall

Live traffic rules in three guarded steps - a mistake can never lock you out.

The Firewall page sets the basics: which adapter reaches the internet (WAN), which reaches your devices (LAN), your client IP range, the trusted management networks (only these may open the dashboard and SSH), NAT sharing, and the automatic-undo countdown length.

1. Preview - press '1 · Check my changes'. The firewall builds the rules and checks them with the kernel. Nothing changes yet.

2. Apply with a safety timer - the new rules go live and a countdown arms. If it runs out, the previous rules return automatically.

3. Confirm - test internet and this dashboard from a client. Works? Press 'Keep these changes'. Doesn't? Press 'Undo now' - or just wait.

7. Security modules

Protection layers you switch on - with the plain-English truth about each one.

Each card is one protection layer: stateful firewall, NAT, anti-spoofing, port-scan quarantine, rate limiting, logging, MAC filtering, DNS enforcement, web filtering, IDS/IPS and more. Every card says what it does - press 'What does this do?' - and its honesty label:

Label	Meaning
Automatic	Protects traffic as soon as it is on
Configured	On, but does nothing until you add rules in the Network section
Needs software	Install it from the card (for example the Suricata IDS/IPS engine)
Planned	Announced capability, not wired to live traffic yet

Recommended resources

A module that wants more than this appliance has shows a warning on its card with the recommended resources - for example IDS/IPS recommends at least 4 GB of RAM and 2 CPU cores. You can still switch it on after acknowledging the warning, but expect a slower appliance. The recommendation appears only when the appliance falls short; a well-sized appliance shows nothing.

GeoIP country policy

The GeoIP country policy panel sits below the module cards, but only while the GeoIP module is switched on. Switch the module off and the panel disappears with it. Switch it back on and your saved country policy is exactly where you left it. In allow-list mode only the chosen countries may connect in; in block-list mode the chosen ones may not.

IDS/IPS (Suricata)

Install the engine from the card. It inspects client traffic inline (NFQUEUE with queue-bypass: if the engine stops, traffic keeps flowing - inspection never becomes an outage). The ET Open signature feed (tens of thousands of rules, updated daily by Proofpoint) is downloaded, validated with the engine's own config test BEFORE touching live traffic, then applied - a rejected ruleset restores the previous one automatically. Alerts appear in Security reports within a minute.

8. Users, groups and permissions

Who can sign in, and exactly what each account may do.

How it works

Every account belongs to one group; a group is a named set of permissions. When an account signs in, the firewall grants exactly what its group allows - and changing a group changes what every member can do on their very next click, no re-login needed.

The 11 permissions

- **Full access** - everything, including user and system management.
- **Dashboard** - the live status page.
- **Devices** - view and block connected devices.
- **Web control** - sites, groups and feeds.
- **Access requests** - review client unblock requests.
- **Reports** - security reports and events.
- **Network** - adapters, DHCP, objects.
- **Firewall** - guarded rule changes.
- **Modules** - security modules.
- **Operations** - backup, restore and updates.
- **Users** - accounts, groups and API tokens.

Built-in groups

Group	Permissions
Administrators	Full access. Can never lose full access; the last enabled administrator cannot be disabled, deleted or demoted.
Operators	Dashboard, devices, web control, access requests, reports, modules, operations - everything except network, firewall and user management.
Viewers	Dashboard and reports, read-only.

Your own groups

New group → name it, tick the permissions, save. Edit permissions any time. A group cannot be deleted while a member is still in it - move them first. On the Accounts panel, each row has a group dropdown (moves the account instantly), Enable/Disable and Delete.

API tokens

Bearer tokens for integrations - scoped, expiring, revocable. The secret is shown once at creation. A token never gets more access than the account that created it.

9. Network

Adapters and roles, IP pools, DHCP and service objects.

Adapters

Each adapter gets a role: the internet side (WAN) takes its address from your router; the client side (LAN) keeps a fixed address so the appliance can serve DHCP and DNS. You can rename adapters (the name appears everywhere, including the setup wizard) and switch between static and DHCP addressing per adapter.

IP pools - more client networks

Each pool is an extra client network (a guest or IoT range). The appliance automatically creates a virtual adapter for it on the LAN adapter, serves DHCP there, and filters it exactly like the main network.

Kea DHCP

The DHCP service hands client addresses. The interface field is locked to the LAN adapter you assigned in Adapters - it cannot drift to another network by accident. Set the pool range, router and lease time here.

Network service objects

Reusable named objects (hosts, networks, services) that rules can refer to, so a change to the object updates every rule that uses it.

10. Operations

Backup, updates, restore, public certificates and the admin port.

Back up and update (one click)

One button saves a timestamped configuration backup on the appliance (downloadable via the link) and reports any pending signed update packages.

Restore configuration

Upload a backup archive; it is validated and staged, then applied only after you type the restore confirmation phrase - the same guarded flow as every risky change.

Public TLS certificate

Real Let's Encrypt certificates via Cloudflare DNS - padlocked HTTPS for the dashboard and block page with no client-side installs. Enter your Cloudflare zone and an API token with Zone/DNS/Edit permission, request the certificate, and the appliance renews it.

Admin page port

Choose the TCP port the admin dashboard answers on (default 80). Reserved ports belong to appliance services: 22, 53, 67, 68, 443, 3128, 8080, 8420. On apply: the firewall is re-applied first so the new port is reachable from your networks, then the web server switches - the current page keeps answering until the very last step, and you are redirected to the new address. Client pages (block page, portal) never move.

11. Reports

What was blocked, what was requested, and the decision trail.

Overview and events

Counts for events, blocked traffic and configured sources. Recent security events shows the last 10 by default - press 'View all (100 events)' for the full list and 'Show last 10 only' to collapse it. Export CSV downloads everything for external analysis. Top categories and destinations show where blocking pressure comes from.

Access requests

When the block page allows requests, each submission appears here with the client's IP - the panel refreshes automatically every 10 seconds. Approve asks how long: 1 hour, 4 hours, 8 hours, 24 hours, 3 days, 7 days, 30 days, or Permanent - until you remove it. Approving can auto-create the allow rule; the decision, duration and note are audited. Clear reviewed removes approved/denied entries while pending ones stay.

12. Licensing

Editions, activation (online and offline), the trial, and what happens when a licence lapses.

What the licence banner shows

The top of the dashboard shows your edition, the licence state, days left and device/account usage. Two ways to activate: paste the purchased key (FA-XXXXX-...) or upload the offline licence file for sites without internet. The 60-day trial unlocks every Professional feature once per installation.

What is included in what

Edition	Includes	Devices	Accounts
Home Lite	Free — full protection, no reports	10	1
Home	Full protection — no reports	25	1
Essential	+ Reports, audit, backup/restore	50	2
Professional	+ IDS/IPS, HTTPS block page, portal, IP pools, API automation, public TLS	250	unlimited
Corporate	Same as Professional with larger device counts per licence	1000+	unlimited

The free Home Lite licence

When nothing is licensed - the trial was never used, it has expired, or a subscription lapsed - the dashboard offers **Get free Home Lite**. One click asks the licence server for a free perpetual Home Lite licence: full protection, no reports, one dashboard account and up to 10 devices. A still-running trial or a paid licence is never replaced automatically - deactivate it first if you want the free edition. The free licence appears in the licence server's dashboard like any other licence, so it can be audited and, if misused, disabled from there; the appliance picks that up on its next licence check.

The honest firewall

When a subscription expires or a key is suspended, filtering, the block page, the portal and DNS keep protecting the network — nothing silently stops. What locks is configuration: every settings change is refused with a clear message until the licence is renewed. Device and account limits are enforced: accounts past the limit cannot be created, and crossing the device limit raises a visible warning.

13. Audit log

Every configuration and access decision, forever searchable.

The audit log records who did what, when, from where: sign-ins (including failures), rule and policy changes, group and permission edits, port changes, portal acceptances, backups and restores. Use it to answer 'what changed?' after any incident.

14. Safety rails (quick reference)

The guarantees that hold on every page.

Rail	What it guarantees
Activation phrases	Destructive steps (activate, restore) require typing the exact phrase - no accidental confirms.
Rollback timers	Every live change runs with a countdown; not confirmed in time means automatic undo.
Last administrator	The final enabled full-access account cannot be disabled, deleted or demoted.
Port moves	Firewall opens the new port before the page moves; a failed switch rolls the setting back.
Feed failures	A broken blocklist or IDS ruleset never replaces the last good one.
Session	8 hours, logout confirmation, and you return to where you were after re-sign-in.