



SENTRA
DOCUMENTATION

USER GUIDES

SENTRA Network Threat Shield — User Guide

What Internet · NTS does for your home or business, in plain language

For SME and home users and customer staff: what protection you get, signing in, reading the dashboard, why a site is blocked, reports, family and office policies, and how to ask for help.

Version 0.18.0 27 October 2026

Contents

01 Welcome

02 Signing in

03 Reading the dashboard

04 When a site is blocked

05 Threats and reports

06 Family and office policies

07 Getting help

08 FAQ

09 Quick quiz

Welcome

What SENTRA Network Threat Shield does for your home or business, in plain language.

Your internet line is protected by **SENTRA Network Threat Shield — Internet · NTS** for short. It is a small security box (or a virtual one at your provider) that sits between the internet and your network. **Everything** that comes in or goes out passes through it first.

What it does for you

Protection	In plain words
Stops attacks at the door	Known bad addresses, floods of junk traffic and break-in attempts are stopped before they reach your computers, phones and cameras.
Learns what's normal	Its AI learns your usual traffic. When something suddenly floods your line, it blocks the senders within seconds.
Catches break-in attempts	An intrusion-prevention engine recognises thousands of known attacks and malware.
Keeps unwanted sites away	It can block adult, gambling, scam and malware sites — and apps you choose — for everyone, or only for some devices (for example the children's tablets).
Safe search	Google, YouTube, Bing and DuckDuckGo show only safe results, with nothing to set up on each device.
Fair sharing	It can keep video calls smooth while backups and downloads wait their turn.
Reports	Daily, weekly or monthly reports of what was stopped.

What it doesn't do

- It **never reads your messages or web pages**. It sees only the *names* of the sites your devices visit — like the address on an envelope, not the letter inside.
- It blocks **whole sites and apps**, not a single video inside a site you allow. If you need to be sure only certain sites open (for young children), your provider can switch on **approved sites only**.

If something goes wrong

The box is built to protect without getting in the way. In the most common setup — where it sits invisibly in the line — traffic keeps flowing even if its software stops. Every change made to it is undone automatically if it causes a problem. Because all your traffic passes through it, a box that loses power or breaks does interrupt the internet until it is fixed; some business units have a bypass that avoids even that — ask your provider.

In this guide

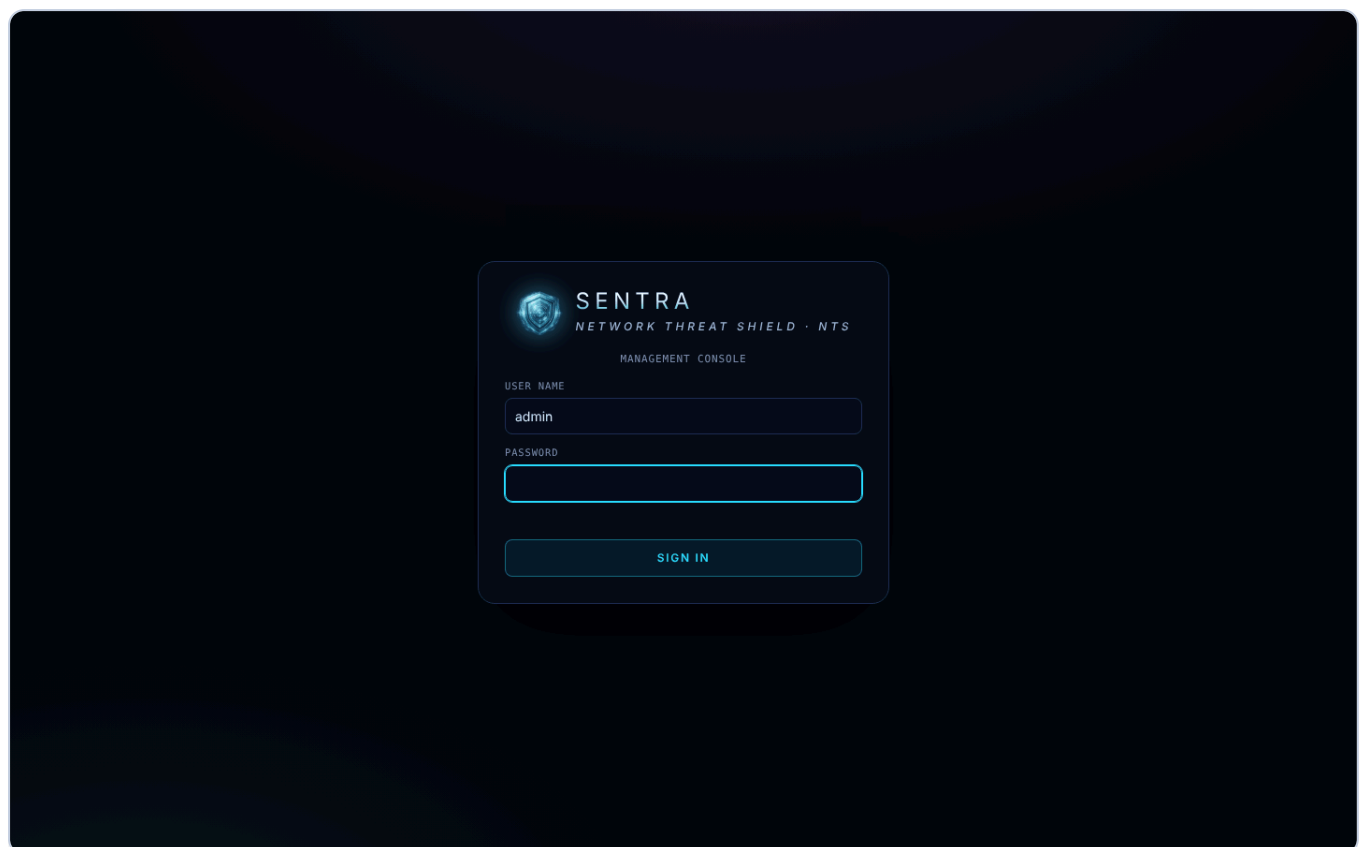
- [Signing in](#) — if your provider gave you an account
- [Reading the dashboard](#)
- [When a site is blocked](#)
- [Threats and reports](#)
- [Family and office policies](#)
- [Getting help](#)
- [FAQ](#) and a short [quiz](#)

Signing in

Opening the NTS console, signing in, setting up two-factor sign-in, changing your password and signing out.

Your provider may give you an account on the NTS console so you can see what is being protected. You need:

- the **console address** — it looks like `https://192.168.1.2:8443` or a name your provider gives you;
- your **user name** and **password**.



The sign-in page.

First time

1. Open the console address in your browser. If the browser warns about the certificate, check the address with your provider before continuing.
2. Type your **user name** and **password** and click **Sign in**.

If your account comes from your provider's SENTRA GUARD, use the same name and password as there.

Two-factor sign-in (recommended)

Two-factor sign-in means a thief needs your phone as well as your password.

1. Click your name at the top right → **Two-factor sign-in** → **Set up with an authenticator app**.
2. Scan the picture with an authenticator app (Google Authenticator, Microsoft Authenticator, 1Password...).
3. Type your password and the 6-digit code the app shows, then **Turn on**.

Next time you sign in, the console asks for the code from your app.

TIP

Lost your phone? Ask your provider to reset your two-factor sign-in. They can do it in a minute.

Change your password

Click your name → type your current password, the new one twice → **Change password**. (If your account comes from a SENTRA GUARD, change it there instead — the window tells you.)

"Too many attempts; wait a minute"

After several wrong passwords the console pauses sign-in from your address for a minute (longer if it keeps happening). Wait and try again carefully, or ask your provider.

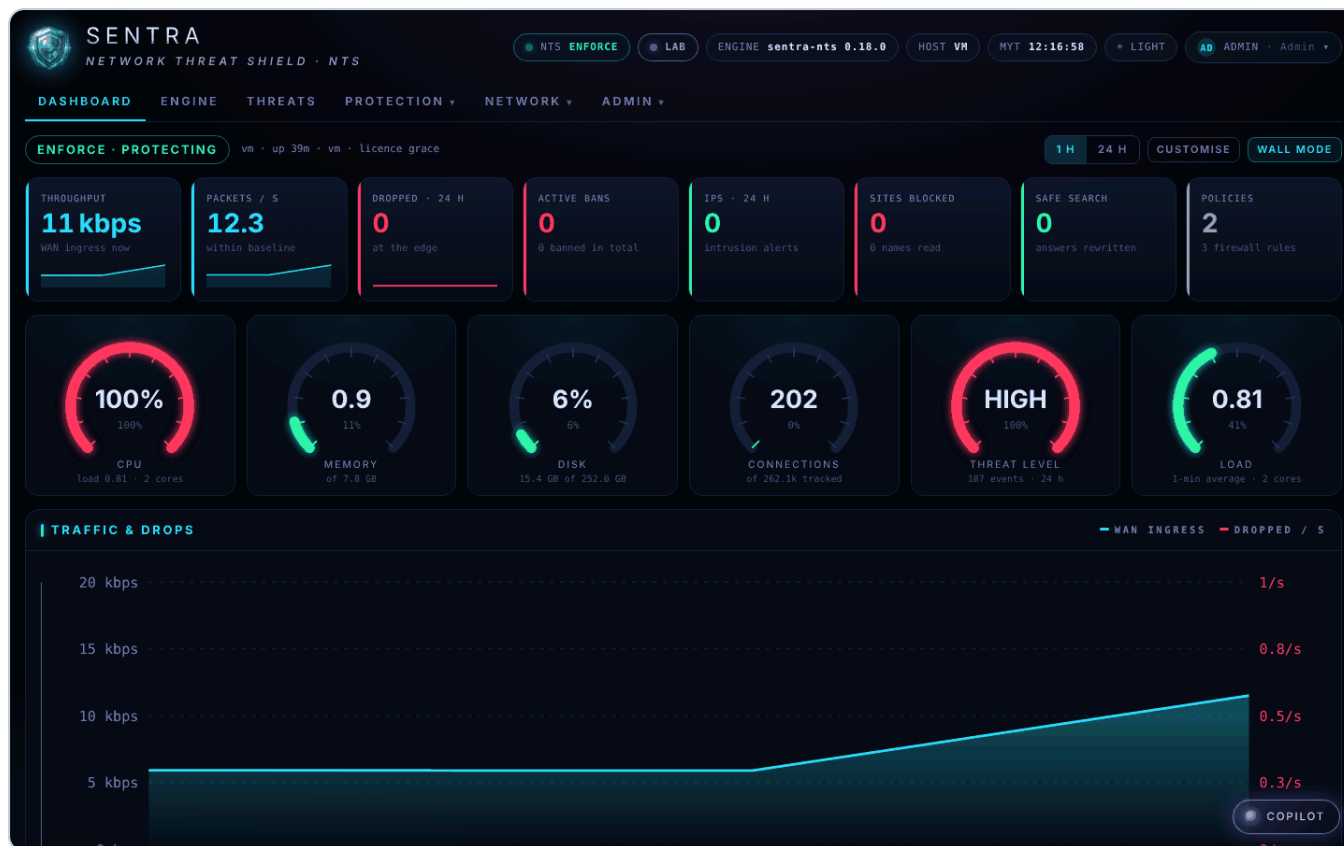
Signing out

Click your name → **Sign out**. You are also signed out automatically after 12 hours.

Reading the dashboard

What the numbers, dials and charts on the NTS dashboard mean, and how to arrange your own view.

After you sign in you see the **dashboard**: a live picture of your internet line.



The dashboard.

The top strip

- **ENFORCE · PROTECTING** (green) — attacks are being stopped. **MONITOR · WATCHING ONLY** means your provider is still watching before switching protection fully on.
- A red **TRAFFIC SPIKE** badge appears while something unusual is flooding the line — the box is dealing with it.
- The licence state and how long the box has been running.

The headline numbers

Tile	Means
Throughput	How much internet traffic is arriving right now
Packets / s	Pieces of traffic per second — <i>within baseline</i> means normal

Title	Means
Dropped · 24 h	Unwanted traffic stopped at the door in the last day
Active bans	Attacking addresses blocked right now
IPS · 24 h	Break-in attempts recognised in the last day
Sites blocked	Websites stopped by your policies
Safe search	Searches made safe
Policies	Internet policies in use and how many firewall rules

The dials

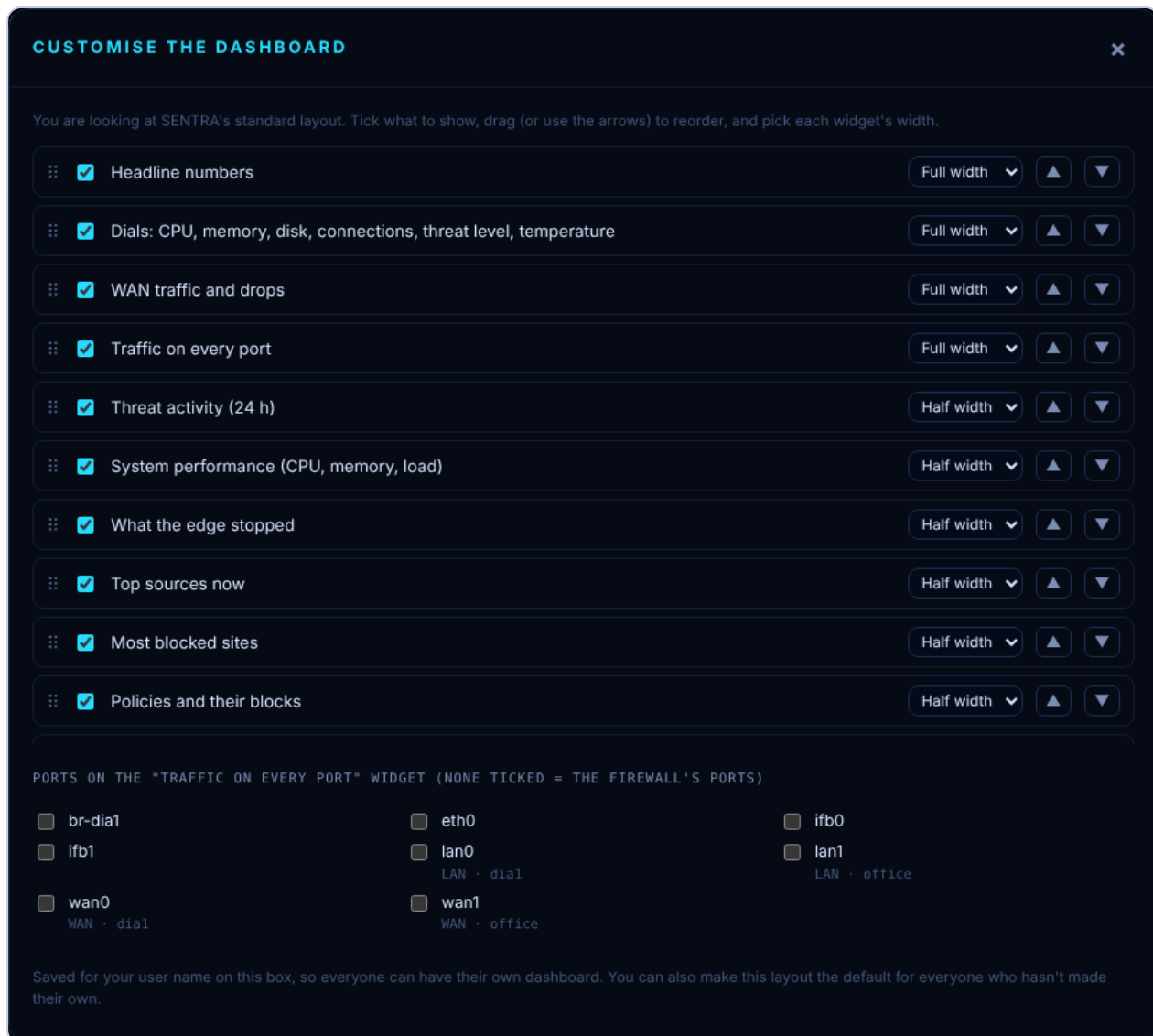
CPU, **memory**, **disk** and **connections** show how busy the box is. **Threat level** is LOW, RAISED or HIGH for the last day. A high value now and then is normal; tell your provider if a dial stays red.

Charts and lists

Further down: traffic over time, traffic on each port (click a port for a bigger graph), threat activity, the sites blocked most, and the newest events. Choose **1 h** or **24 h** at the top right.

Arrange your own dashboard

Click **Customise**:

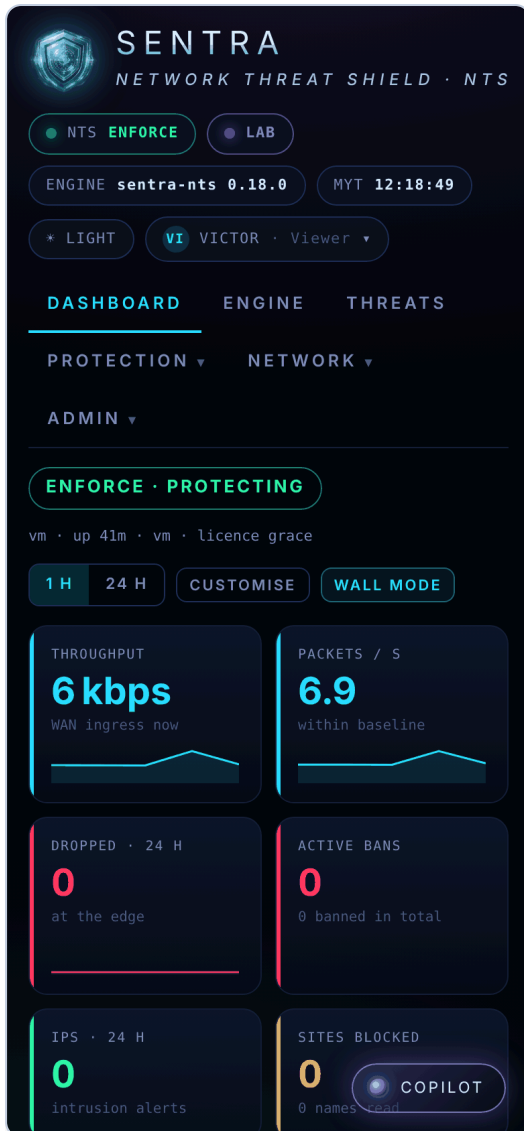


Customise the dashboard.

1. Tick what you want to see.
2. Drag to reorder (or use ▲ ▼).
3. Choose half or full width.
4. **Save.** Your layout is kept for your account, on any browser. **Reset to default** brings back the standard view.

On your phone

The console works on a phone too.



The dashboard on a phone.

Wall mode

Wall mode fills the screen with the dashboard — handy on an office TV. Press **Esc** to leave.

When a site is blocked

What you see when NTS blocks a site or app, why it happened, and how to ask for it to be allowed.

NTS blocks sites and apps by their **name** and never opens your traffic. Because of that, it can't show a "blocked" page inside an encrypted website. Instead your browser or app shows its own error.

What you see

You see	What happened
<i>"This site can't be reached", "Server not found", "DNS_PROBE..."</i>	The name lookup was blocked
<i>"Connection reset", "ERR_CONNECTION_RESET", "The connection was interrupted"</i>	The secure (HTTPS) connection was refused
An app says it can't connect, or keeps loading	The app, or its category, is blocked
Search results look "cleaner" than usual	Safe search is on — explicit results are hidden

Why a site may be blocked

- It is on a **block list** your policy uses (adult, gambling, drugs, scams, malware, piracy...).
- Its **category** is blocked — sometimes decided by the box's AI, which checks sites no list knows yet.
- Your policy allows **approved sites only**, and this site isn't on the approved list yet.
- An **app** rule blocks it (for example games during work hours).
- It is a known attack or malware address.

It's blocked by mistake

Tell your provider (or the person who manages your SENTRA box):

1. the **site name** exactly as you typed it (for example `www.example.com`),
2. the **time** you tried,
3. which **device** you used (the device's network address helps — your provider can find it).

They can test the name, see exactly which list or rule blocked it, and **always allow** it for you if it should open.

NOTE

A site blocked on purpose by your organisation's or family's policy stays blocked until the person responsible for the policy changes it.

Working around the filter

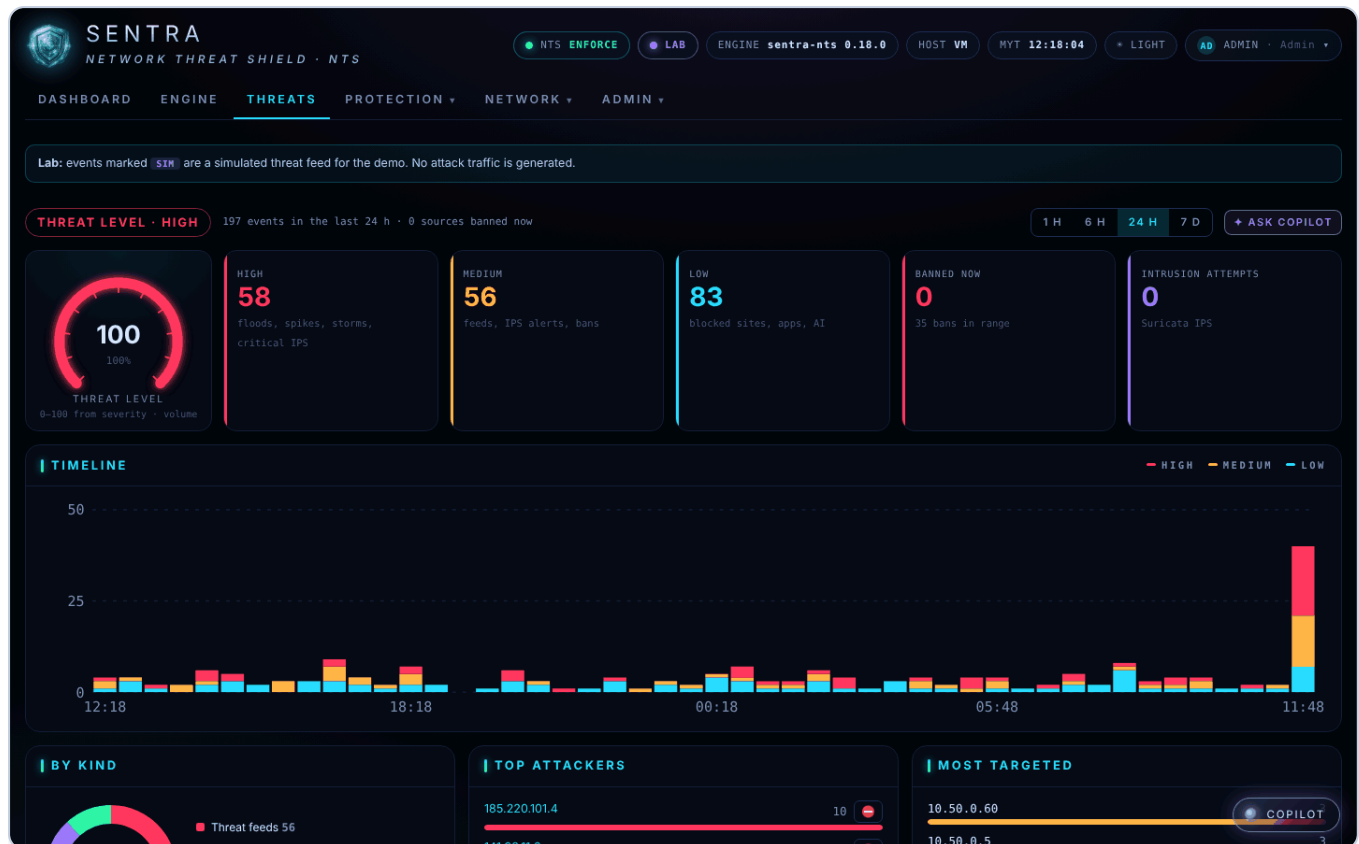
Using a VPN app, a proxy or encrypted DNS to get around the filter is usually blocked too. Ask instead — it is faster.

Threats and reports

Reading the Threats page, the threat level and events, and getting regular reports of what was stopped.

The Threats page

Threats (top menu) shows what NTS stopped or noticed.



The Threats page.

- **Threat level** — LOW, RAISED or HIGH, from how many events happened and how serious they were.
- **High / Medium / Low** — serious events (floods, traffic spikes, critical break-in attempts), medium ones (known bad addresses, break-in alerts, banned senders) and low ones (blocked sites and apps).
- **Timeline** — when things happened. Choose 1 h, 6 h, 24 h or 7 days.
- **Top attackers, Countries, Blocked sites** — where it came from and what was stopped.
- **Events** — every event, newest first. Click one for the details.

NOTE

Seeing attacks on this page is normal and means the box is working: every internet connection is probed all day long. What matters is that they were **stopped**.

Events marked **SIM** appear only on demonstration systems; they are simulated, not real attacks.

Ask Copilot

If your provider has set up an AI model, the **COPILOT** button (bottom right) and **Ask Copilot** on the Threats page answer questions such as *"Is anything attacking us right now?"* in plain language, using the box's own data.

Reports

SENTRA
NETWORK THREAT SHIELD · NTS

NTS ENFORCE LAB ENGINE sentra-nts 0.18.0 HOST VM MYT 12:18:10 * LIGHT AD ADMIN Admin

DASHBOARD ENGINE THREATS PROTECTION NETWORK REPORTS

REPORTS BUILD SAVED & SCHEDULED (0) ARCHIVE (0) AUTOMATIC E-MAIL

TITLE PERIOD
SENTRA NTS report Last 7 days

SECTIONS all none

SECURITY

- ☒ Executive summary
The headline numbers and what stood out
- ☒ Threat activity
Severity, kinds of threat and a timeline
- ☒ Attackers and targets
Top attacking addresses, targets, countries
- ☐ Intrusion prevention
IPS alerts and drops, top signatures
- ☒ Edge drops and bans
Floods, feeds, countries, banned sources
- ☐ AI verdicts
Sites the AI classified and blocked

NETWORK AND PERFORMANCE

- ☒ Traffic per port
In and out per port, internet traffic per hour
- ☒ System performance
CPU, memory, disk, load and connections
- ☐ System health
Link, BGP, HA, storm, error and licence events

USERS AND POLICIES

- ☒ Sites and policies
Sites blocked, who hit them, policies, safe search
- ☐ Applications
Apps seen and blocked

ADMINISTRATION

- ☐ Admin activity
Changes per user and what they did
- ☐ Sign-ins
Successful and failed console sign-ins
- ☒ Change log
Every configuration change, deploy and rollback
- ☐ Configuration snapshot
Segments, policies, rules and protection as they are now

SEGMENT DEVICE OR RANGE (OPTIONAL) THREAT EVENTS
all segments 10.0.0.70 or 10.0.0.64/27 all severities

COPILOT

Every report you make is kept in the Archive, where you can open it again, print it to PDF or download any section as CSV

SAVE AS MAKE REPORT

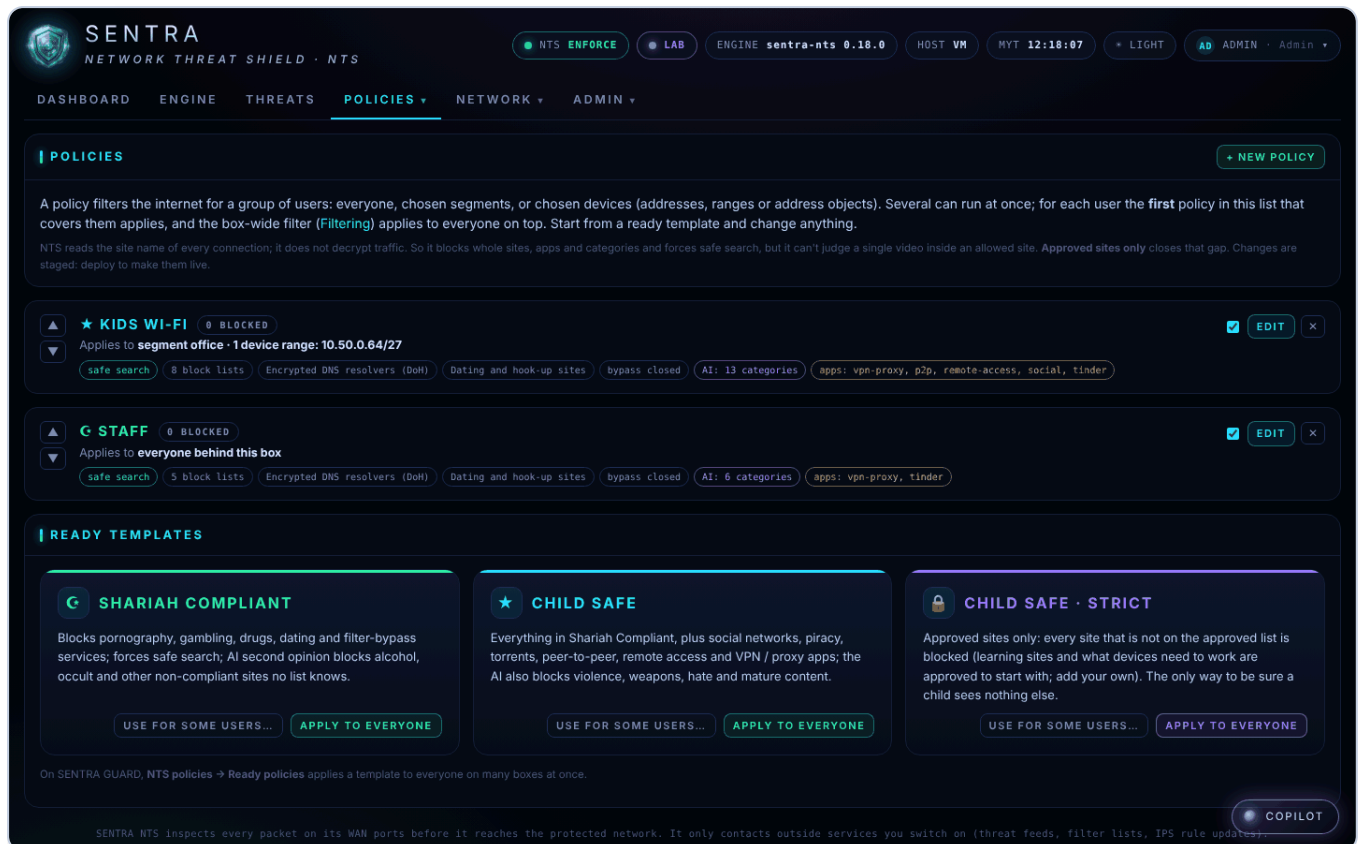
Building a report.

Your provider can send you reports by e-mail — daily, weekly or monthly — with an executive summary, threat activity, what was blocked, traffic and performance. If your account may run reports, open *Admin* → *Reports*, choose a period and the sections you want, and click **Make report**. You can print it to PDF or download the tables as a spreadsheet (CSV).

Family and office policies

The ready-made internet policies — Shariah Compliant, Child Safe and Child Safe strict — and how they can apply to everyone or only to some devices.

A **policy** decides what the people behind your SENTRA box may reach on the internet. Different devices can have different policies: the children's tablets *Child Safe · strict*, the office PCs *Shariah Compliant*, guests something else.



Policies on the NTS console.

The ready-made policies

Policy	Good for	What it blocks
G Shariah Compliant	Families and businesses	Pornography, gambling, drugs, dating, and ways to get around the filter. Forces safe search. The AI also blocks alcohol, occult and other non-compliant sites that no list knows yet
★ Child Safe	Children and teenagers	Everything above, plus social networks, piracy, torrents, peer-to-peer, remote access and VPN apps. The AI also blocks violence, weapons, hate and mature content
🔒 Child Safe · strict	Young children	Approved sites only: everything that isn't on the approved list is blocked. Learning sites (Wikipedia, Khan Academy, Scratch, Duolingo, Britannica, Ministry of Education...) and what devices need to work are approved to start with

Your provider can change any of these: add sites to block, approve more sites, block or allow apps.

Who a policy applies to

A policy can apply to **everyone** behind the box, to one **part of the network** (for example the guest Wi-Fi), or to **chosen devices**. For device policies to follow the right devices, those devices should always get the same network address — your provider or IT person can set that up on the router.

Changing your policy

Ask whoever manages your SENTRA box (your provider, or your IT person if they have an account). Changes take effect within a minute.

Getting help

Who to contact, what to tell them, and what to check before you call.

Who to contact

1. **Your provider** — the company that installed SENTRA for you (your telco, internet provider or IT company). They manage your box and can see its records.
2. If you bought SENTRA **directly**, write to **demo@sentra-ai.com**.

What to tell them

Information	Where to find it
What happened, and when (date and time)	—
The site or app involved, exactly as typed	—
The device (laptop, phone, TV...)	—
The box's name	The HOST pill at the top of the console
The Installation ID (for licence questions)	<i>Admin</i> → <i>Licence & Updates</i> → <i>Licence</i>

Before you call

Problem	Try
No internet at all	Check the cables and that the SENTRA box has power (its lights are on); restart your own router. If the SENTRA box has no power, plug it back in and give it a few minutes to start
One site won't open	See When a site is blocked
Everything is slow	Look at the dashboard: is Throughput at your line's limit? A large download or backup may be using it
Can't sign in	Wait a minute after wrong passwords; ask your provider to reset your password or two-factor sign-in

Your data

SENTRA sees the names of the sites your devices visit and the amount of traffic — never the content of messages or pages. Reports and records stay on the box and with your provider.

FAQ

Quick answers for SME and home users of SENTRA NTS.

Will SENTRA slow my internet down? Your provider chooses a box that matches your line's speed. Fair sharing can even make calls smoother when someone is downloading.

Can SENTRA read my WhatsApp messages or e-mails? No. It sees only the names of the sites and services your devices connect to.

Why do I sometimes see "connection reset" instead of a block page? Because SENTRA never opens your encrypted traffic, it can only refuse the connection. See [When a site is blocked](#).

Does safe search work on every device? Yes, for Google, YouTube, Bing and DuckDuckGo — nothing to set up on the device.

My child uses mobile data, not our Wi-Fi. Is that protected? No. SENTRA protects traffic that goes through your internet line. Mobile data goes through the phone company.

What if the box breaks? In the usual setup it lets traffic through if its software stops. If the box itself loses power or fails, your internet stops until it is fixed or bypassed — tell your provider straight away.

Can I see what was blocked? Yes — on the dashboard and the Threats page, and in reports.

Who can change the rules? Only accounts your provider allows. Every change is recorded with who made it.

Quick quiz

Five questions to check you know how SENTRA NTS protects you.

Check what you learned in this guide.

QUIZ

Check your understanding

5 questions

1. What does SENTRA NTS look at to block a website?

- A The full content of the page
- B **The site's name** ✓ answer
- C Your passwords
- D Your photos

NTS reads only the names of sites and services; it never opens your traffic.

2. You see 'Connection reset' on a site. What is the most likely reason?

- A Your computer has a virus
- B **The site was blocked by your policy** ✓ answer
- C Your line is broken
- D The site is too popular

NTS refuses the secure connection of a blocked site, so the browser shows its own error.

3. Which policy allows approved sites only?

- A Shariah Compliant
- B Child Safe
- C **Child Safe · strict** ✓ answer
- D None of them

Child Safe · strict blocks everything that isn't on the approved list.

4. A site you need is blocked by mistake. What should you do?

- A Install a VPN app
- B **Tell your provider the site name, time and device** ✓ answer
- C Restart the SENTRA box
- D Wait a week

Your provider can see exactly why it was blocked and allow it.

5. The Threats page shows many attacks. Should you worry?

- A Yes, the box has failed

B No — attacks are normal on every connection; what matters is that they were stopped

✓ answer

C Yes, unplug the internet

D Only on Mondays

Every internet connection is probed all day. The page shows the box stopping them.