

NetASX

v3.0

User Manual

Network Analysis Security eXpert
Professional tool for WiFi and Ethernet network analysis and auditing

August 2026
netasx.com · soporte@netasx.com

Table of contents

1. Introduction and system requirements
2. Installation and first launch
3. Login and account management
4. WiFi Scan
5. WiFi Spectrum
6. Configuration and test execution
7. Network Map
8. Network Audit
9. Passive WiFi Audit
10. SSH / Telnet Terminal
11. Site Survey
12. Real-time Monitoring
13. Support
14. PDF report export
15. Frequently asked questions

1. Introduction and system requirements

NetASX v3.0 is a professional desktop tool for analysis, validation and auditing of WiFi and LAN networks. Designed for network technicians and installers, it allows you to perform everything from a quick wireless network scan to a complete Site Survey report with an interactive floor plan.

System requirements

Component	Minimum	Recommended
Operating system	Windows 10 64-bit	Windows 10/11 64-bit
Processor	Intel Core i3	Intel Core i5 or higher
RAM	4 GB	8 GB or more
Storage	500 MB free	1 GB free
WiFi adapter	Windows compatible	Dual-band USB WiFi adapter
Internet connection	Required for activation	Required for support
Dependencies	Npcap (for Audit Phase B)	Npcap pre-installed

Available plans

Plan	Duration	Modules included
Trial	14 days free	Everything except Support — ideal for testing the tool
Silver	Monthly	Scan, Spectrum, Tests, Network Map, SSH/Telnet, PDF
Gold	Monthly	All Silver + Site Survey, Network Audit, Monitoring
Premium	Monthly	All Gold + Support tickets + Remote assistance 3h/month

2. Installation and first launch

NetASX is distributed as a Windows executable file. No installation required — simply download the file and run it.

Installation steps

- Download the NetASX.exe file from netasx.com
 - Save the file in a folder of your choice (e.g. C:\NetASX\)
 - Double-click the file to run it
 - If Windows shows a security warning, click "More info" and then "Run anyway"
 - The application will open directly without any additional installation

IMPORTANT: NetASX requires an internet connection to verify the access key at startup. Make sure you have an active connection before opening the application.

Npcap installation (for Audit Phase B)

Phase B of the Network Audit module requires Npcap for advanced packet capture. If it is not installed, NetASX will automatically show a warning at startup with the official download link.

- Go to <https://npcap.com/#download>
- Download the Npcap installer (free)

- Run the installer and follow the steps
- Check the "WinPcap API compatible mode" option during installation
- Restart the computer if the installer requests it
- Reopen NetASX — Audit Phase B will be available

3. Login and account management

Sign in

When you open NetASX, the access screen appears. Enter your credentials to enter the tool.

- **Username:** Enter your registered username
- **Password:** Enter your password (the eye icon allows you to show or hide it)
- **"Sign in" button:** Access the application
- **"Forgot password":** If you forgot your password, enter your email and you will receive a recovery code

Create a new account

If you are new to NetASX, you can create your account directly from netasx.com:

- Click "Free trial" on the website
- Enter your username, email and password
- You will receive a confirmation email — click the link to activate your account
- Once activated you can sign in with your credentials

***NOTE:** The 14-day trial period is automatically activated when you register. During this period you have access to all modules except Support.*

Profile menu

In the top bar of the application, on the right, you will find the **Profile** menu with your username and active plan. Clicking on it shows the following options:

- **Current plan:** shows your contracted plan
- **User manual:** opens this manual in the browser
- **Change password:** allows you to update your access password
- **Sign out:** closes the current session

Change password

- Click the Profile menu and select "Change password"
- Enter your current password
- Enter the new password (minimum 6 characters)
- Repeat the new password to confirm
- Click "Save"

Device linking

NetASX links your account to a specific device. The first time you sign in on a PC, that computer is registered as your authorized device. If you need to change computers, contact soporte@netasx.com to unlink your device.

4. WiFi Scan

The WiFi Scan module is the starting point for any project. It detects all wireless networks visible from your computer and shows detailed technical information about each one.

How to perform a scan

- Click the **Scan** tab in the top bar
 - Press the "Scan WiFi networks" button to start detection
 - Wait a few seconds — the table will fill with detected networks
 - Click on any column header to sort the results

Information displayed per network

Column	Description
SSID	WiFi network name
BSSID	Access point MAC address
Channel	WiFi channel used (1-13 on 2.4GHz, 36-165 on 5GHz)
Band	Frequency: 2.4 GHz, 5 GHz or 6 GHz
Signal	Signal strength in percentage
Protocol	WiFi generation: WiFi 4, 5, 6, 6E or 7
Security	Encryption type: WPA2, WPA3, WEP, Open
Band Steering	Indicates if the network uses this technology

Selecting networks for testing

- Check the checkbox to the left of each network you want to validate
 - Use "Select all" and "Deselect all" to speed up selection
 - Configured networks are highlighted in blue
 - Once selected, go to the "Configuration" tab to prepare the tests

***NOTE:** Signal quality guide: above 70% is excellent, 40-70% is good, 20-40% is acceptable, below 20% is weak.*

5. WiFi Spectrum

The spectrum analyzer visually shows the distribution of WiFi channels in the environment. It allows you to identify overlap between networks and choose the optimal channel for new access points.

How to use the spectrum analyzer

- First perform a WiFi Scan to detect nearby networks
 - Click the **Spectrum** tab
 - The chart automatically updates with data from the last scan
 - Each network appears represented on its corresponding channel

Spectrum interpretation

- In 2.4 GHz only channels **1**, **6** and **11** do not overlap — always use one of these three
 - In 5 GHz all channels have sufficient separation — any channel is valid
 - If you see many networks on the same channel, that channel is congested — avoid it
 - Look for the channel with the least activity to place your AP

6. Configuration and test execution

Validation tests are performed in two steps: first configure the parameters in the Configuration tab and then run the tests from the Execution tab.

Step 1 — Scan and select networks

Go to the **Scan** tab, perform the scan and check the networks you want to run tests on.

Step 2 — Configure the tests

Go to the **Configuration** tab:

- Enter the **WiFi password** for each selected network — required for NetASX to connect automatically during tests
- If you want to validate **VLANs**, enter the expected subnet (e.g. 192.168.10.0/24) — this allows you to verify that traffic is routed correctly. If there is no VLAN, leave it empty
- You can also access the **AP or router web interface** from this tab to check its configuration
- Click **"Save configuration"** when finished

Step 3 — Run the tests

- Fill in the **"AP / Location"** and **"Firmware"** fields in the top bar — they will appear in the PDF report
 - Go to the **Execution** tab
 - Click **"Run tests"**
 - The real-time log shows the progress of each test as it runs
 - Once finished, export the report in PDF or Excel

Tests performed

Test	Description
DHCP	Verifies that the network correctly assigns IP, mask, gateway and DNS
VLAN	Checks that the assigned IP is in the configured subnet
Gateway Ping	Connectivity and latency with the network router
Internet Ping	Connectivity with the Internet (8.8.8.8 by default)
Speed Test	Real download speed against servers in Europe

7. Network Map

The Network Map module automatically discovers all devices connected to the local network. It shows the IP, MAC address and manufacturer of each device.

Discover devices on the network

- Connect to the WiFi network you want to map
 - Click the **Network Map** tab
 - Click **"Start scan"**
 - NetASX performs a ping sweep of the subnet to detect active devices
 - The table fills with all found devices

Quick SSH or Telnet access from Network Map

- Find the device in the Network Map table
 - Double-click on it to open SSH Client with the IP already filled in automatically
 - Just enter the device username and password and connect

NOTE: Random MACs from mobile devices show the manufacturer as "Private address". This is normal on devices with iOS 14+ or Android 10+.

8. Network Audit

The Audit module analyzes network security by detecting real threats. It is divided into two phases plus a new passive audit feature.

Phase A — Connected audit (available without Npcap)

Connect to the network you want to audit and run the analysis:

- Go to **Network Audit** → **Phase A**
- Select the interface (WiFi or Ethernet)
- Click "Start Phase A audit"
- Wait between 30 and 60 seconds
- Review the results — each finding shows its risk level and recommendation
- Export the PDF report to deliver to the client

Threat detected	Description	Risk
ARP Spoofing	Man-in-the-middle attack that intercepts local traffic	HIGH
Evil Twin	Fake AP impersonating the SSID of a legitimate network	HIGH
Rogue AP	Unauthorized access point on the network	HIGH
Open networks	Networks without encryption where traffic is visible	MEDIUM
Weak encryption (WEP)	WEP is vulnerable and can be easily cracked	HIGH

Phase B — Advanced audit (requires Npcap)

Phase B extends the audit with real-time packet capture and analysis capabilities.

Port Scan: scans the ports of one or more devices to detect exposed services. Enter IPs separated by commas or receive them automatically from Network Map. Export the PDF report with open ports found.

Packet Capture: captures network traffic in real time showing protocol, IPs, MACs and description of each packet. Supports ARP, DNS, DHCP, ICMP, IGMP, mDNS, SSDP, HTTP, HTTPS, SNMP and more. Export the capture in .pcap format to analyze with Wireshark.

9. Passive WiFi Audit

The most powerful feature for the professional technician. Analyzes the WiFi environment without needing to connect to any network or enter any password. Detects threats simply by scanning the surrounding networks.

What it detects

- **Open networks** — no encryption, anyone can connect and see traffic
 - **WEP networks** — obsolete protocol cracked in minutes
 - **Evil Twin** — two APs with the same name but different security
 - **Rogue APs** — multiple suspicious APs with the same SSID
 - **Suspicious SSIDs** — names suggesting trap networks or malicious devices
 - **Channel interference** — congested channels in 2.4 GHz
 - **Anomalous signals** — devices with excessively high signal that may indicate a nearby intruder AP

How to use the Passive Audit

- Go to the **Scan** tab and click "Scan WiFi networks" — no need to connect to any network
 - Go to **Network Audit** → **Passive WiFi Audit**
 - Click "**Start passive audit**"
 - In seconds you will see results organized by risk level with recommendations
 - Use the "**Clear**" button to delete results and start again
 - Export the PDF report

10. SSH / Telnet Terminal

SSH and Telnet client integrated directly into NetASX. Allows you to connect remotely to routers, switches, APs and any network device without the need for external tools.

Connecting to a device

- Go to the **SSH Client** tab
 - Select the protocol: SSH (port 22) or Telnet (port 23)
 - Enter the device IP or hostname
 - Check the port (22 by default for SSH, 23 for Telnet)
 - Enter the device username and password
 - Click "Connect" or press Enter in the password field
 - Once connected, type commands directly in the terminal

The first time you connect to a new server, NetASX automatically verifies its identity without needing any confirmation.

Quick commands

Button	Command sent	Typical use
show ip	show ip int brief	View interfaces on Cisco routers
ifconfig	ifconfig	View interfaces on Linux/Unix
ls	ls -la	List files on Linux
exit	exit	Close session on the device

QUICK ACCESS: Double-click on any device in the Network Map and the IP is automatically filled in the SSH terminal.

11. Site Survey

The Site Survey is the most complete tool in NetASX. It allows you to draw or import a floor plan, place network devices and generate a professional report for the client.

Starting a Site Survey

- **Import floor plan:** Load a JPG/PNG image of the building floor plan as the canvas background
 - **Draw floor plan:** Use drawing tools to trace walls manually
 - **Empty canvas:** Place devices directly without a background floor plan

Drawing tools

Tool	Function
Move	Select and move elements on the canvas
Pencil	Draw freehand lines
Wall	Draw straight walls with configurable material
Zone	Draw rectangles to mark rooms or areas
Arrow	Add directional arrows with interactive rotation
Text	Add text labels (double-click to edit)
Erase	Delete elements from the canvas

Wall materials and WiFi attenuation

Material	Typical attenuation	Typical use
Glass	2 - 3 dB	Windows, partitions, glass doors
Wood	5 - 12 dB	Wooden doors, partitions, furniture
Brick	12 - 15 dB	Standard brick walls
Concrete	20 - 30 dB	Reinforced concrete walls, slabs
Metal	20 - 40 dB	Metal doors, elevators, structures

Adding devices to the floor plan

- In the left panel select the device type (AP, Switch, Router, etc.)
 - Click the device button — it will appear in the center of the canvas
 - Drag it to the correct position on the floor plan
 - Double-click on the device to edit name, IP, channel and notes

***TIP:** Use **Ctrl+Z** to undo and **Ctrl+Y** to redo any action. Save the floor plan frequently with the "Save" button.*

12. Real-time Monitoring

The Monitoring module continuously supervises the network status and launches alerts at any anomaly. Ideal for leaving a site monitored for hours and reviewing the report at the end.

Starting monitoring

- Select the interface type: WiFi or Ethernet

- Set the check interval: 30 sec, 1, 2, 5 or 10 minutes
- Optionally enter critical IPs separated by commas to monitor specifically
- Click "Start monitoring"

Status indicators

Indicator	Information shown when clicked
Gateway	Router IP, MAC address, manufacturer and exact latency in ms
Internet	Latency to Google DNS (8.8.8.8) and Cloudflare (1.1.1.1)
WiFi Signal	Network name (SSID) and signal strength percentage
Devices	Full table with IP, MAC and manufacturer of each device
Speed	History of all speed measurements taken

Alert levels

Level	Color	Meaning
INFO	Blue	General network status information
WARNING	Orange	Situation to watch but not critical
CRITICAL	Red	Serious problem requiring immediate attention
RECOVERY	Green	A previous problem has been resolved

13. Support

The Support module is available for clients with Gold and Premium plans. It allows you to open support tickets directly from the tool.

Creating a support ticket

- Go to the **Support** tab
 - Click "+ New ticket"
 - Enter the issue subject
 - Write a detailed description
 - Click "Send ticket"
 - You will receive a response within 24 hours

Ticket statuses

Status	Meaning
New	Ticket received, pending assignment to technical team
In progress	A technician is working on your case
Answered	The technician has sent a response — review it
Closed	The problem has been resolved

Remote assistance (Premium only)

The Premium plan includes 3 monthly hours of remote assistance. A NetASX technician will connect to your computer to resolve the problem directly. Sessions are coordinated through the ticket system.

Upgrade your plan

Click "**View plans**" in the Support tab to see available options and subscribe directly.

14. PDF report export

All NetASX modules include export to a professional A4 PDF report, ready to print or send to the client.

Module	PDF report contents
Test execution	Results per network, latency, speed, packet loss, VLANs
Network Audit	Detected threats, risk level and security recommendations
Passive WiFi Audit	Environmental threats, open networks, congested channels
Port Scan	Open ports per device with service and category
Site Survey	Device summary, channel analysis and recommendations
Monitoring	Alert log, incident summary and network status

How to export a report

- Complete the work in the corresponding module
 - Click the "Export PDF" button of the module
 - Select the folder and file name
 - Click "Save" — the PDF is generated automatically

15. Frequently asked questions

Q: The application does not detect WiFi networks, what should I do?

A: Make sure your WiFi adapter is active and not in airplane mode. On some computers it is necessary to run NetASX as administrator.

Q: I cannot see Audit Phase B

A: Phase B requires Npcap installed and a Gold or Premium plan. Download Npcap from npcap.com and install it checking the "WinPcap API compatible mode" option.

Q: My account says "unauthorized device"

A: Your account is linked to another computer. Contact soporte@netasx.com to unlink your device.

Q: How do I recover my password if I forgot it?

A: On the access screen click "Forgot password". Enter your email and you will receive a recovery code.

Q: Site Survey does not save my floor plan

A: Use the "Save" button to save the floor plan. Choose a location where you have write permissions such as the Desktop.

Q: Monitoring shows N/A for WiFi signal

A: This happens when you are connected via Ethernet. Change the interface selector to "Ethernet".

Q: Can I use NetASX on Mac or Linux?

A: NetASX is currently available only for Windows 10/11 64-bit. Support for other systems is on the roadmap for future versions.

Q: How do I contact support if I don't have a Gold or Premium plan?

A: Visit netasx.com or write to us at soporte@netasx.com. You can also use the WhatsApp chat available on the website.

