I N S T A L L A T I O N G U I D E

Sat>IP anywhere

This guide describes how to install the Windows server software and connect Android clients (phone, tablet, Android TV, Fire TV). The server app transcodes SAT>IP or DVB-C over IP and serves the programme on your home network and, with HTTPS, away from home as well.

New	1. A first start no longer needs repeated restarts. If SSL is configured, control and the video stream use the same HTTPS port. The HTTP port remains for local use only (Android TV, for example). 2. M3U files can now be created by the app itself, via a transponder scan. 3. The server now detects brute-force attacks.

1 Requirements

- Windows 10 or 11, 64-bit. A SAT>IP server, or a DVB-C device with an IP interface, on the same LAN.
- A fixed IP for the SAT>IP device, or a DHCP reservation in the router. The server app remembers the address it found.
- For access from outside: a DynDNS name in the router and UPnP, or a manual port forward.
- The Android app from the Play Store. iOS and tvOS are still in beta.

2 Install the server

Download and readme are at https://sat-ip-anywhere.com/Download.

Portable / ZIP

- Download the archive and extract it to a folder, for example C:\satipanywhere. A privileged directory is not required, but it is allowed. No administrator rights are needed to run the setup.
- Start the exe. On first start the app creates settings.json and walks you through UPnP, ports and credentials.

Microsoft Store

The Store version installs to Program Files\WegeApps\anywhere. Configuration and the certificate are stored in the user profile (AppData), not next to the EXE. Autostart is configured automatically (remove it if needed: Start, Settings, Apps, sat-ip-anywhere-server, off) and applies only to the account that installed it.

On a few PCs the app is not allowed to bind the HTTPS port itself. In that case run the included script run-after-first-start-for-ssl.bat once and confirm the administrator prompt. That is the exception, not the normal first start.

3 Prepare the router

Automatic port management via UPnP is recommended. The app then opens the HTTPS port, or the HTTP stream ports (legacy, easier on the battery for mobile devices), and closes them again when it exits. The PC must first be allowed to open and close ports in the router. On a FRITZ!Box:

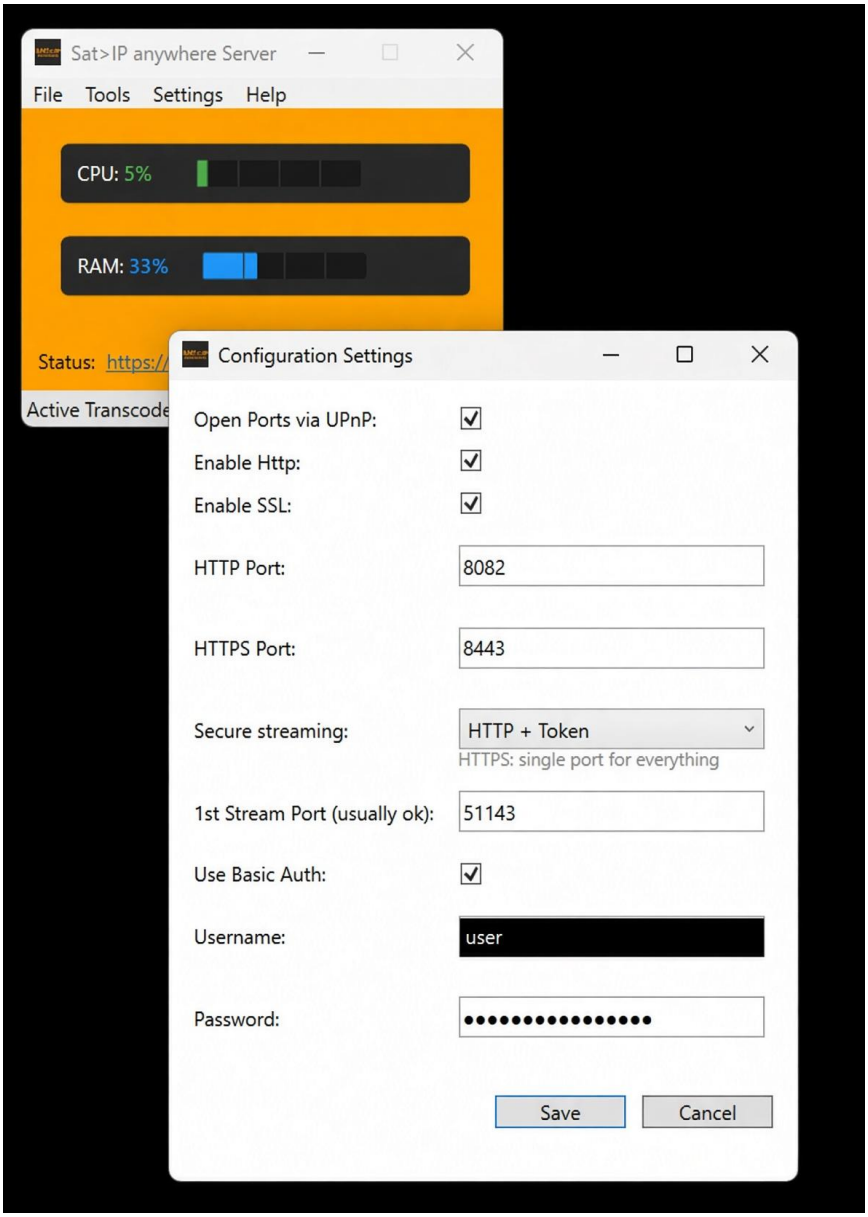
1. Switch to expert view: on the left, click “View: Standard” so that it reads “View: Advanced”.
2. Home Network, Network, Network Settings: enable “Transmit status information over UPnP”.
3. Internet, Permit Access, Windows PC: enable “Allow this device to open ports on its own”.

Other routers have a similar setting, usually under UPnP. A detailed FRITZ!Box guide is here: giga.de, FRITZ!Box UPnP.

On other routers the switch is usually just called UPnP. Enter the DynDNS name in the router, for example via ddnss.de. A FRITZ!Box guide for that is at heimnetz.de.

4 First-time setup

The first decision is whether you want to reach the server app through a VPN, WireGuard or Tailscale (simple HTTP configuration) or through native HTTPS. If you choose HTTPS, pick a long and complex password, even though the server now includes brute-force detection.



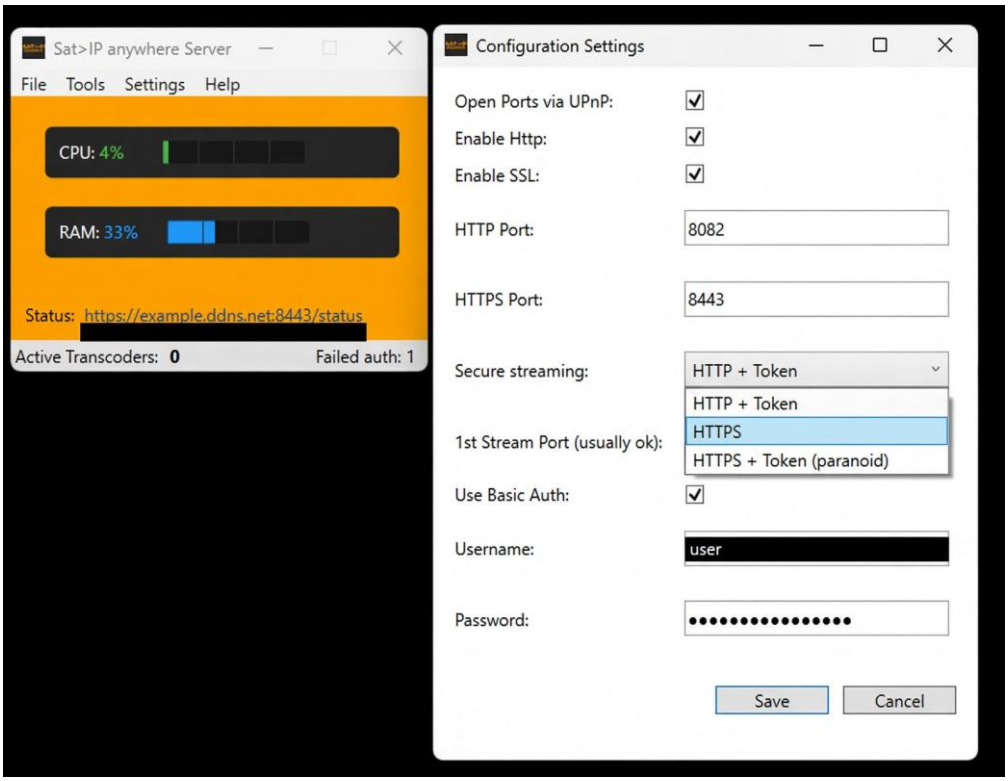
Settings. The username in the picture is a placeholder.

Settings: after saving, the application closes and must be restarted so that the port or ports are bound again and, if needed, a certificate can be created.

- Open Ports via UPnP: on, if the router supports it.
- Enable HTTP: for testing, Android TV, or VPN use. Never forward this port in the router.
- Enable SSL: for use away from home. 8443 is typical. With SSL the whole transfer, control and picture, runs over this one port.
- 1st Stream Port: relevant only for HTTP + Token mode, usually 51111 or higher. A manual forward in the router is strongly discouraged.

- Use Basic Auth, Username and Password: enter the same values in the client app.

Secure streaming



Streaming mode. The address in the background is an example, not a real DynDNS name.

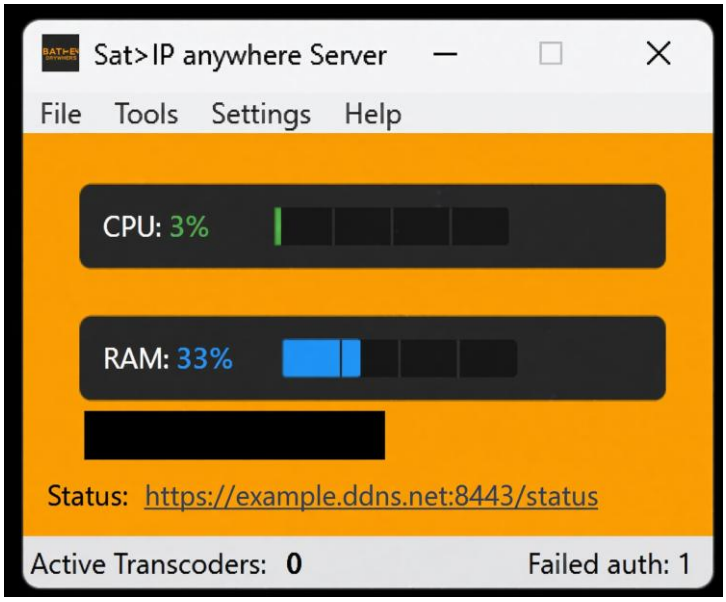
Streaming mode. The address in the background is an example, not a real DynDNS name.

- HTTP + Token: every new connection fetches a new token from the server (over SSL, if SSL was configured). The server discards the token as soon as the connection is up. This should be reasonably safe, but there is no guarantee.[1]
- HTTPS: one port for everything. This is the normal, recommended configuration.
- HTTPS + Token (paranoid): the same single HTTPS port, plus a token on every connect or reconnect. Recommended if you are abroad.

The app creates the certificate from the DynDNS name and a certificate password. The certificate password is not the app login and is not asked for again later. Open the QR code under Settings, Network & Security, Certificate QR-Code. It is valid for all devices and does not change unless the certificate is created again.

[1]The point is that the client does not have to decrypt the video data, which saves battery. For anyone who wants to look into it: “Name potential attacks against plain HTTP/TCP video streaming where the client must present a single-use UUID token on every connect/reconnect, previously sent to the client over SSL. This is live streaming only (unidirectional), so confidentiality is not the priority. What matters is that an attacker cannot reach the VLC transcoder, which should hold because a TCP proxy in front denies access without a token.”

On first start Windows usually asks whether the app may pass the firewall. Allow it. The status line then shows the reachable address, for example https://example.ddns.net:8443/status.

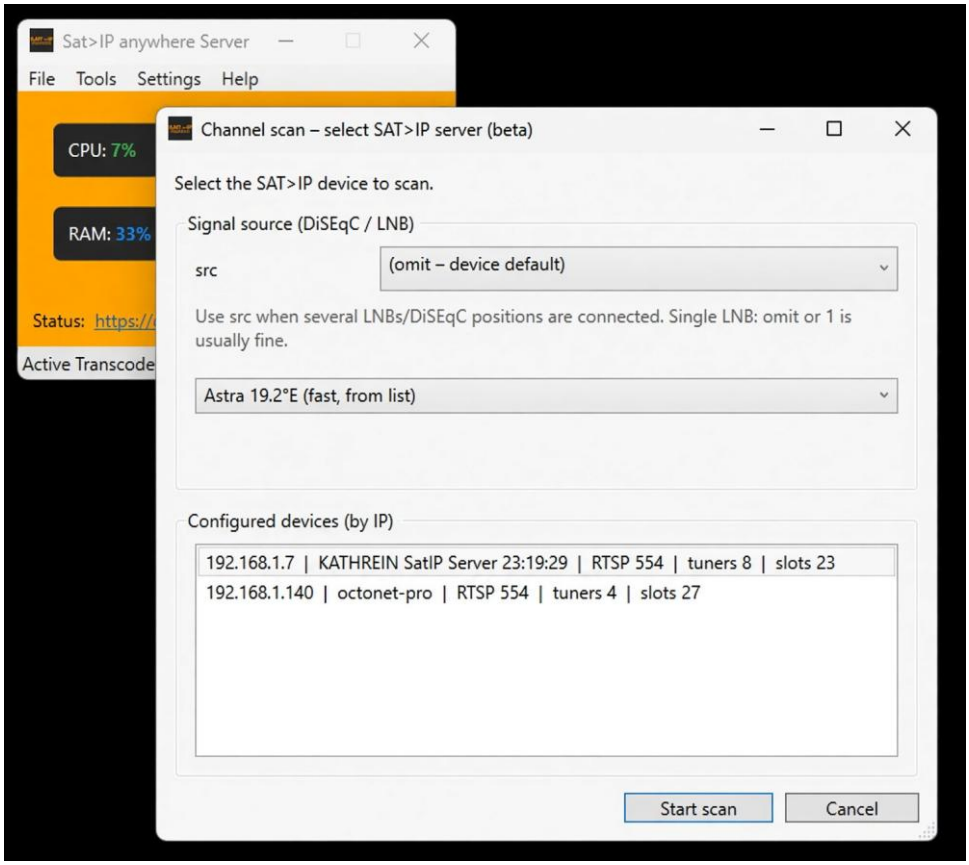


Main window after start. The address is an example.

Main window after start. The DynDNS address is an example.

5 Channels

The app does not ship a ready-made channel list. Either import an external M3U (for example github.com/dersnyke/satipplaylists, or one from the FRITZ!Box Cable web interface) via File, Import M3U Playlist, or use the built-in satellite scan.



Channel scan. One LNB: omit src, or use 1. Several LNBs: set the DiSEqC position.

Channel scan. One LNB: omit src, or use 1. Several LNBs: set the DiSEqC position.

1. Select the device in the list and start the scan. Ku-band frequencies for Astra 19.2° East and Türksat 42° East are already included, so the channel scan is faster than a blind scan.
2. The M3U file is written to the scan folder and can be edited afterwards, which is normally not necessary.
3. Import the M3U file: see above.
4. Tools, Channel Configuration: assign the channels you want to the matching SAT>IP server.
5. Save List as JSON. A restart is not required.
6. Only then does the app answer programme and EPG requests.

If no SAT>IP server is found, restart the SAT>IP device or unplug the network cable briefly. The IP must be the same afterwards.

6 Android app

Play Store, Sat>IP anywhere. Top right, menu, Setup.

1. IP or DDNS Host: the DynDNS name when away from home, or the LAN IP of the Windows PC for local HTTP only. Not the IP of the SAT>IP device.
2. Client Id: one id per device, from 1 upward. Two devices need two different ids.
3. Turn HTTPS on if SSL was configured on the server. The port is then the HTTPS port, for example 8443. For local HTTP, enter the HTTP port and leave HTTPS off.
4. Username and password as in the server app.
5. Scan Certificate: scan the QR code from the server. Keep the marker inside the code. Once is enough.

Recordings run on the server and appear in the app under Recordings. The server app should be up to date for that.

1. If possible, set compatibility mode to off under menu, Playback Settings.
2. Data Saver when away from home, if picture quality is secondary (about 1 Mbit/s).

7 Having troubles?

- Please join the WhatsApp support group. chat.whatsapp.com/IjLmnS03KMPH9GIZgkliE9
- Failed auth in the status line counts failed logins. Check username, password and port in the app.
- HTTPS port does not bind: run the batch file for the URL reservation once as administrator. Menu Settings, Network and Security, Register HTTPS port (Admin).

Current version and readme: sat-ip-anywhere.com

Questions to marco.wegehaupt@gmail.com.