Antlysis VPN Setup Guide

Last updated: 2026-05-07

Overview

Antlysis uses **Tailscale** connected to our self-hosted **Headscale** server to provide secure access to internal infrastructure. This guide will walk you through installing and connecting to the VPN on your device.

> ⚠ **Before you begin:** Make sure you have received your personal **Auth Key** from the DevOps team. Each key is unique to you and expires in **24 hours** — connect as soon as possible after receiving it.

Supported Platforms

Platform	Supported
Windows 10/11	
macOS	
Linux (Ubuntu/Debian/RHEL)	
Android	
iOS	

Creating new account

1. SSH into Bastion-Host server.
2. Create user:

```
docker exec -it headscale headscale users create <username>
```

3. Get user id:

```
docker exec -it headscale headscale users list
```

4. Create preauth key:

```
docker exec -it headscale headscale preauthkey create -u <USER ID> --expiration 24h
--reusable=false
```

Deleting account

1. SSH into Bastion-Host server.
2. Check existing nodes:

```
docker exec -it headscale headscale nodes list
```

3. Delete nodes with corresponding user:

```
docker exec -it headscale headscale nodes delete --identifier <NODE ID> --force
```

4. Get user ID:

```
docker exec -it headscale headscale users list
```

5. Delete user:

```
docker exec -it headscale headscale users destroy --identifier <USER ID>
```

Installation

Windows

1. Download Tailscale from the official website: https://tailscale.com/download/windows
2. Run the installer and follow the on-screen instructions.
3. Once installed, **do NOT sign in through the GUI** — we use our own server, not Tailscale's cloud. Open **Command Prompt** or **PowerShell** instead.
4. Connect to the Antlysis VPN using your auth key:

```
tailscale up --login-server https://vpn.antlysis.com --authkey <YOUR-AUTH-KEY>
```

5. Verify your connection:

```
tailscale status
```

---

macOS

1. Download Tailscale from the Mac App Store: □□
   https://apps.apple.com/app/tailscale/id1475387142
   Or via Homebrew:

```
brew install tailscale
```

2. Open **Terminal** and connect using your auth key:

```
sudo tailscale up --login-server https://vpn.antlysis.com --authkey <YOUR-AUTH-KEY>
```

3. Verify your connection:

```
tailscale status
```

Linux (Ubuntu/Debian)

1. Install Tailscale:

```
curl -fsSL https://tailscale.com/install.sh | sh
```

2. Connect using your auth key:

```
sudo tailscale up --login-server https://vpn.antlysis.com --authkey <YOUR-AUTH-KEY>
```

3. Verify your connection:

```
tailscale status
```

Android

1. Install Tailscale from the Google Play Store: □□ https://play.google.com/store/apps/details?id=com.tailscale.ipn
2. Open the app and tap the **three dots menu (⋮)** in the top right.
3. Tap **Use custom coordination server** and enter:

   ```
   https://vpn.antlysis.com
   ```

4. Tap **Connect** and enter your auth key when prompted.

---

iOS

1. Install Tailscale from the App Store: □□ https://apps.apple.com/app/tailscale/id1475387142
2. Open the app and tap the **three dots menu (⋮)** in the top right.
3. Tap **Use custom coordination server** and enter:

   ```
   https://vpn.antlysis.com
   ```

4. Tap **Connect** and enter your auth key when prompted.

Verifying Your Connection

After connecting, run the following to confirm you are connected:

```
tailscale status
```

You should see output similar to this:

```
100.64.0.X   your-device    antlysis   <OS>   -
100.64.0.1   bastion-host   antlysis   linux  idle; offers exit node
```

Testing Access to Internal Servers

Once connected, test that you can reach internal servers based on your role:

```
# Production Main Server
ping 172.16.0.1
```

```
# Production Apps
ping 172.16.2.1

# Sandbox
ping 172.16.1.101
```

> ℹ You will only be able to reach servers that your role has been granted access to. If you cannot reach a server you need, contact the DevOps team.

Server Access by Role

Access is granted based on your role. Each role gives you access to a specific section of the Antlysis infrastructure:

□□ Production Services

Gives access to the core production services servers:

Server	IP	What's Running
Production-Main.services	172.16.0.1	Portainer, Grafana, Loki, BookStack, Passbolt, NGINX, Node-RED, InfluxDB, MariaDB, MinIO
Production-1A.services	172.16.0.2	EMQX (MQTT), RabbitMQ, Redis
Production-1B.services	172.16.1.2	EMQX (MQTT), RabbitMQ, Redis

---

□□ Production Apps

Gives access to the production application servers running all live customer-facing services:

Server	IP	What's Running
Production-1A.apps	172.16.2.1	Application services (Swarm Worker)
Production-2A.apps	172.16.2.2	Application services (Swarm Worker)
Production-3A.apps	172.16.2.3	Application services (Swarm Worker)

Server	IP	What's Running
Production-4A.apps	172.16.2.4	Application services (Swarm Worker)

> ⚠ These are live production servers. Be careful with any changes made here.

□□ Sandbox

Gives access to the sandbox (testing) environment which mirrors production. Safe to test and develop without affecting live services:

Server	IP	What's Running
Sandbox-1.services	172.16.1.101	Sandbox analog of Production-Main, test/echo services
Sandbox-1A.apps	172.16.2.101	Sandbox application services (Swarm Worker)
Sandbox-1B.apps	172.16.3.104	Sandbox application services (Swarm Worker)

> **i** Sandbox uses `:sandbox` tagged images. All development and testing should be done here first before promoting to production.

□□ Apsara DB

Gives access to the Alibaba Cloud ApsaraDB RDS instances hosted in the database subnet. These are the **main persistent databases** for all applications:

Subnet	Notes
172.23.32.0/20	Apsara RDS instances — PostgreSQL/MySQL (Zone B)

□□ Internal DB

Gives access to specific internal database and storage containers running on **Production-Main.services**:

Service	Port	Purpose
MariaDB	3306	Relational database for internal services
InfluxDB	8086	Time-series database for metrics
MinIO API	9000	Object storage API
MinIO Console	9001	Object storage management UI
Loki	3100	Log aggregation
Prometheus	9090	Metrics collection
BookStack	80/443	Internal documentation wiki

> ⚠ These are production data services. Read/write access depending on your credentials.

Role Assignment Summary

Role	Production Services	Production Apps	Sandbox	Apsara DB	Internal DB
Admin	✅	✅	✅	✅	✅
Senior Developer	✅	✅	✅	✅	✅
Junior Developer	✅	✅	✅	✅	✅
Graduate/Intern	✅	✅	✅	✅	✅

> ℹ If you need access to a section not listed under your role, raise a request with the DevOps team.

Disconnecting from the VPN

Windows / macOS / Linux

```
tailscale down
```

Mobile

Tap the toggle in the Tailscale app to disconnect.

Reconnecting

Your device stays registered permanently after the first connection. To reconnect after disconnecting:

Windows / macOS / Linux

```
tailscale up
```

> **i** You do **not** need your auth key again after the first connection. The auth key is only used once during initial registration.

Troubleshooting

`tailscale up` hangs or times out

- Check your internet connection.
- Make sure no firewall is blocking outbound connections to `vpn.antlysis.com` on port `443`.

Cannot reach internal servers after connecting

- Run `tailscale status` and confirm you are connected.
- Confirm with the DevOps team that your user has been added to the correct ACL groups.

Auth key is invalid or expired

- Auth keys expire after **24 hours**. Contact the DevOps team to generate a new key.

`missing "Bearer" prefix` error

- This is a server-side log message and does not affect your connection. Ignore it.

Revision #4
Created 2026-05-07 09:55:54 UTC by Khayhen
Updated 2026-08-19 06:10:46 UTC by Admin