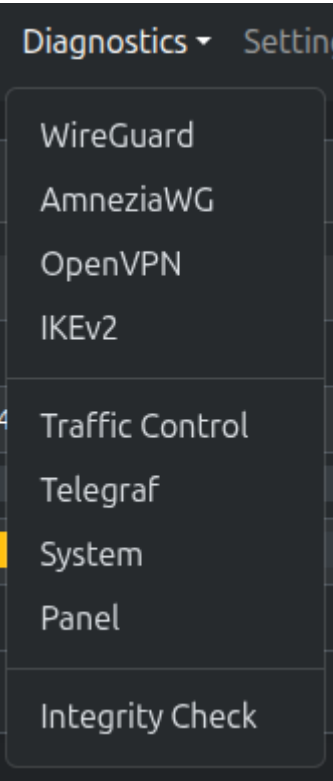


21. Diagnostics

Overview

The **Diagnostics** section provides real-time monitoring, log viewing, and system integrity protocols, traffic control, monitoring services, and the panel itself.



Click on the **Diagnostics** icon in the main menu to access the following pages:

Diagnostics dropdown menu

Page	Description
WireGuard	WireGuard service status, <code> wg show </code> output, kernel logs
AmneziaWG	AmneziaWG service status, <code> awg show </code> output, kernel logs
OpenVPN	OpenVPN service status, certificates, instances, connection events, auth log, server logs
IKEv2	strongSwan service status, certificates, <code> ipsec statusall </code> output, IKEv2 logs
Traffic Control	Overview of TC classes, per-interface bandwidth statistics with live throughput

Page	Description
Telegraf	Telegraf service status, InfluxDB output config, inputs, Telegraf logs
System	Server uptime, memory, disk usage, network interfaces, system logs
Panel	PUQVPNCP application log viewer (<code> puqvpncp. log </code>)
Integrity Check	Full system integrity audit — verifies firewall rules, ipset, routing, TC classes, interfaces

“ **Permission:** All diagnostics pages require the `|diagnostics: read|` permission. Integrity Check requires `|firewall: read|` (audit) and `|firewall: write|` (fix).

All log viewers feature:

- **Auto-refresh** every 3 seconds
- **Pause / Resume** button to stop auto-refresh
- **Line count selector** (50, 100, 200, 500 lines)
- **Color-coded** log entries (errors in red, warnings in yellow, connections in green)

WireGuard

PUQVPNCP

Dashboard

Networks

Clients

VPN Servers

Diagnostics

Settings

About us

Help

admin (45.44.164.152)

Logout

Diagnostics: WireGuard

Service Status

WireGuard

WireGuard Tools

Networks

Clients

Online

1.0.20210914-3

1.0.20210914-3

6

499

1

wg show

```
interface: wgup1
  public key: 3y55X9Flwb99gFEaMtyGkSsyNqQEmp/aNbCDC9jxySo=
  private key: (hidden)
  listening port: 37697

peer: uXw1kT+tp/LvB6n2nSY8IBTjKx0kCNonAIF5Wk//cBo=
  endpoint: 77.87.125.170:123
  allowed ips: 0.0.0.0/0
  latest handshake: 1 minute, 36 seconds ago
  transfer: 342.42 MiB received, 63.71 MiB sent
  persistent keepalive: every 25 seconds

interface: wg51820
  public key: 7jyVv2JCRUGTV8hDPzqZyFvMY1yjt+ya+BLJlutoyA=
  private key: (hidden)
  listening port: 51820

peer: qZWfK0WTE5eWk1DFeCMdpRZrteD1+ZAHaklrXM0pt38=
  allowed ips: 10.100.9.23/32
  persistent keepalive: every 25 seconds
```

Diagnostics: WireGuard — service status, wg show, kernel logs

Service Status

Field	Description
WireGuard	Installed WireGuard kernel module version
WireGuard Tools	Installed <code>wireguard-tools</code> package version
Networks	Number of WireGuard-enabled networks
Clients	Total number of WireGuard clients
Online	Number of currently connected WireGuard peers

If WireGuard or WireGuard Tools are not installed, or no networks are configured, a warning alert is displayed with instructions.

wg show

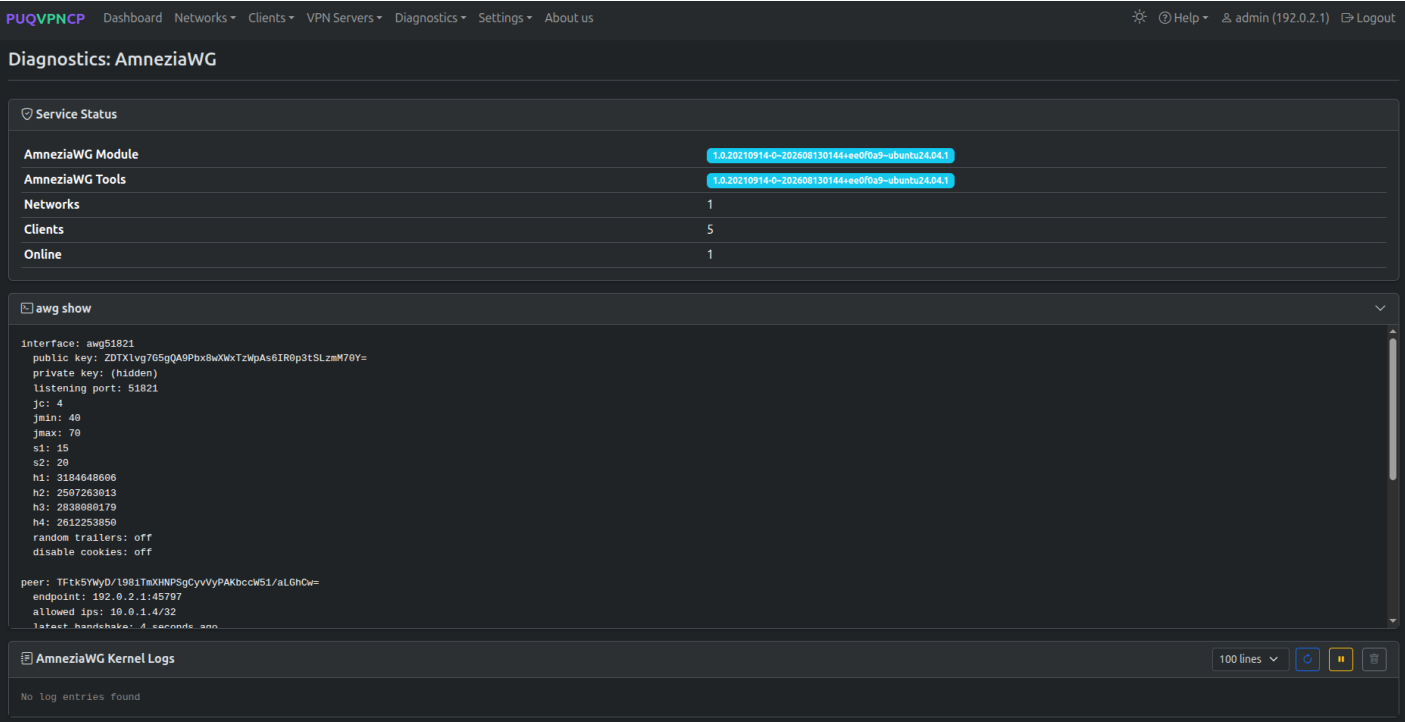
Displays the raw output of the `wg show` command — the standard WireGuard status tool. Shows all active WireGuard interfaces with their public keys, listening ports, and connected peers with handshake times and transfer statistics.

This section is collapsible. Click the header to expand/collapse.

WireGuard Kernel Logs

Displays WireGuard-related kernel messages from `journalctl`. These logs show low-level WireGuard events such as interface creation, peer handshake failures, and kernel module messages.

AmneziaWG



Diagnostics: AmneziaWG — service status, awg show, and kernel logs

Service Status

Field	Description
AmneziaWG	Installed AmneziaWG kernel module (DKMS) version
AmneziaWG Tools	Installed <code>amneziawg-tools</code> package CLI version (<code> awg </code>)
Networks	Number of AmneziaWG-enabled networks
Clients	Total number of AmneziaWG clients
Online	Number of currently connected AmneziaWG peers

If AmneziaWG or AmneziaWG Tools are not installed, or no networks are configured, an informative warning alert is displayed with repository and package installation instructions for Debian (with `|build-essential dkms linux-headers-$(uname -r)|`) and Ubuntu (`|add-apt-repository -y ppa:amnezia/ppa|`).

awg show

Displays the raw output of the `|awg show|` command — the standard AmneziaWG status tool. Shows all active AmneziaWG interfaces with obfuscation parameters (`|Jc|`, `|Jmin|`, `|Jmax|`, `|S1|`, `|S2|`, `|H1|`, `|H2|`, `|H3|`, `|H4|`), public keys, listening ports, and connected peers with handshake times and transfer statistics.

This section is collapsible. Click the header to expand/collapse.

AmneziaWG Kernel Logs

Displays AmneziaWG-related kernel messages from `journalctl`. These logs show low-level AmneziaWG events such as interface creation, handshake negotiations, and kernel module messages.

OpenVPN

Service Status and Certificates

PUQVPNC

Dashboard

Networks

Clients

VPN Servers

Diagnostics

Settings

About us

Help

admin (45.44.164.152)

Logout

Diagnostics: OpenVPN

Service Status

OpenVPN	2.6.14-11deb13u1
easy-rsa	Installed
Global Status	Enabled
Networks	6
Online	1

Certificates

CA Certificate	Valid
Server Certificate	Valid
DH Parameters	Valid
TLS Auth Key	Valid

Instances

Network	Port	Status	PID
loadtest_net12	1196	Running	507342
loadtest_net13	1198	Running	507355
loadtest_net10	1194	Running	507368
loadtest_net14	1199	Running	507381
loadtest_net11	1195	Running	507396
TETS	1197	Running	507329

Diagnostics: OpenVPN — service status, certificates, instances

The page displays two cards side by side:

Service Status:

Field	Description
OpenVPN	Installed OpenVPN package version
easy-rsa	Installed easy-rsa package version
Global Status	Whether OpenVPN is globally enabled or disabled
Networks	Number of OpenVPN-enabled networks
Online	Number of currently connected OpenVPN clients

Certificates:

Field	Description
CA Certificate	Root CA certificate status (Valid / Not generated / Invalid)
Server Certificate	Server TLS certificate status
DH Parameters	Diffie-Hellman parameters status
TLS Auth Key	HMAC authentication key status

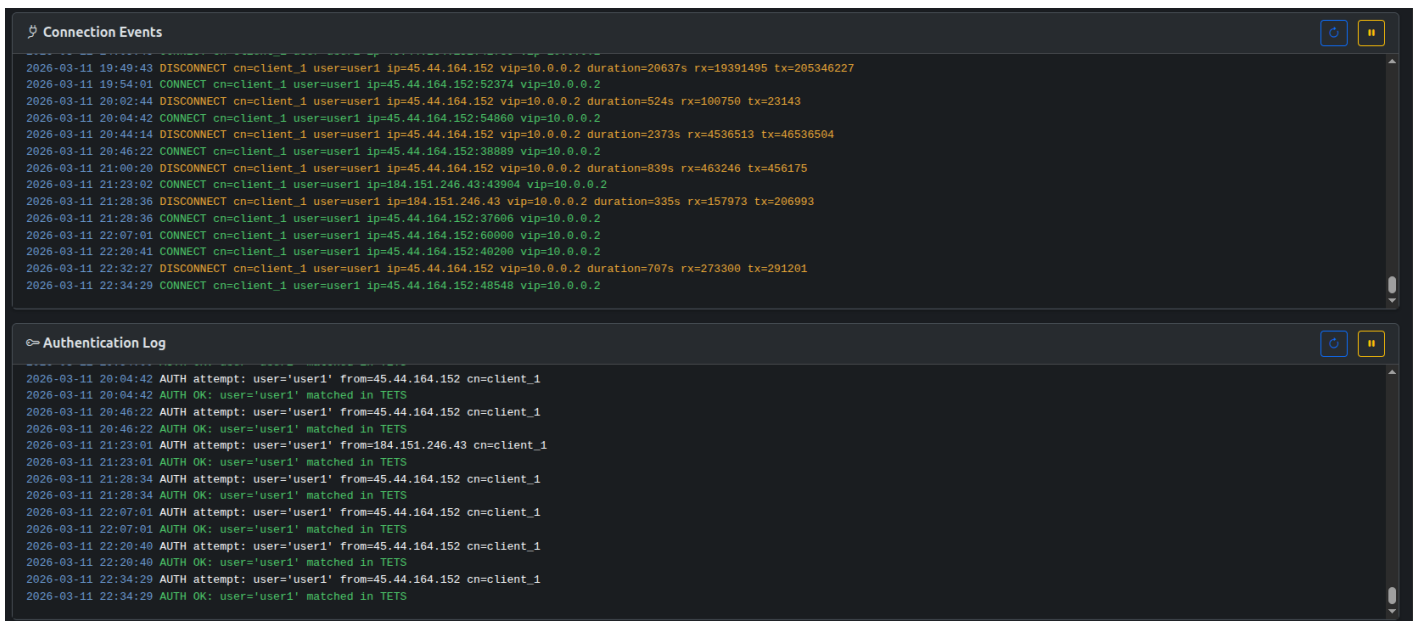
Instances

Shows a table of all OpenVPN network instances:

Column	Description
Network	Network name (link to network edit page)
Port	UDP/TCP port for this instance
Status	Running (green) or Stopped (red)
PID	Process ID (if running)

Each OpenVPN-enabled network runs as a separate `openvpn` process with its own PID file.

Connection Events



Diagnostics: OpenVPN — connection events and authentication log

Displays the OpenVPN connection log (`| /etc/openvpn/puqvpncp/logs/connections.log |`). Shows client connect and disconnect events with color coding:

- **Green** — `|CONNECT|` events
- **Yellow** — `|DISCONNECT|` events

Authentication Log

Displays the OpenVPN authentication log (`| /etc/openvpn/puqvpncp/logs/auth.log |`). Shows authentication attempts with color coding:

- **Green** — `|AUTH OK|` events
- **Red** — `|AUTH FAILED|` or `|AUTH ERROR|` events

Server Logs

Server Logs100 lines

```
[wisevpn] 2026-03-06 20:10:11 us=396209 CRL: loaded 1 CRLs from file /usr/local/puqvpncp/openvpn/pki/crl.pem
[wisevpn] 2026-03-06 20:10:11 us=396433 Outgoing Control Channel Authentication: Using 256 bit message hash 'SHA256' for HMAC authentication
[wisevpn] 2026-03-06 20:10:11 us=396484 Incoming Control Channel Authentication: Using 256 bit message hash 'SHA256' for HMAC authentication
[wisevpn] 2026-03-06 20:10:11 us=396582 TLS-Auth MTU parms [ mss_fix:0 max_frag:0 tun_mtu:1250 tun_max_mtu:0 headroom:126 payload:1600 tailroom:126 ET:0 ]
[wisevpn] 2026-03-06 20:10:11 us=398472 TUN/TAP device ovpn1196 opened
[wisevpn] 2026-03-06 20:10:11 us=398522 do_ifconfig, ipv4=1, ipv6=0
[wisevpn] 2026-03-06 20:10:11 us=398584 net_iface_mtu_set: mtu 1420 for ovpn1196
[wisevpn] 2026-03-06 20:10:11 us=398853 net_iface_up: set ovpn1196 up
[wisevpn] 2026-03-06 20:10:11 us=399675 net_addr_v4_add: 10.0.4.254/24 dev ovpn1196
[wisevpn] 2026-03-06 20:10:11 us=399830 Data Channel MTU parms [ mss_fix:0 max_frag:0 tun_mtu:1420 tun_max_mtu:1600 headroom:136 payload:1768 tailroom:562 ET:0 ]
[wisevpn] 2026-03-06 20:10:11 us=400079 Could not determine IPv4/IPv6 protocol. Using AF_INET
[wisevpn] 2026-03-06 20:10:11 us=400110 Socket Buffers: R=[212992->212992] S=[212992->212992]
[wisevpn] 2026-03-06 20:10:11 us=400148 UDPv4 link local (bound): [AF_INET][under]:1196
[wisevpn] 2026-03-06 20:10:11 us=400164 UDPv4 link remote: [AF_UNSPEC]
[wisevpn] 2026-03-06 20:10:11 us=400226 UID set to nobody
[wisevpn] 2026-03-06 20:10:11 us=400243 GID set to nogroup
[wisevpn] 2026-03-06 20:10:11 us=400253 Capabilities retained: CAP_NET_ADMIN
[wisevpn] 2026-03-06 20:10:11 us=400267 MULTI: multi_init called, r=256 v=256
[wisevpn] 2026-03-06 20:10:11 us=400311 IFCONFIG POOL IPv4: base=10.0.4.2 size=251
[wisevpn] 2026-03-06 20:10:11 us=400372 Initialization Sequence Completed
[wisevpn] 2026-03-06 20:12:09 us=74652 event_wait : Interrupted system call (fd=-1,code=4)
[wisevpn] 2026-03-06 20:12:09 us=75093 TCP/UDP: Closing socket
[wisevpn] 2026-03-06 20:12:09 us=75202 Closing TUN/TAP interface
[wisevpn] 2026-03-06 20:12:09 us=75243 net_addr_v4_del: 10.0.4.254 dev ovpn1196
[wisevpn] 2026-03-06 20:12:09 us=151785 SIGTERM[hard,] received, process exiting
```

Diagnostics: OpenVPN — server logs from all network instances

Displays combined server logs from all OpenVPN network instances (`/etc/openvpn/puqvpncp/logs/*.log`). Each log line is prefixed with the network name in square brackets (e.g., `[ net1 ] ...`).

IKEv2

Service Status and Certificates

Service Status

strongSwan	6.0.1-6+deb13u2
Starter PID	507283
Charon PID	507284
Global Status	Enabled
Server Domain	dev.puqvpncp.com
Online	0

Certificates

CA Certificate	Valid
Server Certificate	Valid

ipsec statusall

Status of IKE charon daemon (strongSwan 6.0.1, Linux 6.12.73+deb13-amd64, x86_64):
 uptime: 42 minutes, since Mar 11 22:33:53 2026
 malloc: sbrk 8167424, mmap 0, used 7335776, free 831648
 worker threads: 11 of 16 idle, 5/0/0/0 working, job queue: 0/0/0/0, scheduled: 0
 loaded plugins: charon test-vectors ldap pkcs11 aesni aes rc2 sha2 sha1 md5 mgf1 rndrand random nonce x509 revocation constraints pubkey pkcs1 pkcs7 pkcs12 pgp dnskey sshkey pem openssl gcrypt pkcs8 a
 f-alg flps-prf gmp curve25519 agent chapoly xcbc cmac hmac kdf ctr ccm gcm drbg curl attr kernel-netlink resolve socket-default connmark forecast farp stroke updown eap-identity eap-aka eap-md5 eap-gtc
 eap-mschapv2 eap-radius eap-tls eap-ttls eap-tnc xauth-generic xauth-eap xauth-pam tnc-tncs dhcp lookip error-notify certexpire led addrblock unity counters
Virtual IP pools (size/online/offline):
 10.0.0.3: 1/0/0
 10.0.0.4: 1/0/0
 10.0.0.18: 1/0/0
 10.0.0.5: 1/0/0
 10.0.0.2: 1/0/0
 10.100.9.16: 1/0/0
 10.100.9.26: 1/0/0
 10.100.9.50: 1/0/0
 10.100.9.74: 1/0/0
 10.100.9.76: 1/0/0
 10.100.9.78: 1/0/0
 10.100.9.82: 1/0/0

Diagnostics: IKEv2 — service status, certificates, ipsec statusall

The page displays two cards side by side:

Service Status:

Field	Description
strongSwan	Installed strongSwan version
Starter PID	PID of the strongSwan starter process
Charon PID	PID of the IKE daemon (charon)
Global Status	Whether IKEv2 is globally enabled or disabled
Server Domain	Domain configured for IKEv2 server certificates
Online	Number of currently connected IKEv2 clients

Certificates:

Field	Description
CA Certificate	Root CA certificate status (Valid / Not generated / Invalid)
Server Certificate	Server certificate status

ipsec statusall

Displays the raw output of the `ipsec statusall` command — the standard strongSwan status tool. Shows detailed information about:

- IKE charon daemon status (version, uptime, memory, threads, plugins)
- Virtual IP pools with size/online/offline counters
- Active security associations (SAs)
- Connection definitions

This section is collapsible.

IKEv2 / strongSwan Logs

IKEv2 / strongSwan Logs

100 lines

```
2026-03-11T10:10:20+01:00 dev.puqvpncp.com charon[143687]: 10[IKE] 00.132.138.193 is initiating an IKE_SA
2026-03-11T10:15:41+01:00 dev.puqvpncp.com charon[143687]: 09[IKE] 167.94.138.35 is initiating an IKE_SA
2026-03-11T10:15:41+01:00 dev.puqvpncp.com charon[143687]: 09[IKE] 167.94.138.35 is initiating an IKE_SA
2026-03-11T12:22:43+01:00 dev.puqvpncp.com charon[143687]: 03[IKE] 193.163.125.239 is initiating an IKE_SA
2026-03-11T12:22:43+01:00 dev.puqvpncp.com charon[143687]: 03[IKE] 193.163.125.239 is initiating an IKE_SA
2026-03-11T12:23:45+01:00 dev.puqvpncp.com charon[143687]: 12[IKE] 87.236.176.81 is initiating an IKE_SA
2026-03-11T12:23:45+01:00 dev.puqvpncp.com charon[143687]: 12[IKE] 87.236.176.81 is initiating an IKE_SA
2026-03-11T14:05:38+01:00 dev.puqvpncp.com charon[143687]: 13[IKE] 45.44.164.152 is initiating an IKE_SA
2026-03-11T14:05:38+01:00 dev.puqvpncp.com charon[143687]: 13[IKE] 45.44.164.152 is initiating an IKE_SA
2026-03-11T14:05:38+01:00 dev.puqvpncp.com charon[143687]: 11[IKE] 45.44.164.152 is initiating an IKE_SA
2026-03-11T14:05:38+01:00 dev.puqvpncp.com charon[143687]: 11[IKE] 45.44.164.152 is initiating an IKE_SA
2026-03-11T14:05:38+01:00 dev.puqvpncp.com charon[143687]: 07[IKE] IKE_SA ikev2-client_1[25] established between 77.87.125.200[dev.puqvpncp.com]...45.44.164.152[user1]
2026-03-11T14:05:38+01:00 dev.puqvpncp.com charon[143687]: 07[IKE] IKE_SA ikev2-client_1[25] established between 77.87.125.200[dev.puqvpncp.com]...45.44.164.152[user1]
2026-03-11T14:05:38+01:00 dev.puqvpncp.com charon[143687]: 07[IKE] CHILD_SA ikev2-client_1{i} established with SPIs c80ae73b_1 109dd6e1_o and TS 0.0.0.0/0 :/0 == 10.0.0.2/32
2026-03-11T14:05:38+01:00 dev.puqvpncp.com charon[143687]: 07[IKE] CHILD_SA ikev2-client_1{i} established with SPIs c80ae73b_1 109dd6e1_o and TS 0.0.0.0/0 :/0 == 10.0.0.2/32
2026-03-11T14:05:42+01:00 dev.puqvpncp.com charon[143687]: 08[IKE] deleting IKE_SA ikev2-client_1[25] between 77.87.125.200[dev.puqvpncp.com]...45.44.164.152[user1]
2026-03-11T14:05:42+01:00 dev.puqvpncp.com charon[143687]: 08[IKE] deleting IKE_SA ikev2-client_1[25] between 77.87.125.200[dev.puqvpncp.com]...45.44.164.152[user1]
2026-03-11T14:05:42+01:00 dev.puqvpncp.com charon[143687]: 08[IKE] IKE_SA deleted
2026-03-11T14:05:42+01:00 dev.puqvpncp.com charon[143687]: 08[IKE] IKE_SA deleted
2026-03-11T15:11:09+01:00 dev.puqvpncp.com charon[143687]: 11[IKE] 206.168.34.193 is initiating an IKE_SA
2026-03-11T15:11:09+01:00 dev.puqvpncp.com charon[143687]: 11[IKE] 206.168.34.193 is initiating an IKE_SA
2026-03-11T15:31:45+01:00 dev.puqvpncp.com charon[143687]: 09[IKE] 167.94.138.195 is initiating an IKE_SA
2026-03-11T15:31:45+01:00 dev.puqvpncp.com charon[143687]: 09[IKE] 167.94.138.195 is initiating an IKE_SA
2026-03-11T15:31:45+01:00 dev.puqvpncp.com charon[143687]: 13[IKE] 206.168.34.126 is initiating an IKE_SA
2026-03-11T15:31:45+01:00 dev.puqvpncp.com charon[143687]: 13[IKE] 206.168.34.126 is initiating an IKE_SA
```

Diagnostics: IKEv2 — strongSwan logs

Displays strongSwan logs from `|journalctl|`. Shows IKE negotiation events, connection establishments, certificate validations, and authentication messages. The system tries `|strongswan|` unit first, then falls back to `|charon|` syslog tag.

Traffic Control

PUQVPNCPDashboardNetworksClientsVPN ServersDiagnosticsSettingsAbout us

☀️🔗 Helpadmin (45.44.164.152)Logout

Diagnostics: Traffic Control

🔗 Overview

Managed Interfaces15

Total TC Classes55

Total Bytes Processed131.95 MiB

Total Drops440

🔍 ens1811 classes

Handle	Type	Rate	Bytes	Packets	Drops	Overlimits	Throughput
1:806e	DL IPv4 #110	1 Mbit	0 B	0	0	0	0 bit/s
1:806f	DL IPv4 #111	3 Mbit	0 B	0	0	0	0 bit/s
1:1	root	10 Gbit	0 B	0	0	0	0 bit/s
1:c078	DL IPv6 #120	3 Mbit	0 B	0	0	0	0 bit/s
1:c06e	DL IPv6 #110	1 Mbit	0 B	0	0	0	0 bit/s
1:c06f	DL IPv6 #111	3 Mbit	0 B	0	0	0	0 bit/s
1:8078	DL IPv4 #120	3 Mbit	0 B	0	0	0	0 bit/s
1:8077	DL IPv4 #119	3 Mbit	0 B	0	0	0	0 bit/s
1:84bc	DL IPv4 #1212	3 Mbit	0 B	0	0	0	0 bit/s
1:c077	DL IPv6 #119	3 Mbit	0 B	0	0	0	0 bit/s
1:c4bc	DL IPv6 #1212	3 Mbit	0 B	0	0	0	0 bit/s

🔍 wg518241 classes

Handle	Type	Rate	Bytes	Packets	Drops	Overlimits	Throughput
1:1	root	10 Gbit	0 B	0	0	0	0 bit/s

Diagnostics: Traffic Control — overview and per-interface TC classes

Overview

Field	Description
Managed Interfaces	Total number of network interfaces with TC rules
Total TC Classes	Total number of HTB traffic control classes across all interfaces
Total Bytes Processed	Sum of all bytes processed by TC classes
Total Drops	Sum of all dropped packets (highlighted in red if > 0)

The overview auto-refreshes every 2 seconds.

Per-Interface Tables

Below the overview, each managed interface is displayed as a separate card showing all its TC classes:

Column	Description
Handle	TC class handle (e.g., <code>1: 806e</code>)
Type	Class type — <code>root</code> for the root class, or direction + protocol (e.g., <code>DL IPv4 #110</code> , <code>UL IPv6 #119</code>)
Rate	Configured bandwidth rate
Bytes	Total bytes processed by this class
Packets	Total packets processed
Drops	Dropped packets (highlighted in red if > 0)
Overlimits	Overlimit events (highlighted in yellow if > 0)
Throughput	Real-time throughput calculated from byte deltas between refreshes

Interfaces include:

- **Gateway interfaces** (e.g., `ens18`) — main server network interfaces
 - **WireGuard interfaces** (e.g., `wg51824`) — per-network WireGuard tunnel interfaces
 - **OpenVPN interfaces** (e.g., `ovpn1197`) — per-network OpenVPN tunnel interfaces
 - **Upstream interfaces** (e.g., `wgup1`) — upstream WireGuard tunnel interfaces
-

Telegraf

PUQVPNCP

Dashboard

Networks

Clients

VPN Servers

Diagnostics

Settings

About us

Help

admin (45.44.164.152)

Logout

Diagnostics: Telegraf

ⓘ Telegraf Service

Version: 1.25.0-1

Running PID: 499895

🔗 InfluxDB Output

Enabled: Yes

URL: https://fdb01.puqpl

Bucket: puqvpncp

Organization: puqvpncp

📶 Inputs

Socket Listener: Active

HTTP Metrics: Active

📜 Telegraf Logs

100 lines

🔄

⏸

🗑

2026-03-11T22:19:10+01:00 dev.puqvpncp.com telegraf[471200]: 2026-03-11T21:19:10Z I! Loaded secretstores:
2026-03-11T22:19:10+01:00 dev.puqvpncp.com telegraf[471200]: 2026-03-11T21:19:10Z I! Loaded outputs: influxdb_v2
2026-03-11T22:19:10+01:00 dev.puqvpncp.com telegraf[471200]: 2026-03-11T21:19:10Z I! Tags enabled: host=dev.puqvpncp.com
2026-03-11T22:19:10+01:00 dev.puqvpncp.com telegraf[471200]: 2026-03-11T21:19:10Z I! [agent] Config: Interval:10s, Quiet:false, Hostname:"dev.puqvpncp.com", Flush Interval:10s
2026-03-11T22:19:10+01:00 dev.puqvpncp.com systemd[1]: Started telegraf.service - Telegraf.
2026-03-11T22:19:10+01:00 dev.puqvpncp.com telegraf[471200]: 2026-03-11T21:19:10Z I! [inputs.socket_listener] Listening on udp://127.0.0.1:8094
2026-03-11T22:32:30+01:00 dev.puqvpncp.com systemd[1]: Stopping telegraf.service - Telegraf...
2026-03-11T22:32:30+01:00 dev.puqvpncp.com telegraf[471200]: 2026-03-11T21:32:30Z I! [agent] Hang on, flushing any cached metrics before shutdown
2026-03-11T22:32:30+01:00 dev.puqvpncp.com telegraf[471200]: 2026-03-11T21:32:30Z I! [agent] Stopping running outputs
2026-03-11T22:32:30+01:00 dev.puqvpncp.com systemd[1]: telegraf.service: Deactivated successfully.
2026-03-11T22:32:30+01:00 dev.puqvpncp.com systemd[1]: Stopped telegraf.service - Telegraf.
2026-03-11T22:32:30+01:00 dev.puqvpncp.com systemd[1]: telegraf.service: Consumed 21.970s CPU time, 58M memory peak.
2026-03-11T22:33:01+01:00 dev.puqvpncp.com systemd[1]: Starting telegraf.service - Telegraf...
2026-03-11T22:33:01+01:00 dev.puqvpncp.com (telegraf)[499895]: telegraf.service: Referenced but unset environment variable evaluates to an empty string: TELEGRAF_OPTS
2026-03-11T22:33:01+01:00 dev.puqvpncp.com telegraf[499895]: 2026-03-11T21:33:01Z I! Starting Telegraf 1.25.0
2026-03-11T22:33:01+01:00 dev.puqvpncp.com telegraf[499895]: 2026-03-11T21:33:01Z I! Available plugins: 228 inputs, 9 aggregators, 26 processors, 21 parsers, 57 outputs, 2 secret-stores
2026-03-11T22:33:01+01:00 dev.puqvpncp.com telegraf[499895]: 2026-03-11T21:33:01Z I! Loaded inputs: http socket_listener
2026-03-11T22:33:01+01:00 dev.puqvpncp.com telegraf[499895]: 2026-03-11T21:33:01Z I! Loaded aggregators:
2026-03-11T22:33:01+01:00 dev.puqvpncp.com telegraf[499895]: 2026-03-11T21:33:01Z I! Loaded processors: starlark
2026-03-11T22:33:01+01:00 dev.puqvpncp.com telegraf[499895]: 2026-03-11T21:33:01Z I! Loaded secretstores:
2026-03-11T22:33:01+01:00 dev.puqvpncp.com telegraf[499895]: 2026-03-11T21:33:01Z I! Loaded outputs: influxdb_v2
2026-03-11T22:33:01+01:00 dev.puqvpncp.com telegraf[499895]: 2026-03-11T21:33:01Z I! Tags enabled: host=dev.puqvpncp.com
2026-03-11T22:33:01+01:00 dev.puqvpncp.com telegraf[499895]: 2026-03-11T21:33:01Z I! [agent] Config: Interval:10s, Quiet:false, Hostname:"dev.puqvpncp.com", Flush Interval:10s
2026-03-11T22:33:01+01:00 dev.puqvpncp.com systemd[1]: Started telegraf.service - Telegraf.
2026-03-11T22:33:01+01:00 dev.puqvpncp.com telegraf[499895]: 2026-03-11T21:33:01Z I! [inputs.socket_listener] Listening on udp://127.0.0.1:8094

Diagnostics: Telegraf — service status, InfluxDB config, inputs, logs

Service Info

Three cards are displayed:

Telegraf Service:

Field	Description
Version	Installed Telegraf version
Status	Running (with PID) or Stopped

InfluxDB Output:

Field	Description
Enabled	Whether InfluxDB output is enabled
URL	InfluxDB server URL
Bucket	InfluxDB bucket name

Field	Description
Organization	InfluxDB organization

Inputs:

Field	Description
Socket Listener	Whether the Unix socket input is active (receives metrics from PUQVPNCP)
HTTP Metrics	Whether the HTTP metrics endpoint is active

Telegraf Logs

Displays Telegraf service logs from `journalctl` with color coding:

- **Red** — Error messages (`|E|`)
 - **Yellow** — Warning messages (`|W|`)
 - **Gray** — Debug messages (`|D|`)
-

System

PUQVPNC

Dashboard

Networks

Clients

VPN Servers

Diagnostics

Settings

About us

☀️

🔍 Help

👤 admin (45.44.164.152)

🚪 Logout

Diagnostics: System

🕒 Uptime

23:17:41 up 7 days, 1:46, 3 users, load average: 6.51, 3.09, 1.38

💾 Memory

	total	used	free	shared	buff/cache	available
Mem:		7.86i	2.26i	328Mi	296Mi	5.86i
Swap:		0B	0B	0B		5.56i

💾 Disk Usage

Mounted on	Size	Used	Avail	Use%
/	31G	25G	4.1G	86%

🌐 Interfaces

lo	UNKNOWN	127.0.0.1/8 ::1/128
ens18	UP	77.87.125.201/25 77.87.125.200/25 fe80::2c30:5bff:fecc:4827/64
ens19	UP	
ens20	DOWN	
ens21	DOWN	
wgup1	UNKNOWN	192.168.123.2/32
wg51820	UNKNOWN	10.100.9.1/24
wg51825	UNKNOWN	10.100.13.1/24
wg51821	UNKNOWN	10.100.10.1/24
wg51823	UNKNOWN	10.0.0.1/24
wg51822	UNKNOWN	10.100.11.1/24
wg51824	UNKNOWN	10.100.12.1/24
wgup0	UNKNOWN	172.16.1.2/24
ovpn1197	UNKNOWN	10.0.0.254/24 fe80::df55:49b1:d735:c374/64
ovpn1196	UNKNOWN	10.100.11.254/24 fe80::ad5c:182c:7371:45a7/64
ovpn1198	UNKNOWN	10.100.12.254/24 fe80::a0ac:cf7d:9360:5aa2/64
ovpn1194	UNKNOWN	10.100.9.254/24 fe80::3ac3:4e20:6db5:28d8/64
ovpn1199	UNKNOWN	10.100.13.254/24 fe80::f739:964e:654b:2044/64
ovpn1195	UNKNOWN	10.100.10.254/24 fe80::c5b8:382a:638a:b5ff/64

📄 System Logs (puqvpncp)

100 lines

🔄 ⏸ 🗑

2026-03-11T23:17:16+01:00	dev.puqvpncp.com	puqvpncp[495129]:	[GIN]	2026/03/11 - 23:17:16	200		0.00.51000ms	45.44.164.152	GET	"/api/v1/diagnostics/logs/wireguard?lines=50"
2026-03-11T23:17:16+01:00	dev.puqvpncp.com	puqvpncp[495129]:	[GIN]	2026/03/11 - 23:17:16	200		1m7s	45.44.164.152	GET	"/api/v1/diagnostics/logs/wireguard?lines=50"
2026-03-11T23:17:18+01:00	dev.puqvpncp.com	puqvpncp[495129]:	[GIN]	2026/03/11 - 23:17:18	200	734.358136ms		45.44.164.152	GET	"/api/v1/diagnostics/logs/wireguard?lines=50"
2026-03-11T23:17:18+01:00	dev.puqvpncp.com	puqvpncp[495129]:	[GIN]	2026/03/11 - 23:17:18	200		1m6s	45.44.164.152	GET	"/api/v1/diagnostics/logs/wireguard?lines=50"
2026-03-11T23:17:19+01:00	dev.puqvpncp.com	puqvpncp[495129]:	[GIN]	2026/03/11 - 23:17:19	200	361.350008ms		45.44.164.152	GET	"/api/v1/diagnostics/logs/wireguard?lines=50"
2026-03-11T23:17:20+01:00	dev.puqvpncp.com	puqvpncp[495129]:	[GIN]	2026/03/11 - 23:17:20	200		1m5s	45.44.164.152	GET	"/api/v1/diagnostics/logs/wireguard?lines=50"

Diagnostics: System — uptime, memory, disk usage, interfaces

System Info Cards

Four cards are displayed:

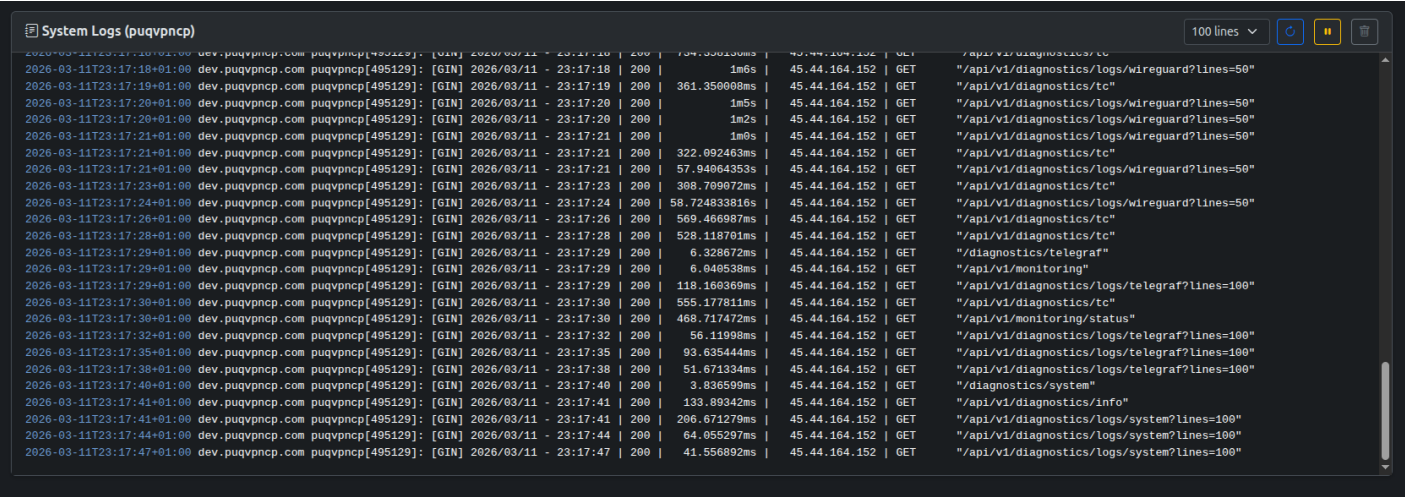
Uptime — output of the `uptime` command showing server uptime, number of users, and load averages.

Memory — output of `free -h` showing total, used, free, shared, buffers/cache, and available memory for both RAM and swap.

Disk Usage — output of `df -h` showing mounted filesystem, size, used space, available space, and usage percentage for the root partition.

Interfaces — output of `ip -br addr` showing all network interfaces with their status (UP/DOWN) and assigned IP addresses. Includes physical interfaces, WireGuard interfaces, OpenVPN tunnel interfaces, and upstream tunnels.

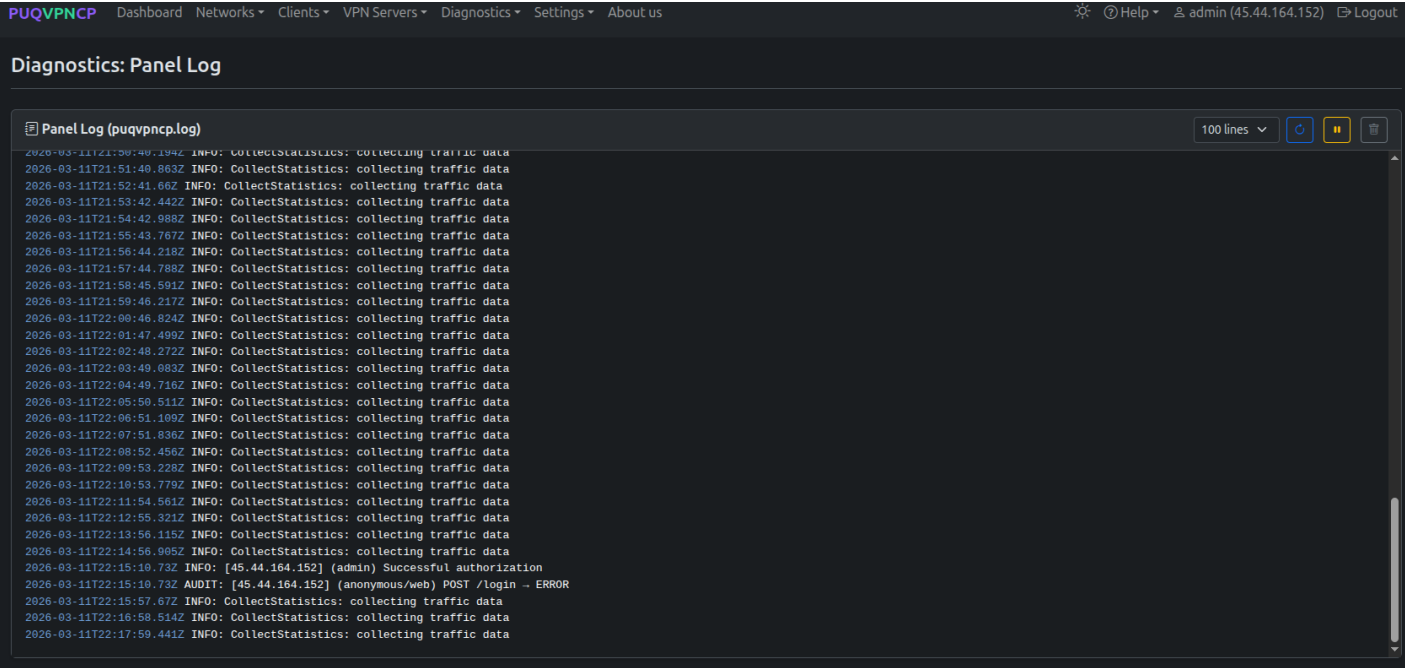
System Logs (puqvpncp)



Diagnostics: System — PUQVPNCP system logs

Displays PUQVPNCP service logs from `journalctl` (syslog tag `puqvpncp`). Shows application events such as API requests, system operations, network changes, and service lifecycle events.

Panel Log



Diagnostics: Panel Log — puqvpncp.log viewer

Displays the PUQVPNCP application log file (`puqvpncp.log`) in the configured `LogDir` directory, default `/var/log/puqvpncp/`.

This is the application's own log file (separate from `journalctl` system logs). Log entries are color-coded by level:

- **Red** — `ERROR:` messages

- **Yellow** — `WARN:` messages
- **Gray** — `DEBUG:` messages
- **Normal** — `INFO:` messages

The log format is: `timestamp LEVEL: message` (e.g., `2026-03-11T17:18:00.000Z INFO: ReloadNetworks: setting iptables`).

Integrity Check

PUQVPNCP

DashboardNetworksClientsVPN ServersDiagnosticsSettingsAbout us

⚙️ Helpadmin (45.44.164.152)Logout

Integrity Check

Summary

2529

Total

2529

OK

0

Failed

0

Fixed

0

Errors

0

Skipped

AllFailedFixedOKSkipped

Log

1420 / 1420 entriesAuto-scroll

Time	Status	Category	Network	Description	Detail
17:18:19	OK	System		IPv4 forwarding enabled	
17:18:19	OK	System		INPUT policy is ACCEPT	
17:18:19	OK	System		FORWARD policy is ACCEPT	
17:18:19	OK	System		OUTPUT policy is ACCEPT	
17:18:19	OK	System		system PUQVPNCP rule in INPUT	
17:18:19	OK	Global Rules		Peering rff A-B	
17:18:19	OK	Global Rules		Peering rff B-A	
17:18:19	OK	Global Rules		Isolation DROP (ipset)	
17:18:19	OK	ipset		ipset puq_vpn_nets exists	
17:18:19	OK	ipset	loadtest_net10	10.100.9.0/24 in ipset	
17:18:19	OK	ipset	loadtest_net14	10.100.13.0/24 in ipset	
17:18:19	OK	ipset	loadtest_net19	10.100.18.0/24 in ipset	
17:18:19	OK	ipset	loadtest_net6	10.100.5.0/24 in ipset	
17:18:19	OK	ipset	loadtest_net11	10.100.10.0/24 in ipset	
17:18:19	OK	ipset	loadtest_net17	10.100.16.0/24 in ipset	
17:18:19	OK	ipset	loadtest_net18	10.100.17.0/24 in ipset	
17:18:19	OK	ipset	loadtest_net2	10.100.1.0/24 in ipset	
17:18:19	OK	ipset	loadtest_net3	10.100.2.0/24 in ipset	
17:18:19	OK	ipset	public_ip	77.87.125.112/28 in ipset	
17:18:19	OK	ipset	Default	10.0.1.0/24 in ipset	

Last Run

Mode

audit

Started

3/11/2026, 4:34:34 PM

Duration

57s

Result

4026 OK, 0 failed, 0 fixed, 0 errors, 0 skipped

Integrity Check — summary, log table, and last run info

The Integrity Check performs a comprehensive audit of the entire PUQVPNCP system configuration. It verifies that all firewall rules, routing tables, ipset entries, traffic control classes, and network interfaces are correctly configured and match the expected state.

Running a Check

Two buttons are available in the page header:

Button	Description
Audit (magnifying glass)	Run a read-only audit — checks all rules and reports issues without making changes

Button	Description
Audit & Fix (wrench)	Run an audit and automatically fix any issues found

The check runs in the background. Results stream in real-time via Server-Sent Events (SSE), with automatic polling fallback if SSE disconnects.

Summary

The summary card shows counters for each check result:

Counter	Color	Description
Total	—	Total number of checks performed
OK	Green	Checks that passed
Failed	Red	Checks that failed (in audit mode, these need fixing)
Fixed	Yellow	Checks that were failed but successfully repaired (fix mode only)
Errors	Blue	Checks where the fix was applied but still failing
Skipped	Gray	Checks that were skipped (e.g., ipset not installed, mangle overflow)

A progress bar shows the proportion of each result type.

Filter Buttons

Filter the log table by status:

- **All** — show all entries
- **Failed** — show failed, fixed, error, and skipped entries (default)
- **Fixed** — show only fixed entries
- **OK** — show only passed entries
- **Skipped** — show only skipped entries

Log Table

Column	Description
Time	Timestamp of the check
Status	Result badge (OK / FAILED / FIXED / ERROR / SKIPPED)

Column	Description
Category	Check category (see below)
Network	Network and/or client name (if applicable)
Description	What was checked
Detail	Additional information (e.g., "Fixed", error message)

Check Categories

The integrity check performs 9 phases, covering all aspects of the system:

Category	Phase	What is Checked
System	1	IPv4 forwarding enabled, INPUT/FORWARD/OUTPUT chain policies, system_PUQVPNCP rule
Global Rules	2	Pre-filter rules, peering ACCEPT rules (A→B, B→A), intra-network ACCEPT, isolation DROP (ipset), post-filter rules
ipset	3	<code> puq_vpn_nets </code> ipset exists, each network subnet is a member
Chains	4	Per-network chains exist in filter (<code> PQ_ </code>), nat SNAT (<code> PQN_ </code>), nat DNAT (<code> PQD_ </code>), mangle (<code> PQM_ </code>) — plus jump rules from built-in chains
NAT	5	SNAT rules for each network's upstream IP
Mangle	5	Per-client mangle marks for download (dst) and upload (src) traffic
Network Rules	5	Route ACCEPT rules for custom routes
Policy Routing	6	Upstream WG tunnel <code> ip rule </code> / <code> ip route table </code> , WG/OpenVPN fwmark-based policy routing
CONNMARK	7	WG and OpenVPN CONNMARK rules in PREROUTING (mangle)
Traffic Control	8	Root HTB qdisc on gateway, VPN, and upstream interfaces; per-client TC classes
Interfaces	9	WireGuard interfaces are UP, upstream WG tunnel interfaces are UP

Last Run

The **Last Run** card shows information about the most recent integrity check:

Field	Description
Mode	<code>audit</code> or <code>fix</code>
Started	When the check started
Duration	How long the check took
Result	Summary of OK, failed, fixed, errors, and skipped counts

--

Revision #6
Created 28 September 2026 17:06:12 by Ruslan
Updated 28 September 2026 18:58:44 by Ruslan