



AEGISTRACE

INTELLIGENCE

User & Administrator Guide

Features, sign-in and step-by-step workflows

Contents

- Part 1: Signing in and getting started (everyone)
- Part 2: Features and how to use them (investigators and analysts)
- Part 3: Administration (administrators)
- Part 4: Data sources, statuses and limits
- Part 5: Quick reference

What AegisTrace is

AegisTrace is a blockchain investigation workstation. It looks up wallets and transactions on live networks, follows funds across bridges, checks risk and sanctions, monitors wallets in real time, and packages findings into cases, evidence and reports. Every result shows where it came from. If a source is missing, rate-limited or not set up, the app says so instead of guessing.

Part 1: Signing in and getting started

1.1 Before your first sign-in

Access is invite-only. Your administrator creates your account, chooses your role and gives you a sign-in email and a starting password. Open sign-up is not available.

1.2 Sign in

1. Open the AegisTrace address your administrator gave you. You'll see the **Sign in to the investigation workstation** page.
2. Enter your email and password, then click **Sign in**. Five wrong attempts lock sign-in for 15 minutes.
3. Change your starting password with the **key icon** at the top right (minimum 12 characters).
4. You land on the **Command Center**. On your first sign-in a short **welcome guide** opens. Click **Next** to go through it, or close it.

1.3 If sign-in fails

Message	What it means	What to do
Email or password is incorrect	The details don't match an account	Check spelling; ask your administrator to reset your password
Too many failed sign-in attempts	5 wrong passwords in a row	Wait 15 minutes, then try again
Account suspended	An administrator disabled your access	Contact your administrator
Session invalid / expired	You were signed out or the session timed out	Sign in again

1.4 Find your way around

- **Left sidebar:** four groups (Investigate, Intelligence, Casework, Platform). You only see pages your role allows.
- **Top search bar:** press **/** (or Ctrl/Cmd+K) and paste any address, transaction hash, block, entity or case.
- **Top right:** your name, role and organisation, the **?** button to reopen the welcome guide, and the sign-out button.
- **Status badges:** VERIFIED LIVE (checked against the live source), CREDENTIALS REQUIRED (a key is needed), PARTIALLY IMPLEMENTED (works with stated limits).

Part 2: Features and how to use them

For investigators and analysts.

Universal Search

Finds the right view for any identifier and detects which networks an address is valid on.

1. Paste the value into the top search bar and press Enter.
2. If the address fits several networks (for example 0x addresses), pick the network.
3. Open the result: wallet, transaction, block, entity or case.

Wallet Intelligence

Shows balance, tokens, transfers with dollar value at the time, named counterparties (Chainalysis and other sources) and a risk summary.

1. Open **Wallet Intelligence**, choose the network and paste the address.
2. Read the banner: entity name, category and risk if known.
3. Scroll transfers; click a counterparty to pivot, or **Graph** to see flows.
4. Use **Add to case** or **Watch** to keep track of it.

Transaction Explorer

Decodes a transaction: transfers, tokens, fees, status, and any bridge or swap activity.

1. Paste the transaction hash and choose the network.
2. Check each transfer with its dollar value.
3. If a bridge is detected, click through to Cross-Chain Tracing.

Fund Flow Graph

Interactive map of where funds came from and went. Nodes show entity names and categories; high-risk nodes have an amber border.

1. Open a wallet and click **Graph**, or open Fund Flow Graph and enter an address.
2. Click a node to expand its next hop.
3. Use the tracing tools: shortest path, distance to risk, multi-path and peel-chain detection.
4. Use **Demixing** for mixer deposits (EVM) or CoinJoin transactions (Bitcoin and Litecoin).

Cross-Chain Tracing

Decodes bridge transfers and shows the matching transaction on the destination chain when it can be proven (Across, deBridge, Celer, Axelar, Chainlink CCIP, Optimism/Base, Hop, Synapse; Wormhole and others where supported).

1. Enter the source-chain transaction hash.
2. Read the protocol, destination chain, recipient and destination transaction.
3. The confidence column says whether the link is deterministic or a lead.

DEX & Swap Intelligence

Decodes token swaps inside a transaction (pools, tokens in and out).

1. Paste the transaction hash; review each swap leg.

Entity Intelligence & Wallet Clustering

Named entities and groups of wallets likely controlled together, with the evidence for each link.

1. Search an entity or open a cluster.
2. Confirm, reject or split clusters. A short justification is required and recorded.

Risk Intelligence

Combines Chainalysis screening, Chainabuse reports, GoPlus, open scam lists, sanctions and behaviour patterns into an explained score.

1. Enter an address and run the assessment.
2. Read each factor and its source; check data completeness.
3. If you disagree, use **Override**, choose a status and give a justification. Overrides are audited.
4. Use exposure, alert rules and blocklists from the same page.

Sanctions Screening

Checks addresses and names against OFAC, EU, UK and UN lists (refreshed daily).

1. Enter an address or a person/organisation name.
2. Matches show which list matched and the list entry.

P2P Intelligence

Looks at peer-to-peer trading patterns in public on-chain data. It does not identify traders.

1. Enter an address and review the pattern indicators.

Monitoring & Alerts

Watched wallets raise alerts the moment they move (instant provider webhooks where available, otherwise polling).

1. Add an address to a watchlist.
2. Alerts appear in the list and by email; linked Telegram users also get them in chat.
3. Acknowledge, assign (enter a colleague's email) or close alerts.

Telegram field checks

Run quick checks from your phone.

1. On **Data Provider Management**, click **Link my Telegram**.
2. Send the code shown (for example /link AB12CD34) to the AegisTrace bot within 10 minutes.
3. Send **/check ADDRESS** (optionally followed by the network). Send **/unlink** to remove the link.

AI Assistant

Answers questions about your investigation data and explains findings. Always confirm against the source data.

1. Type a question; open the cited records.

Investigation Cases

Your workspace for an investigation: subjects, notes, tasks, linked wallets and cross-chain links.

1. Create a case and add subjects (wallets, transactions).
2. Add notes and tasks; mention colleagues to notify them (Mentions).

Evidence Vault

Saves evidence with a SHA-256 fingerprint, a chain of custody, a Bitcoin timestamp (OpenTimestamps) and a write-once copy in Cloudflare R2 (cannot be changed or deleted for 7 years).

1. From a case, save a result or upload a file as evidence.
2. Use **Verify integrity** to check the stored copy, the write-once copy and the custody chain.
3. Use **Transfer custody** and give the reason.
4. After a few hours, the Bitcoin timestamp is confirmed; download the proof file.

Forensic Reports

Generates a report from a case for review and approval.

1. Generate the report, submit for review, then a reviewer approves or returns it with comments.

OSINT & IP Search

IP lookups (location, network owner, VPN/Tor flags, AbuseIPDB score) and automatic scans every 6 hours of GitHub, Bluesky, Hacker News, the Ahmia darknet index and Telegram (once connected).

1. Search an IP, city or country.
2. Add addresses to the scanner; review mentions as they come in.

VASP Directory & Intelligence Sources

Exchange/VASP contacts and information-request drafts; the list of sources behind every finding.

1. Pick a VASP, generate an information-request draft, download and send it through your legal process.

Part 3: Administration

For administrators. Requires the Administrator or Super Administrator role.

Invite users and set roles

Only accounts created by an administrator can sign in.

1. Open **Administration**.
2. Invite the person's email and choose a role, then click **Set password** on their row and share the starting password securely.
3. Change roles, reset passwords or suspend users here; every change is recorded in the Audit Center.

Data provider keys

Keys are stored encrypted on the server and never shown in the browser.

1. Open **Data Provider Management**.
2. Find the provider, paste its key and click **Save**.
3. Click **Test**: the badge turns VERIFIED LIVE when the live check passes.

Telegram bot and channel search

Connect the bot and the channel scanner.

1. In the **Telegram & evidence storage** panel, click **Connect bot** (or **Reconnect to this site** after publishing a new address).
2. For channel search, enter the phone number of the Telegram account to use, then the login code (and 2-step password if set).
3. Join public channels to monitor from the same panel.

Write-once evidence storage

Shows whether the 7-year bucket lock is active.

1. Check the badge is VERIFIED LIVE. If it shows NOT LOCKED, click **Apply bucket lock**.

Monitoring health and audit

Keep the platform trustworthy.

1. **System Health**: provider status, latency and worker state.
2. **Audit Center**: every sign-in, search, change and export.
3. **Compliance & Readiness**: what is verified and what still needs independent validation.

Part 4: Data sources, statuses and limits

Area	Sources	Limits
Blockchain data	Etherscan, Alchemy, Helius, TronGrid, Blockfrost, Subscan via PubFi, toncenter, public RPCs and explorers (37 networks)	Free tiers can be slow under heavy use
Attribution & risk	Chainalysis screening, Chainabuse, GoPlus, open scam lists, behaviour heuristics	Wallets unknown to these sources stay unlabelled
Sanctions	OFAC, EU, UK, UN (daily)	Name matches need analyst review
Prices	DefiLlama (value at transfer time)	Some small tokens have no price
OSINT	GitHub, Bluesky, Hacker News, Ahmia, Telegram (joined chats), AbuseIPDB, ipwho.is	No X/Twitter or Reddit; darknet = search index only
Evidence	MongoDB working copy + Cloudflare R2 write-once copy + OpenTimestamps	Not certified for court use without independent validation

Results labelled as leads (for example CoinJoin change outputs or heuristic clusters) are investigative leads, not proof. Corroborate before acting, and follow your legal process for any request to an exchange.

Part 5: Quick reference

I want to...	Go to
Look up anything	Top search bar (press /)
See where money went	Fund Flow Graph
Follow a bridge transfer	Cross-Chain Tracing
Check if an address is risky	Risk Intelligence
Check sanctions	Sanctions Screening
Get alerted when a wallet moves	Monitoring & Alerts
Check from my phone	Telegram bot: /check ADDRESS
Save proof	Evidence Vault
Write the report	Forensic Reports
Add a key / connect a service	Data Provider Management (admins)
Invite a colleague	Administration (admins)
See the welcome guide again	? button, top right