

MKT MINING SUITE

User Manual

Lite quick start and Full edition operating guide

READ FIRST	MKT Mining Suite is local mining-control and telemetry software. It does not promise income, offer investment advice, custody funds, hold wallet private keys, or ask for seed phrases.

Edition-aware • CoinPack-guided • Local-first

Version 1.0 | Customer release guide

How to use this guide

This manual is arranged in short, searchable sections. In Word, open the Navigation Pane or press Ctrl+F to jump to a named feature such as “ASIC,” “Pool,” “RPC,” “Node,” “CoinPack,” “Loki,” or “Alfred.”

The Lite quick-start appears first. The Full edition chapters then explain fleet, ASIC, pool, explorer, RPC, and node workflows. Menus can change slightly between releases; follow the described purpose if a label is shortened or repositioned.

Contents

1	Before you mine	11	Add and connect a node
2	Choose Lite or Full	12	Configure an RPC endpoint
3	Lite quick start	13	CoinPack management
4	Core concepts	14	Fleet topology and telemetry
5	Full edition overview	15	Loki Guardian
6	Build a coin profile	16	Alfred AI and microphone
7	Add a CPU/GPU computer	17	Phone and QR
8	Add an ASIC miner	18	Troubleshooting
9	Configure mining pools	19	Security and privacy
10	Configure explorers	20	Glossary and support

1. Before you mine

Mining uses your computer or dedicated hardware to perform work for a blockchain network. MKT helps you choose reviewed configuration data, start or observe supported mining lanes, and understand current telemetry. It cannot guarantee a reward, a payout, an exchange value, or that a particular coin will remain mineable.

REALITY CHECK	A faster computer can contribute more hash rate, but more hash rate does not automatically mean more profit. Results can change with network difficulty, pool rules and fees, uptime, share quality, electricity cost, hardware efficiency, coin price, liquidity, and market conditions.

Make an informed decision

Check	Why it matters	What MKT can show
Hardware and cooling	A CPU, GPU, or ASIC has a finite supported algorithm and power draw. Heat and noise can matter as much as speed.	Active lane, hardware telemetry, temperatures, fans, power when reported.
Electricity cost	Energy use may exceed the value of rewards. Use your actual rate rather than an assumed rate.	Estimated electricity and net figures only when an authoritative power reading and your rate are available.
Coin and network	Difficulty, rules, development, market price, liquidity, and security are external to MKT and can change.	CoinPack compatibility, network data and supported telemetry—not a price or profit promise.
Pool and wallet	Payout thresholds, fees, worker names, and address/network compatibility affect whether an earned share becomes a payout.	Pool reachability, submitted/accepted evidence, and a public payout address you provide.

Research before starting

- Read the coin’s official documentation, confirm its network and address format, and understand whether the algorithm is compatible with your hardware.
- Review the pool’s payout method, minimum payout, fees, terms, and status page. A pool route can be reachable while payouts are delayed or subject to its own rules.
- Use an explorer only after confirming that it serves the selected coin and network. A balance or transaction shown on a different network is not a confirmation of your expected payout.
- Avoid claims of guaranteed yield, “risk-free” mining, or requests for a seed phrase. MKT never needs your private key, seed phrase, or exchange password.

Digital-asset values can be volatile and mining can be unprofitable. The U.S. CFTC advises people to research digital assets carefully and be skeptical of guarantees. This guide is operational information, not legal, tax, financial, or investment advice.

2. Choose Lite or Full

Your activation receipt determines the available edition. The interface may show Full-only pages in Lite so you can see the broader product, but those pages remain unavailable until Full is activated.

Capability	Lite	Full
Local CPU/GPU miner	One computer: the computer running Lite.	Supported local CPU/GPU lanes, plus fleet context.
ASIC monitoring	Not available.	Available: private-LAN or approved private-route read-only enrollment.
All Miners and fleet topology	Not available.	Available for saved systems and eligible telemetry sources.
Node and RPC views	Not available.	Available for reviewed, private node and RPC telemetry paths.
Loki Guardian and Alfred AI	Available for the local computer.	Available with broader supported system context.
Phone / QR	Available.	Available.

Activation and account safety

A customer activation receipt is tied to the installation and is checked locally and with MKT's entitlement service when required. Keep it private and do not post it in a screenshot. A trial or purchased entitlement is not transferred by copying program files to a second computer.

3. Lite quick start

Lite is a focused one-computer mining experience. Use it when you want one supported CPU or GPU lane on the computer that is running MKT, with local Loki Guardian, Alfred AI, and Phone / QR features.

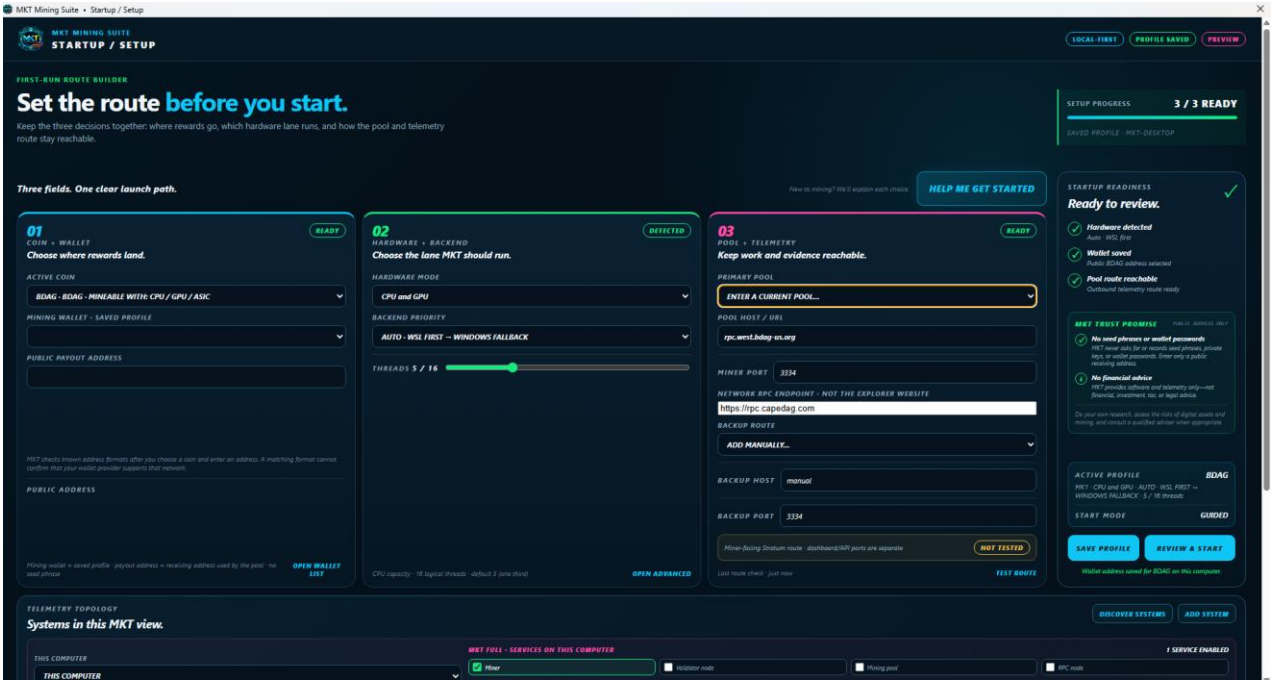


Figure 1. The guided setup selects a coin, a local mining path, and the configuration needed to begin.

First-run sequence

1. Install from the official delivery link. Use the signed installer supplied by MKT. Windows should display the expected publisher for the release. Do not install a package from a file-sharing link or an unknown signer.

2. Open MKT and claim your edition. Choose Lite, then complete the trial or enter the activation receipt associated with this computer. Keep the receipt private.

3. Select a coin. Customer releases begin with no default coin. Choose a reviewed CoinPack profile or add a supported profile. Each coin keeps its own wallet, pool, explorer, and history—nothing is copied automatically between coins.

4. Add a public payout address. Paste only the public receiving address for the selected coin and network. Verify it one character at a time or by a trusted QR source. Never paste a seed phrase, recovery phrase, or private key.

5. Review the pool and explorer. Use the CoinPack-provided pool and explorer only after confirming they match your selected coin. Where no reviewed explorer is needed, leave it as none. See Chapters 9 and 10 for the difference.

6. Save Profile and Start. Save the per-coin configuration, then start the supported CPU/GPU path. MKT first reports a progress state while it prepares the worker and waits for a job. It shows mining only after the worker is live.

7. Watch the first evidence. Check that the pool route is reachable, hash rate is appearing, and submitted/accepted share data is being received. A fresh miner may need time to receive a job or accumulate pool-side share evidence.

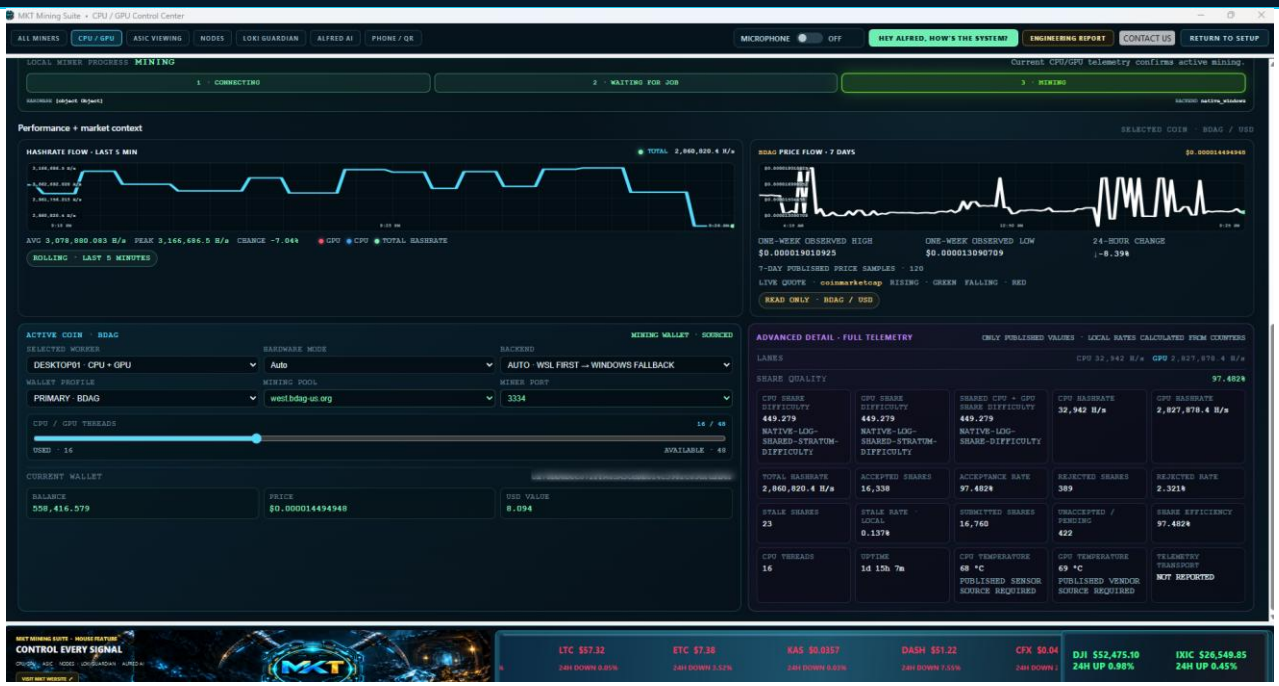


Figure 2. Lite uses the same current CPU/GPU operational surface as Full, restricted to the local computer.

What you should see

- Current mining state: stopped, starting, waiting for job, mining, or a clear runtime/pool condition.
- Hash rate and hardware context: live values when the miner reports them, not made-up zeros.
- Share evidence: submitted, accepted, rejected, and stale information when the pool or miner makes it available.
- Pool route and latency: a connection check, not a promise of a payout.

IF SOMETHING IS BLANK	“Not reported” means MKT has not received that field from the current miner, pool, or telemetry source. It does not mean a value of zero.

4. Core concepts

Term	Plain-language meaning	Do not confuse it with
Hash rate	The speed at which a miner performs the selected work. It can move up and down.	A guaranteed payout, coin price, or total wallet balance.
Share	A unit of work a pool can use to measure contribution. Pool rules decide acceptance and payout credit.	A blockchain block or an immediate wallet deposit.
Mining pool	A service that gives work to miners and applies its own accounting and payout rules.	An explorer, wallet, or node.
Explorer	A public or approved network viewer for blocks, addresses, and transactions.	A mining pool, wallet, or private node.
RPC endpoint	A controlled interface used by software to query a node or service.	A public website or a pool endpoint.
Node	Software that participates in a blockchain's network and may maintain/sync chain data.	A mining worker; running a node does not automatically mine.
ASIC	Dedicated mining hardware. MKT reads eligible telemetry through a private route.	A CPU/GPU worker installed on your desktop.
CoinPack	Reviewed, signed configuration metadata for coins and compatibility lanes.	An untrusted executable downloader or a wallet.

The recommended operating order

Pick a coin first. Then use the CoinPack profile to select a compatible hardware lane, public wallet address, pool route, and optional explorer. Start one miner, verify live evidence, and only then add ASICs, remote miners, RPCs, or nodes. This keeps the source of each measurement understandable.

5. Full edition overview

Full keeps the Lite CPU/GPU controls and adds a topology for saved computers, eligible ASICs, node/RPC telemetry, and All Miners. Full does not turn MKT into a public scanner or a remote-control tool for equipment you have not explicitly added.

Before you add another system

- Use an approved private path: the same private LAN or an approved Tailscale route. Do not open a public port simply to make a system visible.
- Make sure the target device is powered on, reachable, and running the required MKT telemetry service when it is an MKT-managed computer.
- For an ASIC, enable only the vendor's local read-only status API if its firmware requires it. MKT does not need to be installed on the ASIC.
- For a node, ensure the node is actually running and its local/read-only RPC interface is reachable from the MKT computer. A planned profile is telemetry-only; it never starts a coin node.

PRIVATE BY DESIGN	Discovery is bounded to the computer or private route you choose. MKT does not scan the public Internet, open public ports, change pool settings, reboot equipment, or invent a supported protocol.

6. Build a coin profile

A coin profile is a separate workspace for one coin. It prevents the common mistake of mixing a wallet or pool from one network with another. The customer release starts neutral: no coin, wallet, pool, or explorer is preselected.

Create or update a profile

1. Open setup or the Coin Pack Manager. Choose the coin you want to configure. Import the current CoinPack only from an official MKT delivery location, then let MKT verify it before use.

2. Confirm compatibility. Read the profile's hardware lane, algorithm, and readiness status. A visible catalog entry can be research-only or monitor-only; only a reviewed path with the required verified engine can be started.

3. Set the public wallet address. Enter the address for this coin and this network. MKT stores the public payout address and per-coin configuration, never your private key or recovery phrase.

4. Accept or edit the pool route. Use the reviewed CoinPack default when one is supplied, or add a verified custom route. Store a backup only if you understand the pool's terms and it accepts the same coin/algorithm.

5. Set an explorer only when needed. Choose the reviewed explorer for the selected network or leave it blank when none is needed. An explorer is optional and does not prove mining or payout by itself.

6. Save before starting. MKT writes the profile under the selected coin. Switching coins later does not overwrite the current coin's wallet or pool settings.

7. Add a CPU/GPU computer

In Full, a remote MKT computer can be added to the saved system view after it is both visible on an approved private route and publishing MKT telemetry. This avoids creating a topology entry from a mere IP address that cannot supply operating evidence.

Discovery and enrollment

1. Prepare the target. Install and run the supported MKT service on the target computer. Start its local miner only after it has its own saved coin profile.

2. Confirm the private path. Verify the target is online and reachable through the same private LAN or approved Tailscale route. Tailscale must be connected on both applicable devices.

3. Use Discover Systems. From the topology/setup screen, run discovery. Review each candidate's identity, route, and telemetry status rather than selecting every address returned.

4. Add the verified system. Choose the candidate only once the MKT service is reachable and live telemetry is present. Save it to the MKT system view.

5. Validate the topology. The saved computer should appear in Systems and Trusted Paths with its device name, route, and readiness. If the device later restarts, its stable MKT identity should keep it visible rather than producing duplicates.

When discovery does not find a computer

- Check that Tailscale is connected and the target's route is still approved. Turning it off interrupts private reachability even if mining continues locally.
- Confirm the MKT telemetry service is running on the target and that a local firewall is not blocking its approved private path.
- Use the device name and telemetry identity, not an old IP address alone, to decide whether it is the same saved system.

8. Add an ASIC miner

ASIC enrollment is read-only. MKT identifies an ASIC through a private LAN or approved Tailscale route and reads eligible status telemetry. It does not change the ASIC's pool settings, reboot it, or expose its management API to the public Internet.

ASIC enrollment workflow

1. Open Setup and choose Add System. Select the ASIC service role.

2. Choose the route. Choose Private LAN for a miner on the local network, or Tailscale for an ASIC reachable through the approved tailnet.

3. Enter the destination. Enter the ASIC hostname or private IP address. The address is a route, not its permanent identity.

4. Set the read-only endpoint. Leave the ASIC API endpoint blank for bundled read-only probing, or enter a verified endpoint such as cgminer://private-host:4028 or http://private-host:80. Never use a public IP or public port-forwarding rule.

5. Add model details when known. Vendor, model, firmware, serial, DNA, or MAC can help MKT match a model-specific adapter. MKT prefers values reported by the read-only API when available.

6. Check Node. Review detected identity and adapter status. A stable serial, DNA, MAC, or MKT source identity keeps the miner from duplicating after DHCP changes its IP address.

7. Save the enrollment. Save the miner and, if offered, create a pairing code for the mobile viewer. The ASIC should now be visible in the Full topology and All Miners view.

Adapter status

Status	Meaning	What to do
Verified	The bundled read-only adapter and telemetry mapping are approved for the protocol or model family.	Use available telemetry; verify its status against the ASIC's own local page.
Provisional	The vendor API is known but the exact firmware or model needs fixture validation.	Keep it enrolled and review what is actually reported.
Manual	MKT can retain identity and route but has no supported telemetry mapping.	Do not expect invented values; request adapter review if needed.
Unknown	No bundled adapter matches the reported identity.	Confirm model/firmware and do not open the ASIC to the Internet to troubleshoot.

MKT only shows fields the device provides: for example hash rate, temperature, fan, power, share data, difficulty, uptime, pool/worker identity, firmware, or hardware errors. Missing fields display as Not Reported rather than a guessed zero.

9. Configure mining pools

A mining pool distributes work and applies its own rules for shares and payouts. MKT can configure and test an eligible pool route for a selected mining profile, but the pool—not MKT—decides share credit, payout timing, and payment eligibility.

Pool setup workflow

1. Start with the coin profile. Select the coin, hardware lane, and public wallet address before adding a pool. Never use a pool for another coin or incompatible algorithm.

2. Use CoinPack guidance when available. The CoinPack may provide a reviewed default pool and port for the coin. Review the actual pool's terms and current status before relying on it.

3. Enter the route precisely. Enter the protocol, host, and port exactly as supplied by the pool. A CPU/GPU profile may separate host and port; an ASIC may use a Stratum URI. Follow the field format shown by your chosen profile.

4. Set a backup route deliberately. A backup is optional. It should be for the same coin and compatible algorithm. Test it before considering it a recovery path.

5. Test Route. Test reachability from your MKT computer. A successful test confirms the route can be reached; it does not prove your wallet is valid or that a payout has occurred.

6. Start and verify evidence. Once the worker receives a job, watch current hash rate, submitted shares, accepted/rejected/stale information, and pool latency where reported.

Reading share data

- Submitted shares are work reports sent by the miner. Accepted shares are reports the pool or miner has confirmed. Rejected or stale shares are separate categories when available.
- An acceptance rate needs a meaningful denominator. MKT should show unavailable or pending rather than a misleading percentage when the pool has not sent enough data.
- A temporarily stale telemetry reading may still be useful as the last known value if the miner is operating; a fresh boot with no live report should instead say it is waiting for current data.

NEVER ENTER SECRETS	A pool may offer a worker name or public payout address field. MKT does not need a wallet seed phrase, private key, or exchange password. Treat any website requesting one as unsafe.

10. Configure explorers

An explorer is a network viewer. It can help you inspect public chain information, addresses, blocks, and transactions. It is not your mining pool, it is not your wallet, and it does not itself make your miner work.

Explorer setup workflow

1. Select the coin profile. Confirm the exact coin and network. Testnet, mainnet, sidechain, and similarly named coins can use different explorers and address rules.

2. Accept reviewed guidance or enter a verified endpoint. Use the CoinPack's reviewed explorer when listed. If none is listed or no explorer is needed, leave the field empty rather than reusing an unrelated URL.

3. Check the address independently. Open the explorer and check the public address only after confirming its network. Never type private keys, seed phrases, or recovery phrases into an explorer.

4. Separate mining evidence from chain evidence. Use the miner/pool telemetry to understand active work and shares. Use the explorer to inspect public chain data and confirmed on-chain events. A pool payout may not appear until the pool issues it.

Common mistakes

- Using a dashboard or RPC URL as an explorer URL.
- Expecting an explorer to show a pool balance before the pool has paid out on-chain.
- Using an explorer for the wrong network and assuming a zero balance means the address is invalid.

11. Add and connect a node

A node is separate from a miner. It participates in a blockchain network and can maintain or serve chain information. In Full, MKT can add and monitor reviewed node/RPC telemetry paths. It does not make an unreviewed node runnable, download arbitrary node software, or start a profile marked planned.

Node prerequisites

- Install and operate the coin's official node software according to that project's documentation. Confirm its disk, CPU/RAM, bandwidth, synchronization, update, and firewall requirements yourself.
- Keep the node's data directory coin-specific. A node profile must not contain wallet private keys.
- Use a private path: a local listener, private LAN, or approved Tailscale route. Do not publish a node RPC endpoint to the Internet for MKT discovery.
- Confirm that the selected CoinPack or bundled node profile has a reviewed adapter. A planned profile is telemetry-only and cannot be started by MKT.

Attach an existing node

1. Choose Full and select the coin. Open the Nodes or topology area, then select the coin whose node you already operate.

2. Add System and select Node. Enter the private hostname or IP address for that node. Select its approved private route.

3. Use reviewed connection hints. Accept the CoinPack/bundled profile's protocol, port, and read-only health checks when offered. These hints contain no hostnames or credentials and are applied only to the host you chose.

4. Check Node. MKT sends only fixed, read-only health/synchronization checks supported by the installed adapter. It can report identity, reachability, sync/tip information, and adapter status when the node responds.

5. Save and observe. Save the node to topology. Verify that its state is synchronized or progressing before treating it as a dependable source of chain context.

What node discovery does—and does not—do

MKT tries known read-only adapter, port, and path hints on the specific private host you choose. If they do not respond, it can use bounded built-in read-only fallback probes. It does not scan a LAN, start/stop a coin node, alter node configuration, or run arbitrary RPC methods from a CoinPack.

12. Configure an RPC endpoint

RPC (remote procedure call) is the controlled interface through which MKT can query a node or compatible service. It is often used for health, sync, and chain context. It is not the same thing as an explorer page or a mining pool route.

Safe RPC workflow

1. Start with a live node. Confirm the node is already installed, running, and synchronized or actively synchronizing. MKT does not install a missing node through the RPC screen.

2. Use a private endpoint. Enter a local/private hostname and reviewed port/path. Do not use a public endpoint unless your organization has separately designed, secured, and approved it for that purpose.

3. Prefer CoinPack or bundled node defaults. If the current coin profile supplies a reviewed RPC contract, use it. It describes a protocol, default port, and named read-only health checks—not credentials or executable code.

4. Validate before saving. Run Check Node or the equivalent route test. Review the adapter state and expected sync/health information. If no supported adapter is present, keep the route untrusted and do not force an arbitrary method call.

5. Limit exposure. Bind a node RPC service to localhost or a private network according to the node project's documentation. Limit firewall rules and Tailscale ACLs to the devices that actually need access.

Credentials and sensitive data

MKT's reviewed CoinPack contracts intentionally contain no RPC hostnames, credentials, or arbitrary method names. If your own node uses local authentication, keep those credentials out of screenshots, public documentation, and chat messages. Never substitute a wallet private key or seed phrase for a node password.

13. CoinPack management

A CoinPack is a reviewed data package that describes coin compatibility: hardware lanes, algorithms, profile versions, pool defaults, explorer guidance, node/RPC hints, and readiness states. It is not a wallet, a promise of a mining return, or a source of arbitrary executables.

Import and update

1. Get the pack from MKT. Use the official website or release channel. Do not import a CoinPack from a random community link.

2. Let MKT verify it. The manager checks payload checksums, rejects unsafe archive paths, and stages the package before applying it. Runnable profile changes require the trusted publisher signature.

3. Review the status. A listed coin can be reviewed/runnable, adapter-ready, research, planned, or monitor-only. Only a supported profile with a verified local engine becomes a startable mining path.

4. Apply without losing settings. A valid profile update preserves coin-specific wallets, settings, telemetry history, activation, and support records. If a validation or smoke check fails, use the rollback snapshot rather than editing the package manually.

How engines are handled

CoinPack configuration and mining engines are deliberately separate. If a coin needs a new executable, MKT uses a separately signed, versioned, hash-pinned, platform-specific engine bundle. The suite must verify it before installation; a CoinPack cannot drop an executable into the application on its own.

NO DEFAULT COIN	A neutral customer release opens without a preselected coin, pool, explorer, or wallet. The CoinPack gives you reviewed information to make an intentional choice; it does not choose on your behalf.

14. Fleet topology and telemetry

The Full topology is a visual list of saved systems and their trusted private paths. It is designed to make real, enrolled equipment visible—not merely technically reachable in the background.

Reading the topology

Element	Meaning	Operator action
Systems list	The saved local computer, enrolled ASICs, and verified remote MKT computers.	Confirm each item has a recognizable name, route, role, and readiness state.
Trusted Paths	The specific local, private-LAN, or approved tailnet path used for telemetry.	Check the route before assuming a device has failed.
Primary source	The system currently selected for a focused view.	Change it when you need to inspect a different computer or device.
Fleet / saved systems view	Combined context from enrolled devices.	Use it for operations; use individual views to diagnose a single source.
Not current	MKT has a saved identity but no fresh telemetry receipt in the current window.	Check power, private route, Tailscale/service status, then refresh. Do not replace the device solely because its IP changed.

Totals and freshness

A total hash rate should add the current or valid-last-known hash rate of the eligible operating miners in the selected scope. A new boot with no telemetry yet should be marked waiting for current data rather than treated as an arbitrary zero. A stale device that is confirmed stopped should be reported as stopped, not counted as mining.

If a saved device disappears

- Refresh telemetry, then confirm the device is online and its private route is connected.
- For a Tailscale device, confirm Tailscale restarted after any temporary disconnect and that the MKT telemetry service is still running.
- Use the stable MKT source identity, serial/DNA/MAC, or device name to merge a returning device; do not create unnecessary duplicates from a changed IP address.

15. Loki Guardian

Loki Guardian presents local protection, recovery, storage, pool reachability, and operating signals in readable terms. It helps you identify conditions that deserve attention; it does not silently repair hardware, change a pool, or move funds.

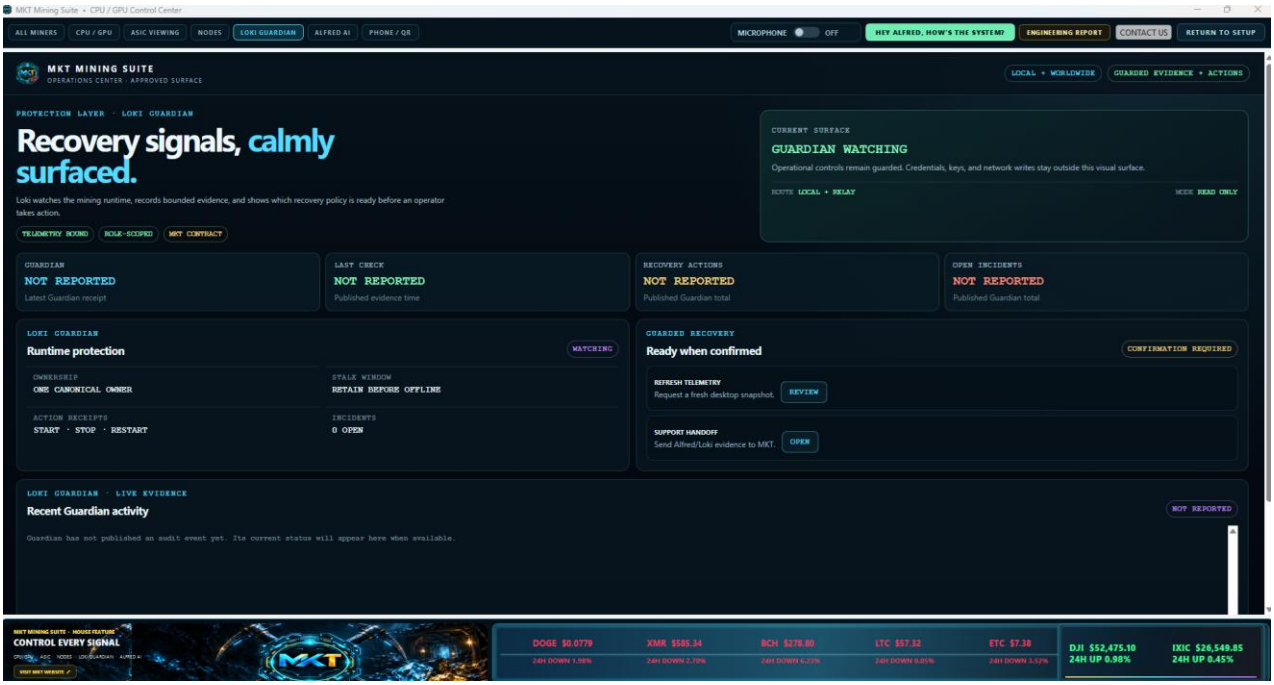


Figure 3. Loki Guardian keeps local recovery and protection signals close to the current miner.

- Review the most recent status, the evidence time, and the recommended next check before assuming a warning is current.
- If storage, connectivity, or a pool route is degraded, use the shown evidence and the support-report path rather than restarting equipment repeatedly.
- Treat a protection status as operating context, not a guarantee against hardware failure, account compromise, fraud, or loss.

16. Alfred AI and microphone

Alfred is a read-only operations assistant. It explains the latest MKT telemetry for the selected scope, such as live miner state, current or valid-last-known hash rate, temperatures when reported, and active warnings. It cannot control the miner or access a wallet's private key.

- Use text whenever you want a record of the question and answer. Use voice only after enabling the microphone intentionally.
- When voice is on, Alfred should wait for its wake phrase, such as "Alfred" or "Hey Alfred," before treating subsequent speech as a question.
- Turning the microphone field on or off should be a single click. "Starting" means the voice service is initializing; "Help" should point to a meaningful recovery action, not leave the listener active in the background.
- Close Alfred to end spoken output. If a question has text evidence but no voice audio, use the text answer and refresh context; submit a support report if it repeats.

17. Phone and QR

Phone / QR lets you pair the eligible MKT view with the mobile experience. The code should be generated from the current MKT screen, treated as private, and revoked or regenerated if it was shared with someone who should not have access.

1. Open Phone / QR. Generate a current pairing code from the selected local or Full view.

2. Scan with the intended device. Use the MKT mobile flow only. Do not upload the QR image to a public website or send it in a public chat.

3. Confirm the visible scope. Check which computer or fleet view is paired. Revoke/regenerate the pairing if the phone changes hands or you suspect it was exposed.

18. Troubleshooting

What you see	Likely meaning	Safe next step
Starting or waiting for job	The miner is initializing or has not received work yet.	Wait briefly, then check the selected pool route and activity status. Do not keep pressing Start.
No hash rate after start	The worker, selected hardware lane, or pool connection has not provided a live report.	Open logs, confirm the coin/profile/engine combination, test the pool route, then refresh telemetry.
Submitted shares but no accepted rate	A pool confirmation may be delayed or the denominator is not yet meaningful.	Wait for a pool receipt; use unavailable/pending rather than treating a tiny percentage as a final result.
ASIC has no telemetry	Route may be private/unreachable, API may be disabled, or adapter is manual/unknown.	Confirm LAN/tailnet path and the exact model/firmware; never expose the API publicly.
Remote computer says Not Current	MKT knows the saved system but lacks a fresh receipt.	Check power, private route, Tailscale, and MKT telemetry service; keep the stable identity.
Explorer shows no funds	The explorer may be the wrong network or the pool has not paid on-chain.	Verify coin/network/address and check the pool's payout threshold and history.
Node/RPC cannot be checked	The node may not be running/synced, or its private read-only endpoint is unavailable.	Confirm node service, local firewall, approved route, port/path, and reviewed adapter status.

19. Security and privacy

- Install only signed releases obtained from an official MKT delivery link. Verify the Windows publisher before installing.
- MKT stores public payout addresses and per-coin configuration. It does not require a wallet seed phrase, private key, recovery phrase, or exchange password.
- Keep ASIC management APIs, node RPC endpoints, and MKT telemetry routes on a private LAN or approved Tailscale route. Do not forward them to the public Internet just to make discovery work.
- Use CoinPacks and engine bundles only when their verification checks pass. Do not replace package files, telemetry adapters, or activation receipts with files obtained from informal sources.
- Keep your operating system, driver, ASIC firmware, node software, and MKT installation current. Read release notes before applying a major update.

20. Glossary and support

Before you contact support

- Record the coin profile, hardware lane, approximate time, and what the screen showed. A support report is more useful than a memory of an error.
- Use Open Logs or Support Report where offered. Remove any wallet secrets or unrelated personal information before sharing—MKT should never ask for those items.
- Include the device name, stable identity (not just a changing IP), whether the path is local or Tailscale, and the model/firmware for an ASIC or node.

Operational glossary

Term	Meaning
Accepted share	A submitted work report the pool/miner confirms according to its current rules.
Activation receipt	The private, installation-bound record that unlocks the selected edition or trial.
Adapter	The signed MKT component that knows how to read a supported miner, ASIC, or node protocol.
Current data	A fresh telemetry receipt from a running source in the active time window.
Private route	A local network or approved tailnet path, not a publicly exposed port.
Read-only	MKT can inspect supported status information but does not change the external device or service.
Telemetry	Operational evidence reported by miners, pools, ASICs, nodes, or MKT services.

External learning sources

For independent risk education, review the U.S. Commodity Futures Trading Commission's "Use Caution When Buying Digital Coins or Tokens" and "Understand the Risks of Virtual Currency Trading" advisories at cftc.gov. They emphasize due diligence, volatility, and the absence of guaranteed returns. MKT does not endorse any coin, pool, wallet, or external service.