

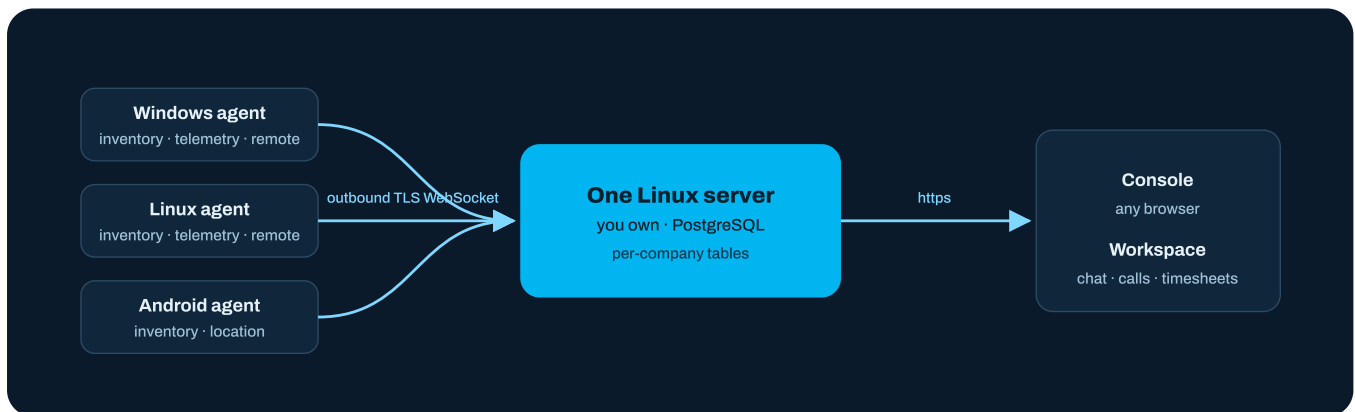


AssureIT Remote technical datasheet

AssureIT Remote is a self-hosted platform for endpoint monitoring, remote management, IT asset management, service desk and employee collaboration. It runs on a single Linux virtual machine the customer owns. Agents on Windows, Linux, macOS and Android connect outbound over WebSocket to report inventory, hardware detail, event logs and metrics, and to accept remote sessions and commands. All data stays on the customer's server.

ARCHITECTURE

One Linux virtual machine runs the application server, a PostgreSQL database and an HTTP reverse proxy terminating TLS. Each customer organisation gets its own set of database tables inside that instance, and the four-tier channel hierarchy (vendor, distributor, dealer, customer) restricts every query to the caller's own branch. Endpoint agents open a single outbound WebSocket to the server and hold it open, which is how the device list, metrics and remote sessions stay live rather than polled; no inbound port is opened on the endpoint. Remote desktop, terminal and file manager are multiplexed over that same connection. Agent updates are RSA-signed and verified by the agent before installation. Workspace chat and presence pass through the server; call, meeting and screen-share media is peer-to-peer WebRTC and is not stored on the server. Alert email leaves through an SMTP account you configure. There is no second node and no cluster: sizing is vertical, and the reverse proxy's worker limit must exceed the fleet size because each connected agent holds a worker for the life of its connection.



PLATFORM SUPPORT

What works where

✓ full · 🕒 partial · — not available. Coverage is not uniform, and this table says so rather than implying parity.

CAPABILITY	WINDOWS	LINUX	MACOS	ANDROID
Agent deployment	✓	✓	✓	🕒
Device inventory and heartbeat	✓	✓	✓	🕒
Hardware inventory with part and serial numbers	✓	🕒	🕒	🕒
Hardware change history by serial	✓	🕒	🕒	—
Software inventory	✓	✓	🕒	—
Remote desktop	✓	✓	—	—
Remote terminal	✓	✓	—	—
Remote file manager	✓	✓	—	—
Service start / stop / disable	✓	🕒	—	—
Process kill and remote software uninstall	✓	🕒	—	—
On-device consent prompt, revocable mid-session	✓	—	—	—
Windows Update scan and install	✓	—	—	—
BitLocker drive status	✓	—	—	—
Antivirus, Defender real-time and firewall profile status	✓	—	—	—
USB attachment alerts	✓	—	—	—
Event log collection (push and pull sweep)	✓	✓	—	—
Resource metric thresholds and alerting	✓	✓	🕒	—
Offline and back-online alerting	✓	✓	✓	✓
Device location and geofencing	✓	✓	—	—
Timesheets from measured foreground application time	✓	🕒	—	—
Signed agent self-update	✓	🕒	🕒	🕒
Employee workspace (browser, no agent required)	✓	✓	✓	🕒

SPECIFICATIONS

The detail an evaluator asks for

ARCHITECTURE

Deployment model	Self-hosted on a single Linux virtual machine owned by the customer. On-premises or in the customer's own cloud account. No vendor-side copy of customer data.
Server components	Application server, PostgreSQL database, HTTP reverse proxy terminating TLS, outbound SMTP for alert email.
Tenancy	Per-company database tables inside one instance. The four-tier hierarchy (vendor, distributor, dealer, customer) scopes every read and write to the caller's branch; dealer customer lists are not visible to the distributor above them.
Agent transport	One persistent outbound WebSocket per endpoint, carrying inventory, metrics, event logs, remote desktop, terminal and file transfer. No inbound port on the endpoint.
Console	Browser-based. Live device list with filter, search and sort; 12-tab device record; Monitor Grid video wall up to 20 pages of 60 panels at 5-second refresh, with fullscreen slideshow.
Collaboration media	WebRTC peer-to-peer for calls, meetings and screen share. Media does not traverse or rest on the server. External guests join meetings by link without an account. Not end-to-end encrypted.
Licensing	Per device per year, tier assigned per device so one organisation can mix. Silver Rs600 (inventory, hardware, accessories, e-waste); Gold Rs1,200 (adds update manager, resource monitor, services, event manager, alerts); Platinum Rs2,400 (adds remote desktop, terminal, file manager, device location). Trial licences carry full capability. Co-termed fleet expiry with proration; GST invoices generated in-product.

SECURITY AND ACCESS CONTROL

Sign-in	Username and password with server-side sessions. No multi-factor authentication and no account lockout — see Current boundaries.
Authorisation model	18 capabilities expressed as 29 separate read and write permissions, assigned per user.
Destructive commands	Action password required and verified server-side, not in the browser.
End-user consent	Windows agents show an on-device prompt before a remote session and the user can revoke consent mid-session. Not available on Linux, macOS or Android.
Reseller support access	No standing access. The customer grants a 24-hour, 7-day or 30-day window; the grant is re-evaluated on every request, so revocation takes effect on the engineer's next click.
Agent update integrity	Update packages are RSA-signed and the signature is verified by the agent before installation.
Agent tamper resistance	Uninstall is gated by a password checked on the device, and the agent respawns within about a minute if killed. Effective against a standard user; an administrator on the machine can still remove it.
Hardware change log	Swap records are append-only and cannot be edited from the console.
Encryption reporting	Reads BitLocker status on Windows only. A drive encrypted by any other product will not be reported as protected, and the console says so explicitly when Windows will not report.

Transport

TLS on the console and on agent connections, using a certificate you supply for your own domain.

MONITORING AND ALERTING

Metrics	14 alert metrics, each with an independent warning and critical threshold.
Scope	Thresholds set company-wide, per device group or per individual device. Each threshold has separate alert and email switches.
Offline detection	Edge-triggered from last contact: exactly one alert per outage plus one back-online notice, not a repeat every cycle. Uptime freezes at the last contact time while a device is offline.
Email behaviour	Alert email is batched into a 120-second digest with a 12-hour cooldown per condition, and the cooldown state survives a server restart.
Automatic tickets	A breach sustained for a full hour opens a ticket automatically and closes it when the condition recovers.
Event logs	Windows and Linux event logs centralised by agent push every 5 minutes plus a server pull sweep every 15 minutes.
Security events	USB attachment alerts; alerts on antivirus and firewall configuration changes.
Location	Geofencing raises an alert when a machine leaves its assigned area. No MDM enrolment involved.

DATA, EXPORTS AND RETENTION

Data location	All operational data is held in the PostgreSQL database on your own server. Nothing is replicated to the vendor.
Exports	47-column hardware inventory XLSX; software by publisher; uptime timeline with real clock times; timesheet report; tickets; events; alerts; e-waste register.
Export format	XLSX, generated on demand from the console. No PDF output and no scheduled or emailed reports.
Timestamps	All displayed and exported timestamps are IST. The database itself stores UTC.
Asset records	Purchase date, AMC vendor, contract dates and uploaded invoice files; custody history opening and closing on each reassignment with named actor and reason; separate register for switches, printers and peripherals with custom fields; printable 46mm QR asset tags.
Disposal	E-waste register with an approval step; approval returns the device's licence to the available pool.
Timesheet data	Foreground application time measured on the device, scored against logged hours within a tolerance band, drillable to day, task and application.
Retention and backup	Retention is whatever your database and disk policy allows; there is no built-in retention scheduler and no automated backup. Back the database up with your own tooling.

DEPLOYMENT REQUIREMENTS

Server	One Linux virtual machine. Size vertically for the fleet; the platform is proven today at 650+ endpoints across 30+ organisations.
Database	PostgreSQL on the same machine.
Network	TCP 443 reachable by every endpoint for the console and the agent WebSocket, and 80 if you want HTTP redirect and certificate renewal. Endpoints need outbound access only.
Reverse proxy tuning	Each connected agent holds one proxy worker for the life of its connection. The proxy's maximum worker count must comfortably exceed the number of agents, or new connections will queue and the console will appear to hang while the application is healthy.
DNS and TLS	A public hostname you control, with a TLS certificate. Agents are built against that hostname.
Email	An SMTP account for alert email. Sending is pooled with a circuit breaker on bulk mail so an alert flood cannot take out the mailbox.
Windows agent	Installer run per machine or pushed by your existing deployment method, with an enrolment code.
Linux agent	Install script. Full remote desktop support included.
macOS agent	Agent only. Inventory and heartbeat; no screen streaming.
Android agent	Sideloaded APK, enrolled by QR code or enrolment code. Inventory, hardware data and heartbeat only.
Client requirements	A current browser for the console and the employee workspace. Workspace users need no agent.

AGENT FOOTPRINT AND BEHAVIOUR

Form	A single background service per device, started at boot.
Connectivity	One outbound TLS WebSocket held open to the server. Reconnects on its own after a network drop; no inbound firewall rule required on the endpoint.
Reporting intervals	Heartbeat and live metrics on the open connection; event log push every 5 minutes; server-side pull sweep every 15 minutes as a backstop.
Data collected	System, processor, memory, storage, graphics, network, sound, security and battery detail including part and serial numbers; installed software; running services and processes; foreground application time; and, where the platform supports it, location.
Remote session load	Screen streaming is started only for the duration of a session and stops when the operator disconnects or the user revokes consent.
Updating	Agents on the current generation download and apply RSA-signed updates themselves. Older agents already deployed must be replaced by reinstallation.
Removal	Uninstall from the console, or on the device with the uninstall password. The service respawns within about a minute if terminated without that password.

CURRENT BOUNDARIES

What it deliberately does not do

This list exists so you can plan around it rather than discover it after purchase.

- No multi-factor authentication. Sign-in is username and password only.
- No account lockout after repeated failed sign-in attempts.
- No high availability, clustering or failover. It is one server, and if that server is down the console and agent connections are down.
- No automated backup. Backing up the PostgreSQL database is your responsibility, with your own tooling.
- No security certification, third-party audit or penetration-test attestation of any kind.
- No patch management in the policy sense: no rings, no approval workflows, no maintenance windows and no third-party application patching. It scans for and installs Windows Updates, and that is the whole of it.
- No mobile device management. The Android agent reports inventory; it does not enforce policy, wipe, or manage applications.
- No iOS support.
- No scheduled reports and no emailed reports. Exports are generated on demand from the console. Alert email is the only mail the product sends on its own.
- No PDF output. Exports are XLSX.
- No BI or data-warehouse connectors.
- No operator audit log. Hardware changes, asset custody, disposals and support grants are recorded, but there is no separate immutable trail of every action an administrator takes in the console.
- No compliance scoring and no mapping to any framework such as ISO 27001 or CERT-In guidance.
- Encryption reporting is BitLocker on Windows only. Drives encrypted by another product, and drives on Linux, macOS or Android, are not reported as protected.
- The on-device consent prompt is Windows-only. Remote sessions on Linux do not present one.
- macOS is agent-only: no remote desktop, no terminal and no file manager.
- The Android agent is sideloaded and is not distributed through Google Play.
- The employee workspace is not end-to-end encrypted, and calls and meetings are not recorded — media is peer-to-peer and never reaches the server.
- Agent tamper resistance stops a standard user, not a local administrator.

Sales & enquiries: +91 91563 88728 · info@theforum.co.in — The Forum, Authorised Distributor. Product by AssureIT Networks, Ahmedabad · assureitnetworks.com