

TIER-1 TROUBLESHOOTING

Faction Four Systems Inc.

Applies to Smart Squad 2.8 and 2.9 · agency service desk, network, MDM and server teams · Revised October 2026

Internal triage steps for agency IT teams to complete before escalating to Faction Four. Each section maps to a specific internal team, so only the relevant team needs to be engaged.

CONTENTS

1 · Scope the issue	2
2 · Device and MDM checks	3
3 · Network and VPN checks	4
4 · Server and database checks	6
5 · Integration checks	7
6 · Authentication and account issues	8
7 · Printers and licence scanners	8
8 · Escalating to Faction Four	10
Appendix A · Self-serve guides	11
Appendix B · Quick symptom index	13

How to use this guide. Start with section 1 — it tells you which team-specific section applies. Complete the applicable checklists, record the results, and escalate only if the issue still points at the application. Include the completed checklist results in the escalation (section 8).

1 · SCOPE THE ISSUE

Service desk — five minutes. Four questions decide which team owns the next step.

QUESTION	IF YES	IF NO
Is it affecting multiple users?	Likely server, network or integration → sections 3, 4, 5	Likely device-specific → section 2
Is it affecting multiple locations or networks — in-station Wi-Fi <i>and</i> cellular?	Server or application → sections 4, 5	Network or VPN path → section 3
Is only one feature failing? Attachments won't upload, but everything else works.	Note which feature — it matters for escalation → section 5	Whole-app outage → sections 3, 4
Did anything change recently? MDM policy push, VPN config, firewall rule, Windows patching, RMS/CAD maintenance.	Investigate that change first — roll back or exempt Smart Squad and retest	Continue with the checklists

The ten-second question that routes most calls. Ask the user what colour the bar at the top of the app is. **Orange** means the app believes it is offline — a network path problem, section 3. **Red** indicates an error state. A normal header with one feature failing points at the server or an integration, sections 4–5.

Two direct routes, which skip the table entirely:

- Login, password or MFA problem → **section 6**
- Only printing or licence scanning failing → **section 7**

The golden question: can the user open the Smart Squad server URL in the device's own web browser?

No — this is a connectivity problem (network, VPN, MDM), not an application problem. Sections 2–3.

Yes, but the app still fails — continue to sections 2, 4, 5.

A "yes" rules out DNS and VPN basics only. Real-time features — messaging, alerts, live locations — have additional network requirements; see section 3.3 before ruling out the network.

2 • DEVICE AND MDM CHECKS

MDM / mobile team. Smart Squad devices are typically MDM-managed and authenticate with device certificates. Most single-user issues are resolved here.

- ☐ **App version** — is the device on the currently deployed version? Staged MDM rollouts leave devices on old versions that no longer match the server.
- ☐ **MDM policy changes** — was a new profile, restriction or compliance policy pushed recently? Check whether the device fell out of compliance; MDM may block network access or revoke certificates silently.
- ☐ **Certificates** — device identity certificate not expired or revoked; any CA or root certificates pushed by MDM still present (a profile removal can strip them); per-device Smart Squad certificates not expired, where the agency uses them.
- ☐ **Date and time** — device clock correct and set to automatic. Clock drift breaks certificate validation and one-time-password login.
- ☐ **OS updates** — was one installed recently? Retest on a device that has not been updated, to isolate.
- ☐ **App permissions** — camera, location, microphone, notifications. MDM policy changes can revoke these.
- ☐ **Storage** — low free storage causes upload, attachment and autosave failures.
- ☐ **Location sharing** — for "officer not showing on the map", confirm Location Sharing is enabled in the user's app settings before checking anything else. This toggle, not infrastructure, is the usual cause.
- ☐ **The classic pair** — restart the app; if that fails, restart the device. Retest.
- ☐ **Cross-device test** — same user on a known-good device. Works there? The issue is the device, not the account or the application.

- ☐ **Cross-user test** — different user on the affected device. They succeed? The issue is account-specific; check for a lockout in the admin portal before escalating.

Do not uninstall, reinstall or wipe the app as a troubleshooting step. Unsynced notes and attachments live only on the device until they upload. Reinstalling or wiping before the upload queue is empty **permanently destroys that data**. If uploads appear stuck, escalate first — do not reinstall.

3 • NETWORK AND VPN CHECKS

Network team. Agency devices usually reach Smart Squad through a VPN or a filtered path. Smart Squad also holds persistent WebSocket connections and uses PubNub for real-time messaging — these have different requirements from ordinary web traffic, and are the thing a VPN or proxy most often breaks silently.

3.1 Basic reachability

- ☐ **VPN tunnel up?** Confirm it is connected *and passing traffic*, not just showing "connected". Test with the affected device, not a desktop.
- ☐ **Server URL from the device browser**, over the same VPN. If the login page loads, basic reachability is fine.
- ☐ **DNS** — the hostname resolves correctly on the VPN's DNS, and split-tunnel DNS is not sending it to the wrong resolver.
- ☐ **Cellular vs Wi-Fi** — test the same device on both. If one path works and the other does not, the issue is in the failing path.

3.2 VPN-specific checks

- ☐ **Recent VPN changes** — new gateway, new client version, new split-tunnel rules, certificate rotation. Exempt and retest.
- ☐ **Split tunnelling** — confirm Smart Squad server traffic *and* PubNub traffic (`*.pubnub.com` , port 443) are both routed correctly. A rule covering the server but not PubNub produces "the app works but no messages or alerts arrive".
- ☐ **Idle and session timeouts** — Smart Squad holds long-lived WebSocket connections. A VPN that drops idle sessions aggressively (under 5 minutes) produces disconnect/reconnect symptoms, delayed messages or repeated re-logins.
- ☐ **VPN capacity** — is the concentrator at session or bandwidth capacity at shift change? Symptoms that cluster at predictable times of day point here.

- ☐ **MTU and fragmentation** — VPN plus cellular can pass small requests and fail large ones. If small actions work and large uploads fail, test MTU on the tunnel.

3.3 Firewall, proxy and inspection

- ☐ **TLS inspection** — if the path inspects SSL/TLS, Smart Squad and PubNub must be exempted. Certificate-pinned and WebSocket traffic does not survive interception.
- ☐ **WebSocket support** — proxies and firewalls must allow the upgrade (`Connection: Upgrade`) and must not terminate long-lived connections. Symptom: login works, data loads, but real-time updates stop after a few minutes.
- ☐ **Recent firewall changes** — new rules, IPS signatures or geo-blocking that could match Smart Squad or PubNub traffic.
- ☐ **Outbound allowances, server side** — outbound 443 open from the Smart Squad server to its external dependencies. A server-side change breaks these for everyone at once.

PURPOSE	ENDPOINTS
Real-time messaging (required)	<code>*.pubnub.com</code> , <code>*.pndsn.com</code> , <code>*.pubnub.net</code> , <code>*.pubnub.io</code>
Map services	<code>*.mapbox.com</code> , <code>*.hereapi.com</code>
Weather (required)	<code>*.openweathermap.org</code>
Communications	<code>*.twilio.com</code> , <code>*.api.flagsmith.com</code> ; virtual interview and calling uses <code>*.dyte.io</code> on 2.9.0 and earlier, Cloudflare RealtimeKit domains from 2.9.1
Authentication	<code>api.yubico.com</code> , <code>*.evidence.com</code>
Cloud and AI services, if used	<code>blob.core.windows.net</code> , <code>file.core.windows.net</code> , <code>cognitive.microsoft.com</code> , <code>*.openai.azure.com</code> , <code>*.sendgrid.net</code> , <code>*.azurewebsites.net</code> , <code>*.smartsquad.online</code>
Monitoring and support	<code>*.rollbar.com</code> , <code>*.freshdesk.com</code>

This table is a snapshot. The authoritative allow-list for your installed version is the On-Premise Preparation Guide that shipped with it. Re-check it at every upgrade before locking firewall rules to this list.

A block on one of these produces a single-feature failure while the rest of the app works — blocked Mapbox gives a blank or grey map, blocked PubNub gives no real-time messages, blocked transcription or AI endpoints stall drafting. Match the failing feature to its endpoint before escalating.

- ☐ **Map tiles from devices** — tiles load from `*.mapbox.com` on 443. If the map is blank on devices but everything else works, confirm the device VPN, split-tunnel and TLS inspection exempt Mapbox as well as the server URL.

Rules of thumb. Works on cellular but not agency Wi-Fi, or the reverse, is a network path issue. Real-time features dying after N minutes while the rest works is an idle timeout or WebSocket handling on the path.

4 · SERVER AND DATABASE CHECKS

Server / DBA team. For issues affecting multiple users or whole-app slowness.

4.1 Application server (IIS)

- ☐ **Site and app pool** — Smart Squad site started, application pool running. Check the Windows Application event log for recent recycles or crashes (`w3wp` errors, APPCRASH).
- ☐ **Server resources** — CPU, memory and disk. A `w3wp` process consuming abnormal memory, or a full system drive, degrades everyone.
- ☐ **Windows updates and reboots** — was the server patched or rebooted? Confirm every Smart Squad component came back up afterwards.
- ☐ **Smart Squad Windows services** — in `services.msc`, filter on "SmartSquad" and confirm all are running: the background Processor and each installed interface service (RMS, CAD, evidence/DEMS, report execution; the exact set depends on your deployment). A stopped interface service produces "queries to RMS return nothing" or "transcriptions stuck" while the rest of the app works.
- ☐ **Server certificate** — TLS certificate not expired or about to.

4.2 SQL Server

- ☐ **Service and connectivity** — SQL Server running, app server able to connect.
- ☐ **Blocking and long-running queries** during the problem window. Whole-app slowness for all users is very often database blocking.
- ☐ **Disk space** on every SQL volume: data, log, tempdb and **the FILESTREAM volume**. Attachment binaries are stored on the filesystem via FILESTREAM, so a full FILESTREAM volume breaks attachment upload while the rest of the app looks healthy.
- ☐ **Maintenance windows** — do symptoms line up with backup jobs, index maintenance or antivirus scans on the database volumes?
- ☐ **Recent SQL changes** — patching, configuration changes, new agents or monitoring on the SQL host.

5 • INTEGRATION CHECKS

Server team / RMS and CAD administrators. If only integration-backed features fail — record queries, person and vehicle lookups, CAD events, evidence retrieval — while notes, messaging and tickets work, check the source system.

- ☐ **Is the source system itself up?** Verify in the RMS, CAD or evidence system's own client, not through Smart Squad.
- ☐ **Source system maintenance** — scheduled maintenance, upgrades or index rebuilds on that side.
- ☐ **Interface service running** on the Smart Squad server (see 4.1).
- ☐ **Credentials and service accounts** — were passwords rotated, or accounts disabled or expired, on the source system? This is the leading cause of "the integration suddenly stopped".
- ☐ **Network path between servers** — can the Smart Squad server reach the source system's endpoints? Check for firewall changes between server VLANs.
- ☐ **External query systems** — queries to national or provincial systems (CPIC, motor vehicle, courts) take a different path from RMS lookups. If only external queries fail, check that service, the path and firewall to it, and whether the external system has posted an outage.

Rule of thumb. If the same query fails in the source system's own client, the issue is the source system — engage that vendor or team, not Faction Four.

6 • AUTHENTICATION AND ACCOUNT ISSUES

Service desk and MDM. For login failures specifically.

- ☐ **Scope** — one user or all? All users failing is a server or network issue, sections 3–4. One user, continue here.
- ☐ **Account logout** — check the user's status in the admin portal: failed login count, disabled status.
- ☐ **OTP and MFA delivery** — confirm the delivery method (SMS or email) is working and the device clock is correct (section 2).
- ☐ **SSO** — if the agency uses external SSO, confirm the identity provider is healthy and the account there is active.
- ☐ **Device certificate** — see section 2. Expired or revoked certificates present as a login failure.
- ☐ **Yubikey MFA** — confirm the key is enrolled, and that the server's outbound access to `api.yubico.com` is not blocked (section 3.3). The latter breaks Yubikey login for every user at once.
- ☐ **SSO credential update** — if external-system access fails for one user after their password changed in that system, have them update their stored credentials.
- ☐ **Password reset** — try a self-serve or admin-initiated reset before escalating.

7 • PRINTERS AND LICENCE SCANNERS

Service desk and MDM. Mobile printers and driver's licence scanners are the most common source of "Smart Squad is broken" reports that turn out to be a peripheral problem.

The key triage question: does the peripheral work outside Smart Squad? If the printer cannot print a test page, or the device cannot see the scanner at the OS level, it is a hardware, pairing or MDM issue — the application never gets involved.

7.1 Mobile printers

- ☐ **Printer basics first** — powered on, battery charged, paper loaded the right way round (thermal paper inserted upside down prints blank), lid fully closed, no error LED. A surprising share of print failures end here.
- ☐ **Self-test page** — print the printer's built-in self test. If that fails, it is the printer.
- ☐ **Bluetooth pairing** — paired *and connected*, not just paired. Mobile printers typically hold one active pairing, so if another officer's device paired to it the original pairing is silently dropped.

Unpair and re-pair.

- ☐ **Bluetooth on and permitted** — enabled on the device, and the app holds Bluetooth / nearby-devices permission. OS updates and MDM pushes can revoke this.
- ☐ **MDM Bluetooth restrictions** — a policy restricting Bluetooth, limiting pairing to allow-listed devices, or blocking the printer's device class breaks printing fleet-wide overnight and looks exactly like an app failure.
- ☐ **Range** — trunk-mounted printer plus officer away from the vehicle equals out of range.
- ☐ **Cross-device test** — pair the printer to a known-good device. Works there, the original device's pairing or permissions are at fault; fails there too, it is the printer.
- ☐ **Scope** — one printer, one device, or all printers agency-wide? All at once means an MDM policy change or an app deployment, not hardware.

Prints, but misformatted — ticket splitting across two pages, wrong scale, cut off. Ask whether anyone recently printed to this printer from a Windows computer. The mobile app relies on settings stored *on the printer itself*, and printing from Windows silently overwrites them. No amount of Bluetooth troubleshooting will find this.

Restore the printer's settings, or escalate noting the Windows print history, and instruct staff not to print to fleet mobile printers from PCs.

7.2 Driver's licence scanners

- ☐ **Recognised by the device** — confirm the OS sees the scanner, Bluetooth paired and connected or USB accessory detected. If the OS cannot see it, Smart Squad cannot either.
- ☐ **Scan outside Smart Squad** — for keyboard-wedge scanners, scan a licence into a plain text field. Data appears there but not in Smart Squad, escalate; nothing appears anywhere, it is the scanner or the pairing.
- ☐ **Physical read quality** — clean the scan window and test with a known-good licence. Worn or scratched licences fail on any scanner, so try a second one before blaming the hardware.
- ☐ **Out-of-jurisdiction licences** — another province or state may use a different barcode format. If only those fail, note the issuing jurisdiction in the escalation — that is application-relevant, not a hardware fault.
- ☐ **Camera-based scanning** — confirm camera permission (section 2), a clean lens and adequate light. Test the camera in another app.
- ☐ **Pairing exclusivity and MDM** — same checks as printers.
- ☐ **Cross-device and cross-scanner tests** to isolate which side owns the fault.

The keyboard-wedge caveat. The "scan into a notes app" test only applies to scanners that type into text fields. Some models integrate directly with the app and will never produce text elsewhere. Confirm with your Smart Squad administrator which mode your fleet uses before declaring a unit faulty on that test alone.

7.3 Browser client — Smart Squad Tray

On Windows workstations using the browser client, peripherals — printer, licence scanner, GPS source — connect through the Smart Squad Tray application. The browser cannot talk to them directly.

- ☐ **Tray installed and running** in the system tray. If it is not, printing, scanning and GPS fail silently while the web app otherwise works.
- ☐ **Tray after updates** — Windows updates, browser updates or endpoint-protection changes can remove or block it. If peripherals stopped after a patch cycle, reinstall.
- ☐ **Peripheral configured in the Tray** before treating it as a failure.
- ☐ **Endpoint protection or application-control policy** blocking the Tray executable or its local browser communication presents as "worked yesterday, all workstations broken today".

Rule of thumb. Peripheral works outside the app but not inside it → escalate with the model, firmware and what you observed. Peripheral fails outside the app too → hardware, pairing or MDM policy; resolve internally.

8 · ESCALATING TO FACTION FOUR

Escalate when the checklists are complete and the issue still points at the application — typically: it reproduces across multiple devices and networks, errors reference the application itself, or a feature misbehaves while all infrastructure checks pass.

Escalations should come through your designated Smart Squad support contact — one channel, not per team. Every escalation must include:

1. **Platform** — iOS, Android or browser client, with app version and device model, or browser and OS for workstations.
2. **User** — the affected accounts and devices, or "all users".
3. **Issue** — the feature, the exact error message or behaviour, dates and times with timezone, and whether it is ongoing or intermittent.
4. **Steps to reproduce** — the exact sequence, starting from where the user was in the app.
5. **Reproducible in non-production?** If yes, say which environment — it lets both sides investigate without touching production.

6. **Screenshots** of the error, including the app header or status area where visible.
7. **Logs uploaded?** Confirm whether, from which devices, and for what time window.
8. **Contact for the user** — name and direct contact for someone who can reproduce it, so follow-up questions don't round-trip through several teams.
9. **Scope answers from section 1** — multiple users? multiple networks? one feature? recent changes?
10. **Checklist results** — which sections were run, and what was found or ruled out.
11. **Environment notes** — anything that changed in the window (patching, MDM pushes, VPN or firewall changes, RMS/CAD maintenance), even if believed unrelated.

A complete package lets us go straight to a targeted application log review and return a clear statement of what failed and where the cause sits — application, environment or integration — usually in one pass instead of several rounds of questions.

APPENDIX A • SELF-SERVE GUIDES

Step-by-step how-to guides are in the Smart Squad knowledge base. Most peripheral and account tickets end with one of these, no escalation needed.

GUIDE	USE FOR	SECTION
Configure Printer — iOS / Android	Printer setup and re-pairing on mobile devices	7.1
Configure Printer — Browser Client	Printer setup on Windows workstations	7.3
Configure License Scanner — Browser Client	Scanner setup on workstations	7.2, 7.3
Configure GPS Source — Browser Client	GPS source setup on workstations	7.3
Installing Smart Squad Tray for Browser	Tray install and reinstall	7.3
Install / Uninstall Smart Squad — Windows	Windows client install and upgrade	2
How to Login to Smart Squad	First-time login walkthrough	6
How To Reset Your Smart Squad Password	Password resets	6
How to Enrol a Yubikey Device for MFA	Yubikey MFA enrolment	6
How to update Single-Sign-On credentials	Stored external-system credentials after a password change	6
How To Create an Officer Signature	Signature setup	—

APPENDIX B · QUICK SYMPTOM INDEX

SYMPTOM	MOST LIKELY AREA	SECTION
One user can't log in	Account lockout, device certificate, clock	2, 6
All users can't log in	Server, VPN, TLS certificate	3, 4
Works on cellular, not Wi-Fi, or the reverse	Network path or firewall	3
Messages or alerts delayed, or stop after minutes	WebSocket / PubNub path, VPN idle timeout	3.2, 3.3
Small actions work, large uploads fail	MTU / VPN fragmentation, device storage, FILESTREAM disk	3.2, 2, 4.2
App slow for everyone	SQL blocking, server resources, maintenance jobs	4
Record, person or vehicle queries fail, rest works	RMS integration or interface service	5
Only external queries fail, RMS lookups work	External system or the path to it	5
CAD events not appearing	CAD system or interface service	5
Map blank or grey, rest works	Mapbox blocked — firewall, TLS inspection, split tunnel	3.3
Officer not showing on map	Location Sharing toggle in app settings	2
Ticket won't print	Printer power, paper, pairing; MDM Bluetooth policy	7.1
Printer prints self-test but nothing from the app	Pairing, Bluetooth permission, MDM	7.1
Ticket prints blank	Thermal paper inserted upside down	7.1
Ticket misformatted or splits across pages	Printer-stored settings overwritten by a Windows print	7.1

SYMPTOM	MOST LIKELY AREA	SECTION
Licence scan produces nothing anywhere	Scanner hardware or pairing — see the keyboard-wedge caveat	7.2
Only out-of-jurisdiction licences fail	Barcode format — escalate with the jurisdiction	7.2
All mobile printers or scanners failed at once	MDM / Bluetooth policy change	7.1, 2
Peripherals fail on a workstation (browser client)	Smart Squad Tray not running or blocked	7.3
Peripherals broke on workstations after a patch cycle	Tray removed or blocked by an update or AV policy	7.3
Attachments fail, rest works	FILESTREAM or storage, device storage, MTU	4.2, 2, 3.2
Transcriptions or reports stuck in processing	Background Processor service	4.1
Uploads stuck, pending items on the device	Escalate — do not reinstall the app	2
Everything broke after a change window	The change	1