Level 5 – Technical FAQ

Last updated by | Houston, Cody L | Feb 17, 2026 at 9:45 AM CST

L5Connect & ATC System FAQ

> **Author:** Cody Houston
> **Last Updated:** 2026-02-17
> **Version:** 1.0
> **Applies To:** L5Connect v9.16.1+

Architecture & System Design

▼ 1. What server architecture is recommended for L5Connect?

We recommend a **two-server architecture**:

- **Server 1:** Application + File Storage
- **Server 2:** Microsoft SQL Database

Improves performance, scalability, and troubleshooting.

SQL Express on a single server is acceptable for smaller deployments.

▼ 2. What are the minimum and recommended server specifications?

System requirements:
https://l5connectdemo.com/documents/ARCHIVE/ZL5C-SYSREQ .pdf

▼ 3. Why should OS and data be on separate drives?

- Improves I/O performance
- Simplifies backup/recovery
- Reduces OS impact on data

Networking & Connectivity

▼ 4. What network ports and protocols are used?

Client → Application Server

- Protocol: HTTPS or TCP
- Port: 443 or 59008 + 59009 (customer defined)

Application Server → Database

- Protocol: SQL
- Port: Customer defined

⚠️ Clients never connect directly to the database.

▼ 5. Does the system require internet access?

❌ No. Fully self-contained system.

▼ **6. Does the device support DHCP or static IP?**

Supports all standard Windows networking configurations (DHCP and static).

▼ **7. What is required for static IP configuration?**

- IP Address
- Subnet Mask

▼ **8. Can the device operate offline?**

Yes.

- Device caches usage data locally
- Automatically uploads when connection is restored

▼ **9. Is Wi-Fi supported and recommended?**

- Supports all Windows-supported Wi-Fi standards
- **Ethernet is strongly recommended**

Security & Encryption

▼ **10. What certificates are used?**

- **Internal:** Snap-on issued X.509 certificates
- **External (HTTPS):** Customer-provided SSL certificate

▼ **11. Where are certificates stored?**

- X.509 certificates: Stored within application (server + client)
- SSL certificates: Stored in Windows certificate store

▼ **12. Who manages certificate lifecycle?**

- X.509: Snap-on (via software updates)
- SSL: Customer

▼ **13. What happens if a certificate expires?**

- Connectivity to service fails
- System will not allow incoming connections

▼ **14. How are private keys stored?**

- X.509: Encrypted within certificate file
- SSL: Windows certificate store

▼ **15. Does the system support CRL/OCSP?**

Yes — supports all Windows certificate capabilities.

Authentication & Identity

▼ **16. Does the system support SSO or external identity providers?**

❌ Not supported (OAuth, SSO, Azure AD, etc.)

▼ **17. How is authentication handled?**

- Fully internal authentication
- Role-based access control

▼ 18. Can the device join Active Directory?

✅ Yes, with conditions:

- Must use a **dedicated OU**
- Avoid heavy security packages and GPOs
- Device has limited system resources

▶ 19. Are there AD/GPO limitations?

ATC Device – OS & Configuration

▼ 20. What operating system is used?

- Windows 10 IoT Enterprise LTSC 2019
- Windows 11 IoT Enterprise LTSC 2024

▼ 21. Can the OS be modified?

✅ Yes — customers can apply security baselines and configurations.

▼ 22. What local accounts exist?

- **user** – Standard account (auto-login, runs system)
- **user1** – Local Admin (primary elevated account)
- **user2** – Local Admin (backup account)

▼ 23. Can admin passwords be changed?

✅ Yes, but **not recommended**.

⚠️ Snap-on technicians require access for support.

Data, Storage & Performance

▼ 24. What data is transferred?

- Drawer event images
- Usage data
- Software updates

▼ 25. Bandwidth requirements?

- ~240 KB/sec per device

▼ 26. Storage requirements?

- ~800 MB/device/month

▼ 27. Database size?

- Typically 10–50 GB

Updates & Maintenance

▼ **28. How are updates delivered?**

- `.MSI` installer on Application Server
- Devices auto-update on check-in

▼ **29. What happens during updates?**

- All devices update automatically
- Must match server version

⚠️ All-or-nothing update process.

Logging & Monitoring

▼ **30. What logs are generated?**

All L5Connect events:

- Device activity
- Drawer usage
- Errors

▼ **31. Where are logs stored?**

- Within the application

▼ **32. Log retention?**

- Managed within the application

▼ **33. Can logs be sent to SIEM?**

- Not tested

▼ **34. Can logs be accessed locally?**

- Yes, via Administration Client diagnostic pull

▼ **35. Is operational data stored?**

Yes:

- Tool usage
- User activity
- Diagnostics

Also uploaded to server.

Remote Support

▼ **36. Is remote access required?**

❌ Not required, but helpful.

▼ **37. What remote tool is used?**

- ScreenConnect

▼ **38. How is access controlled?**

- Customer approval required
- Session must be manually approved
- Session removed after completion

Security Hardening & Device Behavior

▼ 39. Are Windows services disabled?

❌ No — all standard services remain enabled.

▼ 40. Network behavior of the device?

- No inbound connections
- All communication is outbound to service

▼ 41. Firewall configuration?

- Allow all traffic to L5Connect application

▼ 42. Are USB ports restricted?

- ❌ No — fully open

▼ 43. Hardening recommendations?

- Determined by customer

Cloud, Updates & Connectivity

▼ 44. Does the system use cloud services?

❌ No

▼ 45. Can outbound internet be blocked?

✅ Yes — no impact to operation

Security Limitations & Compliance

▼ 46. Are there known limitations with security tools?

Yes:

- CrowdStrike and similar EDR tools can **severely impact performance**
- Standard desktop GPOs may interfere

⚠️ Test all security tools before deployment.

▼ 47. Security risks in enterprise environments?

- Must ensure proper network segmentation
- Avoid overloading device with security tooling

▼ 48. Does Snap-on provide security certifications?

- Software tested via **Veracode**

- Vulnerabilities addressed

- No formal penetration testing performed

Change Log

Date	Author	Change Description
2026-02-17	Cody Houston	Initial FAQ