ATG SECURITY — BEST PRACTICES

Securing your Automatic Tank Gauge system

ATG systems are increasingly networked — and two configuration steps account for the vast majority of preventable security incidents. Here is what every operator needs to do.

1 CHANGE YOUR ATG PASSWORD TODAY

Priority action — do this first.
Leaving the factory-default password in place is the single highest-risk configuration error for any ATG deployment. Default credentials for major ATG brands are publicly known and actively exploited. Similarly, reusing a password can be a critical risk to multiple systems if bad actors get a hold of that password.

01 Change it at the physical console

Make the initial password change directly at the console — not over a network connection — to eliminate any risk of credential interception during setup.

02 Create a site-specific password

The new password must be unique to this installation — not reused from another site or system. Use at least 12 characters, mixing letters, numbers, and symbols.

03 Store it securely near the console

Record the password and keep it in your setup documentation or a tamper-evident sleeve near the console. If physical access is uncontrolled, use a locked cabinet.

04 Verify the change took effect

Log out, then log back in with the new password to confirm setup is complete. Verify the default credential no longer grants access.

05 Rotate it periodically

Review and update the password at least once a year, or immediately after any personnel change involving staff with console access.

06 Replace vulnerable legacy devices

If you have a legacy device which doesn't support having a password or passcode at all, then you should prioritize getting it replaced with a newer and more secure device. If you have an older device which only supports less complex passwords or passcodes (such as no special characters allowed), then consider replacing the device.

DO

- Use a unique password per site
- Store in a controlled, documented location
- Rotate after any staff turnover
- Change before the system goes live

DON'T

- Reuse passwords across ATG units
- Leave the factory default in place
- Write the password on the unit itself
- Share credentials over unencrypted channels

2 ISOLATE ATG SYSTEMS

Why this matters.
Thousands of ATG systems are directly reachable from the internet with no firewall in place. An ATG exposed to the open internet — even with a strong password — is a serious and unnecessary risk. Network isolation is a fundamental control.

01 Place the ATG behind a dedicated firewall or router

The ATG should never be connected directly to an internet-facing network. A dedicated firewall/router is the minimum acceptable configuration.

02 Segment the ATG onto its own network

Keep it off the POS, office, and guest Wi-Fi segments. Segmentation contains any breach and limits lateral movement.

03 Block inbound access by default

Configure the firewall to deny all inbound connections to the ATG unless specifically required. Only allow traffic on ports your ATG actually needs (commonly TCP 10001).

04 Confirm with your IT provider or ATG technician

If unsure, ask them to verify and document the network configuration before the system goes live.

05 Use a VPN for any remote access

If remote monitoring or management is required, require access through a VPN — never expose the management port directly to the internet.

PORT EXPOSURE
ATG systems commonly use TCP 10001. Confirm which ports are needed with your vendor and block all others at the firewall.

SHODAN VISIBILITY
Tools like Shodan index internet-exposed ATGs. Ask your IT provider to verify your system does not appear in public scans.

FLAT NETWORKS
A flat network where ATG, POS, and office systems share the same segment amplifies the impact of any single breach.

ANNUAL REVIEW
Firewall rules drift over time. Have your IT provider reconfirm the ATG network configuration at least once a year.

SETUP VERIFICATION CHECKLIST

- [ ] Default ATG passwords have been changed to unique, site-specific credentials
- [ ] New password is documented and stored securely near the console
- [ ] ATG is connected behind a dedicated firewall or router
- [ ] ATG is on a separate network segment from POS and office systems
- [ ] Inbound firewall rules deny all unnecessary ports
- [ ] Remote access (if required) is only permitted through a VPN
- [ ] IT provider or ATG technician has confirmed and documented network configuration

REFERENCE LINKS

CISA ICS Advisory	cisa.gov/ics — Advisories on ATG vulnerabilities and industrial control system security guidance
NIST SP 800-82r3	nvlpubs.nist.gov — Guide to OT/ICS security, including network segmentation and access control best practices
Veeder-Root Security	veeder.com — Official ATG security documentation and firmware update guidance for TLS-450PLUS and related systems
EPA UST Guidance	epa.gov/ust — US EPA underground storage tank program; compliance requirements relevant to ATG system operators

YOUR POLICY INCLUDES ZEGURO CYBER SAFETY

As a policyholder, you have complimentary access to Zeguro Cyber Safety — a resource included with your policy that can help you strengthen your cyber defenses and stay ahead of threats like this one. You can register for your Cyber Safety account here:

https://www.zeguro.com/federated

If you have questions or aren't sure where to start, our Cyber Concierge service is here to help — at no extra cost. You can reach the team directly at **concierge@zeguro.com**, or book a convenient time to speak with them here:

https://concierge-scheduling.zeguro.com