

KESTREL LABS

Kestrel Labs, Inc.
816 Congress Ave #2271,
Austin, TX 78701

<https://kestrellabs.net>
(800) 879-1234

Kestrel GridWatch 7 – Secure Deployment Guide

This summary outlines baseline hardening practices for deploying Kestrel GridWatch in regulated operational technology environments, consistent with IEC 62443 and NERC CIP expectations. The complete guide, including reference architectures and configuration templates, is available to licensed customers through the Kestrel support portal.

Network Placement:

- Deploy GridWatch servers within a dedicated OT/SCADA security zone. Never expose management interfaces directly to the internet or the corporate IT network.
- Terminate all remote access through an audited jump host or vendor-approved secure remote access solution.
- Permit only required protocol flows (IEC 61850, DNP3, IEC 60870-5-104) between the control center and substation gateways.

Baseline Hardening Checklist:

Area	Recommendation
Identity & Access	Enforce RBAC with least-privilege operator scopes; integrate with LDAP/AD or SAML SSO; require MFA for administrative roles.
Transport Security	Enable TLS 1.2/1.3 for all client and inter-node traffic; deploy mutual TLS to substation gateways using organization-issued certificates.
Integrity	Verify vendor-signed firmware and configuration bundles; enable dual-approval for privileged configuration changes.
Logging & Monitoring	Forward audit and system logs to a central SIEM; alert on cross-scope reads, failed authentications, and failover events.

Patch Management

Subscribe to Kestrel PSIRT advisories; apply security fixes within your organization's OT maintenance windows.

Before You Go Live:

- Remove or disable any default or evaluation accounts and sample configurations.
- Confirm backups are taken and restorable, and that the standby node is synchronized.
- Validate that only expected TCP services are reachable from each network zone.