ACS Export

Lenel OnGuard

For Lenel OnGuard:

1. **Scope the data you actually need.** For device/config/security analysis, you typically want: hardware status and communication logs (panels, readers, controllers, interfaces), event history (access granted/denied, forced door, door held open, tamper, comm loss, power fail), and alarm history.
2. **Confirm your access path.** Check which of these you have rights to: the OnGuard client (System Administration / Alarm Monitoring / Reports), the underlying SQL Server "AccessControl" database, DataConduIT (Lenel's WMI-based data service), or OpenAccess (the REST API, OnGuard 7.2+). Each unlocks a different export method.
3. **Pick an export method.**
    a. *Built-in Reports (easiest, limited).* In System Administration → Reports, run the canned reports for Events, Hardware Status, Audit Trail, Cardholders, etc. Set the date filter to the last 30 days. Use "Export" → CSV or Excel from the report viewer.
4. **Run the export with consistent parameters.** Use a single 30-day window (UTC vs. local time matters — pick one and document it), include the primary key/ID columns so you can join across exports, and pull lookup tables (event types, panel models, reader types) so codes are decodable later.
5. **Normalize and stage the output.** Save each data category as its own CSV (events.csv, panels.csv, readers.csv, audit.csv, cardholders.csv). If you want a single workbook, combine into an .xlsx with one tab per dataset. Keep raw timestamps and add a derived local-time column.
6. **Sanity-check before analysis.** Spot-check row counts against the OnGuard client (e.g., does events.csv match the count in Alarm Monitoring's event history for the same window?), confirm no truncation on long descriptions, and verify joins (panel ID in events matches panel ID in the hardware table).

Practical notes for telemetry analysis specifically: the EVENTS table is where most device-health signal lives — look for event types tied to comm loss, line fault, tamper, power fail, AC fail, low battery, and offline panels. The AUDIT table will show config drift (who changed what reader mode, access level, time zone). Pair those with the hardware inventory to flag devices that are misconfigured, chronically offline, or have stale firmware.