

From legacy risk to EST4 lifecycle readiness

An executive roadmap for Edwards EST3 fire alarm migration to EST4



December 2026 marks a critical lifecycle milestone for EST3.

Nearly three years after Edwards removed EST3 systems from their product portfolio, the platform is approaching end of life in December 2026. The milestone does not automatically disable a functioning system, but it changes the support environment as legacy components and repair options become less predictable.

Executive perspective

For organizations still operating Edwards EST3 fire alarm systems, the question is no longer simply whether each system functions today. Leaders need to understand whether every facility has a viable path forward as parts, repair options, and serviceability become more constrained.

Organizations that establish a structured fire alarm capital strategy before a failure occurs retain greater control over budget, schedule, operational continuity, and risk. A planned migration also creates time to evaluate system condition, compatibility, operational requirements, applicable codes, Authority Having Jurisdiction (AHJ) expectations, and enterprise priorities.

What leaders need to know

- The milestone changes supportability, not system functionality. An operating EST3 system may continue to function after December 2026, but component availability and repair paths are expected to become less predictable over time.
- Early planning preserves control. A proactive program provides more flexibility over scope, capital allocation, approvals, installation sequencing, and operational windows than a failure-driven response.
- EST4 migration may preserve viable investments. Compatible wiring, Signature Series devices, Genesis notification appliances, network infrastructure, and most EST3 local rail modules may be retained, subject to site review.
- The correct scope is site-specific. System condition, configuration, modifications, operational criticality, local code, and AHJ expectations determine what can remain and what should change.

Executive action

Why act now

- Identify all EST3 installations and establish an accurate installed-system baseline.
- Prioritize facilities based on operational criticality, lifecycle exposure, and supportability.
- Develop a phased migration and capital plan before a failure determines the timeline.

Plan the EST3 migration before a system failure determines the timeline

Fire alarm modernization is both an operational continuity decision and a capital-planning decision. Beginning the process while an EST3 system remains operational provides more time to assess alternatives, coordinate stakeholders, and determine the appropriate migration strategy.

The business case for a planned migration

Business return

Retain compatible infrastructure.
Preserve viable wiring, devices, cabling, and selected modules where condition, compatibility, and requirements allow.

Reduce future migration costs.
Use planned scope and phasing to avoid unnecessary replacement and manage labor, procurement, and shutdown windows.

Standardize enterprise platforms.
Apply a repeatable EST4 roadmap to reduce site-to-site variation and simplify documentation, training, and support.

Improve operational visibility.
Use modern status access and communications capabilities to provide clearer system awareness across facilities.

Risk mitigation

Reduce exposure to constrained legacy components.
Decrease dependence on parts and repair options that are expected to become less predictable.

Avoid emergency replacement decisions.
Make capital and system-design choices before an impairment or failure compresses the timeline.

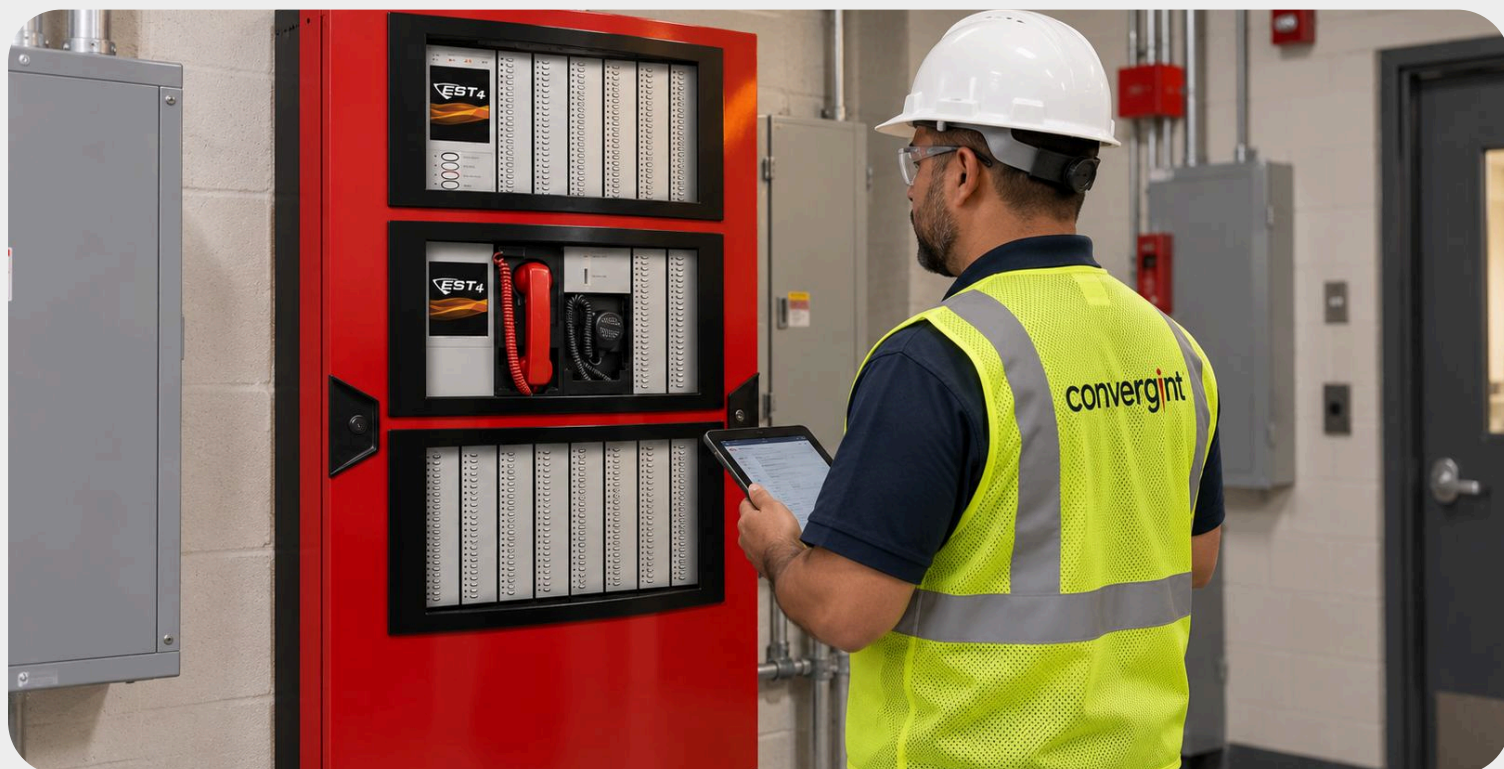
Support cybersecurity objectives.
Move toward a current platform with security capabilities designed for increasingly connected environments.

Improve long-term serviceability.
Align preventive maintenance, inspection, documentation, and lifecycle planning around Edwards' current platform.

EST3 to EST4 migration at a glance

Planning area	Legacy EST3 consideration	EST4 migration path
Lifecycle and supportability	EST3 is at the end of its lifecycle. Component availability and repair options are expected to become increasingly constrained.	EST4 is Edwards' current platform, designed for continued serviceability, system performance, and future expansion.
Initiating devices	Legacy smoke detectors use outdated technology. Additionally, older detectors may have reached the end of useful service.	Edwards currently offers an additional incentive of a ten-year extended warranty for customers who upgrade their legacy platform to EST4 and replace existing legacy smoke detectors for Optica smoke detection.
Migration investment	Reactive replacement after a failure can reduce an organization's ability to control scope, timing, and budget.	Compatible EST3 wiring, devices, network cabling, and most local rail modules may be retained, helping preserve usable infrastructure.
Network architecture	EST3 uses an earlier-generation architecture, and installed configurations can vary significantly by site.	EST4 supports flexible TCP/IPv6 networking using fiber, Ethernet, or copper, with multiple network classes and full-mesh options.
Cybersecurity	EST3 was developed before today's increasingly connected building and network environments.	EST4 includes a proxy firewall, AES encryption, secure communications protocols, and FIPS Pub 197 certification.
Operations and communications	Existing EST3 environments may rely on local displays and earlier-generation service, communications, and audio capabilities.	EST4 provides a full-color touchscreen, webserver-based system status access, email and email-to-SMS messaging, and high-fidelity audio across 200 channels.

Frequently asked questions about EST3 migration



01. Will an EST3 fire alarm system stop working after December 2026?

No. December 2026 does not automatically disable a functioning EST3 system. It represents a lifecycle milestone that changes the support environment as legacy component availability and repair options become less predictable.

02. Does an EST3-to-EST4 migration require replacing every fire alarm device and wire?

Not necessarily. Edwards documents backward-compatible migration options that may allow portions of the existing infrastructure to remain. Compatibility should be confirmed based on the installed system, equipment condition, configuration, modifications, and applicable local requirements.

Edwards is currently offering a 10-year extended warranty for those systems that upgrade from an EST3 to an EST4 and replace existing legacy smoke detectors for new Optica smoke detectors.

03. Can an EST3 migration be completed in phases across a campus or enterprise portfolio?

Often, yes. Organizations may be able to sequence migration panel by panel, building by building, or site by site. The appropriate approach depends on system interdependencies, compatibility, operational priorities, capital planning, and AHJ expectations.

04. How should organizations decide which EST3 systems to migrate first?

Start by assessing each system's condition, service history, component availability, and importance to facility operations. Convergent can use those findings, along with system dependencies and capital priorities, to build a sequenced migration roadmap.

How Convergent supports EST3-to-EST4 migration

Convergent combines fire and life safety expertise, local knowledge, system engineering, enterprise program management, and lifecycle services to help organizations develop an EST3 migration strategy appropriate for each facility.

The objective is not simply to replace legacy equipment. It is to determine the appropriate path forward based on system condition, operational needs, compatibility, and long-term lifecycle requirements while creating greater consistency across the enterprise.

- **Assess and prioritize.**
Convergent fire and life safety specialists evaluate installed-system condition, lifecycle exposure, compatibility, operational requirements, and site-specific migration readiness.
- **Engineer the migration strategy.**
Convergent develops retrofit and modernization approaches based on the installed environment and supports coordination with AHJs and other stakeholders while translating technical decisions into operational, schedule, and capital considerations.
- **Reduce disruption during migration.**
Where compatible and permitted, existing infrastructure may be retained and migration work phased around occupied buildings, mission-critical operations, and multi-site environments.
- **Standardize and sustain.**
Enterprise program management is supported by local service capabilities, preventive maintenance, inspections, reporting, monitoring, training, documentation, and long-range lifecycle planning.

Recommended next step: schedule an EST3 lifecycle assessment

A structured EST3 lifecycle assessment provides the technical baseline for a prioritized, budget-ready migration roadmap. It helps determine what can remain, what should change, which facilities should move first, and how EST4 migration can be sequenced around operational and capital priorities.

Protect the migration investment

Qualifying EST4 upgrade projects may be eligible for an Edwards 10-year extended product limited warranty on new equipment. Coverage may also extend to eligible existing Edwards field devices when the facility maintains an annual testing and inspection contract with an authorized Edwards partner and meets all other program requirements. Ask Convergent to evaluate eligibility as part of your EST3 lifecycle assessment.

*Edwards program terms, exclusions, approval requirements, and ongoing test and inspection requirements apply.

[Deadline June 30, 2027](#)

Schedule an EST3 lifecycle assessment

Convergent can help identify migration priorities and build a phased roadmap aligned with your operational needs, timeline, and budget.

[Build a migration plan](#)

Effective security and safety is a multi-layered approach involving people, processes, and technologies. Convergent-provided products and services are only one part of this approach, will not detect or prevent all threats or solve every risk, and should not be the sole method of security or safety. See the 'IMPORTANT PRODUCT SAFETY AND SERVICE INFORMATION' at convergent.com/terms before using a Convergent-installed system.