

SOFTWARE HOUSE

Product Bulletin – March 2026

In this bulletin, we provide important information on the Software House product portfolio.

Product Updates

OSDP Verified™ Certification Achieved for Software House's New Line of I/O Modules

Software House has successfully achieved OSDP Verified certification from the Security Industry Association (SIA) for our six Peripheral Device (PD) RS485 I/O modules. All devices passed the full suite of required OSDP test cases, including File Transfer (for centralized firmware updates) with no deficiencies noted. The OSDP Verified mark is fast becoming a requirement for OSDP-based projects, as it provides that extra level of assurance that products will interoperate.



The I/O modules are the industry's **first products** to include certification for Supervised Inputs, which were added to OSDP Standard v2.2.2.

OSDP provides AES-128 encrypted, bi-directional communication, protecting against eavesdropping, credential cloning, and line tampering—major weaknesses in legacy protocols like Wiegand. Certification ensures that a device implements these protections correctly.

Certified Devices:

- G2-RM-4E OSDP Enhanced Door Module
- OSDP-R8 OSDP 8-output expansion module
- OSDP-I8 OSDP 8-input expansion module
- OSDP-I16-R16 OSDP 16-input, 16-output expansion module
- OSDP-I16-R2 OSDP 16-input, 2-output expansion module
- OSDP-I4-R4 OSDP 4-input, 4-output expansion module

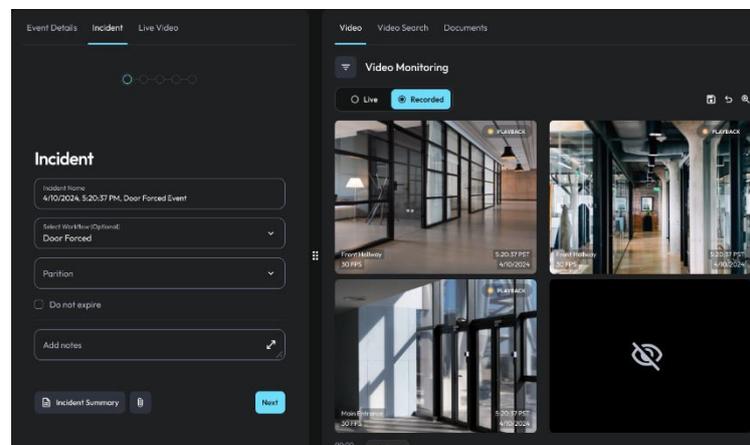
Key Capabilities:

- File Transfer Supported
- Tested to latest OSDP Specification v2.2.2
- Supervised Inputs Supported

[Link to SIA Verified Products page](#)

C•CURE v3.10.1 released to the Support Portal

We are pleased to announce the release of C•CURE v3.10.1, **introducing our native Incident Management solution to C•CURE IQ.** The Incident Management feature set is designed to help security teams manage the full lifecycle of incidents – or more critical security events. From creation to investigation, to documentation, this structured process allows security operators to document the incident thoroughly and respond quickly. They can attach images, files, video clips and screenshots to provide context and fill in SOP steps to ensure every detail is captured.



This release also introduces a powerful, customizable workflow engine (with advanced license option) that allows security teams to build guided SOP processes for any type of incident—ranging from high-severity security events to non-security incidents such as a medical emergency. Operators are then guided through these workflows in real time, ensuring consistent documentation, improved compliance, and faster, more coordinated response across the security team.

| Part Number | Description | MSRP | CAT |
|-------------|--|----------|-----|
| CC-IMW-SM | C•CURE IQ Incident Management Workflow, Small, Series L to N | \$6,750 | MFG |
| CC-IMW-MD | C•CURE IQ Incident Management Workflow, Medium, Series P to R | \$12,150 | MFG |
| CC-IMW-LG | C•CURE IQ Incident Management Workflow, Large, Series RP to T | \$22,950 | MFG |
| CC-IMW-SM-S | C•CURE IQ SSA Uplift for Incident Management Workflow, Small, Series L to N | \$1,550 | SSA |
| CC-IMW-MD-S | C•CURE IQ SSA Uplift for Incident Management Workflow, Medium, Series P to R | \$2,750 | SSA |
| CC-IMW-LG-S | C•CURE IQ SSA Uplift for Incident Management Workflow, Large, Series RP to T | \$5,250 | SSA |

For more information on C•CURE IQ Incident Management, please view our [Incident Management video](#) or [Configuring a Workflow video](#).

C•CURE v3.10.1 includes support for Windows Server 2025

C•CURE 3.10.1 is available now through the [Software House Support Portal](#).

C•CURE TLS 1.2 Default Certificate Has Expired

The default C•CURE 9000 TLS 1.2 host certificate used for secure communication with iSTAR controllers **expired on February 18, 2026**. Any panels still using this default certificate will lose the ability to re-establish communications with the C•CURE server after any interruption. A planned certificate update is required to avoid outages.

Systems Affected:

iSTAR eX, iSTAR Edge, iSTAR Ultra / Ultra SE, and iSTAR Ultra LT controllers using TLS 1.2 with the default certificate. Controllers using Host-based, Controller-based, and Custom certificates are not affected.

New Recovery Guidance Available

A new TAB—**iSTAR Controller Recovery After February 18, 2026**—has been published to provide a step-by-step recovery process for systems that did not update certificates before the expiration date.

Visit the [Software House Support Portal](#) to access the TABs, FAQs, and instructional videos, and begin remediation immediately.

Connected Partner Program – Compatibility Matrix Update

We are excited to announce the launch of our new [Software House C•CURE 9000 Integration Compatibility Matrix](#), designed to help maximize partner and product information in an organized, user-friendly interface.

Key Features:

- Clear Product Listings: Easily review our integrating partners' company descriptions and product listings.
- Detailed Compatibility Information: Discover which software and hardware combinations are supported.
- Third-Party Integration: Check compatibility with select partner devices and solutions.
- Regular Updates: Stay informed with the latest product relationships and support statuses.

Whether planning a new installation or upgrading existing systems, the Compatibility Matrix helps you optimize your security ecosystem for reliability and performance.

Connected Partner Program Integrations – Updates

It has been a busy quarter for our partners updating and adding new integrations for C•CURE 9000. Please see the snapshot of integration updates below. The [Compatibility Matrix](#) is up to date with all integration changes.

For additional integration information and support, please see the Partner Contact information tab available in the partner products listed in the compatibility matrix.

Prior to updating C•CURE 9000 software, you must confirm that integrations utilized on the system are certified for that software version. Integrations not certified for that version may not function correctly and cause issues on the C•CURE 9000 system.

| Connected Partner | Integration | Integration Type | C•CURE version | Update or New | Part Number |
|-------------------|---------------------|-----------------------|---------------------|---------------|-------------------------|
| Alert Enterprise | ServiceNow Guardian | Visitor Management | 3.0 | NEW | CC9WS-ALRTESNG |
| Allegion | AD NDE LE | Wireless Locks | 3.10 | Update | N/A - Hardware |
| Assa Abloy | Aperio | Wireless Locks | 2.8, 2.9, 3.0, 3.10 | Update | N/A - Hardware |
| BACnet | BACnet | Building Management | 3.10 | Update | CC9-BACNET-SM, -MD, -LG |
| Crisis24 | TopoOne | Alarm | 2.9 | NEW | CC9WS-CRISIS24 |
| Encode Labs | CR-PRO-V2-QRCG | Visitor Management | 2.8, 2.9, 3.0, 3.10 | NEW | CC9000-ELQRCG |
| Encode Labs | CR-PRO-V2-ANPR | Parking Management | 2.8, 2.9, 3.0, 3.10 | NEW | CC9000-ENANPR2 |
| Geutebruck | G-Connect | Video Management | 3.10 | Update | CC9WS-GCONNECT |
| HID | Origo Bridge | Credential Management | 3.0 | NEW | CC9WS-HIDOB |
| HID | Amico Connector | Biometric Reader | 3.0 | NEW | CC9000-HIDAMICO |
| Kone | Access 1000 | Elevator | 3.0 | NEW | CC9-KONEAC1-SM/MD/LG |
| Milestone | VideoPush | Video Management | 3.10 | Update | CC9-MSTVID-SM/MD/LG |
| Milestone | Xprotect Access | Access Control | 3.10 | Update | CC9WS-MSTVD-SM/MD/LG |

| | | | | | |
|----------------------|--------------------|-----------------------|------|--------|------------------|
| Savance | Visitor Management | Visitor Management | 3.10 | Update | CC9WS-SAVANCE |
| Securitas Healthcare | Mobileview | Real Time Location | 3.0 | Update | CC9000-STANLEYHC |
| SoloInsight | CloudGate | Visitor Management | 3.10 | Update | CC9000-SOLOCG |
| Suprema | Biometrics | Biometric Reader | 3.10 | Update | CC9000-SUPREMA |
| Sureview | Enterprise | PSIM/Alarm | 3.10 | Update | CC9-SUREVIEW |
| SwiftConnect | AccessCloud | Credential Management | 3.10 | Update | CC9-SWIFT |

For information on the Connected Partner Program, please contact BE-US-ConnectedPartner@jci.com

OEM Program Updates

PLAI Integration Part Numbers Update

Please note that PLAI integration part numbers will be removed from the upcoming price book. Going forward, all PLAI-related integration work will be handled exclusively through Software House Professional Services.

For assistance, quotes, or additional details on PLAI integration support, please contact the Software House Professional Services team.

Systech and Digi Hardware Communications Products No Longer Available

Please note that the legacy serial-to-Ethernet communications products from Systech and Digi are no longer available and will be removed from the April price book. This includes:

- CC800-906 DigiBoard 8-port Serial I/O Board
- TRM-6008 Systech 8-port Device Server
- TRM6204 Systech 4-port Device Server
- TRM6102 Systech 2-port Device Server

Pricing Updates

Software House Hardware Products

The current 8% tariff surcharge that applies to Software House hardware products will now be rolled into a new 8% higher MSRP, effective April 13. This will help streamline the ordering and invoicing processes for these products.

Upcoming OEM Price Increases – Effective April 1st

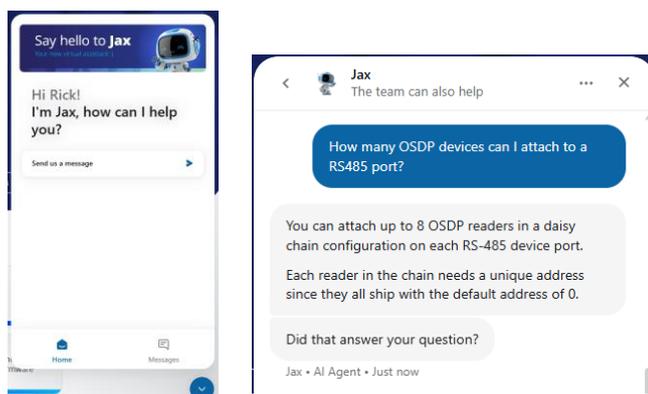
Please be advised that several OEM partners have announced price increases effective April 1. The affected manufacturers include Wavelynx, Schlage, LifeSafety Power, Penguin/EverRun, and Dormakaba. Updated pricing will be reflected in the next price book release.

- Wavelynx – 10% increase for Ethos readers
- Schlage – 9.5% increase for readers and locksets
- LifeSafety Power – 3% increase across the board
- Penguin/everrun - 3% increase
- DormaKaba – various increases

Technical Support

Have You Met Jax Yet?

Say hello to our new virtual AI assistant, Jax, on the Software House support portal – he may turn out to be your best friend! Ask him anything – you'll be surprised by the depth of knowledge that will be provided. And please provide feedback – we're always looking for ways to improve our support experience.



Are You Signed Up for Software House Cybersecurity Advisories?

Software House C•CURE software and iSTAR controllers undergo continuous internal and external security testing. Customers can report suspected issues through our cybersecurity site, and when a vulnerability is identified, we issue advisories to subscribed users, integrators, and consultants, followed by updates if a fix is required.

If you have not signed up yet, please do!

[Register Now | Johnson Controls](#)

A list of current advisories can be found on the Johnson Controls web site: [Product Security Advisories \(johnsoncontrols.com\)](#). Note that this list includes all Johnson Controls products.

Connect with Us



For additional information, please visit www.swhouse.com.

©2026 Johnson Controls. All rights reserved. All trademarks are the property of their respective owners. Product offerings and specifications are subject to change without notice. Actual products may vary from photos. Not all products include all features. Availability varies by region; contact your sales representative.