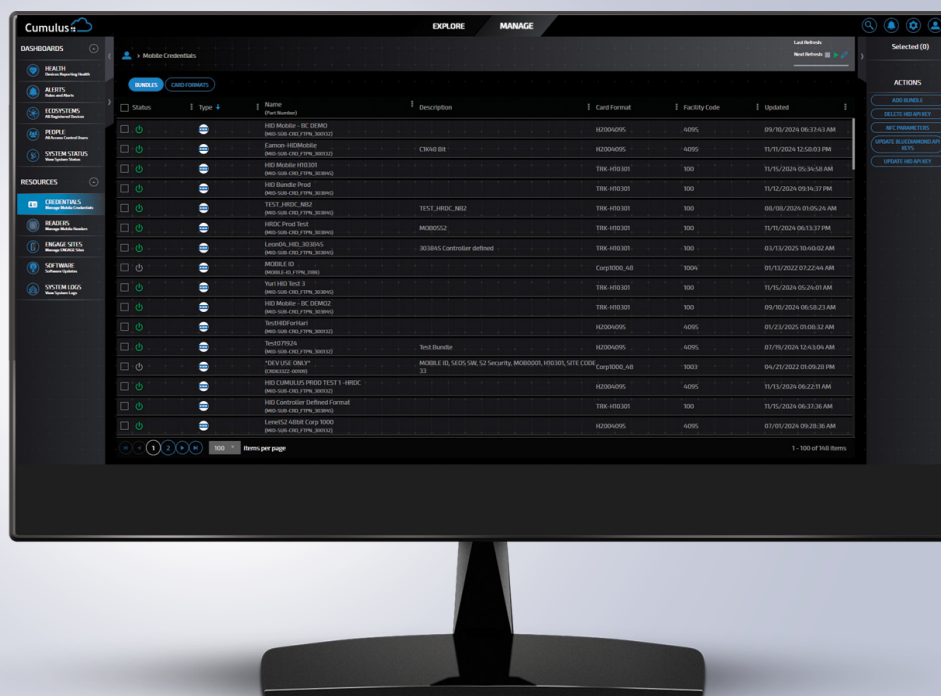


Manage and monitor your LenelS2 systems from the cloud



Cumulus™ is a Honeywell cloud-based solution that provides the capability to monitor the health of platform-connected devices, manage licenses (Magic Monitor), and access the Cumulus Credential Factory to enable and manage mobile credentials.

With Cumulus Health Monitoring, system users can monitor the health of devices across their entire ecosystem of connected physical security systems from a single screen. Additionally, security personnel can now receive alerts when devices exceed predetermined thresholds to take proactive action and resolve concerns before larger issues arise.

Cumulus securely brokers LenelS2's entire Mobile Credentials portfolio. The Credential Factory manages the mobile credential lifecycle between LenelS2's physical access control systems (OnGuard or NetBox), any required third-party partners (e.g. NFC wallet providers), and end-user mobile devices. It also keeps track of NFC Credential activations and renewals.

Cumulus greatly enhances mobile credential management, device ecosystem monitoring, and proactive system maintenance.

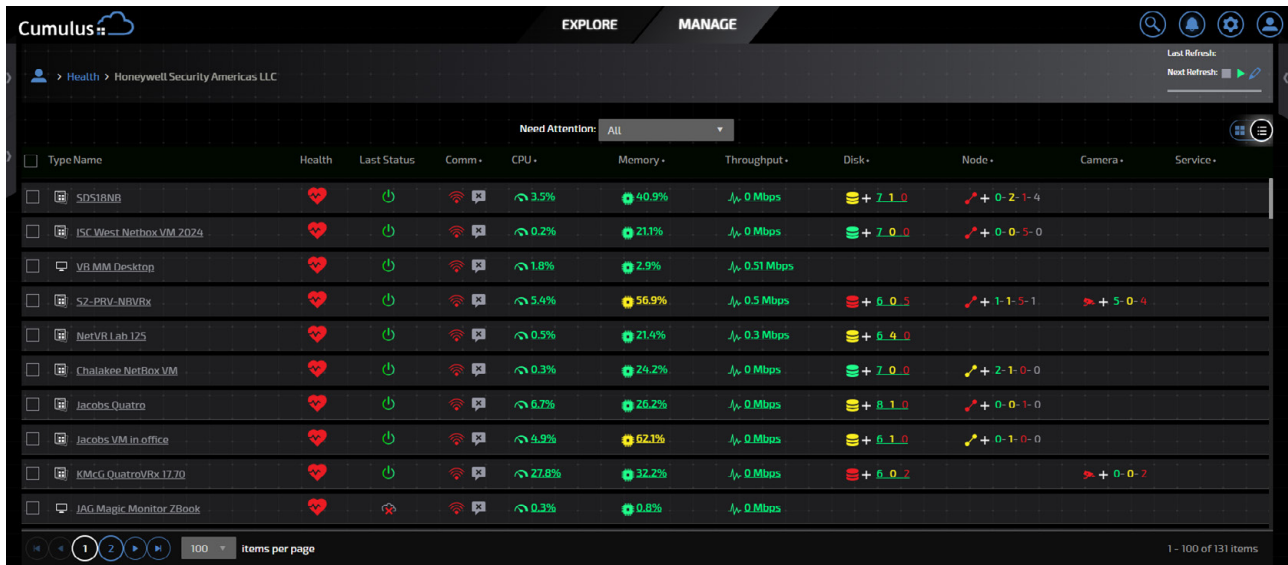
Key Features

Credential Factory Services

- Mobile credential account setup & onboarding
- Issuance, management & tracking of BlueDiamond Mobile Credentials
 - Near Field Communication (NFC)
 - Employee Badge in Apple Wallet
 - Corporate Badge in Google Wallet
 - Bluetooth (BLE)
 - Apple phone compatible
 - Android phone compatible
- Issuance & management of HID Mobile Credentials (BLE)

Device Monitoring Services

- Monitors device diagnostics to proactively manage and maintain systems to reduce unexpected system outages & onsite maintenance appointments
- Monitored device diagnostics include:
 - Device connection to Cumulus
 - Access Control System
 - Cameras
 - Nodes
 - CPU utilization
 - Throughput of devices on network
 - Disk space availability
 - Memory utilization of devices
 - Running monitoring services

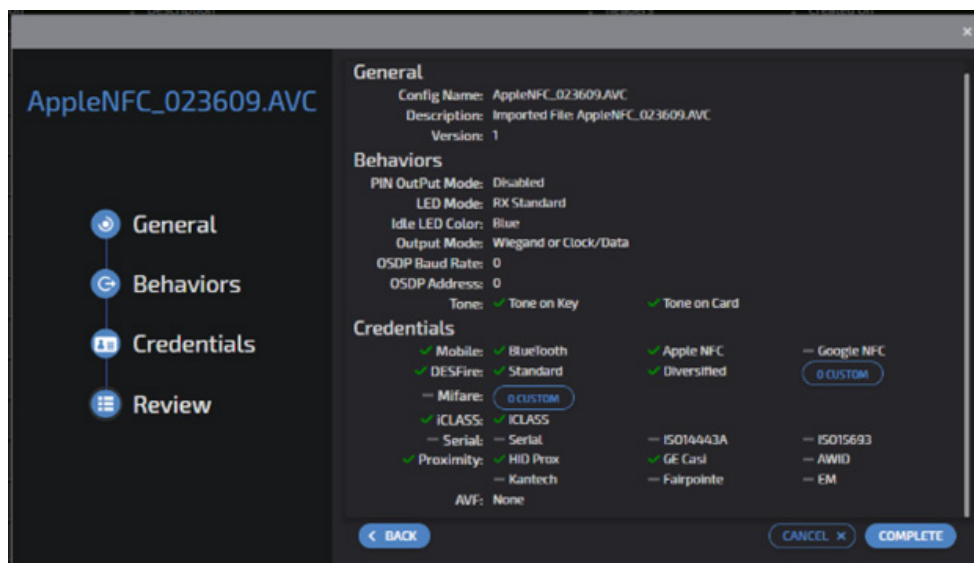


Cumulus Health Page displays device diagnostics.

BlueDiamond Reader Secure Configuration Tool

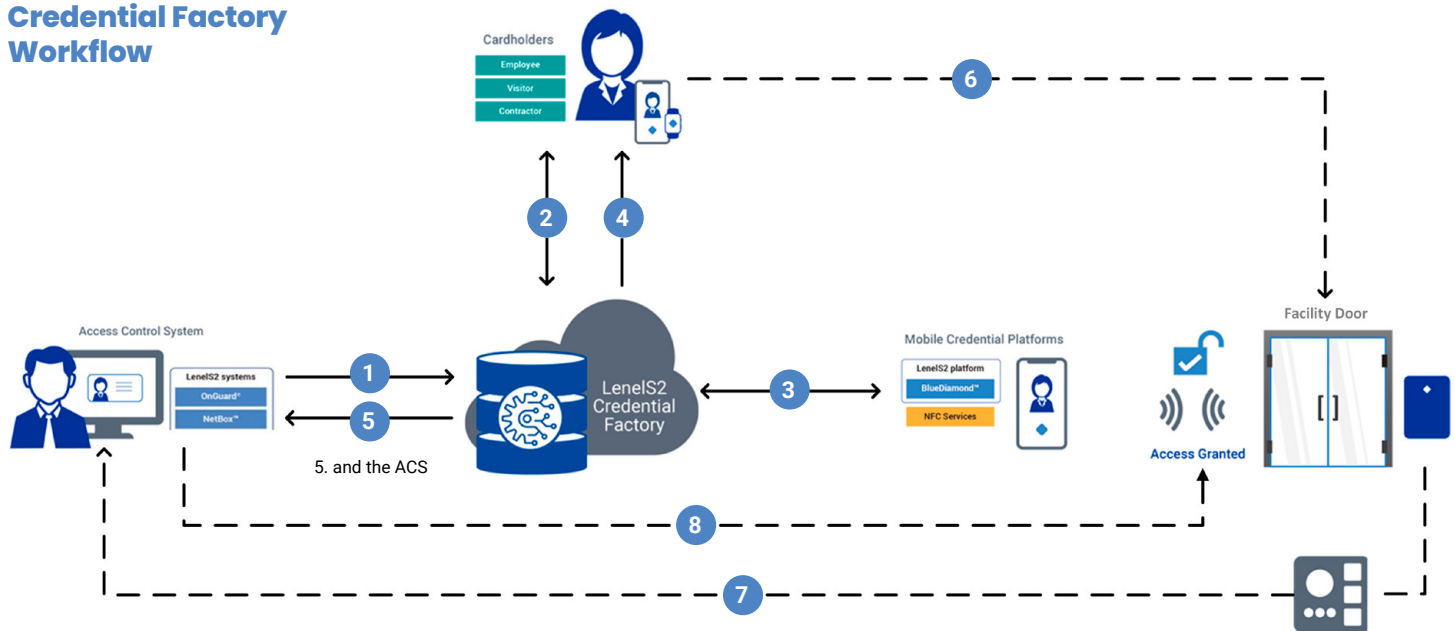
- Cumulus provides the capability to remotely configure BlueDiamond readers, allowing system users to:
 - Create, view, edit & delete readers within Cumulus
 - Create, import, export & customize reader configurations within Cumulus
 - Import & export reader formatters within Cumulus

LenelS2 Solution	Health Monitoring	Credential Factory
NetBox	5.6.2 & later	5.6.2 & later
VRx	4.9.10 & later	N/A
NetVR	4.9.10 & later	N/A
NetBox Global	3.1.4 & later	N/A
OnGuard	8.0 & later	8.1 & later
Magic Monitor	4.2 & later	N/A



Cumulus Reader Configuration Tool, allowing reader config of supported behaviors & credential types.

Credential Factory Workflow



1. Credential is issued in the Access Control System (ACS), and data is sent to the Credential Factory.
2. Credential Factory sends a message to the Cardholder requesting to download the BlueDiamond Mobile App and activate the credential using their phone number. Activation information from the Cardholder is then sent back to the Credential Factory.
3. Credential Factory sends activation information to the Mobile Credential Platform, which sends back the validated credential. This information is sent from the Credential Factory to:
 4. The Cardholder
 5. And the ACS.
6. The mobile credential user then uses the NFC Credential in their mobile device's wallet on the reader.
7. The reader communicates via the controller back to the ACS, which receives the mobile credential request to unlock the door.
8. The ACS validates the request and sends transmission back to the facility door, effectively unlocking it.

Key Cumulus Integrations

- OnGuard
- NetBox
- VRx
- NetVR
- Magic Monitor
- BlueDiamond BLE Credential Server
- Schlage (Allegion) Wireless Locks
- HID Origo
- Apple Wallet
- Google Wallet



Cloud-based
monitoring and
administration

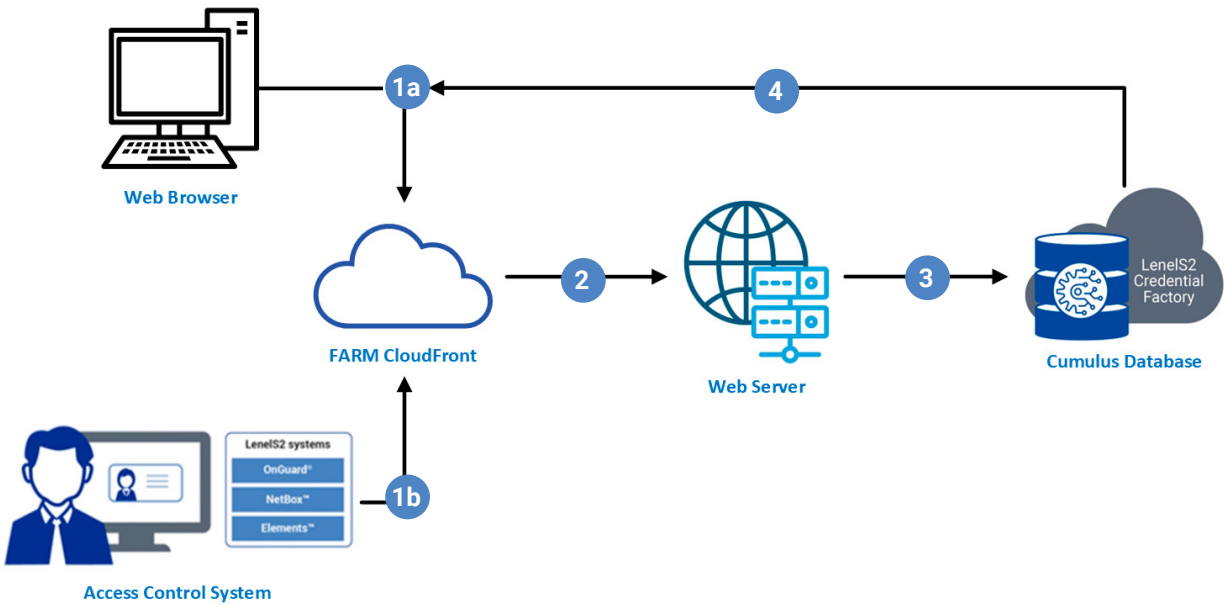


Proactive
health
monitoring

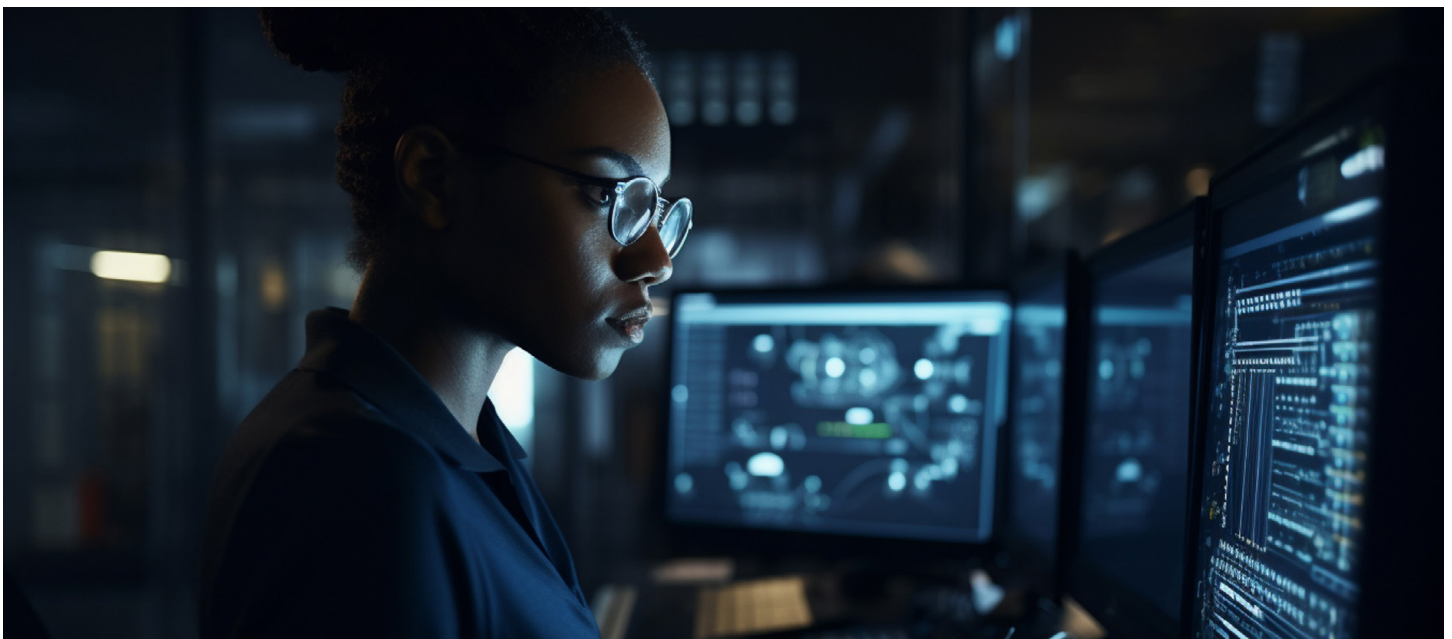


Unlock
additional
LenelS2
product features
and benefits

Health Monitoring Workflow



- 1a.** The client's Web Browser makes an HTTPS request to the File Access and Replication Manager (FARM) CloudFront to fetch information related to device diagnostics, health, and more.
- 1b.** The Access Control System makes an HTTPS request to the FARM CloudFront to update information related to device diagnostics, health, and more.
- 2.** The FARM CloudFront makes an HTTPS request to the Web Server to fetch/update data from the Cumulus database.
- 3.** The Web Server calls to the Cumulus database to fetch/update the required information.
- 4.** If the data is being fetched, the Cumulus database sends the information back to the Web Browser.



Cybersecurity

Secure Software Development Lifecycle (SSDLC) ensures product security practices are implemented consistently and effectively and that the product development process follows a vetted, standardized method of secure development.

To accomplish this, engineering and cybersecurity experts define appropriate cybersecurity design guidelines and continuously evaluate the security posture of the product from its initial design concept to its release:

- Data at-rest (AES 256) & transit (TLS 1.2+)
- ISO27001 certified
- CSA Star Level 1
- IEC/ANSI/ISA 62433 4-1 certified
- Recurring third-party pen testing by policy
- Third-party static and dynamic application security testing

Solution Sourcing

Ready to take the next step? Get connected and explore how Cumulus can support your goals:

- For Cumulus Account access, please contact orderentry.lenels2@honeywell.com.
- To learn more about Cumulus, contact your LenelS2 Regional Sales Manager (RSM).
- Visit lenels2.com for additional resources and product details.

Let's build what's next—together.

