

CYBERSECURITY AND DATA PRIVACY SHEET

Johnson Controls Lifecycle Manager

Streamline every stage of your site's lifecycle with a unified, intelligent platform offering seamless oversight, efficiency, and control from a single, intuitive dashboard.

The Johnson Controls Lifecycle Manager streamlines facility management from design to renewal, centralizing control of HVAC, lighting, and energy systems. With real-time insights, predictive analytics, and automation, it optimizes performance, reduces costs, and extends asset life. Powerful tools for sustainability, compliance, and risk mitigation enhance efficiency, occupant comfort, and adaptability. The intuitive dashboard provides portfolio-level insights, service recommendations, and remote Metasys access, ensuring seamless collaboration and maximum ROI.



Data encryption

AES-256 encryption protects data-at-rest and TLS-1.3 for data-in-transit



User management

Integrates with industry leading federated identity such as Entra ID and Okta to manage users and enforce password policies



Role-based access control (RBAC)

Assigns permissions according to authorized roles



Network security

Web Application Firewall (WAF) protects against sophisticated attacks



Validated authentication

For non-federated accounts Multi-Factor Authentication (MFA) is enforced. MFA is also configurable through federated identity integration



Vulnerability monitoring

The Lifecycle Manager environment is continuously monitored for cyber-events using automated tools

About Lifecycle Manager

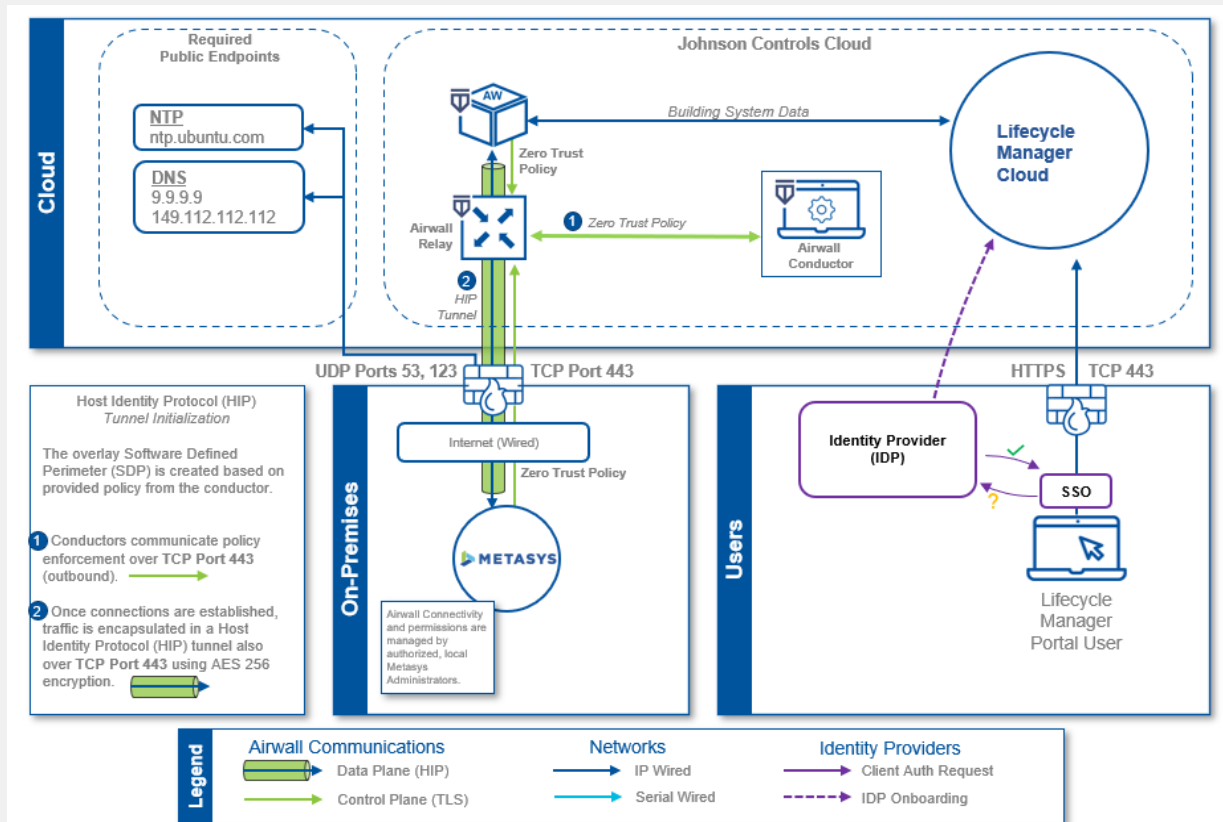
Lifecycle Manager is your all-in-one solution for managing and operating your building automation system. Designed to simplify workflows while fortifying defenses, this powerful platform integrates cybersecurity at its core - ensuring every stage of your building lifecycle remains protected against evolving threats.

With built-in encryption, automated compliance monitoring, and real-time threat detection, organizations can confidently manage their operations without compromising security. Stay ahead of risks, streamline processes, and safeguard your building automation system with a portal that combines efficiency with resilience

Learn more [here](#)



How Johnson Controls Lifecycle Manager protects your people and assets



* For Metasys 14.1 hardening details please visit <https://www.johnsoncontrols.com/trust-center/cybersecurity/resources>

ISASecure® Security Development Lifecycle Assurance (SDLA) certified

All Johnson Controls global development locations comply with this security lifecycle development certification conforming with ISA/IEC 62443-4-1 and encompassing all associated brands. This certification reinforces our customer commitment to provide cyber-resilient solutions that follow best-in-class industry practices.



ISASecure® Security Development Lifecycle Assurance (SDLA) program certified

Data privacy

Johnson Controls has a Global Privacy Office and a Global Privacy Program, involved at the beginning and throughout the design and development of our processes, activities, products, services and solutions, in accordance with internationally accepted principles of Privacy by Design. The Johnson Controls Global Privacy Program is led by our privacy experts and designed in accordance with the global privacy and data protection laws. In addition to product-related information provided in this section, please visit www.johnsoncontrols.com/trust-center/privacy for more details on our Global Privacy Program.

Personal data processing details of Lifecycle Manager:

See below details on each category of personal data processed by Lifecycle Manager, types of personal data within each category and the purpose of processing each type:

Personal data category	Type of personal data	Purpose of processing
User information	· Account administrator's full name · Account administrator's business address · Account administrator's email ID · Account administrator's business phone number · User's full name · User's business address · User's email ID · User's business phone number	· Portal access management · User identification · User notification · Account management
End customer contact information	· End-customer contact person's full name · End-customer contact person's business address · End-customer contact person's email ID · End-customer contact person's business phone number	· Identification of and communication with End-customer
System Integrator contact information	· System Integrator contact person's full name · System Integrator contact person's business address · System Integrator contact person's email ID · System Integrator contact person's business phone number	· Identification of and communication with System Integrator

Retention and deletion of personal data

Johnson Controls has a Global Records Management Program which includes a Global Records Retention Policy and procedures. The purpose of our Global Records Management Program is to detail the responsibilities and working instructions necessary for the use, maintenance, retention or deletion of data Johnson Controls is processing. The Global Records Management Program applies to all worldwide locations and legal entities controlled by Johnson Controls.

When Johnson Controls processes personal data on behalf of a customer, **and/or a partner**, or when products are operating on the customer's site **and/or a partner site**, to the extent provided by a product's functionalities and upon a system's configuration, customers **and/or partners** may access such data and delete it at any time on their own. The default retention periods as predefined by Johnson Controls apply. See the below table for the default retention periods applied to **Lifecycle Manager**.

If, during the 90 days following the end of a subscription, Johnson Controls receives from customer **or partner** a request to export a customer's **or partner's** personal data, Johnson Controls will provide the customer **or partner** with an export of their personal data in a structured commonly used machine-readable format as reasonably determined by Johnson Controls. **Such request must be made to the Johnson Controls Field Support Center (FSC).** If not already deleted by the customer **and/or partner** using available internal product deletion features, the customer's **and/or partner's** personal data will be deleted after such 90-day period or as otherwise agreed. During any retention period, the provisions of the underlying agreement that are applicable to the retention and product of a customer's **and/or partner's** personal data continue to apply.

Default retention periods for customer personal data are as set forth in the table below:

Personal Data category	Retention period	Reason for retention
User information	· For the period of Systems Integrator's active subscription +90 days	· User account management
End-Customer Contact Information	· For the period of Systems Integrator's active subscription +90 days	· Notifications to End-Customer
System Integrator Contact Informationn	· For the period of Systems Integrator's active subscription +90 days	· Maintenance of an active subscription

Sub-processors for Lifecycle Manager

Please see below the list of current sub-processors used to support Lifecycle Manager:

Sub-processor	Service type	Location of data center
Microsoft Azure Cloud	· Third Party Cloud Hosting	· United States

Cross-border data transfers

Many countries and jurisdictions have laws governing the transfer of personal data. As a multinational organization, Johnson Controls has substantial experience in dealing with cross-border transfer issues and restrictions. When Johnson Controls processes personal data for our own purposes or on behalf of a customer, we use the following transfer mechanisms which can assist our customers:

Binding Corporate Rules (BCRs)	The Johnson Controls BCRs are designed to ensure an adequate level of protection for personal data no matter where in world it is processed by Johnson Controls. With respect to the European Union (EU), the Johnson Controls BCRs have been specifically approved by the EU Data Protection Authorities (DPAs) for transfer of EU personal data globally within Johnson Controls.
Asia-Pacific Economic Cooperation Cross-Border Privacy Rules (APEC CBPR)	The CBPR is a government-backed privacy certification which demonstrates that Johnson Controls complies with internationally recognized data privacy protections and is the framework approved for the transfer of personal data by Johnson Controls between participating APEC member economies: the United States, Mexico, Japan, Canada, Singapore, Republic of Korea, Australia, Chinese Taipei and the Philippines.
Asia-Pacific Economic Cooperation Privacy Recognition for Processors (APEC PRP)	The PRP is a government-backed privacy certification that enables Johnson Controls to demonstrate to customers our accredited enterprise-wide Privacy Program, and to transfer data processed on behalf of our customers (including our cloud solutions) between the United States, Mexico, Japan, Canada, Singapore, Republic of Korea, Australia, Chinese Taipei and the Philippines. Please see the PRP Directory and the Johnson Controls PRP TRUSTe validation page for more information.
EU Standard Contractual Clauses (SCCs)	Johnson Controls incorporates the EU's approved standard contractual clauses, also referred to as the "Model Contract," into the Johnson Controls Data Protection Agreement located at www.johnsoncontrols.com/dpa to afford the contractual protection under the SCCs to our customers.
US Data Privacy Framework (DPF)	Johnson Controls is certified under the US Data Privacy Framework for transfers of personal data from the EU, United Kingdom and Switzerland to the United States.

Please note that this document is for customer guidance purposes only, is not legal advice and is subject to changes from time to time due to modifications of our solutions. Johnson Controls is not a law firm and does not provide legal advice. While Johnson Controls products and solutions are designed for use in compliance with applicable law, implementation and deployment of Johnson Controls products and solutions should be reviewed by appropriate customer advisors and stakeholders for such compliance.

We combine our critical focus on cybersecurity and privacy with digital innovation and building expertise to deliver smart building solutions.

To learn more, please visit our website at www.johnsoncontrols.com/trust-center or contact us at TrustCenter@jci.com.

Visit johnsoncontrols.com or follow us [@johnsoncontrols](https://twitter.com/johnsoncontrols)

© 2025 Johnson Controls. All rights reserved. OB2502008 |
GPS0066-CE-EN Rev A 2025-10-10

