



Chiller Access Manager

Cybersecurity and data privacy

General cybersecurity features

Security is designed into all Johnson Controls products, hardware, hosted services and software. YORK® Chiller Access Manager Web and Mobile Application incorporates industry and government best practices to help keep your building, systems and data secure.



Data encryption

Various forms of encryption to protect sensitive data at rest and in transit. Examples include disk encryption, FIPS 140-2 compliance, AES-256 and TLS-1.3



Role-based access control (RBAC)

Roles and permissions managed through Okta allow for the application of the principle of least privilege



User management

A range of features to manage users, including the ability for administrators to easily invite and remove users. Administrators can choose to limit access to a given chiller serial number – to their own employees and to external contractors, and user access code generation history is traceable



Validated authentication

Authentication using Okta for external users and Azure Entra ID for Johnson Controls users

About YORK® Chiller Access Manager

YORK Chiller Access Manager is a feature that provides secure access to YORK chiller control panels. Users download the app, create an account, and use the app to generate dynamic access codes.

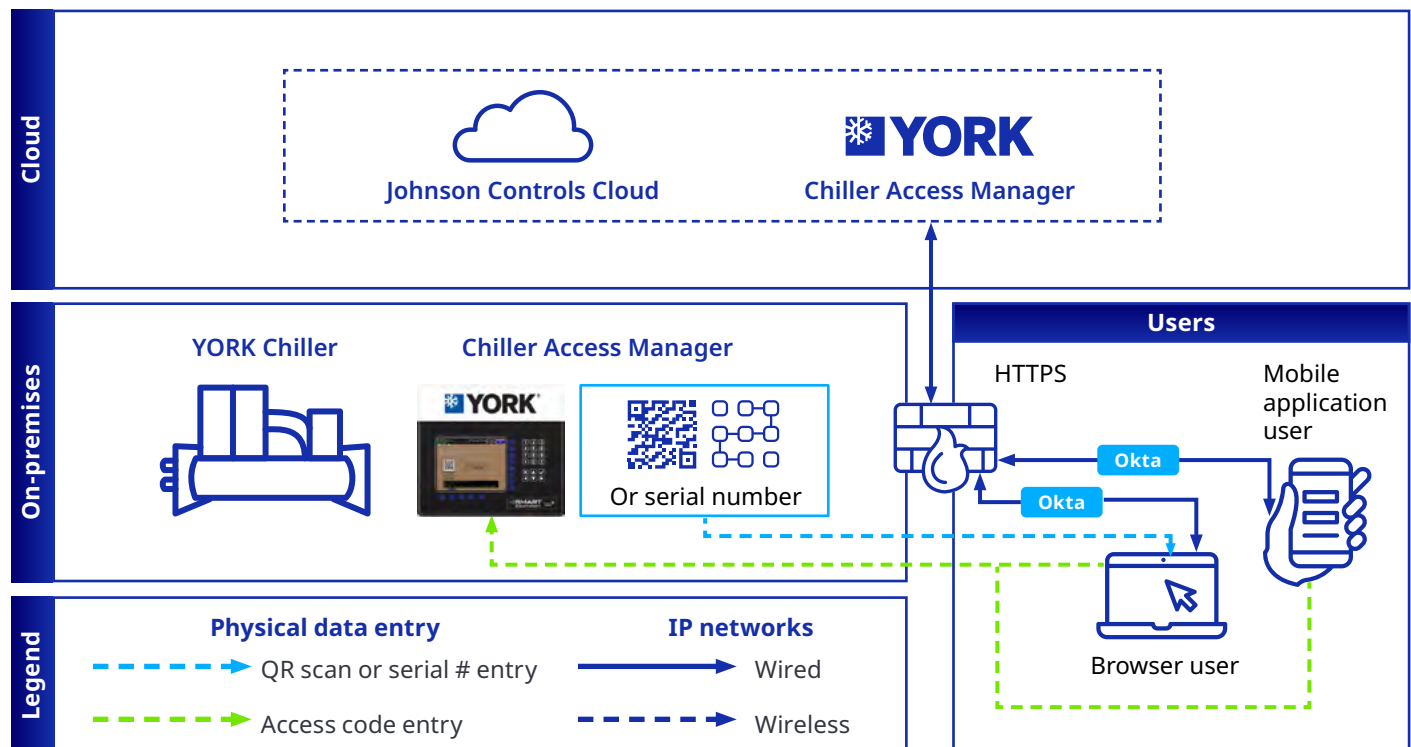
Owners can use YORK Chiller Access Manager to view and control who can operate, maintain and service the chiller. This ensures protection of an asset that is critical to facility operation. To invalidate all outstanding access codes, owners can obtain a new private key and reinitialize security.

[Learn more here](#)

Key benefits

- Prevent unauthorized access
- Reduce operational risk
- Meet compliance requirements
- Gain peace of mind

YORK® Chiller Access Manager architecture and data flow



Data flow specifics will depend on the components chosen and how the solution is implemented.

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® Component Security Assurance (CSA) certified

Johnson Controls became the industry's first to achieve ISA/IEC 62443 CSA certification for its YK and YZ Centrifugal Chillers, awarded on September 15, 2021. These chillers are a strategic solution for data centers worldwide, emphasizing our leadership in secure and reliable cooling technologies.

Johnson Controls is committed to expanding its portfolio of ISASecure-certified products. For a comprehensive list of our current certifications, please visit the [ISASecure website](#). We continue to pursue additional certifications across various chiller models, underscoring our dedication to delivering secure and reliable solutions.

Our organization remains focused on the future, continually striving to earn additional recognition and drive excellence across the industry.



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 Privacy Program is led by our privacy experts and designed with the most stringent global privacy and data protection laws. In addition to the product-related information provided in this section, please visit www.johnsoncontrols.com/trust-center/privacy for more details on our Global Privacy Program.

a. Personal data processing details

See below details on each category of personal data processed by YORK Chiller Access Manager Web and Mobile Application, types of personal data within each category and the purpose of processing each type.

Personal data category	Type of personal data	Purpose of processing
Work-related identification details	• Full name • Full email address • User ID • Phone number • Preferred language • Picture (optional)	Account management

b. 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, or when products are operating on customer site, to the extent provided by a product's functionalities and upon a system's configuration, customers may access such data and delete it at any time on their own. The default retention periods that are predefined by Johnson Controls apply. See the below table for the default retention periods to YORK Chiller Access Manager Web and Mobile Application.

If, during the 90 days following the end of a subscription, Johnson Controls receives a request from a customer to export the customer's personal data, Johnson Controls will provide the customer with an export of their personal data in a structured commonly used machine-readable format as reasonably determined by Johnson Controls. Such requests must be made to the JCI Digital Customer Support email currently at BE-COSC-ChillerSupport@jci.com. If not already deleted by the customer using available internal product deletion features, the customer'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 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 and account information	For the subscription period +90 days	• Required for user identification • Required for user notifications • Required for audit records of actions taken by specific users for security and compliance • Tailoring the user experience based on individual profiles and preferences • Enables a system administrator to generate a user account report that the administrator may use to take action on dormant accounts

c. Sub-processors for YORK Chiller Access Manager Web and Mobile Application

Please see below the list of current-sub-processors utilized for YORK Chiller Access Manager Web and Mobile Application.

Sub-processor	Service type	Location of data centers
Microsoft Azure Cloud	Third-party cloud hosting	United States
Oracle	Subscription management	United States

d. 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 utilize the following transfer mechanism that can assist our customers:

Sub-processor	Location of data centers
Binding Corporate Rules (BCRs)	The Johnson Controls BCRs are designed to ensure an adequate level of protection for personal data no matter where in the 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.

To learn more about our cybersecurity and privacy solutions, visit our website at www.johnsoncontrols.com/trust-center or contact us at TrustCenter@jci.com.

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.

About Johnson Controls:

At Johnson Controls (NYSE:JCI), we transform the environments where people live, work, learn and play. As the global leader in smart, healthy and sustainable buildings, our mission is to reimagine the performance of buildings to serve people, places and the planet.

Building on a proud history of 140 years of innovation, we deliver the blueprint of the future for industries such as healthcare, schools, data centers, airports, stadiums, manufacturing and beyond through OpenBlue, our comprehensive digital offering.

Today, Johnson Controls offers the world's largest portfolio of building technology and software as well as service solutions from some of the most trusted names in the industry.

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