Cloudvue

Cloudvue Hardening Guide

GPS0058-CE-EN
Version 24.12
Rev B
Revised 2025-02-28

Johnson Controls

Introduction

Our solution provides peace of mind to our customers with a holistic cyber mind set beginning at initial design concept, continues through product development, and is supported through deployment, including a rapid incident response to meet the comprehensive and evolving cybersecurity environments.

The Cloudvue Hardening Guide provides cybersecurity guidance used in planning, deployment, and maintenance periods.

Because cybersecurity threats have become a risk impacting all connected devices, it is important to ensure that cybersecurity is considered throughout the planning, deployment and maintenance phases associated with a solution's functional operation.

This guide provides hardening guidance for updates, blocking ports, user accounts, user roles and alerts. It is broken down into three main sections depicting the overall process for hardening:

1. Planning	2. Deployment	3. Maintain
Provides an introduction, general knowledge, and overall guidance for you to prepare your system for security and hardening	Guides you through the execution and hardening steps based on the products and security features of the target system components	Provides a checklist for future checkpoints to keep your system safe and secure

An appendix is included at the end for acronyms used within this document.

Legal disclaimer

The cybersecurity practices described in this guide are recommended practices to facilitate the secure installation and configuration of the products described herein. However, Johnson Controls cannot guarantee that the implementation of the cybersecurity practices or recommendations described in this guide will ensure the security of the relevant product or system, or prevent, or alter the potential impact of, any unauthorized access or damage caused by a cybersecurity incident. This guide is provided “as is”, and Johnson Controls makes no representation or warranty, express or implied, as to the efficacy of the cybersecurity practices or recommendations described in this guide. Johnson Controls disclaims all liability for any damages that may occur as a result of, or despite, reliance on this guide or compliance with any cybersecurity practices or recommendations set forth herein.

Contents

Introduction....2
Legal disclaimer....3
1. Planning....6
1.1 Cloudvue Overview....6
1.1.1 Deployment Architecture....6
1.1.2 Cloudvue Components....7
1.1.3 Supporting Components....7
1.2 Security feature set....7
1.2.1 User Authentication Safeguards....8
1.2.2 User Management....8
1.2.3 Audit Log Support....9
1.2.4 Communication Safeguards....9
1.2.5 Firmware Updates....9
1.3 Intended environment....9
1.3.1 Internet connectivity....9
1.3.2 Integration with IT networks....9
1.3.3 Integration with external systems....10
1.4 Patch Policy....10
1.5 Hardening Methodology....10
1.6 Communication....10
1.6.1 Communication port configuration....10
1.6.2 Communications Path Table....11
2. Deployment....13
2.1 Deployment overview....13
2.1.1 Physical installation considerations....13
2.1.2 Default security behavior....13
2.1.3 Recommended knowledge level....13
2.2 Hardening....13
2.2.1 Hardening Checklist....14
2.3 Cloudvue gateway firmware updates....14
2.4 Disable unused ports....15
2.5 User Accounts....15
2.5.1 Password policies....15

2.5.2 Two-factor authentication 15
2.5.3 User account setup 17
2.5.4 Temporary user accounts 18
2.6 Cloudvue Alerts 19
3 Maintain 20
3.1.0 Cybersecurity maintenance checklist 20
3.1.1 Lock accounts on termination of employment 22
3.1.2 Remove inactive user accounts 22
3.1.3 Update user account roles 22
3.1.4 Disable unused ports 23
3.1.5 Check for and prioritize software updates 23
3.1.6 Plan and execute software updates 23
3.1.7 Periodically validate the health of your hardware 24
3.1.8 Review organizational policy updates 24
3.1.9 Review updates to regulations 24
3.1.10 Update as-built documentation 24
3.1.11 Conduct security audits 25
3.1.12 Update standard operating procedures 25
3.1.13 Renew subscriptions 25
3.1.14 Check for end-of-life announcements and plan for replacements 25
3.1.15 Periodically delete sensitive data in accordance with policies or regulations. 26
3.1.16 Monitor for cyber attacks 26
3.2 Cloudvue testing process 26
Appendix A – Acronyms 28

1. Planning

This section helps plan for the implementation of security best practices for a Cloudvue system installation. Section1 Planning guides you through the product, its features, intended environment and networking requirements. This information is a pre-requisite for section 2 Deployment, where hardening steps will occur based on your customized solution.

1.1 Cloudvue Overview

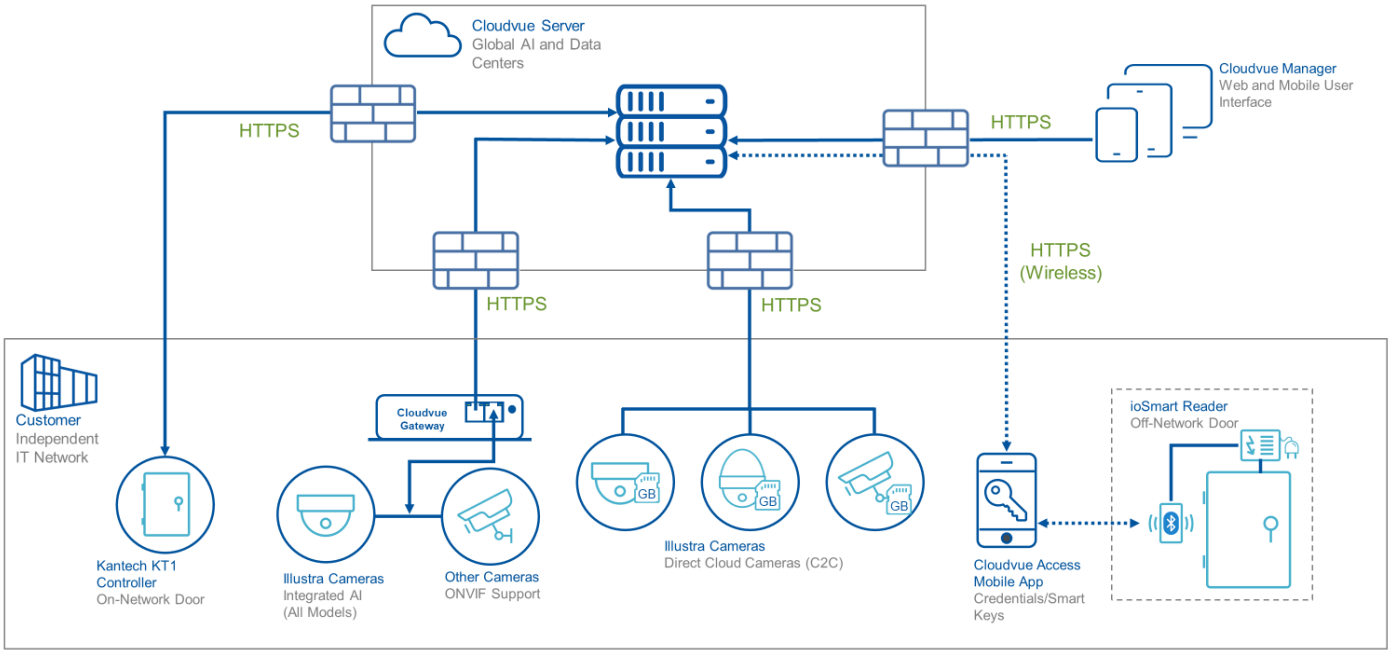
Cloudvue has been an expert in cloud video surveillance since 1999. Tyco Cloud Security Suite is used to simplify surveillance, streamline access control, provides powerful intelligence that improves security operations and helps with organizational efficiency. The Tyco Cloud Security System is browser-based. This means it must be accessed through a web browser.

For additional details and a full catalogue of our offerings visit the Cloudvue website through the following link - [Cloud Products | Johnson Controls](#) .

1.1.1 Deployment Architecture

Below are two sample architecture drawings of Cloudvue. Each installation will vary based upon the components selected for your specific installation. Figure 1.1.1.1 depicts on-premises, cloud and client communications for Windows and Linux, while figure 1.1.1.2 focuses on the camera edge server.

Figure 1.1.1.1 Cloudvue Architecture



1.1.2 Cloudvue Components

The sections below contain a subset of the many components included in a custom solution. These components are the primary focus of hardening in section 2 Deployment.

Cloudvue User Interface – Web based interface used to access video and device features.

Cloudvue Local. Used to monitor devices attached to a single gateway via local IP address.

Cloudvue Cloud (cloudvue.com). Used to monitor devices attached across multiple gateways. Cloudvue is used with cloud cameras (section 1.1.3)

Cloudvue Manager. Web user interface designed for integrators for tasks such as setting up User accounts, generating reports, and monitoring system performance.

Cloudvue gateway. Cloudvue hardware device where users can setup and configure cameras.

Direct Cloud Cameras. Cameras which do not need a gateway for a connection.

KT-1 Controller. Single door IP controller, which supports 2 readers (entry and exit).

1.1.3 Supporting Components

Networking and other components are also included as part of the deployment architecture. Some components such as a Router and/or Switch may be pre-existing, on site, and / or supplied by the customer.

NOTE: Details on hardening Supporting Components are out of scope, and not included within this guide. For specific hardening steps on supporting components, components out of scope, and those provided by third parties, see their specific hardening guide or installation documentation.

Access Control Reader. Scans access control keys and connects to the KT-1 controller.

Cameras (C2G). Cameras which connect directly to the gateway via an ethernet cable which also supplies Power over Ethernet (PoE).

Cloudvue App. Used to enroll devices, view live video, and search archived video.

Cloudvue Access Mobile App. Used as a mobile credential for access control.

PoE Switch - PoE Camera may be powered by a standard off the shelf PoE Switch rated for the speed and power requirements of the PoE.

1.2 Security feature set

This section describes Cloudvue’s many security features.

Table 1.2.1 – Security features

Section	Type	Feature name
1.2.1	User Authentication Safeguards	User auth 2 Factor / (MFA) authentication SAML integration
1.2.2	User Management	Role based access control (RBAC)
1.2.3	Audit Log support	Audit logs Gateway sync to NTP
1.2.4	Communication safeguards	Machine authentication TLS 1.3 HTTPS WebSockets Encryption
1.2.5	Firmware Updates	Over the Air (OTA) device updates

1.2.1 User Authentication Safeguards

Two-factor or multi-factor authentication (MFA) is a method to login after the user has presented two or more pieces of evidence. In addition to their username, a user will provide an additional identification verification such as a code received from a mobile device.

Cloudvue can use Security Assertion Markup Language (SAML) to authenticate a user with their organizations identity provider. See section 1.3.3 for additional details.

1.2.2 User Management

Initial Use account creation: Cloudvue requires a minimum of 1 user account to function. During the account creation process, the user account is established, and a role must be applied. Johnson Controls recommends using the principle of least privilege as shown below for every account which is created.

Least Privilege. The principal of least privilege means the following:

- Only the minimum necessary rights should be assigned to a user that requests access to Cloudvue
- Access rights should be in effect for the shortest duration necessary to do their job

Granting permissions to a user beyond the scope of the necessary rights of an action can allow that user to obtain or change information in unwanted ways. The best practice when assigning access rights is to only give an individual user the necessary role and permissions to their job and nothing more.

Note: If an employee changes roles, you may need to update their role or remove their account.

Cloudvue offers Role Based Access Control (RBAC) authorizations. Roles are defined as privileges with different levels of permissions. Below is a list of the available roles for a user account:

- Enterprise – Default role; Can see live video, recorded video and make settings changes (except subscriptions). Can see the subscriptions (Tyco Cloud VMS and Cloud Drive), but cannot make changes.
- Administrator – Can view and access everything; manages everything.
- View Only – Can see live and recorded video in custom camera views; cannot make changes.
- Live Only – Can only see live video. Cannot see recorded video.
- Account Administrator – View and manage devices for a given account.

1.2.3 Audit Log Support

Audit logs are available for certain operations in the Cloud, but not for the devices. Log files are protected by administrative roles and are kept for 180 days.

1.2.4 Communication Safeguards

Machine authentication. Cloudvue uses Certificate based authentication to verify device connections to the cloud. Device certificates are managed and rotated automatically through the Cloudvue system.

TLS 1.3. Cloudvue uses by default TLS 1.3 encryption.

HTTPS. All connections to the cloud are secured through HTTPS.

Encrypted WebSockets. WebSockets keep all the communications between the device and the cloud secure, including video streams.

Encryption algorithm. Cloudvue uses AES-192 encryption for all video stored in the cloud.

1.2.5 Firmware Updates

Over the Air (OTA) firmware updates can be pushed out to customers or downloaded periodically to NVRs and cloud cameras. Specific devices can also be patched individually by the administrator of the device as necessary. For additional details see section 2.3.

1.3 Intended environment

The Cloudvue gateway and Direct cloud cameras are installed on-premises. Physical access and installation of devices can greatly impact cybersecurity. The gateway is to be installed within a locked closet or in a secured, temperature-controlled location, such as within a data center or IT Server room with restricted access.

Cameras are installed in a range of environments, including internally and externally to a building. It is important that a qualified installer provides and defines physical mounting and network infrastructure.

1.3.1 Internet connectivity

Connecting any Operational Technology (OT) system to the internet always increases cybersecurity risk. This product does not require Internet access; however internet access is recommended for the cloud features, which will require additional hardening.

1.3.2 Integration with IT networks

When using a PoE switch with the Cloudvue gateway, Johnson Controls strongly recommends that cameras are installed on an isolated network. This means connecting them to port #2.
Note: When devices are connected to port #2, they are assigned an IP address by default from the DHCP Server. These devices are also shielded from the internet which is on port #1.

1.3.3 Integration with external systems

Optionally, Cloudvue may be integrated with your SAML identity provider to authenticate. Contact Johnson Controls Support (see your support contract) for assistance in setting up SAML.

1.4 Patch Policy

The policy documented here sets forth the current internal operating guidelines and process regarding Cloudvue, which may change from time to time at the sole discretion of Johnson Controls. Johnson Controls employs commercially reasonable efforts to pursue the operating guidelines and process described herein. However, other mitigating factors may prevent complete adherence to this policy, as determined by Johnson Controls at its discretion. Regardless, Johnson Controls endeavors to address issues that arise within Cloudvue with the severity that they warrant.

Security Updates are provided for the latest release of Cloudvue as follows:

- When **CRITICAL** severity security vulnerabilities are discovered within Cloudvue, Johnson Controls will use commercially reasonable efforts to issue a critical update for the current release of Cloudvue.

When non-CRITICAL vulnerabilities are discovered within Cloudvue, Johnson Controls will use commercially reasonable efforts to:

- Apply fixes for **HIGH** severity vulnerabilities in the next immediate Release of Cloudvue
- Johnson Controls will assess **MEDIUM** severity vulnerabilities and plan accordingly

Release schedule

- An update to Cloudvue including new features and security fixes is released approximately every 6 months.
- No Cloudvue update will be released without undergoing extensive quality assurance testing.

1.5 Hardening Methodology

While Cloudvue provides many onboard security safeguards, including secure-by-default settings, we recommend that the system is hardened according to the guidance outlined in section 2, Deployment.

Generally, a defense-in-depth strategy employing standard IT hardening methods and compensating controls is needed to compliment the base security features of each component.

1.6 Communication

1.6.1 Communication port configuration

In an Cloudvue system, when using a feature that requires a communication protocol, ensure that the corresponding port is open. Hardening your system involves blocking any port that is not used.

Port	Process / Service	Protocol	Direction	Destination System	Description
443	au-preview-inbound.cloudvue.com	TCP	Bi-directional	JCI-MC	Live video streams - Australia
443	preview-inbound.cloudvue.com	TCP	Bi-directional	JCI-MC	Live video streams – North America
443	uk-preview-inbound.cloudvue.com	TCP	Bi-directional	JCI-MC	Live video streams – EMEA
443	au-messaging.cloudvue.com	TCP	Bi-directional	JCI-MC	Main communication channel between JCI cloud and the device - Australia
443	messaging.cloudvue.com	TCP	Bi-directional	JCI-MC	Main communication channel between JCI cloud and the device – North America
443	uk-messaging.cloudvue.com	TCP	Bi-directional	JCI-MC	Main communication channel between JCI cloud and the device – EMEA
443	s12archiveauprod001.blob.core.windows.net	TCP	Outbound	Cloudvue server	Video upload - Australia
443	s12archiveukprod001.blob.core.windows.net	TCP	Outbound	Cloudvue server	Video upload – EMEA
443	s12archiveauprod002.blob.core.windows.net	TCP	Outbound	Cloudvue server	Video upload - Australia
443	s12archives02.blob.core.windows.net	TCP	Outbound	Cloudvue server	Video upload – North America
443	s12archiveukprod002.blob.core.windows.net	TCP	Outbound	Cloudvue server	Video upload – EMEA
443	s12archives03.blob.core.windows.net	TCP	Outbound	Cloudvue server	Video upload – North America
443	s12archive004.blob.core.windows.net	TCP	Outbound	Cloudvue server	Video upload – North America
443	s12updatesprod.blob.core.windows.net	TCP	Bi-directional	Cloudvue server	Firmware updates
7627	tunnel.cloudvue.com	TCP	Bi-directional	JCI-MC	(Optional) SSH support tunnel
8000	analytics.cloudvue.com	TCP	Bi-directional	JCI-MC	(Optional) People and vehicle detection analytics

* JCI-MC = Johnson Controls managed cloud

1.6.2 Communications Paths

Preview socket (Default view)

Cloudvue app / Browser <-> [Required] – (https, port 443) <-> API message to NVR (Websockets)

Messaging socket

Cloudvue device <-> [Required] – (https, port 443) <-> Websocket server VM

Upload storage accounts

Cloudvue device -> [Required] – (https, port 443) -> SaaS Storage account

Firmware updates

SaaS Storage account <-> [Required] – (https, port 443) <-> Cloudvue device

SSH support tunnel

Cloudvue device <-> [Optional] – (RSA, port 7627) <-> Intermediate tunnel server <-> Cloudvue staff

Analytics

Cloudvue device <-> [Optional] – (http, port 8000) <-> Analytics server

2. Deployment

The contents within this section address how to initiate secure deployment for new installations, how to harden the solution and additional steps after commissioning required before turning over the solution to runtime operations.

2.1 Deployment overview

Security hardening of Cloudvue begins prior to deployment with careful planning as outlined in section 1 of this guide. It is a good practice to review that section prior to deployment to fully understand the security feature set of Cloudvue, its architecture, data flow and requirements before physically installing and making application specific configuration changes.

In this section more details are provided to help the installer prepare for deployment:

- Physical installation considerations
- Default security behavior
- Recommended knowledge level

2.1.1 Physical installation considerations

The physical access and installation of the devices can impact the cybersecurity.

Cameras are designed to be placed in open areas where they can capture the best video footage. When possible, install cameras in a location that is difficult to reach without a ladder or has added physical protection which does not obstruct the camera's line of sight.

To prevent unauthorized access to the Cloudvue gateway, be sure to place the device in a secured rack or room that can restrict access (for example, mechanical lock or physical access control).

2.1.2 Default security behavior

On initial start-up, a registration form is displayed for you to create the default user account, user password, and assign the device to a partner. Note: After the device is connected, it may also be registered through a web browser via https://dashboard.cloudvue.com/login.

2.1.3 Recommended knowledge level

The person confirming that the proper hardening steps are executed should be experienced in Cloudvue administration and networking technologies. For additional support see the following link - https://support.cloudvue.com/#/product/cloudvue/support .

2.2 Hardening

While Cloudvue has several secure-by-default safeguards, we recommend additional hardening to meet the security requirements of the target environment.

It is important to apply to the correct level of protection as warranted by policies and regulations that may govern the application security settings for a deployment instance of Cloudvue.

2.2.1 Hardening Checklist

- ☐ Hardening step 1: Update software (manual only if required)
- ☐ Hardening step 2: Disable unused Ports
- ☐ Hardening step 3: Configure Two-factor authentication
- ☐ Hardening step 4: Setup user
- ☐ Hardening step 5: Setup or modify user roles
- ☐ Hardening step 6: Remove unused user accounts
- ☐ Hardening step 7: Setup or modify alerts

2.3 Cloudvue gateway firmware updates

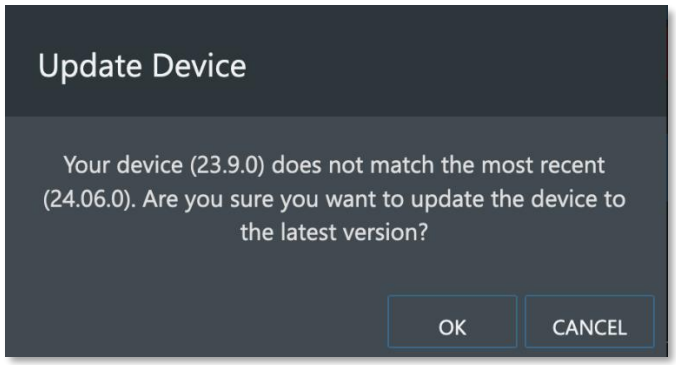
The Cloudvue gateway receives software upgrades automatically from the cloud when a new version of software is available via the messaging socket. The gateway checks for a firmware upgrade during startup, when connection to the cloud is re-established, and periodically during an established connection.

Hardening Step 1 – Update software (manual only if required)

With the cloud service, local updates of the Cloudvue gateway are not required. However, it is possible to manually update the gateway.

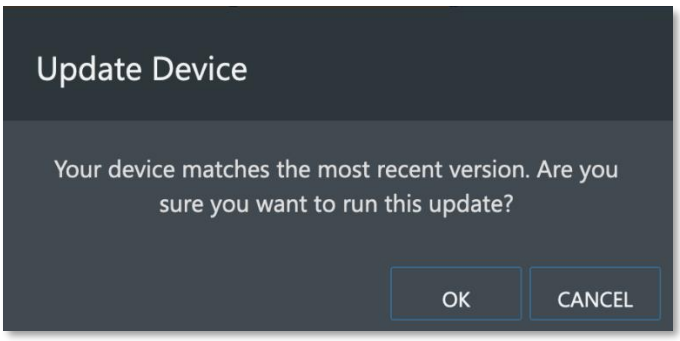
1) Log on to the dashboard at Cloudvue.com
2) Navigate to the Cloudvue gateway device
3) Click the **Update Device** button

4) Click the **OK** Button to have the Cloudvue gateway device use the latest version



The gateway goes offline temporarily while the updates are applied.

Note: If the gateway is already running the latest version, the message below appears. Click **CANCEL**.



2.4 Disable unused ports

Unused ports should be blocked unless they are specifically needed for Cloudvue or another approved use / application to function. In section 1.6.1 we reviewed the ports and protocols that need to be open based on the requirements of the application.

Hardening Step 2: Disable unused ports

Ensure that the ports corresponding to Cloudvue gateway from section 1.6.1 are open. To harden your system, block all ports that are not in use.

2.5 User Accounts

2.5.1 Password policies

The password policy in Cloudvue is turned on by default but does not include any configurable attributes. However, SAML integration could be utilized to use Active Directory (AD) or OKTA to support your organization's more stringent password requirements if necessary. For additional information on enabling SAML, contact your Cloudvue support team - https://www.cloudvue.io/support.

2.5.2 Two-factor authentication

Two-factor is a method to login after the user has presented two pieces of evidence. In addition to their username, a user will provide an additional identification verification such as a code received from a mobile device.

Hardening Step 3: Configure Two-factor authentication

For each user added, Johnson Controls recommends setting up Two-factor authentication. In the Add user / Edit account box in either Cloudvue Manager (figure 2.5.2.1) or Cloudvue.com (figure 2.5.2.2), fill in all the relevant user fields, then check the box for **Two Factor Authentication**. If a user account is already created, edit the account, check the box for **Two Factor Authentication,** and click **Submit**.

Note: Ensure one or more delivery option (Email, SMS, App) is selected.

Figure 2.5.2.1 Cloudvue Manager

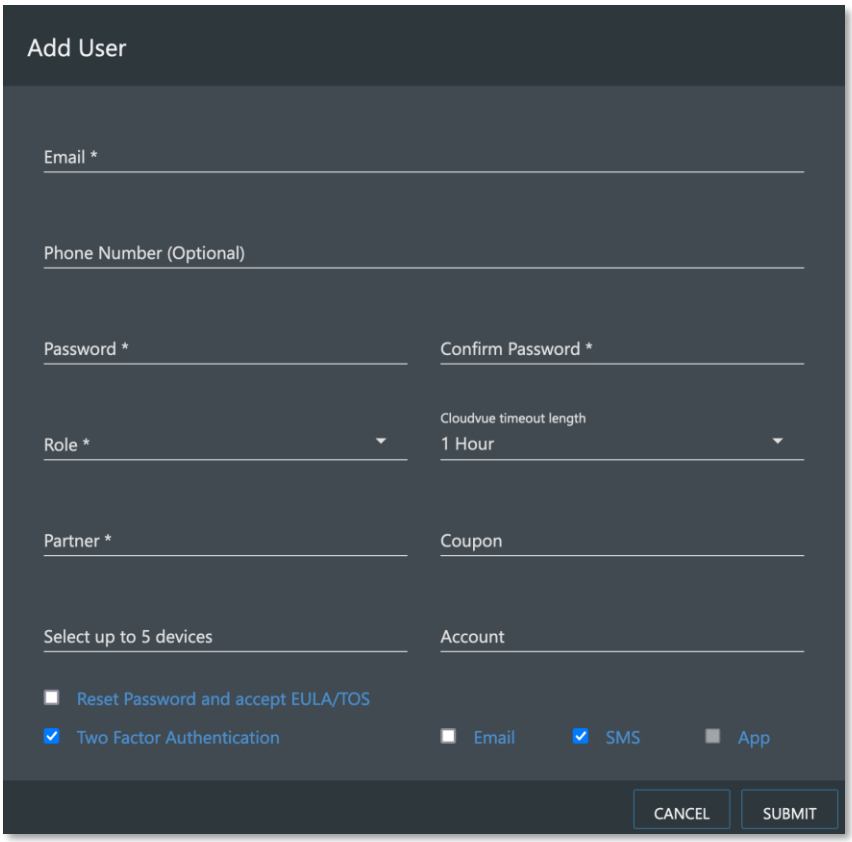
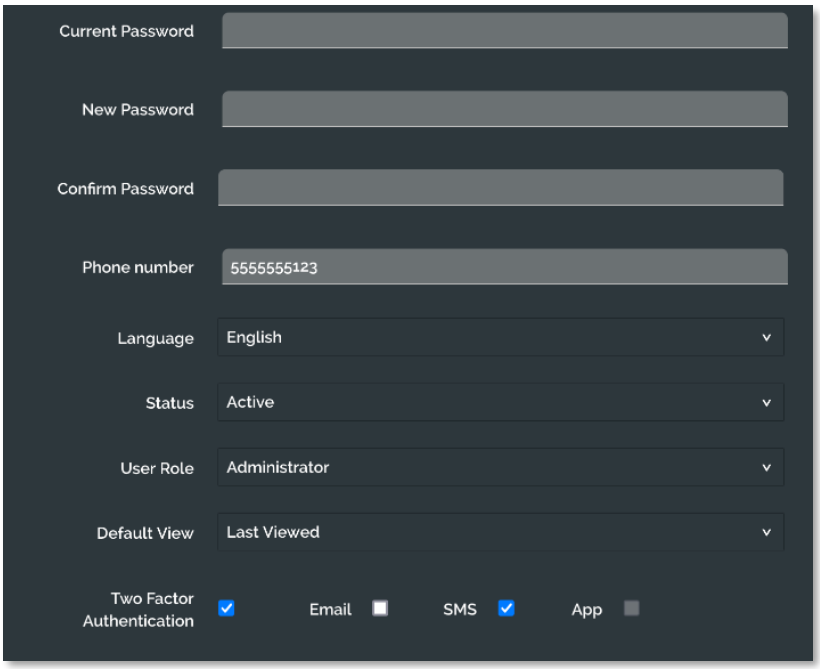


Figure 2.5.2.2 Cloudvue.com



2.5.3 User account setup

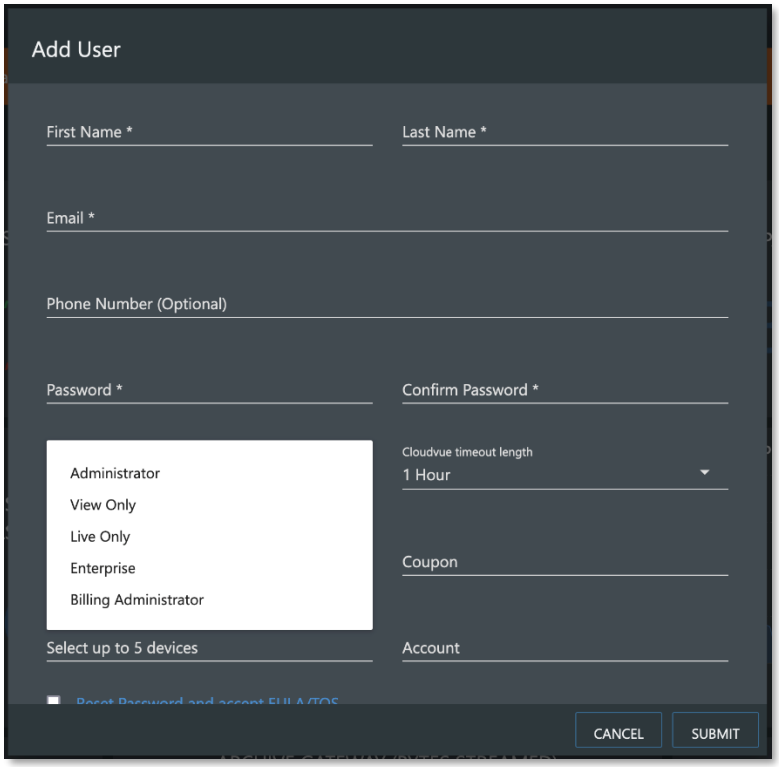
Cloudvue provides the following Roles:

- Enterprise – Default setting. Can be assigned to devices, view live and archived video
- Administrator – Highest level of access, configure devices, add users and all roles below
- View Only – Can view collections or archives
- Live Only – Can only watch live video on assigned devices
- Account Administrator – Can update subscriptions

Hardening Step 4: Setup initial user

In the Add user box in either Cloudvue Manager (figure 2.5.2.1) or Cloudvue.com (figure 2.5.2.2), fill in all the required fields (indicated by an asterisk), including the **User Role** , which is discussed in further detail in the next hardening step.

Figure 2.5.3.1 Add User

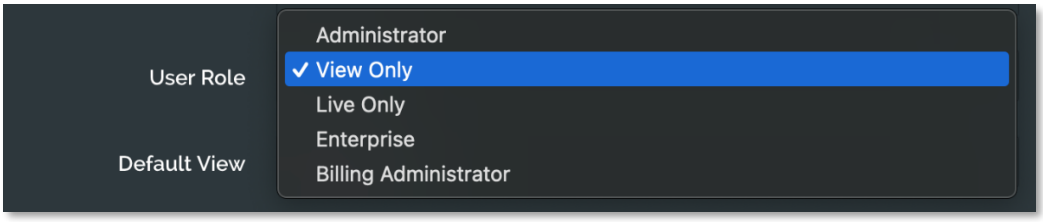


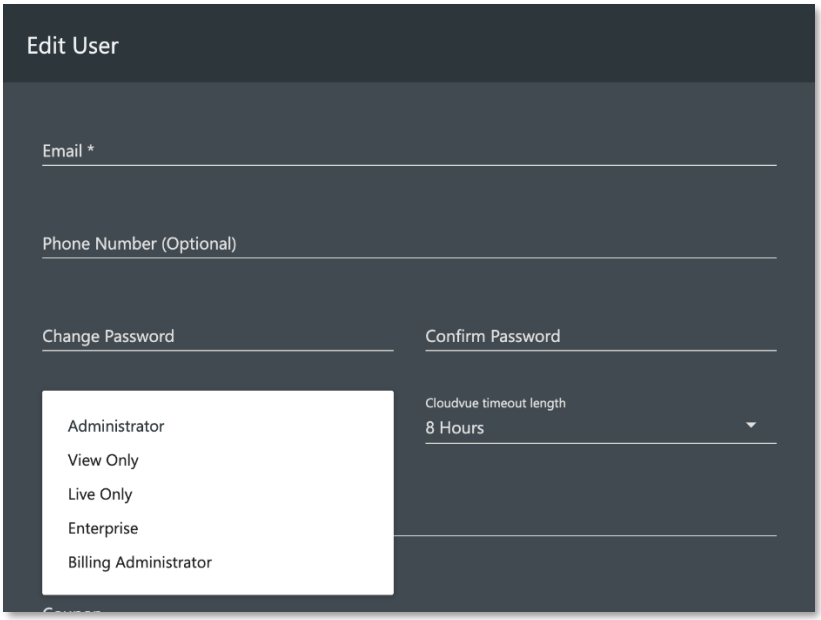
Periodically review the user roles and adjust as users require less or more privileges.

Hardening Step 5: Setup or modify user roles

In the Add user / Edit account box in either Cloudvue Manager (figure 2.5.2.1) or Cloudvue.com (figure 2.5.2.2), select the **User Role** drop-down box and assign the appropriate role.

Figure 2.5.3.2 Edit User



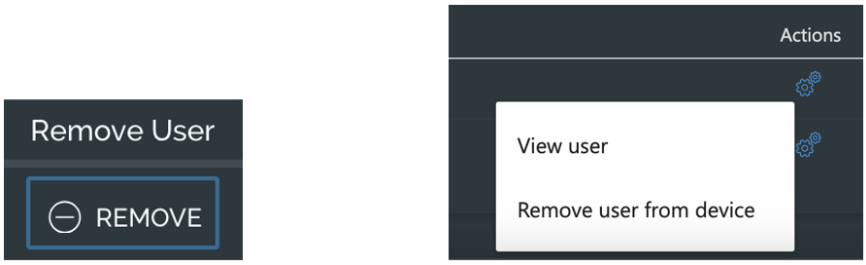


2.5.4 Temporary user accounts

During the commissioning phase, temporary accounts may be setup for installers, technicians or contractors that are only needed for a short duration, until the system is turned over to runtime operations. If these accounts are no longer needed, they must be removed from the device. If they are needed again in the future, they can be re-added to the device.

Hardening Step 6: Remove unused user accounts

In the **Device Settings** page in either Cloudvue Manager (figure 2.5.2.1) or Cloudvue.com (figure 2.5.2.2), select Remove User / Remove user from device, as shown below.



Cloudvue.com - Or - Cloudvue Manager

2.6 Cloudvue Alerts

Users can setup multiple types of alerts depending on what they require monitoring for their organization. For timely response, notification can be setup for email or SMS.

Hardening Step 7: Setup or modify alerts

Navigate to the **Alerts** tab.

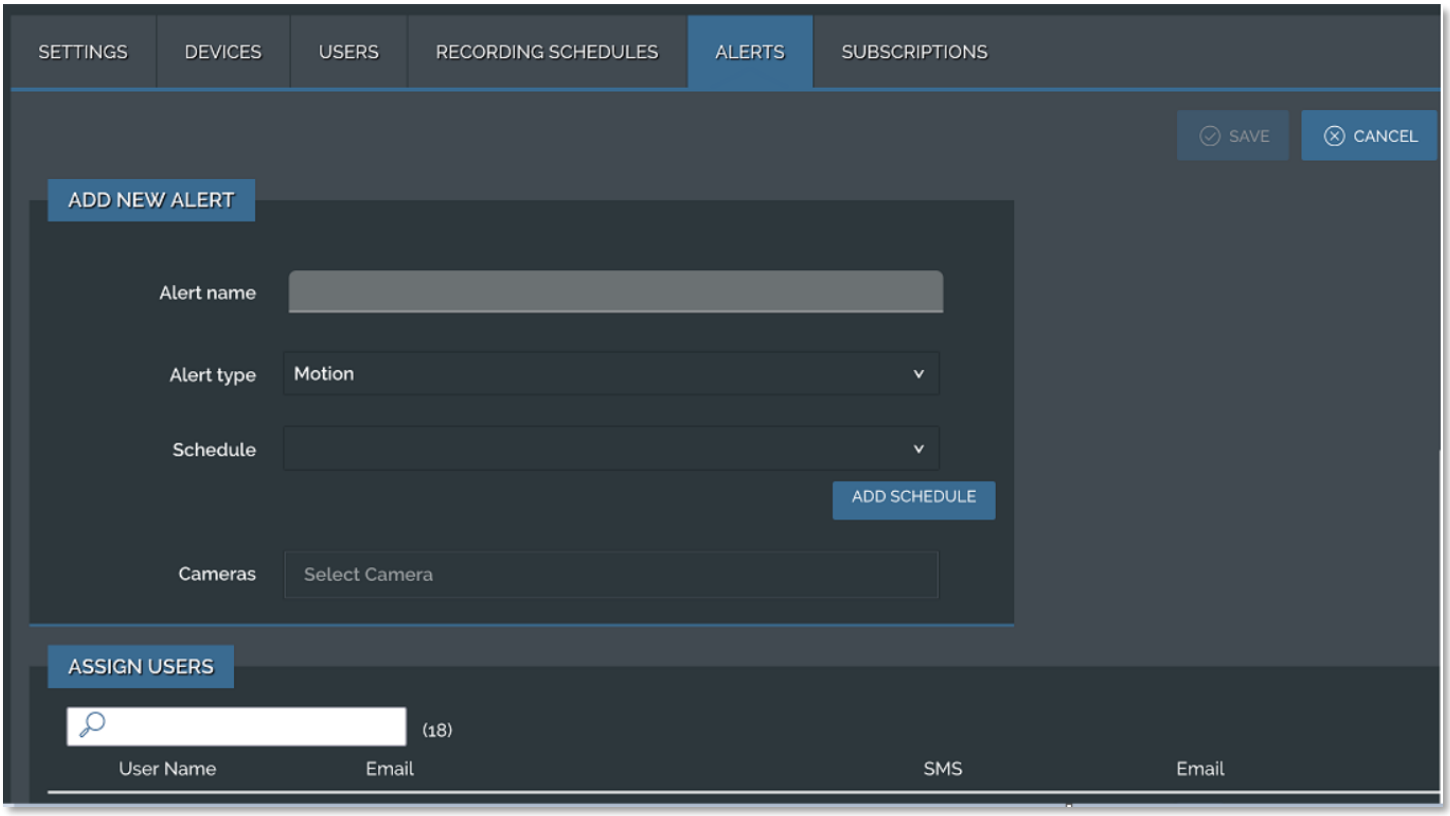
To add a new alert:

- If an existing schedule has not been created, click the **Add Schedule** button
  - Fill in schedule details and click **SAVE**
  - Navigate back to the **Add New Alert** page
- Fill in the required details in the **Add New Alert** box
- Click the **SAVE** button

To modify an existing alert:

- Select an existing alert
- Modify the changed details in the **Edit Alert** box
- Click the **SAVE** button

Figure 2.6.1



3 Maintain

The contents within this section address how to monitor for potential cybersecurity issues and maintain protection levels because conditions change.

An audit that produces a report indicating low cybersecurity risk is a very positive result and suggests that the deployment was conducted with a high degree of care and consideration. However, new attack vectors combined with enhanced hacking tools and more advanced testing techniques may, in the future, disclose vulnerabilities with the technologies used.

The impacted technologies and their implementation may have been previously well regarded by cybersecurity experts. The discovery of vulnerabilities post the final deployment audit may not reflect the quality of that audit. You may require a higher degree of protection for the environment that Cloudvue is serving because policies, regulations and guidance may change over time.

3.1.0 Cybersecurity maintenance checklist

Continuously or periodically practice the following cybersecurity maintenance items. The frequency of their execution will depend on the policies and regulations which govern the site. The typical maintenance periods provided are a starting point and adjusted to best suit the target conditions of the deployed environment.

Item	Description	Immediate	Base on Priority	Daily	Weekly	Monthly	Quarterly	Annual
1	*Lock user accounts of terminated employees*	✓						
2	*Remove inactive user accounts*					✓		
3	*Update user account roles*						✓	
4	*Disable unused ports*						✓	
5	*Check for and prioritize software updates*					✓		
6	*Plan and execute software updates*		✓					
7	*Periodically validate the health of your hardware*					✓		
8	*Review organizational policy updates*							✓
9	*Review updates to regulations*							✓
10	*Update as built documentation*	✓						✓
11	*Conduct security audits*							✓
12	*Update standard operating procedures*							✓
13	*Renew subscriptions*							✓
14	*Check for end-of-life announcements and plan for replacements*						✓	
15	*Periodically delete sensitive data in accordance with policies or regulations*		✓					
16	*Monitor for cyber attacks*			✓				

3.1.1 Lock accounts on termination of employment

Disable user accounts of personnel who voluntarily or non-voluntarily are terminated from employment immediately.

Table 3.1.1.1

Action	Details	Suggested frequency
Disable accounts	Disable accounts or terminated employees in Cloudvue Manager	Immediate

3.1.2 Remove inactive user accounts

While an employee may still be employed by an organization in which the system is owned, managed, serviced, or used by, they may not have utilized it for a long period. This suggests that independent of being authorized to use the system, they do not have a need to use the system, and their user account should be removed. This is sometimes referred to as a “use it or lose it” policy. This best practice reduces the amount of active user accounts in the system and therefore lowers the potential attack footprint.

One final note: Cloudvue is less of a traditional Information Technology (IT) system and more of an Operational Technology (OT) system. This means that it may be acceptable for employees, contractors, and/or service technicians to not sign into this system as often as they would traditional business systems such as email. OT Systems are designed to be used on an as-needed basis, meaning access may be sporadic. Use discretion when defining “inactive accounts”.

Table 3.1.2.1

Action	Details	Suggested frequency
Remove inactive accounts	Remove inactive accounts in Cloudvue Manager	Monthly

3.1.3 Update user account roles

While an employee may still be employed by an organization in which the system is owned, managed, serviced, or used by, they may have changed roles or have increased or decreased their need to utilize the system. When adding a role or a permission to a user's account when that user has been granted new authorizations due to an organizational role change, be sure to remove the Cloudvue roles and permissions no longer required or utilized in their new role.

Table 3.1.3.1

Action	Details	Suggested frequency
Update user account roles	Update accounts in Cloudvue Manager	Quarterly

3.1.4 Disable unused ports

Reassess the need for ports that are not required and disable them. For example, if software was reinstalled or new features were added, ensure that any ports originally disabled remain disabled. This practice will lower the attack surface of Cloudvue resulting in a higher level of protection.

Table 3.1.4.1

Action	Details	Suggested frequency
Disabled unused features	See section 1.6.1 for Communication ports	Quarterly

3.1.5 Check for and prioritize software updates

While an Cloudvue update may or may not relate to a security advisory, it is always best practice to apply the most current update. These updates can include cybersecurity enhancements and fixes to known issues.

Note: Critical updates to Cloudvue will be pushed automatically, while non-critical updates will be made available for review in **Cloudvue Manager**.

Review the release notes and prioritize the benefits of the update. The overall benefit should include the improved protection that will aid in lowering the cybersecurity risk. Be sure also to check for updates and patches of third-party components such as cameras, networking equipment and operating systems by consulting with the respective vendor.

See section 2.3 for additional details.

Table 3.1.5.1

Action	Details	Suggested frequency
Check for and prioritize software updates	Check for new releases and updates devices in Cloudvue Manager	Monthly

3.1.6 Plan and execute software updates

Follow the plan determined in maintenance step 5. Consult with all parties who may be impacted by updates or downtime and choose the best time for deployment.
Note: Downtime for Cloudvue updates is usually less than 5 minutes

Table 3.1.6.1

Action	Details	Suggested frequency
Plan and execute software updates	Plan and execute the software update for 3.1.5	Base on priority

3.1.7 Periodically validate the health of your hardware

Cloudvue Manager provides a **Health Check** button which validates the real-time health through a test of each device and reports back their status. Look for any devices that require your attention. Cloud Camera devices can include an SD card. Be sure to routinely check the SD card's capacity and status.

Table 3.1.7.1

Action	Details	Suggested frequency
Periodically validate the health of your hardware	Validate the health of your hardware each month to ensure your solutions continue to work	Monthly

3.1.8 Review organizational policy updates

Organizations may update their policies which include cybersecurity requirements. Changes to these policies can impact systems which complied prior to the change. Periodically check to see if policy changes were made and re-assess compliance with those policies.

Table 3.1.8.1

Action	Details	Suggested frequency
Review organizational policy updates	Collect most recent security policies for your organization	Annual

3.1.9 Review updates to regulations

If Cloudvue is deployed in a location that is governed by regulation, it is important to check to see if there are any updates to those regulations. In some cases, new regulations are introduced. Whether it is a review of an updated regulation to maintain compliance or a new regulation, an assessment of the changes should be conducted periodically.

Table 3.1.9.1

Action	Details	Suggested frequency
Review updates to regulations	Collect most recent copies of regulations as applicable. Perform a gap analysis against the deployed configuration.	Annual

3.1.10 Update as-built documentation

Update as-built documentation if the deployment architecture or component configuration changes. Some configuration changes happen without a formal project or plan and in such cases, it may be common to negate updating the as-built documentation. Schedule a full update of the as-built documentation on a regular basis to ensure that all changes are documented.

Table 3.1.10.1

Action	Details	Suggested frequency

Update as-built documentation	Update as-built documentation of your system as needed	As changes are made or annual

3.1.11 Conduct security audits

Periodic security audits are necessary as cybersecurity guidance, organizational policies, regulations, auditing processes, system use, configuration, and threats have likely changed since the last audit. By conducting periodic security audits, the latest knowledge and conditions can be applied revealing gaps in protection previously undetected or created by changes in system use or configuration. Consult with your IT department for guidance toward security audits.

Table 3.1.11.1

Action	Details	Suggested frequency
Conduct security audits	Conduct yearly security audits	Annual

3.1.12 Update standard operating procedures

Including best practices for cybersecurity within standard operating procedures can complement the protection that the system can deliver on its own. Depending on the procedures an operator uses, a gap in protection can be created, prevented, or closed. Therefore, it is important to update standard operating procedures periodically.

Table 3.1.12.1

Action	Details	Suggested frequency
Update standard operating procedures	Collect standard operating procedures for use of Cloudvue within the organization	Annual

3.1.13 Renew subscriptions

Be sure to review and renew subscriptions (i.e. camera base [VMS only] subscription, or cloud storage) or update payment methods (i.e. credit card info, monthly or annual statements) if needed.

Table 3.1.13.1

Action	Details	Suggested frequency
Renew subscriptions	Collect active subscription details. Be sure to review payment information.	Annual

3.1.14 Check for end-of-life announcements and plan for replacements

Review product announcements to determine if any of the components of the Cloudvue system have a planned end-of-life announcement, including cameras.

Table 3.1.14.1

Action	Details	Suggested frequency
Check for end-of-life announcements and plan for replacements	Collect end-of-life details	Quarterly

3.1.15 Periodically delete sensitive data in accordance with policies or regulations.

Collect details on policies and regulations that apply to your location and delete sensitive data according to these findings.

Table 3.1.15.1

Action	Details	Suggested frequency
Periodically delete sensitive data in accordance with policies or regulations	Collect details on policies and regulations, then delete sensitive data as it applies to your Cloudvue location	As required

3.1.16 Monitor for cyber attacks

Monitoring site perimeters, networks and endpoints for cyber-attacks is a part of good cybersecurity operation.

Table 3.1.16.1

Action	Details	Suggested frequency
Monitor for cyber attacks	Determine which security monitoring tools and services to implement	Run continuously once implemented

3.2 Cloudvue testing process

As part of the requirements of the Product Security Program, Cloudvue receives regular vulnerability and penetration testing from both our internal product security engineers. Cloudvue is also subjected to both internal engineering team and third-party penetration testing annually and for major releases.

Vulnerability assessment

Vulnerabilities discovered in Cloudvue proprietary software are assessed on the CVSS score.

CVSS Score, Assessment

≥ 9, Critical

≥ 7, High

< 7, Medium

Vulnerability assessment – third party components

Vulnerabilities discovered in Cloudvue proprietary software are assessed on the CVSS score.

CVSS Score	Assessment
≥ 9	Critical
≥ 7	High
< 7	Medium

Vulnerability assessment – third party software

Cloudvue must use commercially reasonable efforts to monitor third party and open-source software included within the Cloudvue ecosystem for disclosed vulnerabilities from the product vendors and open-source communities. Vulnerabilities that are discovered and disclosed will be assessed first on its assigned CVSS score from the product vendor or the National Vulnerability Database and then on the ability to be exploited within Cloudvue.

CVSS Score	Exploitability	Assessment
≥ 9	Exploitable	Critical
≥ 9	Not Exploitable	High
≥ 7	Exploitable	High
≥ 7	Not Exploitable	Medium
< 7	Exploitable	Medium
< 7	Not Exploitable	Low

If an update is not available to correct the vulnerability, Johnson Controls will use commercially reasonable efforts to mitigate the vulnerability within its capabilities.

Cloudvue vulnerability reporting

To better protect our customers and honor the trust they put in us, we are firm believers in responsible coordinated disclosure. Security Researchers, consultants and others who believe they may have found a potential security vulnerability in a Security Product can make immediate notice to our Cyber Protection Team through email to **TrustCenter@jci.com** or by the **Building Products Vulnerability Reporting** webpage at https://www.johnsoncontrols.com/trust-center/cybersecurity/security-advisories to make immediate notice to our Product Security Incident Response Team (PSIRT).

Those working directly on behalf of a Security Products customer should also notify their local Security Products representative. Thank you for your partnership with us in creating a smarter, safer more sustainable world.

Appendix A – Acronyms

Acronym	Description
AD	Active Directory
C2G	Camera to gateway
CVSS	Common Vulnerability Scoring system
HTTP / HTTPS	Hypertext Transfer Protocol / Secure
IT	Information Technology
LDAP	Lightweight Directory Access Protocol
MFA	Multi-factor authentication
NVR	Network Video Recorder
OS	Operating System
OT	Operational Technology
OTA	Over the air
PoE	Power over Ethernet
PSIRT	Product Security Incident Response Team
RBAC	Role based access control
SaaS	Software as a Service
SAML	Security Assertion Markup Language
SMTP	Simple Messaging Transfer Protocol
SSL	Secure Socket Layer
TLS	Transport Layer Security
VMS	Video Management System