Hik-ProConnect & Hik-Connect Cloud Services

Security Whitepaper

Contents

1 Introduction

Hangzhou Hikvision Digital Technology Co., Ltd. and its affiliates (together as “HIKVISION”) provide Hik-ProConnect & Hik-Connect Cloud Services, covering a range of overseas regions, including the Americas, Europe, the Middle East, Africa, and Asia. Note that the available services might vary by country or region.

This White Paper introduces how Hik-ProConnect & Hik-Connect Cloud Services ensure the security and reliability of its infrastructure, data, service design, internal processes, deployment, operation, and maintenance.

1.1 User Terminology Description

User: those who use Hik-ProConnect/Hik-Connect, including B Users and C Users.

B User: those who use Hik-ProConnect App/Portal (generally the Installers).

C User (owner of IoT devices): those who use Hik-Connect App/Portal (generally the end users).

Developer: those who perform secondary development of Hik-ProConnect & Hik-Connect.

1.2 Cloud Services

Hik-ProConnect & Hik-Connect Cloud Services include the following types:

Cloud Service	Description
Device Management Service	● Device Configuration: Users can configure devices remotely, including network configuration, image configuration, event configuration, etc. ● Device Health Monitoring: Users can check device health status, including online/offline status, channel status, HDD status, etc. ● Cross-Device Linkage: Users can configure linkage rules among various devices. Thus, via the Cloud Services, event detected by one device will trigger linkage actions of another device.
Stream Media Service	● Live View: C Users can view live video via website or terminals, and B Users can view live video after getting authorization from C Users. ● Playback: C Users can play back videos stored in the device locally, and B Users can play back these videos after getting authorization from C Users; C Users can play back videos stored in the Cloud after activating the Cloud Storage Service.
Alarm Service	For devices that support motion detection, when this function is enabled on Hik-ProConnect & Hik-Connect Cloud Services, C Users can receive real-time alarm notifications if any motion is detected, and can check alarm notification records generated in the last 7 days.
Cloud Storage Service	When B Users activate the Cloud Storage Service and hand over it to C Users, event-related videos recorded by Hikvision devices will be

Cloud Service	Description
	automatically stored in C Users' Cloud. B Users can subscribe to a storage plan to meet C Users' needs. There are two options available: • 7-Day Package: users can access cloud storage videos uploaded in the last 7 days. • 30-Day Package: users can access cloud storage videos uploaded in the last 30 days. For devices that support the Cloud Storage Service, C Users can view cloud storage videos when B Users subscribe to and activate the Cloud Storage Service and hand over it to them.

2 Network Security of IoT Devices

IoT (Internet of Things) devices are physical objects that are embedded with computers and can connect to the Internet. IoT devices include but not limited to: cameras, NVR/DVR, access control devices, intercom devices, alarm devices, thermal imaging devices, and switches.
Communication between IoT devices and Hik-ProConnect & Hik-Connect Cloud Services is run over TLS cryptographic protocol. To ensure that access is limited to authorized users, password authentication is required to access the service.
Users and the Cloud Services use the client software, and the IoT devices use P2P (Peer-to-Peer) cross-communications technology. Thus, IoT devices do not need to open or map ports or use fixed IP addresses, which greatly limits the visibility of Internet-based attackers.

3 Infrastructure Security

3.1 Overview

Cloud Service Providers (CSPs) such as Amazon Web Services (AWS) provide Hik-ProConnect & Hik-Connect Cloud Services with Infrastructure as a Service (IAAS) and Platform as a Service (PAAS) solutions. Hikvision's CSPs provide a reliable and secure foundation for Hik-ProConnect & Hik-Connect Cloud Services and help build a security framework of cloud infrastructure.

3.2 Physical and Environmental Security

The physical and environmental security of Hik-ProConnect & Hik-Connect Cloud Services is managed by Hikvision's CSPs. They provide security solutions covering fire and smoke detection, fire extinguishing, power control, climate control, and temperature control. Hikvision reviews CSP security reports regularly to ensure the reliability of their commitments.

3.3 Host Infrastructure and Network Control

Hikvision's CSPs protect the infrastructure that runs all the services offered in the Cloud. The infrastructure is composed of hardware, software, network and facilities that run the Cloud Services. Hikvision regularly reviews CSP third party assessment reports or allows the Cloud Service Operation & Maintenance Team to conduct security assessments, to ensure that CSPs' security solutions are working properly.
Hikvision performs the necessary security configurations, including operating system configuration, network configuration, and firewall configuration.

3.3.1 Operating System Configuration

Hikvision manages the Guest Operating System, including its upgrades and security patches. The Linux-based AMIs provided by CSPs are regularly updated with the latest patches. Hikvision customizes new Amazon Machine Images (AMI) based on them, deploys some configurations, tests AMI security, checks AMI integrity, and finally relaunches new instances with the updated AMI.

3.3.2 Network and Firewall Configuration

The production environment, test environment and development environment are isolated from one another through network segmentation.
The production environment is further divided into different security zones by using the Virtual Private Cloud (VPC) subnets and the firewall provided by CSPs (called a security group) in each instance.
VPC enables Hikvision to create an isolated portion of the Cloud and launch computing instances. Hikvision defines two subnets in its own VPC, groups similar types of instances according to their IP address range, and then builds a routing and security mechanism to control the traffic flow in and out of the instances and subnets. The two subnets play the same role as hot-spare data centers to ensure high availability of the Cloud Services.
The initial mandatory inbound firewall –as provided by the CSP - is configured with the default deny-all mode, and Hikvision explicitly opens the ports needed to allow inbound traffic. The traffic may be restricted by the protocol, service port and source IP. The firewall can be configured in different groups, allowing different types of instances to have different rules. Hikvision is responsible for configuring these security groups on each instance. Having learned from the best practices of network security protection in the industry, Hikvision designs its own rule for the division of security zones.
Hikvision divides the Cloud Services into multiple security zones according to service functions and network security risk. Backend servers are in the Trust Zone. All accesses to the backend servers will be filtered by security groups. The security group in the boundary of each security zone enables Hik-ProConnect & Hik-Connect Cloud Services to enhance the network's self-protection, fault-tolerance, and recovery capabilities to defend itself against intrusions.

3.3.3 Network Boundary Protection

Hik-ProConnect & Hik-Connect Cloud Services are equipped with anti-DDoS protection which can detect and clear exceptions and big traffic attacks.
Hikvision deploys a Web Application Firewall (WAF) – provided by the CSP - to respond to Web attacks such as SQL injection, cross-site scripting (XSS), etc., protecting the Web application service and system from external network attacks. The Hikvision Cloud Service Operation & Maintenance team maintains this WAF.
Hikvison deploys a defense system on the host, which can protect it against viruses/Trojan, various intrusions coming through ports, bugs, etc. Defense system is an automatic security assessment service provided by CSP, which helps to improve the security and compliance of applications deployed on the cloud. For example, AWS Inspector.

4 Data Security

4.1 Data Encryption and Key Management

Hik-ProConnect & Hik-Connect Cloud Services are deployed with encryption measures to store user's unstructured sensitive data (videos and/or pictures) and structured data, including telephone number, email address, authentication materials (password, API authentication information, etc.), providing security solutions for encrypting the server-side of these sensitive data elements (protection of data at rest).
The information transmission channel between the client software and the platform is encrypted using the TLS cryptographic protocol. Currently only TLS 1.2 cryptographic Protocol is allowed.
Hikvision applies a Key Management Service (KMS) to manage all keys and deploys security solutions covering the entire management process from key generation to key revocation and replacement.

4.2 Data Isolation

Hik-ProConnect & Hik-Connect Cloud Services implement data isolation measures in the application layer, database layer and network layer to prevent the leakage of sensitive information and fault involvement.
Hik-ProConnect & Hik-Connect Cloud Services isolate each user accessing the portal. Each user should access the application with a unique ID. B Users' data is isolated from C Users' data and data from different business lines is isolated from one another.

4.3 Secure Disposal of Data

Hikvision will set data deletion rules according to users' requests and according the national

security and privacy laws (e.g. GDPR, CCPA, LGPD, etc.). There are several ways to delete data.
As for the videos stored in Hik-ProConnect & Hik-Connect Cloud Platform, rather than physical deletion, the data deletion process of Hik-ProConnect & Hik-Connect Cloud Services is performed as a release of the database storage space. Hik-ProConnect & Hik-Connect Cloud Services mark corresponding storage blocks as unassigned, and our CSPs will redistribute the storage blocks through a secure mechanism. The videos will automatically be deleted after 7 days or 30 days, depending on the users' choices and applicable legislation. Users cannot manually delete stored videos.
As for the users' other personal data such as mobile phone numbers, email addresses, accounts, credentials, etc., Hik-ProConnect & Hik-Connect Cloud Services provides a function to permanently delete the above information once an end user deletes their account voluntarily.

4.4 Interoperability and Portability

We fully consider users' data interoperability requirements by adopting common ELX, MP4, JPEG format as the data export format.
We fully consider developers' service-to-service application (API) interoperability requirements by adopting the RESTful architecture.

5 Application Business Design of Data Security

Based on the national security and privacy laws (e.g. GDPR, CCPA, LGPD, etc.), and the principle of data minimization, Hikvision protects users' data privacy in application business design.
The service functions provided by Hik-ProConnect & Hik-Connect Cloud Services to B users need to be authorized by C Users before they can query the equipment. C Users can only authorize part of the operation permission to B users, including live view, playback, PTZ control, parameter configuration, alarm reception, etc.
C Users can select the duration of authorization, and the authorization will be cancelled automatically after the duration expires.
C Users can view all the permissions authorized to B users, and can revoke the authorization to B users at any time.
Hik-ProConnect & Hik-Connect Cloud Services record the operation logs of B users for them to view and trace back.
Hik-ProConnect & Hik-Connect Cloud Services provide B users with hierarchical and multi-authority sub account management function to ensure that users can manage sub accounts with decentralized authority to avoid unauthorized operation.
Hik-ProConnect & Hik-Connect Cloud Services manage the password configuration of different accounts according to the established password management policies, including the minimum password length, password complexity, maximum failed login attempts, mandatory password update frequency, etc.
Hik-ProConnect & Hik-Connect Cloud Services will clearly inform users of the service terms,

privacy policy and other policy statements, and provide services after getting the user's authorization. When the terms of service, privacy policy and other policies change, users will be informed and at the same time be asked to authorize the continuation of our services.
On the function interface related to user data, necessary prompts will be given to users to ensure that they can use data-related functions correctly and securely.

6 Internal Organization, Process and Standard Security

6.1 Legal Compliance and Standards

Hikvision has fully developed the required security measures to meet the requirement of respective national security laws and regulations.
Hikvision has established a sound internal security program and conducted regular internal audit activities to ensure the legal compliance of Hik-ProConnect & Hik-Connect Cloud Services security implementation.
Hikvision has set up a holistic information security management system (ISMS) by adopting international security standards such as: ISO27001:2013, and has obtained ISO27001:2013 certification through external agency audits.
Hikvision has taken measures to guarantee the security and normal operation of business when performing the assessment and independent verification of legal compliance.

6.2 Security Organization

Hikvision has designed an information security management organization structure for Hik-ProConnect & Hik-Connect Cloud Services, and implements information security from three levels: executive level, management level and decision-making level. Hikvision has established an information security department to provide overall management, technical support, and audit works to ensure compliance with information security best practices, standards, and laws.
Hikvision has established a sound personnel management mechanism to ensure that the backgrounds of employees are appropriate; the behavior of employees is in line with all laws, policies, and Hikvision's business practice requirements. Thus, it further ensures that Hikvision employees have the knowledge, skills and experience to fulfil their duties.
Hikvision has established a strict security responsibility system and implemented the accountability mechanism for violations. Hikvision requires each employee to be responsible for the practice and results of his or her work, not only for technology and services, but also for legal responsibility.
Hikvision conducts risk assessment before signing a service contract with a third-party organization; requests the third-party to sign a confidentiality agreement before cooperation; conducts service and security monitoring during cooperation; revokes access rights and ensures that third-parties return assets in time after a contract expires.

6.3 Engineering Security

Hikvision attaches great importance to the security of internal security processes, and implements security risk control at each stage of the cloud service life cycle. From the design of requirements, to the release and operation of systems, every aspect is integrated with the security principle and the principle 'Secure-by-Design' is applied.

6.3.1 Demand Phase

The information security department designs the security baseline requirements and requires all project development to comply with the requirements. Besides, in the demand phase, the project team invites the security team to participate in their project, conducting security risk analysis, and identifying customized security requirements in product planning. Hikvision stipulates that security requirements are equal to product requirements.

6.3.2 Design Phase

In the internal design phase, the security team participates or evaluates the security of the software architecture design and works with the project team to ensure key security solutions have been correctly implemented.

6.3.3 Development Phase

During the system development phase, the security team developed a security development specification that requires developers to comply and minimize security holes occurred during code programming. Before the code is submitted a security self-test must be performed and the code security scan tool must be used to ensure code security and robustness.

6.3.4 Test Phase

In addition to routine testing, security tests are mandatory in each development projects. The security team develops security test cases, and the R&D team executes tests based on these cases and records test results. At the same time, the security team will simulate cyber-attacks to conduct penetration tests in each project, and the related problems will be solved by the R&D team, and then verified. The project can only be released after passing the verification.

6.3.5 Release Phase

When Hik-ProConnect & Hik-Connect Cloud products are to be released, they must be evaluated

by relevant teams such as product, R&D, testing, security, operation and maintenance, etc. They will detect security requirements compliance, code test results, business deployment, etc. The security team has a one-vote veto, and if there is a problem after checking according to the above processes, the release will be rejected.

6.3.6 Operational Phase

The security team and the operation and maintenance team monitor the security vulnerability information in real time, and discover the security threats and risks involved in Hik-ProConnect & Hik-Connect Cloud Services in time, responding and repairing them in time.

7 Operation and Maintenance Security

Hikvision pays great attention to operation & maintenance security. This chapter mainly introduces specific practices of Hik-ProConnect & Hik-Connect Cloud Services in operation and maintenance account security, change management, vulnerability management, security event management, business continuity, and disaster recovery management.

7.1 Operation and Maintenance Account Security

Hikvision uses the following systems or tools to operate and maintain for the Hik-ProConnect & Hik-Connect Cloud Services. The identity authentication mechanism for the systems and tools is as follows:

- Operation Platform: Hikvision Cloud Service Operation & Maintenance team uses an internal Operation Platform to deploy program changes into the production environment.
- IT Infrastructure: Access to background servers is restricted to an authorized jump server using allow-lists. Network ports are configured to allow access only via the SSH protocol.
- Computing Instances and Storage Resources: Operation personnel use CSPs' platform account to access these resources.
- VPN: Employees can only access the Company's internal network from the external network through the VPN.

Hikvision information security department manages password configurations for different accounts according to the established password policy, covering the requirements in the minimum password length, password complexity, maximum failed login attempts, the frequency of mandatory password changes, etc. Our account password rules is "Use a minimum of 8 characters, including at least three of the following categories: upper case letters, lower case letters, numbers, and special characters.".

While operation and maintenance personnel access Hik-ProConnect & Hik-Connect Cloud

Services in the above scenarios, their accounts and permissions are managed based on the RBAC (Role Based Access Control) model.
Hikvision information security department has established an account lifecycle management process to ensure that account creation, editing and termination have been reviewed and processed in a timely manner.

7.2 Change Management

In addition to development projects, important changes to Hik-ProConnect & Hik-Connect Cloud Services include virtual machine image changes, security group policy changes, and AWS instance changes. All of the above changes have been established with a standardized change process. Changes are made within the specified timeframe, unless in the circumstance of an urgency. Additionally, all changes require mandatory testing before implementation, to ensure information security requirements are met.
Hik-ProConnect & Hik-Connect Cloud Services will timely notify all customers and other business relationships impacted changes that are likely to affect users before implementation.

7.3 Vulnerability Management

Hikvision regularly conducts vulnerability scanning and penetration testing on the Hik-ProConnect & Hik-Connect Cloud Services to discover and patch any vulnerabilities. The information security department determines the processing priority based on the severity of the vulnerability and takes measures to fix vulnerabilities. Common methods include system security enhancement, configuration adjustment, and patch deployment.
If a vulnerability or security event has impact on customers or business partners, Hik-ProConnect & Hik-Connect Cloud Services will notify those stakeholders of the situation in a timely manner.

7.4 Security Event Management

Cloud security incidents are security incidents that are caused by suspicious network traffic, cyber-attacks or destruction of data that causes cloud service system information leakage, data tampering, system intrusion, service unavailability and other problems that may affect reliability of cloud service brand.
Given the professionalism and urgency of security incident handling, Hikvision has established professional security incident response team and a corresponding security expert resource pool. Hik-ProConnect & Hik-Connect Cloud Services adheres to the principle of security incident response for rapid discovery, fast demarcation, fast isolation and fast recovery.
Hik-ProConnect & Hik-Connect Cloud Services will inform affected customers and other service-related parties of information security incidents (or confirmed violations) in a timely manner.

7.5 Business Continuity and Disaster Recovery Management

Hikvision has established policies and procedures, implemented supporting business processes and technical measures to ensure appropriate planning, delivery and support of Hik-ProConnect & Hik-Connect Cloud Services. Hikvision has recognized the problems of any disruption to the cloud services and established a consistent unified framework for business continuity planning and plan development. Business continuity and security incident response plans are tested at planned intervals or upon significant organizational or environmental changes.

7.5.1 Global Distributed Multi-server Deployment

In order to ensure faster access speed and stronger disaster recovery capability, Hik-ProConnect & Hik-Connect Cloud Services deploy multiple servers around the world. When users access Hik-ProConnect & Hik-Connect Cloud Services, the requests will be automatically routed to the corresponding server according to users' location.

Specifically, when users enter the domain name of Hik-ProConnect & Hik-Connect Cloud Services in the browser, or log in to Hik-ProConnect & Hik-Connect Cloud Services with the App, the access requests of users will be sent to the DNS parsing service. Based on the Geolocation Routing Policy, DNS parsing service determines users' area according to source IP, and then parses the requests to the nearest server for access.

Since DNS cannot guarantee that users' requests are accurately parsed to the most appropriate server, Hik-ProConnect & Hik-Connect Cloud Services synchronize basic information between servers to allow a server to redirect requests from users in other areas to their corresponding servers to ensure the correctness of subsequent requests, so as to achieve the minimum delay of access.

At the same time, the technical solution based on global multi-server deployment makes the disaster recovery capability of Hik-ProConnect & Hik-Connect Cloud Services stronger. If a server in any area fails temporarily, other areas will not be affected, because users in different regions are isolated and independent, service downtime in a certain region will not affect other regions, such as Asia will not affect Europe.

7.5.2 High Service Availability

Based on micro service architecture design, each micro service of Hik-ProConnect & Hik-Connect Cloud Services carry business requests with independent responsibilities. When a micro service fails or fails to respond in time, it will not affect other businesses.

Each micro service is based on a cluster or hot spare deployment plan, and runs multiple service instances at the same time. According to load policy, users' requests are evenly distributed to multiple service instances. When any of the service instances fails, the requests will be distributed to other service instances to ensure that the users' requests are not affected.

The deployment plan based on a cluster or hot spare can also dynamically adjust the number of service instances according to the real-time concurrency of users' requests to ensure timely

response to users' requests.
In addition, even for the service cluster of an area server (refer to Global Distributed Multi-server Deployment), multiple server room deployment plans will be adopted. Multiple instances of the same micro service will run in different server rooms in different places. When any server room has abnormal conditions such as power failure and network disconnection, other server rooms will balance loading of users' requests to ensure high availability of cloud services.
The database of Hik-ProConnect & Hik-Connect Cloud Services also adopt Mechanism of Multiple Server Room Deployment and Data Synchronization, and the data update of one database instance will be synchronized to other database instances in real time. When any server room has abnormal conditions such as power failure and network disconnection, micro service can access data from the database instances of other server rooms. When the failure room is recovered, the synchronization of missing data will also be carried out automatically.
Hik-ProConnect & Hik-Connect Cloud Services can flexibly replace computing instances and storage between multiple subnets in the same area, called Availability Zone, which are equivalent to hot spare data centers, ensuring high availability of cloud services. Each Availability Zone is an independent domain, that is, each availability zone is physically isolated.
Distributed deployment of platform applications based on multiple Availability Zones ensures continuous operation in most failure scenarios, including natural disasters and system failures.

7.5.3 Multi-level Cache

Hik-ProConnect & Hik-Connect Cloud Services adopt multi-level cache technology from database cache, to the cloud service cache, to the edge service cache, and to the App or the browser cache. When users use the App or the browser to access a cloud service, the requests will first search for the data to be returned in the cache level closest to users. If the data exists, it will be returned directly, if the data does not exist, the request will search for it in the next level cache. With this technology, most of users' requests will be found and returned directly from local cache of the App or browser to reduce the consumption of traffic, and the other users' requests will be found and returned from the edge service cache nearest to users to reduce network delay. Therefore, only a few requests are found and returned from cloud, so as to ensure the instant response of requests and reduce the network traffic consumption.

7.5.4 Network Self-adaption

When users view live videos or play back video footage, the device may be in the same LAN as users, or may be in a different or even outside multi-layer network, which makes it difficult for the App or browser to select the optimal path to access the device.
Hikvision uses network self-adaption technology to analyze and determine network environment of the current users, and select the optimal path to access the device from multiple methods such as direct connection, P2P, and streaming media forwarding. On the premise of ensuring the minimum delay of live view and playback, it ensures the minimum occupation of users' mobile traffic and LAN bandwidth.

7.6 Operation Security Review

In order to prevent the security risk caused by non-compliances of the system due to improper operation or unauthorized update of system configuration in the daily operation and maintenance activities, the operation and maintenance team regularly conduct security health check on the operation system, database, Middleware and network devices to ensure that all configurations are compliant with the security baseline.

For non-compliant items, a risk assessment is required followed by remediation within a specified period of time based on the risk level. Otherwise, an exception should be raised. All the exceptions need to be approved by the information security department, including security manager, maintained by designated personnel and reviewed regularly afterwards.

The bastion host, a gateway between internal and external world, monitors the operations of the operator. The operation logs of all activities are saved. System logs and business logs are collected by the establishment of ELK (ElasticSearch, Logtash, Kibana), a real-time log analysis platform. The above logs can be reviewed within a certain period of time.