HIKVISION

Hikvision's White Paper on GDPR

www.hikvision.com

Copyright Disclaimer.

Trademarks Acknowledgement

HIKVISION and other Hikvision's trademarks and logos are the properties of Hikvision in various jurisdictions. Other trademarks and logos mentioned below are the properties of their respective owners.

Contact Information

No.555 Qianmo Road, Binjiang District, Hangzhou 310052, China

Tel: +86-571-8807-5998

Fax: +86-571-8993-5635

Email: overseasbusiness@hikvision.com; sales@hikvision.com

Technical Support: support@hikvision.com

HSRC (Hikvision Security Response Center) Email: HSRC@hikvision.com

Legal Disclaimer

TO THE MAXIMUM EXTENT PERMITTED BY APPLICABLE LAW, THE CONTENT DESCRIBED IN THIS DOCUMENTATION IS PROVIDED "AS IS", AND HIKVISION MAKES NO WARRANTIES, EXPRESS OR IMPLIED, INCLUDING WITHOUT LIMITATION, FITNESS FOR COMMERCIAL USE OF A PARTICULAR PURPOSE.

HIKVISION PROVIDES NO WARRANTY ON THE ACCURACY OF THIS DOCUMENTATION CONTENT, AND RESERVES RIGHTS TO CORRECT OR MODIFY THE CONTENT WITHOUT FURTHER NOTICE.

ANY DECISIONS RELIED ON OR BY THE USE OF THIS DOCUMENTATION TOGETHER WITH ANY CONSEQUENCES THAT IT MAY CAUSE SHALL BE UNDER YOUR OWN RESPONSIBILITY.

IN THE EVENT OF ANY CONFLICTS BETWEEN THIS WHITE PAPER AND THE APPLICABLE LAW, THE LATER PREVAILS.

Content

Part1 Introduction to GDPR

1.1 What is GDPR

The General Data Protection Regulation (GDPR) which comes into force on May 25, 2018, is Europe's new framework for data protection laws. The new regulation replaces the Data Protection Directive 95/46/EC (Directive 95) and was designed to harmonize data privacy laws across Europe, to protect and empower all EU citizens' data privacy and to reshape the way organizations across the region approach data privacy.

1.2 Background

After four years of preparation and debate, the new GDPR was finally approved by the EU Parliament on 14 April 2016. As of May 25, 2018, after two years transition, it comes into force and potentially impacts all the companies and organizations doing business in the European Union (EU). The new regulation entitles more rights to data subjects (users) and enhances data protection level - protection by design and by default - and the security level of personal data. It also requires for organizations and businesses to be fully transparent about how they are using and safeguarding personal data, and to be able to demonstrate accountability for their data processing activities.

The regulation has 99 articles in 11 chapters, including the specifications on rights of the data subjects, and the obligations of data controllers and data processors. Compared with the Directive 95, which already established minimum standards for legislative protection on personal data in EU members, there are several major changes in terms of the subject rights, the controller obligations, the data transmission rules, etc., and the GDPR is more inclusive and adaptable.

1.3 The Objectives of GDPR

The GDPR was designed to enhance the privacy protection for individuals within the EU and privacy protection in IoT (Internet of Things), and simplify the management of data protection.

The key areas of GDPR are as follows:

- Enhance personal right, and provide individuals with more control over their own personal information;
- Strengthen data privacy laws within the EU;
- A transfer of personal data to a third party or country must take place where adequate protection is ensured. The data must be protected as adequately as it is within the EU.

1.4 Who does GDPR affect

The GDPR not only applies to organizations located within the EU but it will also apply to organizations located outside of the EU if they offer goods or services to, or monitor the behavior of, EU data subjects. It applies to all companies processing and holding the personal data of data subjects residing in the European Union, regardless of the company's location.

1.5 What constitutes personal data?

Personal data means any information relating to an identified or identifiable natural person (data subject); an identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or

more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person.

1.6 What is the difference between a data controller and a data processor?

A data controller is a natural or legal person, public authority, agency or other body which, alone or jointly with others, determines the purposes, conditions and means of the processing of personal data. The data processor is a natural or legal person, public authority, agency or other body which processes personal data on behalf of the controller.

The relationship between data subject, data controller and data processor is shown in figure 1.

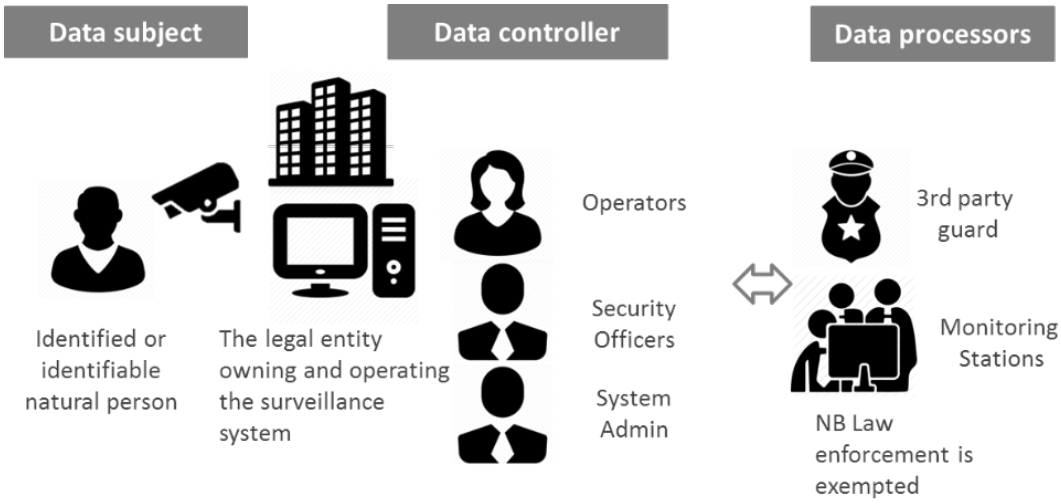


Figure.1 the relationship between data subject, data controller and data processor

1.7 GDPR video surveillance guidelines

In terms of Data subject 	Implement data minimization: 1. Optimize camera placement & field of view 2. Apply privacy masks	Notice to individuals affected, including: 1. Purpose of surveillance 2. Kept by who (Data Controller/ Data Processor) 3. Retention policy (how long)
In terms of Data controller 	Apply & maintain high general cybersecurity Protection mechanism of personal data 1. organizational requirements 2. Data Protection Officer 3. Maintain overview of personal data records & processing flows 4. Data breach notification within 72 hours	Training of personnel (mandatory) 1. Cybersecurity incl. user administration 2. Export of video data incl. masking of persons of non-interest User rights management 1. Limit user access on a strictly need basis 2. Keep audit logs of user access and activities

In terms of Data processors 	Any 3rd party that processes personal data must sign a Data Processing Agreement 1. Export of video data incl. masking of persons of non-interest 2. Transfer of personal data outside the EU 3. Seek legal advice!

1.8 What are the penalties for non-compliance?

Organizations can be fined up to 4% of annual global turnover for breaching the GDPR or up to €20 Million. This is the maximum fine that can be imposed for the most serious infringements e.g. not having sufficient customer consent to process data or violating the core of Privacy by Design concepts. There is a tiered approach to fines e.g. a company can be fined 2% for not having their records in order (article 28), not notifying the supervising authority and data subject about a breach or not conducting impact assessment.

Part2 Impact to the video surveillance industry

2.1 What does GDPR mean for the video surveillance industry?

GDPR makes no explicit mention of the video surveillance industry. However, it is impacted indirectly as users of video surveillance solutions process large amount of data generated by the cameras and their sensors.

Data controllers running video surveillance applications in the EU, including public video surveillance systems, need to pay special attention to the provisions in the GDPR relating to the identification, management, and mitigation of risks. Data controllers performing video surveillance in the EU have to undertake very specific tasks, including conducting risk assessments, ensuring privacy by design in their systems, and developing appropriate signage.

As a global market leader, Hikvision is committed to protecting personal data and fully supports the implementation of the GDPR requirements. Hikvision has been taking several initiatives to protect personal data in the use of its products and solutions. That includes communication encryption through AES algorithms and the HTTPS protocol, minimized data collection, data anonymization, user authorized data collection, data security audit, and more.

Part 3 Data and cybersecurity in Hikvision products

Hikvision Security Achievement / GDPR Compliance

As the world's leading supplier of innovative video surveillance products and solutions, Hikvision is committed to investing every effort to provide customers with the ultimate security products and solutions, and to educate partners and end users about Data Security.

Hikvision has always attached great importance to international data security laws and regulations, actively coordinating and meeting high market standards with high-quality products and systems.

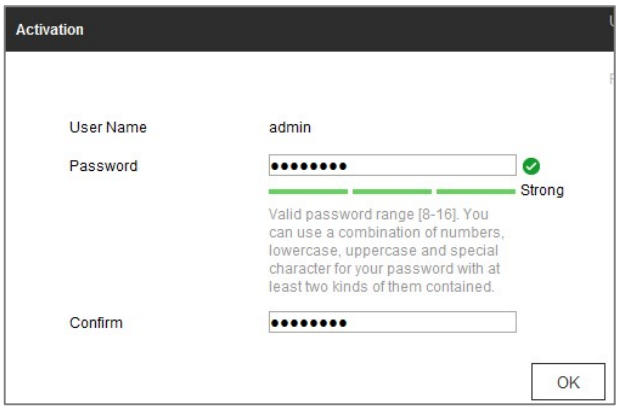
Hikvision encourages all data controllers and data processors to enhance their security in the following four ways:

- Identity
- Access
- Privacy
- Status

3.1 Identity authentication

3.1.1 Strong password

Hikvision highly recommends users create a strong password of their own choosing (using a minimum of 8 characters, including at least three of the following categories: upper case letters, lower case letters, numbers and special characters) in order to increase the security of your product. Hikvision also recommends users reset passwords regularly, especially in high security systems - resetting the password monthly or weekly can better protect their product.



Step 1 Turn on the camera, and connect the camera to the network

Step 2 Enter the IP address into the address bar of the web browser, and click **Enter** to enter the activation interface

Step 3 Create a password and input the password into the password field

Step 4 Confirm the password

Step 5 Click **OK** to save the password and enter the live view interface

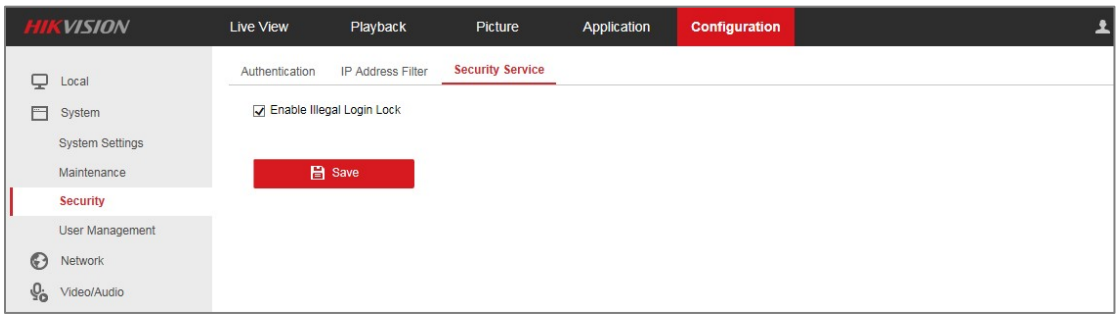
3.1.2 Activation

You are required to activate the camera first by setting a strong password for it before you can use the camera.

Activation via Web Browser, Activation via SADP, and Activation via Client Software are all supported.

3.1.3 Lock Illegal Login IP Address

In order to effectively prevent illegal attacks, the IP address will be locked if the admin user has 7 failed user name/password attempts (5 times for the operator/user).



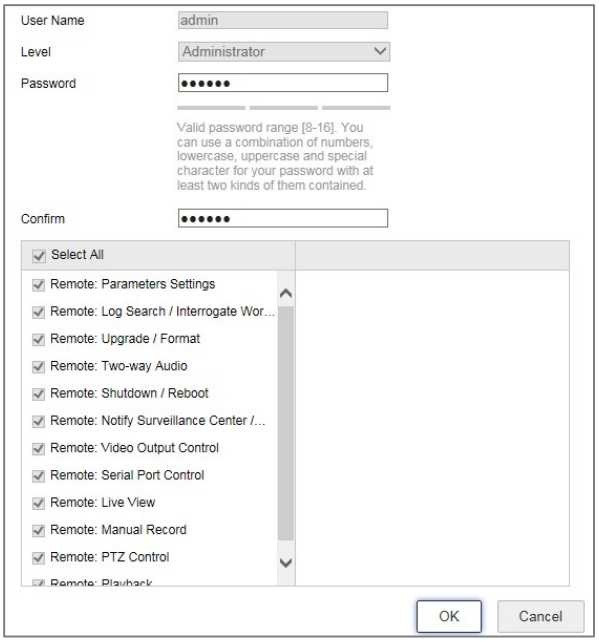
Step 1 Enter the security service configuration interface: **Configuration** > **System** > **Security** > **Security Service**

Step 2 Check the checkbox of **Enable Illegal Login Lock**, and then the IP address will be locked if the admin user performs 7 failed user name/password attempts (5 times for the operator/user)

Note: If the IP address is locked, you can only log back into the device after 30 minutes.

3.1.4 Set Permission Level to Users

To limit user access in a strict way and to prevent sensitive information becoming available to unauthorized access, Hikivision provides different permission levels for each user to set limitations on camera control.



Step 1 Enter the User Management interface: **Configuration** >**System** >**User Management**

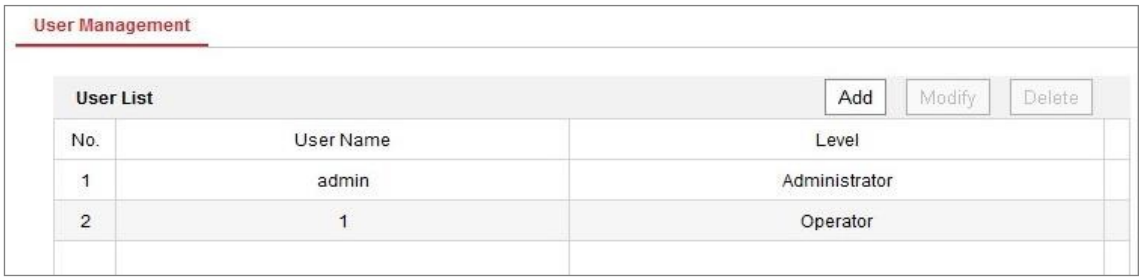
Step 2 Click **Add** to add a user

Step 3 Input the **User Name**, select **Level** and input **Password**

Note: Up to 31 user accounts can be created; Users of different levels own different default permissions. Operator and user are selectable

Step 4 You can check or uncheck the permissions for the new user

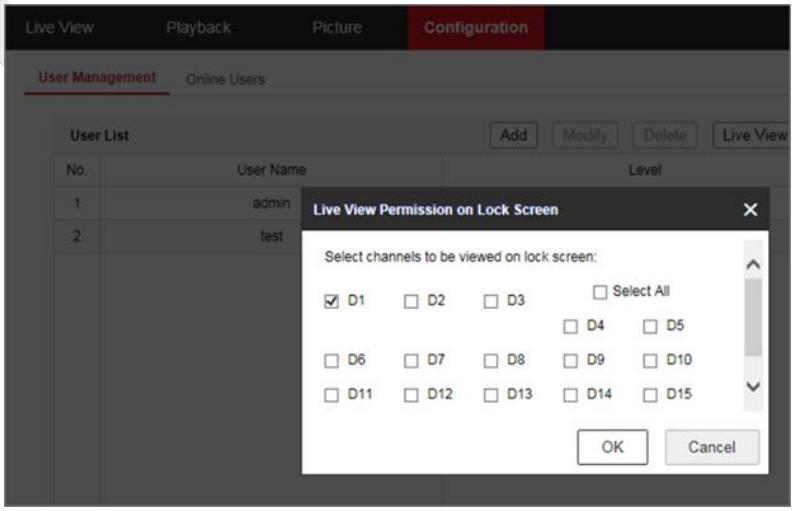
Step 5 Click **OK** to finish the user addition

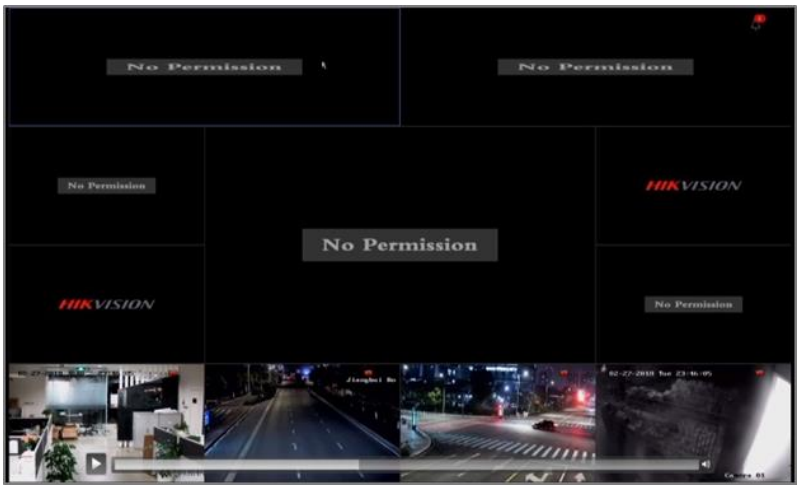


3.2. Access Control

3.2.1 Live View Permission on Lock Screen

This function enables the administrator to configure local live view permissions in the remote web site. All the users will have local live view permission of selected channels.





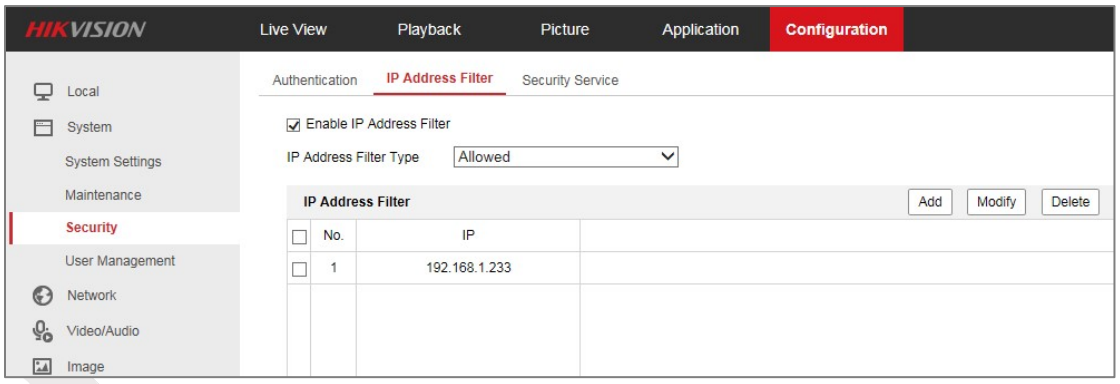
Step 1 Enter the User Management interface: **Configuration >System >User Management**

Step 2 Click **Live View Permission**

Step 3 Select **channel(s)** to enable live view permission on locked screen

3.2.2 Set IP Address Filter

Enabling IP filtering for authorized clients will prevent the camera from being accessed by any other unauthorized clients.



Step 1 Enter the IP Address Filter interface: **Configuration > System > Security > IP Address Filter**

Step 2 Check the checkbox of **Enable IP Address Filter**

Step 3 Select the type of IP Address Filter in the drop-down list, **Forbidden** and **Allowed** are selectable

Step 4 Set the **IP Address Filter** list: Click the **Add** to add an IP; Input the IP Address; Click the **OK** to finish adding

3.2.3 Port Security

Hikvision adopts the "secure by default" approach.

The following function is cancelled for network security：

Hikvision's devices provide no Telnet interface.

The following functions are disabled by default to make sure that it is not connected to an insecure network in the first place：

Hikvision's devices disable SSH by default.

Hikvision's devices disable SNMP by default.

Hikvision's devices disable UPNP by default.

Multicasting is disabled to prevent a camera from multicasting video streams.

If you need these functions, be aware that they may bring network security risks.

3.2.4 ONVIF

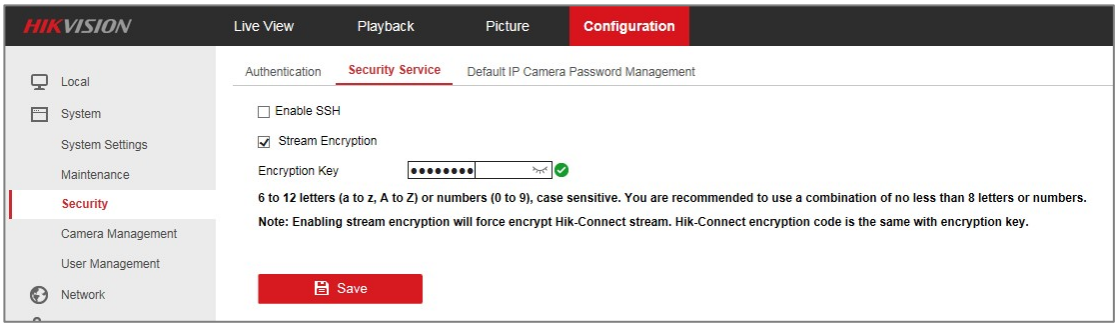
ONVIF functionality is disabled by default. The path of ONVIF configuration in web component is **Configuration->Network->Advanced Settings->Integration Protocol**. ONVIF user accounts need to be created for application of ONVIF. Three ONVIF user

levels of Administrator, User and Operator are selectable, with up to 32 user accounts. Web component, iVMS-4200 and Batch Configuration tool are available for ONVIF configuration.

3.3 Privacy control*

3.3.1 Data Encryption –stream encryption

The stream encryption enables administrators to encrypt streams for live view, playback, download, backup, etc. to guarantee the safety of data transfer.



Step 1 Enter the security service configuration interface: **Configuration > System > Security > Security Service**

Step 2 Check the checkbox of **Stream Encryption**, and input the encryption key.

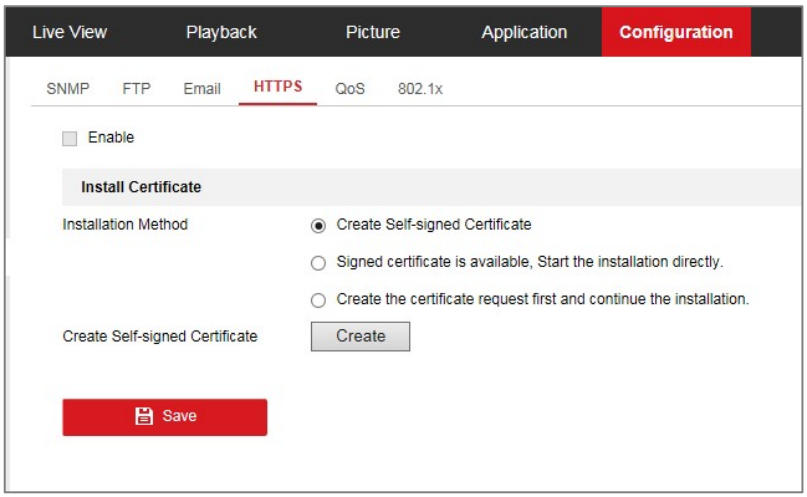
Note: Enabling stream encryption will force encrypt Hik-Connect stream. Hik-Connect encryption code is the same with encryption key.

3.3.2 Data Encryption - HTTPS

HTTPS provides authentication of the website and its associated web server, which protects against 'Man-in-the-middle' attacks. Perform the following steps to set the port number of HTTPS.

* Due to different hardware or software versions, some functions may be different. If there is inconsistency of the function between the actual product and the one in the guide, the actual product shall govern.

E.g., If you set the port number as 443 and the IP address is 192.168.1.64, you may access the device by inputting https://192.168.1.64:443 via the web browser.



Step 1 Enter the HTTPS settings interface. **Configuration > Network > Advanced Settings > HTTPS**.

Step 2 Check the checkbox of **Enable** to enable the function.

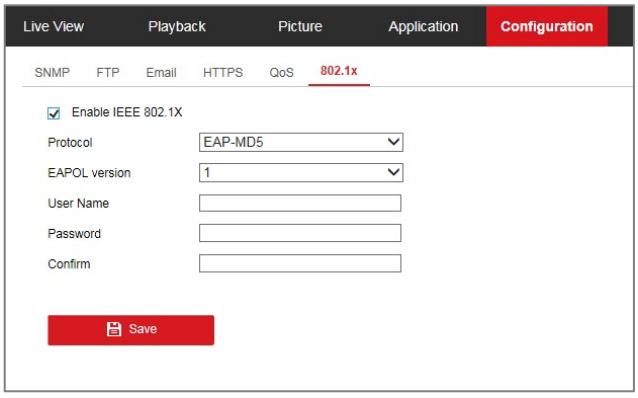
Step 3 Create the self-signed certificate or authorized certificate.

Step 4 The certificate info will be available after you successfully create and install the certificate.

Step 5 Click the **Save** button to save the settings.

3.3.3 Network Access Control – 802.1X

The IEEE 802.1X standard is supported by network cameras and, when the feature is enabled, the camera data is secured and user authentication is needed when connecting the camera to the network protected by the IEEE 802.1X. Before you start the authentication server must be configured. Please apply and register a user name and password for 802.1X in the server.



Step 1 Enter the 802.1X Settings interface, **Configuration > Network > Advanced Settings > 802.1X**

Step 2 Check the **Enable IEEE 802.1X** checkbox to enable the feature.

Step 3 Configure the 802.1X settings, including Protocol, EAPOL version, User Name, Password and Confirm.

Note: The EAPOL version must be identical with that of the router or the switch.

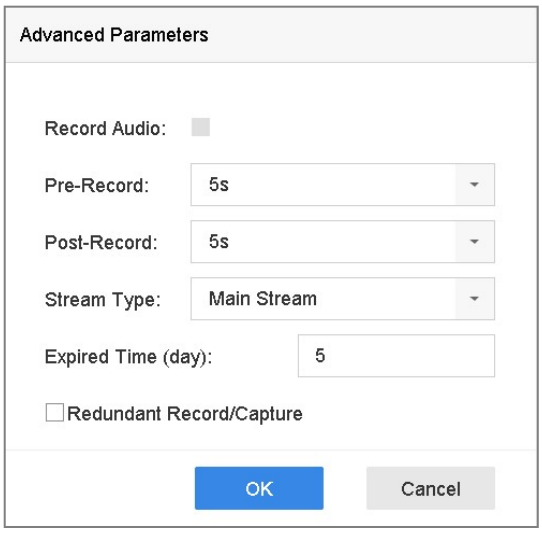
Step 4 Enter the user name and password to access the server.

Step 5 Click **Save** to finish the settings.

Note: A reboot is required for the settings to take effect.

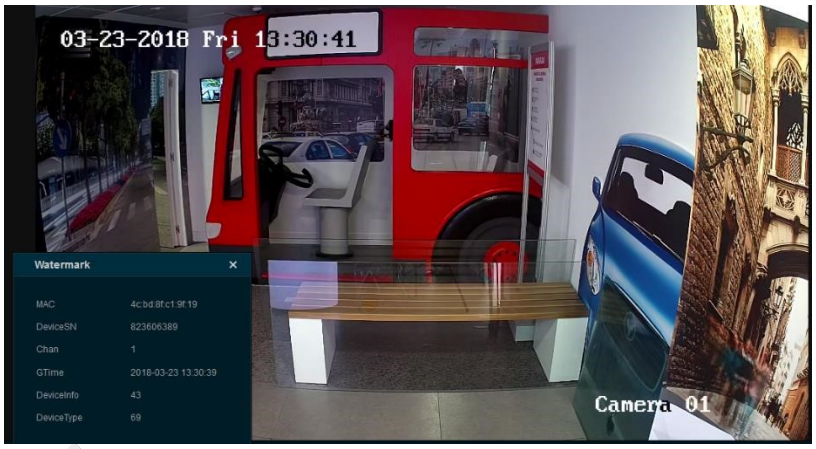
3.3.4 Expiry Date (Date Retention Setting)

Expired time is the period that a recorded file is kept in the HDD. When the deadline is reached, the file will be deleted. If you set the expired time to 0, the file will not be deleted. The amount of time the file is kept should be determined by the Data Controller when setting an Operational Requirement (OR) or objectives for the use of a CCTV system and will also be influenced by the capacity of the HDD.



3.3.5 Watermark

Adding a watermark in the video stream is an ideal method to deal with video manipulation issues. The watermark is concealed in the original files. You can see the information only with a Hikvision VSPlayer.



3.3.6 Privacy Mask*

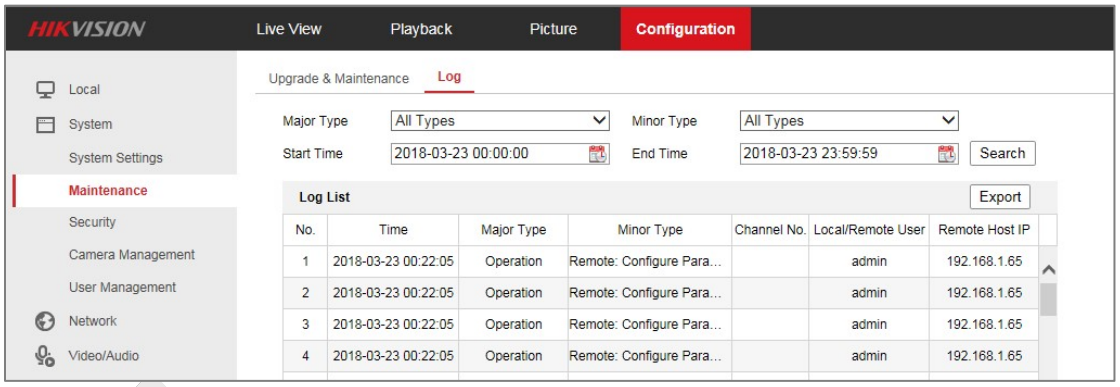
Hikvision developed a human body mosaic solution to support this rising request. It uses a dual-lens face recognition camera based on our deep learning algorithm and powerful GPU.

* The Privacy Mask is only available for some models of Deepview IPC and Deepmind NVR.

3.4 Status monitoring

3.4.1 Log Management

To ensure all the operations can be traced, the operation, alarm, exception and information of the camera can be stored in log files. You can also export the log files on your demand and log alarm is also provided.

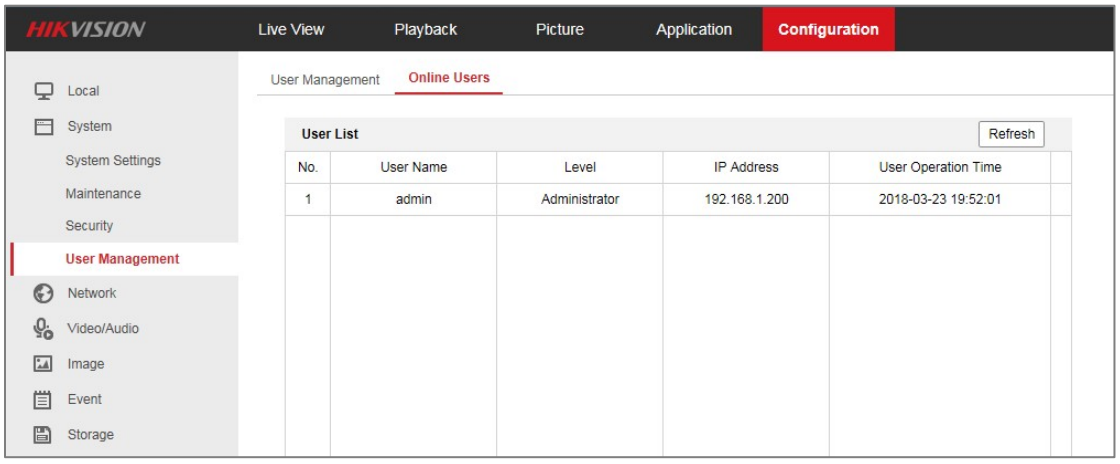


Step 1 Enter log searching interface: **Configuration > System > Maintenance > Log**.

Step 2 Set the log search conditions to specify the search, including the Major Type, Minor Type, Start Time and End Time. Click Search to search log files. The matched log files will be displayed on the log list interface.

3.4.2 Online User Management

You can see the current users who are visiting the device through this interface. User information, such as user name, level, IP address and operation time, is displayed in the User List.

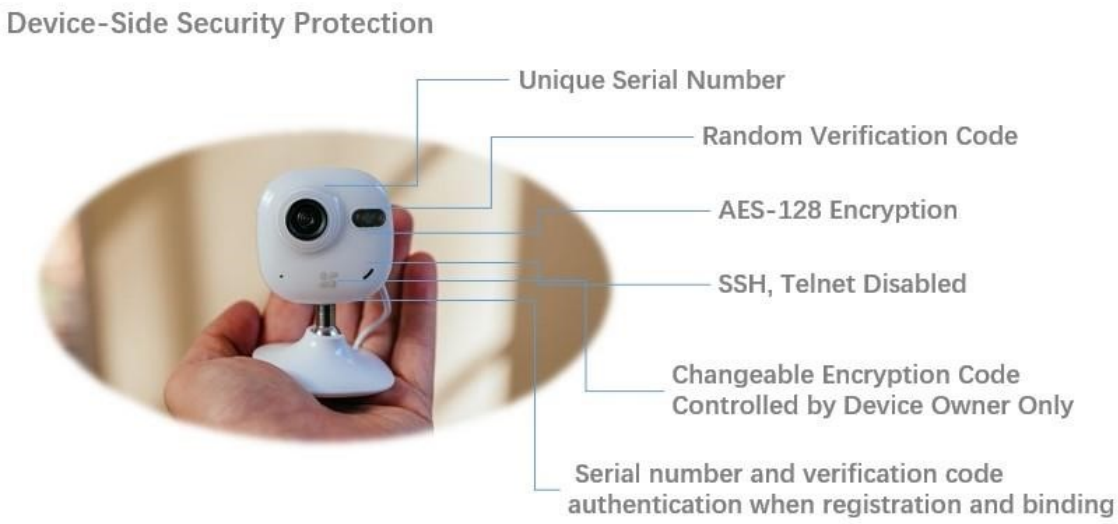


Step 1 Click **Refresh** to refresh the list.

Part 4 Cloud Data Security*

4.1 Device security

4.1.1 Device-Side Security Protection



4.1.2 Device binding

- Serial number and verification code authentication
- One device for one account only

4.1.3 Video Streaming Encryption

- AES-128 bit
- Encryption code required for new terminal
- Changeable encryption code controlled by device owner only
- End-to-end encryption

* Cloud services cover Hik-Connect, EZVIZ's services.

4.2 Cloud storage security

- **Transmission security**

HTTS security channel is applied during the transmission from the device to the S3

- **Storage security**

The AWS S3 is applied for the physical storage, and all data stored on S3 is encrypted by AES-256.

- **Data deletion**

Based on the service time of specific cloud storage, the data in cloud storage will be deleted automatically by S3 after service expiration. The picture information generated by the device alarm will be automatically deleted by S3 after 7 days.

4.3 Other security guarantee

- Quarterly system testing of our system integrity from security threats by 3rd parties
- Setup an external vulnerability collection platform
- Full R&D engineering team dedicated to security
- Use of Trend Micro's Deep Security to safeguard the data

Third party certification

- ISO 27001 Certification
    - Assurance to Clients

When a client is working with you, he/she would concern about the assurance of his/her data. When you have an ISO 27001 certification on your side, you would have your client's confidence, and this would help you retain your clients, and bring in more clients at the same time.

➢ SOC 2 Type 1 Report

- Service Organization Controls 2 are strict regulations designed by the AICPA, covered under SSAE 16, to ensure that technology-based service providers have proper systems in place to protect client information and data.

- What it reports on?

  Security—This addresses protection against both physical and logical unauthorized access.

  Availability—This pertains to the system's availability for operation and use as previously agreed.

  Processing integrity—This ensures system processing is authorized, complete, accurate and timely.

  Confidentiality—The protection of information that is confidential, as committed or agreed.

  Privacy—This regulation ensures personal information is collected, used, retained and disclosed in accordance to the organizations' privacy notice, as well as the privacy principles of the AICPA and CICA.

Appendix: key points of some important articles in the GDPR

Key points of some important Articles in the regulation are as follows. Please find the original articles for more details.

1. Territorial scope（Art.3）

This Regulation applies to:

1) the processing of personal data in the context of the activities of an establishment of a controller or a processor in the Union, regardless of whether the processing takes place in the Union or not

2) the processing of personal data of data subjects who are in the Union by a controller or processor not established in the Union, where the processing activities are related to:

   a) the offering of goods or services, irrespective of whether a payment of the data subject is required, to such data subjects in the Union; or

   b) the monitoring of their behavior as far as their behavior takes place within the Union.

3) the processing of personal data by a controller not established in the Union, but in a place where Member State law applies by virtue of public international law.

2. Principles relating to processing of personal data (Art.5)

Personal data shall be:

a) processed lawfully, fairly and in a transparent manner;

b) collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes;

c) adequate, relevant and limited to what is necessary ('data minimization');

d) accurate and, where necessary, kept up to date;

e) kept in a form which permits identification of data subjects for no longer than is necessary for the purposes for which the personal data are processed;

f) processed in a manner that ensures appropriate security of the personal data, using appropriate technical or organizational measures.

The controller shall be responsible for, and be able to demonstrate compliance with, the above.

3. Lawfulness of processing (Art.6)

Processing shall be lawful only if that at least one of the following applies:

a) the data subject has given consent to the processing of his or her personal data for one or more specific purposes;

b) processing is necessary for the performance of a contract to which the data subject is party;

c) processing is necessary for compliance with a legal obligation to which the controller is subject;

d) processing is necessary in order to protect the vital interests of the data subject or of another natural person;

e) processing is necessary for the performance of a task carried out in the public interest or in the exercise of official authority vested in the controller;

f) processing is necessary for the purposes of the legitimate interests pursued by the controller, except where such interests are overridden by the interests of the data subject.

4. Conditions applicable to child's consent in relation to information society services (Art.8)

Where the child is below the age of 16 years, such processing shall be lawful only if and to the extent that consent is given or authorized by the holder of parental responsibility over the child. Member States may provide by law for a lower age for those purposes provided that such lower age is not below 13 years.

5. Processing of special categories of personal data (Art.9)

Processing of personal data shall be prohibited to reveal racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership, and the processing of genetic data, biometric data for the purpose of uniquely identifying a natural person, data concerning health or data concerning a natural person's sex life or sexual orientation. This shall not apply if, for example, the data subject has given explicit consent to the processing of those personal data, or the processing is necessary for the purposes of carrying out the obligations and exercising specific rights of the controller or of the data subject in the field of employment and social security

6. Right to be forgotten (Art.17)

When the personal data are no longer necessary in relation to the purposes, or the data subject withdraws consent on which the processing is based, or there is no other legal ground for the processing, the data subject shall have the right to obtain from the controller the erasure of personal data concerning him or her without undue delay. If the data has been transmitted to any third party (or third party websites), the data controller should inform the third party to erase the data.

7. **Right to data portability (Art.20)**

The data subject shall have the right to receive the personal data concerning him or her, which he or she has provided to a controller, and have the right to transmit those data to another controller.

8. **Notification of a personal data breach (Art.33, 34)**

In the case of a personal data breach, the controller shall without undue delay and, where feasible, not later than 72 hours after having become aware of it, notify the personal data breach to the supervisory authority. When the personal data breach is likely to result in a high risk to the rights and freedoms of natural persons, the controller shall communicate the personal data breach to the data subject without undue delay.

9. **Designation of the data protection officer (Art.37, 38, 39)**

The controller and the processor shall designate a data protection officer to ensure the compliance of the data protection and deal with relevant affairs relating to the data protection.

10. **General Conditions for imposing administrative fines (Art.83)**

Supervisory authorities are empowered to assess penalties, and the results of the infraction would be severe sanctions and huge fines. According to the

GDPR, there are two tiers of maximum fines, based on the severity of the violation:

a) 2% of the organization's revenue or €10M, whichever is higher

b) 4% of the organization's revenue or €20M, whichever is higher

The amount of the administrative fine shall be based on:

1) the nature, gravity and duration of the infringement;

2) the intentional or negligent character of the infringement;

3) the degree of responsibility of the controller or processor;

4) any relevant previous infringements by the controller or processor;

5) the categories of personal data affected by the infringement;

6) the level of damage suffered by the subject;

7) any action taken to mitigate the damage;

8) any financial benefits gained, directly or indirectly, from the infringement.

Hikvision

White Paper on GDPR

See Far, Go Further

HIKVISION®

Hikvision Digital Technology Co., Ltd.

No.555 Qianmo Road, Binjiang District, Hangzhou 310052, China