HikCentral Professional
ISUP Device Accessing
Operation Guide

Legal Information

About this Manual

The Manual includes instructions for using and managing the Product. Pictures, charts, images and all other information hereinafter are for description and explanation only. The information contained in the Manual is subject to change, without notice, due to firmware updates or other reasons. Please find the latest version of this Manual at the Hikvision website (https://www.hikvision.com/).

Please use this Manual with the guidance and assistance of professionals trained in supporting the Product.

Trademarks

HIKVISION and other Hikvision's trademarks and logos are the properties of Hikvision in various jurisdictions.

Other trademarks and logos mentioned are the properties of their respective owners.

Disclaimer

TO THE MAXIMUM EXTENT PERMITTED BY APPLICABLE LAW, THIS MANUAL AND THE PRODUCT DESCRIBED, WITH ITS HARDWARE, SOFTWARE AND FIRMWARE, ARE PROVIDED "AS IS" AND "WITH ALL FAULTS AND ERRORS". HIKVISION MAKES NO WARRANTIES, EXPRESS OR IMPLIED, INCLUDING WITHOUT LIMITATION, MERCHANTABILITY, SATISFACTORY QUALITY, OR FITNESS FOR A PARTICULAR PURPOSE. THE USE OF THE PRODUCT BY YOU IS AT YOUR OWN RISK. IN NO EVENT WILL HIKVISION BE LIABLE TO YOU FOR ANY SPECIAL, CONSEQUENTIAL, INCIDENTAL, OR INDIRECT DAMAGES, INCLUDING, AMONG OTHERS, DAMAGES FOR LOSS OF BUSINESS PROFITS, BUSINESS INTERRUPTION, OR LOSS OF DATA, CORRUPTION OF SYSTEMS, OR LOSS OF DOCUMENTATION, WHETHER BASED ON BREACH OF CONTRACT, TORT (INCLUDING NEGLIGENCE), PRODUCT LIABILITY, OR OTHERWISE, IN CONNECTION WITH THE USE OF THE PRODUCT, EVEN IF HIKVISION HAS BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES OR LOSS.

YOU ACKNOWLEDGE THAT THE NATURE OF THE INTERNET PROVIDES FOR INHERENT SECURITY RISKS, AND HIKVISION SHALL NOT TAKE ANY RESPONSIBILITIES FOR ABNORMAL OPERATION, PRIVACY LEAKAGE OR OTHER DAMAGES RESULTING FROM CYBER-ATTACK, HACKER ATTACK, VIRUS INFECTION, OR OTHER INTERNET SECURITY RISKS; HOWEVER, HIKVISION WILL PROVIDE TIMELY TECHNICAL SUPPORT IF REQUIRED.

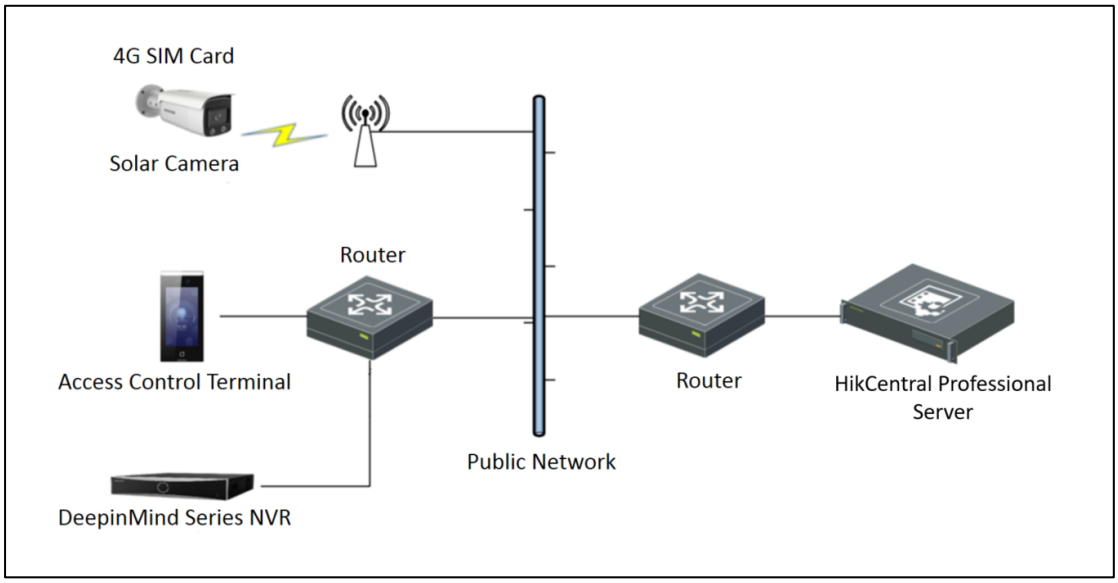
YOU AGREE TO USE THIS PRODUCT IN COMPLIANCE WITH ALL APPLICABLE LAWS, AND YOU ARE SOLELY RESPONSIBLE FOR ENSURING THAT YOUR USE CONFORMS TO THE APPLICABLE LAW. ESPECIALLY, YOU ARE RESPONSIBLE, FOR USING THIS PRODUCT IN A MANNER THAT DOES NOT INFRINGE ON THE RIGHTS OF THIRD PARTIES, INCLUDING WITHOUT LIMITATION, RIGHTS OF PUBLICITY, INTELLECTUAL PROPERTY RIGHTS, OR DATA PROTECTION AND OTHER PRIVACY RIGHTS. YOU SHALL NOT USE THIS PRODUCT FOR ANY PROHIBITED END-USES, INCLUDING THE DEVELOPMENT OR PRODUCTION OF WEAPONS OF MASS DESTRUCTION, THE DEVELOPMENT OR PRODUCTION OF CHEMICAL OR BIOLOGICAL WEAPONS, ANY ACTIVITIES IN THE CONTEXT RELATED TO ANY NUCLEAR EXPLOSIVE OR UNSAFE NUCLEAR FUEL-CYCLE, OR IN SUPPORT OF HUMAN RIGHTS ABUSES.

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

Table of Contents

1 Network Configuration

1.1 Typical Network Topology



1.2 Device Network

The devices are connected to the public network via 4G SIM cards (solar cameras) or by port mapping (access control devices and NVRs).

1.3 HikCentral Professional Platform Network

1.3.1 Public Network Configuration of the Server

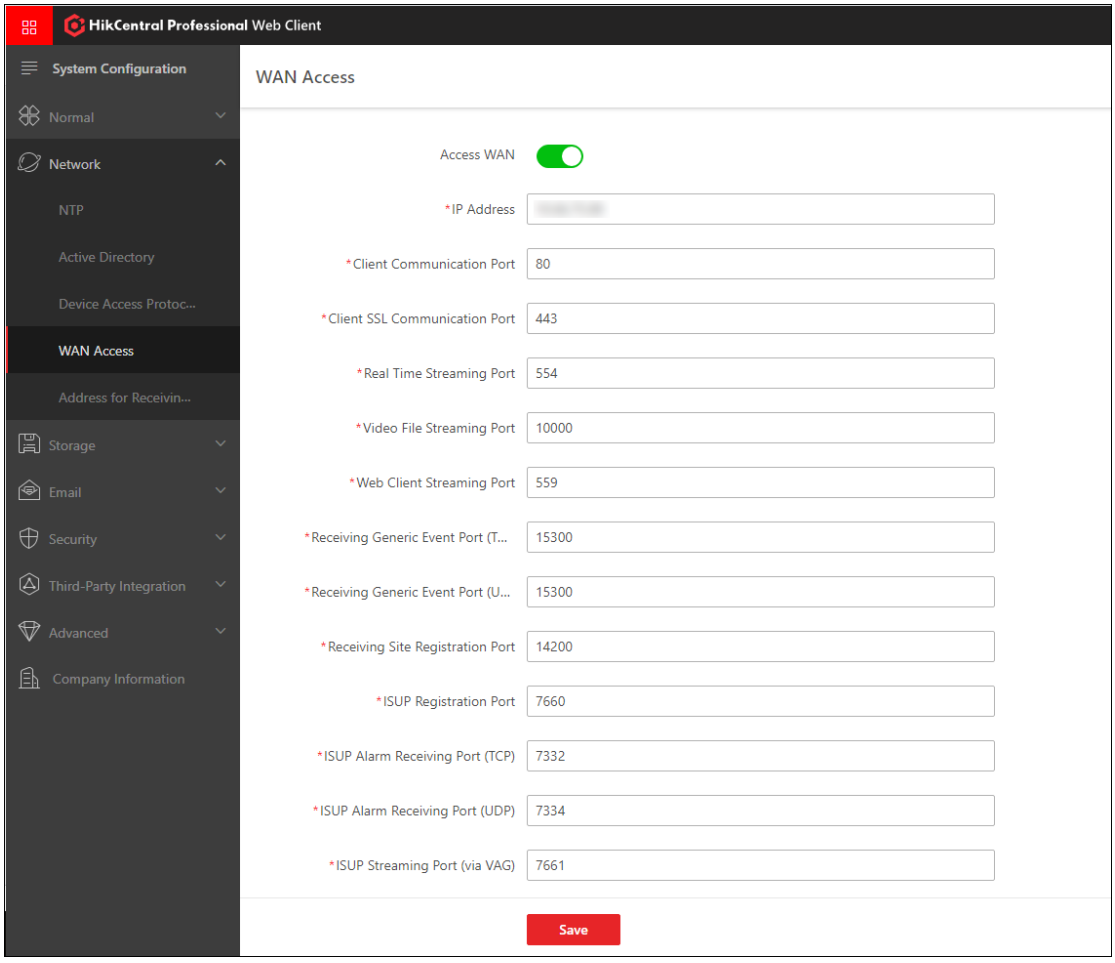
The HikCentral Professional server opens the following ports of the platform to the public network by configuring a fixed IP address or domain name of the public network or port mapping.

Port	Protocol	Port Description
80	HTTP/WebSocket	Used for Web Client & Control Client to access the platform via HTTP.
443 (Optional)	HTTPS	Used for Web Client & Control Client to access the platform via HTTPS.
7332	TCP	Used for receiving alarms from ISUP devices.
7334	UDP	Used for receiving alarms from ISUP devices.
7660	TCP	Used for receiving registration from ISUP devices.

7661	TCP	Used for getting the stream from ISUP devices via Streaming Server.
6123	HTTP	Used for picture storage of ISUP devices.
27661	HTTP	Used for calling back the ISUP signaling.
554	RTSP	Used for getting the stream for live view (real-time streaming port).
559	WebSocket	Used for getting the stream for Google Chrome, Firefox, or Safari.
10000	TCP	Used for getting the stream for playback (video file streaming port).
16000	TCP	Used for getting the stream from ISUP devices via the plugin.

1.3.2 Public Network Configuration of HikCentral Professional Platform

Log in to the Web Client of HikCentral Professional, click **System Configuration**->**Network**->**WAN Access** to enter the WAN Access page. Switch on **Access WAN**, enter the IP address or domain name and mapped port(s) of the public network, and click **Save** to save the settings.



1.4 (Optional) pStor Network

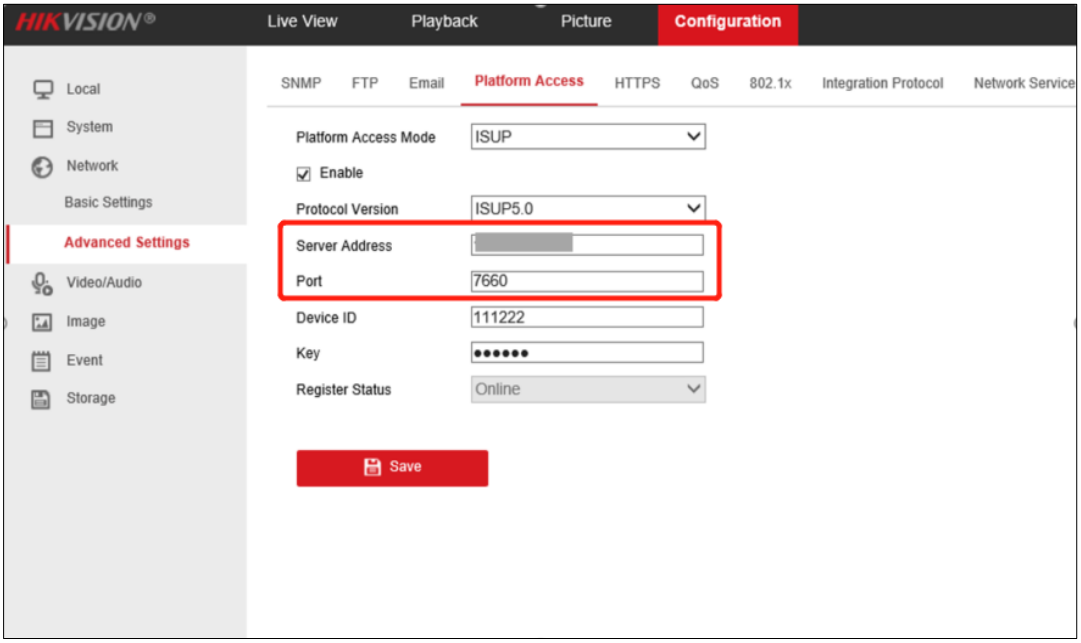
If pStor is accessed in the overall solution, the following ports of pStor need to be opened to the public network.

Port	Protocol	Port Description
6022	TCP	Used for applying recording schedules.
6027	TCP	Used for writing video data.
6112	TCP	Used for uploading data via HTTPS.
6111	TCP	Redirection port for uploading data via HTTPS.
6041	TCP	Used for uploading data via HTTP.
6011	TCP	Redirection port for uploading data via HTTP.
6114	TCP	Used for downloading data via HTTPS.
6113	TCP	Redirection port for downloading data via HTTPS.
6040	TCP	Used for downloading data via HTTP.
6120	TCP	Redirection port for downloading data via HTTP.
6045	TCP	Used for transmitting object data.
6037	TCP	Used for transmitting video data.
6036	TCP	Used for transmitting video data.
6060	TCP	Used for transmitting web data.
6098	TCP	Used for receiving media data from Stream Media Server.
6042	TCP	Used for forwarding storage data.
6038	TCP	Used for forwarding storage data.
6044	TCP	Used for forwarding storage data.
6039	TCP	Used for forwarding storage data.
6046	TCP	Used for transmitting RESTful data of object storage.
6201	TCP	Communication port for object storage.
6021	TCP	Used for login.

2 Access Solar Camera

2.1 Configure Device

After activating the device and configuring the network, you can log in to the device via the web browser and click **Network**->**Advanced Setting**->**Platform Access** to enter the Platform Access page. You need to enter the IP address and port No. for platform registration and record the device ID, ISUP Key, and other information.

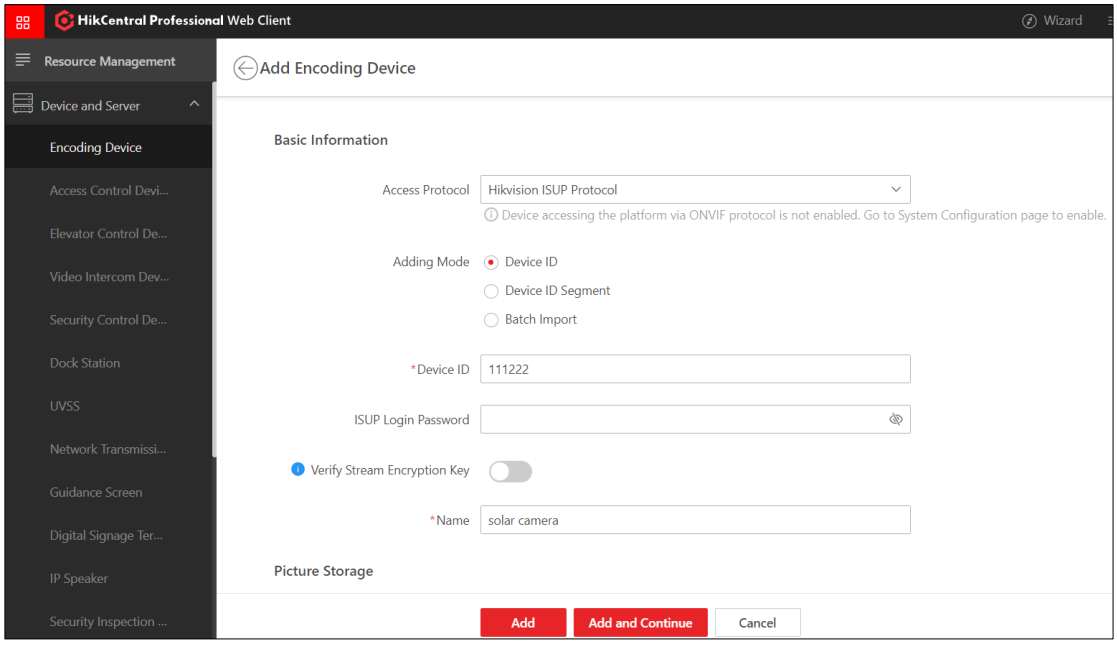


Note:

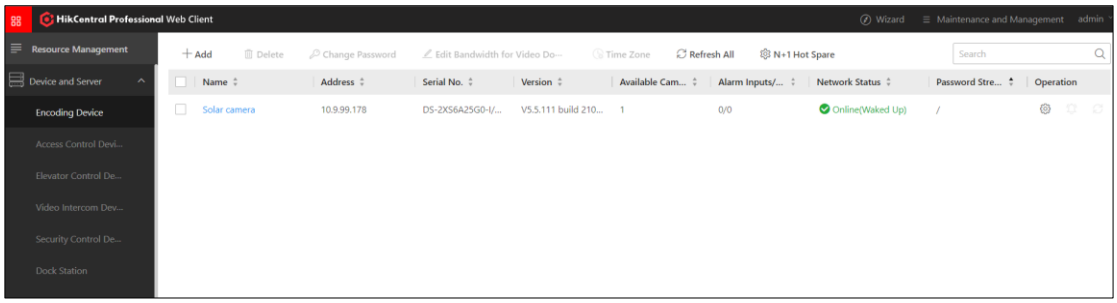
- Server Address refers to the IP address of HikCentral Professional on the WAN.
- Device ID refers to the user-defined name for the device.

2.2 Add Device

Log in to the Web Client of HikCentral Professional, click **Resource Management**->**Device and Server**->**Encoding Device** to enter the Encoding Device page. Click + to enter the Add Encoding Device page, select **Hikvision ISUP Protocol** as the access protocol, enter the device ID, name, and other information, and click **Add** to add a device.



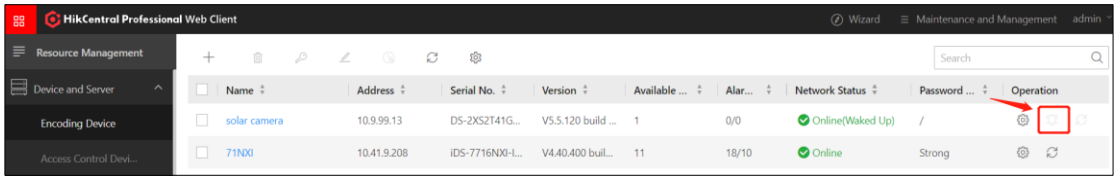
After the device is added, the network status of the device will be "Online" after a while.



2.3 Wake Up Device

When the device power is lower than the configured threshold, the device will be in sleep mode. You can wake up an asleep device on HikCentral Professional.

2.3.1 Wake Up Device on the Page of Adding Devices

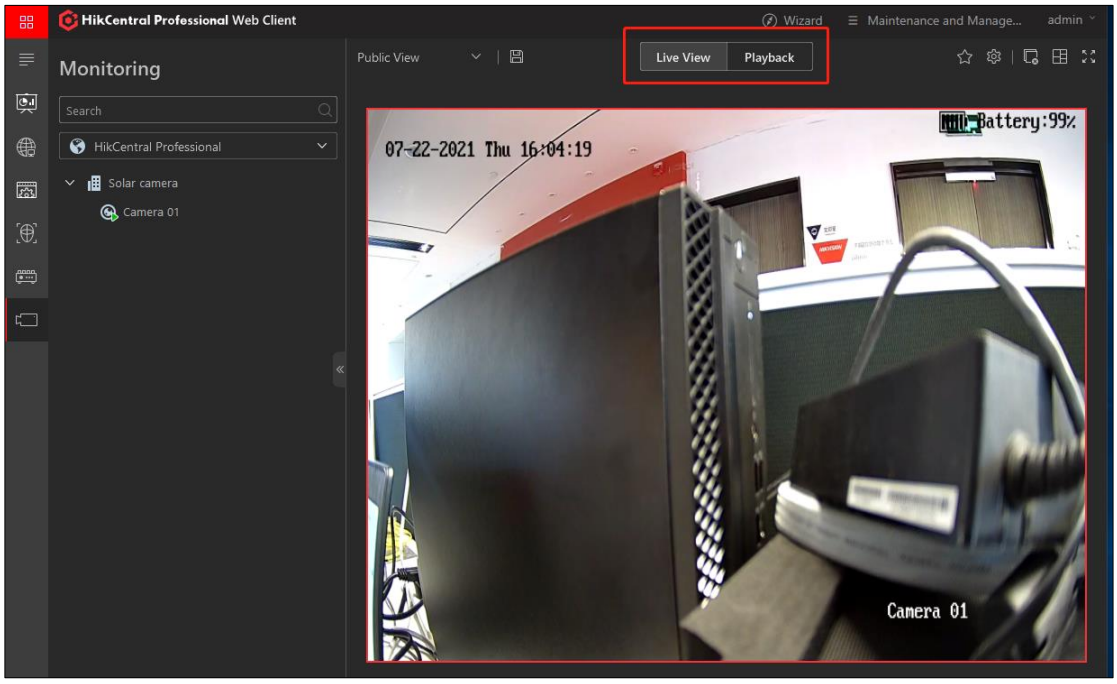


2.3.2 Wake Up Device During Live View

Click the channel of the solar camera on the Client, the Client will prompt that the device is in sleep mode and you need to wake it up.

2.4 Start Live View and Playback

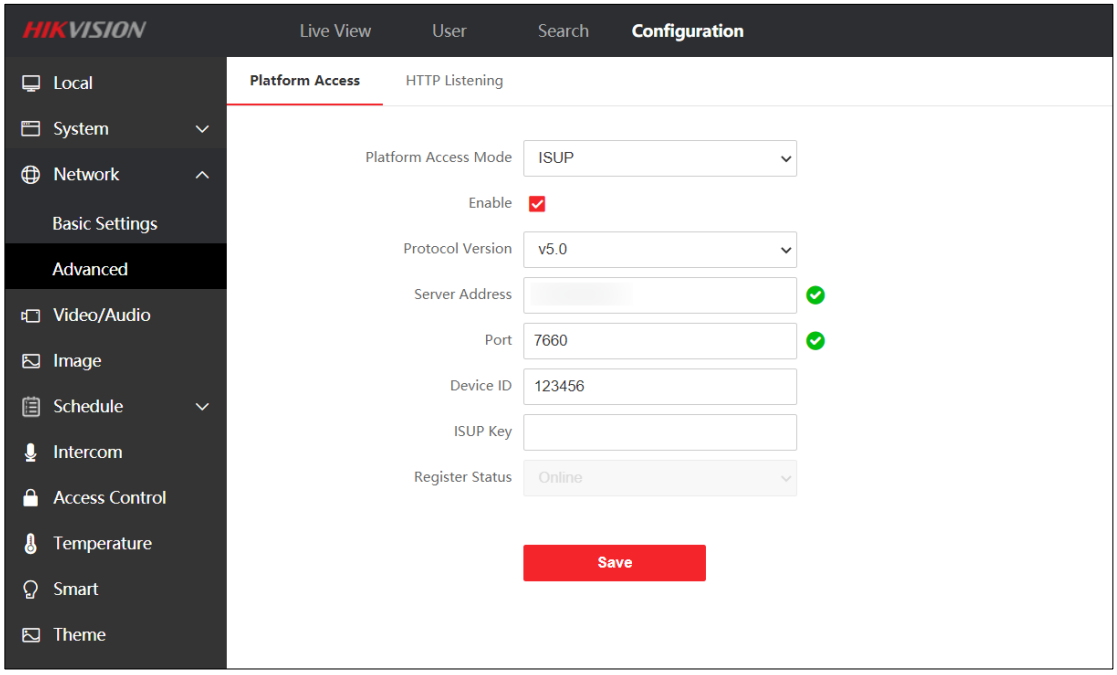
Log in to the Control Client, enter the Monitoring module, and double-click the channel of the solar camera to start live view or playback.



3 Access MinMoe Series Facial Recognition Terminal

3.1 Configure Device

1. Log in to the device via web browser.
2. Click **Network**->**Advanced**->**Platform Access** to enter the Platform Access page.
3. Enter the public IP address of the platform and the port No. for registration
4. Record the device ID, ISUP Key, and other information.

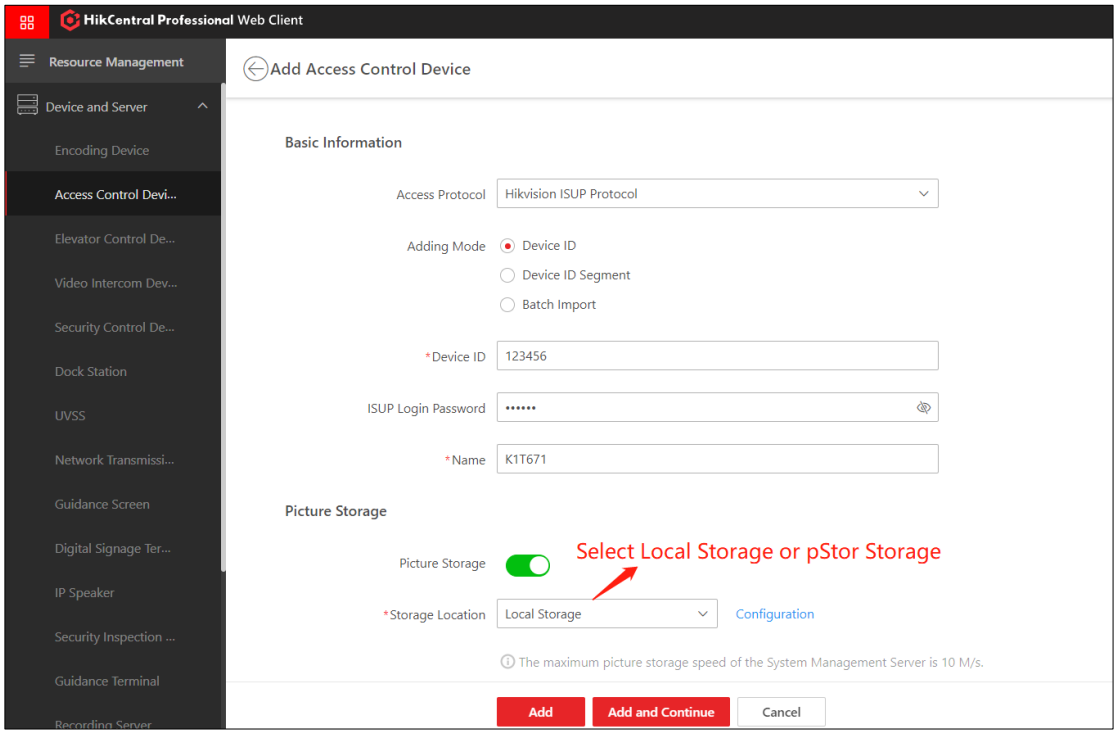


Note:

- Server Address refers to the IP address of HikCentral Professional on the WAN.
- Device ID refers to the user-defined name for the device.

3.2 Add Device

Log in to the Web Client of HikCentral Professional, click **Device and Server**->**Access Control Device**, click **Add**, and enter the device ID, ISUP Login Password (ISUP Key of the device), etc.

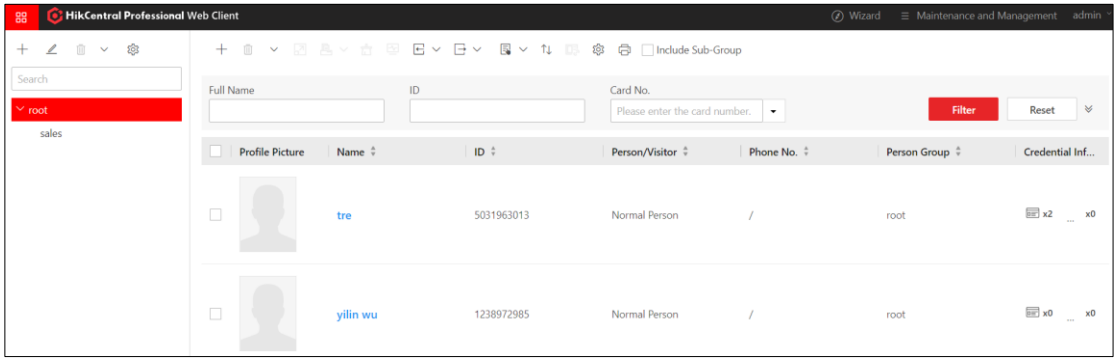


Note:

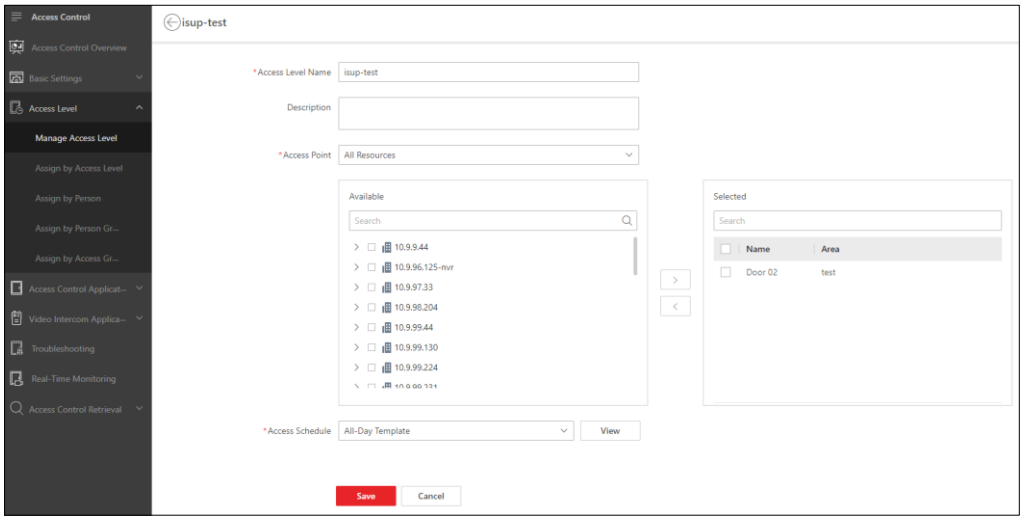
- For HikCentral Professional with version 2.0 and below, ISUP devices only support saving pictures in pStor, so the pStor storage must be configured, the authorization of saving pictures should be enabled for pStor, and the port configured in *(Optional) pStor Network* needs to be mapped to the public network.
- For HikCentral Professional with version 2.1 and above, ISUP devices also support saving pictures on the local storage, so configuring pStor is optional.

3.3 Apply Person Permission

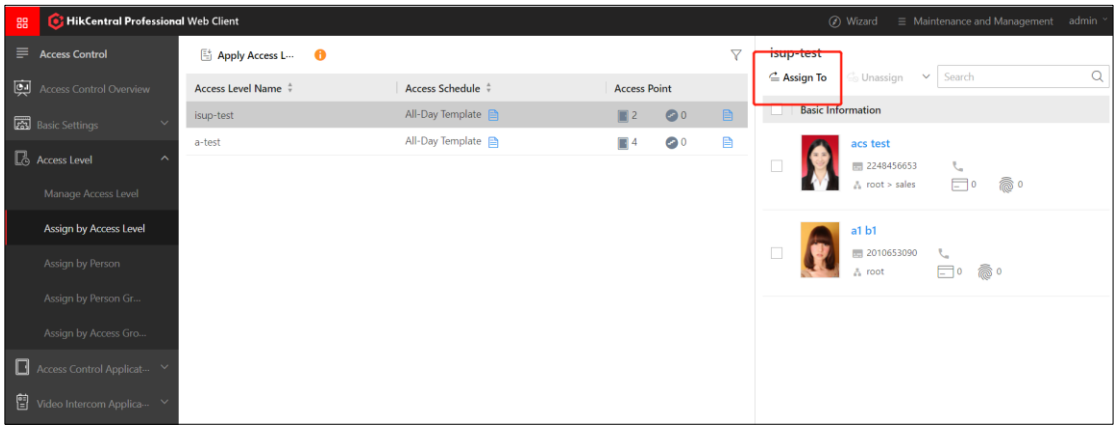
1) Log in to the Web Client of HikCentral Professional, click **General**->**Person**, click **Add**, enter the person information, and click **Add** to save the added person information.



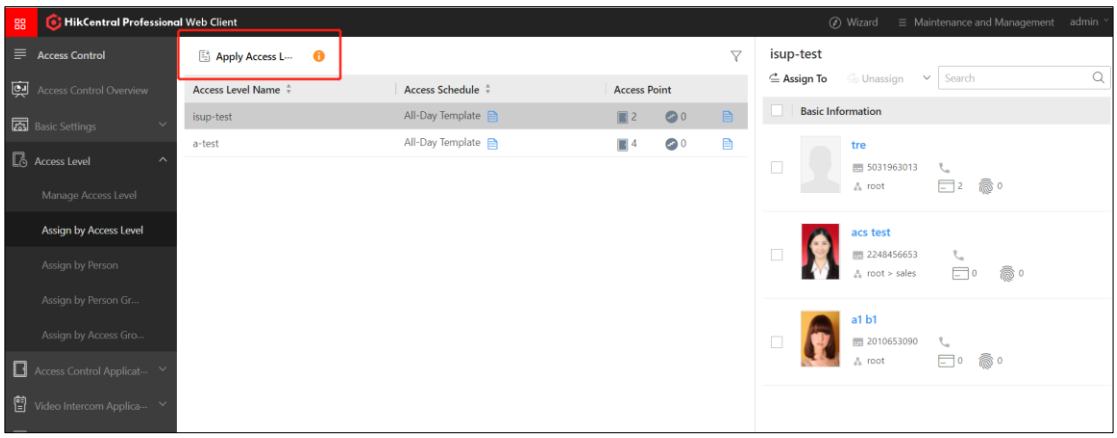
2) Click **Access Control**->**Access Level** and select access point(s) to add them to the access level.

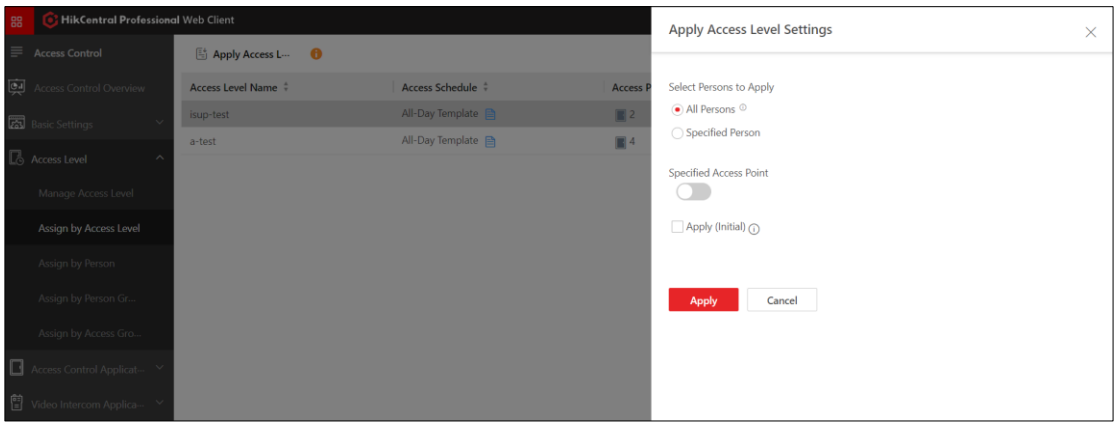


3) Select a method to assign the access level to the person(s).



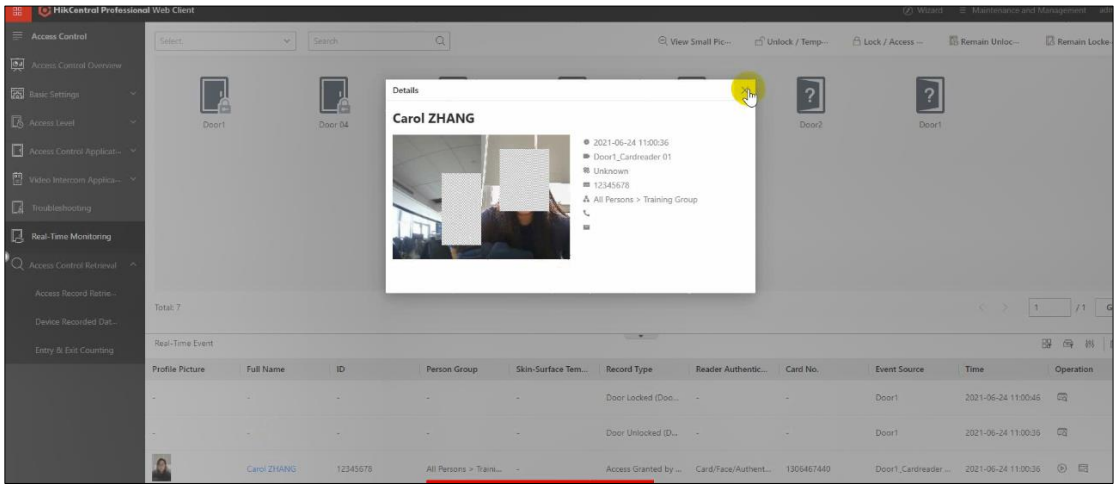
4) Click **Apply Access Level Settings** to apply the access level.



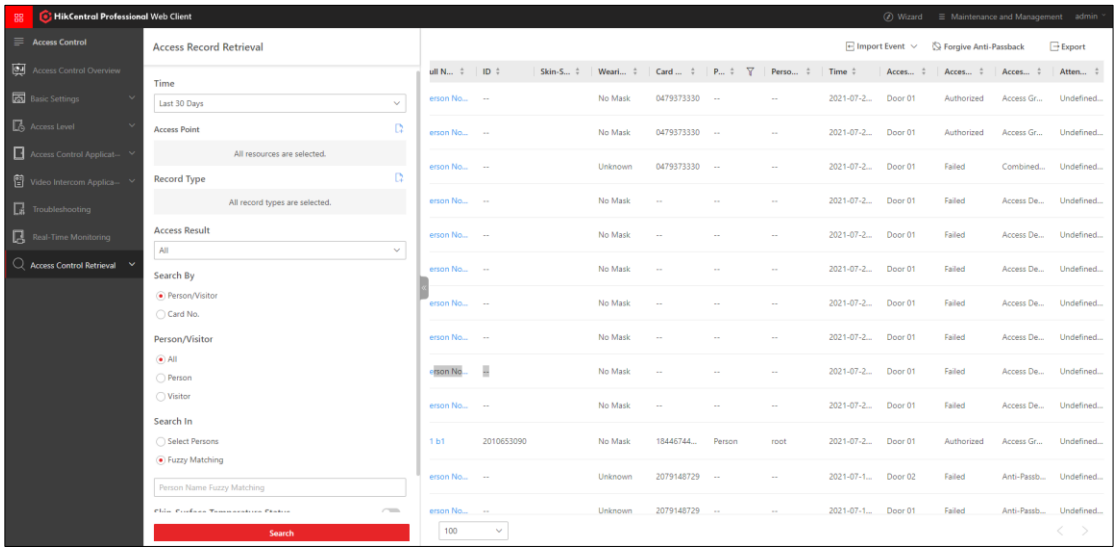


3.4 Functions and Applications

1) Enter the Real-Time Monitoring page on the Web Client to view the access point status and real-time access control events.



2) Enter the Access Control Retrieval page on the Web Client to search the historical event records of access control.

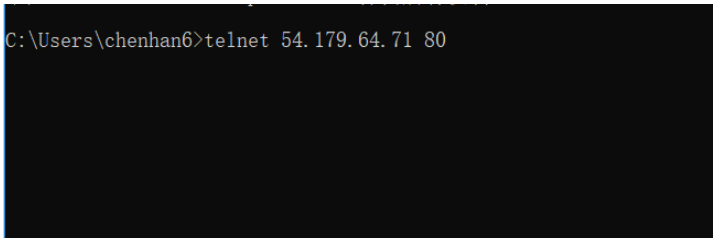


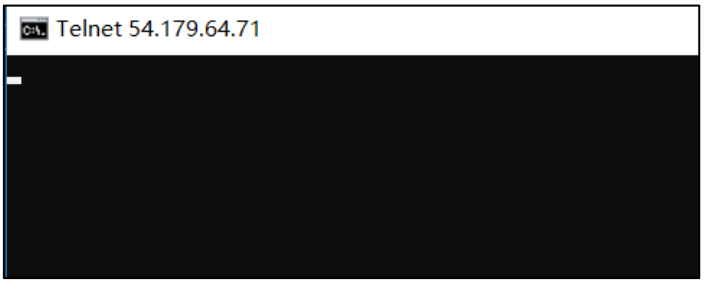
4 FAQ

4.1 How to check whether the needed ports are open?

For TCP and HTTP ports, you can test using the command `telnet+public IP address+port No.` in CMD.

As shown in the figure below, the result indicates that the port is open.





For UDP ports, you can test using the port testing tool Socket Tool.

4.2 Why applying face pictures to access control devices failed?

1) Version 2.0 and Earlier
   a. Check whether the pStor storage is configured.
   b. Check whether the port configured in *1.4 (Optional) pStor Network* for saving pictures in pStor has been mapped to the public network.
   c. Check whether the authorization for saving pictures in pStor is enabled.
2) Version 2.1
   a. If the pStor storage is configured, the troubleshooting steps are the same as those in 1).
   b. If the local picture storage is configured, you need to check whether the following port of the HikCentral Professional server is open.

6123	HTTP	Used for picture storage of ISUP devices.

4.3 Why the platform cannot receive events uploaded by access control devices or get the door status?

Check whether the following ports of the HikCentral Professional server are open.

7332	TCP	Used for receiving alarms from ISUP devices.
7334	UDP	Used for receiving alarms from ISUP devices.

4.4 Why starting live view or playback of cameras failed?

Check whether the following ports of the HikCentral Professional server are open.

7661	TCP	Used for getting the stream from ISUP devices via Streaming Server.
554	RTSP	Used for getting the stream for live view (real-time streaming port).
559	WebSocket	Used for getting the stream for Google Chrome, Firefox, or Safari.
10000	TCP	Used for getting the stream for playback (video file streaming port).
16000	TCP	Used for getting the stream from ISUP devices via the plugin.

Appendix Feature List

Appendix A. Feature List of Cameras Supporting ISUP 5.0

Module	Sub-Module	Features	ISUP 5.0
Video	Device Management	Adding devices	√
		Domain name (platform) registration	√
		Remote configuration via web browser (the network is disconnected between the Control Client and the device)	√
		Firmware upgrading	√
		Getting capability sets of various cameras	√
		Encoding device online/offline	√
		Network camera online/offline	√
		Video loss	√
		Channel communication exception.	√
		Channel recording exception	√
		Device log search	√
		ANR (Automatic Network Replenishment)	Only supports copying back data from network cameras to NVRs, but to the central storage is not supported.
		VQD (Video Quality Diagnosis)	×
		Resource tree thumbnail	×
		Getting configured PTZ presets of devices	×
	Recording	Recording schedule of main stream/sub-stream	√
		Video copy-back schedule	√ (Only supported by pStor and CVR)
		Event-based recording schedule	√ (Not supported by center storage)
		Command-based recording schedule	√ (Not supported by center storage)
		Recording schedule of local dual-stream	√
		Manual recording (manual/event linkage)	√
	Live View	Live view of main stream/sub-steam	√
		Live view of channel-zero	√
		Switching stream (main stream, sub-stream, etc.)	√
		Audio control	√
		Capture	√
		Stream encryption	√

		Two-way audio	√
		Alarm output control	√
		Displaying live view on video wall	√
		Digital zoom	√
		Fisheye expansion	√
		PTZ control (direction and rotation)	√
		Wiper control/batch wiper control	√
		3D positioning	×
		Getting presets	×
		Smooth stream	×
		POS live view	×
		ATM live view	×
	Basic Playback	Main stream playback	√
		Sub-stream playback	√
		Switching stream (main stream, sub-stream, etc.)	√
		Audio control	√
		Capture	√
		Video clipping/downloading	√
		Tagging video	√
		Digital zoom	√
		Fisheye expansion	√
		Playback in DST mode	√
		Pausing and resuming recording	√
		Channel-zero	√
		Displaying playback on video wall	√
		Encrypted stream playback	√
		Video locking	×
		Smooth stream playback	×
		Transcoding playback	×
		Thumbnail playback	×
		Frame-extracting playback	×
	Search and Exporting	VCA search	√
		Tag search	√
		Exporting videos	√
		POS search	×
		ATM search	×
		NVR bandwidth limit of downloading videos	×
	Solar Camera	Adding device	√
		Remote configuration via web browser	√
		Wake up	√
		Live view	√

		Playback	√
		Two-way audio	√
		Alarm output control	√
Intelligent Application	Face Picture Management	Face picture group/list management and applying	√
	Live View	Viewing captured face pictures in real time	√
		Face attribute	√
		Human body attribute	√
		Viewing face pictures by group	√
	DeepinMind Series NVR	Searching by picture	√
		Search	√
	Face Attribute	Age group	√
		Gender	√
		Wear glasses	√
		Wear a mask	√
		Wear glasses	√
		Wear a mask	√
		Gender	√
	Human Body Attribute	Top color	√
		With backpack or not	√
		Riding	√
	Person Search	Searching in face picture group	√
		Person information search (ID/name)	√
		Searching by picture	√
		Searching captured picture	√
		Face attribute report-age group	√
		Face attribute report-gender	√
	Queue Management Camera	Queue-report of waiting time in queue	√
		Queue-report of person waiting time	√
	Fisheye	Heat map	×
		Path analysis	×
	Alarm	Face detection	√
		Face capture	√
		Frequently appeared person	√
Vehicle	List Management	Vehicle list management	√
	Passing Vehicle Event	License plate number	√
		Captured vehicle picture	√
		Passing vehicle event details	√
	License Plate	License plate number	√
		Country/Region	√

		Vehicle owner	√
		Vehicle model	√
		List	√
		Custom information	√
	Vehicle Attribute	Brand	√
		Color	√
		Driving direction	√
	Report	Passing vehicle report	√
People Counting	Real-Time People Counting	Real-time people counting OSD (enter/exit)	√
		Customer traffic limit	√
		People counting deduplication OSD	√
		People amount correction	√
		Regularly clearing all	√
	Alarm	Real-time people counting overload pre-alarm	√
		Real-time people counting overload alarm	√
	Historical People Counting Deduplication	ANR of people counting data	√
		People counting deduplication	√
		Historical people counting (enter/exit)	√
Alarm	Basic Features	Alarm linked live view/playback	√
		Uploading alarms with pictures	√
		Event/Alarm linked capture	√
	Exception Alarm	HDD full	√
		HDD error	√
		Illegal access	√
		Hot spare monitoring station exception	√
		Recording exception	√
		Logical disk exception in array	√
		No video signal	√
		Video quality exception	√
		High temperature exception detected by SHM	√
		Low temperature exception detected by SHM	√
		HDD shock exception detected by SHM	√
		Bad sector exception detected by SHM	√
		Severe failure exception detected by SHM	√
	Normal Alarm	IO alarm	√
		Motion detection	√

		Video loss	√
		Video tampering alarm	√
		Face detection	√
		Face capture	√
		Defocus detection	√
		Audio input exception	√
		Scene change detection	√
		pir alarm	√
		People counting alarm	√
		Heat map alarm	√
		Vehicle detection/license plate detection	√
		Vehicle blocklist detection	√
		Vehicle allowlist detection	√
	Behavior Analysis Alarm	Intrusion	√
		Line crossing detection	√
		Region entrance	√
		Region exiting	√
		Loitering detection	√
		People gathering	√
		Fast moving	√
		Parking detection	√
		Unattended baggage	√
		Object removal	√
	Thermal Alarm	Temperature measurement	√
		Temperature measurement pre-alarm	√
		Fire source detection	√
		Ship detection	√
	New Service Alarm	Face picture comparison	√
		Face picture comparison failed	√
		People density over threshold	√
		Frequently appeared person detection	√
		Hard hat detection	√
		Queuing-up time over threshold	√
		Queue length over threshold	√
		Human body detection	√

Module	Sub-Module	Features	ISUP 5.0
Video	Device Management	Adding devices	√
		Domain name (platform) registration	√
		Remote configuration via web browser (the network is disconnected between the Control Client and the device)	√
		Firmware upgrading	√
		Getting capability sets of various cameras	√
		Encoding device online/offline	√
		Network camera online/offline	√
		Video loss	√
		Channel communication exception.	√
		Channel recording exception	√
		Device log search	√
		ANR (Automatic Network Replenishment)	Only supported by people counting cameras and NVRs and not supported by ANPR cameras
		VQD (Video Quality Diagnosis)	×
		Resource tree thumbnail	×
		Getting configured PTZ presets of devices	×
	Recording	Recording schedule of main stream/sub-stream	√
		Video copy-back schedule	√ (Only supported by pStor and CVR)
		Event-based recording schedule	√ (Not supported by center storage)
		Command-based recording schedule	√ (Not supported by center storage)
		Recording schedule of local dual-stream	√
		Manual recording (manual/event linkage)	√
	Live View	Live view of main stream/sub-steam	√
		Live view of channel-zero	√
		Switching stream (main stream, sub-stream, etc.)	√
		Audio control	√
		Capture	√
		Stream encryption	√

		Two-way audio	√
		Alarm output control	√
		Displaying live view on video wall	√
		Digital zoom	√
		Fisheye expansion	√
		PTZ control (direction and rotation)	√
		Wiper control/batch wiper control	√
		3D positioning	×
		Getting presets	×
		Smooth stream	×
		POS live view	×
		ATM live view	×
	Basic Playback	Main stream playback	√
		Sub-stream playback	√
		Switching stream (main stream, sub-stream, etc.)	√
		Audio control	√
		Capture	√
		Video clipping/downloading	√
		Tagging video	√
		Digital zoom	√
		Fisheye expansion	√
		Playback in DST mode	√
		Pausing and resuming recording	√
		Channel-zero	√
		Displaying playback on video wall	√
		Encrypted stream playback	√
		Video locking	×
		Smooth stream playback	×
		Transcoding playback	×
		Thumbnail playback	×
		Frame-extracting playback	×
	Search and Exporting	VCA search	√
		Tag search	√
		Exporting videos	√
		POS search	×
		ATM search	×
		NVR bandwidth limit of downloading videos	×
	Solar Camera	Adding device	√
		Remote configuration via web browser	√
		Wake up	√
		Live view	√

		Playback	√
		Two-way audio	√
		Alarm output control	√
Intelligent Application	Face Picture Management	Face picture group/list management and applying	√
	Live View	Viewing captured face pictures in real time	√
		Face attribute	√
		Human body attribute	√
		Viewing face pictures by group	√
	DeepinMind Series NVR	Searching by picture	√
		Search	√
	Face Attribute	Age group	√
		Gender	√
		Wear glasses	√
		Wear a mask	√
		Wear glasses	√
		Wear a mask	√
		Gender	√
	Human Body Attribute	Top color	√
		With backpack or not	√
		Riding	√
	Person Search	Searching in face picture group	√
		Person information search (ID/name)	√
		Searching by picture	√
		Searching captured picture	√
		Face attribute report-age group	√
		Face attribute report-gender	√
	Queue Management Camera	Queue-report of waiting time in queue	√
		Queue-report of person waiting time	√
	Fisheye	Heat map	×
		Path analysis	×
	Alarm	Face detection	√
		Face capture	√
		Frequently appeared person	√
Vehicle	List Management	Vehicle list management	√
	Passing Vehicle Event	License plate number	√
		Captured vehicle picture	√
		Passing vehicle event details	√
	License Plate	License plate number	√
		Country/Region	√

		Vehicle owner	√
		Vehicle model	√
		List	√
		Custom information	√
	Vehicle Attribute	Brand	√
		Color	√
		Driving direction	√
	Report	Passing vehicle report	√
People Counting	Real-Time People Counting	Real-time people counting OSD (enter/exit)	√
		Customer traffic limit	√
		People counting deduplication OSD	√
		People amount correction	√
		Regularly clearing all	√
	Alarm	Real-time people counting overload pre-alarm	√
		Real-time people counting overload alarm	√
	Historical People Counting Deduplication	ANR of people counting data	√
		People counting deduplication	√
		Historical people counting (enter/exit)	√
Alarm	Basic Features	Alarm linked live view/playback	√
		Uploading alarms with pictures	√
		Event/Alarm linked capture	√
	Exception Alarm	HDD full	√
		HDD error	√
		Illegal access	√
		Hot spare monitoring station exception	√
		Recording exception	√
		Logical disk exception in array	√
		No video signal	√
		Video quality exception	√
		High temperature exception detected by SHM	√
		Low temperature exception detected by SHM	√
		HDD shock exception detected by SHM	√
		Bad sector exception detected by SHM	√
		Severe failure exception detected by SHM	√
	Normal Alarm	IO alarm	√
		Motion detection	√

		Video loss	√
		Video tampering alarm	√
		Face detection	√
		Face capture	√
		Defocus detection	√
		Audio input exception	√
		Scene change detection	√
		pir alarm	√
		People counting alarm	√
		Heat map alarm	√
		Vehicle detection/license plate detection	√
		Vehicle blocklist detection	√
		Vehicle allowlist detection	√
	Behavior Analysis Alarm	Intrusion	√
		Line crossing detection	√
		Region entrance	√
		Region exiting	√
		Loitering detection	√
		People gathering	√
		Fast moving	√
		Parking detection	√
		Unattended baggage	√
		Object removal	√
	Thermal Alarm	Temperature measurement	√
		Temperature measurement pre-alarm	√
		Fire source detection	√
		Ship detection	√
	New Service Alarm	Face picture comparison	√
		Face picture comparison failed	√
		People density over threshold	√
		Frequently appeared person detection	√
		Hard hat detection	√
		Queuing-up time over threshold	√
		Queue length over threshold	√
		Human body detection	√

Appendix B. Feature List of Access Control Devices Supporting ISUP 5.0

	Module	Sub-Module	V2.1
Access Control	Device Access	Access Control Devices	√ Camera channels of MinMoe series facial recognition terminals are not imported.
		Elevator Control Devices	×
		Video Intercom Devices	×
	Permission Management	Permission Applying (Person, Card, Fingerprint, and Face Pictures)	Applying face pictures depends on pStor.
		Collecting Card No. by Remote Devices	√
		Collecting Fingerprints by Remote Devices	√
		Collecting Face Pictures By Remote Devices	√
		Getting Persons from Remote Devices	√
		Getting Fingerprints from Remote Devices	√
		Getting Face Pictures from Remote Devices	√
		Getting the Device's All Parameters (Specifications of the Device)	√
		Remote Door Control	√
	Access Control Applications	Permission Schedule Template Configuration	√
		Door Schedule Configuration (Remain Open/Closed)	√
		Reader Authentication Mode Configuration	√
		Area Anti-Passback Configuration (Single Device and Across Devices)	√
		Route Anti-Passback Configuration (Single Device and Across Devices)	×

		Multi-Door Interlocking Configuration (Single Device)	√
		Multi-Factor Authentication (Single Device)	√
		First Person In Rule (Single Device)	√
		Authentication Code (Old Solution)	×
		Authentication via PIN Code (New Solution)	×
	Parameter Configuration	Alarm Output Control	√
		Zone Arming And Disarming	√
		Getting and Setting Door Parameters: Door Name, Door Open Duration, Password Settings, etc.	√
		Getting and Setting Reader Parameters: Tampering, Failed Attempts Alarm, Fingerprint Sensitivity, Face Parameter Configuration, etc.	√
		Getting and Setting Device Time Parameters: NTP Time Synchronization and DST (Daylight Saving Time).	√
		Getting and Setting Capture Parameters	√
		Getting and Setting Parameters of M1 Card Encryption Verification	√
		Getting and Setting Custom Wiegand Parameters	√
		Getting and Setting NFC Parameters	√
		Getting and Setting Card Swiping Parameters	√
	Access Control Events	Getting Lost Events (Automatically by Schedule and Manually)	√
		Device Log Search	√
		Receiving Real-Time Events from Devices	√
		ANR of Device Offline Events	√
		Receiving Events with Pictures	√

		Event Card Linkage (Single Device)	√
		Event, Card No., and Employee No. Linkage (Cross-Device Supported)	√
		Getting Access Control Events from Remote Devices	×
	Other	Getting Status	√
		Getting Capability Set	√
		Two-Way Audio	×


See Far, Go Further