



Video Intercom and Access Control NVR Integration

Quick Start Guide (QSG)

TABLE OF CONTENTS

Chapter 1 Adding Devices	6
1.1 Adding Video Intercom Products.....	6
1.2 Adding Access Control Products.....	8
1.3 Recording Settings.....	9
1.4 Linkage Actions	10
1.5 Live View	11
1.6 Playback	13
1.7 File Management	17
1.8 Logs	17
Chapter 2 Accessing by Web Browser	19

Video Intercom and Access Control NVR Integration Quick Start Guide

COPYRIGHT ©2016-2017 Hangzhou Hikvision Digital Technology Co., Ltd.

ALL RIGHTS RESERVED.

Any and all information, including, among others, wording, pictures, and graphs are the properties of Hangzhou Hikvision Digital Technology Co., Ltd., or its subsidiaries (hereinafter referred to as “Hikvision”). This user manual (hereinafter referred to as “the Manual”) cannot be reproduced, changed, translated, or distributed, partially or wholly, by any means, without the prior written permission of Hikvision. Unless otherwise stipulated, Hikvision does not make any warranties, guarantees or representations, express or implied, regarding to the Manual.

About this Manual

This Manual is applicable to Network Video Recorder (NVR).

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. Find the latest version on the company website (<http://overseas.hikvision.com/en/>).

Please use this user manual under the guidance of professionals.

Trademarks Acknowledgement

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

Legal Disclaimer

TO THE MAXIMUM EXTENT PERMITTED BY APPLICABLE LAW, THE PRODUCT DESCRIBED, WITH ITS HARDWARE, SOFTWARE AND FIRMWARE, IS PROVIDED “AS IS,” WITH ALL FAULTS AND ERRORS, AND HIKVISION MAKES NO WARRANTIES, EXPRESS OR IMPLIED, INCLUDING WITHOUT LIMITATION, MERCHANTABILITY, SATISFACTORY QUALITY, FITNESS FOR A PARTICULAR PURPOSE, AND NON-INFRINGEMENT OF THIRD PARTY. IN NO EVENT WILL HIKVISION, ITS DIRECTORS, OFFICERS, EMPLOYEES, OR AGENTS 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 OR DOCUMENTATION, IN CONNECTION WITH THE USE OF THIS PRODUCT, EVEN IF HIKVISION HAS BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES. REGARDING TO THE PRODUCT WITH INTERNET ACCESS, THE USE OF PRODUCT SHALL BE WHOLLY AT YOUR OWN RISKS. HIKVISION SHALL NOT TAKE ANY RESPONSIBILITIES FOR ABNORMAL OPERATION, PRIVACY LEAKAGE OR OTHER DAMAGES RESULTING FROM CYBER ATTACK, HACKER ATTACK, VIRUS INSPECTION, OR OTHER INTERNET SECURITY RISKS; HOWEVER, HIKVISION WILL PROVIDE TIMELY TECHNICAL SUPPORT IF REQUIRED.

SURVEILLANCE LAWS VARY BY JURISDICTION. PLEASE CHECK ALL RELEVANT LAWS IN YOUR JURISDICTION BEFORE USING THIS PRODUCT IN ORDER TO ENSURE THAT YOUR USE CONFORMS THE APPLICABLE LAW. HIKVISION SHALL NOT BE LIABLE IN THE EVENT THAT THIS PRODUCT IS USED WITH ILLEGITIMATE PURPOSES.

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

Regulatory Information

FCC Information

Please take attention that changes or modification not expressly approved by the party responsible for compliance could void the user's authority to operate the equipment.


FCC Compliance: This equipment has been tested and found to comply with the limits for a Class A digital device, pursuant to part 15 of the FCC Rules. These limits are designed to provide reasonable protection against harmful interference when the equipment is operated in a commercial environment. This equipment generates, uses, and can radiate radio frequency energy and, if not installed and used in accordance with the instruction manual, may cause harmful interference to radio communications. Operation of this equipment in a residential area is likely to cause harmful interference in which case the user will be required to correct the interference at his own expense.


FCC Conditions


This device complies with part 15 of the FCC Rules. Operation is subject to the following two conditions:

1. This device may not cause harmful interference.
2. This device must accept any interference received, including interference that may cause undesired operation.

EU Conformity Statement

 This product and, if applicable, the supplied accessories too are marked with "CE" and comply therefore with the applicable harmonized European standards listed under the EMC Directive 2014/30/EU, the LVD Directive 2014/35/EU, the RoHS Directive 2011/65/EU.

 2012/19/EU (WEEE directive): Products marked with this symbol cannot be disposed of as unsorted municipal waste in the European Union. For proper recycling, return this product to your local supplier upon the purchase of equivalent new equipment, or dispose of it at designated collection points. For more information see: www.recyclethis.info.

 2006/66/EC (battery directive): This product contains a battery that cannot be disposed of as unsorted municipal waste in the European Union. See the product documentation for specific battery information. The battery is marked with this symbol, which may include lettering to indicate cadmium (Cd), lead (Pb), or mercury (Hg). For proper recycling, return the battery to your supplier or to a designated collection point. For more information see: www.recyclethis.info.

Industry Canada ICES-003 Compliance

This device meets the CAN ICES-3 (A)/NMB-3(A) standards requirements.




Applicable Models

NVRs support the video intercom and access control products shown below:

Product	Model	FW
Video Intercom	DS-KD8002-VM	V1.4.70_170510
	DS-KV8x02-IM	V1.4.70_170510
	DS-KB8112-IM	V1.4.6_170522
	DS-KB6003-WIP	V1.4.6_170510
	DS-KH8300-T	V1.4.6_170321
	DS-KH8301-WT	
Access Control	DS-K260X	V2.0.0_170531
	DS-K1T200	V2.0.0_170601
	DS-K1T105	
	DS-K1T500	V1.1.0_build170601
	DS-K1T803	TBD

Symbol Conventions

The symbols that may be found in this document are defined as follows.

Symbol	Description
 NOTE	Provides additional information to emphasize or supplement important points of the main text.
 WARNING	Indicates a potentially hazardous situation, which if not avoided, could result in equipment damage, data loss, performance degradation, or unexpected results.
 DANGER	Indicates a hazard with a high level of risk, which if not avoided, will result in death or serious injury.

Safety Instructions

- Proper configuration of all passwords and other security settings is the responsibility of the installer and/or end-user.
- In the use of the product, you must be in strict compliance with the electrical safety regulations of the nation and region. Please refer to technical specifications for detailed information.
- Input voltage should meet both the SELV (Safety Extra Low Voltage) and the Limited Power Source with 100 to 240 VAC or 12 VDC according to the IEC60950-1 standard. Please refer to technical specifications for detailed information.
- Do not connect several devices to one power adapter as adapter overload may cause over-heating or a fire hazard.
- Please make sure that the plug is firmly connected to the power socket.
- If smoke, odor, or noise rise from the device, turn off the power at once and unplug the power cable, and then contact the service center.

Preventive and Cautionary Tips

Before connecting and operating your device, please be advised of the following tips:

- Ensure unit is installed in a well-ventilated, dust-free environment.
- Unit is designed for indoor use only.
- Keep all liquids away from the device.
- Ensure environmental conditions meet factory specifications.
- Ensure unit is properly secured to a rack or shelf. Major shocks or jolts to the unit as a result of dropping it may cause damage to the sensitive electronics within the unit.
- Use the device in conjunction with a UPS if possible.
- Power down the unit before connecting and disconnecting accessories and peripherals.
- A factory recommended HDD should be used for this device.
- Improper use or replacement of the battery may result in hazard of explosion. Replace with the same or equivalent type only. Dispose of used batteries according to the instructions provided by the battery manufacturer.

Chapter 1 Adding Devices

1.1 Adding Video Intercom Products

Before you start:

Ensure the network connection is valid and correct. Before you add video intercom products to the NVR, first activate the device and set all parameters.

Add video intercom products in the Cameras Setup interface (refer to the following figure for the menu structure):



Figure 1, Add Video Intercom Products

You can select one of the following two options to add video intercom products.

- **OPTION 1**

Select the detected video intercom product(s) and click **Add** to add it directly.

 **NOTE**

Click **Search** to refresh the online device list.

- OPTION 2

Click **Custom Adding** to add video intercom product(s) by editing the parameters in the corresponding text field, and then click **Add** to add it.

 **NOTE**

After adding video intercom product(s) as above, it will appear in the System Configuration interface as a door(s).

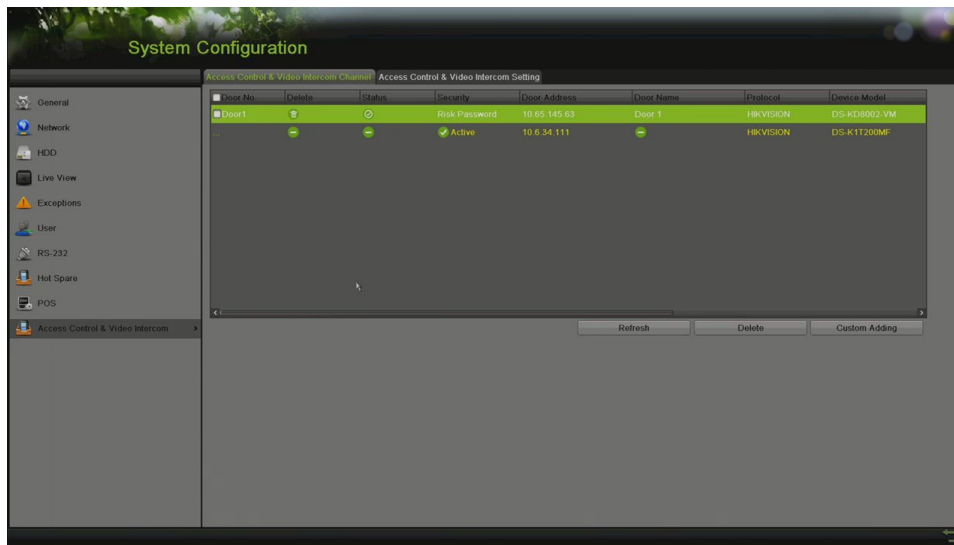


Figure 2, System Configuration

 **NOTE**

Double-click "Door Name" to change it. After changing the name, all related records will display the new name, refer to 1.6.

The maximum number of video intercom and access control products that can be added is half the number of NVR channels.

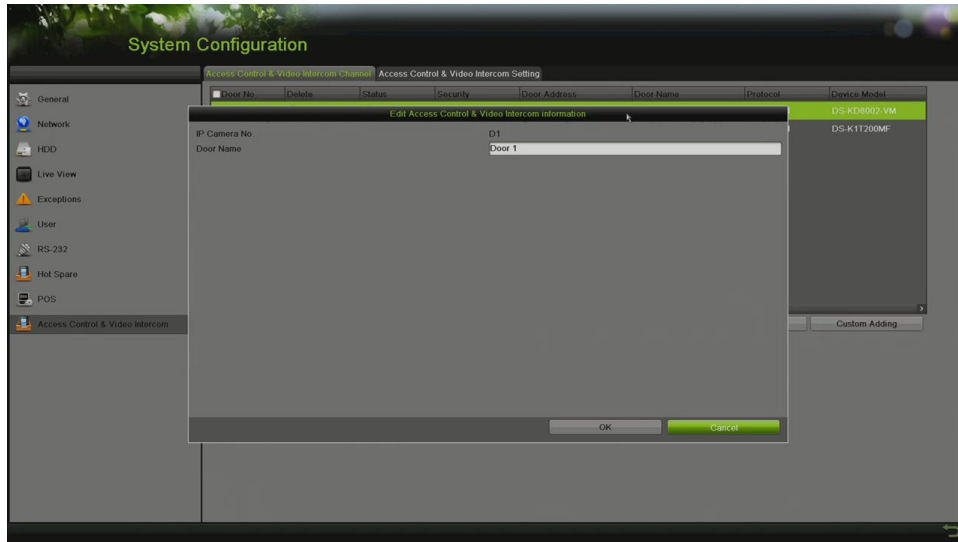


Figure 3, Change Door Name

1.2 Adding Access Control Products

Before you start

Ensure the network connection is valid and correct. Before you add access control products to the NVR, first activate the device and set all parameters.

1. Go to Menu > System Configuration > Access Control and Video Intercom (see figure below).

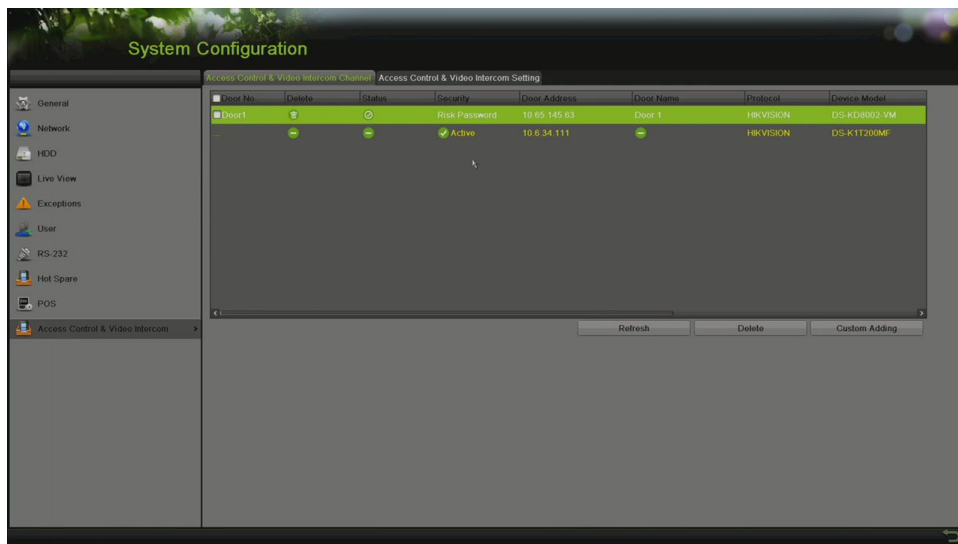


Figure 4, Add Access Control Product

2. Click **Custom Adding** to add access control products by editing the parameters in the corresponding text fields.
3. Click **Add** to add device(s). It will then appear in the System Configuration interface as a door(s).

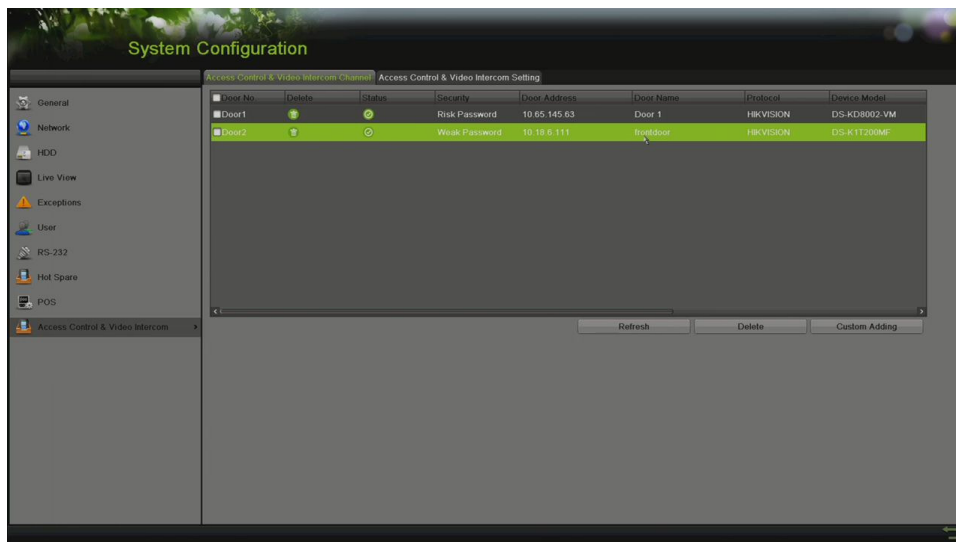


Figure 5, System Configuration

 **NOTE**

Double click “Door Name” to change it. After changing the name, all related records will display the new name, refer to Figure 6.

DS-K1T500 can be added as a video intercom product, refer to Figure 1.

The maximum number of video intercoms and access control products that can be added is half the number of channels.

1.3 Recording Settings

Before you start:

Make sure that a hard drive has been installed. If not, install a hard drive and initialize it.

Now, video products can send event notifications to the NVR if the NVR supports event recording.

To record non-video events, choose the event recording template:



Figure 6, Recording Settings

1.4 Linkage Actions

Before you start:

Make sure that IP cameras have been added to the system; they are required for the NVR to trigger cameras to record.

Set linkage actions in the **Access Control & Video Intercom setting** interface

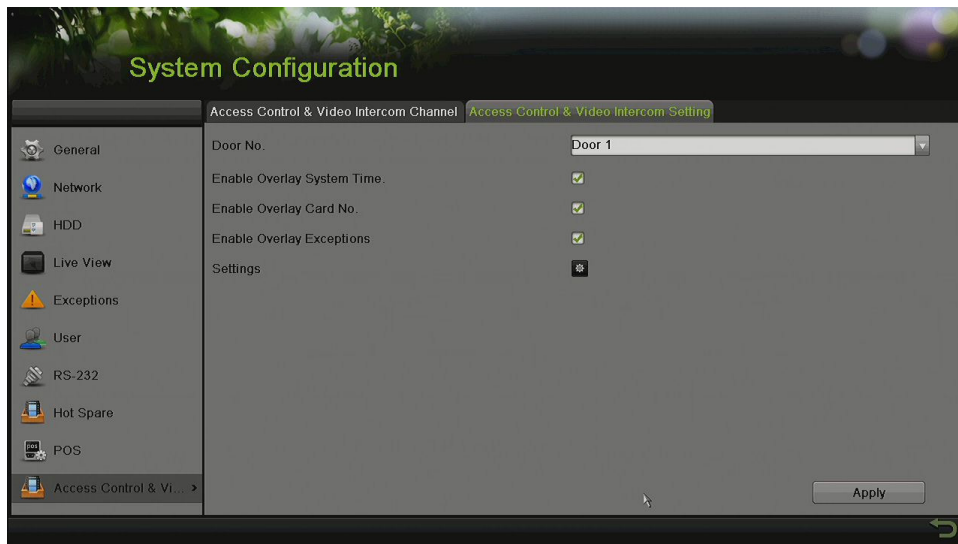


Figure 7, Access Control & Video Intercom Setting

Enable Overlay System Time: NVR can overlay NVR system time in the left corner of the channel during Live View and playback.

Enable Overlay Card No.: NVR can overlay a card no. in the left corner of the channel when in Live View and during playback.

Enable Overlay Exceptions: NVR can overlay an event name in the left corner of the channel when in Live View and during playback.

Choose **Settings** to configure other linkage actions:

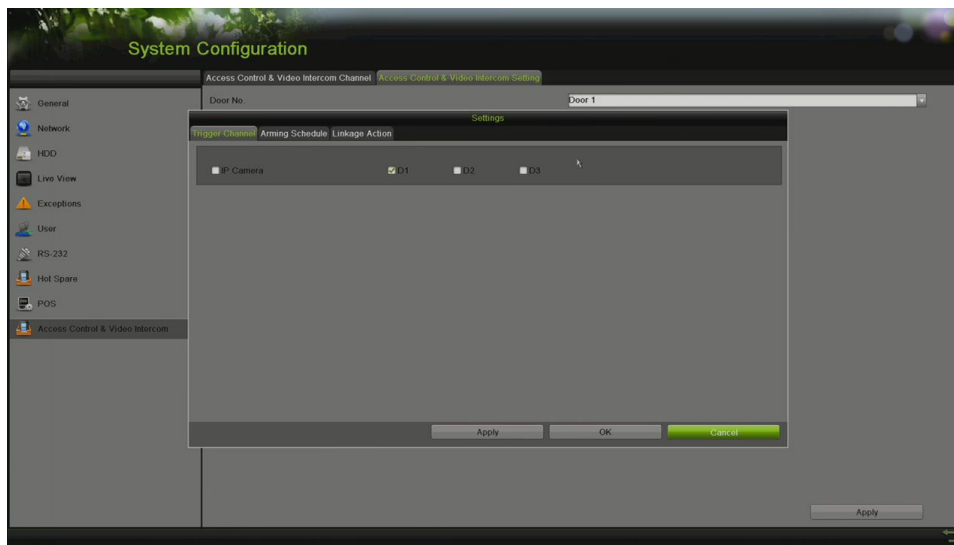


Figure 8, Other Linkage Actions

Trigger Channels: The NVR can trigger channels to record. The maximum number varies by NVR.

Arming Schedule: The NVR can receive notifications according to the arming schedule.

Linkage Actions: The NVR can trigger additional linkage actions such as **Full Screen Monitoring**, **Audible Warning**, **Send Email**, and **Trigger Alarm Output**.

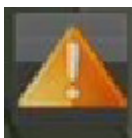
1.5 Live View

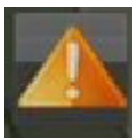
Only video intercom products and the DS-K1T500 support Live View.

If you enable **Enable Overlay Card No.** and **Enable Overlay Exceptions**, once an event happens, the NVR will overlay the info on the left corner of the channel's screen.



Figure 9, Live View



Click  to check the exception.

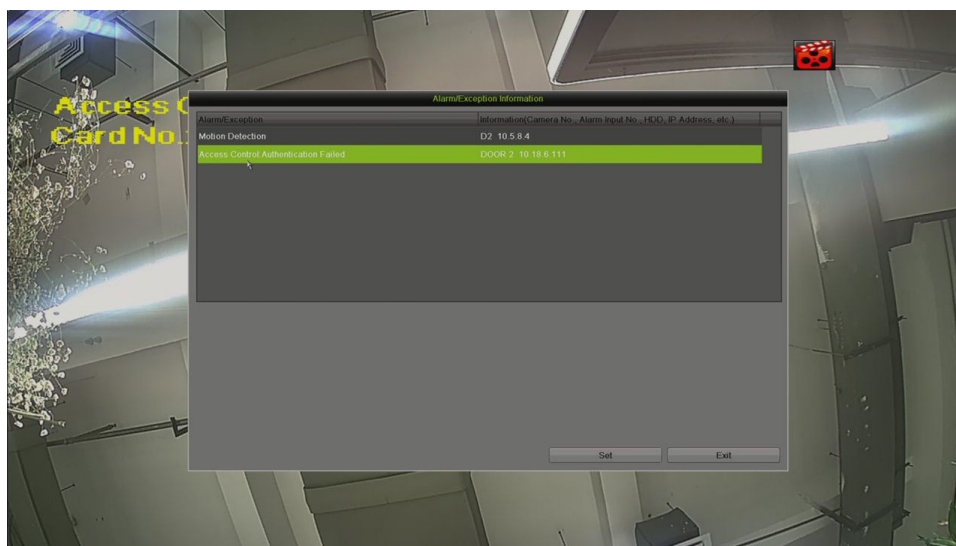


Figure 10, Exception

 **NOTE**

If Enable Overlay System Time is set, the NVR will overlay the NVR system time in the left corner of the channel if an event happens.

The overlay information appears only on the Live View main stream; this information will not appear on the Live View sub stream.

Full screen monitoring features will trigger only when there is no mouse operation since this feature can't stop user operations.

1.6 Playback

The recorded video files on the hard disk can be played back in the following modes: instant playback, all-day playback for the specified channel, and playback by normal/event/smart/tag/sub-periods/external file search.

To play back video intercom and access control records, do the following:

1. Go to Menu > Playback.
2. Choose **Event** in the left corner.
3. Choose **Access Control/Video Intercom** Major type.
4. Choose a **Major Alarm** or input **Card No.** to search record file.

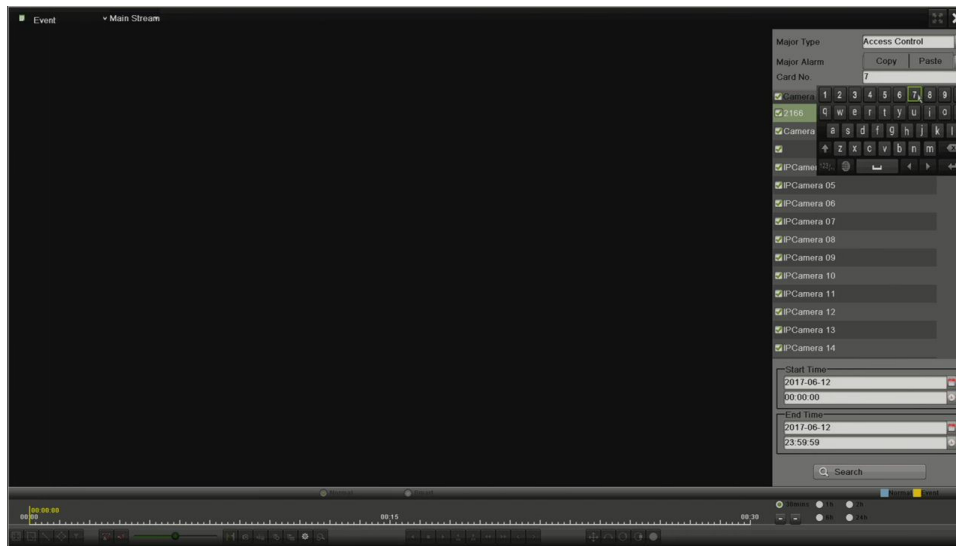


Figure 11, Playback Interface

5. Choose the Start Time and End Time.
6. Click **Search**.
7. Use the toolbar on the bottom of the Playback interface to control playing progress.



Figure 12, Playback Interface

The following chart shows the major video intercom and access control alarms:

Product	Major Type	Description
Video Intercom	Unlock by Password	Password input unlocked the door
	Unlock by Duress	Input duress password unlocked the door, duress password can be set in 4200
	Unlock by Card	Card swipe unlocked the door
	Unlock by Resident	Resident unlocked the door at indoor station or through mobile app
	Card Access Denied	Card swipe to unlock the door failed
	Unlock by Center	Door unlocked in 4200
	Tampering Alarm	Unit taken down
	Duress Alarm	Duress password input
	Multiple unlock failures via password	Maximum 3 attempts to opening door via password, the third attempt will trigger alarm
	Door Not Open Alarm	Door unlocking succeeds, but the door is not open. Need to disable "upload alarm for Not-closed Door" first.
	Door Not Closed Alarm	Door opening succeeds, but the door doesn't close after the door-unlocked duration. Need to enable "upload alarm for Not-closed Door" first.
Access Control	Intercom Alarm	Button pressed for an intercom call
	Authentication Passed	Controller and Terminal successfully authenticates the open door conditions, like card, password, fingerprint, etc.
	Authentication Failed	Controller and Terminal fails to authenticate the open door conditions, like card, password, or fingerprint, etc.
	Open Door	Once authentication has passed and the door has been opened, if users open the door remotely or any other open door event will produce an open door alarm
	Close Door	Any close door event
	Device Exception Event	Device Power Off, Card Reader Offline, or any other device exception event has occurred
	Device Recovered Event	Device Power On, Card Reader Connection Recovered, or any other device recovered event has occurred
	Alarm and Event	/
Alarm Recovered Event	/	
Call System/Doorbell Rang	User pressed call center button/users pressed doorbell rang button (DS-K1T500 only)	

To trigger an access control major type of event, you can trigger a major alarm (refer to the table below)
 To trigger a major alarm, refer to the access control user manual.

Major Type	Major Alarm
Authentication Passed	Legal Card Authentication Passed
	Card and Password Authentication Passed
	Multiple Authentication Passed
	Multiple Authentication: Remotely Open Door
	Multiple Authentication: Super Password Authentication Passed
	Fingerprint Authentication Passed
	Card and Fingerprint Authentication Passed
	Card, Fingerprint, and Password Authentication Passed
	Fingerprint and Password Authentication Passed
	Authentication in System
Authentication Failed	Card and Password Authentication Failed
	Card and Password Authentication Timed Out
	Max. Card and Password Authentication Times
	Permission Not Assigned
	Invalid Duration
	Card No. Expired
	No Card No. Found
	Anti-passing Back Authentication Failed
	Interlocking Door Not Closed
	Card Not in Multiple Authentication Group
	Card Not in Multiple Authentication Duration
	Multiple Authentication: Super Password Authentication Failed
	Multiple Authentication: Remotely Authentication Failed
	Multiple Authentication: Repeated Authentication
	Multiple Authentication Timed Out
	Fingerprint Matching Failed
	Card and Fingerprint Authentication Failed
	Card and Fingerprint Authentication Timed Out
	Card, Fingerprint, and Password Authentication Failed Out
	Card, Fingerprint, and Password Authentication Timed Out
Fingerprint and Password Authentication Failed	
Fingerprint and Password Authentication Timed Out	
Fingerprint Not Exist	
Open Door	Remote: Open Door
	Remote: Remain Open
	Door Remaining Open Status with First Card Started
	Remain Open Started
	Door Unlocked
	Press Down Button
	Normally Open Door
	Abnormally Open Door
	Alarm Output On
Close Door	Opening Door with First Card Ended
	Remain Open Status Ended
	Door Locked
	Release Button
	Normally Close Door
	Open Door Timeout
	Alarm Output Off
	Remain Closed Status Started
	Remain Closed Status Ended
	Remote: Close Door
Remote: Remain Closed	

Major Type	Major Alarm
Device Exception Event	Device Power Off
	Reset Watchdog
	Low Battery Voltage
	AC Power Off
	Reading and Writing FLASH Exception
	Card Reader Offline
	Indicator Offline
	Access Portal Controller Offline
	Secure Door Control Unit Offline
Device Recovered Event	Device Power On
	Battery Voltage Recovered
	AC Power On
	Network Recovered
	Card Reader Connection Recovered
	Indicator Recovered
	Access Portal Controller Recovered
	Secure Door Control Unit Online
Alarm and Event	Zone Short Circuited Alarm
	Zone Disconnected Alarm
	Zone Exception Alarm
	Access Control Device Tampering Alarm
	Card Reader Tampering Alarm
	Event Input Alarm
	Duress Alarm
	No Memory Alarm
	Alarm of Max. Card No. Authentication Failed Attempts
	SD Card Full Alarm
	Capture Linkage Alarm
	Secure Door Control Unit Tampering Alarm
Alarm Recovered Event	Zone Alarm Recovered
	Access Control Device Tamper-Proof Recovered
	Tamper-Proof Card Reader Recovered
	Event Input Alarm Recovered
	Secure Door Control Unit Tamper-Proof Recovered
Call System/Doorbell Rang	Call System
	Doorbell Rang

1.7 File Management

The recorded video files on the hard disk can be searched and export in the File Management interface.

1. Go to Menu > File Management.
2. Choose **Event**.
3. Choose **Access Control/Video Intercom** as the Major type.
4. Choose **Major Alarm Type** and input **Card No.** and other parameters to search record files.
5. Choose files to export.

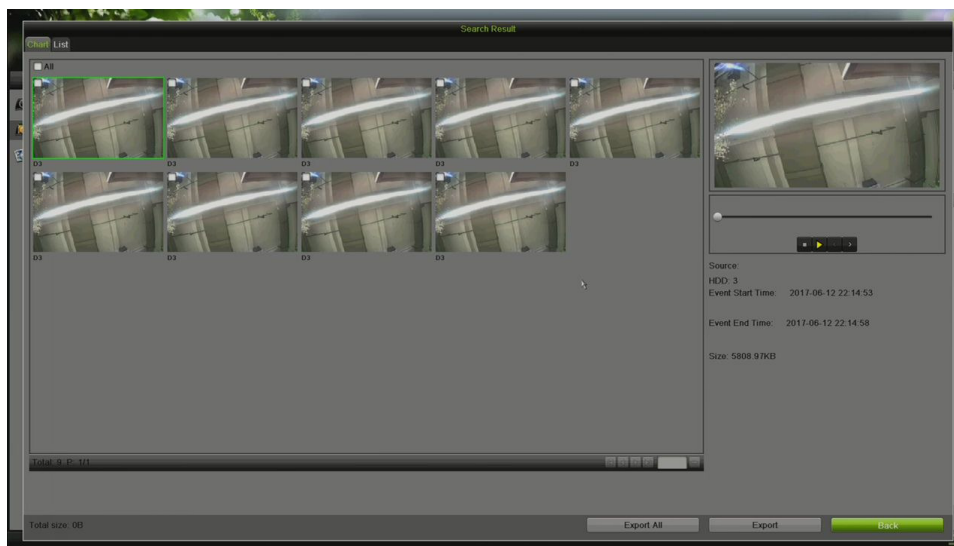


Figure 13, File Management

1.8 Logs

You can search the logs for video intercom and access control events in the NVR.

1. Go to Menu > Maintenance > System Logs.
2. Choose **Alarm** as the Major type.
3. Select Start Time and End Time.
4. Check **Major Type** as Intercom and access control and search logs.

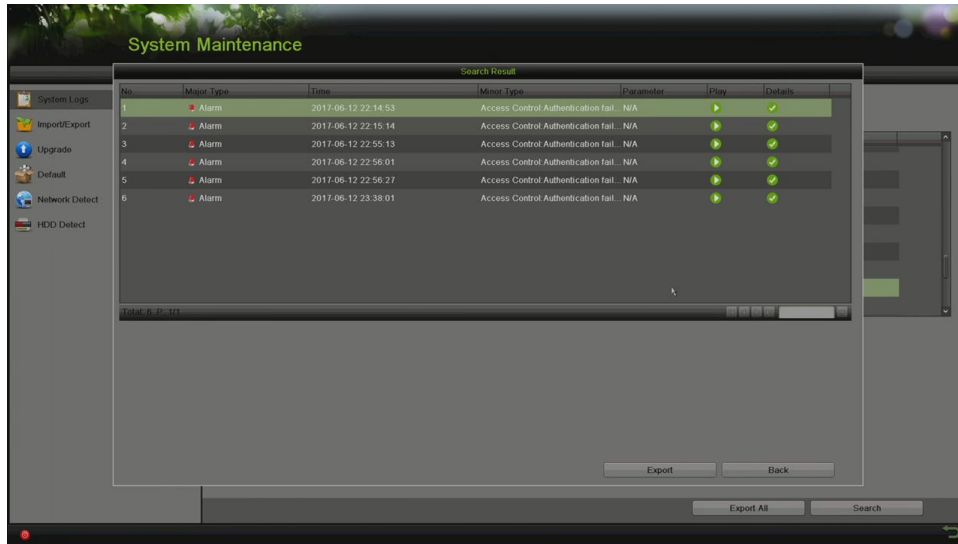


Figure 14, Logs

5. Check a log to show its description such as overlay type, Card no., door name, and door IP.

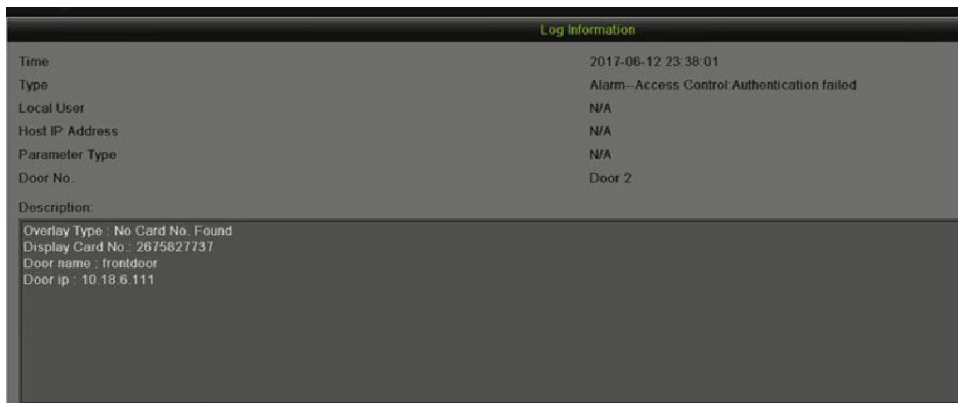


Figure 15, Logs

Chapter 2 Accessing by Web Browser



Video intercom and access control devices currently don't support operation in a Web browser.



First Choice for Security Professionals