

Quick Start Guide (QSG)

T710xQxTx
TurboHD DVR/Camera Kit

© 2016 Hikvision USA Inc. • All Rights Reserved • Any and all information, including, among others, wordings, 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 the Manual.

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 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 or meir 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 SUCHDAMAGES.

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 TO THE APPLICABLE LAW. HIKVISION SHALL NOT BE LIABLE IN THE EVENT THAT THIS PRODUCT IS USED FOR ILLEGITIMATE PURPOSES.

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

Regulatory Information

FCC Information

FCC Compliance: This equipment has been tested and found to comply with the limits for 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:

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

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 2004/108/EC, 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.

Safety Instruction: These instructions are intended to ensure that the user can use the product correctly to avoid danger or property loss. The precaution measure is divided into "Warnings" and "Cautions.

- Warnings: Serious injury or death may occur if any of the warnings are neglected.
- Cautions: Injury or equipment damage may occur if any of the cautions are neglected.



Warnings Follow these safeguards to prevent serious injury or death.



Cautions Follow these precautions to prevent potential injury or material



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. Refer to technical specifications for detailed information. Input voltage should meet both the SELV (Safety Extra Low Voltage) and the Limited Power Source with 24 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. When the product is mounted on wall or ceiling, the device shall be firmly fixed.
- If smoke, odor or noise rise from the device, turn off the power at once and unplug the power cable, and then please contact the service center.



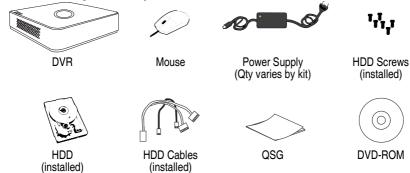
Make sure the power supply voltage is correct before using the camera.

- Do not drop the camera or subject it to physical shock.
- Do not touch sensor modules with fingers. If cleaning is necessary, use clean cloth with a bit of ethanol and wipe it gently. If the camera will not be used for an extended period, Do not aim the camera at the sun or extra bright locations. Blooming or smearing may occur (which is not a malfunction) and affect the endurance of the sensor.

 Do not aim the camera at the sun or extra bright locations. Blooming or smearing may occur (which is not a malfunction) and affect the endurance of the sensor will not be exposed to the laser.
- The sensor may be burned out by a laser beam, so when any laser equipment is in use, make sure that the surface of the sensor will not be exposed to the laser beam. Do not place the camera in extremely hot, cold (the operating temperature shall be -30° C to +60°C, or -40° C to +60° C if the camera model has an "H" in its suffix), dusty, or
- damp locations, and do not expose it to high electromagnetic radiation.
- To avoid heat accumulation, good ventilation is required for the operating environment. Keep the camera away from liquid while in use.
- While in delivery, the camera shall be packed in its original packing, or packing of the same durability
- Regular part replacement is some equipment parts (e.g., electrolytic capacitor) shall be replaced regularly according to their average endurance time. The average time varies because of differences between operating environments and usage history, so regular checking is recommended for all users. Contact your dealer for more details.
- 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.
- If the product does not work properly, contact your dealer or the nearest service center. Never attempt to disassemble the camera yourself. (We shall not assume any responsibility for problems caused by unauthorized repair or maintenance.)

WHAT'S IN THE BOX

Make sure the following items are in your box:



MENU TREE

Use this menu tree to navigate the embedded menus.

	Menu							
Play	back	File Management	VCA Search	Manual	Rec. Config.	Cameras Setup	Maintenance	System Info.
Normal	Main Stream	Record	Behavior Search	Record	Schedule	Cameras	System Logs	Device Info
Event	Sub Stream	Event	Face Search	Alarm	Record Quality	PSD	Import/Export	Camera
Tag	External File		Plate Search	Man. Video Quality	Motion Detect	Image	Upgrade	Record
Smart]		People Counting		Trigger	PTZ	Default	Alarm
Sub-Periods]		Heat Map		Holiday	Privacy Mask	Network Detect	Network
						Video Tamper Det.	HDD Detect	HDD
						Video Loss		
						VCA		
						Video Qual. Diag.		

TOP PANEL



Figure 1, DS-710xHQHI-F1/N Top Panel

Top Panel LEDs				
<u></u>	Red when DVR is powered up			
9	Red when data is being written to or read from the HDD			
品	Flickers blue when network connection is functioning properly			

Figure 2, DS-7104HQHI-F1/N Rear Panel

Figure 3, DS-7108HQHI-F1/N Rear Panel

	DS-710xHQHI-F1/N				
	Description		Description		
1	VIDEO IN	4	AUDIO OUT, RCA Connector	7	USB Ports
2	HDMI Interface	5	AUDIO IN, RCA Connector	8	GND
3	VGA Interface	6	LAN Network Interface	9	12 VDC Power Input

1

CONNECT DEVICES

- 1. Connect power supply to the DVR.
- 2. Connect DVR to LAN using Cat 5e cable.
- 3. Connect video monitor(s) to DVR using HDMI and/or VGA cables, as appropriate.
- 4. Connect mouse to USB port (wireless mouse can be used in lieu of included mouse).
- 5. Connect to audio I/O using RCA connectors.

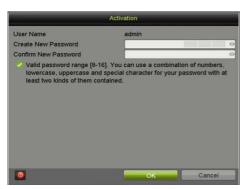
2

START THE DVR

- 1. Plug power supply plug into 110 to 240 VAC outlet (surge suppressor is recommended).
- 2. Turn power switch on. Power indicator LED will turn red to indicate unit is starting.
- 3. After startup, power indicator LED will remain red.

LOCAL ACTIVATION

System access requires a secure, user-assigned password.



▼ Set Admin Password

First-time access requires user to create an admin password.

Input same password in Create New Password and Confirm New Password text fields.



Strong Password REQUIRED

Password must contain 8 to 16 characters, combining numbers, lower and upper case letters, and special characters. At least two types of the above-mentioned characters are required. Also, reset password regularly.

Click **OK** to save password and activate device.

Password Strength Levels

STRENGTH LEVEL	DESCRIPTION			
Level 0 (Risky)	Password is fewer than 8 characters, contains only 1 type of			
DVRs will not accept password	character, is same as the user name, or is mirror writing of user name			
Level 1 (Weak)	Password contains number + lowercase letter or number + uppercase			
DVRs will accept password	letter and is at least 8 characters.			
Level 2 (Medium/Fair)	Password contains 2 types of characters (<i>neither</i> number + lowercase			
DVRs will accept password	letter <i>nor</i> number + uppercase letter) and is at least 8 characters.			
Level 3 (Strong)	Password contains more than three types of characters and is at least			
DVRs will accept password	8 characters.			

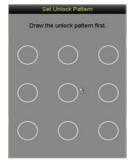
NOTE 1: The strength level indicator colors can vary by activation process, model number, and device type. Typical: Risky (no color), Weak (pink), Fair (yellow), Strong (green).

NOTE 2: PASSWORD CHARACTERS ALLOWED (ASCII Only):

- Lowercase ASCII Letters

 a b c d e f g h l j k l m n o p g r s t u v w x y z
- Uppercase ASCII Letters
 ABCDEFGHIJKLMNOPQRSTUVWXYZ
- Numerals 0 1 2 3 4 5 6 7 8 9
- Special Characters
 _ : / @ , ?! ' () \$ & "[] { } # % ^ * + = \ | < >





▼ Export Password Reset (GUID) Key

Insert a USB device to export the GUID key. This file can be imported to allow a new password to be created should the original password be lost or maliciously changed.

▼ Set Unlock Pattern

Admin user will be prompted to configure an unlock pattern for login in place of a password.

- Hold down left mouse button and draw a pattern connecting at least four dots on the screen, each dot connected only once.
- 2. Release mouse button when done.
- 3. Draw the same pattern again to confirm it.

NOTE: If you forget your pattern, click on "Forgot Password" to display the normal admin login dialog box.

Log In Using the Unlock Pattern

1. Draw the unlock pattern to unlock system.

4

INITIALIZE THE HARD DRIVE (IF NEEDED)

The system is set up to record upon power up and will beep and display "Do you want to initialize drive" prompt if the hard drive(s) are not initialized.

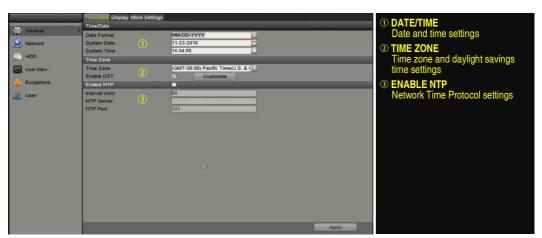
- Go to MENU > SYSTEM CONFIGURATION > HDD.
- 2. Use the checkboxes to select the HDDs that need to be initialized.
- Press INIT. (Factory installed HDDs come initialized. Initializing again will erase any record video. This does not affect settings).



5

SET DATE AND TIME

1. Go to MENU > SYSTEM CONFIGURATION > GENERAL.

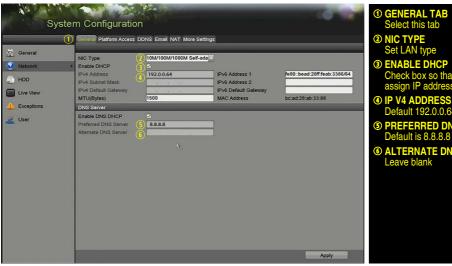


6

SET UP NETWORK ACCESS

A network connection is required to access the cameras remotely.

- 1. Go to MENU > SYSTEM CONFIGURATION > NETWORK.
- 2. Enable DHCP (check the checkbox).
- 3. Press **Refresh** button to update the IPv4 address, subnet mask, and IPv4 default gateway.
- 4. Disable DHCP (uncheck the checkbox).
- 5. Change "Preferred DNS Server" value to 8.8.8.8 (leave Alternate DNS Server blank).



① GENERAL TAB Select this tab

Set LAN type

3 ENABLE DHCP Check box so that router will assign IP address

IP V4 ADDRESS Default 192.0.0.64

⑤ PREFERRED DNS SERVER

6 ALTERNATE DNS SERVER Leave blank

SET REMOTE VIEWING PORTS

After assigning the IP information, click the More Settings tab.



The **More Settings** tab contains the ports that need to be forwarded for remote access.



- **SERVER PORT** is responsible for the mobile app and client software log-in
- HTTP PORT is responsible for Web browser log-in
- RTSP PORT is responsible for video/audio streaming

The HTTP port, server port, and RTSP port can be changed to avoid NOTE: conflicts with the ISP or if multiple devices are installed at a single location.

SET UP PORT FORWARDING

Port forwarding redirects communication from one address/port number to another to make services on a protected network available to hosts on an external network.

Log into the router, and proceed with port forwarding. Port forwarding steps differ by router. For
port forwarding assistance, contact your Internet Service Provider (ISP) or router manufacturer. Also
refer to www.portforward.com for step-by-step instructions.

NOTE: Hikvision USA is not associated with www.portforward.com and is not

responsible for any activity between the user and www.portforward.com. Avoid

accidentally downloading any software from www.portforward.com.

2. Proceed to the **Routers** section on the website for step-by-step instructions.

9

SET UP DDNS (Dynamic Domain Name System)

DDNS allows users with dynamic (changing) IP address to access their unit remotely.

- Click on the **DDNS** tab.
- Check the **DDNS** checkbox.
- 3. **DDNS Type**: HiDDNS (default)
- 4. Continent/Country: Auto Detection (default)
- 5. Server Address: www.hik-online.com (U.S. default)
- Create a **Device Domain Name** (cannot begin with a number, contain spaces, special characters, or upper case letters).
- Create a User Name.
- 8. **Password**: System uses device serial number; cannot be changed.



 Once the changes have been made, press Apply to display the Succeeded message. (If the Domain Name does not meet acceptable criteria, or is already registered, an error message will appear.)

10

ADD <u>ANALOG CAMERAS</u>

- 1. Plug cameras into the Video In BNC ports.
- 2. Apply power to the cameras.

VIEW LIVE VIDEO

Live View displays real-time video.



Icons in the upper right of screen show each camera's record and alarm status.

- Alarm (video loss, tampering, motion) detection, sensor alarm, or VCA alarm)
- Record (manual record, continuous record, motion detection, alarm, or VCA triggered record)
- Event/Exception (event and exception information appears at lower-left corner of screen)

12 SET UP RECORDING

The system defaults to record video continuously at at maximum frame rate. Consider adjusting to 8 fps for continuous and 15 fps for event recording for optimum recording.

Recording Schedule

Default is to record continuously every day. Do the following to change the recording schedule:

- 1. Go to MENU > RECORDING CONFIGURATION > SCHEDULE.
- 2. Choose **CONTINUOUS** or **EVENT/(MOTION DETECTION)** under the **Type** pull-down menu.
- 3. Use cursor to select (days will turn blue [continuous] or yellow [event/motion detect]) or deselect (days will turn gray [off]) the calendar days you wish to record.
- 4. Apply time settings as desired.
- 5. Press APPLY.



ion or Continuous (default)

Shows Recording Schedule days:

- Blue=Continuous
- Yellow=Event (motion/alarm)
- Grey=None

TIMES Customize schedule times (ignore for "motion only" recording)

Press to add time settings to schedule

S ENABLE SCHEDULE If not checked, camera will not record

Motion Detection Areas

To define the image areas that Motion Detection will monitor for each camera, do the following:

- Go to MENU > RECORDING CONFIGURATION > MOTION DETECT.
- 2. Use Camera pull-down menu to select camera to configure.
- 3. Check the **Enable Motion Detection** checkbox to enable motion detection.
- Use the Sensitivity boxes to select how responsive the detection should be (the more green boxes lit, the greater the sensitivity).
- 5. Drag a grid(s) over the area(s) on the image that will be sensitive to motion.
- Click the Settings Set button to configure Arming Schedule (when detection is enabled) and Linkage Actions (what action(s) to take when motion is detected).



▼ Record Quality

Main Stream

- Go to RECORDING CONFIGURATION > RECORD QUALITY > MAIN STREAM and set the following items:
 - Stream Type enables/disables audio streaming from the cameras (if the camera does not have audio capabilities, Stream Type will have only Video option).
 - Resolution sets recording resolution.
 - Bitrate Type:
 - > Variable saves HDD space
 - > Constant provides more stable stream



- Video Quality adjusts picture clarity (high setting = four green squares is default).
 Consider highest if hard drive space allows. Medium setting is a balance between good picture and saving HDD space.
- Frame Rate sets recording frame rate The system defaults to record video continuously at maximum frame rate. Consider adjusting to 8 fps for continuous and 15 fps for event recording for optimum recording. Higher frame rates require more storage, but allow better slow motion playback.
- Max Bitrate Mode chooses between pre-set bitrate values and customized values (General setting is default).
- Max Bitrate (kbps) is the chosen bitrate for streaming the video. Max Bitrate should be adjusted to meet or exceed the rate recommended by the system for the chosen parameters.
- Max Bitrate Recommended is impacted by resolution, quality, and frame rate.
- Record Audio turns on audio recording. Requires connection of external microphone or camera with built-in mic.
- Video Stream determines which stream is recorded. Leave at default (Main Stream).

Substream

 Go to RECORDING CONFIGURATION > RECORD QUALITY > SUBSTREAM to set up the Sub Stream to stream to mobile devices and display multiple cameras locally.

NOTE: If the upload speed is not sufficient, lower the frame rate, bitrate, and or resolution for more fluent mobile viewing.



- More Settings...
 - Click the More Settings... button to display additional settings.



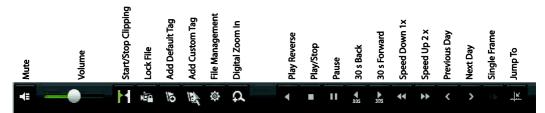
13 PLAY BACK RECORDED VIDEO

- Go to MENU > PLAYBACK. 1.
- 2. Select the desired camera(s) from the menu on the right of the screen.
- 3. Select the desired date (days that contain recordings will be blue if recording was continuous only or yellow if all or part of the day was event recording).
- 4. Press PLAY.
- 5. Click within the timeline to jump to desired time.



- PLAYBACK TYPE MENU Select type of record to play
- Goes to full screen for multiple channel playback
- Begin playback (toggles between
- CAMERA LIST Select camera(s) to play back
- **CALENDAR**
- Select date to play back
- Click on timeline to jump to desired playback time
- SMART PLAYBACK OPTIONS Click to initiate Smart playback

Playback Controls



▼ Play Back Record Files

- 1. Go to MENU > LIVE VIEW.
- 2. Left click a Live View window to bring up a shortcut toolbar and click on the licon for instant playback.

▼ Playback Controls

1. Right click a Live Image to display a Quick menu and click on 😜 icon for instant playback.

1 4 BACK UP VIDEO RECORDINGS AND CLIPS

Back up recorded video clips to ensure important video is not lost or destroyed.

▼ Choose Recorded Video Clips to Back Up

- 1. Connect a USB flash drive, HDD, or DVD writer to an available USB port (this step is mandatory).
- 2. Go to MENU > PLAYBACK.
- 3. Select cameras for playback.
- 4. Select the date and beginning time of the incident.
- 5. Click **START CLIPPING** button.

- 6. Select the ending time of the incident.
- 7. Click END CLIPPING button (same button as START CLIPPING). Clip will be marked.
- 8. Repeat steps 1-6 as many times as required.
- 9. Click **FILE MANAGEMENT** button to display a new window containing all marked clips.
- 10. Select the desired clips.
- 11. Click **EXPORT** to save files to the inserted USB device.

▼ Lock Video Clips

- 1. Click on the images of the clips you want to lock.
- 2. Press the **LOCK** button to prevent the file from being erased.

▼ Back Up Video Clips

- Connect a USB flash drive, HDD, or DVD writer to an available USB port.
- 2. Click on the **File Management** button to display the File Management window.
- 3. In the File Management window, choose video clip(s) to back up and click **Export** button.
- 4. Choose backup device (USB flash drive, USB HDD, or DVD writer).
- 5. Click **Export** (to check backup, choose recorded file in Export interface and click button).
- 6. Select items you wish to back up.
 - Video and log
 - Player
 - · Video splicing backup (merge files)
- 7. Click OK.













First Choice for Security Professionals

Hikvision USA Inc., 18639 Railroad St., City of Industry, CA 91748, USA Hikvision Canada, 4485 Dobrin, St-Laurent, Quebec, Canada, H4R 2L8 Telephone: +1-909-895-0400 • Toll Free in USA: +1-866-200-6690 E-Mail: sales.usa@hikvision.com • www.hikvision.com © 2016-2017 Hikvision USA Inc. • All Rights Reserved

Specifications subject to change without notice. QSG022817NA