

Video Access Control Terminal

Quick Start Guide

V1.1.0

<u>UD</u>

Quick Start Guide

©2016 Hangzhou Hikvision Digital Technology Co., Ltd.

It includes instructions on how to use the Product. The software embodied in the Product is governed by the user license agreement covering that Product.

About this Manual

This Manual is subject to domestic and international copyright protection. Hangzhou Hikvision Digital Technology Co., Ltd. ("Hikvision") reserves all rights to this manual. This manual cannot be reproduced, changed, translated, or distributed, partially or wholly, by any means, without the prior written permission of Hikvision.

Trademarks

HIKVISION and other Hikvision marks are the property of Hikvision and are registered trademarks or the subject of applications for the same by Hikvision and/or its affiliates. Other trademarks mentioned in this manual are the properties of their respective owners. No right of license is given to use such trademarks without express permission.

Disclaimer

TO THE MAXIMUM EXTENT PERMITTED BY APPLICABLE LAW, HIKVISION MAKES NO WARRANTIES, EXPRESS OR IMPLIED, INCLUDING WITHOUT LIMITATION THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE, REGARDING THIS MANUAL. HIKVISION DOES NOT WARRANT, GUARANTEE, OR MAKE ANY REPRESENTATIONS REGARDING THE USE OF THE MANUAL, OR THE CORRECTNESS, ACCURACY, OR RELIABILITY OF INFORMATION CONTAINED HEREIN. YOUR USE OF THIS MANUAL AND ANY RELIANCE ON THIS MANUAL SHALL BE WHOLLY AT YOUR OWN RISK AND RESPONSIBILITY.

REGARDING TO THE PRODUCT WITH INTERNET ACCESS, THE USE OF PRODUCT SHALL BE WHOLLY AT YOUR OWN RISKS. OUR COMPANY 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, OUR COMPANY 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. OUR COMPANY 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.

Support

Should you have any questions, please do not hesitate to contact your local dealer.

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 B digital device, pursuant to part 15 of the FCC Rules. These limits are designed to provide reasonable protection against harmful interference in a residential installation. This equipment generates, uses and can radiate radio frequency energy and, if not installed and used in accordance with the instructions, may cause harmful interference to radio communications. However, there is no guarantee that interference will not occur in a particular installation. If this equipment does cause harmful interference to radio or television reception, which can be determined by turning the equipment off and on, the user is encouraged to try to correct the interference by one or more of the following measures:

-Reorient or relocate the receiving antenna.

-Increase the separation between the equipment and receiver.

 $-\mbox{Connect}$ the equipment into an outlet on a circuit different from that to which the receiver is connected.

-Consult the dealer or an experienced radio/TV technician for help.

This equipment should be installed and operated with a minimum distance 20cm between the radiator and your body.

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 RE Directive 2014/53/EU, the EMC Directive 2014/30/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: <u>www.recyclethis.info</u>



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

Safety Instruction

These instructions are intended to ensure that user can use the product correctly to avoid danger or property loss.

The precaution measure is divided into Warnings and Cautions:

Warnings: Neglecting any of the warnings may cause serious injury or death.

Cautions: Neglecting any of the cautions may cause injury or equipment damage.

A Warnings	A Cautions
Follow these	Follow these precautions
safeguards to prevent	to prevent potential injury
serious injury or death.	or material damage.

Warnings

- All the electronic operation should be strictly compliance with the electrical safety regulations, fire prevention regulations and other related regulations in your local region.
- Please use the power adapter, which is provided by normal company. The power consumption cannot be less than the required value.
- Do not connect several devices to one power adapter as adapter overload may cause over-heat or fire hazard.
- Please make sure that the power has been disconnected before you wire, install or dismantle the device.
- When the product is installed on wall or ceiling, the device shall be firmly fixed.
- If smoke, odors or noise rise from the device, turn off the power at once and unplug the power cable, and then please contact the service center.
- If the product does not work properly, please contact your dealer or the nearest service center. Never attempt to disassemble the device yourself. (We shall not assume any responsibility for problems caused by unauthorized repair or maintenance.)

- Do not drop the device or subject it to physical shock, and do not expose it to high electromagnetism radiation. Avoid the equipment installation on vibrations surface or places subject to shock (ignorance can cause equipment damage).
- Do not place the device in extremely hot (refer to the specification of the device for the detailed operating temperature), cold, dusty or damp locations, and do not expose it to high electromagnetic radiation.
- The device cover for indoor use shall be kept from rain and moisture.
- Exposing the equipment to direct sun light, low ventilation or heat source such as heater or radiator is forbidden (ignorance can cause fire danger).
- Do not aim the device at the sun or extra bright places. A blooming or smear may occur otherwise (which is not a malfunction however), and affecting the endurance of sensor at the same time.
- Please use the provided glove when open up the device cover, avoid direct contact with the device cover, because the acidic sweat of the fingers may erode the surface coating of the device cover.
- Please use a soft and dry cloth when clean inside and outside surfaces of the device cover, do not use alkaline detergents.
- Please keep all wrappers after unpack them for future use. In case of any failure occurred, you need to return the device to the factory with the original wrapper. Transportation without the original wrapper may result in damage on the device and lead to additional costs.
- 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.

Contents

1 Installation
2 Terminal Connection
2.1 Terminal Description
3 Wiring Description
3.1 External Device Wiring Overview5
3.2 The Wiring of External Card Reader6
3.2.1 The Wiring of External RS-485 Card Reader6
3.3 Card Reader Connection
3.3.1 The Wiring of Wiegand6
3.3.2 The Wiring of RS-485 Output7
4 Activating the Access Control Terminal
4.1 Activating via SADP Software8
4.2 Activating via Client Software9
5 Appendix:
5.1 Tips for Scanning Fingerprint12
5.2 Specification

1 Installation

Before You Start:

- Make sure that the device in the package is in good condition and all the assembly parts are included.
- Make sure that the wall is strong enough to withstand three times the weight of the terminal.
- Set the DIP address before installation.

Steps:

- Connect the cables with the connecter on the rear panel of the device. Route the cables through the cable hole of the mounting plate. The cable holes are on the right side, left side and lower side of the rear cover. If the right/left side cable hole is selected, remove the plastic sheet of the cable hole.
- After routing the cable, pour glues(recommended model: Devcon 24105) into the pouring area.
- 3. Secure the mounting plate on the wall with 4 supplied screws.
- 4. Connect the corresponding cables.
- 5. Push the terminal in the mounting plate from bottom up.
- 6. Tighten the screws on the bottom of the terminal to fix the terminal on the mounting plate and complete the installation.



2 Terminal Connection

2.1 Terminal Description



Figure 2-1 Terminal Diagram of Access Control Terminal

Group	No.	Function	Color	Terminal Name	Description	
Group A	A1	Power Input	Red	+12V	12V DC Power Supply	
	A2		Black	GND	GND	
	B1		Yellow	IN1	Alarm Input 1	
	B2	Alarm Input	Orange	IN2	Alarm Input 2	
Crown P	B3		Black	GND	GND	
Group B	B4		Red	NC		
	B5	Alarm Output	White	СОМ	Alarm Output Wiring	
	B6		Purple	NO		
	C1		Black	GND	GND	
	C2		Green	W0	Wiegand Wiring 0	
	C3		White	W1	Wiegand Wiring 1	
Group C	C4	Wiegand	Black	GND	GND	
	C5		Brown	LED-OK	Wiegand Authenticated	
	C6		Orange	LED-ERR	Wiegand Authentication Failed	
	C7		Gray	TAMPER	Tampering Alarm Wiring	
	C7		Purple	BEEP	Buzzer Wiring	
	D1		Yellow	NC		
	D2		White	СОМ	Lock Wiring	
	D3		Red	NO		
Group D	D4	Lock	Green	SENSOR	Door Magnetic Signal Input	
	D5		Gray	BUTTON	Exit Door Wiring	
	D6		Black	GND	GND	
Group F	E1		Yellow	485 +	PS 485 Wiring	
Group E	F2	K3-483	Blue	485 -	KS-485 Wiring	

Table 2-1 Terminal Description

3 Wiring Description



Figure 3-1 External Device Connection Diagram

3.2 The Wiring of External Card Reader

3.2.1 The Wiring of External RS-485 Card Reader



Figure 3-2 External RS-485 Card Reader Connection Diagram

3.3 Card Reader Connection

The access control terminal can be switched into the card reader mode. It can access to the access control as a card reader, and supports Wiegand communication port and RS-485 communication port.

NOTE

When the access control terminal works as a card reader, it only supports being connected to the controller, but does not support alarm input or output, or the connection of external devices.



3.3.1 The Wiring of Wiegand

Figure 3-3 Wiegand Connection Diagram



 When the access control terminal works as a card reader, you must the WG_ERR, BUZZER and WG_OK interfaces if you want to control the LED and buzzer of the Wiegand card reader.

- Set the working mode of the terminal as card reader, if the terminal is required to work as a card reader. The card reader mode support to communicate by Wiegand or RS-485.
- The distance of Wiegand communication should be no longer than 80 m.
- The external power supply and the access control terminal should use the same GND cable.

3.3.2 The Wiring of RS-485 Output





- Set the working mode of the terminal as card reader, if the terminal requires working as a card reader.
- When the access control terminal works as a RS-485 card reader, the default RS-485 address is 1.
- The external power supply and the access control terminal should use the same GND cable.

4 Activating the Access Control Terminal

Purpose:

You are required to activate the terminal first before using it. Activation via SADP, and Activation via client software are supported. The default values of the control terminal are as follows.

- The default IP address: 192.0.0.64.
- The default port No.: 8000.
- The default user name: admin.

4.1 Activating via SADP Software

SADP software is used for detecting the online device, activating the device, and resetting the password.

Get the SADP software from the supplied disk or the official website, and install the SADP according to the prompts. Follow the steps to activate the control panel.

Steps:

- 1. Run the SADP software to search the online devices.
- 2. Check the device status from the device list, and select an inactive device.

Ŭ	SADI									0 1 1 1
То	al number c	of online devices: 6					l	Export	Refresh	Activate the Device
•	ID 🔺	Device Type	Security	IPv4 Address	Port	Software Version	IPv4 Gateway	HTTP Port	Device Serial No	
	001		Active		8000	V1.4.0build 1609		80		201
	002		Active		8000	V1.4.2build 1608		80		160
	003		Active		8000	V1.4.0build 1609		80		24
	004		Active		8000	V5.4.0build 1602		80		The device is not activated
	005		Active		8000	V2.0.1build 1605		80		
	006	DS-K	Inactive	192.0.0.64	8000	V	0.0.00	80		160
										You can modify the network parameters after the device activation.
										Activate Now
										New Password:
										Confirm Password:
										Activate
4										b

Figure 4-1 SADP Interface



STRONG PASSWORD RECOMMENDED– We highly recommend you create a strong password of your own choosing (using a minimum of 8 characters, including upper case letters, lower case letters, numbers, and special characters) in order to increase the security of your product. And we recommend you reset your password regularly, especially in the high security system, resetting the password monthly or weekly can better protect your product.

- 4. Click **Active** to active the device.
- 5. You can change the device IP address to the same subnet with your computer by either modifying the IP address manually or checking the Enable DHCP checkbox.

Modify Network	Parameters
Enable DHCP	
Device Serial No.:	
IP Address:	
Port:	8000
Subnet Mask:	
Gateway:	
IPv6 Address:	::
IPv6 Gateway:	:
IPv6 Prefix Length:	0
HTTP Port:	80
S	ecurity Verification
Admin Password:	
	Modify
	Forgot Password

Figure 4-2 Modify Network Parameters Interface

6. Input the password and click the **Modify** button to save your IP address modification.

4.2 Activating via Client Software

The client software is versatile video management software for multiple kinds of devices. Get the client software from the supplied disk or the official website, and install the software according to the prompts. Follow the steps to activate the control panel. *Steps:*

1. Run the client software and the control panel of the software pops up, as shown in the figure below.

File System View Tool Help	i.	iVMS-4200 Access Control Cli	ent	admin 11:26:09 🚨 🗕 🗖 🗙
Control Panel				
Basic Settings				
	2	<u> </u>		
Device Management	Person Management	Card Management	Template	Access Control Permission
Adding, editing, and deleting of access controllers.	Adding, editing, and deleting of person and departments.	Adding, editing, and deleting the card information.	Adding, deleting, and editing of duration, week plan, and	Adding, deleting, and applying the access control
Advanced Function		Attendanc	e Management	
				<u>~</u>
Advanced Function	Linkage Configuration	Attenda	nce Configuration Attend	lance Statistics
Configuring advanced functions including access	Configuring event alarm, event card, and client	Setting sh including	ift schedule Calculatii attendance rule, the attend	ng and analyzing dance results.
Access Control Maintenance				
		2	ō	18
Status Monitor	Door Group Management	Account Management	Event Management	Log Search
Displaying access control status and provides anti-	Adding, editing, and deleting the access control group.	Adding, editing, and deleting the user and assigning	Searching the access control event.	Searching the configuration logs and control logs.
Alarm Information				∦ □ \$
	Figure	4-3 Control Panel	Interface	

Click Device Management icon on the control panel to enter the access control device management

interface.

2.

Online Device	e (2)	😯 Refresh Every 60s)			
+ Add to C	Client + Add All Device	Modify Netinfo	A Reset	Password	Activate	Filter
IP	Device Type	Firmware Version	Security	Port	Device Serial No.	Start Time Added
	10 × 10 00 × 1	V1.0.1build 160	Active	8000		2016-10-21 14:2 No
192.0.0.64	the second second	V .	Inactive	8000	1	2016-10-21 14:2 No

Figure 4-4 Online Device List

- 3. Select an inactive device in the Online Device list.
- 4. Click the **Activate** button to pop up the Activation interface.
- 5. Create a password and input the password in the password field, and confirm the password.

STRONG PASSWORD RECOMMENDED– We highly recommend you create a strong password of your own choosing (using a minimum of 8 characters, including upper case letters, lower case letters, numbers, and special characters) in order to increase the security of your product. And we recommend you reset your password regularly, especially in the high security system, resetting the password monthly or weekly can better protect your product.

	Activation ×
User Name:	admin
Password:	
	Valid password range [8-16]. You can use a combination of numbers, lowercase, uppercase and special character for your password with at least two kinds of them contained.
Verification:	
	OK Cancel

Figure 4-5 Input Password Window

- 6. Click **OK** button to start activation.
- 7. Click the **Modify Netinfor** button to pop up the Network Parameter Modification interface.

	Modify Network Parameter	×
Device Information:		
MAC Address:	44-19-b6-c7-62-f3	Сору
SoftVersion:		Сору
Serial No.:	DS-K1T600SF20161107V010000CH6465039330	Сору
Network Information:		
IP Address:	192.0.0.64	
Port:	8000	
Subnet Mask:	255.255.255.0	
GateWay:	0.0.0.0	
Password:		
	ОК	Cancel

Figure 4-6 Modify Network Parameters Window

- 8. Change the device IP address to the same subnet with your computer by either modifying the IP address manually.
- 9. Input the password and click the **OK** button to change the device network information.

5 Appendix:

5.1 Tips for Scanning Fingerprint

Recommended Finger

Forefinger, middle finger or the third finger.

Correct Scanning

The figure displayed below is the correct way to scan your finger:



You should press your finger on the scanner horizontally. The center of your scanned finger should align with the scanner center.

Incorrect Scanning

The figures of scanning fingerprint displayed below are wrong:

Vertical



Side

Edge I

Edge II



Environment

The scanner should avoid direct high light, high temperature, humid conditions and rain.

When it is dry, the scanner may not recognize your fingerprint successfully. You can blow your finger and scan again after drying the finger.

Others

If your fingerprint is shallow, or it is hard to scan your fingerprint, we recommend you to use other authentication methods.

If you have injuries on the scanned finger, the scanner may not recognize. You can change another finger and try again.

5.2 Specification

Model	DS-K1T500SF/DS-K1T500S			
Camera	1080P, More than 2 Megapixel; Recognition Distance<= 1m; Support IR Light; Support Outdoor Operation; Support Scanning QR Code			
Fingerprint Capacity	3000 (DS-K1T500SF)			
Card Capacity	50,000			
Recording Capacity	200,000			
Authentication Speed	1: N Fingerprint Recognition Duration (Matching with All Fingerprints) <= 1s (DS-K1T500SF)			
FAR	Fingerprint<= 0.001 %(DS-K1T500SF)			
FRR	Fingerprint<= 0.01 %(DS-K1T500SF)			
Fingerprint Scanner	Optical Fingerprint Collecting Instrument (DS-K1T500SF)			
Card Reading Format	Mifare Card / CPU Serial No. / Other Cards. Supports Operating in Metal Environment			
Card Reading Distance	Mifare Card > 2cm; Other Cards > 1cm			
Button	1 Doorbell Button; 1 Voice Talk Button			
Communication	TCP/IP 10/100Mbps*1, RS485*1, Wiegand26/34*1, Alternative WIFI/4G/3G/GPRS			
Input / Output Interface	1 Door Magnetic, 1 Exit Button, 1 Door Lock, 2 Alarm Input, 1 Alarm Output (Door Bell), 1 SD Card Slot, and 1 Audio Input			
Voice Prompt	1 Buzzer and 1 Loud Speaker			
Two-way Audio	Supports Communicating with Monitoring System			
Wi-Fi Probe	Alternative			
Storage	Built-in Micro SD Card; HIK SD Card, up to 128G; Support NVR Storage			
Protection Level	IP65			

Tamper-Proof	Support
Working Temperature	-40°C to 70°C
Working Humidity	10% to 90% (No Condensation)
Appearance	Metal
Mount Option	Wall Mounting; Metal Door Mounting
Dimensions	Cuboid



HIKVISION | www.hikvision.com