



Hik Device Gateway

User Manual

Legal Information

About this Document

- This Document 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 Document is subject to change, without notice, due to firmware updates or other reasons. Please find the latest version of the Document at the Hikvision website (<https://www.hikvision.com>). Unless otherwise agreed, Hangzhou Hikvision Digital Technology Co., Ltd. or its affiliates (hereinafter referred to as "Hikvision") makes no warranties, express or implied.
- Please use the Document with the guidance and assistance of professionals trained in supporting the Product.

About this Product

This product can only enjoy the after-sales service support in the country or region where the purchase is made.

Acknowledgment of Intellectual Property Rights

- Hikvision owns the copyrights and/or patents related to the technology embodied in the Products described in this Document, which may include licenses obtained from third parties.
- Any part of the Document, including text, pictures, graphics, etc., belongs to Hikvision. No part of this Document may be excerpted, copied, translated, or modified in whole or in part by any means without written permission.
- **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.

LEGAL DISCLAIMER

- TO THE MAXIMUM EXTENT PERMITTED BY APPLICABLE LAW, THIS DOCUMENT 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 DOCUMENT AND THE APPLICABLE LAW, THE LATTER PREVAILS.

© Hangzhou Hikvision Digital Technology Co., Ltd. All rights reserved.

Contents


Chapter 1 Overview	1
Chapter 2 Step 1: Install Device Gateway	2
2.1 Port Instruction	2
2.2 Install Device Gateway on Windows	2
2.3 Install Device Gateway on Linux	2
2.4 Activate Device Gateway	6
Chapter 3 Step 2: Add Devices	7
Chapter 4 Step 3: Test APIs	8
4.1 Test Transmitting Device ISAPI	8
4.2 Test General Protocol	9
4.3 Test Video Protocol	10
4.3.1 Test Video Playback	10
4.3.2 Test Two-Way Audio	11
Chapter 5 Other Configuration	13
5.1 ISAPI Management	13
5.2 Basic Configuration	14

Chapter 1 Overview

Overview

As a protocol converter, the Hik Device Gateway connects access control devices and encoding devices with third-party platforms for data transmission over LAN or WAN. You can add and manage ISUP-enabled encoding devices and ISUP5.0/ISAPI-enabled access control devices for intergration with third-party platforms. You can also test the available APIs on the Device Gateway to check if a function works well.

System Requirements

Features	Requirements
Operating System	<ul style="list-style-type: none">• Microsoft(R) Windows 10 (64-bit), Windows Server 2012 R2 (64-bit), Windows Server 2016 (64-bit), Windows Server 2019 (64-bit) <div> Note For Windows Server 2012 R2 (64-bit), install the patch KB2999226.</div> <ul style="list-style-type: none">• CentOS 7 (64-bit)• Ubuntu 20.04 (64-bit)• Red Hat Enterprise Linux9 (64-bit)
CPU	Intel(R) Core(TM) i5-7500 @ 3.0 GHz, 4 core or more
RAM	8GB or more
NIC	Gigabit-NIC with a latest driver

Chapter 2 Step 1: Install Device Gateway

You can install the Device Gateway service to your server or PC to use the service remotely. This part contains the following sections.

2.1 Port Instruction

Before using this service, check if the default ports of the Device Gateway are used. You can configure them if the default ports are used.

2.2 Install Device Gateway on Windows

1. Right-click the program file, run as the administrator to enter the welcome panel, and select **Next**.
2. (Optional) Select **Browse...** to select the path of legacy configuration files, and select **Next**.




Note

- If you have kept the configuration files of an uninstalled Device Gateway, the Device Gateway will reuse the files saved in the selected path when you install a new version.
- If the configuration file path of previous version is detected, it is selected by default.

3. Select **Browse...**, select a proper directory as required to install the service, and select **Next**.
4. (Optional) If the default HTTP port is used, edit the port number.
5. Select **Install**.
6. Read the post-install information and select **Finish** to complete the installation process.



Note

- After the Device Gateway is installed, the login page will automatically open in your default web browser.
 - After the Device Gateway is installed, the Watchdog service will get started and hide in the notification area of the desktop. Right-click  and select the option to stop the service and start the Device Gateway service, or exit the Watchdog service.
 - If you install the Device Gateway remotely, log into the local computer to show the Watchdog service.
-

2.3 Install Device Gateway on Linux

1. Add a folder such as /opt/test/DeviceGateway as the installation directory of the Device Gateway, and put the installation package in the folder.

Hik Device Gateway User Manual

```
[root@localhost opt]# cd /opt/test/
[root@localhost test]# ls
[root@localhost test]# mkdir DeviceGateway
[root@localhost test]# ls
DeviceGateway
[root@localhost test]# cd ./DeviceGateway/
[root@localhost DeviceGateway]# ls
HikDeviceGateway_V1.6.0.2Build20220718_Linux64.tar.gz
[root@localhost DeviceGateway]#
```

Figure 2-1 Installation Folder

2. Execute tar command to extract the file to the installation directory.

```
[root@localhost DeviceGateway]# tar -zxvf ./HikDeviceGateway_V1.6.0.2Build20220718_Linux64.tar.gz -C ./
./
./7za
./apps/
./apps/das_media_x64/
./apps/das_media_x64/plugins/
./apps/das_media_x64/plugins/ehomeV5_plugin/
./apps/das_media_x64/plugins/ehomeV5_plugin/HCAapSDKCom/
./apps/das_media_x64/plugins/ehomeV5_plugin/HCAapSDKCom/libSystemTransform.so
./apps/das_media_x64/plugins/ehomeV5_plugin/HCAapSDKCom/libconv2.so
./apps/das_media_x64/plugins/ehomeV5_plugin/libhpr.so
./apps/das_media_x64/plugins/ehomeV5_plugin/libNetUtils.so
./apps/das_media_x64/plugins/ehomeV5_plugin/libhlog.so
./apps/das_media_x64/plugins/ehomeV5_plugin/libHCISUPStream.so
./apps/das_media_x64/plugins/ehomeV5_plugin/libcrypto.so
./apps/das_media_x64/plugins/ehomeV5_plugin/libcrypto.so.1.0.0
./apps/das_media_x64/plugins/ehomeV5_plugin/libehomeV5_stream_plugin.so
./apps/das_media_x64/plugins/ehomeV5_plugin/libssl.so
./apps/das_media_x64/plugins/ehomeV5_plugin/libssl.so.1.0.0
./apps/das_media_x64/plugins/ehomeV5_plugin/libidentify.so
```

Figure 2-2 Extract File

```
[root@localhost DeviceGateway]# ls
7za
apps
Config_Template.xml
ConfigUpgrade.sh
DeviceGatewayGuard
DeviceGatewayService
DeviceGatewayService.hservice
drivers
HCAapSDKCom
HikDeviceGateway_V1.6.0.2Build20220718_Linux64.tar.gz
install.sh
ISAPICongif_Template.xml
ivmsservice.sh
libboost_chrono.so
libboost_chrono.so.1.60.0
libboost_regex.so
libboost_regex.so.1.60.0
libboost_system.so
libboost_system.so.1.60.0
libboost_thread.so
libboost_thread.so.1.60.0
libcrypto.so
libcrypto.so.1.0.0
libDriverMgr.so
libDrvNetLib.so
libGuardClient.so
libHCISUPSS.so
libHCNetUtils.so
libHCAAlarmBus.so
libHCAAlarmSendBus.so
libHBase.so
libHDeviceCfBus.so
libHDeviceMgrBus.so
libHDeviceMgr.so
libHGatewayCfBus.so
libHGatewayProtocol.so
libHHTTPService.so
libHGISAPIMgrBus.so
libHGISAPIProtocol.so
libHMediaBus.so
libHServiceMgr.so
libhlog.so
libhplug.so
libhprocessClient.so
libhprocess.so
libhpr.so
libhservice.so
libconv.so.2
libidentify.so
libsoncpp.so
libsoncpp.so.20
libson.so
libsqlcipher.so
libsqlcipher.so.0
libsqlite3.so
libssl.so
libssl.so.1.0.0
libtynxml.so
libutils.so
libz.so
log4cxx.properties
nginx
PrivateConfig_Template.xml
protocol_debug
restart.sh
sfrzcfg
start.sh
status.sh
stop.sh
uninstall.sh
```

Figure 2-3 Extract File

3. Execute chmod command to configure permissions for install.sh in the installation directory.

```
[root@localhost DeviceGateway]# ll
total 217292
-rw-rw-r-- 1 1002 1007 1163592 Jul 18 20:58 7za
drwxrwxr-x 4 1002 1007 42 Jul 18 20:58 apps
-rw-rw-r-- 1 1002 1007 3836 Jul 18 20:58 Config_Template.xml
-rw-rw-r-- 1 1002 1007 899 Jul 18 20:58 ConfigUpgrade.sh
-rw-rw-r-- 1 1002 1007 31400 Jul 18 20:58 DeviceGatewayGuard
-rw-rw-r-- 1 1002 1007 8944 Jul 18 20:58 DeviceGatewayService
-rw-rw-r-- 1 1002 1007 457 Jul 18 20:58 DeviceGatewayService.hservice
drwxrwxr-x 7 1002 1007 147 Jul 18 20:58 drivers
drwxrwxr-x 2 1002 1007 55 Jul 18 20:58 HCAapSDKCom
-rw-r--r-- 1 root root 175272026 Jul 19 10:12 HikDeviceGateway_V1.6.0.2Build20220718_Linux64.tar.gz
-rw-rw-r-- 1 1002 1007 7273 Jul 18 20:58 install.sh
-rw-rw-r-- 1 1002 1007 206 Jul 18 20:58 ISAPICongif_Template.xml
-rw-rw-r-- 1 1002 1007 7578 Jul 18 20:58 ivmsservice.sh
-rw-rw-r-- 1 1002 1007 41905 Jul 18 20:58 libboost_chrono.so
-rw-rw-r-- 1 1002 1007 41905 Jul 18 20:58 libboost_chrono.so.1.60.0
-rw-rw-r-- 1 1002 1007 1258950 Jul 18 20:58 libboost_regex.so
-rw-rw-r-- 1 1002 1007 1258950 Jul 18 20:58 libboost_regex.so.1.60.0
```

Figure 2-4 Before Configuration

```
[root@localhost DeviceGateway]# chmod 777 ./install.sh
[root@localhost DeviceGateway]# ll
total 217292
-rw-rw-r-- 1 1002 1007 1163592 Jul 18 20:58 7za
drwxrwxr-x 4 1002 1007 42 Jul 18 20:58 apps
-rw-rw-r-- 1 1002 1007 3836 Jul 18 20:58 Config_Template.xml
-rw-rw-r-- 1 1002 1007 899 Jul 18 20:58 ConfigUpgrade.sh
-rw-rw-r-- 1 1002 1007 31400 Jul 18 20:58 DeviceGatewayGuard
-rw-rw-r-- 1 1002 1007 8944 Jul 18 20:58 DeviceGatewayService
-rw-rw-r-- 1 1002 1007 457 Jul 18 20:58 DeviceGatewayService.hservice
drwxrwxr-x 7 1002 1007 147 Jul 18 20:58 drivers
drwxrwxr-x 2 1002 1007 55 Jul 18 20:58 HCApSDKCom
-rw-rw-r-- 1 root root 175272026 Jul 19 10:12 HikDeviceGateway_V1.6.0.2Build20220718_Linux64.tar.gz
-rwxrwxrwx 1 1002 1007 7273 Jul 18 20:58 install.sh
-rw-rw-r-- 1 1002 1007 298 Jul 18 20:58 ISAPIConfig_Template.xml
-rw-rw-r-- 1 1002 1007 7570 Jul 18 20:58 iwmService.sh
-rw-rw-r-- 1 1002 1007 41905 Jul 18 20:58 libboost_chrono.so
-rw-rw-r-- 1 1002 1007 41905 Jul 18 20:58 libboost_chrono.so.1.60.0
```

Figure 2-5 After Configuration

4. Execute istall.sh to install the Device Gateway.
 - a. (Optional) Execute --help of the install.sh script to view the available options.

```
[root@localhost DeviceGateway]# ./install.sh --help
Usage:
./install.sh [--port=port number] [--path=the path of legacy configuration file]
Options:
--port=port number      HTTP port, if you enter nothing, the default port will be used.
--path=the path of legacy configuration file      it is the path of legacy configuration file. If there are any legacy configuration files, you can enter the path of it.
[root@localhost DeviceGateway]#
```

Figure 2-6 Options

- b. (Optional) You can configure --port of the install.sh to set the HTTP port number which you use to visit the Device Gateway. The port number is 80 by default.
 - c. (Optional) You can configure --path of the install.sh to set the directory of legacy files. If there are any legacy files including device and the Device Gateway parameters, enter the path of it so that you do not need to configure it again.
 - d. (Optional) You can also install without options.

```
[root@localhost DeviceGateway]# ./install.sh
checking ports completed. Port 80 will be used.
hpr tls index[0]
schina GetAdapterInfo_Inter_Posix link: 1 interface: ens192
schina GetAdapterInfo_Inter_Posix link: 1 interface: lo
recvfrom end. len [1340]
mac[0:0:0:0:0:0] index[1]
mac[0:c:20:7d:63:a5] index[2]
recvfrom end. len [20]
recvfrom end. len [144]
ipv6[00::00:00:00:00] index[1]
ipv6[fe80::00:00:00:f564] index[2]
recvfrom end. len [20]
loop[2] find 2 mac and 2 ip
schina get ipv6[0000] index[1]
schina get ipv6[fe80] index[2]
/proc/11022/cmdline
./DeviceGatewayService-install
please wait, install DeviceGatewayService service may take a few minutes...
0+1 records in
0+1 records out
14 bytes (14 B) copied, 5.0351e-05 s, 278 kB/s
setenforce: SELinux is disabled
install DeviceGatewayService service successfully.
Port rules are added to firewalld by default.
success
```

Figure 2-7 No Options



Note

- You need to run the Device Gateway as the administrator.
- After installation, the system parameters will be changed by default: the DefaultLimitNOFILE in /etc/systemd/system.conf will be changed to 1000000, and SELinux will be disabled.
- When you install the Device Gateway, you can automatically get all permissions of the files under the installation directory to ensure that the Device Gateway works well.
- When you install the Device Gateway, the default ports of firewall will be automatically used. The ports are as follows:

Hik Device Gateway User Manual

Port	Number
tcp	80 (the HTTP port you set), 443, 554, 7091, 7661-7667, 15000-17000
udp	7661, 7662, 15000-17000

```
[root@localhost DeviceGateway]# firewall-cmd --list-port
22/tcp 80/tcp 443/tcp 7661/tcp 7661/udp 554/tcp 7663/tcp 7665/tcp 7666/tcp 7664/tcp 15000-17000/tcp 15000-17000/udp 27000/tcp 7667/tcp 88/tcp 7091/tcp 7661-7667/tcp 7662/udp 28000/t
cp 8000/tcp 27801/tcp 28001/tcp 17664/tcp
```

Figure 2-8 Ports

- Execute status.sh to view the Device Gateway status.
- Execute start.sh to start the Device Gateway which is in stopped status, and execute stop.sh to stop the Device Gateway which is in running status.

```
[root@localhost DeviceGateway]# ./status.sh
DeviceGatewayService.service - SYSV: DeviceGatewayService
Loaded: loaded (/etc/rc.d/init.d/DeviceGatewayService; bad; vendor preset: disabled)
Active: active (running) since Tue 2022-07-19 11:58:07 +08; 7min ago
Docs: man:systemd-sysv-generator(8)
Process: 11141 ExecStart=/etc/rc.d/init.d/DeviceGatewayService start (code=exited, status=0/SUCCESS)
CGroup: /system.slice/DeviceGatewayService.service
└─1150 /opt/test/DeviceGateway/DeviceGatewayService -service -instance=DeviceGatewayService
└─11308 /opt/test/DeviceGateway/apps/das_media_x64/stream/das_media rtsp port=554;ehomeMinStreamPort=15000;ehomeMaxStreamPort=17000;ehomeV5StreamPort=7664;ehomeV5PlayB...
└─11310 /opt/test/DeviceGateway/apps/pss_x64/pss pssDownloadPort=10081;controlPort=30001;operationPort=30002;alarmPort=30003;id=app_picture_storage_server_1.0.0;index=...
└─11745 /opt/test/DeviceGateway/drivers/drv_ehome2_video_x64/bin/vag/drv_ehome2_video ;controlPort=30001;operationPort=30002;alarmPort=30003;id=drv_ehome2_video_x64.1.0;in...
└─11747 /opt/test/DeviceGateway/drivers/drv_ehome5_acs_x64/bin/vag/drv_ehome5_acs ;controlPort=30001;operationPort=30002;alarmPort=30003;id=drv_ehome5_acs_x64.1.0.0;in...
└─11748 /opt/test/DeviceGateway/drivers/drv_ehome5_video_x64/bin/vag/drv_ehome5_video ;controlPort=30001;operationPort=30002;alarmPort=30003;id=drv_ehome5_video_x64.1.0.0;in...
└─11749 /opt/test/DeviceGateway/drivers/drv_isapi_acs_x64/bin/vag/drv_isapi_acs ;controlPort=30001;operationPort=30002;alarmPort=30003;id=drv_isapi_acs_x64.1.0.0;index=...
└─11752 /opt/test/DeviceGateway/drivers/reg_ehome_register_srv_x64/bin/ehome_reg_srv/RegisterService ;controlPort=30001;operationPort=30002;alarmPort=30003;id=reg_ehome_reg...
└─12163 nginx: master process /opt/test/DeviceGateway/nginx/DeviceGateway-nginx -p /opt/test/DeviceGateway/nginx
└─12164 nginx: worker process

Jul 19 11:58:07 localhost.localdomain DeviceGatewayService[11141]: rcvfrom end. len [144]
Jul 19 11:58:07 localhost.localdomain DeviceGatewayService[11141]: ipv6[00:00:00:00:00] index[1]
Jul 19 11:58:07 localhost.localdomain DeviceGatewayService[11141]: ipv6[fe80::00:00:00:f564] index[2]
Jul 19 11:58:07 localhost.localdomain DeviceGatewayService[11141]: rcvfrom end. len [20]
Jul 19 11:58:07 localhost.localdomain DeviceGatewayService[11141]: schina get ipv6[0000] index[1]
Jul 19 11:58:07 localhost.localdomain DeviceGatewayService[11141]: schina get ipv6[fe80] index[2]
Jul 19 11:58:07 localhost.localdomain DeviceGatewayService[11141]: /proc/11149/cmdline
Jul 19 11:58:07 localhost.localdomain DeviceGatewayService[11141]: /opt/test/DeviceGateway/DeviceGatewayService.service-instance=DeviceGatewayService
Jul 19 11:58:07 localhost.localdomain DeviceGatewayService[11141]: [578 blob data]
Jul 19 11:58:07 localhost.localdomain systemd[1]: Started SYSV: DeviceGatewayService.
```

Figure 2-9 Current Status


- Execute uninstall.sh to uninstall the Device Gateway. The files in the installation directory will all be kept after uninstillation, and you can manually delete them.

```
[root@localhost DeviceGateway]# ./uninstall.sh
The files in the directory will all be kept after uninstillation.
hpr tls index[0]
schina GetAdapterInfo Inter_Posix Link: 1 interface: ens192
schina GetAdapterInfo Inter_Posix Link: 1 interface: lo
rcvfrom end. len [1348]
mac[0:0:0:0:0:0] index[1]
mac[8:c:29:7d:63:a5] index[2]
rcvfrom end. len [20]
rcvfrom end. len [144]
ipv6[00:00:00:00:00] index[1]
ipv6[fe80::00:00:00:f564] index[2]
rcvfrom end. len [20]
loop[2] find 2 mac and 2 ip
schina get ipv6[0000] index[1]
schina get ipv6[fe80] index[2]
/proc/29822/cmdline
./DeviceGatewayService-uninstall
please wait, uninstall DeviceGatewayService service may take a few minutes...
uninstall DeviceGatewayService service successfully.
[root@localhost DeviceGateway]# ls
7za                                install.sh                          libDriverMgr.so                   libHGGatewayProtocol.so          libIdentify.so                   libr.so.1
apps                               ISAPIConfig.xml                    libDriverMetaLib.so               libHGHttpService.so             libjsoncpp.so                   log4cxx.properties
Config.db3                         ivmservice.sh                     libGuardClient.so                 libHGISAPIMgrBus.so             libjsoncpp.so.20                logs
ConfigUpgrade.sh                  libboost_chrono.so                 libHCISUPSS.so                   libHGISAPIProtocol.so           libjson.so                      nginx
Config.xml                        libboost_chrono.so.1.60.0          libHGNetUtils.so                 libHGMediaBus.so               libsqlite3.so                   PictureStorageServer.db
Device.db3                        libboost_regex.so                  libHGAlarmBus.so                 libHGServiceMgr.so             libsqlite3.so.0                 PrivateConfig.xml
DeviceGatewayGuard                 libboost_regex.so.1.60.0           libHGAlarmSendBus.so             libhlog.so                      libsqlite3.so                   protocol_debug
DeviceGatewayService               libboost_system.so                 libHGBase.so                     libhplug.so                    libssl.so                       restart.sh
DeviceGatewayService.hsresource    libboost_system.so.1.60.0          libHGDeviceCfgBus.so             libhprocessclient.so           libssl.so.1.0.0                sfrzcfg
drivers                            libboost_thread.so                 libHGDeviceMgrBus.so             libhprocess.so                 libtinyxml.so                   start.sh
HCAppSDKCom                       libboost_thread.so.1.60.0          libHGDeviceMgr.so                libhpr.so                      libtrace.so                     status.sh
HikDeviceGateway_V1.6.0.28Build20220718_Linuxx64.tar.gz libcrypto.so                       libHGGatewayCfgBus.so            libhservice.so                 libutils.so                     stop.sh
hprocess.xml                      libcrypto.so.1.0.0                libHGGatewayCfg.so               libiconv.so.2                  libr.so                          uninstall.sh
```

Figure 2-10 Uninstall Device Gateway

2.4 Activate Device Gateway

By default, the administrator user name is set to **admin** by default. When you log in to the Device Gateway for the first time, you are required to create a password for the admin user to activate the service.

Scenario	Activation Process
Install the Device Gateway on Windows and activate it on your local PC.	<p>After the Device Gateway is installed, the login page will automatically open in your default web browser.</p> <ol style="list-style-type: none"> 1. Enter the password and confirm password for the admin user. 2. Select Activate. 3. Select Configure to enter the Configuration page, and configure the parameters.
<ul style="list-style-type: none"> • Install the Device Gateway on Windows and activate it remotely. • Install the Device Gateway on Linux 	<ol style="list-style-type: none"> 1. Enter the address of the computer or server running with the Device Gateway service and port number in the address bar of the web browser, and press Enter key. <p> Note</p> <p>If the IP address of your computer is 172.6.21.96, and the port number is 80, enter <i>http://172.6.21.96:80</i> in the address bar.</p> <ol style="list-style-type: none"> 2. Enter the password and confirm password for the admin user. 3. Select Activate. 4. Select Configure to enter the Configuration page, and configure the parameters.

Chapter 3 Step 2: Add Devices

You can add and manage ISUP-enabled encoding devices and ISUP5.0/ISAPI-enabled access control devices for intergration with third-party platforms. This topic will guide you through adding encoding devices.

Steps

1. Configure the port mapping to ensure the device is connected normally.
 - 1) Select **Configuration** → **Network Settings** → **NAT** → **Device Connection Port** → **Enable** .
 - 2) Configure the external port to ensure the ports of the Device Gateway and those of your network devices are consistent.

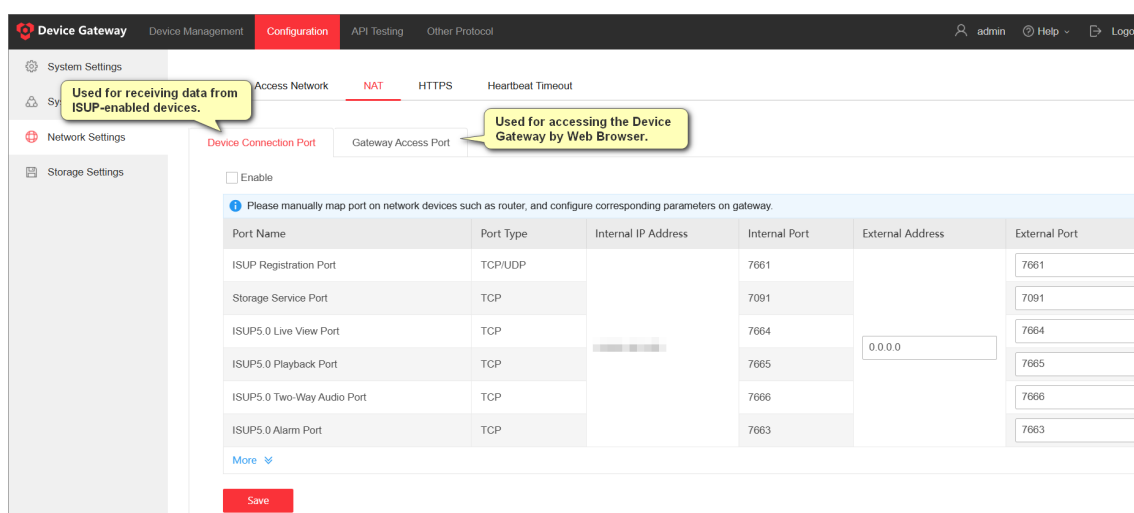


Figure 3-1 Port Mapping

Note

We recommend **15000-17000** for the external ISUP2.0 stream port.

2. Add devices in the following ways.
 - For ISUP5.0-enabled devices in the pre-registered device list, select **Add to Device List** **Add to Device List**, and enter the key.
 - To manually add devices, select **Add**, set the adding mode and protocol type, and configure other parameters.

Note

If you manually add the devices in the pre-registered device list, these devices will be removed from the pre-registered device list when they are added.

What to do next

Select a device to check if the available APIs work well. For details, see **Step 3: Test APIs** .

Chapter 4 Step 3: Test APIs

After adding devices, you can select a device to test the available APIs such as adding face pictures and starting live view of access control devices. This topic will guide you through testing the API of adding face pictures to the face picture library, the API of starting live view, the API of starting playback, and the API of starting the two-way audio.

4.1 Test Transmitting Device ISAPI

This section will introduce how to add face pictures to the face picture library.

Steps

1. Select **API Testing → General Protocol → Transmit Device ISAPI → Transmit ISAPI**.
2. Click **Select** to select a encoding device supported adding face pictures. You can select a device by the device ID and device name.
After you selecting a device, **<uuid>** in the request URL will be automatically filled.
3. Get the information of the face picture library such as **FDID**.
 - 1) Set the request method to **Get**.
 - 2) Replace **<ISAPIURI>** with **/ISAPI/Intelligent/FDLib**.
 - 3) **Optional**: Set the timeout.
 - 4) select **Send Request**.
4. After you get the information, upload face pictures to the library, call **/ISAPI/Intelligent/FDLib/pictureUpload?format=json** to upload face pictures to the library.
 - 1) Select **Video Protocol → Device Operation → Add Face Picture**.
 - 2) Enter **FDID** you get in the step 3.
 - 3) Upload a face picture as an attachment.
 - 4) Select **Send Request**.



Note

The following GIF (The PDF version is not supported) will help you visualize the testing process.

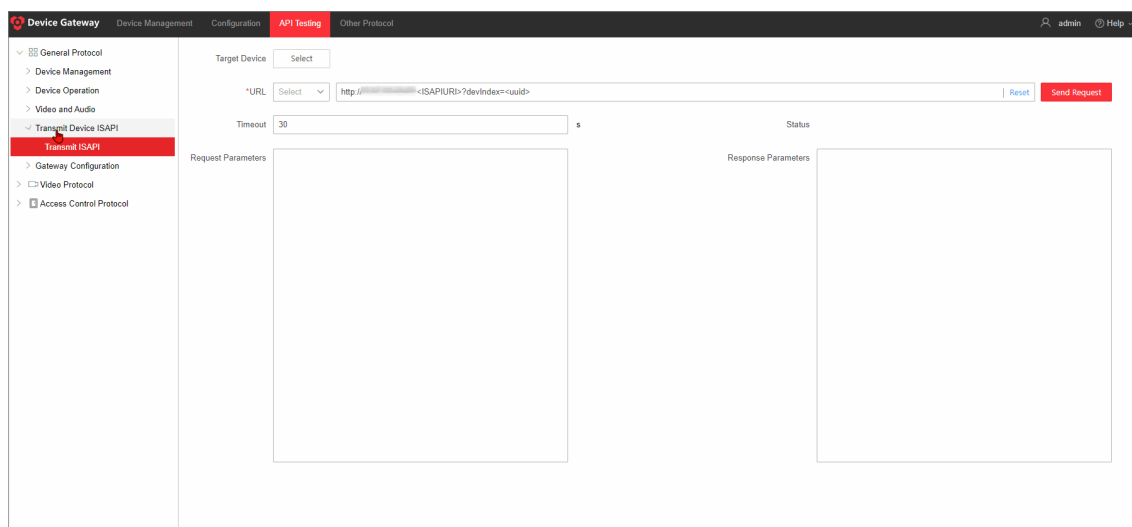


Figure 4-1 Add Face Pictures to Library

4.2 Test General Protocol

This section will introduce how to test the API of starting the live view of encoding devices and access control devices. You can only preview videos under 1080p resolution on the Firefox, Chrome, or Edge browser. Only G.711 a-law, G.711 u-law, and ACC codecs are supported on the web page.

Steps

1. Select **API Testing** → **General Protocol** → **Video and Audio** → **Start Live View** .
2. Click **Select** to select an access control device supporting live view.

The <uuid> in the request URL will be automatically replaced.

3. **Optional:** To capture pictures on ISUP2.0 devices, go to **Configuration** → **System Settings** , and enable **Alarm Forwarding**.
4. Set the request parameters, and then select **Send Request** → **Start Live View** .

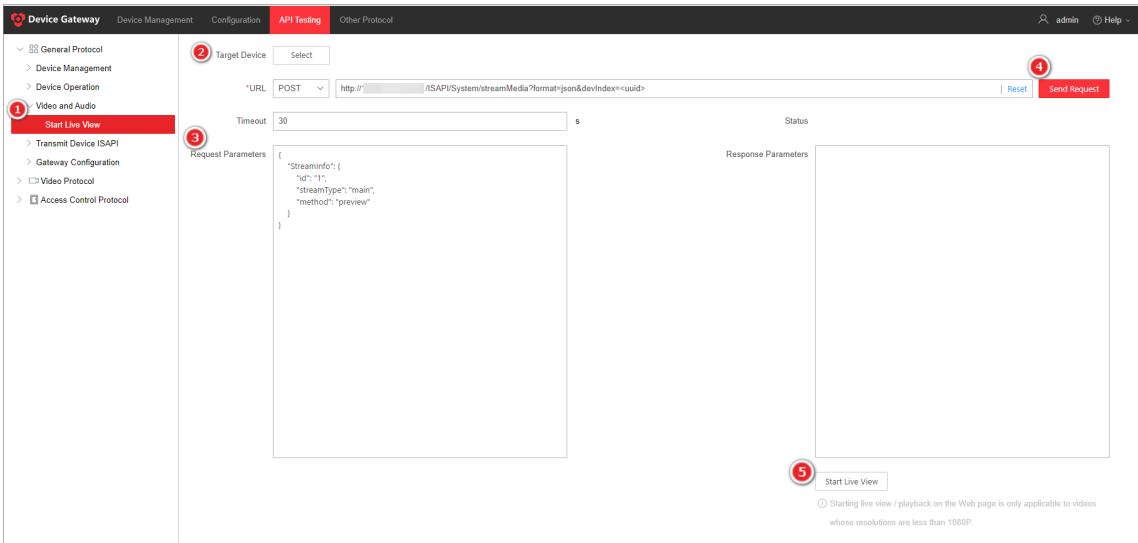


Figure 4-2 Start Live View

5. **Optional:** Perform the following operations as needed.

Operation	Description
Start/Pause Live View	Click / to start or pause live view.
Start/Stop Recording	Click / to start or stop recording. Note This function is not supported on Firefox.
Audio On/Off	Click / to turn the audio on or off.
Capture Picture (BMP)	Click to capture a picture in BMP.
Capture Picture (JPEG)	Click to capture a picture in JPEG.

4.3 Test Video Protocol

This section will introduce how to test the API of starting the playback and two-way audio. You can only play back videos under 1080p resolution on the Firefox, Chrome, or Edge browser. Only G.711 a-law, G.711 u-law, and ACC codecs are supported on the web page.

4.3.1 Test Video Playback

Steps

- 1. Select **API Testing → Video Protocol → Video and Audio → Start Playback** .

2. Click **Select** to select a device supporting playback.
3. Set the start time and end time in the Request Parameters.
4. Set the request parameters, and then select **Send Request** → **Start Playback** .

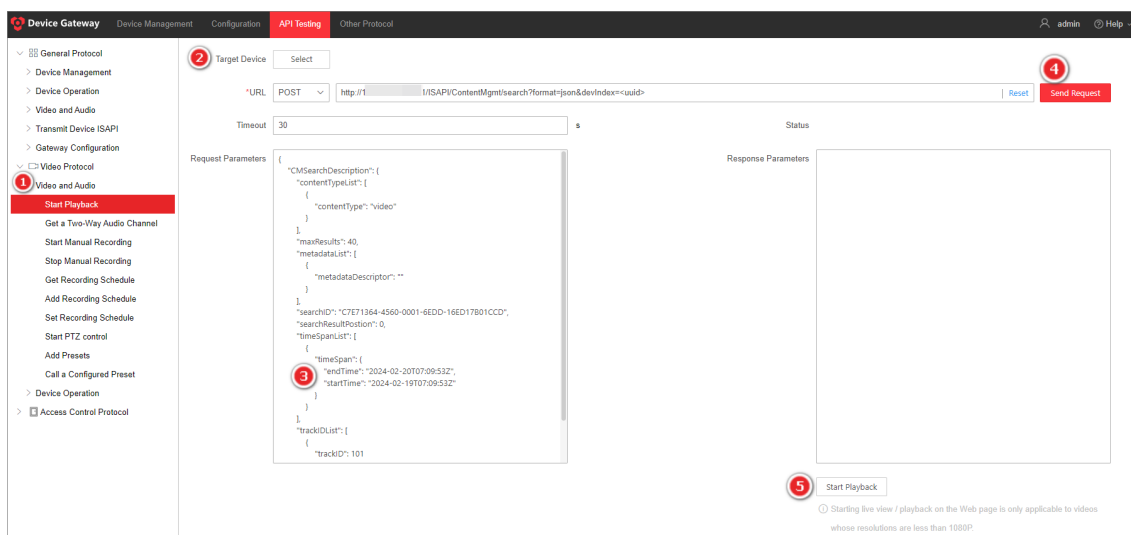












Figure 4-3 Test Video Playback

5. Perform the following operations as needed.

Operation	Description
Start/Pause Playback	Click  /  to start or pause playback.
Start/Stop Recording	Click  /  to start or stop recording. <div>  Note This function is not supported on Firefox. </div>
Fast/Slow Forward	Click  /  to play the recorded video slower or faster.
Audio On/Off	Click  /  to turn the audio on or off.
Select Video	Click  in the upper-right corner of the playback page, and select a video to play it. By default, the first video within the set time period will be automatically played.

4.3.2 Test Two-Way Audio

You can test the two-way audio only when you log in to the Device Gateway via HTTPS.

Steps

1. Set HTTPS.
 - 1) Set the HTTPS certificate. For details, see [Set HTTPS](#) .

- 2) Go to **Configuration → Network Settings → Port → Gateway Access Port** to check if the HTTPS port is in the normal status.
- 3) Log in to the Device Gateway by entering the HTTPS URL.
2. Test the two-way audio.
 - 1) Select **API Testing → Video Protocol → Video and Audio → Get a Two-Way Audio Channel** .
 - 2) Click **Select** to select a device supporting two-way audio.
 - 3) Set the request parameters, and then select **Send Request → Start/Stop Two-Way Audio** .

Chapter 5 Other Configuration

5.1 ISAPI Management

To achieve the communication between the Device Gateway and the third-party platforms over the ISAPI protocol, you need to ensure that the parameters configured on the Device Gateway are consistent with those of the third-party platform.

Enable ISAPI

The ISAPI function is disabled by default. You can enable this function for the third-party platform (which supports ISAPI protocol, such as Milestone XProtect platform) to access the devices added to the Device Gateway.


Select **Other Protocol** → **ISAPI** , and then enable **ISAPI**

Device Name	Device ID	Device Model	Supervision	HTTP Port	RTSP Port	Operation
a00003	a00003		Online	27002	28000	
a00004	a00004		Online	27001	28001	

Figure 5-1 ISAPI Management

Bind Device with the Device Gateway

In order for a third-party platform (such as Milestone) to access ISUP devices, you need to bind devices with the Device Gateway, so that the Device Gateway can assign ISAPI ports to the bound devices.

1. Select **Add** to enter the Bind Device page.
2. Select the unbound device(s) in the device list.
3. Select  to add the selected device(s) to the selected list.
4. Check the device(s) to be bound, and select **OK**.



Note

Up to 200 devices can be bound.



Note

- Port occupation by another program may cause the failure of device binding, so make sure you have ended the program occupying the port(s) before you rebind the device.
- If the program cannot be ended, you can unbind the device first, and then bind the device again. In this case, the Device Gateway will assign new ports to the device.
- The available HTTP port ranges from 27000 to 27800, while the available RTSP port ranges from 28000 to 28800.

- Only ISUP devices can be bound with the Device Gateway.
 - You need to add corresponding firewall rules after binding ports for the Device Gateway on Linux, or the Device Gateway may be unable to start.
 - You need to enable **Alarm Forwarding** if you want to arm the bound devices.
-

5.2 Basic Configuration

The configuration module provides basic settings such as editing system information, setting network, searching operation logs, enabling alarm forwarding, and setting storage pathway. This section will introduce some major configurations.

Forward Alarm

If you enable this function, the alarm forwarding port will be used to forward the alarms reported by ISUP 5.0 devices to Hik Device Gateway. The Device Gateway can forward alarms and events in the XML format reported by ISUP5.0-enabled devices. This function is disabled by default.

You can enable **Alarm Forwarding** and ensure that the alarm forwarding port is available.

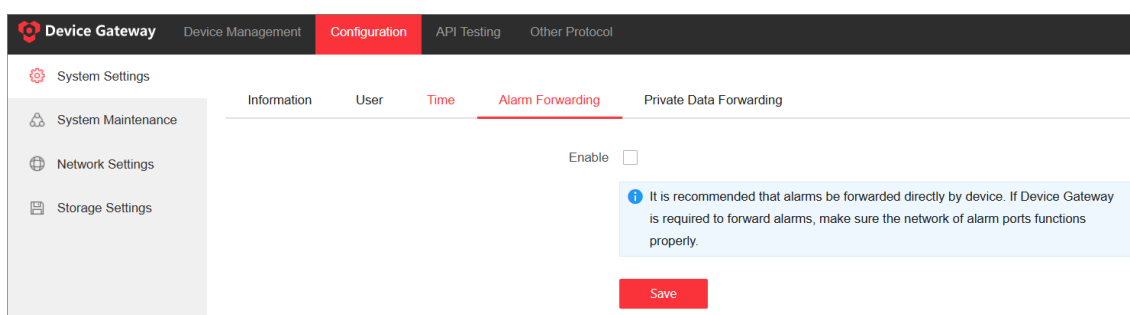


Figure 5-2 Forward Alarm

Forward Private Data

Support forwarding private data contained in streams of live view and playback (such as bounding box annotations and attributes of detected objects). This function is disabled by default.

Go to **Configuration → System Settings → Private Data Forwarding** .

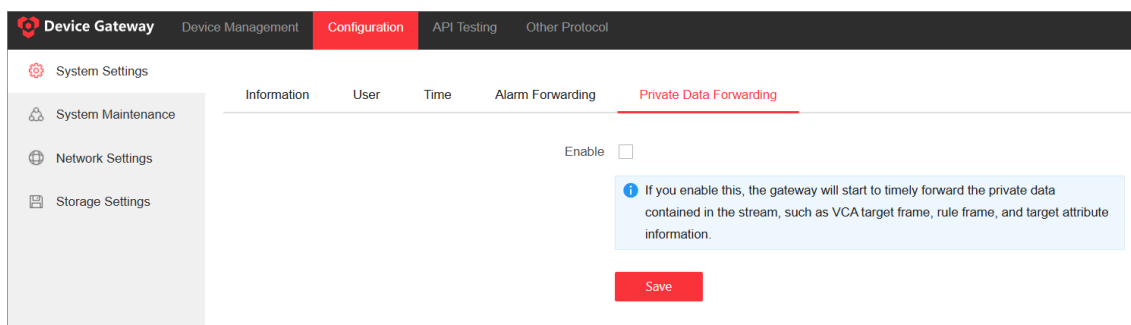


Figure 5-3 Forward Private Data

Export System Log

Export the system log for debugging.

1. Select **Configuration** → **System Maintenance** → **Log**.
2. Select a log level, and select **Export** to export the log to your local PC.



Note

If you select the log level to **Debug**, logs with a higher log level will also be exported.

3. (Optional) Select **Save** to save the configuration such as the log level.

Record Device Operation Log

To prevent log file bloat, the system supports configuring whether to record the device operation logs of testing available APIs and API passthrough for security audit and troubleshooting. If enabled, it stores operation records for existing devices (deleted devices are not recorded) and automatically cleans up logs every 180 days. This function is disabled by default.

Go to **Configuration** → **System Maintenance** → **Device Operation Log**.

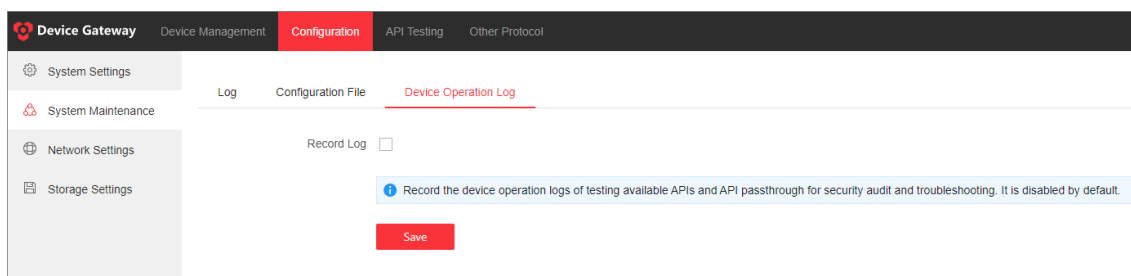


Figure 5-4 Record Log

Set Port

If the default ports are used by other services, you can edit them.

Select **Configuration** → **Network Settings** → **Port**, edit the gateway access port numbers and device port numbers and save the port settings. The port status indicates whether the ports are already occupied.

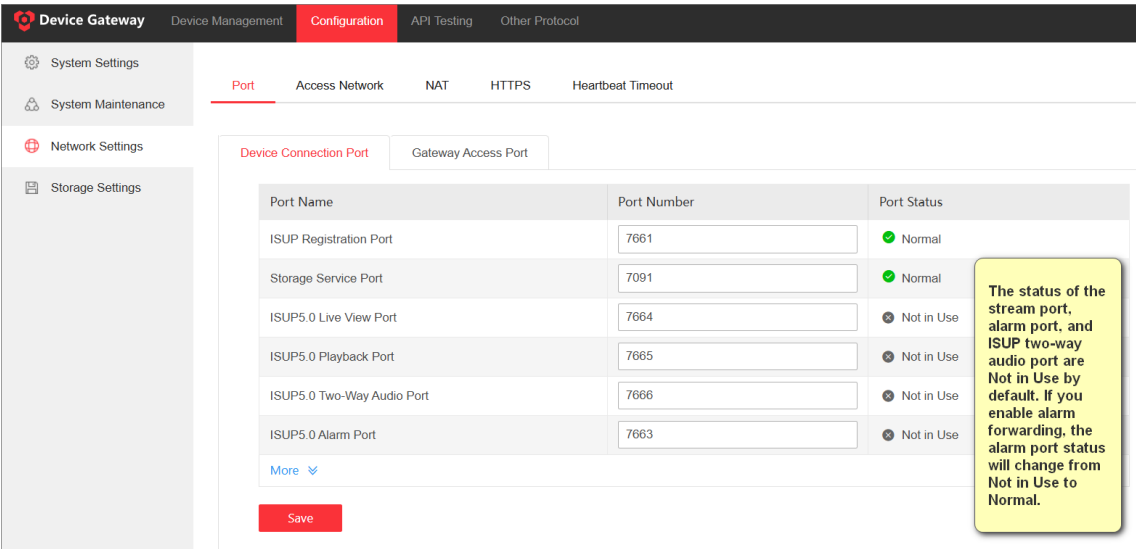



Figure 5-5 Port Settings

Set HTTPS

HTTPS provides authentication of the web site and its associated web server, which protects against attacks. For example, if you set the port number as 443 and the IP address is 192.168.1.64, you may access the device by entering https://192.168.1.64:443 via a web browser. The Device Gateway provides three installing methods of HTTPS certificate.

- 1. Select **Configuration** → **Network Settings** → **HTTPS** to enter the HTTPS Setting page.
- 2. Check one of the installation methods to set HTTPS certificate.

Method	Description
Create self-signed certificate.	Enter the Country, Domain/IP, Validity and other information, and then click Save .

Method	Description
	 Note If you already had a certificate installed, the "Create self-signed certificate." is grayed out.
Signed certificate is available, start the installation now.	Click Browse to select a signed certificate saved in the PC, and then click Install .
Create the certificate request first and continue the installation.	a. Select Create to create the certificate request. Enter the required information in the pop-up window and click OK to save. b. Download the certificate request and submit it to the trusted certificate authority for signature. c. After receiving the signed valid certificate, select Browse to select the downloaded certificate saved in the PC, and then select Install .

Heartbeat Timeout

To prevent frequent device disconnections due to network instability, Device Gateway supports configuring heartbeat timeout parameters. By default, the heartbeat interval is set to 30 seconds with 3 retries to determine if a device is offline. This means that the device accessed by ISUP protocol will send a heartbeat packet every 30 seconds. If Device Gateway does not receive a heartbeat packet within 30 seconds, it counts as one timeout. After 3 consecutive timeouts, the device is considered offline.

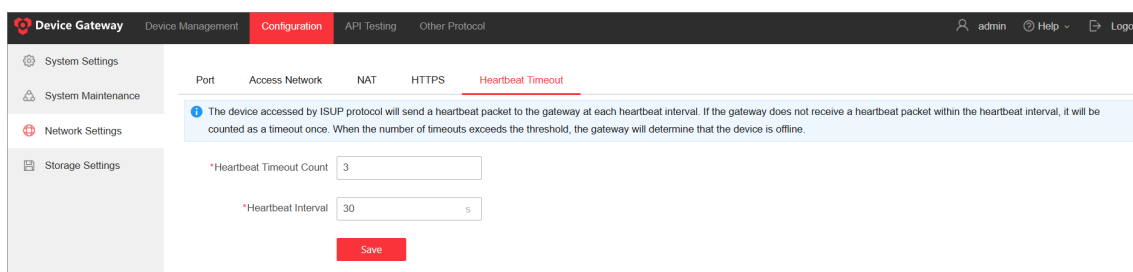


Figure 5-6 Heartbeat Timeout



See Far, Go Further