Hik-Gateway

User Manual

Legal Information and Symbol Conventions

Legal Information

User Manual

©2019 Hangzhou Hikvision Digital Technology Co., Ltd.

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.
Please use this user manual under the guidance of professionals.

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. 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.

Symbol Conventions

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

Symbol	Description
Danger	Indicates a hazardous situation which, if not avoided, will or could result in death or serious injury.
Caution	Indicates a potentially hazardous situation which, if not avoided, could result in equipment damage, data loss, performance degradation, or unexpected results.
Note	Provides additional information to emphasize or supplement important points of the main text.

Contents

Chapter 1 Overview

1.1 Introduction

As a protocol converter, the Hik-Gateway connects Hikvision products and third-party systems for data transmission, through LAN or WAN.

The Hik-Gateway manages EHome devices (including encoding devices and security control panels supporting EHome protocol) and connects to a third-party system (including alarm receiving center (hereinafter referred to as ARC)). The Hik-Gateway trans-forwards data from encoding devices to a third-party system, and trans-forwards alarm notifications and alarm-related videos from security control panels to an ARC.

This manual guides you to configure the Hik-Gateway service. To ensure a proper usage and stability of the Hik-Gateway service, refer to the contents below and read the manual carefully before installation and operation.

1.2 Running Environment

The following is recommended system requirement for running the Hik-Gateway.

Operating System

Microsoft Windows 10 (64-bit) / Windows Server 2012 R2 (64-bit) / Windows Server 2016 (64-bit)

Note

For Windows Server 2012 R2 (64-bit), the patch KB2999226 is required to be installed.

CPU

Intel Core I5 @ 3.0 GHz or above

RAM

8 GB or above

Chapter 2 Installation

You can install the Hik-Gateway service to your server or PC, and activate the service. Then you can use the service remotely.

2.1 Port Instruction

Before installing Hik-Gateway service, ensure the default ports of the Hik-Gateway are not used by other services, otherwise the Hik-Gateway service will be unavailable.

The default ports are listed as follows.

- 80 (TCP) : HTTP port
- 443 (TCP) : HTTPS port
- 554 (TCP) : RSTP port, used for getting stream from the Hik-Gateway during live view, remote playback, and two-way audio.
- 7661 (TCP/UDP) : used for device registration to the Hik-Gateway by EHome protocol.
- 7662 (TCP/UDP) : used for devices' sending alarm notifications to the Hik-Gateway by EHome protocol.
- 15000 to 17000 (TCP) : used for forwarding stream from EHome devices to the Hik-Gateway.
- 7091 (TCP) : used for sending alarm-related videos from device to the Hik-Gateway by EHome protocol.

Note

Scan the QR code below to get more details.

2.2 Install Hik-Gateway

You can install the Hik-Gateway service on a computer or server. After that, you can start the service, stop the service or exit the service by watchdog.

Steps

1. Right-click the program file and run as the administrator to enter the welcome panel of the InstallShield Wizard.
2. Click **Next** to start the InstallShield Wizard.
3. Click **Change...** and select a proper directory as required to install the service.
4. Click **Next** to continue.
5. Read the pre-install information, and click **Install** to begin the installation.
6. Read the post-install information and click **Finish** to complete the installation.

Result

After successful installation, 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, start the service, or exist the service.

Note

If you install Hik-Gateway remotely, you need to log into the local computer to show the Watchdog service.

2.3 Activate Hik-Gateway

By default, Hik-Gateway predefined the administrator user named **admin**. When you log in to Hik-Gateway for the first time, you are required to create a password for the admin user to activate Hik-Gateway before you can properly configure and operate.

Before You Start

Make sure you have installed the Hik-Gateway service.

Steps

1. Enter the address of the computer or server running with Hik-Gateway service and port number in the address bar of the web browser, and press **Enter** key.

   Note

   The default port is 80. For configuring the port number, see ***Edit Port*** for details.

   Example

   If the IP address of the computer running Hik-Gateway service is 172.6.21.96, and the port number is 80, and you should enter ***http://172.6.21.96:80*** in the address bar.

2. Enter the password and confirm password for the admin user in the pop-up Activate Hik-Gateway window.

   Caution

   The password strength of the device can be automatically checked. We highly recommend you change the password of your own choosing (using a minimum of 8 characters, including at least

three kinds of following categories: 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.
Proper configuration of all passwords and other security settings is the responsibility of the installer and/or end-user.

3. Click **Activate**.

Chapter 3 Device Management

Encoding devices (including mobile device, body camera, portable speed dome, etc) and security control panels can be added to the Hik-Gateway via the Web Client. You can manage them on the Web Client, including adding, editing, deleting, refreshing device information, etc.

Note

Up to 10,000 devices can be added.

3.1 Add Encoding Device by EHome Protocol

You can add the encoding device (such as body camera, portable speed dome, mobile device, etc.) which has been registered to Hik-Gateway service for converting the device's protocol. The third-party system can access the device by connecting to the Hik-Gateway.

Steps

1. Click **Device Management → Encoding Device** to enter the Encoding Device page.
2. Click **Add** to enter the Add Device page.
3. Select **EHome** as the adding mode.
4. Enter the required information.

   Device ID

   The Device ID you defined on the device for registering it to the Hik-Gateway service.

   Device Name

   You can customize the device name.
5. Click **OK** to add the device.
6. Perform the following operation(s) after adding the device.

Edit Device	Click in the Operation column to edit the name and ID of a device.
Delete Device	Click × in the Operation column to delete a device. **Note** You can also check multiple devices and click **Delete** to delete them in a batch.
Refresh Device Information	Click **Refresh** to get updated device information such as device model, device status, and channel number.
View Channel List	Click in the Operation column to view channel list of a device, including encoding channel, alarm input, alarm output, and two-way audio channel.

Note

You can click to edit the name of the online encoding channel.

Search Device Enter a keyword of the device name/model/ID in the search field in the upper-right corner, and then click to search an encoding device.

Filter Device Click to filter online/offline encoding devices.

3.2 Add Encoding Devices in a Batch

When there are multiple encoding devices (such as body camera, portable speed dome, mobile device, etc.) to add, you can enter the device information into a predefined template and then import it to the Hik-Gateway to add them in a batch.

Steps

1. Click **Device Management → Encoding Device** to enter the Encoding Device page.
2. Click **Add** to enter the Add Device page.
3. Select **Batch Import** as the adding mode.
4. Click **Export** and save the predefined template (CSV file) on your PC.
5. Open the exported template file and enter the required information of the devices to be added.

   Device Name

   You can customize the device name.

   Device ID

   The Device ID you defined on the device for registering it to the Hik-Gateway service.

   Note

   Device Name is optional. The device ID will be used as the device name if you do not enter the device name.

6. Click and select the template file.
7. Click **OK** to add the devices in a batch.
8. Perform the following operation(s) after adding the devices.

   Edit Device Click in the Operation column to edit the name and ID of a device.

   Delete Device Click × in the Operation column to delete a device.

   Note

   You can also check multiple devices and click **Delete** to delete them in a batch.

   Refresh Device Information Click **Refresh** to get updated device information such as device model, device status, and channel number.

View Channel List	Click in the Operation column to view channel list of a device, including encoding channel, alarm input, alarm output, and two-way audio channel.
	Note You can click to edit the name of the online encoding channel.
Search Device	Enter a keyword of the device name/model/ID in the search field in the upper-right corner, and then click to search an encoding device.
Filter Device	Click to filter online/offline encoding devices.

3.3 Add Security Control Panel by EHome Protocol

You need to add security control panel to the Hik-Gateway, so that you can get alarm notification and view alarm-related videos by the ARC connected to the Hik-Gateway. After adding a security control panel to the Hik-Gateway, the device information will be displayed on the security control panel page including MAC address, device model, alarm times, visual verification status, offline duration, etc.

Steps

1. Click **Device Management → Security Control Device** to enter the Security Control Panel page.
2. Click **Add** to enter the Add Device page.
3. Select **EHomeV5** as the adding mode.
4. Enter the required information of the security control panel.

   Device Name

   You can customize the device name.

   Account ID

   The account ID you defined on the device for registering it to the Hik-Gateway service.

   EHome Key

   The EHome key you defined on the device for registering it to the Hik-Gateway service.
5. **Optional:** Enable **Visual Verification**.

   Note

   Make sure this function is enabled for video verification via ARC.
6. Click **OK**.

   The added security control panel will be displayed in the device list.

   MAC Address

   The MAC address of the device, which is reported by the device.

   Version

The version of the device.

Device Status

Network connection status of the device.

Visual Verification

Visual verification enabled/disabled.

First Alarm

Occurring time of the first alarm.

Last Alarm

Occurring time of the last alarm.

Alarm Times

The amount of the alarms reported by the device.

Offline Duration (s)

The duration of the device's being offline.

7. Perform the following operation(s) after adding the device.

Edit Device	Click in the Operation column to edit the name, account ID, and EHome key for the device.
Delete Device	Click × in the Operation column to delete a device.
	Note You can also check multiple devices and click **Delete** to delete them in a batch.
Refresh Device Information	Click **Refresh** to get updated device information MAC address, device model, version, device status, visual verification, etc.
Search Device	Enter a keyword of the device /name/model/account ID in the search field in the upper-right corner, and then click to search a security control panel.
Filter Device	Click to filter security control panels by device status and visual verification status.

3.4 Add Security Control Panels in a Batch

When there are multiple security control panels to add to the Hik-Gateway, you can enter the device information in a predefined template and then import it to the Hik-Gateway to add them in a batch.

Steps

1. Click **Device Management → Security Control Device** to enter the Security Control Panel page.

2. Click **Add** to enter the Add Device page.
3. Select **Batch Import** as the adding mode.
4. Click **Export** and save the predefined template (CSV file) on your PC.
5. Open the exported template file and enter the required information of the devices.

Device Name

You can customize the device name.

Note

Device Name is optional. The account ID will be used as the device name if you do not enter the device name.

Account ID

The account ID you defined on the device for registering it to the Hik-Gateway service.

EHome Key

The EHome key you defined on the device for registering it to the Hik-Gateway service.

Visual Verification

If you do not enable this function, the event-related videos cannot be viewed by the ARC when an event is triggered.

6. Click and select the template file.
7. Click **OK** to add the devices in a batch.
8. Perform the following operation(s) after adding the devices.

Edit Device	Click in the Operation column to edit the name, account ID, and EHome key for the device.
Delete Device	Click × in the Operation column to delete a device.
	Note You can also check multiple devices and click **Delete** to delete them in a batch.
Refresh Device Information	Click **Refresh** to get updated device information MAC address, device model, version, device status, visual verification, etc.
Search Device	Enter a keyword of the device /name/model/account ID in the search field in the upper-right corner, and then click to search a security control panel.
Filter Device	Click to filter security control panels by device status and visual verification status.

Chapter 4 Hik-Gateway Configuration

You can configure the Hik-Gateway, such as editing Hik-Gateway name, changing password for admin user, and setting network ports. You can also enable log.

4.1 System Settings

You can set the system parameters, including admin password and Hik-Gateway name.

4.1.1 Configure Hik-Gateway Name

You can view the Hik-Gateway information and edit the Hik-Gateway name according to the actual needs.

Perform this task when you need to configure Hik-Gateway name.

Steps

1. Click **Hik-Gateway Configuration → System Settings → Hik-Gateway Information** to enter the Hik-Gateway Information page.
2. View the Hik-Gateway information, including the version, model, and operating system.
3. Enter a name according to the actual needs.
4. Click **Save**.

4.1.2 Change Password for Admin User

By default, the system predefined the administrator user named admin. You can change password for admin user.

Perform this task when you need to change password for admin user.

Steps

1. Click **Hik-Gateway Configuration → System Settings → User Management** to enter the User Management page.
2. Click **Change** to enter the Change Password page.
3. Enter the old password, password, and confirm password.
4. Click **Save**.

What to do next

You are required to log in to the Hik-Gateway service again.

4.2 System Maintenance

You can enable log and export logs to your local PC.

Steps

1. Click **Hik-Gateway Configuration → System Maintenance** to enter the System Maintenance page.
2. Check **Enable Logging**.
3. Select the log level.

Note

- Only the logs with the log level higher than the configured level can be recorded.
- The log level is **Warning** by default. We recommend setting **Debug** as the log level to make it easier to find error details. If you select **Debug** as the log level, the Hik-Gateway performance will be degraded.

4. Click **Export**.

4.3 Network Settings

You need to configure network parameters of the Hik-Gateway correctly to ensure the normal communication.

Various network configuration services are provided, including port editing, NIC card switching, Network Address Translation (NAT) configuration, and HTTPS certification installation.

4.3.1 Edit Port

Some default ports of the Hik-Gateway can be edited if they are used by other services.

Steps

1. Click **Hik-Gateway Configuration → Network Settings → Port** to enter the editable port page.
2. Edit the ports.

   HTTP Port

   Used for web browser access in HTTP protocol. By default, the HTTP Port is ***80***.

   RTSP Port

   Used for getting stream from Hik-Gateway during live view, remote playback, and two-way audio. By default, the RTSP Port is ***554***.

   HTTPS Port

   By default, the HTTPS Port is ***443***.

3. Click **Save**.

4.3.2 Set NIC for Hik-Gateway

For the Hik-Gateway running on the PC with multiple NICs, you need to select one NIC for communication.

Steps

1. Click **Hik-Gateway Configuration → Network Settings → Access Network** to enter the NIC setting page.
2. Click ⌄ in the **IP Address** column to switch the NIC.
3. Click **Save** to save the settings.

Note

- By default, the Hik-Gateway will restart automatically after saving the settings.
- If you have changed NIC for the Hik-Gateway, make sure the server address configured on the device is the same with the selected NIC.

4.3.3 Set NAT

If port mapping is needed, you need to set the parameters of port mapping on a router beforehand, and then enter the external port number and external IP address on the NAT page.

Steps

1. Click **Hik-Gateway Configuration → Network Settings → NAT** to enter the NAT setting page.
2. Check **Enable** to enable port mapping function.
3. Enter the corresponding external ports and external IP addresses of the Hik-Gateway.
4. Click **Save** to save the settings.

Note

- By default, the Hik-Gateway will restart automatically after saving the settings.
- We recommend ***15000 to 17000*** for external port of the EHome Stream Port.

4.3.4 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 Hik-Gateway provides three installing methods of HTTPS certificate.

Steps

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

Create Self-Signed Certificate	Enter the **Country**, **Domain/IP**, **Validity** and other information, and then click **Save**. **Note** If you already had a certificate installed, the Create Self-signed Certificate is grayed out.
Signed certificate is available, start the installation directly.	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. Click **Create** to create the certificate request. Fill in 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, click **Browse** to select the downloaded certificate saved in the PC, and then click **Install**.

There will be the certificate information after successfully creating and installing the certificate.

3. Check **Enable** to enable the installed certificate.
4. Click **Save** to save the settings.

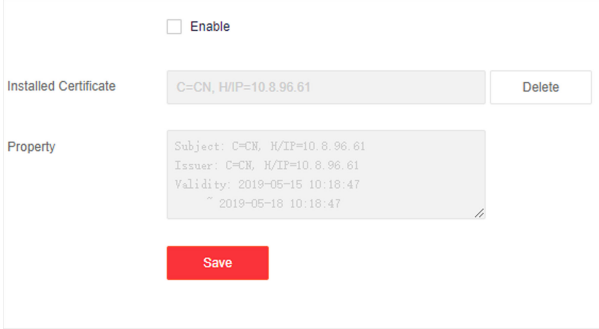

Figure 4-1 Installed Certificate

4.4 ARC Settings

To get alarm notification and alarm-related videos successfully by the ARC connected to the Hik-Gateway, you need to configure the ARC parameters on the Hik-Gateway.

Steps

Note

Only one ARC could be connected to the Hik-Gateway, otherwise the connection between the Hik-Gateway and the ARC will fail.

1. Click **Hik-Gateway Configuration → ARC Settings** to enter the Universal Protocol 1 Settings page.
2. Enter ***1025*** in the **Port** field.
3. Set the **Heartbeat Interval** and the **Reported Event Type**.

   Heartbeat Interval

   For example, if you select 10s, the Hik-Gateway will perform a heartbeat interaction with the ARC every 10 seconds, to make sure a normal work of the Hik-Gateway.

   Reported Event Format

   Select **CID (4-digit account)/CID (10-digit account)/SIA** as the protocol type supported by the ARC. For example, if you select **CID (4-digit account)**, you need to make sure the added security control panels support CID, and the account ID of the security control panels consists of 4 digits.

   Note

   - Select **SIA** as the reported event format for video verification via ARC.
   - When the Hik-Gateway connected to the ARC successfully, the IP address of the ARC will be displayed in the field of the **ARC IP**.

4. Click **Save** to save the settings.

4.5 Select Storage Disk for Alarm-Related Video

When there are triggered alarms, the Hik-Gateway will automatically store the alarm-related videos in the PC, so that you can view the videos by the ARC connected to the Hik-Gateway. You need to configure the storage disk of the videos beforehand.

Steps

Note

The videos could not be stored normally with free space less than 200 MB. Please make enough free space to avoid storage failure. We recommend 50 GB and above.

1. Click **Hik-Gateway Configuration → Storage** to enter the Storage Settings page.

   The available storage disks of the current PC is displayed.
2. Select a disk to store the videos.
3. Click **Save** to save the settings.

   Note

   The downloaded videos will stay in the PC for 48 hours, after which they will be deleted automatically.

   The downloaded videos will be stored in a folder named **HikGatewayStorage**.


See Far, Go Further