



Hik IP Receiver

User Manual

Legal Information and Symbol Conventions

Legal Information

©2020 Hangzhou Hikvision Digital Technology Co., Ltd. All rights reserved.

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 of this Manual at the Hikvision website (<https://www.hikvision.com/>).

Please use this Manual with the guidance and assistance of professionals trained in supporting the Product.

Trademarks

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.

Disclaimer

TO THE MAXIMUM EXTENT PERMITTED BY APPLICABLE LAW, THIS MANUAL 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 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 INSPECTION, 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 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
1.1 Introduction	1
1.2 Running Environment	1
Chapter 2 Installation	2
2.1 Port Instruction	2
2.2 Install Hik IP Receiver	3
2.3 Activate Hik IP Receiver	3
Chapter 3 Device Management	5
3.1 Add Single Security Control Panel	5
3.2 Add Security Control Panels in a Batch	7
Chapter 4 Hik IP Receiver Configuration	9
4.1 System Settings	9
4.1.1 Configure Hik IP Receiver Name	9
4.1.2 Change Password for Admin User	9
4.1.3 Configure Time	9
4.2 System Maintenance	10
4.3 Network Settings	10
4.3.1 Edit Port	10
4.3.2 Set NIC for Hik IP Receiver	11
4.3.3 Set NAT	11
4.3.4 Set HTTPS	12
4.4 Select Storage Disk	13
Chapter 5 Automation Output Management	14
5.1 Configure Sur-Gard Parameters	14
5.2 Check Event Monitor Logs	16
5.3 Configure Sur-Gard Event	16

Chapter 1 Overview

1.1 Introduction

As a protocol converter, the Hik IP Receiver connects Hikvision products and third-party systems (e.g. alarm receiving center (hereinafter referred to as ARC)) for data transmission, through LAN or WAN.

You can add and manage ISUP security control devices via Hik IP Receiver, in order to integrate them to third-party system through ISUP protocol. And then you can use third-party system to perform operations such as receiving alarms from the devices.

This manual guides you to configure the Hik IP Receiver service. To ensure a proper usage and stability of the Hik IP Receiver 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 IP Receiver.

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 i5-7500 @ 3.0 GHz, four-core or above

RAM

8 GB or above

NIC

Gigabit-NIC with latest driver

Chapter 2 Installation

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

2.1 Port Instruction

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

Platform Ports

- 80 (TCP) : HTTP port
- 443 (TCP) : HTTPS port

Device Ports

Port Number	Protocol	Port Description
7661	TCP	Used for registering devices to the Hik IP Receiver by ISUP5.0 protocol.
7662	TCP	Used for sending alarms from ISUP5.0 security control devices to the Hik IP Receiver.
7091	TCP	Used for sending picture data from ISUP5.0 security control devices to the Hik IP Receiver.



Note

Scan the QR code below to get more details.




2.2 Install Hik IP Receiver

You can install the Hik IP Receiver 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. **Optional:** Edit the HTTP port if the port number is conflict, otherwise the installation cannot be continued.
6. Click **Install** to begin the installation.
7. 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 IP Receiver remotely, you need to log into the local computer to show the Watchdog service.
 - A window will pop up asking whether to keep the configuration file when you re-install the Hik IP Receiver. You can choose to keep it or not.
-

2.3 Activate Hik IP Receiver

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

Before You Start

Make sure you have installed the Hik IP Receiver service.

Steps

1. Enter the address of the computer or server running with Hik IP Receiver 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 IP Receiver 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 IP Receiver window.



Note

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.

3. Click **Activate**.

Chapter 3 Device Management

You can add security control devices to the Hik IP Receiver for further third-party platform applications and manage them via Hik IP Receiver, including editing, deleting, refreshing device information, etc.

3.1 Add Single Security Control Panel

You need to add security control panel to the Hik IP Receiver, so that you can get alarm notification and view alarm-related videos by the ARC connected to the Hik IP Receiver. After adding a security control panel to the Hik IP Receiver, 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** → **Security Control Device** to enter the Security Control Panel page.
2. Click **Add** to enter the Add Device page.
3. Select **ISUP5.0** 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 IP Receiver service.

Key

The key you defined on the device for registering it to the Hik IP Receiver service.

5. Enter the **Heartbeat Interval** which should range from 10 to 90 seconds.

Example

When you enter **10** here, the Hik IP Receiver will perform a heartbeat every 10 seconds to make sure the communication between the Hik IP Receiver and the ARC goes well.

6. Enter the heartbeat timeout times in **Heartbeat Timeout** field. The number you enter here should range from 3 to 65535.

Heartbeat Timeout

The total duration of all heartbeats. $\text{Heartbeat Timeout} = \text{Heartbeat Interval} \times \text{Heartbeat Timeout Times}$

Example

When you enter **3** here, the Hik IP Receiver will try again for 3 times if the heartbeat fails. If the third heartbeat retrying fails, the Hik IP Receiver will stop trying.

7. **Optional:** Switch **Visual Verification** on.

Note

Make sure this function is enabled for video verification via ARC.

8. 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.

Supervision

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.

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


Edit Device	Click  in the Operation column to edit the name, account ID, key, heartbeat interval, and heartbeat timeout 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.
----------------------	--

3.2 Add Security Control Panels in a Batch

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

Steps

1. Click **Device → 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 IP Receiver service.

Key

The key you defined on the device for registering it to the Hik IP Receiver 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.


Heartbeat Interval

Ranges from 10 to 90.

Heartbeat Timeout

Ranges from 3 to 65535.

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, key, heartbeat interval, and heartbeat timeout 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 IP Receiver Configuration

Configuration module provides basic settings of the Hik IP Receiver such as account management, log searching, and network settings.

- **System Settings:** Edit Hik IP Receiver name, change password for admin user, and set date and time.
- **System Maintenance:** Enable log and save logs in your computer.
- **Network Settings:** Set network ports, NIC, NAT, and HTTPS.
- **Storage:** Edit the disk for storing data.

4.1 System Settings

You can set the system parameters, including admin password, Hik IP Receiver name, and time.

4.1.1 Configure Hik IP Receiver Name

You can view the Hik IP Receiver information and edit the its name according to the actual needs.

Steps

1. Click **Configuration → System Settings → Information** .
2. View the 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

You can change password for login if you need.

Steps

1. Click **Configuration → System Settings → User** .
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 IP Receiver service again.

4.1.3 Configure Time

The Hik IP Receiver supports editing the time zone, date, and time for it.

Steps

1. Click **Configuration** → **System Settings** → **Time** .
2. Select a time zone for the computer where the Hik IP Receiver is running. Generally, you select the time zone where this computer locates.
3. Set the date and time for the Hik IP Receiver.
 - Click  to select a date and time.
 - Check **Synchronize with Computer Time** to used the current computer's date and time.
4. Click **Save**.

4.2 System Maintenance

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

Steps

1. Click **Configuration** → **System Maintenance** to enter the System Maintenance page.
2. Check **Enable Log**.
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 IP Receiver performance will be degraded.
-

4. Click **Save** to save the settings.
5. **Optional:** Click **Export** to download logs to your PC.

4.3 Network Settings

You need to configure network parameters of the Hik IP Receiver 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 IP Receiver can be edited if they are already used by other services.

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

Normal

The port is not occupied.

Conflict

The port is already occupied. You need to enter another port number to avoid communication failures.

Platform Port

Click **Platform Port** to edit the following ports used for data transmission from devices to the Hik IP Receiver.

HTTP Port

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

HTTPS Port

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

Device Port

Click **Device Port** to edit the ports used for data transmission from the Hik IP Receiver to devices.




Note

Restart the Hik IP Receiver after editing the device port, or the settings will not take effect.

4.3.2 Set NIC for Hik IP Receiver

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

Steps

1. Click **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 IP Receiver will restart automatically after saving the settings.
 - You should restart the Hik IP Receiver after editing the IP address of the computer where the Hik IP Receiver runs.
 - If you have edited NIC for the Hik IP Receiver, 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 required, 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.

Click **Configuration** → **Network Settings** → **NAT** to enter the NAT setting page. Check **Enable** to enable Platform Port Mapping or Device Port Mapping function. Enter the corresponding external ports and external IP addresses of the Hik IP Receiver and save the settings.

Platform Port Mapping

Used for accessing the Hik IP Receiver by a web browser and getting stream from the Hik IP Receiver.

Device Port Mapping

Used for sending data from the Hik IP Receiver to ISUP devices.



Note

- By default, the Hik IP Receiver will restart automatically after saving the settings.
-

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 IP Receiver provides three installing methods of HTTPS certificate.

Steps

1. Click **Configuration** → **Network Settings** → **HTTPS** to enter the HTTPS 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 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. Click **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, 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.

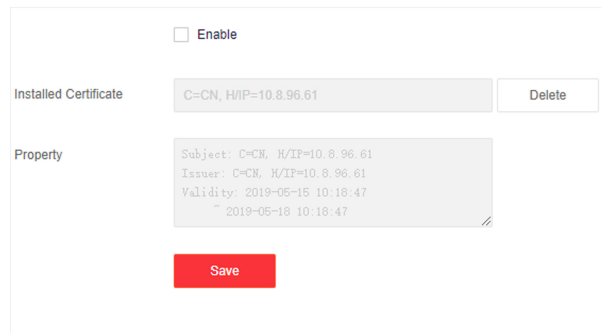


Figure 4-1 Installed Certificate

4.4 Select Storage Disk

When there are triggered alarms, the Hik IP Receiver will automatically store the alarm-related videos in the PC, so that you can view the videos by the third-party system connected to the Hik IP Receiver. You need to select the storage disk 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 **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 files.
 3. Click **Save** to save the settings.
-

Note

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

The videos will be stored in a folder named **DeviceGatewayStorage**.

Chapter 5 Automation Output Management

You need to configure related protocol parameters to conduct the communication between the Hik IP Receiver and ARC.

The Hik IP Receiver communicates with ARC by Sur-Gard protocol. So that you need to configure the Sur-Gard parameters which are supposed to be the same with those parameters configured in the ARC. Meanwhile, the Hik IP Receiver supports viewing and managing security control panel's events. You can view event details and add/edit/delete an event.

5.1 Configure Sur-Gard Parameters

To perform communication between the Hik IP Receiver and the third-party system, you need to configure Sur-Gard Parameters first.

Steps

1. Click **Automation Output → Sur-Gard** .
2. Check **Enable** to enable Sur-Gard protocol.
3. Check **TCP/IP** or **RS-232** as the **Interface** used for communication between the Hik IP Receiver and third-party system.
4. Select **Server** or **Client** as the Mode.

Server

The Hik IP Receiver works as a server for communication.

Client

The Hik IP Receiver works as a client connecting to third-party system which works as a server for communication. You need to provide the third-party system's IP address if you select this mode.

5. Set the following parameters.

Port

For TCP/IP mode, enter the port number which is **1025** by default.

Compatibility

The versions of Sur-Gard protocol.

Receiver Number

The number used for marking the Hik IP Receiver as an information receiver. You can customize this parameter. Keep it the same with the number set on third-party system.

Linecard Number

The number of the line used for communication between the Hik IP Receiver and third-party system. You can customize this parameter. Keep it the same with the number set on third-party system.

Baud Rate

Keep it the same with the baud rate set on third-party system.

Data Bit

Keep it the same with the data bit set on third-party system.

Parity

Keep it the same with the parity set on third-party system.

Stop Bit

It cannot be edited and is **2** by default.

The screenshot shows a configuration window for the Hik IP Receiver. It contains the following fields and options:

- Enable:** A checkbox that is currently unchecked.
- Interface:** Two radio buttons: **TCP/IP** (selected) and **RS-232** (unselected).
- Mode:** Two radio buttons: **Server** (selected) and **Client** (unselected).
- * Port:** A text input field containing the value **1025**.
- Compatibility:** A dropdown menu showing **MLR2000**.
- Receiver Number *:** A text input field containing the value **01**.
- Linecard Number *:** A text input field containing the value **001**.
- Enable Heartbeat:** A checkbox that is checked.
- Heartbeat Interval:** Two radio buttons: **10s** (unselected) and **30s** (selected).
- Automation Status:** A label with a red asterisk icon.
- Save:** A red button at the bottom center.


Figure 5-1 Configure Sur-Gard Parameters

6. Check **Enable Heartbeat** to enable heartbeat between third-party system and Hik IP Receiver so that the Hik IP Receiver can communicate with the third-party system.
7. Select a heartbeat interval.

Example

If you select **10s**, a heartbeat will be performed every 10 seconds if there is no event occurred during this period.

Automation Status

The communication status between the Hik IP Receiver and third-party system. When the Hik IP Receiver receives data from the third-party system, the third-party system's IP address and port number will show if you select **TCP/IP** as the interface, while the serial port number of the third-party system will show if you select **RS-232** as the interface. When the Hik IP Receiver receives no data from the third-party system,  will show.

8. Click **Save**.

5.2 Check Event Monitor Logs

The Hik IP Receiver displays the real-time events triggered by the communication between it and the third-party system. On the Event Monitor page, you can view the event details including the access protocol between it and the third-party system, the time at which an event happens, communication bugs, etc. Each event type is marked by different colors for attention. For example, you will be noticed quickly when there are communication bugs between the Hik IP Receiver and the third-party system.

Click **Automation Output → Event Monitor**.

The real-time events triggered by communications between the Hik IP Receiver and third-party system are displayed.

Protocol	Time	Content
Sur-Gard	2020-01-21T10:25:59+08:00	[101000 @] sent
Sur-Gard	2020-01-21T10:25:49+08:00	[10.19.166.129:1025] connected
Sur-Gard	2020-01-21T10:25:49+08:00	[10.19.166.129:1025] disconnected
Sur-Gard	2020-01-21T10:25:49+08:00	Sending [101000 @] failed

Figure 5-2 Real-Time Events

Different event types are marked by different colors:

Red

Communication failure between the Hik IP Receiver and third-party system. The Hik IP Receiver cannot get communication results.

Yellow

The third-party system responding to the message sent by the Hik IP Receiver timed out.

White

The communication between the Hik IP Receiver and the third-party system goes well.



Note

No more than 10 pages of events can be printed.

5.3 Configure Sur-Gard Event

The third-party system recognizes security control panel's events by recognizing their event codes. The Hik IP Receiver will receive an event code (which is defined as an original code) when a

security control panel added to the Hik IP Receiver triggers an event. Then, the Hik IP Receiver transfers the original code to a target code which could be recognized by the third-party system. After that, the Hik IP Receiver sends the target code to the third-party system. In this way, you can receive event notifications by the third-party system.

Click **Automation Output → Event** to enter the Event Configuration page. Perform the following operations and save the settings.

- Click **Add** to enter the event name, original code, and target code in the Add Event window.
- Click **×** to delete an event.
- In the **Event Name** and **Target Code** column, you can edit the event name and target code.

Note

The Hik IP Receiver will send the original code to the third-party system without trans-coding and the third-party system will not receive an event notification if you delete it in this list.



See Far, Go Further