



Interface Converter

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.
- If the product you choose is a video product, please scan the following QR code to obtain the "Initiatives on the Use of Video Products", and read it carefully.



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.

Symbol Conventions

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

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

TABLE OF CONTENTS

Chapter 1 Introduction	1
1.1 Product Introduction.....	1
1.2 Key Features	1
Chapter 2 Overview	2
Chapter 3 Activation and Login	3
3.1 Activation	3
3.1.1 Default Information	3
3.1.2 Activate via SADP.....	3
3.1.3 Activate via Web Browser	4
3.2 Login	5
Chapter 4 Configuration	6
4.1 Set Network Parameters	6
4.2 Set RS-485 Parameters.....	6
4.3 Select Working Mode.....	7
4.4 Set Network Camera Parameters	7
Chapter 5 Maintenance	9
5.1 View Device Information.....	9
5.2 Synchronize Time.....	9
5.3 Debug Device	10
5.4 System Maintenance	10
5.5 Change Password.....	10
5.6 Search Log	11

Chapter 1 Introduction

1.1 Product Introduction

Interface Converter (hereinafter referred to as “device”) is a reliable industrial-grade controller. It can be used for the control and conversion of interface signals such as serial port, network port, and switch value, and realize the communication between different signal interfaces, such as RS-485 signal to network signal. It has the characteristics of anti-strong electric interference, lightning protection, stability and reliability, and can be applied to various industrial and civil scenarios with harsh environments.

1.2 Key Features

- Supports 16-channel signal inputs and 16-channel signal outputs.
- Supports bidirectional conversion between I/O signals and both RS-485 serial communication protocols and Ethernet-based network protocols.
- Integrating traffic flow detection cameras allows traffic data to be relayed to third-party signal controllers in real time.
- Utilizing solid-state relays effectively enhances operational longevity.

Chapter 2 Overview

Refer to the figure and table below for the overview of the device.

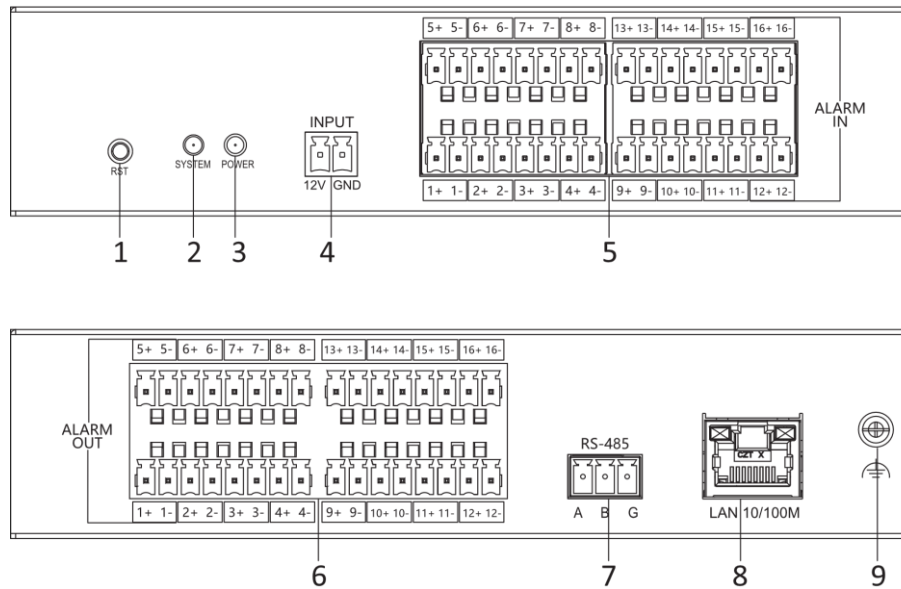


Figure 2-1 Overview

Table 2-1 Overview Description

No.	Name	Description
1	RST	Hold it for 3 seconds to reset the device.
2	System Indicator	Solid green: The system is running normally.
3	Power Indicator	Solid green: The device is powered on.
4	Power Input	12 VDC
5	ALARM IN	16-channel signal input
6	ALARM OUT	16-channel signal output
7	RS-485	Communication port
8	LAN	10/100 M network interface
9	GND	Grounding

Chapter 3 Activation and Login

3.1 Activation

For the first-time access, you need to activate the device by setting an admin password. No operation is allowed before activation. The device supports multiple activation methods, such as activation via SADP software, web browser, and iVMS-4200 Client.



Refer to the user manual of iVMS-4200 Client for the activation via client software.

3.1.1 Default Information

The device default information is shown as below.

- Default IP address: 192.168.1.64
- Default user name: admin

3.1.2 Activate via SADP

SADP is a tool to detect, activate, and modify the IP address of the device over the LAN.

Before You Start

- Get the SADP software from the supplied disk or the official website (<http://www.hikvision.com/>), and install it according to the prompts.
- The device and the computer that runs the SADP tool should belong to the same network segment.

The following steps show how to activate one device and modify its IP address. For batch activation and IP address modification, refer to *User Manual of SADP* for details.

Steps

Step 1 Run the SADP software and search the online devices.

Step 2 Find and select your device in online device list.

Step 3 Enter a new password (admin password) and confirm the password.

! Caution

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.

Step 4 Click **Activate** to start activation.

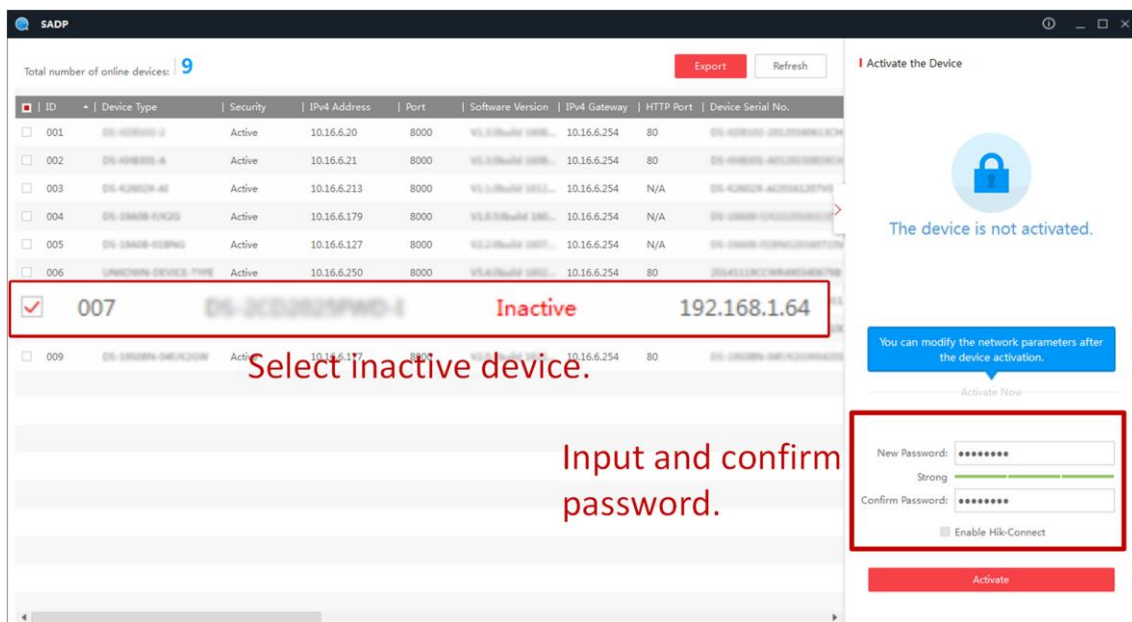


Figure 3-1 Activate via SADP

Status of the device becomes **Active** after successful activation.

Step 5 Modify IP address of the device.

- 1) Select the device.
- 2) Change the device IP address to the same network segment as your computer by either modifying the IP address manually or checking **Enable DHCP** (Dynamic Host Configuration Protocol).
- 3) Enter the admin password and click **Modify** to activate your IP address modification.

3.1.3 Activate via Web Browser

Use web browser to activate the device. For the device with the DHCP enabled by default, use SADP software or client software to activate the device.

Before You Start

Ensure the device and the computer are in the LAN with the same network segment.

Steps

Step 1 Change the IP address of your computer to the same network segment as the device.

Step 2 Open the web browser, and enter the default IP address of the device to enter the activation interface.

Step 3 Create and confirm the admin password.



Caution

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.

Step 4 Click **OK** to complete activation.

Step 5 Go to the network settings interface to modify IP address of the device.

3.2 Login

You can log in to the device via web browser for further operations.

Before You Start

Connect the device to the network directly, or via a switch or a router.

Steps

Step 1 Open the web browser, and enter the IP address of the device to enter the login interface.

Step 2 Enter **User Name** and **Password**.

Step 3 Click **Log In**.

Step 4 Optional: Click **Exit** on the upper right corner of the interface to log out of the device.

Chapter 4 Configuration

4.1 Set Network Parameters

Set the wired network parameters to connect the device to Internet.

Before You Start

Connect the LAN interface of the device to a router with a network cable.

Steps

Step 1 Go to **Network Configuration** → **Wired Configuration**.

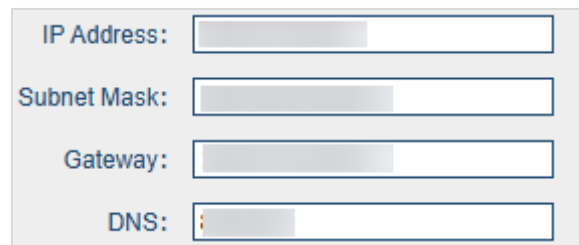
A screenshot of a web-based configuration interface for network settings. It contains four labeled input fields stacked vertically: 'IP Address:', 'Subnet Mask:', 'Gateway:', and 'DNS:'. Each label is in blue text. The input fields are white with a light gray border and a light gray shadow. The 'DNS:' field has a small orange icon to its left. The entire form is set against a light gray background.

Figure 4-1 Set Network Parameters

Step 2 Optional: Click **Get** to get the network parameters of the current device.

Step 3 If you want to change the network parameters, set **IP Address**, **Subnet Mask**, and **Gateway**.

Step 4 Optional: Set **DNS** address. It stands for domain name server. It is required if you need to visit the device with domain name.

Step 5 Click **Save**.

What to Do Next

If you have changed the IP address of the device, access to the device via the new IP address the next time.

4.2 Set RS-485 Parameters

Set RS-485 parameters if the device needs to be connected to other peripheral devices for control signal transmission.

Before You Start

The peripheral device has been connected via the RS-485 serial port of the device.

Steps

Step 1 Go to **Serial Port Configuration** → **485 Configuration**.

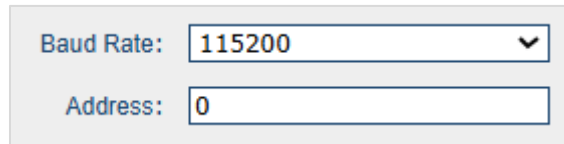


Figure 4-2 Set RS-485 Parameters

Step 2 Optional: Click **Get** to get the RS-485 parameters of the current device.

Step 3 Set **Baud Rate** and **Address**.

Note

The baud rate should be same with that of the connected peripheral device. For remote signal transmission, it is recommended to set a higher baud rate to guarantee the signal transmission quality.

Step 4 Click **Save**.

4.3 Select Working Mode

Click **Working Mode**. Click **Get** to get the working mode of the current device. Change **Work Mode** according to your needs. You can select **Active Reporting Mode** and **Search Mode** to upload the traffic signal light status.

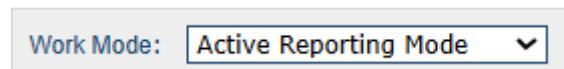


Figure 4-3 Select Working Mode

4.4 Set Network Camera Parameters

The device can connect to a network camera. Set the corresponding parameters to guarantee the camera is online.

Steps

Step 1 Click **Channel Settings**.

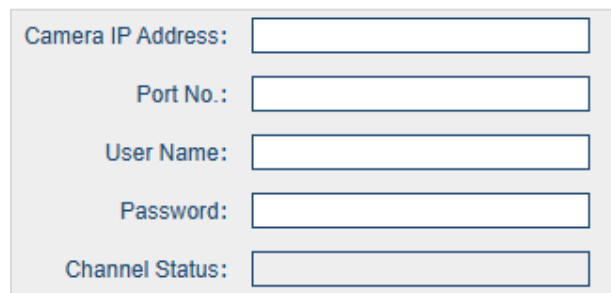


Figure 4-4 Set Network Camera Parameters

Step 2 Optional: If a camera is already connected, click **Get** to get the parameters of the connected camera.

Step 3 Set **Camera IP Address**, **Port No.**, **User Name**, and **Password** of the camera.

Step 4 Click **Save**.

Step 5 Optional: Click **Clear** to clear the parameters.

Chapter 5 Maintenance

5.1 View Device Information

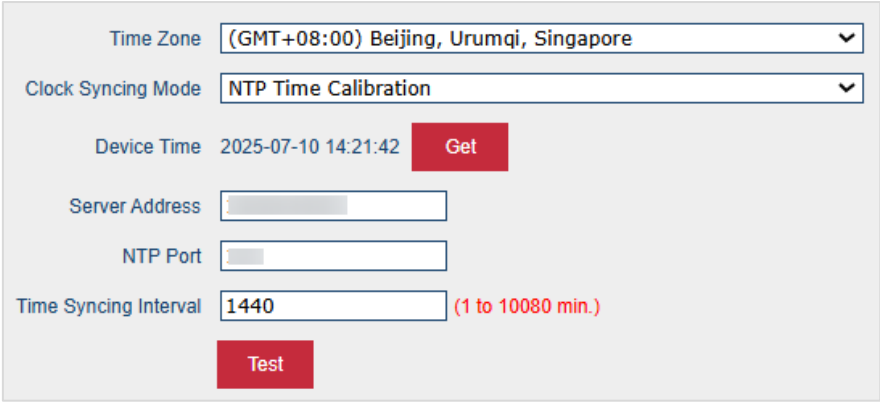
Click **Device Information** to view the device information such as device model, software version, etc. You can edit **Device Name** and **Device No.** The device No. is used to control the device. It is recommended to reserve the default value.

5.2 Synchronize Time

Synchronize the device time when it is inconsistent with the actual time.

Steps

Step 1 Click **Timing Configuration**.



The screenshot shows a configuration window with the following elements:

- Time Zone:** A dropdown menu currently showing "(GMT+08:00) Beijing, Urumqi, Singapore".
- Clock Syncing Mode:** A dropdown menu currently showing "NTP Time Calibration".
- Device Time:** Displays "2025-07-10 14:21:42" next to a red "Get" button.
- Server Address:** An empty text input field.
- NTP Port:** An empty text input field.
- Time Syncing Interval:** A text input field containing "1440", with a red note "(1 to 10080 min.)" to its right.
- Test:** A red button located at the bottom of the form.

Figure 5-1 Synchronize Time

Step 2 Click **Get** after **Device Time** to get the current time of the device.

Step 3 Select **Time Zone**.

Step 4 Select **Clock Syncing Mode**.

NTP Time Calibration

Select it to synchronize the device time with that of the NTP server. Set **Server Address**, **NTP Port**, and **Time Syncing Interval**. Click **Test** to test if the connection between the device and the server is normal.

Manual Timing

Select it to synchronize the device time with that of the computer. Set time manually.

Step 5 Click **Save**.

5.3 Debug Device

You can debug the device remotely.

Steps

Step 1 Click **Debug Settings**.

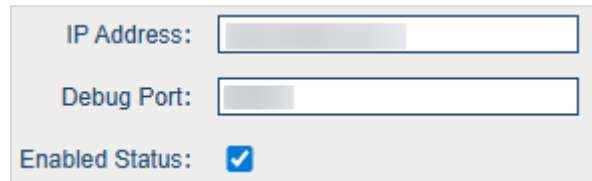
A screenshot of a web interface for configuring debug settings. It contains three fields: 'IP Address' with a text input box, 'Debug Port' with a text input box, and 'Enabled Status' with a checked checkbox.

Figure 5-2 Debug Device

Step 2 Set **IP Address** and **Debug Port**.

Step 3 Check **Enabled Status** to debug the device.

Step 4 Click **Save**.

5.4 System Maintenance

Go to **System Configuration** → **System Maintenance**.

- **Restart Device:** Click **Restart Device** to restart the device.
- **Restore Default Value:** Select the restoration mode and the device will reboot automatically after restoration.
 - Click **Fully Restore** to restore the device to inactive status.
 - Click **Partially Restore** to restore the user parameters only.
- **Upgrade:** Click **Browse** to select the upgrade file saved in the computer. Click **Upgrade** to upgrade the device. Wait for until the upgrade completes. The device will reboot automatically after upgrade.

5.5 Change Password

You can change the login password of the admin.

Steps

Step 1 Go to **System Configuration** → **Change Password**.

A screenshot of a web form titled 'Change Password'. It contains three input fields stacked vertically. The first field is labeled 'Current Password:', the second is labeled 'New Password:', and the third is labeled 'Confirm New Password:'. Each label is in a blue font and is followed by a white rectangular input box with a thin blue border.

Figure 5-3 Change Password

Step 2 Enter **Current Password**, **New Password**, and confirm the new password.

 Note

The password must contain 8 to 16 characters and include a combination of two or more of the following: numbers, lowercase letters, uppercase letters, and special characters.

Step 3 Click **Save**.

What to Do Next

Use the new password to log in the next time.

5.6 Search Log

You can search the download the device logs.

Steps

Step 1 Go to **System Configuration** → **Log**.

Step 2 Set the search conditions.

Step 3 Click **Search**. The searched results will be displayed in the table.

Step 4 Optional: Click **Download** to download and save the logs to the default saving directory of the web browser.

Step 5 Optional: Click **Clear** to clear the logs.



See Far, Go Further