



# Network Volume Controller

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.**

## Symbol Conventions

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

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

# Contents

|                                                        |           |
|--------------------------------------------------------|-----------|
| <b>Chapter 1 Device Activation and Accessing .....</b> | <b>1</b>  |
| <b>1.1 Activate the Device via SADP .....</b>          | <b>1</b>  |
| <b>1.2 Activate the Device via Browser .....</b>       | <b>1</b>  |
| <b>1.3 Login .....</b>                                 | <b>2</b>  |
| <b>Chapter 2 Channel Management.....</b>               | <b>3</b>  |
| <b>Chapter 3 Network Settings .....</b>                | <b>6</b>  |
| <b>3.1 TCP/IP .....</b>                                | <b>6</b>  |
| <b>3.2 HTTP(S) .....</b>                               | <b>6</b>  |
| <b>Chapter 4 System and Security .....</b>             | <b>7</b>  |
| <b>4.1 System Settings.....</b>                        | <b>7</b>  |
| <b>4.1.1 View Device Information.....</b>              | <b>7</b>  |
| <b>4.1.2 Time and Date .....</b>                       | <b>7</b>  |
| <b>4.2 User Management .....</b>                       | <b>8</b>  |
| <b>4.3 Maintenance .....</b>                           | <b>8</b>  |
| <b>4.3.1 Restart.....</b>                              | <b>8</b>  |
| <b>4.3.2 Upgrade.....</b>                              | <b>9</b>  |
| <b>4.3.3 Restore and Default .....</b>                 | <b>9</b>  |
| <b>4.3.5 Search Security Audit Logs .....</b>          | <b>9</b>  |
| <b>4.3.6 SSH .....</b>                                 | <b>10</b> |
| <b>4.3.7 Export Diagnose Information .....</b>         | <b>10</b> |

# Chapter 1 Device Activation and Accessing

To protect the security and privacy of the user account and data, you should set a login password to activate the device when access the device via network.

## 1.1 Activate the Device via SADP

Search and activate the online devices via SADP software.

### Before You Start

Access [www.hikvision.com](http://www.hikvision.com) to get SADP software to install.

### Steps

1. Connect the device to network using the network cable.
2. Run SADP software to search the online devices.
3. Check **Device Status** from the device list, and select **Inactive** device.
4. Create and input the new password in the password field, and confirm the password.



### Caution

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.

---

5. Click **OK**.  
**Device Status** changes into **Active**.
6. Optional: Change the network parameters of the device in **Modify Network Parameters**.

## 1.2 Activate the Device via Browser

You can access and activate the device via the browser.

### Steps

1. Connect the device to the PC using the network cables.
2. Change the IP address of the PC and device to the same segment.

---

### Note

The default IP address of the device is 192.168.1.64. You can set the IP address of the PC from 192.168.1.2 to 192.168.1.253 (except 192.168.1.64). For example, you can set the IP address of the PC to 192.168.1.100.

---

3. Input **192.168.1.64** in the browser.
  4. Set device activation password.
- 

### Caution

We highly recommend you create a strong password of your own choosing (using a minimum of 8 characters, including at least three of the 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.

---

5. Click **OK**.
6. Input the activation password to log in to the device.
7. Optional: Go to **Configuration** → **Network** → **Network Settings** → **TCP/IP** to change the IP address of the device to the same segment of your network.

## 1.3 Login

Log in to the device via Web browser.

Certain operating systems and web browsers may restrict the display and operation of the device function. For detailed restricted function, refer to the actual device.

---

### Note

To improve the user experience on certain devices, it's recommended to use a more advanced web browser for access. Please refer to the actual device or product specification.

---

## Chapter 2 Channel Management

### Add Devices and Controlled Items

Steps

- 1. Go to **Channel Management**.
- 2. Click **+ Add**.
- 3. Add controlled device: Enter the device name, IP address, port No., user name, and password.  
Click **Next**.

Add Device

1 Basic Information

2 Associate Controller

Device Name \*

IP \*

Port No. \*

80

User Name \*

Password \*

.....

Next

Cancel

Figure 3-1 Add Device Basic Information

- 4. Select volume controlled item: Associate the volume controlled item with the controller channel.

 **Note**

- Each channel can add up to 16 controlled items.
- Controlled items cannot be repeatedly added to different channels.

- 5. Click **Save** to complete the addition. After adding successfully, the added device and controlled items will be displayed in the **Channel Management** list.

|                                   |                                                                                                                                            |
|-----------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------|
| Delete a Single Associated Device | 4-channel volume controller: Click  on the right side |
|-----------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------|

|                                 |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                       |
|---------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
|                                 | <p>of the device to delete all controlled items of the device under the selected channels of the controller. If the device is not bound to any of the four channels, the device will be deleted.</p> <p>1-channel volume controller: Click  on the right side of the device to delete the device.</p>                                                                                                                                                              |
| Batch Delete Associated Devices | <p>4-channel volume controller: Select multiple devices, click  Delete to delete all controlled items of the selected devices under the selected channels of the controller. If the device is not bound to any of the four channels, the corresponding device will be deleted.</p> <p>1-channel volume controller: Select multiple devices, click  Delete to batch delete them.</p> |
| Delete a Single Controlled Item | <p>Method 1: Click  below the controlled item to delete it.</p> <p>Method 2: Click  on the right side of the device and uncheck the controlled item.</p>                                                                                                                                                                                                                            |
| Batch Delete Controlled Items   | Select multiple controlled items and click  Delete to batch delete them.                                                                                                                                                                                                                                                                                                                                                                                          |

## Adjust Volume

Check the controlled items, click **Reinforcement Volume**, and adjust the volume in the pop-up box. All selected controlled items will be adjusted to the same volume level.

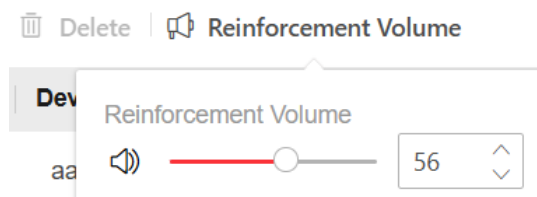


Figure 3-2 Reinforcement Volume

## Mute

### Note

Only certain models support this function. Please refer to the actual interface.

Check the controlled items, click **Mute**, and all selected controlled items will be muted. Click

**Unmute** to restore the volume of the controlled items to the settings before muting.

### Rename

- Channel Rename: Click  on the right side of the channel, modify the channel name, and click **Save**.
- Device Rename: Click the device name to be modified, the name becomes editable. After modification, click anywhere on the interface to save.
- Controlled Item Rename: Click  below the controlled item to edit it. Modify the controlled item name in the pop-up box and click **Save**.

## Chapter 3 Network Settings

### 3.1 TCP/IP

TCP/IP settings must be properly configured before you operate the device over network.

#### Steps

1. Go to **Configuration → Network → Network Configuration → TCP/IP** to enter the configuration page.
2. Configure network parameters.
3. Select **NIC Type**, slide to enable **DHCP**, and manually enter **IPv4 Address**, **IPv4 Subnet Mask**, **IPv4 Default Gateway**, **MTU**, **Preferred DNS Server** address, and **Alternate DNS Server** address.



#### Note

Click **Test** to test if IPv4 address is used.

---

4. Click **Save** to complete the configuration.

### 3.2 HTTP(S)

HTTP is an application-layer protocol for transmitting hypermedia documents. HTTPS is a network protocol that enables encrypted transmission and identity authentication, which improves the security of remote access.

#### Steps

1. Go to **Configuration → Network → Network Service → HTTP(S)**.
2. Enter **HTTP Port**.



#### Note

It refers to the port through which the browser accesses the device. For example, when the **HTTP Port** is modified to 81, you need to enter `http://192.168.1.64:81` in the browser for login.

---

3. Enter **HTTPS Port**.
4. Click **Save**.

## Chapter 4 System and Security

It introduces system maintenance, system settings and security management, and explains how to configure relevant parameters.

### 4.1 System Settings

#### 4.1.1 View Device Information

You can view device information, such as Device Model, Serial No. and Firmware Version.

Go to **Configuration** → **System** → **System Configuration** → **Basic Information** to view the device information.

#### 4.1.2 Time and Date

You can configure time and date of the device by configuring time zone and time synchronization.

##### Synchronize Time Manually

###### Steps

1. Go to **Configuration** → **System** → **System Configuration** → **Time Settings**.
  2. Select **Time Zone**.
  3. Select **Manual Time Sync**.
  4. Choose one time synchronization method.
    - Select **Set Time**, and manually input or select date and time from the pop-up calendar.
- Click **Sync With Computer Time** to synchronize the time of the device with that of the local PC.
5. Click **Save**.

##### Set NTP Server

You can use NTP server when accurate and reliable time source is required.

###### Before You Start

Set up a NTP server or obtain NTP server information.

###### Steps

1. Go to **Configuration** → **System** → **System Configuration** → **Time Settings**.
2. Select **Time Zone**.
3. Click **NTP Sync**.
4. Set **Server Address**, **NTP Port** and **Interval**.



**Note**

Server Address is NTP server IP address.

---

5. Click **Test** to test server connection.
6. Click **Save**.

## 4.2 User Management

Go to **Configuration → System → User Management → User Management**.

You can click  to change the administrator password.

---



**Caution**

- The admin is the default user. The user name cannot be edited. Only its password can be edited.
  - To ensure the security of account information, it is recommended to set a password between 8 and 16 characters, including at least digits, lowercase letters, uppercase letters, and special characters (!"#\$%&'()\*+,-./:;<=>?@[\\]^\_`{|}~. space) and cannot contain user name.
  - Password length should be less than 8 characters. Password should contain only 1 type of character. Password should be the same as user name, or the password should be the reverse of user name. The above types of passwords are risky. To better protect your privacy and improve product security, it is recommended to change the risky password to high-intensity.
  - Password strength rule:
    1. If the password contains 3 or more types (digits, lowercase letters, uppercase letters, and special characters), the password security strength is strong.
    2. If the password is a combination of digits and special characters, lowercase letters and special characters, uppercase letters and special characters, lowercase letters and uppercase letters, the password security strength is medium.
    3. If the password is a combination of digits and lowercase letters, digits and uppercase letters, the password security strength is weak.
- 

## 4.3 Maintenance

### 4.3.1 Restart

You can restart the device via browser.

Go to **Maintenance and Security → System Maintenance → Restart**, and click **Restart**.

## 4.3.2 Upgrade

### Before You Start

You need to obtain the correct upgrade package.

---



### Caution

DO NOT disconnect power during the process, and the device restarts automatically after upgrade.

---

### Steps

1. Go to **Maintenance and Security** → **System Maintenance** → **Upgrade**.
2. Click  to select the upgrade file.
3. Click **Upgrade**.

## 4.3.3 Restore and Default

Restore and Default helps restore the device parameters to the default settings.

### Steps

1. Go to **Maintenance and Security** → **System Maintenance** → **Backup and Reset**.
2. Click **Restore Default** or **Default Factory** according to your needs.

#### Restore Default

All data except network parameters and user accounts will be cleared.

#### Default Factory

All functions and parameters will be restored to factory settings.

---



### Note

Be careful when using this function. After resetting to the factory default, all the parameters are reset to the default settings.

---

## 4.3.5 Search Security Audit Logs

You can analyze the security log files of the device so as to find out the illegal intrusion and troubleshoot the security events.

### Steps



### Note

This function is only supported by certain camera models.

---

1. Go to **Maintenance and Security** → **System Maintenance** → **Security Audit Log**.
-

2. Enable **Enable Log Upload Server**.

3. Input **Server IP** and **Port No.**

The log files that match the search conditions will be displayed on the Log List.

4. Click **Save**.

### 4.3.6 SSH

Secure Shell (SSH) is a cryptographic network protocol for operating network services over an unsecured network.

Go to **Maintenance and Security** → **System Maintenance** → **Device Debugging**, and enable **Enable SSH**.



#### Caution

Use the function with caution. The security risk of device internal information leakage exists when the function is enabled.

---

### 4.3.7 Export Diagnose Information

Diagnose information includes running log, system information, hardware information.

Go to **Maintenance and Security** → **System Maintenance** → **Device Debugging**. Click **Export** to export corresponding diagnose information of the device.



See Far, Go Further