HIKVISION SI Series

Wireless Access Points

Web-Based Configuration Guide

Hangzhou Hikvision Digital Technology Co., Ltd.
http://www.hikvision.com

Document version: 5W100-20250530
Product version: V1.1.6300 build250402

About this Manual

This Manual is applicable to the HIKVISION SI series.

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 in the company website (http://overseas.hikvision.com/en/).

Please use this user manual under the guidance of professionals.

Legal Disclaimer

TO THE MAXIMUM EXTENT PERMITTED BY APPLICABLE LAW, THE PRODUCT DESCRIBED, WITH ITS HARDWARE, SOFTWARE AND FIRMWARE, IS PROVIDED “AS IS”, WITH ALL FAULTS AND ERRORS, AND HIKVISION MAKES NO WARRANTIES, EXPRESS OR IMPLIED, INCLUDING WITHOUT LIMITATION, MERCHANTABILITY, SATISFACTORY QUALITY, FITNESS FOR A PARTICULAR PURPOSE, AND NON-INFRINGEMENT OF THIRD PARTY. IN NO EVENT WILL HIKVISION, ITS DIRECTORS, OFFICERS, EMPLOYEES, OR AGENTS 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 OR DOCUMENTATION, IN CONNECTION WITH THE USE OF THIS PRODUCT, EVEN IF HIKVISION HAS BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES.

REGARDING TO THE PRODUCT WITH INTERNET ACCESS, THE USE OF PRODUCT SHALL BE WHOLLY AT YOUR OWN RISKS. HIKVISION SHALL NOT TAKE ANY RESPONSIBILITES 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.

Environmental protection

This product is environment-friendly by design to minimize its environmental impact. The storage, use, and disposal of this product must be compliant with the applicable national laws and regulations.

Preface

This document describes the Web-based configuration guide for the Hikvision SI series APs and uses a DS-3WAP622E-SI AP of the V1.1.6300 build250402 version as an example. Figures in this document are for illustration only.

This preface includes the following topics about the documentation:

Audience

This documentation is intended for:

- Network planners.
- Field technical support and servicing engineers.
- Network administrators working with the Hikvision SI series APs.

Conventions

The following information describes the conventions used in the documentation.

Command conventions

Convention	Description
Boldface	**Bold** text represents commands and keywords that you enter literally as shown.
Italic	*Italic* text represents arguments that you replace with actual values.
[ ]	Square brackets enclose syntax choices (keywords or arguments) that are optional.
{ x | y | ... }	Braces enclose a set of required syntax choices separated by vertical bars, from which you select one.
[x | y | ...]	Square brackets enclose a set of optional syntax choices separated by vertical bars, from which you select one or none.
{ x | y | ... } *	Asterisk marked braces enclose a set of required syntax choices separated by vertical bars, from which you select a minimum of one.
[x | y | ...] *	Asterisk marked square brackets enclose optional syntax choices separated by vertical bars, from which you select one choice, multiple choices, or none.
&<1-n>	The argument or keyword and argument combination before the ampersand (&) sign can be entered 1 to n times.
#	A line that starts with a pound (#) sign is comments.

GUI conventions

Convention	Description
Boldface	Window names, button names, field names, and menu items are in Boldface. For example, the **New User** window opens; click **OK**.
>	Multi-level menus are separated by angle brackets. For example, **File** > **Create** > **Folder**.

Symbols

Convention	Description
WARNING!	An alert that calls attention to important information that if not understood or followed can result in personal injury.
CAUTION:	An alert that calls attention to important information that if not understood or followed can result in data loss, data corruption, or damage to hardware or software.
IMPORTANT:	An alert that calls attention to essential information.
NOTE:	An alert that contains additional or supplementary information.
TIP:	An alert that provides helpful information.

Network topology icons

Convention	Description
	Represents a generic network device, such as a router, switch, or firewall.
	Represents a routing-capable device, such as a router or Layer 3 switch.
	Represents a generic switch, such as a Layer 2 or Layer 3 switch, or a router that supports Layer 2 forwarding and other Layer 2 features.
	Represents an access controller, a unified wired-WLAN module, or the access controller engine on a unified wired-WLAN switch.
	Represents an access point.
	Represents a wireless terminator unit.
	Represents a wireless terminator.
	Represents a mesh access point.
	Represents omnidirectional signals.
	Represents directional signals.
	Represents a security product, such as a firewall, UTM, multiservice security gateway, or load balancing device.
	Represents a security module, such as a firewall, load balancing, NetStream, SSL VPN, IPS, or ACG module.

Examples provided in this document

Examples in this document might use devices that differ from your device in hardware model, configuration, or software version. It is normal that the port numbers, sample output, screenshots, and other information in the examples differ from what you have on your device.

Contents

NOTE:

This document applies only to the Hikvision SI series. It uses a DS-3WAP622E-SI AP of the V1.1.6300 build250402 version as an example. Figures in this document are for illustration only.

Logging in to a device

Web management restrictions and guidelines

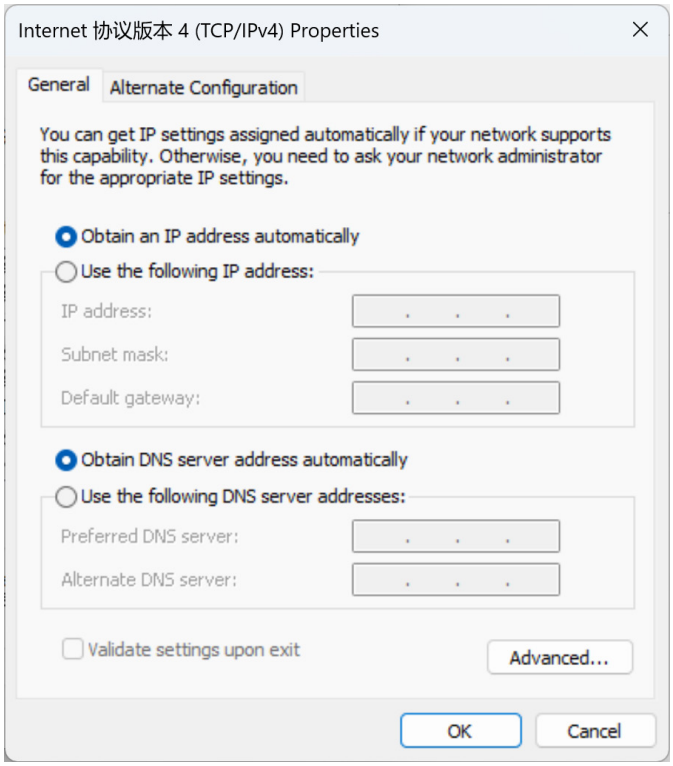
- The supported operating systems include Windows XP, Windows 2000, Windows Server 2003 enterprise edition, Windows Server 2003 standard edition, Windows Vista, Windows 7, Windows 8, Windows 10, Linux, and MAC OS.
- The supported browsers include Microsoft Edge 79 and later, Mozilla Firefox 78 and later, Google Chrome 64 and later, and Safari 12 and later. Using other browsers might result in compatibility issues or suboptimal rendering.
- The Windows firewall limits the number of TCP connections, and you might fail to open the web management page due to this restriction. As a best practice to avoid this issue, disable the Windows firewall.
- As a best practice to avoid display issues, if the device software version changes, clear the browser cache before logging into the Web interface.
- As a best practice, make sure only one user logs into the device and perform system configuration and management operations at a time.

Logging in to the Web interface

Prerequisites

1. View the IP address of the device on the DHCP server.
2. Configure an IP address for the PC using either of the following methods for the PC and the device to reach each other:
   - Configure the PC to obtain an IP address and the DNS server address automatically.

Figure 1 Configuring a PC to automatically obtain an IP address



- Manually specify an IP address on the same subnet as the device for the PC.

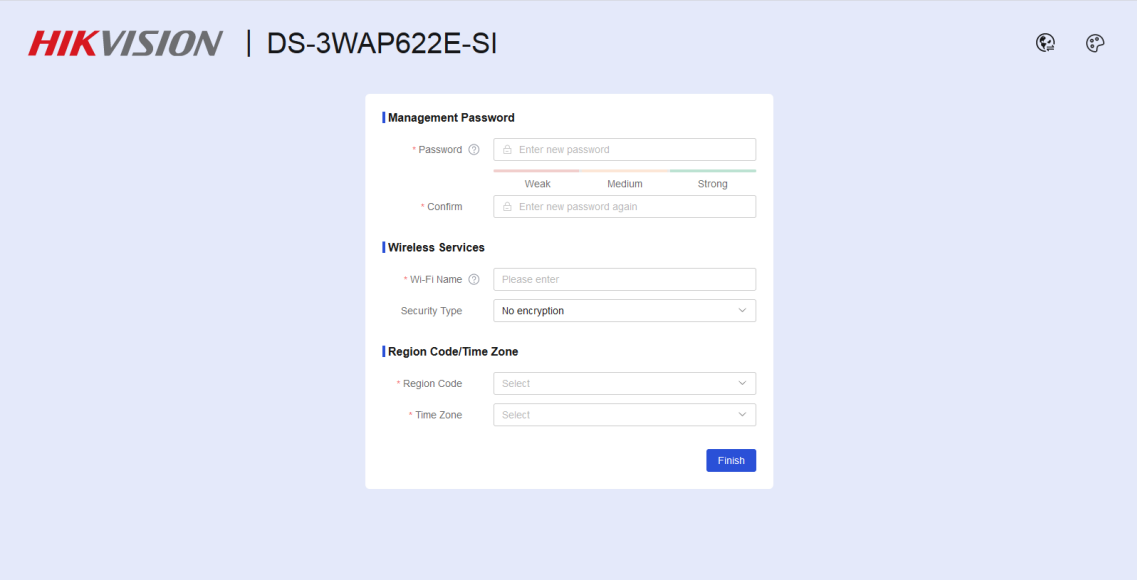
Configuring initialization

NOTE:

The device does not have a default password. You must set the login password on the initialization page after you power on the device for the first time or perform factory restoration.

1. Open a browser and enter **https://***ip-address* in the address bar, where *ip-address* represents the IP address of the device. You can view the address on the DHCP server.
2. Press **Enter**, and then configure the management password, wireless services, and region code/time zone.
3. Click **Finish**. The login page opens.

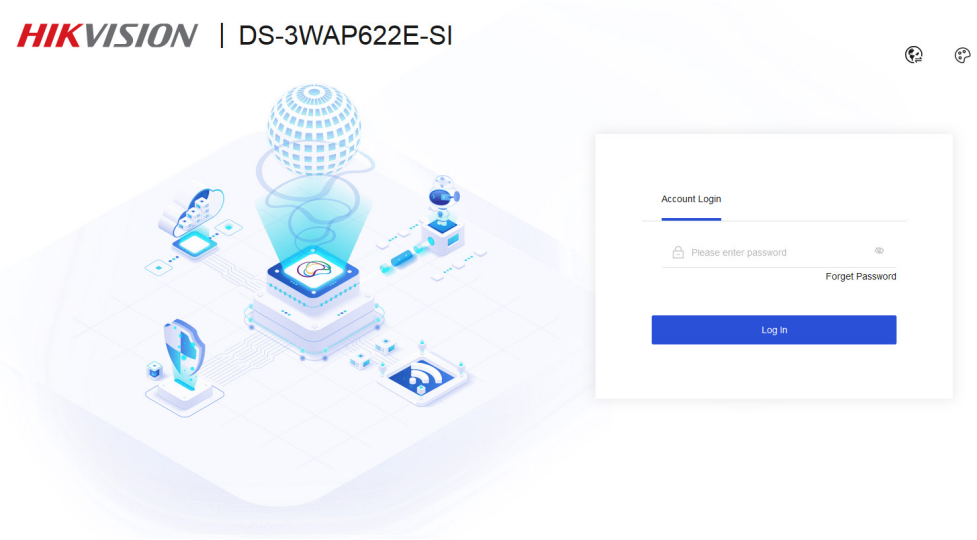
Figure 2 Initialization configuration page



Logging in to the Web interface

1. Enter **https://***ip-address* in the browser address bar, where *ip-address* represents the IP address of the device. You can view the address on the DHCP server.
2. Press **Enter**.
3. Enter the login password and press **Enter**.

Figure 3 Web management login page



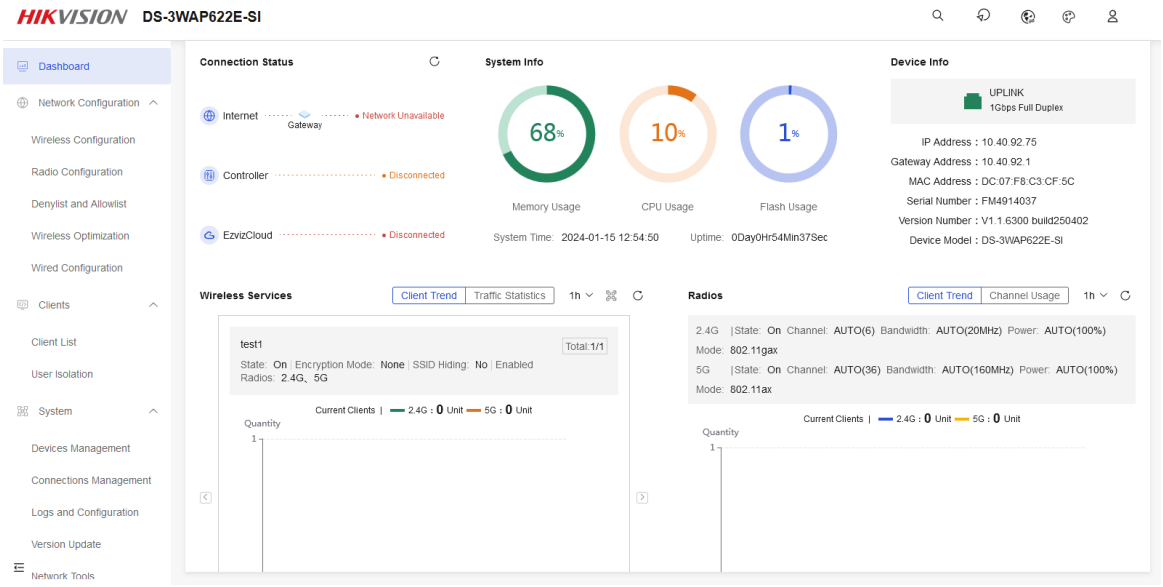
Logging out of the web management interface

1. From the left navigation pane, select **Dashboard**. Then, click the icon at the upper-right corner of the page.
2. Click **OK** in the dialog box that opens.

Dashboard

On the **Dashboard** page, you can view the connection status, system information, device information, wireless services, radios, and traffic statistics.

Figure 4 Dashboard page



- **Connection Status**:
  - Connection status between device and Internet:
    - **Network Available**: The device is connected to the external network.
    - **Network Unavailable**: The device is not connected to the external network.
  - Connection status between device and AC:
    - **Connected**: The device is connected to an AC. You can manage the device through the AC.
    - **Disconnected**: The device is not connected to an AC.
  - Connection status between device and cloud platform:
    - **Connected**: The device has been registered to the cloud platform and is online. You can manage the device through the cloud platform.
    - **Disconnected**: The device has been registered to the cloud platform but is offline.
    - **Unregistered**: The device is not registered to the cloud platform.
- **System Information**:

  View the memory usage, CPU usage, flash usage, system time, and uptime of
- **Device Information**:

  View the status, speed, IP address, gateway address, MAC address, serial number, version number, and device model for the UPLINK and LAN ports on the device.

NOTE:

The system displays LAN information only when the device has LAN ports.

- **Wireless Services**:

View the status, encryption mode, SSID hiding status, and enabled radios of the wireless services.

You can click the arrow next to the chart to switchover the wireless service you want to view. To view the number of wireless clients, click **Client Trend**. To view real-time upstream and downstream traffic of the wireless service, click **Traffic Statistics**. You can select to view traffic statistics in real time, or for the past 1 hour, 6 hours, or 24 hours.

- **Radios**:

  View the status, channel, bandwidth, power, and mode of the radios.

  To view the total number of clients connected to the radios, click **Client Trend**. To view the real-time channel usage, click **Channel Usage**. You can select to view channel usage in real time, or for the past 1 hour, 6 hours, or 24 hours.

- **Traffic Statistics**:

  View the real-time inbound and outbound traffic of the device.

  To view the inbound and outbound traffic of the UPLINK or LAN ports, click **UPLINK** or **LAN**.

Network configuration

NOTE:

Certain Intel wireless network cards cannot detect wireless signals emitted by 802.11ax radios. In this case, access the Intel official website and try to update the network card driver.

Wireless configuration

From the left navigation pane, select **Network Configuration** > **Wireless Configuration,** and configure and optimize wireless features.

NOTE:

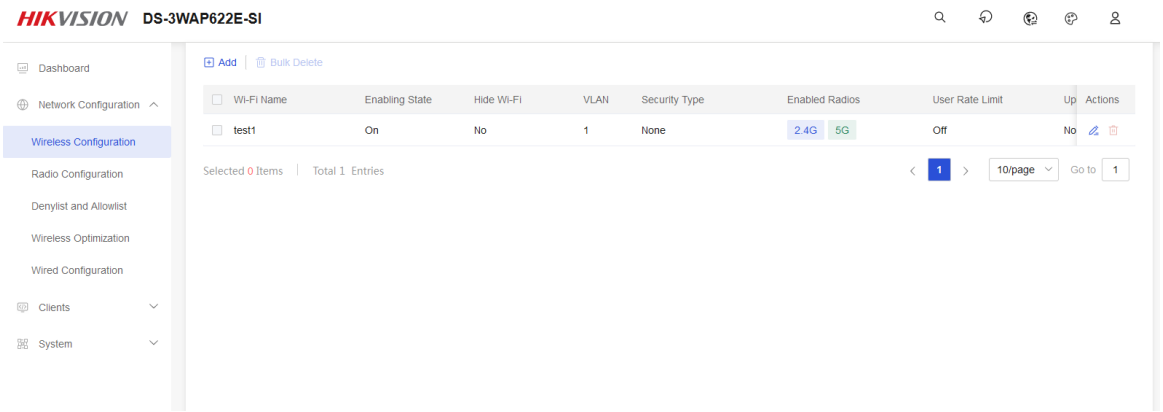
If the device is connected to the cloud platform or managed by an AC, some wireless features are unavailable from the local Web interface. The webpages might vary.

Wireless configuration

On the **Wireless Configuration** page, you can view the Wi-Fi name, enabling status, Wi-Fi hiding status, VLAN, security type, enabled radios, user rate limit, and uplink/downlink rate limit for all wireless services.

You can manually add wireless services to access both the Web management interface and the external network. During initial setup, the system creates a user Wi-Fi that can be edited but cannot be deleted. After completing initial setup, you can manually add up to seven user Wi-Fi networks.

Figure 5 Wireless Configuration page

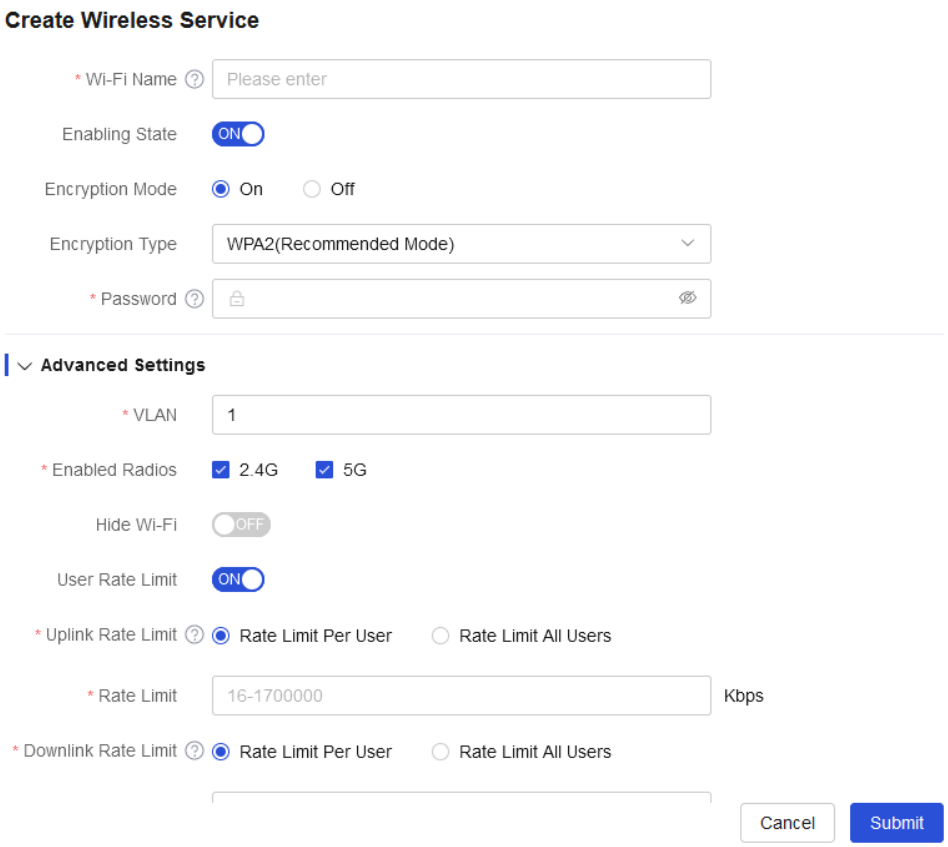


To add a new wireless service, click **Add**. Configure the following parameters as needed:

- Wi-Fi Name.
- Enabling State.
- Encryption Mode: If you disable the encryption mode, the wireless service uses open-system authentication (no authentication).
- Encryption Type: Options include WPA/WPA2 (compatibility mode), WPA2 (recommended mode), and WPA3 (security mode).

- Password: The password is a case-sensitive string of 8 to 63 characters. Only letters, digits, and special characters `,~!@$%^&#*()+=|<>.-_[]:;/\{} are supported. If you disable the encryption mode, no password is required.
- Advanced Settings:
  - VLAN: VLAN that a client joins when it comes online.
  - Enable Radios: Radios bound to the wireless service.
  - Hide Wi-Fi: With this feature enabled, clients cannot find the Wi-Fi service through scanning. A user must manually enter the Wi-Fi name to connect to the Wi-Fi.
  - User Rate Limit: Only user Wi-Fi supports this feature. The management Wi-Fi does not support this feature. You can enable this feature to limit the rate of connected clients on the wireless service. You can configure the following rate limit modes for the uplink and downlink, separately:
    - **Rate Limit Per User**: Limits the rate of each user associated with the wireless service. For example, if the rate limit per user is 1 Mbps, the rate of any user associated with the SSID cannot exceed 1 Mbps.
    - **Rate Limit All Users**: Limits the total rate of all users associated with the wireless service. For example, if the rate limit value for SSID1 is set to M and the SSID1 is bound to two radios (radio1 and radio2). For radio1, when N users are connected simultaneously, each user rate is limited to M/N. For radio2, if K users are connected, each user rate is limited to M/K.

Figure 6 Creating a new wireless service



To edit a wireless service, click the **Edit** icon in the **Actions** column for the service.

To delete a wireless service, click the **Delete** icon in the **Actions** column for the service.

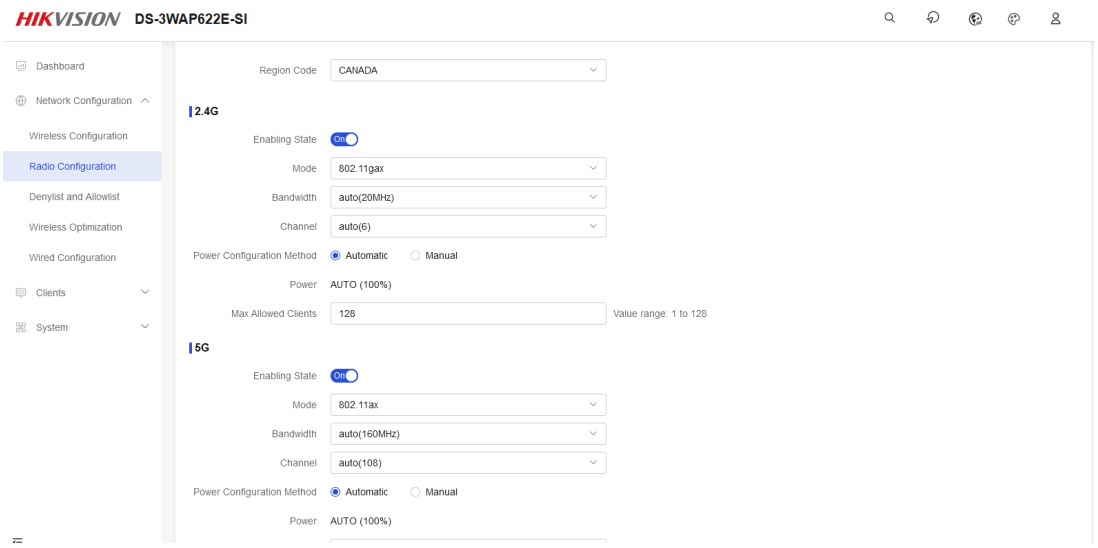
To delete multiple wireless services in bulk, select the target services, and then click **Bulk Delete**.

Radio configuration

On the **Radio Configuration** page, configure the following radio parameters:

- Region Code: Select the region code. Select the correct region code to ensure compliance with the local regulations. The supported region codes depend on the device model.
- Enabling State: Enable or disable the radio.
- Mode: Select the radio mode according to the IEEE 802.11 wireless communication standards.
- Bandwidth: Select the bandwidth of the radio. The default bandwidth varies by device model.
- Channel: Select the working channel of the radio. The default channel varies by device model.
- Power Configuration Method: Options include **Automatic** and **Manual**. If you select **Manual**, you must set the transmit power manually.
- Power: Set the transmit power of the radio. This field is required if you select the **Manual** power configuration method. The higher the transmit power, the wider the radio coverage, and the stronger the signals received by a client at the same location, making it easier to interfere with nearby networks.
- Max Allowed Clients: Select the maximum number of clients that can associate with the radio. The maximum number of supported clients varies by device model.

Figure 7 Radio Configuration page



Denylist and allowlist

CAUTION:

Switching between denylist and allowlist disconnects online clients.

On the **Denylist and Allowlist** page, you can configure the denylist or allowlist for wireless clients. The settings take effect immediately on online clients. The denylist and allowlist cannot take effect simultaneously.

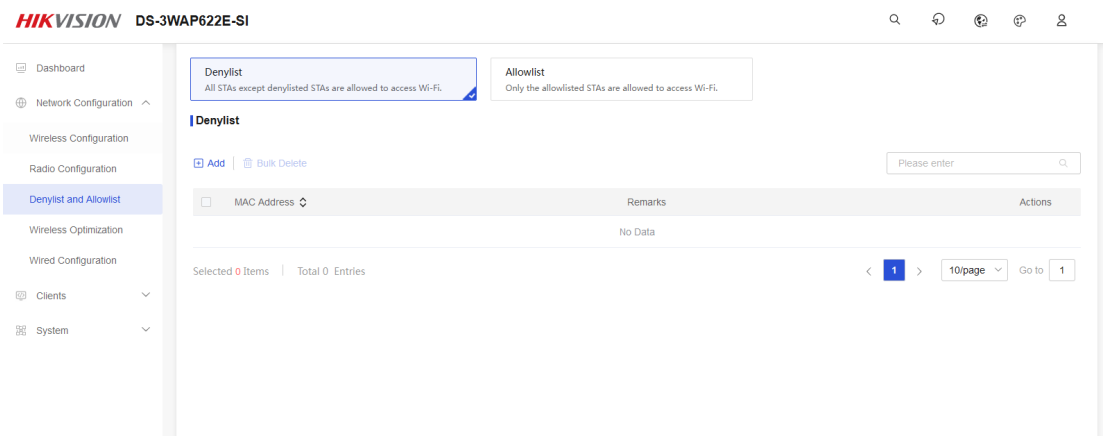
- **Denylist**: Forbid all clients in the denylist from accessing the wireless network. You can add a maximum of 64 client MAC addresses to the denylist. By default, the denylist is empty and all devices can access the wireless network.

- **Allowlist**: Allow only clients in the allowlist to access the wireless network. You can add a maximum of 64 client MAC addresses to the allowlist. If the allowlist is empty, all clients can access the wireless network.

To configure the denylist or allowlist:

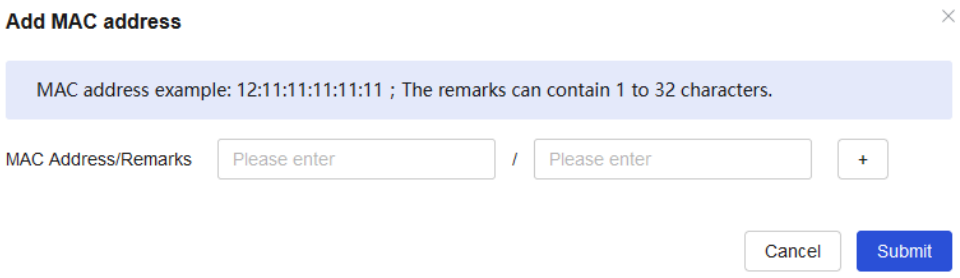
1. Add a client to the denylist or allowlist. Switching between allowlist and denylist forces all online clients to go offline.

   Figure 8 Configuring the allowlist or denylist



2. Click **Add** and enter the target client MAC address in the window that opens. Then, click **Submit**.

   Figure 9 Adding a client MAC address



Wireless optimization

On the **Wireless Optimization** page, configure features to optimize your wireless network.

Intelligent network optimization

Perform this task to enable automatic adjustment of radio channel and transmit power. It helps the wireless network quickly adapt to radio environment changes and maintain optimal radio resource conditions. The specific functions are as follows:

- Channel optimization

  In a WLAN, channel resources are limited, so each AP can only operate on a few channels. To optimize wireless performance, it is critical to intelligently assign the best channel to each AP.

  Intelligent network optimization can periodically scan and detect channels. It ensures that APs use the optimal channels and avoids interference from interference sources, such as radars and microwaves.

- Power optimization

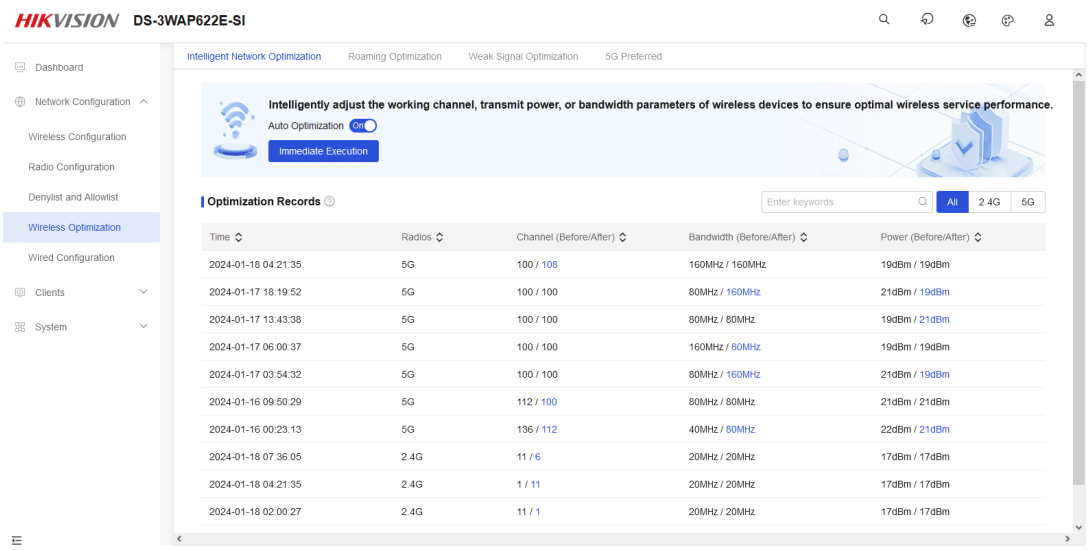
Traditional radio power control methods simply set the transmit power of a radio to the maximum value statically, focusing only on expanding the coverage area. However, excessive power might cause unnecessary interference to other radio equipment. Therefore, it is critical to select the optimal power that balances the coverage area of all radios and meets usage requirements.

Intelligent network optimization regularly measures inter-radio signal strength and automatically adjusts the transmit power to ensure optimal performance.

Intelligent network optimization supports both automatic and manual optimization:

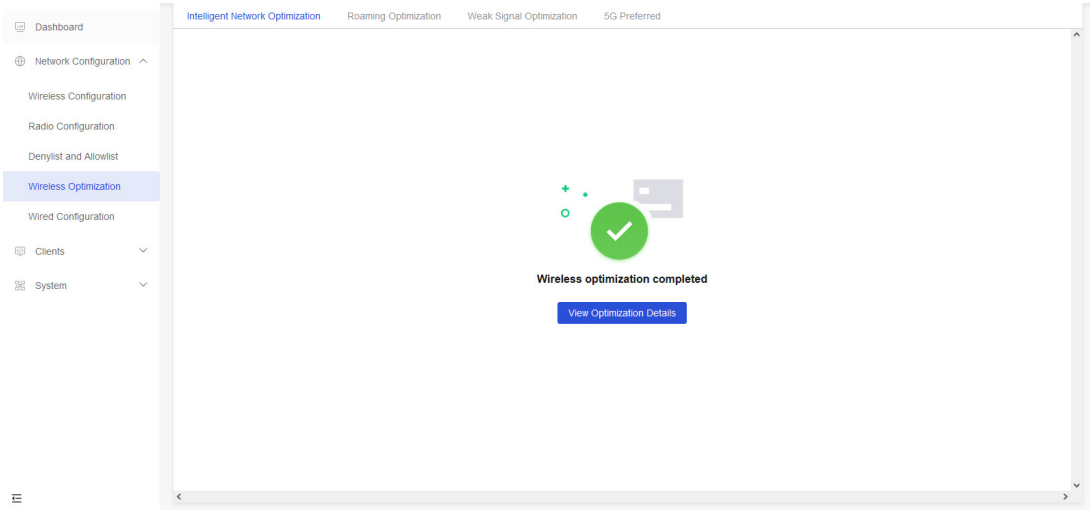
- **Auto optimization**: Enables the device to automatically adjust the power of 2.4GHz radios at intervals of 10 minutes and the channels of 2.4GHz and 5GHz radios at intervals of 80 minutes to 8 hours.

Figure 10 Auto optimization



- **Manual optimization**: You can manually optimize the power and channels of 2.4GHz radios, as well as the channels of 5GHz radios. The optimization process includes four steps: **Start** > **Scan** > **Optimize** > **Complete**. The process takes a few minutes. Do not close the page during the process. To stop optimization, click **Stop Optimization**.

Figure 11 Manual optimization



Once the optimization completes, you can view the optimization time, optimized radio, and channel and power settings before and after the optimization on the **Optimization Records** page.

Roaming optimization

Perform this task to optimize the roaming performance and adjust the roaming sensitivity. The roaming sensitivity defines the signal strength threshold for clients to initiate roaming as follows:

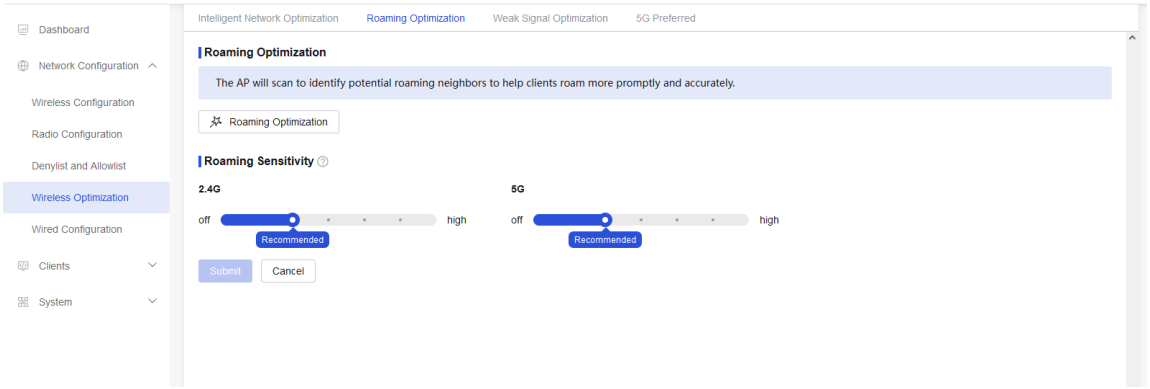
- A high roaming sensitivity allows clients to roam even if the signal strength is strong.
- A low roaming sensitivity means clients roam only when the signal strength is weak.

To configure roaming optimization:

1. Click **Roaming Optimization**. The APs will scan to identify potential roaming neighbors to help clients roam more promptly and accurately.
2. Manually adjust the roaming sensitivity, and then click **Submit**.

   In dense AP deployments, increase the roaming sensitivity to help clients connect to better APs with stronger signals. Decrease the roaming sensitivity in sparse deployments.

Figure 12 Roaming optimization

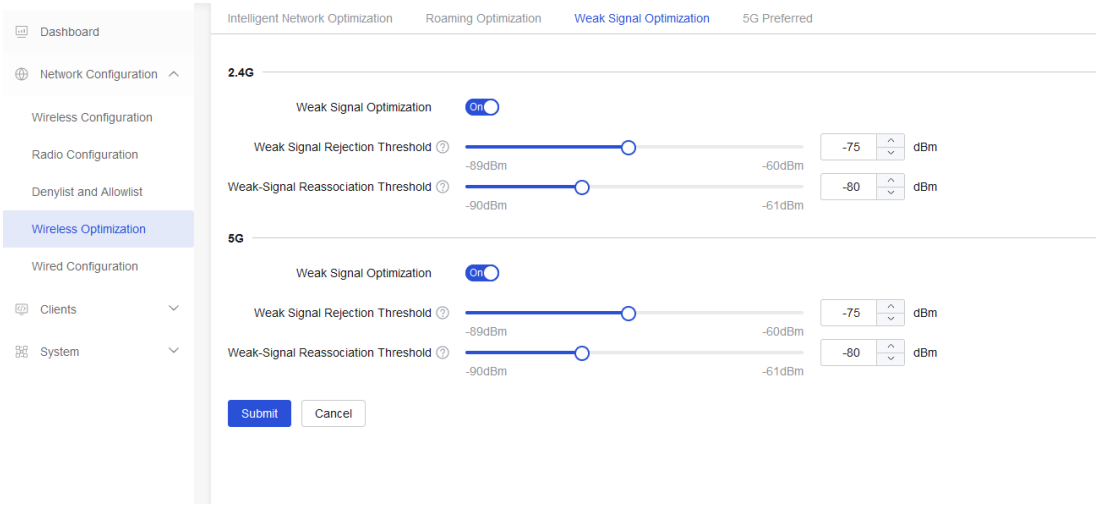


Weak signal optimization

Perform this task to prevent weak-signal clients from occupying excessive channel resources, thus reducing their impact on other clients in the network and improving the user experience.

- **Weak Signal Rejection Threshold**: For clients that have not accessed the wireless service, they will be unable to connect when the signal strength is below the threshold. A high threshold makes it difficult for clients to connect. Configure the threshold reasonably as required.
- **Weak-Signal Reassociation Threshold**: For clients that have accessed the wireless service, they will be forced to go offline and attempt to reconnect when the signal strength is below the threshold. Make sure the threshold is lower than the weak signal rejection threshold. Some specific clients might fail to connect to wireless services after repeated forced disconnections. Enable this feature with caution for such clients.

Figure 13 Weak signal optimization

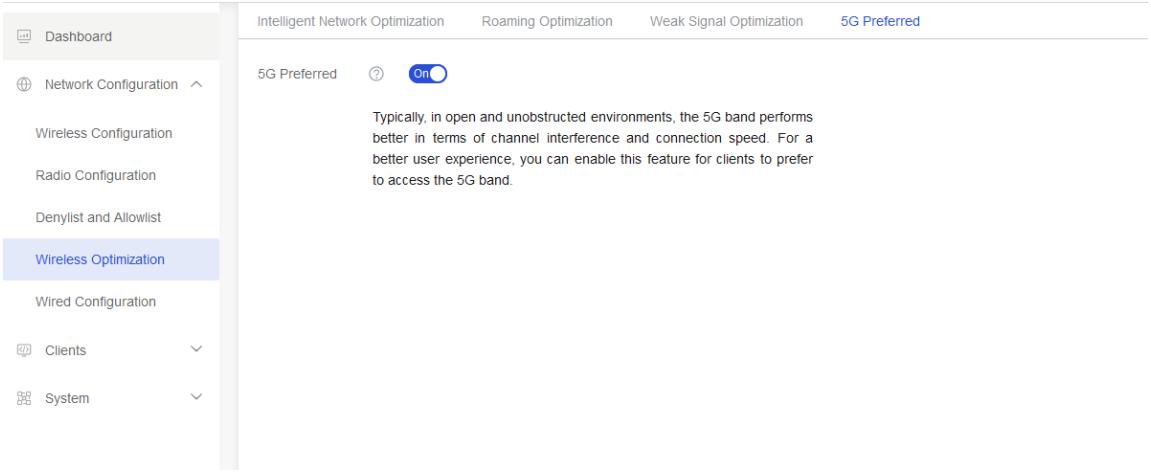


5G preferred

In a wireless network, some clients can only operate on the 2.4GHz band, while others can operate on either the 2.4GHz or 5GHz band. This might lead to the 2.4GHz radio being overloaded while the 5GHz radio underutilized. In this case, you can enable this feature for dual-band clients to first connect to 5GHz radios, which can balance the number of clients on both bands and improve the overall network performance.

With this feature enabled, the device guides clients with a signal strength above –45dBm on a 2.4GHz radio to roam to a 5GHz radio.

Figure 14 5GHz preferred



Wired configuration

From the left navigation pane, select **Network Configuration** > **Wired Configuration**. You can view the operating status of the UPLINK or LAN ports on the device and the device VLAN information.

UPLINK

You can view the operating status and assigned VLAN of the UPLINK ports on the device.

Figure 15 UPLINK

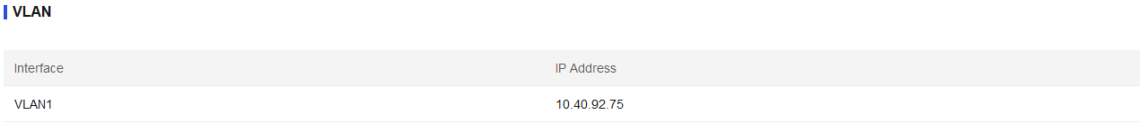
LAN

This feature is available only when the device has LAN ports. You can view the operating status and assigned VLAN of the LAN ports on the device.

VLAN

You can view the assigned VLAN and IP address of the device.

Figure 16 VLAN



Clients

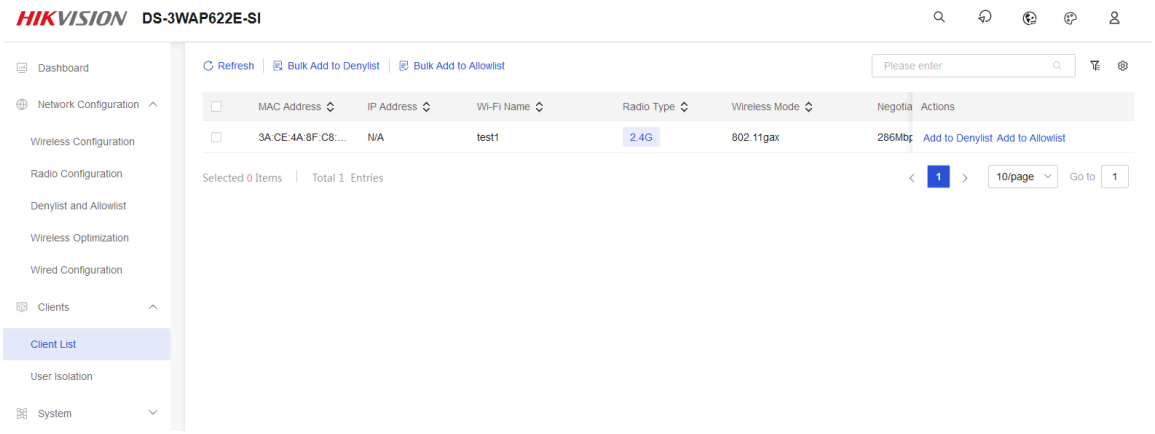
From the left navigation pane, select **Clients** to view the client list and configure the user isolation feature.

Client list

From the left navigation pane, select **Clients** > **Client list** to view the MAC address, IP address, Wi-Fi name, radio type, wireless mode, negotiated rate, uptime, and signal strength of the online clients.

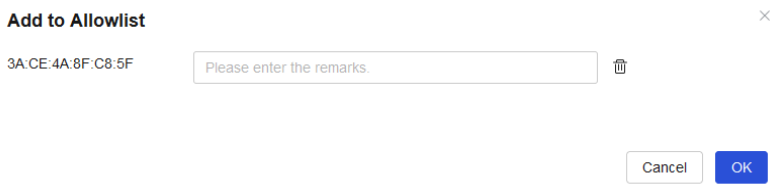
You can click the **Settings** icon in the upper-right corner to display more information, such as bandwidth, upstream traffic statistics, downstream traffic statistics, upstream real-time rate, and downstream real-time rate.

Figure 17 Client information



To add a client to the denylist, click **Add to Denylist** in the **Actions** column. To add multiple clients to the denylist, select the clients and click **Bulk Add to Denylist**. To add a client to the allowlist, click **Add to Allowlist** in the **Actions** column. To add multiple clients to the allowlist, select the clients and click **Bulk Add to Allowlist**. You can also enter remarks when adding a client to the denylist or allowlist.

Figure 18 Adding a client to the allowlist



User isolation

CAUTION:

User isolation might affect services that rely on Layer 2 discovery, such as screen casting or printing.

This feature isolates packets between clients within the same VLAN, achieving the purpose of protecting user privacy and reducing the number of packets in the network.

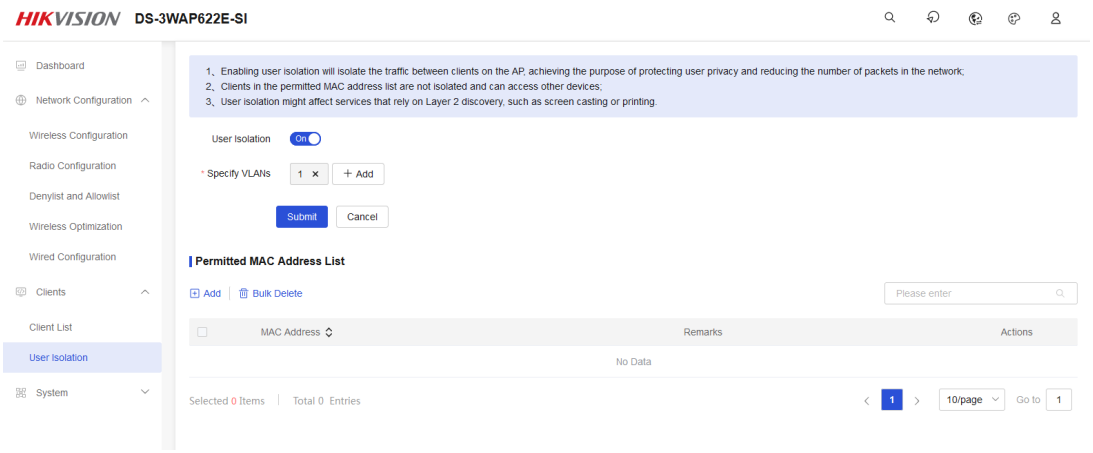
With this feature enabled, the device isolates clients in a VLAN effective on the device as follows:

- Unicast packets: The device directly discards the unicast packets.
- Broadcast/multicast packets: The device forwards the packets only to other clients in the same VLAN through wired interfaces, not to wireless clients in the effective VLAN.
- Permitted MAC address list: Clients in the permitted MAC address list are not isolated. You can add a maximum of 64 MAC addresses.

To configure user isolation:

1. Enable user isolation.
2. Specify VLANs that require user isolation.
3. Add permitted MAC addresses and remarks.

Figure 19 User isolation



System

From the left navigation pane, select **System** and configure device management, connection management, logs, version update, and network tools.

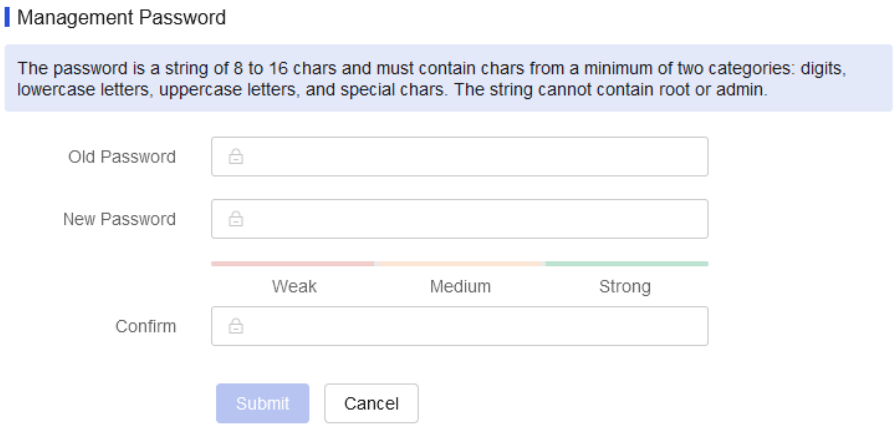
Device management

From the left navigation pane, select **System** > **Device Management** and configure the management password, LED, system time, device restart, and restore factory settings.

Management password

The management password is used to log into the Web interface of the network management platform. To change the management password, you must first enter the old password, and then set a new password as prompted.

Figure 20 Management password

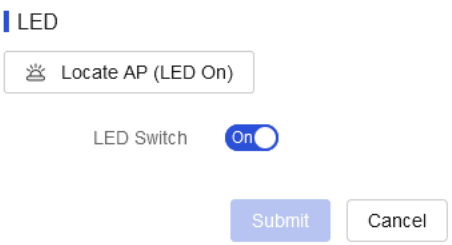


LED

Perform this task to control the device LED as follows:

- **Locate AP (LED On)**: Enable the device LED to flash at 4 Hz for 60 seconds, helping identifying the device.
- **LED Switch**: Turn on or turn off the device LED.

Figure 21 LED

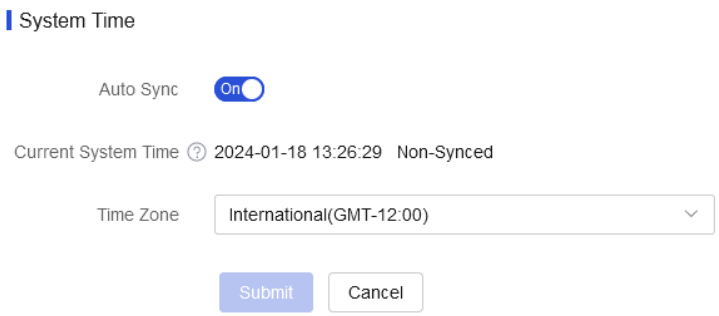


System time

Perform this task to enable automatic system time synchronization or configure the system time zone manually.

- Auto Sync: Allow the device to automatically synchronize the network time when it connects to the Internet.
- Current System Time: View and configure the current system time. If auto synchronization is enabled, you do not need to manually configure the system time. To manually configure the system time, disable auto synchronization and click **Edit**.
- Time Zone: Select the time zone for the device.

Figure 22 System time

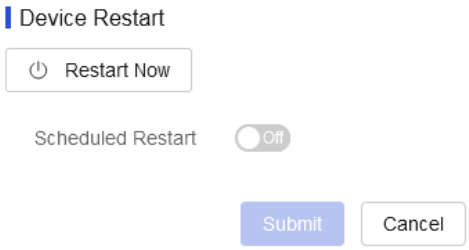


Device restart

Perform this task to save the device configuration and restart the device. You can configure the device to restart immediately or restart as scheduled.

If you select **Scheduled Restart**, you must also specify the restart time. The device restarts weekly at the scheduled time, for example, at 00:00 every Sunday.

Figure 23 Device restart



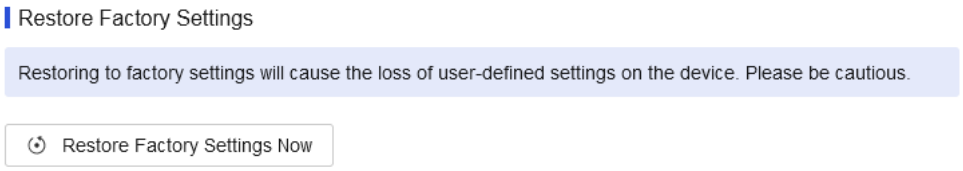
Factory restoration

CAUTION:

Restoring factory settings will cause the loss of user-defined settings on the device. Use this feature with caution.

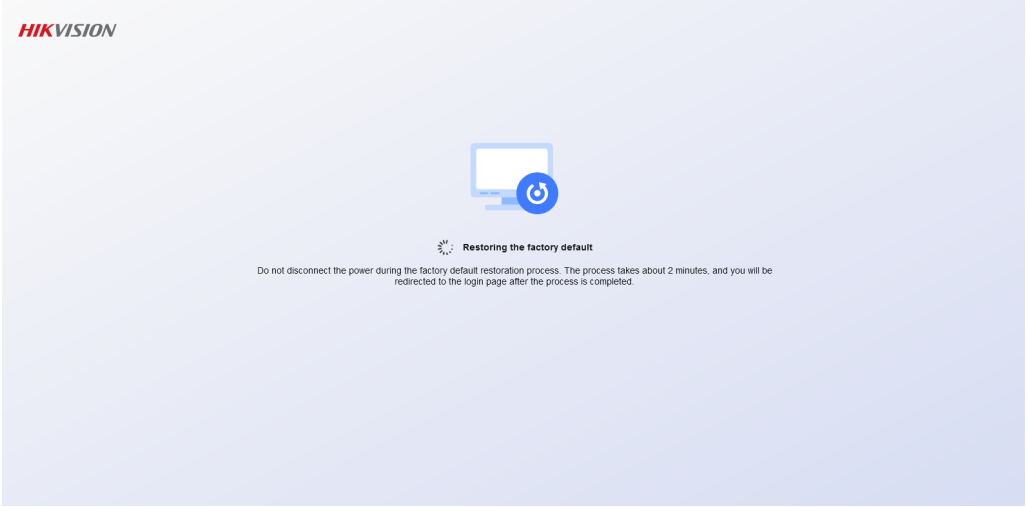
Click **Restore Factory Settings Now**, and confirm the operation in the dialog box that opens.

Figure 24 Restoring the factory setting



The restoration process takes about 2 minutes. You will be redirected to the login page upon completion.

Figure 25 Restoring factory settings



Connection management

From the left navigation pane, select **System** > **Connection Management** and configure the centralized management feature.

Centralized management

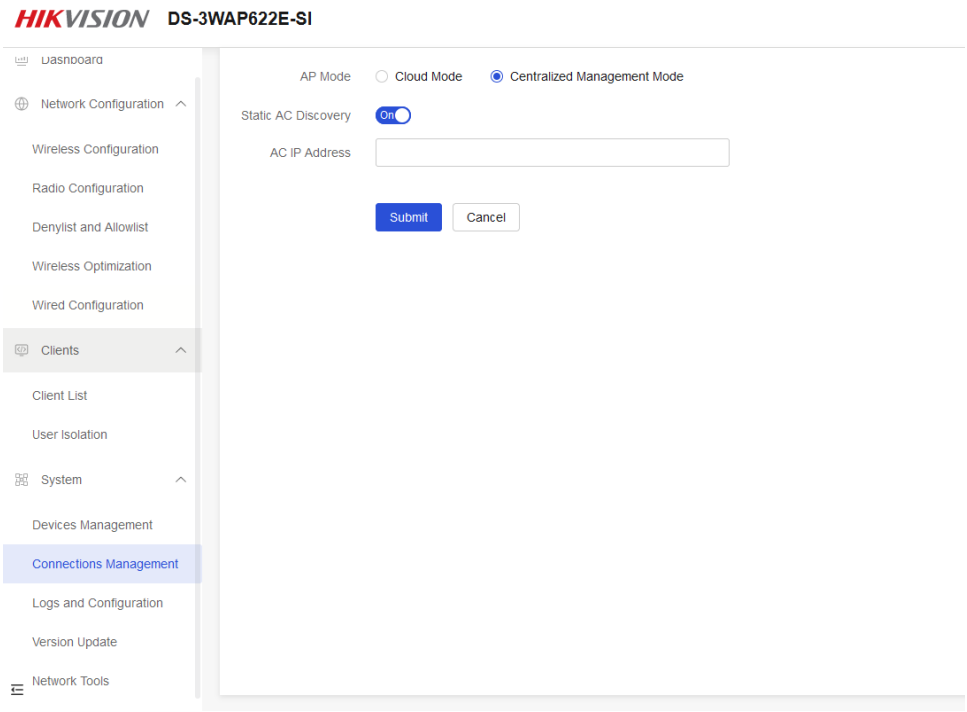
The device can discover ACs statically or dynamically and establish a CAPWAP tunnel with an AC for centralized management.

- **Static AC discovery**: Requires manual configuration of the AC IP address for an AP.
- **Dynamic AC discovery**: Supports the following methods:
  - **DHCP option method**: An AP obtains the IPv4 address of an AC through Option 43 returned by the DHCP server. This method supports both the IP address type and HEX type.
  - **Broadcast method**: An AP sends Discovery requests with broadcast address 255.255.255.255 as the destination address to discover ACs.

If the dynamic discovery method is used, an AP uses the DHCP option method and the broadcast method in turn to discover ACs. Once the AP establishes CAPWAP tunnels with the optimal AC, it stops AC discovery.

To use the static discovery method, enable **Static AC Discovery** and specify the IPv4 address of the AC.

Figure 26 Static AC discovery



To use the dynamic discover method, disable **Static AC Discovery**.

Figure 27 Dynamic AC discovery

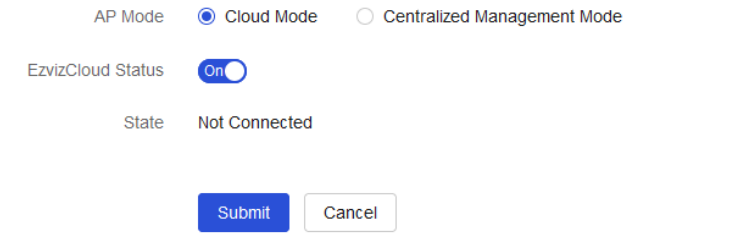
Cloud management

NOTE:

For the device to connect to the cloud platform, do not block the TCP port for cloud management on the upstream device.

You can enable or disable cloud mode as needed.

Figure 28 Cloud mode



Logs and configuration

From the left navigation pane, select **System** > **Logs and Configuration** to collect device logs and configurations.

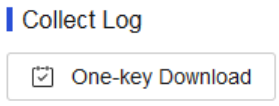
Log collection

CAUTION:

The system clears previously generated log messages and restarts logging after the device restarts. Back up the log messages before you reboot the device.

To download the system log file, click **One-key Download**. You can view the file in download history of the browser.

Figure 29 Collecting Logs



Configuration export

To export the configuration file, click **One-Key Export**. You can view the file in download history of the browser.

Figure 30 Exporting configuration

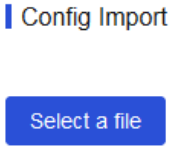
Configuration import

CAUTION:

Importing a configuration file restarts the device.

Perform this task to import a previously exported configuration file to the device and restore the previous settings. Click **Select a file** to import the saved configuration file to the device.

Figure 31 Importing Config



Version update

CAUTION:

To avoid device startup failures, do not power off the device during the update process.

To update the version of the device, select **System** > **Version Update** from the left navigation pane.

Offline update

Prerequisites

Download the version file from the official website and copy it to your PC. Then, log in to the Web management interface of the device from your PC.

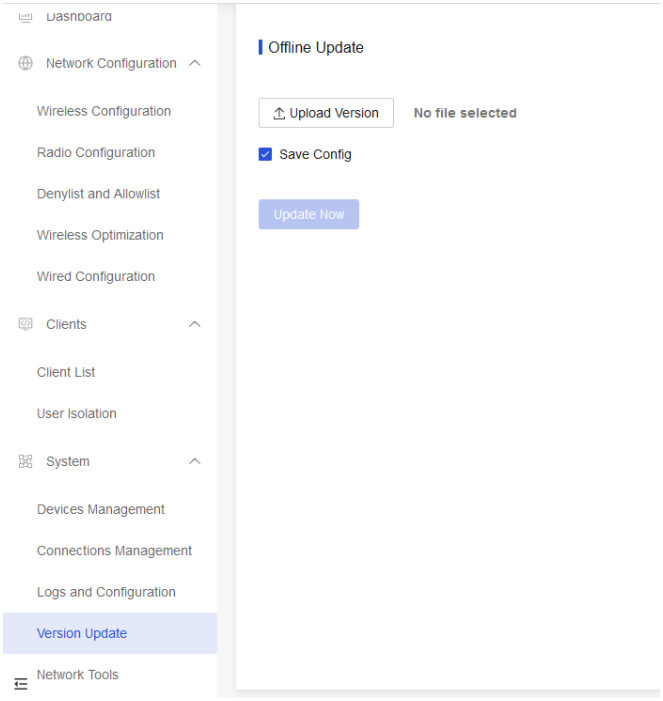
Procedure

1. From the left navigation pane, select **Dashboard**. View the current software version of the device in the **Device Info** section.
2. From the left navigation pane, select **System** > **Version Update**.
3. In the **Offline Update** section, click **Upload Version** and upload the version file from your PC.

   The system deletes the previous uploaded version file when you upload a new one.
4. To save the user-defined settings, select **Save Config**. If you do not do so, the system clears user-defined settings after the update. Then, click **Update Now**.

   After the device completes update, view the current software version of the device in the **Device Info** section on the **Dashboard** page.

Figure 32 Offline update



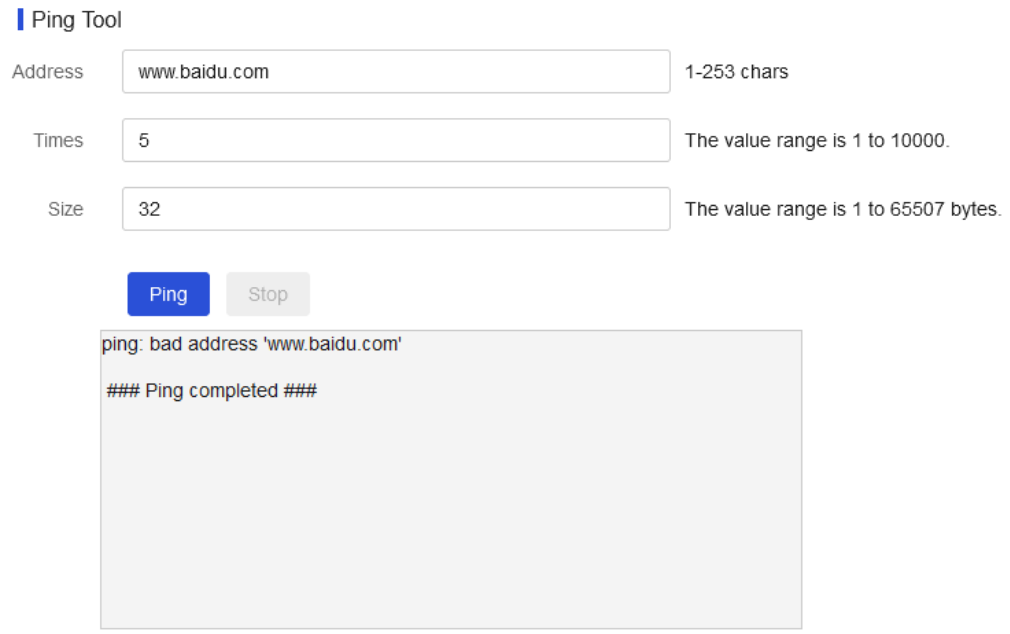
Network tools

Ping tool

The ping tool is used to examine whether the specified address is reachable.

From the left navigation pane, select **Network Tools** > **Ping Tool**. Enter the destination IP address or host name, specify the number of packet sendings and the packet size, and then click **Ping**.

Figure 33 Ping tool

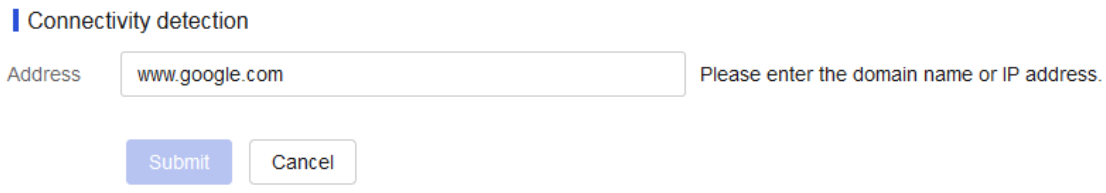


Connectivity detection

The connectivity detection is used to diagnose network connectivity.

From the left navigation pane, select **Network Tools** > **Connectivity detection**. Enter the domain name or IP address to be tested, and then click **Submit**. You can view the result in the **uplinkquality.log** file on the AP.

Figure 34 Connectivity detection



Traceroute tool

The traceroute tool is used to view the path that IPv4 packets take from the device to the destination.

In the **Traceroute Tool** dialog box, you can enter the destination IPv4 address or host name, and the click **Traceroute** to view the result.

Figure 35 Traceroute tool