HIKVISION

Smart Managed Switch

Network Security Hardening Guide

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.

Applicable Models

This manual is applicable to Smart Managed Switch • Network Security Hardening Guide.

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

Network security hardening is a comprehensive and systematic process that aims to enhance the security posture of a network infrastructure, systems, and applications. It involves a series of proactive measures and techniques designed to protect against a wide range of potential security threats and vulnerabilities.

In today's digital age, where organizations rely heavily on networked systems and the Internet for their day-to-day operations, the necessity of network security hardening cannot be overstated. The increasing prevalence of cyberattacks, such as malware infections, hacking attempts, data breaches, and denial-of-service (DoS) attacks, poses significant risks to the confidentiality, integrity, and availability of sensitive information and critical business processes.

A network that is not properly hardened is like an open door inviting malicious actors to exploit weaknesses and gain unauthorized access. This can lead to the theft of valuable data, including customer information, financial records, and intellectual property, which can have severe consequences for an organization's reputation, legal compliance, and financial stability. For example, a data breach can result in costly lawsuits, regulatory fines, and loss of customer trust, potentially leading to a decline in business revenues.

Moreover, network security vulnerabilities can also disrupt normal business operations. A successful DoS attack can render a network or website inaccessible, causing downtime and loss of productivity. In a highly competitive business environment, even a short period of downtime can have a significant impact on an organization's ability to serve its customers and maintain its market position.

By implementing network security hardening measures, we can significantly reduce the likelihood and impact of security incidents. Network security hardening is an essential aspect of any organization's overall security strategy. It is a proactive and continuous effort that helps protect against the ever-evolving threat landscape and ensures the secure and reliable operation of networked systems and applications.

Chapter 2 Initial Security Operations

2.1 Activating

Heading in this template has 4 levels: 1-level heading (Alt +F1), 2-level heading (Alt +F2), 3-level heading (Alt +F3), and 4-level heading (Alt +F4).

Section headings (Alt +F5) are also included in this template. Section headings like Purpose, Before You Start, Steps, Result, Example.

To enhance the security of the system and data, the initialization of the equipment is completed through an activation mechanism, and fixed initial passwords are no longer provided. Users can activate the equipment in several ways, namely through the SADP tool, client software, and web browser.

The factory default values of the equipment are as follows：

- The default IP address is： 192.168.1.64
- The default port is： 80
- The default username (administrator) is： admin

2.2 Password Security

2.2.1 Password settings need to comply with the requirements for common passwords and strong passwords.

The input of the equipment password is divided into four categories: digits, lowercase letters, uppercase letters, and special symbols. The levels are divided into three grades, and the specific definitions are as follows：

- Grade 0 (Risky Password): The password length is less than 8 characters, or it only contains any one of the four categories of characters.
- Grade 1 (Common Password): It contains two categories of characters and the length is greater than or equal to 8 characters.
- Grade 2 (Strong Password): It contains three or more categories of characters and the length is greater than or equal to 8 characters.

2.2.2 Avoid using common risky passwords.

The password should not contain the username, "123", "admin" (regardless of case), consecutive four or more digits in increasing or decreasing order (such as "1234", "12345", "4321", etc.), more than four consecutive identical characters (such as "1111", "8888", "aaaa", etc.), and the list of common risky passwords.

2.2.3 Set Complex Passwords

During the activation process or subsequent system maintenance, setting a complex password with a high security level can effectively ensure the security of the system. To enhance the security of the product's network usage, it is recommended to update the password once every three months. If the product has higher security requirements for the usage environment, it is advisable to update the password monthly or weekly.。

2.2.4 Password Error Limits

When a user enters an incorrect password, the device will display a lockout message as a reminder. If the "admin" user enters an incorrect password consecutively for seven times, the device will automatically enter a locked state.

2.2.5 Password Reset Limits

If the number of password reset attempts exceeds seven times, password reset operations will not be allowed within 30 minutes.

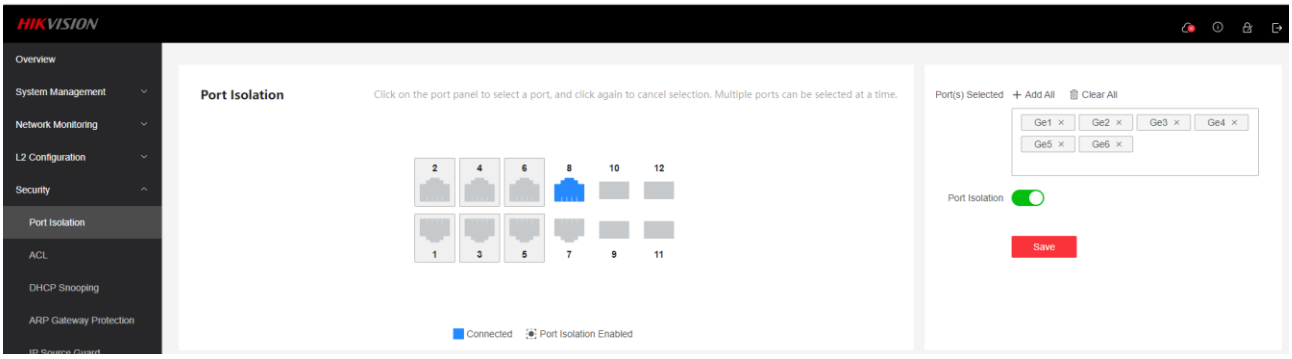
2.3 Remote Login Restrictions

Enabling the illegal login lock means that on the Web login interface, if the "admin" user enters the wrong password consecutively for seven times, a lockout message will be displayed as a reminder and the system will automatically enter a locked state.

Chapter 3 Security Management Business

3.1 Port Isolation

Limit the communication between different network ports to enhance network security. Ports within the same isolation group cannot communicate with each other. Through port isolation, direct communication between different users or devices in the internal network can be prevented, thereby reducing potential security threats.



Click on the port panel to select a port, and click again to cancel selection. Multiple ports can be selected at a time.

Port(s) Selected: Ge1 ×, Ge2 ×, Ge3 ×, Ge4 ×, Ge5 ×, Ge6 ×

Port Isolation: On

Figure 3-1 Port Isolation

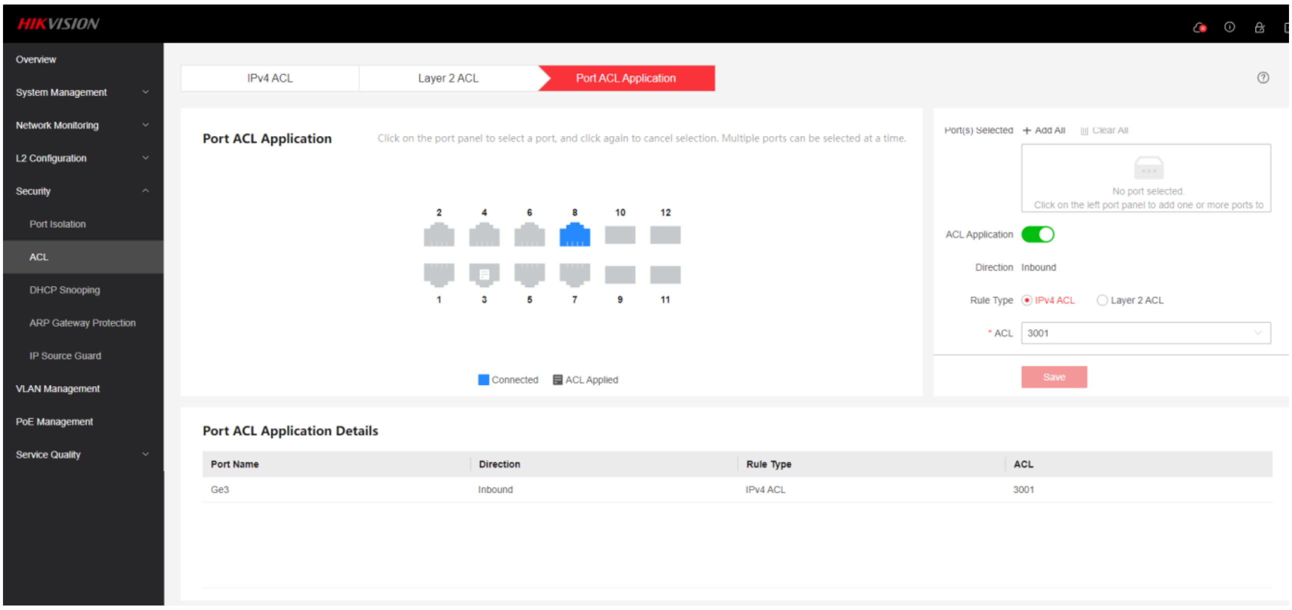
Step 2 Select "Main Menu → Security → Port Isolation".

Step 3 Select ports to enable the port isolation function.

Step 4 Click "Save", and the function will take effect.

3.2 ACL

Access Control List (ACL) is a security mechanism used in network devices to control the entry and exit of data packets in the network. By configuring ACL, it is possible to precisely control which data packets can enter or leave specific network interfaces, thereby enhancing network security.



Port ACL Application

Click on the port panel to select a port, and click again to cancel selection. Multiple ports can be selected at a time.

Port(s) Selected + Add All Clear All

No port selected.
Click on the left port panel to add one or more ports to

ACL Application: on

Direction: Inbound

Rule Type: ● IPv4 ACL ○ Layer 2 ACL

* ACL: 3001

Port ACL Application Details

Port Name	Direction	Rule Type	ACL
Ge3	Inbound	IPv4 ACL	3001

Figure 3-2 ACL

Step 2 Select "Main Menu → Security → ACL".

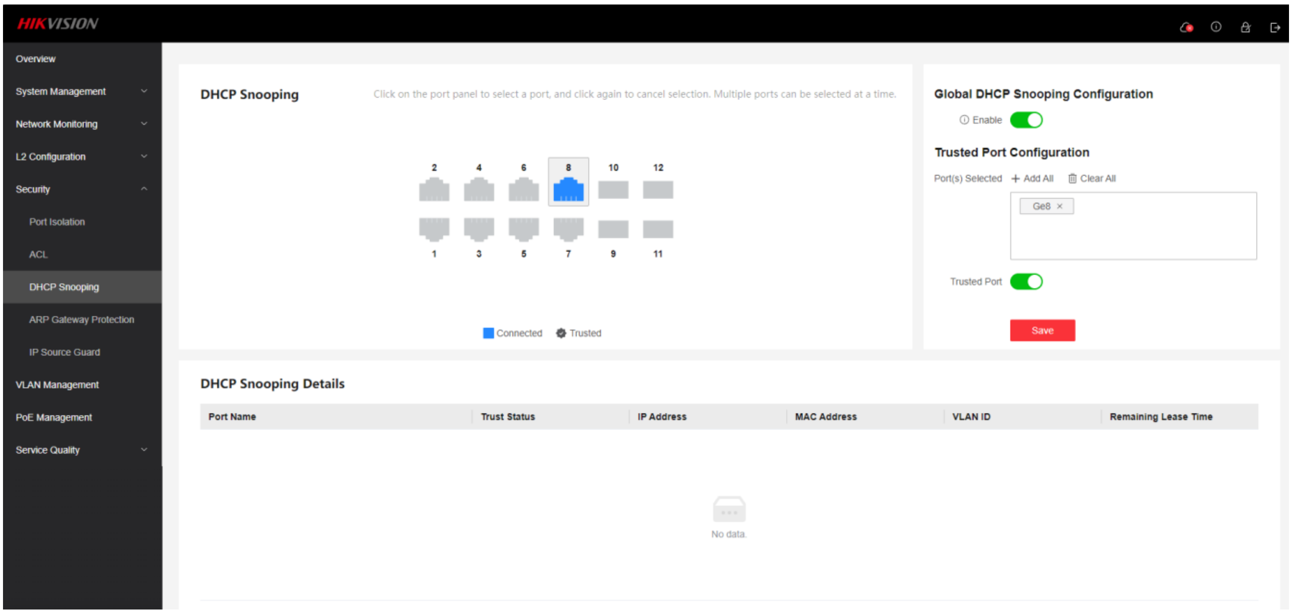
Step 3 Add IPv4 or Layer 2 ACL rules.

Step 4 Select ports and apply the created ACL rules.

Step 5 Click "Save", and the function will take effect.

3.3 DHCP Snooping

DHCP Snooping is a network security feature that is used to prevent unauthorized DHCP servers from providing IP addresses in a local area network, thus preventing DHCP spoofing attacks.



DHCP Snooping

Click on the port panel to select a port, and click again to cancel selection. Multiple ports can be selected at a time.

Global DHCP Snooping Configuration

Enable: on

Trusted Port Configuration

Port(s) Selected + Add All Clear All

Ge8 ×

Trusted Port: on

DHCP Snooping Details

Port Name	Trust Status	IP Address	MAC Address	VLAN ID	Remaining Lease Time

Figure 3-3 DHCP Snooping

Step 2 Select "Main Menu → Security → DHCP Snooping".

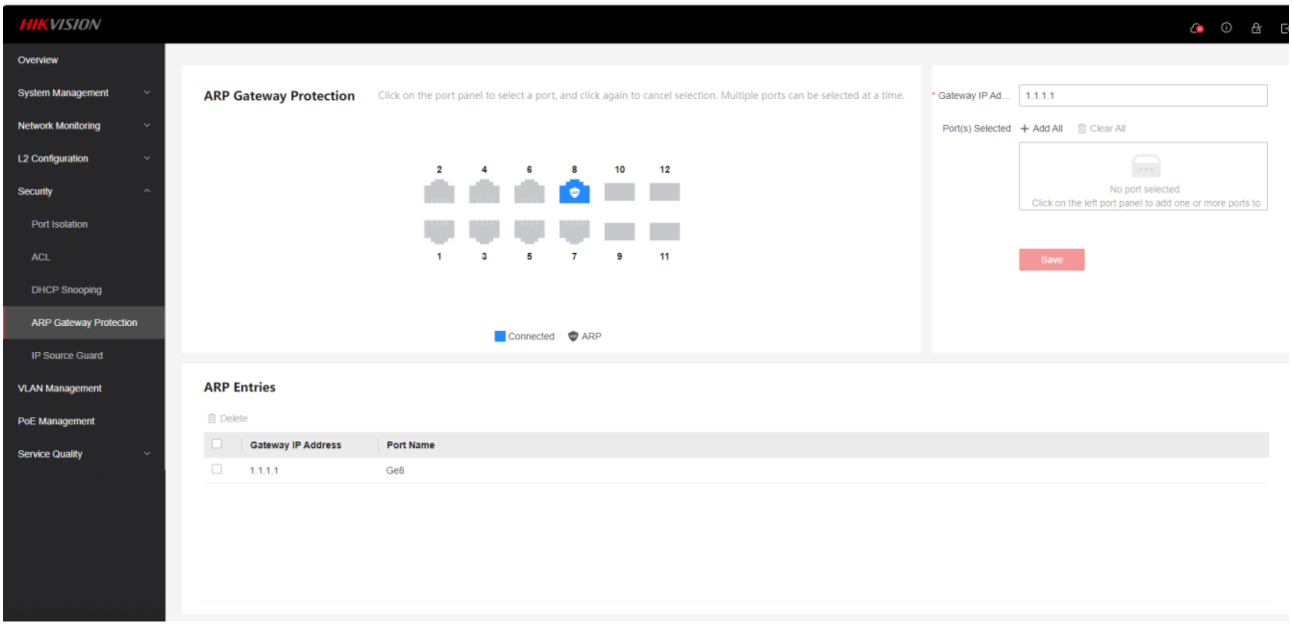
Step 3 Enable the DHCP Snooping function of the device.

Step 4 Select ports and enable port trust.

Step 5 Click "Save", and the function will take effect.

3.4 ARP Gateway Protection

Gateway ARP Protection is a network security measure used to prevent ARP (Address Resolution Protocol) spoofing attacks.



ARP Gateway Protection

Click on the port panel to select a port, and click again to cancel selection. Multiple ports can be selected at a time.

* Gateway IP Ad... 1.1.1.1

Port(s) Selected

No port selected.
Click on the left port panel to add one or more ports to

ARP Entries

□	Gateway IP Address	Port Name
□	1.1.1.1	Ge8

Figure 3-4 ARP

Step 2 Select "Main Menu → Security → ARP Gateway Protection".

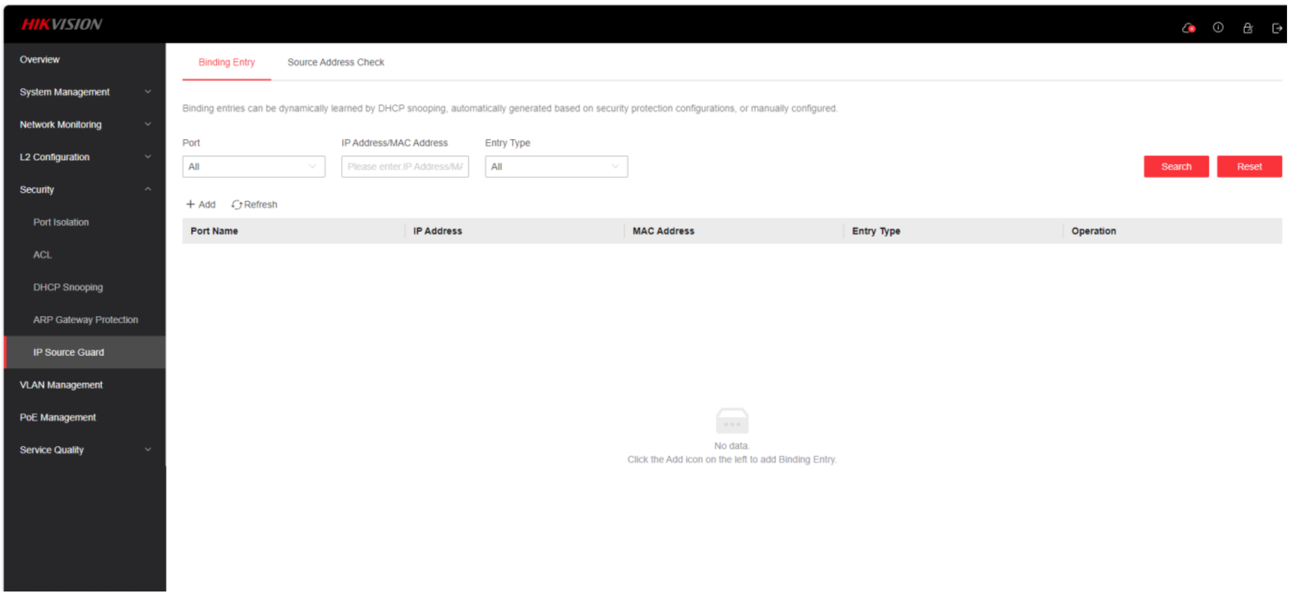
Step 3 Set the gateway address.

Step 4 Select ports and set the gateway protection address.

Step 5 Click "Save", and the function will take effect.

3.5 IPSG

IP Source Guard (IPSG) is a network security feature used to prevent unauthorized devices from using specific IP addresses in a local area network. IPSG prevents IP address spoofing and unauthorized use of IP addresses by checking the source IP address of each data packet to ensure that it complies with the configuration policies of network administrators.



Binding entries can be dynamically learned by DHCP snooping, automatically generated based on security protection configurations, or manually configured.

Port: All

IP Address/MAC Address: Please enter IP Address/M/

Entry Type: All

Port Name	IP Address	MAC Address	Entry Type	Operation

No data.
Click the Add icon on the left to add Binding Entry.

Figure 3-5 IPSG

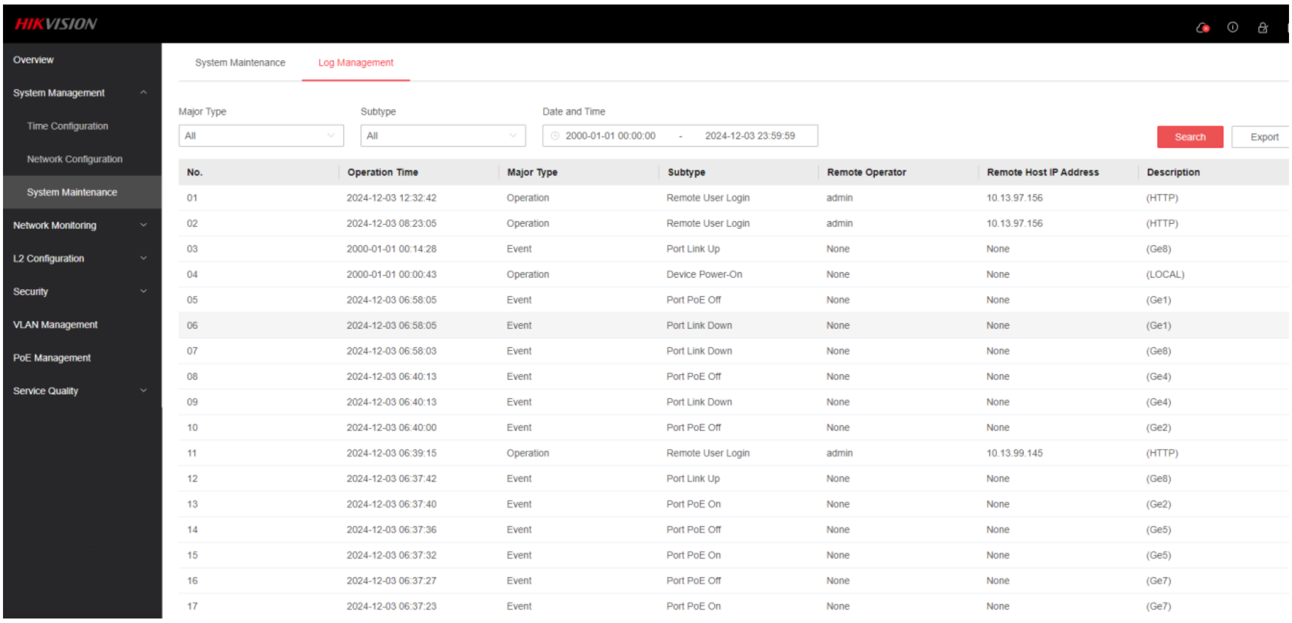
Step 2 Select "Main Menu → Security → IP Source Guard".

Step 3 Add binding entries and set ports, IP addresses or MAC addresses.

Step 4 Click "Save", and the entries will take effect.

Chapter 4 Log Query and Backup

The device provides functions for logging, classifying, querying and backing up logs. Log information, as one of the important ways to monitor the device, can record the operation information, operation records and alarm log information of the device, etc. It is recommended that users collect and back up device logs regularly.



Major Type: All
Subtype: All
Date and Time: 2000-01-01 00:00:00 - 2024-12-03 23:59:59

No.	Operation Time	Major Type	Subtype	Remote Operator	Remote Host IP Address	Description
01	2024-12-03 12:32:42	Operation	Remote User Login	admin	10.13.97.156	(HTTP)
02	2024-12-03 08:23:05	Operation	Remote User Login	admin	10.13.97.156	(HTTP)
03	2000-01-01 00:14:28	Event	Port Link Up	None	None	(Ge8)
04	2000-01-01 00:00:43	Operation	Device Power-On	None	None	(LOCAL)
05	2024-12-03 06:58:05	Event	Port PoE Off	None	None	(Ge1)
06	2024-12-03 06:58:05	Event	Port Link Down	None	None	(Ge1)
07	2024-12-03 06:58:03	Event	Port Link Down	None	None	(Ge8)
08	2024-12-03 06:40:13	Event	Port PoE Off	None	None	(Ge4)
09	2024-12-03 06:40:13	Event	Port Link Down	None	None	(Ge4)
10	2024-12-03 06:40:00	Event	Port PoE Off	None	None	(Ge2)
11	2024-12-03 06:39:15	Operation	Remote User Login	admin	10.13.99.145	(HTTP)
12	2024-12-03 06:37:42	Event	Port Link Up	None	None	(Ge8)
13	2024-12-03 06:37:40	Event	Port PoE On	None	None	(Ge2)
14	2024-12-03 06:37:36	Event	Port PoE Off	None	None	(Ge5)
15	2024-12-03 06:37:32	Event	Port PoE On	None	None	(Ge5)
16	2024-12-03 06:37:27	Event	Port PoE Off	None	None	(Ge7)
17	2024-12-03 06:37:23	Event	Port PoE On	None	None	(Ge7)

Figure 4-1 Log

Chapter 5 Data Recovery and Backup

5.1 System Restoration

If the device becomes abnormal due to issues such as unreasonable device parameter settings or system upgrades, the system restoration function can be used to restore the device parameters to the factory default state.

5.1.1 Restoration via Physical Buttons

Step 1: Press and hold the "reset" button on the device panel for more than 5 seconds.
Step 2: Release the "reset" button, and the device will automatically restart and restore to the factory default state.

5.1.2 Remote Restoration

Step 1 Select "Main Menu → System Maintenance → Full Restoration".

Step 2 Enter the device login password. After the verification is passed, the device will automatically restart and restore to the factory default state.

5.2 Configuration Backup

Data backup can prevent the loss of device configurations in abnormal situations and enable timely data restoration. The device supports the "export" operation for configuration files, facilitating the timely backup of configuration files。

Chapter 6 Security Response Mechanism

6.1 Approaches to Handling Security Issues

When users encounter security issues during the use of the equipment and are unable to resolve them, it is recommended to report them to Hikvision immediately. Hikvision will handle the issues according to the specific circumstances.

Two recommended handling approaches are as follows:

- If a security incident occurs on site, Hikvision's technical support engineers will provide remote or on-site support and work with customer personnel to mitigate the impact of the problem.

- If no security incident has occurred, Hikvision's technical support engineers will enter the problem into the database and transmit it to the R&D team. After the R&D team finds a solution, the technical support engineers will analyze the impact of implementing the solution on the on-site business and provide recommended solutions.

6.2 Security Emergency Contact Information

In case of an emergency, please seek help through Hikvision's official website or the customer service hotline.

See Far, Go Further