Network Security Guide

About This Document

This document provides necessary operations and configurations to help users secure network video recorder to enhance the network security.

Trademarks Acknowledgement

HIKVISION and other Hikvision’s trademarks and logos are the properties of Hikvision in various jurisdictions. Other trademarks and logos mentioned below are the properties of their respective owners.

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.

TABLE OF CONTENTS

Chapter 1 Introduction

As the network devices, when accessing to the network, may be exposed to the risk of network security.

To protect the device from possible network attack, Hikvision has promoted the network hardening for all the network devices, e.g., initial operation security, strong password requirement, disabling some network services as demand, etc. And for the users, you may also be aware of the security protection and take measures like checking the system logs, changing the password regularly, etc.

Chapter 2 Initial Access Security

2.1 Activating Your Device by Setting a Strong Password

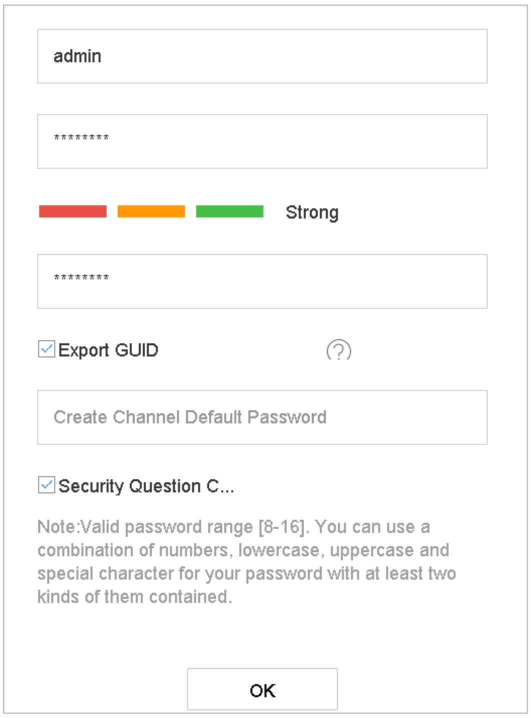
For the first-time access, you need to activate the device and IP camera (s) by setting an admin password. No operation is allowed before activation.

You can activate the device via local GUI, Web Browser, SADP or Client Software.

The following section we introduce the activation via local GUI and SADP as the example.

2.1.1 Activating via Local GUI

Step 1 Input the same password in the text field of **Create New Password** and **Confirm New Password**.



admin

****

🟥 🟧 🟩 Strong

****

☑ Export GUID

Create Channel Default Password

☑ Security Question C...

Note:Valid password range [8-16]. You can use a combination of numbers, lowercase, uppercase and special character for your password with at least two kinds of them contained.

Figure 2-1 Set Admin Password

WARNING

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.

Step 2 In the **Create Channel Default Password** text field, create a default password of IP camera (s) connected to the device.

Step 3 (Optional) Check **Export GUID** and **Security Question Configuration.**

Export GUID: export the GUID for future password resetting.

Security Question Configuration: configure the security questions which can be used for resetting the password.

Step 4 Click **OK**.

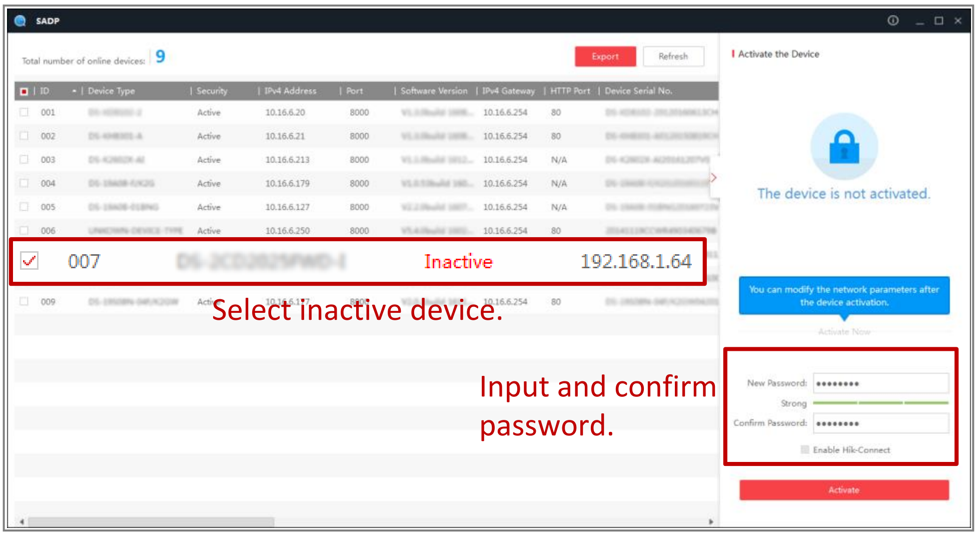
2.1.2 Activating via SADP Software

SADP software is used for detecting the online device, activating the device, and resetting the password.

Get the SADP software from the supplied disk or the official website, and install the SADP according to the prompts. Follow the steps to activate the device.

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

Step 2 Check the device status from the device list, and select the inactive device.



SADP

Total number of online devices: 9

ID	Device Type	Security	IPv4 Address	Port	Software Version	IPv4 Gateway	HTTP Port	Device Serial No.
001	[illegible]	Active	10.16.6.20	8000	[illegible]	10.16.6.254	80	[illegible]
002	[illegible]	Active	10.16.6.21	8000	[illegible]	10.16.6.254	80	[illegible]
003	[illegible]	Active	10.16.6.213	8000	[illegible]	10.16.6.254	N/A	[illegible]
004	[illegible]	Active	10.16.6.179	8000	[illegible]	10.16.6.254	N/A	[illegible]
005	[illegible]	Active	10.16.6.127	8000	[illegible]	10.16.6.254	N/A	[illegible]
006	UNKNOWN-DEVICE-TYPE	Active	10.16.6.250	8000	[illegible]	10.16.6.254	80	[illegible]
☑ 007	DS-2CD2025FWD-I	Inactive	192.168.1.64					
009	[illegible]	Active	10.16.6.177	8000	[illegible]	10.16.6.254	80	[illegible]

Select inactive device.

Activate the Device

The device is not activated.

You can modify the network parameters after the device activation.

New Password: ••••••••

Strong

Confirm Password: ••••••••

☐ Enable Hik-Connect

Input and confirm password.

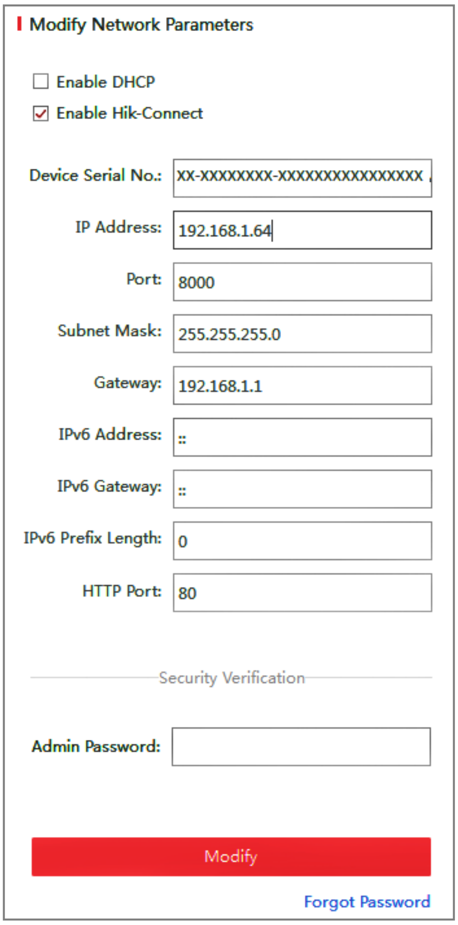
Figure 2-2 SADP Interface

Step 3 Create a password and input the password in the password field, and confirm the password.

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

You can check whether the activation is completed on the popup window. If activation failed, please make sure that the password meets the requirement and try again.

Step 5 Change the device IP address to the same subnet with your computer by either modifying the IP address manually or checking the checkbox of **Enable DHCP**.



Modify Network Parameters

☐ Enable DHCP
☑ Enable Hik-Connect

Device Serial No.:	XX-XXXXXXXX-XXXXXXXXXXXXXXXX
IP Address:	192.168.1.64
Port:	8000
Subnet Mask:	255.255.255.0
Gateway:	192.168.1.1
IPv6 Address:	::
IPv6 Gateway:	::
IPv6 Prefix Length:	0
HTTP Port:	80

Security Verification

Admin Password:

Figure 2-3 Modify the IP Address

Step 6 Input the password and click the **Modify** button to activate your IP address modification.

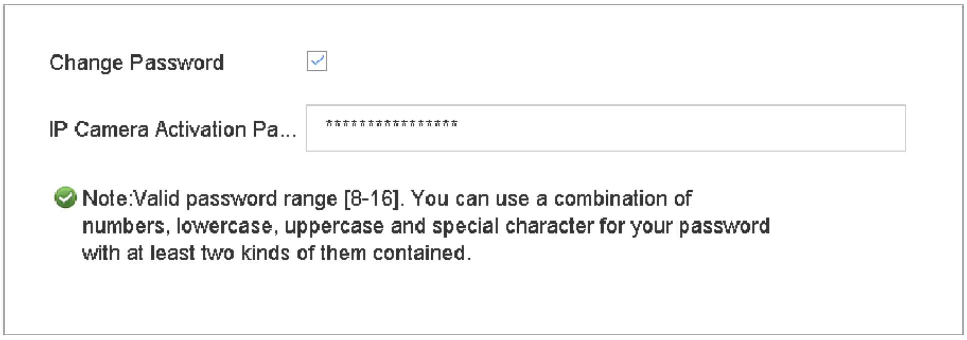
2.2 Managing IP Camera Activation

When you activate the device for the first-time access, you can set the activation password for the IP camera (s) as well. Refer to Chapter 2.1 Activating Your Device by Setting a Strong Password. And you can also manage the password to enhance the security.

Step 1 Go to **Menu** > **Maintenance** > **System Service** > **IP Camera Activation**.

Step 2 Check the **Change Password** to enable the permission.

Step 3 Enter the admin password of the device to obtain the permission.



Change Password ☑

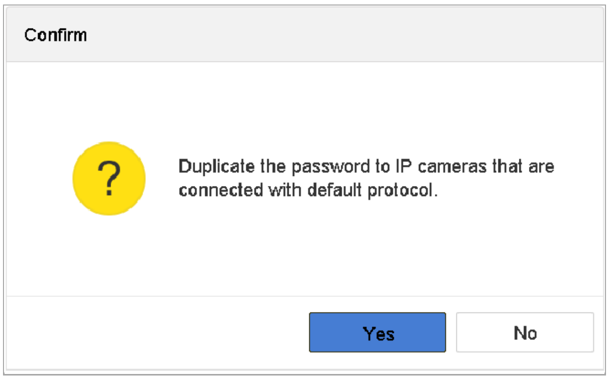
IP Camera Activation Pa... ****************

Note:Valid password range [8-16]. You can use a combination of numbers, lowercase, uppercase and special character for your password with at least two kinds of them contained.

Figure 2-4 Change IP Camera Activation Password

Step 4 In the text filed of the **IP Camera Activation Password**, enter the new strong password for the cameras. Refer to Chapter 2.1 Password Security for the strong password requirement.

Step 5 Click **Apply** to have the following pop-up attention box.



Confirm

Duplicate the password to IP cameras that are connected with default protocol.

Figure 2-5 Attention

Step 6 Click **Yes** to duplicate the current password to the IP cameras which are connected with the default protocol.

2.3 Password Security

2.3.1 Password Settings

Strong Password Requirement

During the device activation and the password change, we highly recommend you create a strong password of your own choosing 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.

Wrong Password Denied

The IP address will be locked if the admin user performs 7 failed user name/password attempts (5 times for the operator/user).

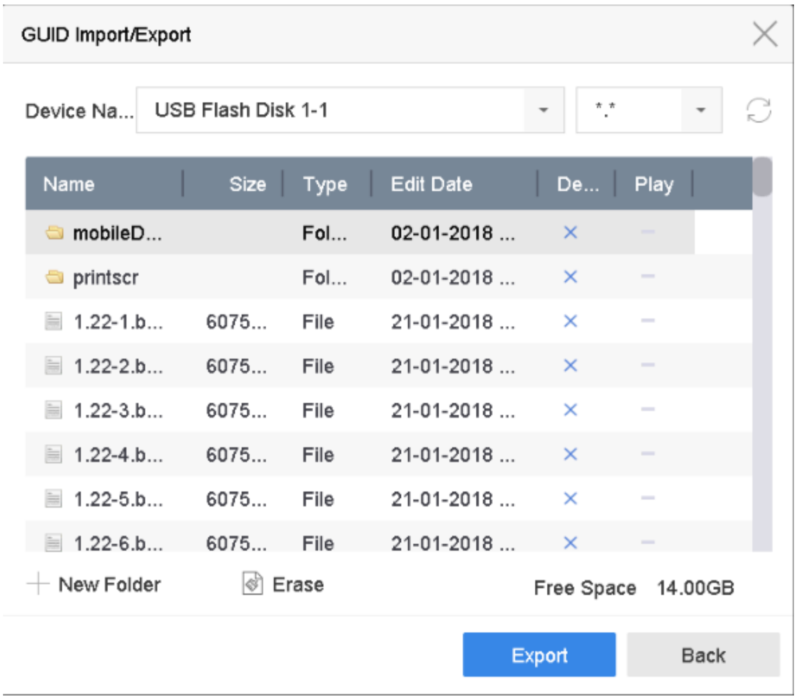
2.4 Configure Password Security

2.4.1 Export GUID File

The GUID file may help you to reset password when you forget password.

Step 1 Select to export GUID file when you are activating the device, or editing the admin user account.

Step 2 Insert the U flash disk to your device, and export the GUID file to the U flash disk.



GUID Import/Export

Device Na... USB Flash Disk 1-1 *.*

Name	Size	Type	Edit Date	De...	Play
mobileD...		Fol...	02-01-2018 ...	×	−
printscr		Fol...	02-01-2018 ...	×	−
1.22-1.b...	6075...	File	21-01-2018 ...	×	−
1.22-2.b...	6075...	File	21-01-2018 ...	×	−
1.22-3.b...	6075...	File	21-01-2018 ...	×	−
1.22-4.b...	6075...	File	21-01-2018 ...	×	−
1.22-5.b...	6075...	File	21-01-2018 ...	×	−
1.22-6.b...	6075...	File	21-01-2018 ...	×	−

Free Space 14.00GB

Figure 2-6 Export GUID File

NOTE

Please keep your GUID file properly for future password resetting.

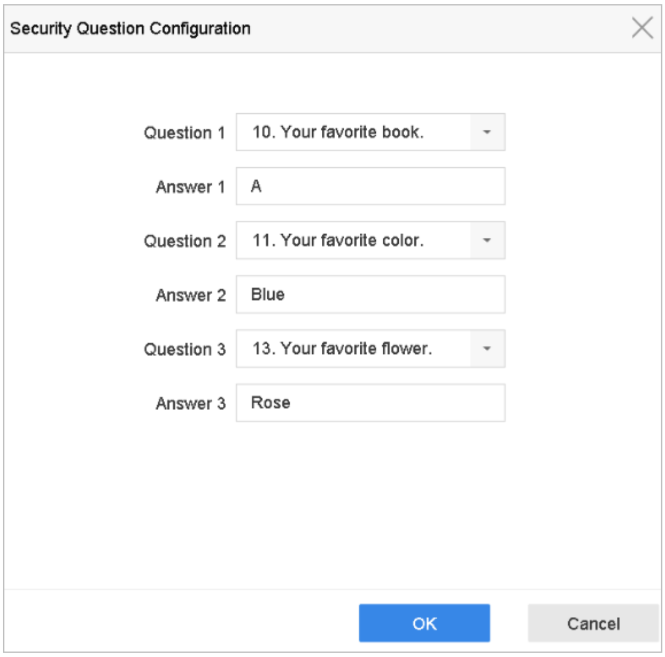
2.4.2 Configure Security Questions

The security question configuration may help you to reset password when you forget your password or encounter security issues.

Step 1 Click **Security Question Configuration** when you are activating the device, or editing the admin user account.

Step 2 Select three security questions from the drop-down list and input the answers.

Step 3 Click **OK**.



Security Question Configuration

Question 1: 10. Your favorite book.

Answer 1: A

Question 2: 11. Your favorite color.

Answer 2: Blue

Question 3: 13. Your favorite flower.

Answer 3: Rose

Figure 2-7 Configure Security Questions

2.5 Reset Password

When you forget the admin password, you can reset the password by importing the GUID file or by answering security questions.

2.5.1 Reset Password by GUID

Before You Start

The GUID file must be exported and saved in the local U flash disk after you have activated the device or edited the admin user account. (Refer to Chapter 2.4.1 Export GUID File).

Step 1 On the user login interface, click **Forgot Password**.

Step 2 Select the password resetting type to **Verify by GUID**.

NOTE

Please insert the U flash disk stored with the GUID file to the NVR before resetting password.

Step 3 Select the GUID file from the U flash disk and click **Import** to import the file to the device.

NOTE

If you have imported the wrong GUIE file for 7 times, you will be not allowed to reset the password for 30 minutes.

Step 4 After the GUID file is successfully imported, enter the reset password interface to set the new admin password.

Step 5 Click **OK** to set the new password. You can export the new GUID file to the U flash disk for future password resetting.

NOTE

When the new password is set, the original GUID file will be invalid. The new GUID file should be exported for future password resetting. You can also enter the User>User Management interface to edit the admin user and export the GUID file.

2.5.2 Reset Password by Security Questions

Before You Start

You have configured the security questions when you activate the device or edit the admin user account. (Refer to Chapter 2.4.2 Configure Security Questions).

Step 1 On the user login interface, click **Forgot Password**.

Step 2 Select the password resetting type to **Verify by Security Question**.

Step 3 Input the correct answers of the three security questions.

Step 4 Click **OK**.

NOTE

If the answers mismatch, the verification is failed.

Create the new admin password on the **Reset Password** interface.

2.5.3 Menu Auto Logout

You can set the auto logout of the device to enable the current user account, after a period of no operation, to automatically log out from the system. And you must log in to the system again to restore the operation.

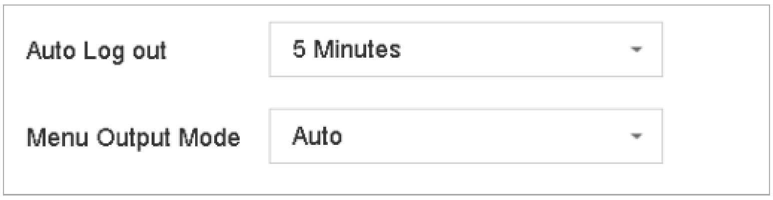
Step 1 Go to **Menu** > **System** > **General.**

Step 2 Set the **Auto Logout** to 1/2/5/10/20/30 minutes.

Step 3 Click **Apply**.

Example:

When the auto logout time is set to 5 Minutes, the system will exit from the current operation menu to live view screen after 5 minutes of menu inactivity.



Auto Log out: 5 Minutes

Menu Output Mode: Auto

Figure 2-8 Auto Logout

Chapter 3 User Account Management

3.1 Setting User Permissions

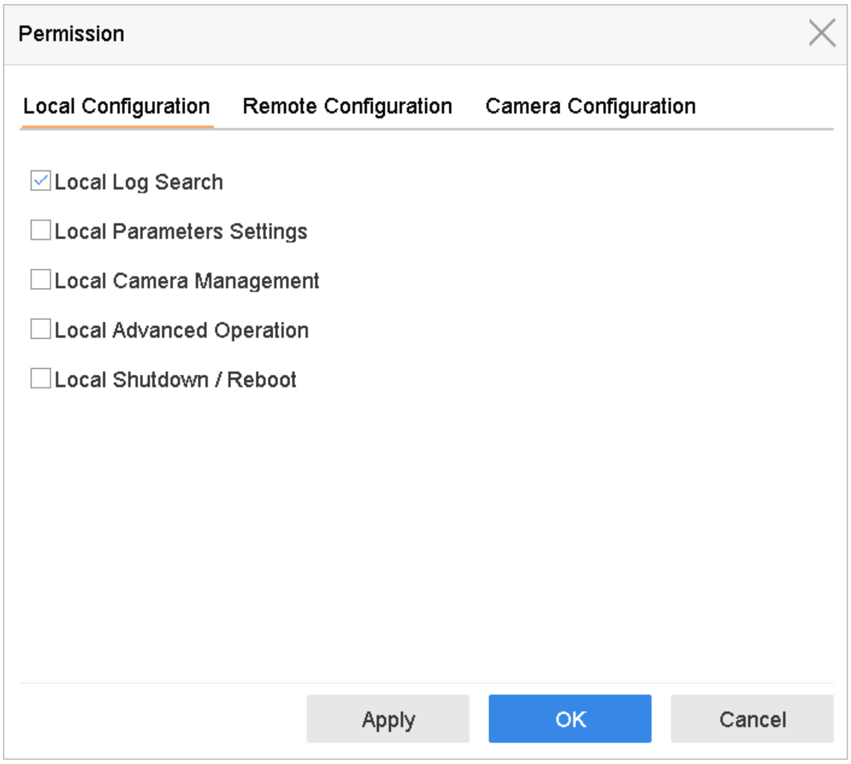
3.1.1 Setting Permissions to Multi-level Users

The *administrator* user account can create two levels of user accounts: operator and guest. And different user can be assigned with the different operating permissions. By default, the operator and guest users have different permissions.

Step 1 Go to **Menu** > **System** > **User**.

Step 2 Select a user (operator/guest) from the list.

Step 3 Click ✓ to enter the permission settings interface.



☑ Local Log Search

□ Local Parameters Settings

□ Local Camera Management

□ Local Advanced Operation

□ Local Shutdown / Reboot

Figure 3-1 User Permission Settings Interface

Step 4 Set the operating permission of Local Configuration, Remote Configuration and Camera Configuration for the user.

Step 5 Click **OK** to save the settings.

3.1.2 Set Local Live View Permissions for Non-Admin Users

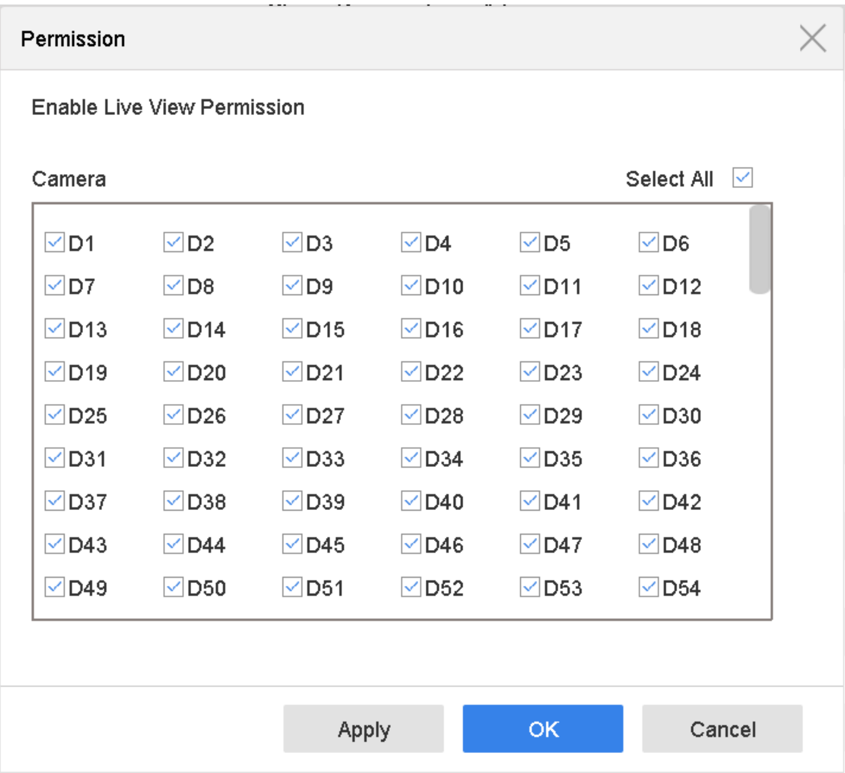
The admin user can assign to normal users (Operator or Guest) the live view permission for specific cameras.

Step 1 Go to **System** > **User**.

Step 2 Click ✓ of the admin user.

Step 3 Input admin password and click **OK**.

Step 4 Select cameras that a non-admin user can view locally and click **OK.**



Permission

Enable Live View Permission

Camera

Select All ☑

☑D1	☑D2	☑D3	☑D4	☑D5	☑D6
☑D7	☑D8	☑D9	☑D10	☑D11	☑D12
☑D13	☑D14	☑D15	☑D16	☑D17	☑D18
☑D19	☑D20	☑D21	☑D22	☑D23	☑D24
☑D25	☑D26	☑D27	☑D28	☑D29	☑D30
☑D31	☑D32	☑D33	☑D34	☑D35	☑D36
☑D37	☑D38	☑D39	☑D40	☑D41	☑D42
☑D43	☑D44	☑D45	☑D46	☑D47	☑D48
☑D49	☑D50	☑D51	☑D52	☑D53	☑D54

Figure 3-2 Set Live View Permissions

Step 5 Click ✓ of non-admin user.

Step 6 Click the **Camera Configuration** tab.

Step 7 Select Camera Permission as **Local Live View**.

Step 8 Select cameras to display in Live View.

Step 9 Click **OK**.

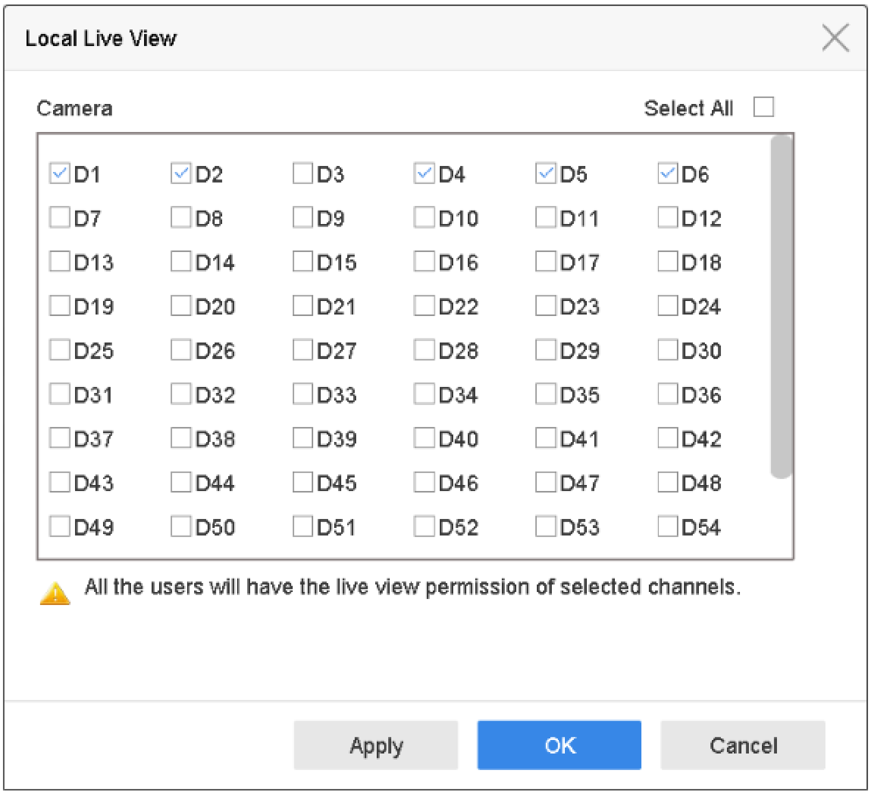
3.1.3 Set Live View Permissions on Lock Screen

The admin user can set live view permission for specific cameras in the screen lock status of device.

Step 1 Go to **System** > **User**.

Step 2 Click **Live View Permission on Lock Screen**.

Step 3 Input admin password and click **Next.**



Local Live View

Camera Select All □

☑ D1	☑ D2	□ D3	☑ D4	☑ D5	☑ D6
□ D7	□ D8	□ D9	□ D10	□ D11	□ D12
□ D13	□ D14	□ D15	□ D16	□ D17	□ D18
□ D19	□ D20	□ D21	□ D22	□ D23	□ D24
□ D25	□ D26	□ D27	□ D28	□ D29	□ D30
□ D31	□ D32	□ D33	□ D34	□ D35	□ D36
□ D37	□ D38	□ D39	□ D40	□ D41	□ D42
□ D43	□ D44	□ D45	□ D46	□ D47	□ D48
□ D49	□ D50	□ D51	□ D52	□ D53	□ D54

⚠ All the users will have the live view permission of selected channels.

Figure 3-3 Set Live View Permissions on Lock Screen

Step 4 Set the permissions.

- Select the camera (s) to allow live view when the current user account is in logout status.
- Deselect the camera (s) to forbidden the camera (s) being viewed when the current user account is in logout status.

Step 5 Click **OK**.

NOTE

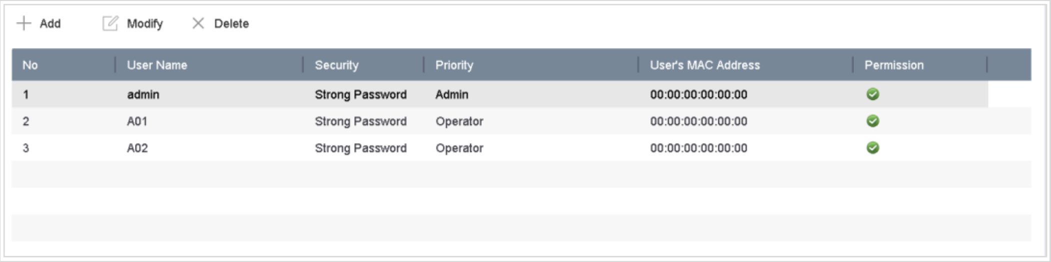
- The *admin* user can set this permission for user accounts.
- When the normal user (Operator or Guest) has no local live view permission for specific camera (s) (refer to 3.1.2 Set Local Live View Permissions for Non-Admin Users), the live view permission for such camera (s) on lock screen status cannot be configured (live view not allowed by default).

3.2 Deleting Idle User

We recommend you regularly delete the idle user accounts (if exist) on the device to avoid some unnecessary operations.

Step 1 Go to **Menu** > **System** > **User**.

Step 2 Select a user from the list to delete.



No	User Name	Security	Priority	User's MAC Address	Permission
1	admin	Strong Password	Admin	00:00:00:00:00:00	✓
2	A01	Strong Password	Operator	00:00:00:00:00:00	✓
3	A02	Strong Password	Operator	00:00:00:00:00:00	✓

Figure 3-4 User List

Step 3 Click **Delete** to delete the selected user account.

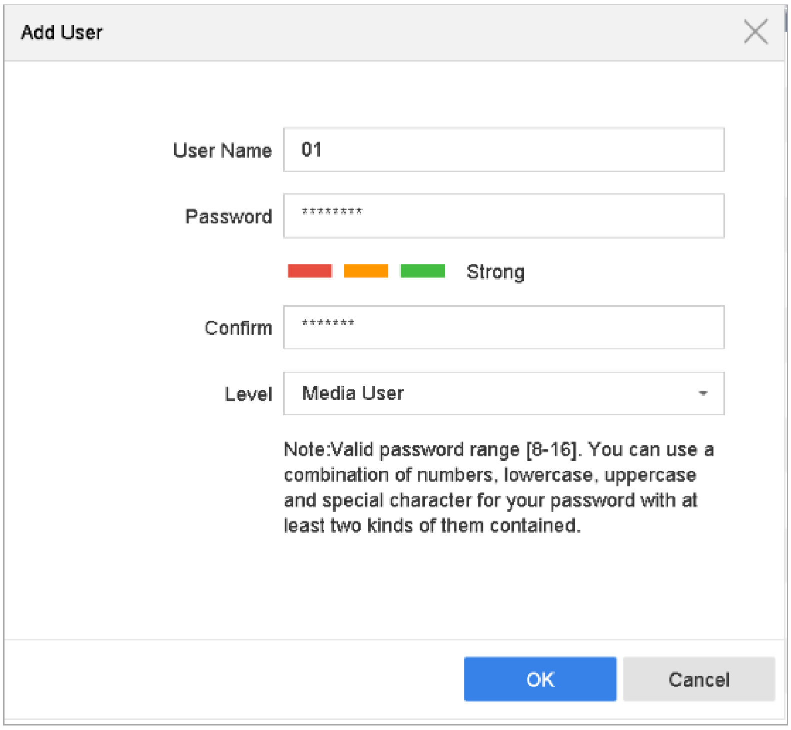
3.3 Managing ONVIF User Accounts

For the third-party camera connection to the device via ONVIF, you can enable ONVIF function and manage the user accounts.

Step 1 Go to **Menu** > **Maintenance** > **System Service** > **ONVIF**.

Step 2 Check **Enable ONVIF** to enable the ONVIF access management.

Step 3 Click **Add** to enter the Add User interface.



User Name: 01

Password: ********

🟥 🟧 🟩 Strong

Confirm: *******

Level: Media User

Note:Valid password range [8-16]. You can use a combination of numbers, lowercase, uppercase and special character for your password with at least two kinds of them contained.

Figure 3-5 Add User

Step 4 Edit the user name, and enter the strong password.

Step 5 Select the user level to **Media User**, **Operator** and **Admin**.

Step 6 Click **OK** to save the settings.

Result:

The added user accounts have the permission to connect other devices to the DVR/NVR via ONVIF protocol.

NOTE

ONVIF protocol is disabled by default.

Chapter 4 Remote Access Control

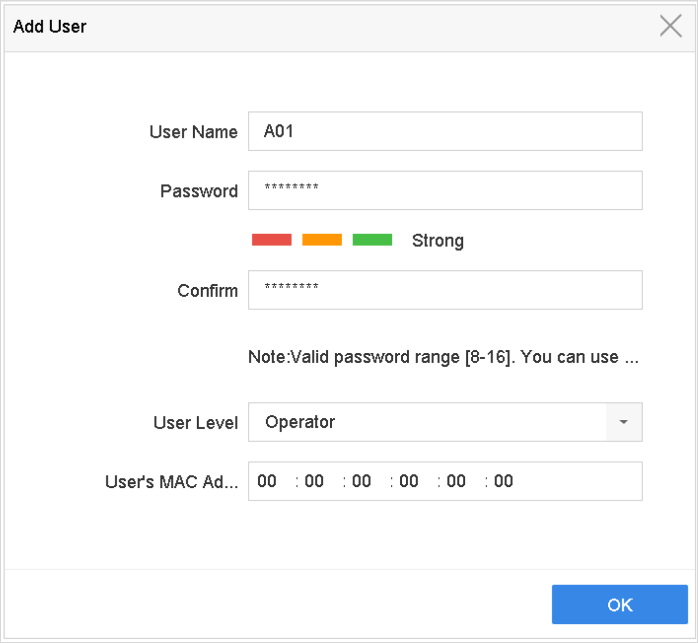
4.1 Setting User's MAC Address

The User's MAC address refers to MAC address of the remote PC which logs onto the device. If it is configured and enabled, it only allows the remote user with this MAC address to access the device.

Step 1 Go to **Menu** > **Configuration** > **User**.

Step 2 Click **Add** to enter the Add User interface.

Step 3 Enter the information for new user, including **User Name**, **Admin Password, Password**, **Confirm**, **Level** and **User's MAC Address**.



Add User

User Name	A01
Password	********
	🟥 🟧 🟩 Strong
Confirm	********
	Note:Valid password range [8-16]. You can use ...
User Level	Operator
User's MAC Ad...	00 : 00 : 00 : 00 : 00 : 00

Figure 4-1 Add User Menu

Step 4 Click **OK** to save the settings.

4.2 Illegal Access Lock

The user account will be locked if the admin user performs 7 failed user name/password attempts (5 times for the operator/user).

NOTE

If the user account is locked, you can try to log in the device only after 30 minutes.

Chapter 5 System Services

5.1 Removing Services

The following functions and services are removed for network security:

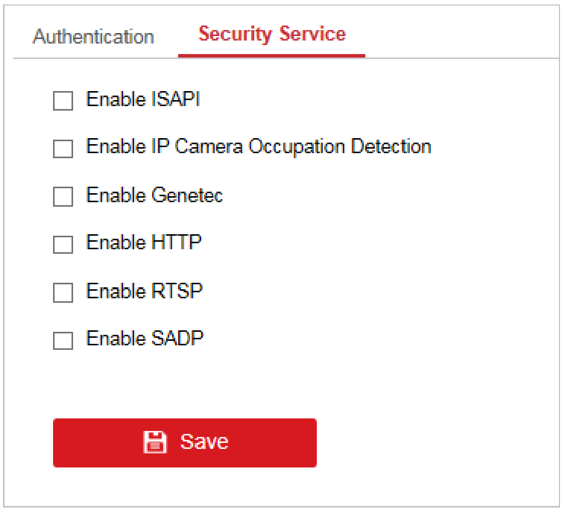
- Telnet.
- PSIA server.
- PSIA IPC access.
- SSH.

5.2 Disabling Services

You can disable the following functions to enhance the access security, e.g., when you are in the untrusted network environment.

- Multicast.
- Genetec.
- ISAPI (Internet Server Application Program Interface).
- SADP.

Step 1 Go to **Menu** > **Maintenance** > **System Service** from local GUI or **Configuration** > **System** > **Security** > **Authentication** from Web browser.



□ Enable ISAPI

□ Enable IP Camera Occupation Detection

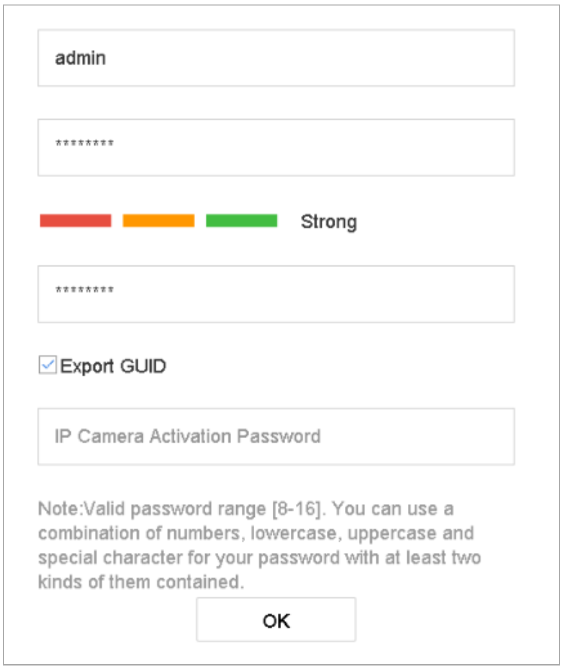
□ Enable Genetec

□ Enable HTTP

□ Enable RTSP

□ Enable SADP

Figure 5-1 Disable Services (Web Browser)



admin

****

🟥 🟧 🟩 Strong

****

☑ Export GUID

IP Camera Activation Password

Note:Valid password range [8-16]. You can use a combination of numbers, lowercase, uppercase and special character for your password with at least two kinds of them contained.

Figure 5-2 Disable Services (Local GUI)

Step 2 Uncheck the **Enable Genetec/Enable ISAPI/Enable SADP** to disable the services.

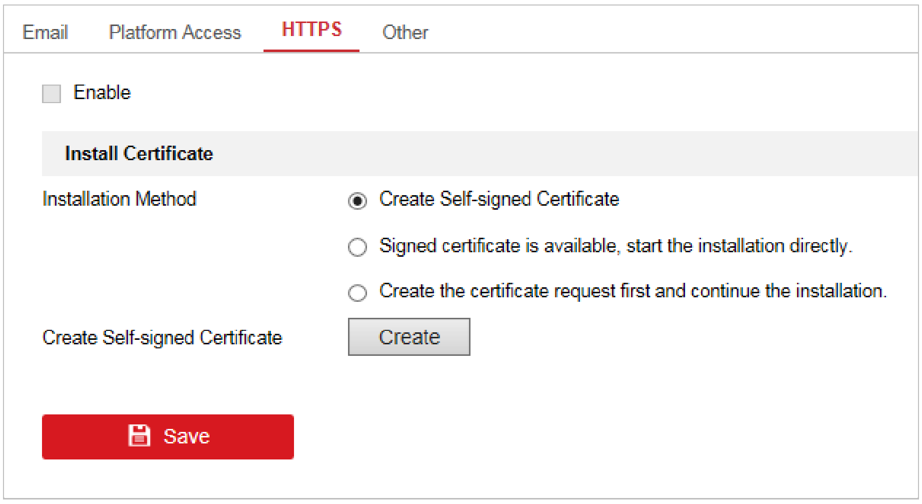
5.3 HTTPS

HTTPS provides authentication of the web site and its associated web server, which protects against Man-in-the-middle attacks. Perform the following steps to set the port number of HTTPS.

E.g., If you set the port number as 443 and the IP address is 192.168.1.64, you may access the device by inputting https://192.168.1.64:443 via the web browser.

Step 1 Go to **Configuration** > **Network** > **Advanced Settings** > **HTTPS** (from Web browser).

Step 2 Check the checkbox of **Enable** to enable the function.



□ Enable

Install Certificate

Installation Method
● Create Self-signed Certificate
○ Signed certificate is available, start the installation directly.
○ Create the certificate request first and continue the installation.

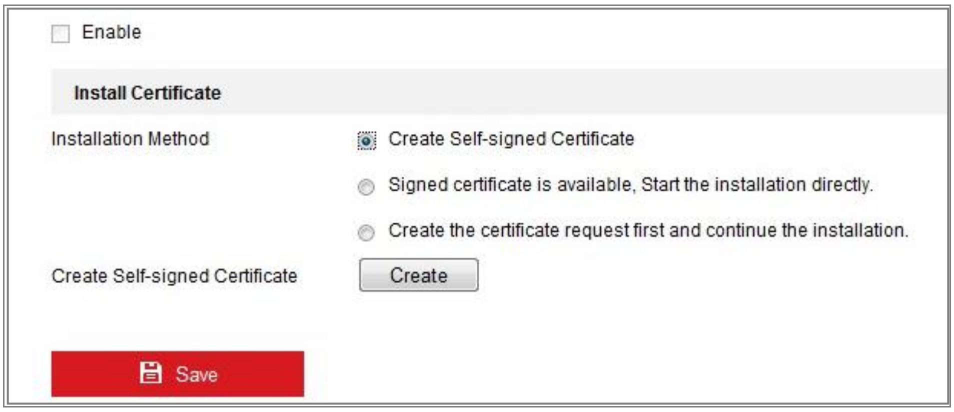
Create Self-signed Certificate [Create]

Figure 5-3 HTTPS Configuration Interface

Step 3 Create the self-signed certificate or authorized certificate.

- **Create the self-signed certificate**

  1) Select **Create Self-signed Certificate** as the Installation Method.
  2) Click **Create** to enter the creation interface.



□ Enable

Install Certificate

Installation Method
● Create Self-signed Certificate
○ Signed certificate is available, Start the installation directly.
○ Create the certificate request first and continue the installation.

Create Self-signed Certificate [Create]

Figure 5-4 Create Self-signed Certificate

  3) Enter the country, host name/IP, validity and other information.
  4) Click **OK to** save the settings.

NOTE

If you already had a certificate installed, the Create Self-signed Certificate is grayed out.

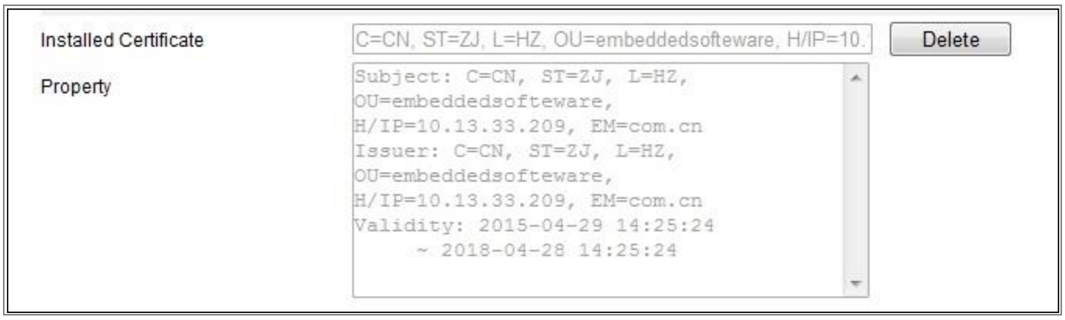
- **Create the authorized certificate**

  1) Select **Create the certificate request first and continue the installation** as the Installation Method.
  2) Click **Create** to create the certificate request. Fill in the required information in the popup window.

3) Download the certificate request and submit it to the trusted certificate authority for signature.

4) After receiving the signed valid certificate, import the certificate to the device.

Step 4 There will be the certificate information after your successfully creating and installing the certificate.



Installed Certificate: C=CN, ST=ZJ, L=HZ, OU=embeddedsofteware, H/IP=10.

Property:

```
Subject: C=CN, ST=ZJ, L=HZ,
OU=embeddedsofteware,
H/IP=10.13.33.209, EM=com.cn
Issuer: C=CN, ST=ZJ, L=HZ,
OU=embeddedsofteware,
H/IP=10.13.33.209, EM=com.cn
Validity: 2015-04-29 14:25:24
     ~ 2018-04-28 14:25:24
```

Figure 5-5 Installed Certificate

Step 5 Click **Save** to save the settings.

5.4 HTTP

You can choose to disable the HTTP, or set the HTTP authentication when it is enabled as demand to enhance the access security.

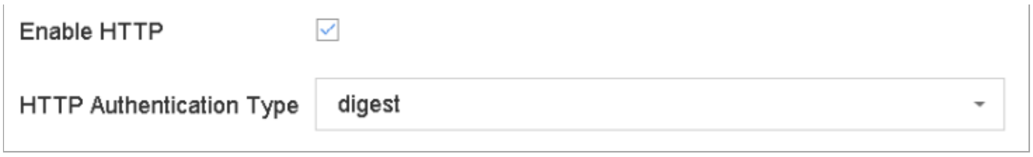
NOTE

By default, the HTTP service is enabled.

Setting HTTP Authentication

If you need to enable the HTTP service, you can set the HTTP authentication to enhance the access security.

Step 1 Go to **Menu** > **Maintenance** > **System Service** from local GUI or **Configuration** > **System** > **Security** > **Authentication** from Web browser.



Enable HTTP ☑

HTTP Authentication Type: digest

Figure 5-6 HTTP Authentication

Step 2 Check the **Enable HTTP** to enable the HTTP service.

Step 3 Select the **digest** as the **HTTP Authentication** in the drop-down list.

Step 4 Click **Save** to save the settings.

NOTE

Two authentication types are selectable: **digest** and **digest/basic**. For security reasons, it is recommended to select digest as the authentication type.

Disabling HTTP

The admin user account can disable the HTTP service from the GUI or the web browser.

After the HTTP is disabled, all its related services, including the HTTPS, UPnP, ISAPI, Onvif and Gennetc, will terminate as well.

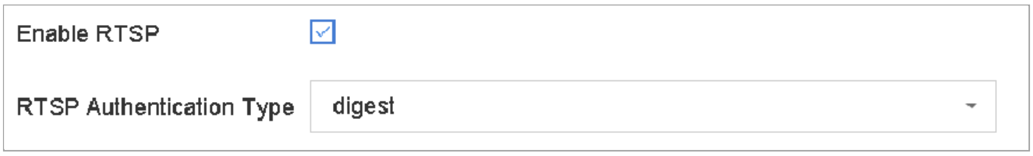
Step 1 Go to **Menu** > **Maintenance** > **System Service** from local GUI or **Configuration** > **System** > **Security** > **Authentication** from Web browser.

Step 2 Uncheck the **Enable HTTP** to disable the HTTP service.

5.5 RTSP/WEB Authentication

You can specifically secure the stream data of live view by setting the RTSP and WEB authentication.

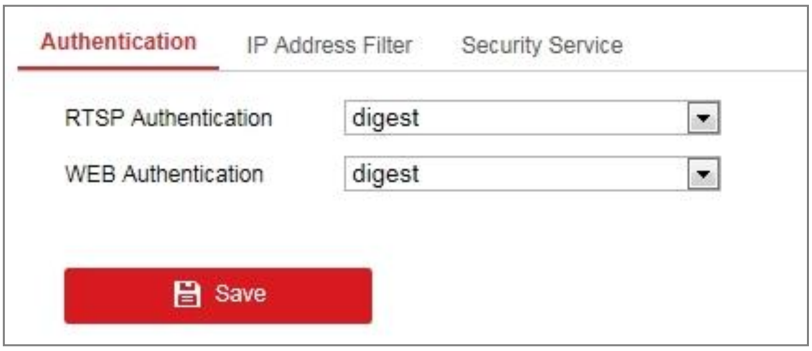
Step 1 Go to **Menu** > **Maintenance** > **System Service** from local GUI or **Configuration** > **System** > **Security** > **Authentication** from Web browser.



Enable RTSP ☑

RTSP Authentication Type: digest

Figure 5-7 RTSP Authentication (Local GUI)



RTSP Authentication: digest

WEB Authentication: digest

Figure 5-8 RTSP Authentication (Web Browser)

Step 2 Select the authentication type.

- Select the **digest** as the **RTSP Authentication** in the drop-down list.
- Select the **digest** as the **Web Authentication** in the drop-down list.

NOTE

Two authentication types are selectable: **digest** and **digest/basic**. If you select **digest**, as the RTSP authentication, only the request with digest authentication can access the video stream by the RTSP protocol via the IP address. For security reasons, it is recommended to select digest as the authentication type.

Step 3 Click **Save** to save the settings.

5.6 Disabling UPnP

Universal Plug and Play (UPnP™) is a networking architecture that provides compatibility among networking equipment, software and other hardware devices. The UPnP protocol allows devices to connect seamlessly and to simplify the implementation of networks in the home and corporate environments.

Step 1 Go to **Menu** > **Maintenance** > **System Service** from local GUI or **Configuration** > **Network** > **Basic Settings** > **NAT** from Web browser.

Step 2 Uncheck the checkbox of **Enable UPnP** to disable the UPnP function.

5.7 Disabling Control4

The Control4 protocol enables you to search the Hikvision devices via SDDP, get the basic network parameters, device information, or access some device operations.

Step 1 Go to **Menu** > **Maintenance** > **System Service** > **More Settings** > **Control4**.

Step 2 Uncheck the checkbox of **Enable SDDP** and **Enable CGI**.

Step 3 Click **Apply**.

5.8 Disabling I-VIEW-NOW UPNP Reporting

The I-VIEW-NOW UPNP Reporting service enables the system to automatically send the device network parameters to authorized receivers by e-mail.

Step 1 Go to **Menu** > **Maintenance** > **System Service** > **More Settings** > **I-VIEW-NOW UPNP Reporting**.

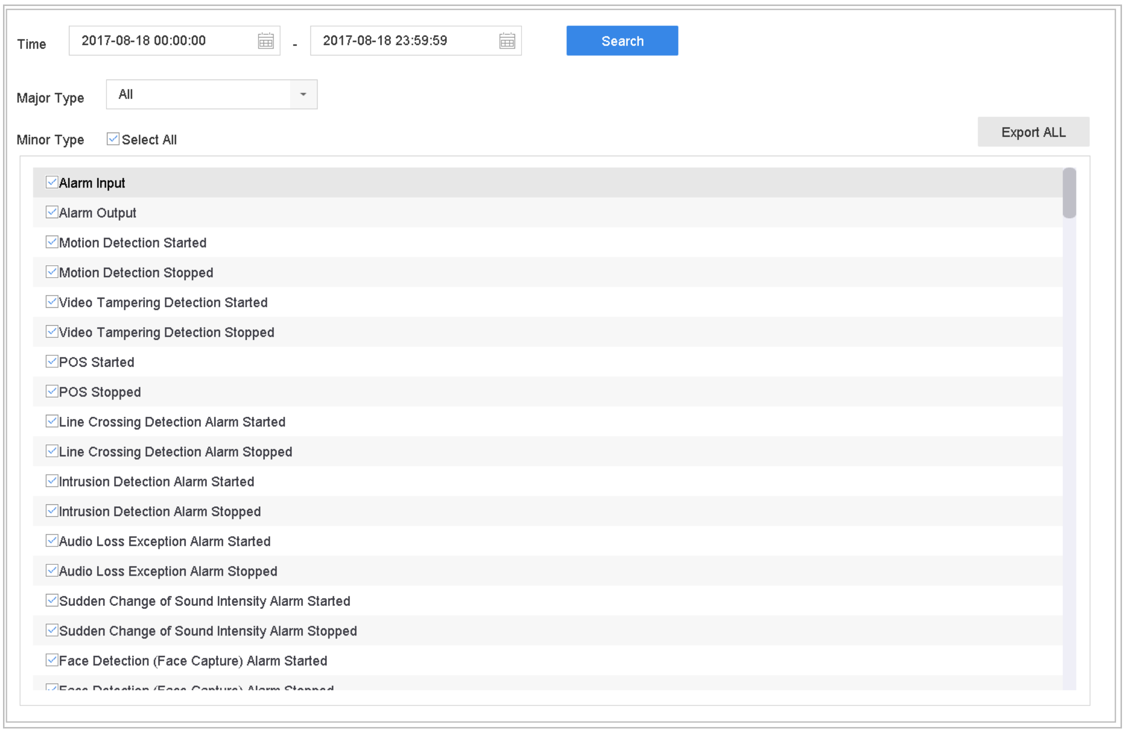
Step 2 Uncheck the checkbox of **I-VIEW-NOW UPNP Reporting**.

Step 3 Click **Apply**.

Chapter 6 System Logs

The system stores the operation, alarm, exception and information of the device in log files, which can be viewed and exported at any time. You can check and export the logs regularly to monitor the system security.

Step 1 Go to **Menu** > **Maintenance** > **Log Information**.



Time 2017-08-18 00:00:00 - 2017-08-18 23:59:59

Major Type All

Minor Type ☑ Select All

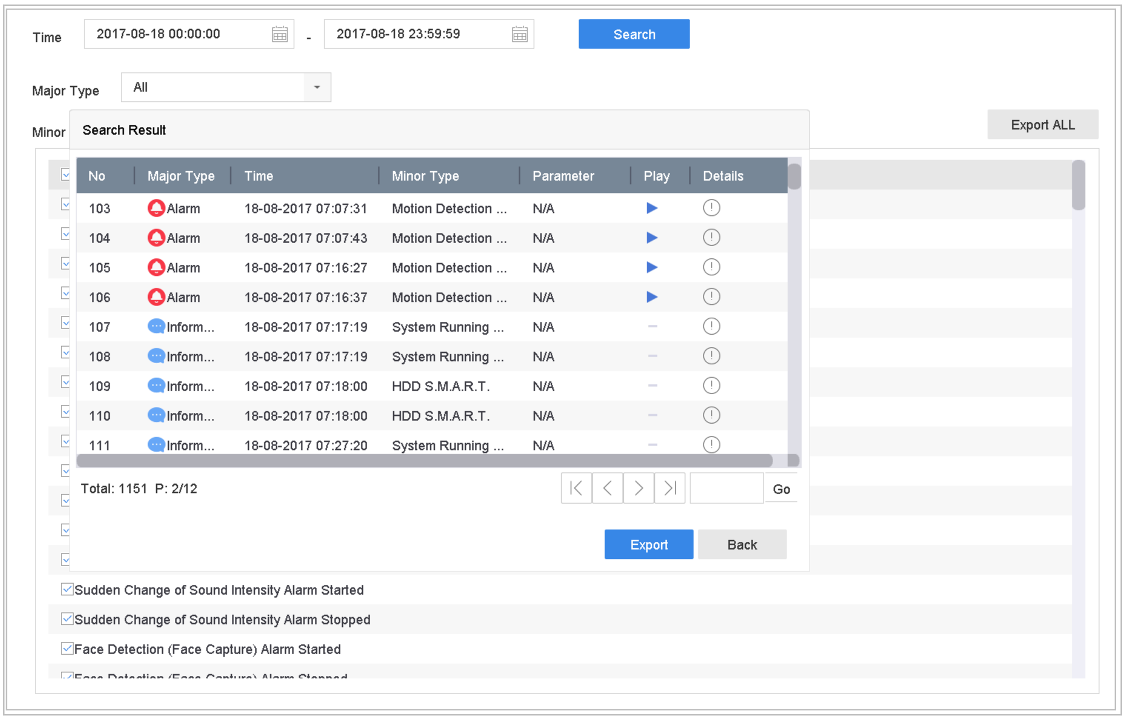
- ☑ Alarm Input
- ☑ Alarm Output
- ☑ Motion Detection Started
- ☑ Motion Detection Stopped
- ☑ Video Tampering Detection Started
- ☑ Video Tampering Detection Stopped
- ☑ POS Started
- ☑ POS Stopped
- ☑ Line Crossing Detection Alarm Started
- ☑ Line Crossing Detection Alarm Stopped
- ☑ Intrusion Detection Alarm Started
- ☑ Intrusion Detection Alarm Stopped
- ☑ Audio Loss Exception Alarm Started
- ☑ Audio Loss Exception Alarm Stopped
- ☑ Sudden Change of Sound Intensity Alarm Started
- ☑ Sudden Change of Sound Intensity Alarm Stopped
- ☑ Face Detection (Face Capture) Alarm Started
- ☑ Face Detection (Face Capture) Alarm Stopped

Figure 6-1 Log Search

Step 2 Set the log search conditions, including the Time, Major Type and Minor Type.

Step 3 Click **Search** to start search log files.

The matched log files will be displayed on the list shown below.



No	Major Type	Time	Minor Type	Parameter	Play	Details
103	Alarm	18-08-2017 07:07:31	Motion Detection ...	N/A	▶	ⓘ
104	Alarm	18-08-2017 07:07:43	Motion Detection ...	N/A	▶	ⓘ
105	Alarm	18-08-2017 07:16:27	Motion Detection ...	N/A	▶	ⓘ
106	Alarm	18-08-2017 07:16:37	Motion Detection ...	N/A	▶	ⓘ
107	Inform...	18-08-2017 07:17:19	System Running ...	N/A	—	ⓘ
108	Inform...	18-08-2017 07:17:19	System Running ...	N/A	—	ⓘ
109	Inform...	18-08-2017 07:18:00	HDD S.M.A.R.T.	N/A	—	ⓘ
110	Inform...	18-08-2017 07:18:00	HDD S.M.A.R.T.	N/A	—	ⓘ
111	Inform...	18-08-2017 07:27:20	System Running ...	N/A	—	ⓘ

Total: 1151 P: 2/12

☑Sudden Change of Sound Intensity Alarm Started

☑Sudden Change of Sound Intensity Alarm Stopped

☑Face Detection (Face Capture) Alarm Started

☑Face Detection (Face Capture) Alarm Stopped

Figure 6-2 Log Search Results

NOTE

Up to 2000 log files can be displayed each time.

Related Operation:

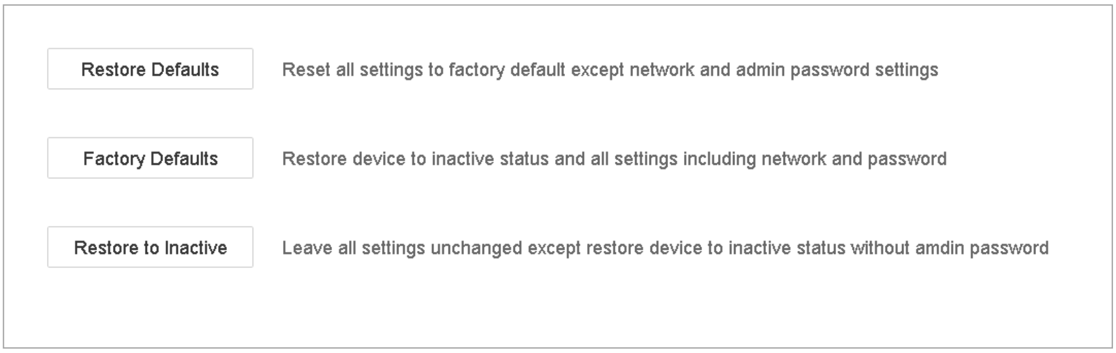
- Click the ⓘ button or double click it to view its detailed information.
- Click the ▶ button to view the related video file.

Chapter 7 System Restore and Upgrade

You are recommended to upgrade the device or restore the default settings when the network risks may exist.

7.1 Restoring System Defaults

Step 1 Go to **Menu** > **Maintenance** > **Default**.



Restore Defaults — Reset all settings to factory default except network and admin password settings

Factory Defaults — Restore device to inactive status and all settings including network and password

Restore to Inactive — Leave all settings unchanged except restore device to inactive status without amdin password

Figure 7-1 Restore Defaults

Step 2 Select the restoring type from the following three options.

Restore Defaults: Restore all parameters, except the network (including IP address, subnet mask, gateway, MTU, NIC working mode, default route, server port, etc.) and user account parameters, to the factory default settings.

Factory Defaults: Restore all parameters to the factory default settings.

Restore to Inactive: Restore the device to the inactive status.

Step 3 Click **OK** to restore the default settings.

7.2 Upgrading System

Always use the latest firmware to get all possible security updates. You can upgrade your system from local GUI, Web browser or client software.

See Far, Go Further

UD09222B