HIKVISION
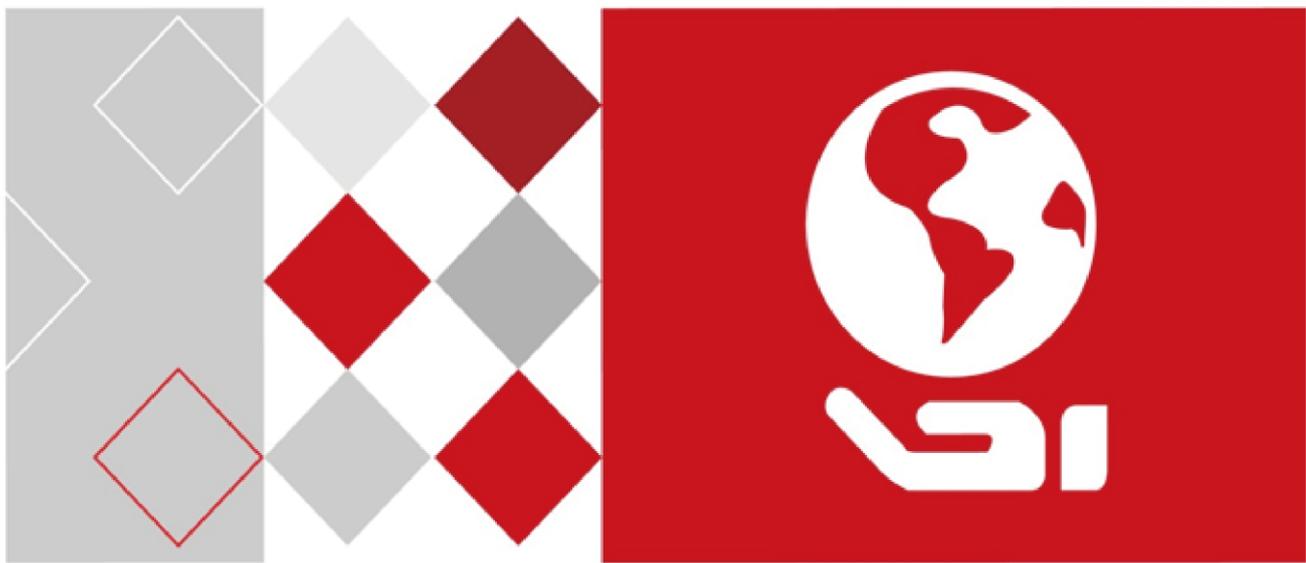
Network Security Guide

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

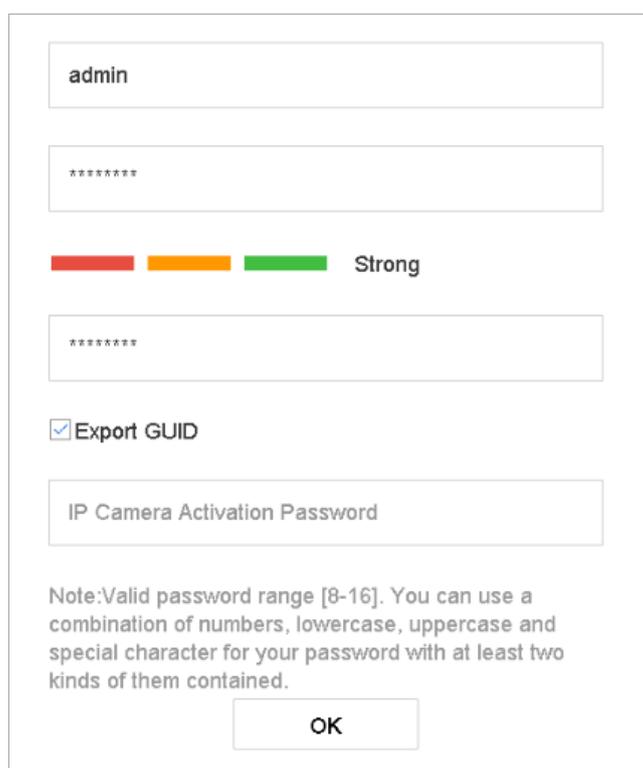## 2.1 Activating Your Device by Setting a Strong Password

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**.

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 **IP Camera Activation** text field, enter the password to activate the IP camera (s) connected to the device.

Step 3 Click **OK** to activate the device.

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.

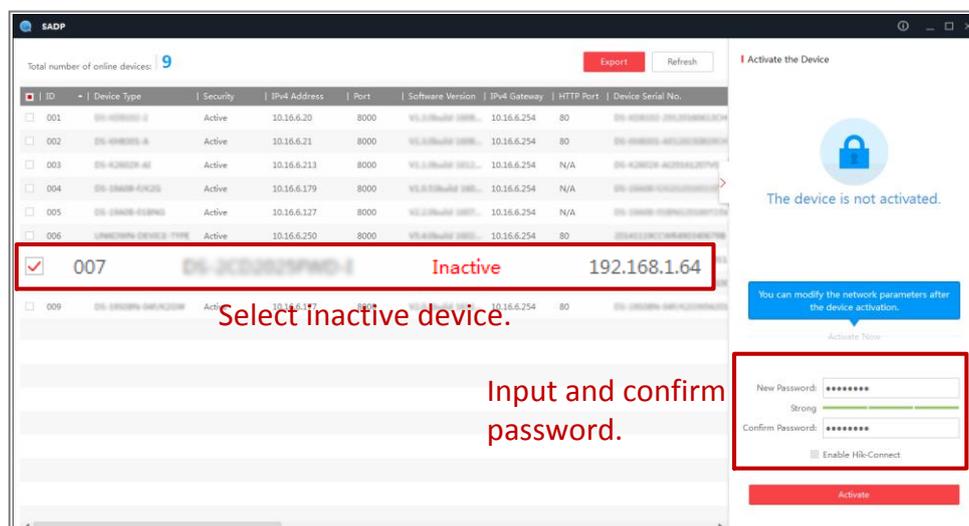Step 2 Check the device status from the device list, and select the inactive device.

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**.

Figure 2-3 Modify the IP Address

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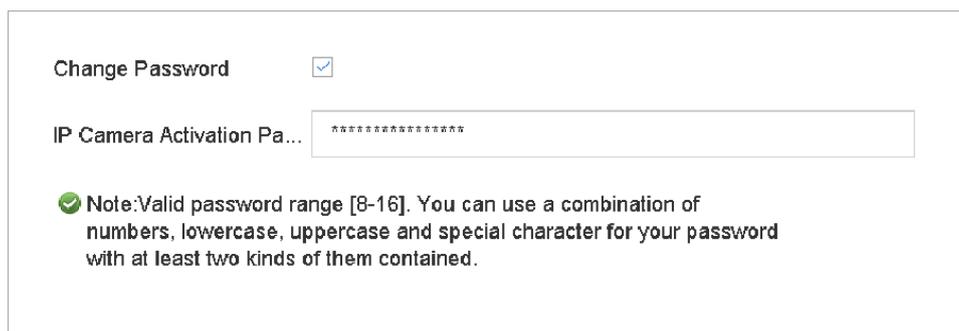
2.2 Managing IP Camera Activation

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.

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.

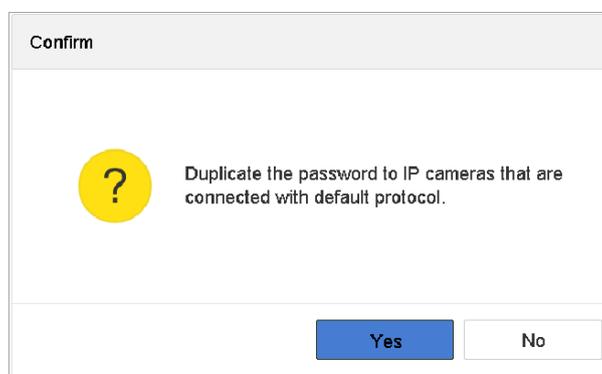Step 5 Click **Apply** to have the following pop-up attention box.

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).

2.3.2 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.
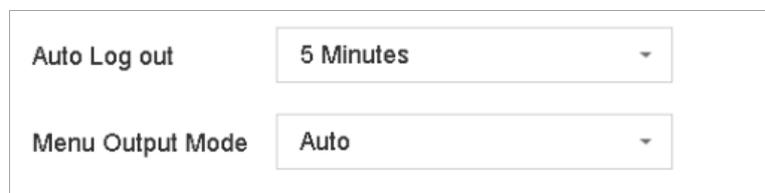
Step 1 Go to **Menu** > **System** > **General.**

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.

Figure 2-6 Auto Logout

Chapter 3 User Account Management

3.1 Setting Permission 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.

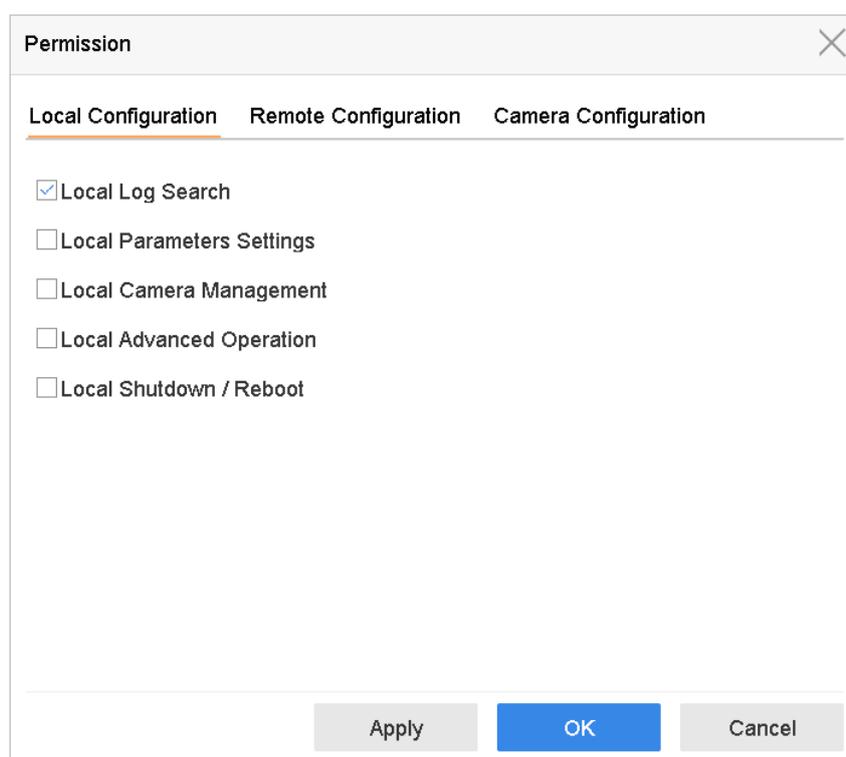Step 3 Click ✅ to enter the permission settings interface.

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.

3.2 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.

Figure 3-2 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.

Figure 3-3 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**.
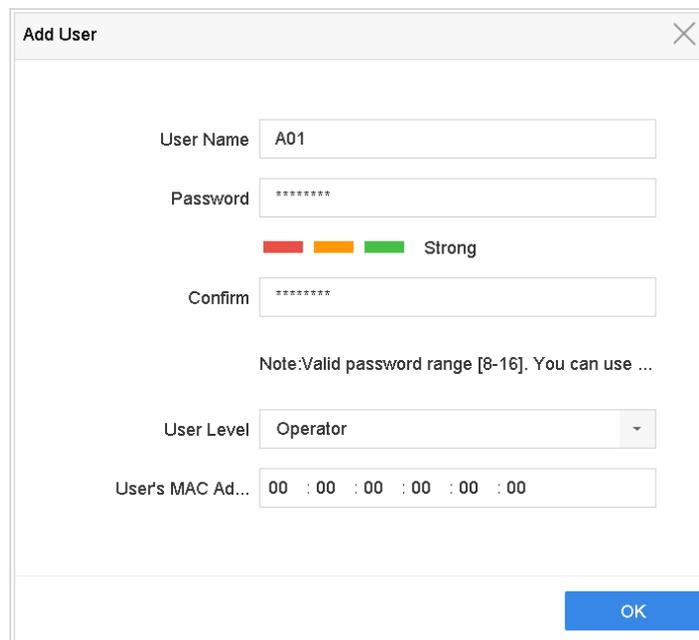
Figure 4-1 Add User Menu

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 Network Security Settings

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
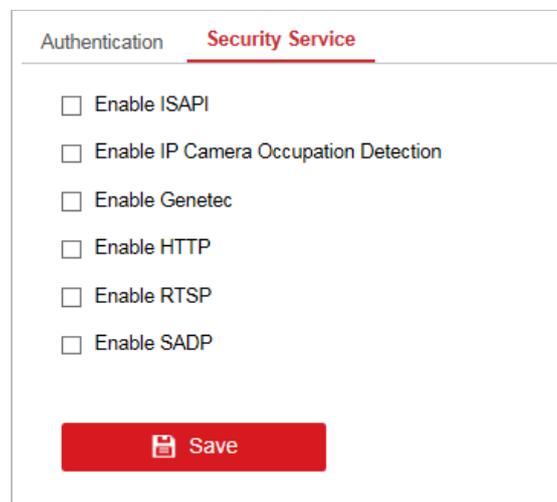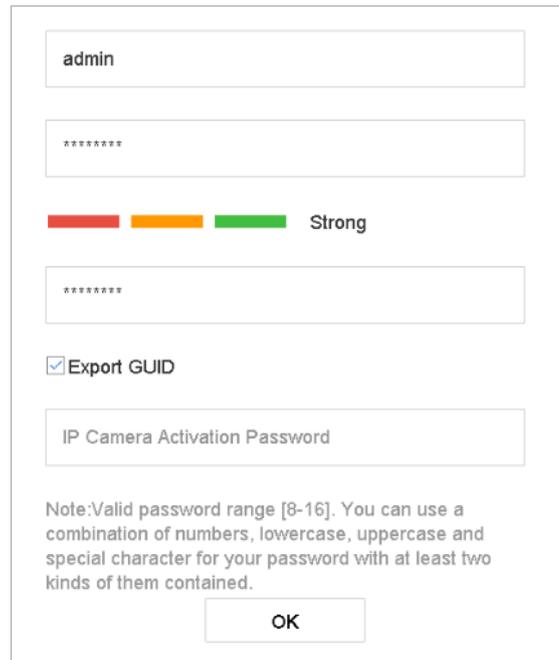   **Configuration** > **System** > **Security** > **Authentication** from Web browser.

Figure 5-1 Disable Services (Web Browser)

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).

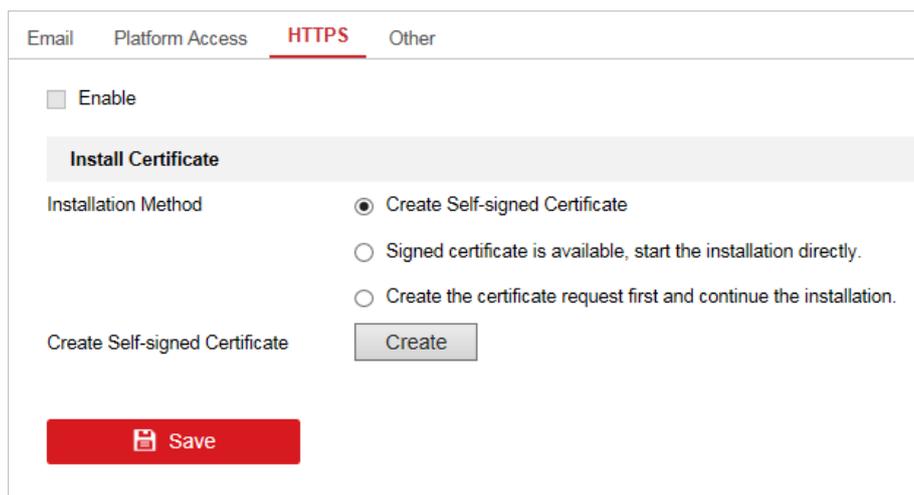Step 2 Check the checkbox of **Enable** to enable the function.

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.
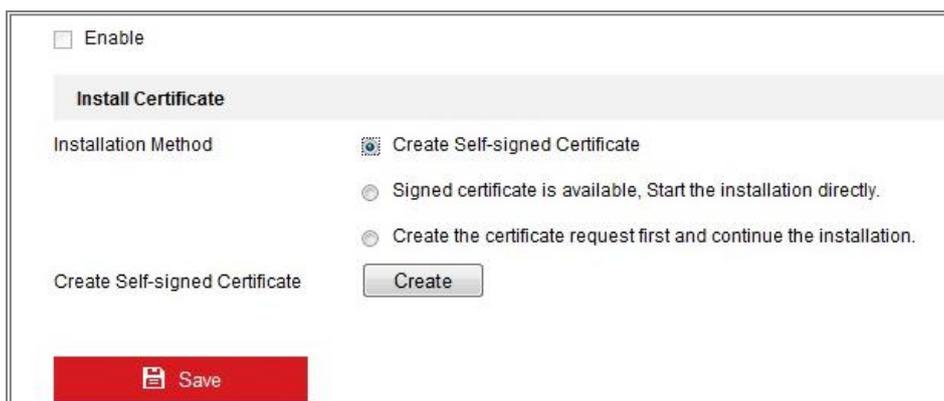2) Click **Create** to enter the creation interface.

Figure 5-4 Create Self-signed Certificate

3) Enter the country, host name/IP, validity and other information.
4) Click **OK t**o 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.
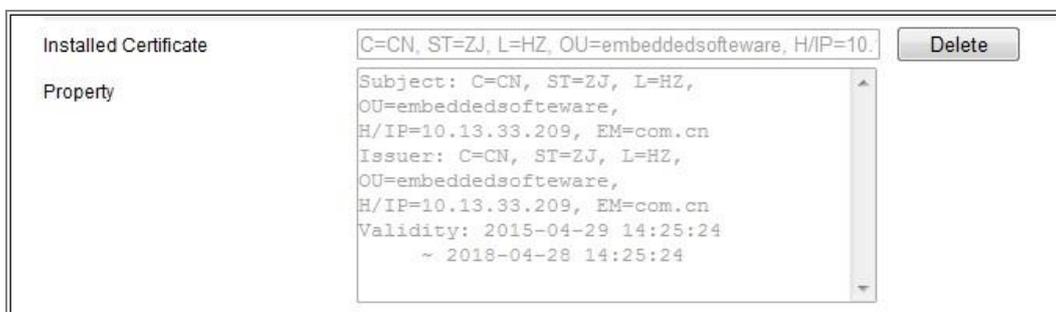

Figure 5-5 Installed Certificate

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.

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.

Figure 5-7 RTSP Authentication (Local GUI)

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.

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**.

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.

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**.

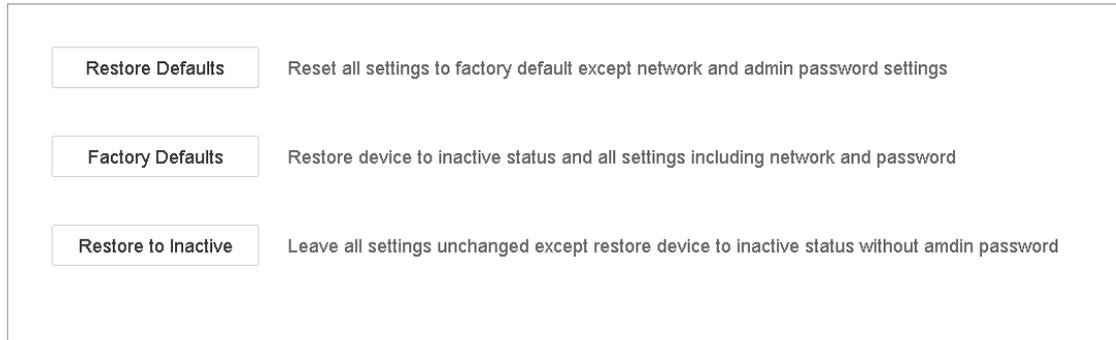|	
Restore Defaults	Reset all settings to factory default except network and admin password settings
Factory Defaults	Restore device to inactive status and all settings including network and password
Restore to Inactive	Leave all settings unchanged except restore device to inactive status without amdin 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.

First Choice for Security Professionals

www.hikvision.com