www.use-ip.co.uk
01304 827609

Network Security Hardening Guide

v1.2 June 2017

About This Document

This document provides information and explains measures that users can take to secure network devices to improve network security.

Trademarks Acknowledgement

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

Contact Information

No.555 Qianmo Road, Binjiang District, Hangzhou 310052, China

Tel: +86-571-8807-5998

Fax: +86-571-8993-5635

Email: overseasbusiness@hikvision.com; sales@hikvision.com

Technical Support: support@hikvision.com

HSRC (Hikvision Security Response Center) Email: HSRC@hikvision.com

Table of Contents

Introduction ... 4
Passwords ... 4
What is a firewall? ... 5
Standard Configuration ... 6
Activate the device by setting a strong password ... 6
System restoring and upgrading ... 12
Enable encryption ... 15
User access control ... 16
Disable UPnP ... 17
Disable QoS ... 18
Disable multicast video ... 18
Set IP address filter ... 19
Lock illegal login IP address ... 19
Disable SSH ... 20
Choose SNMP V3 ... 20
Firewall setup on router ... 22
Port forwarding ... 23
Conclusion ... 27

Introduction

Hikvision network devices, like any other network devices, may be exposed to cybersecurity risks. To protect the network from the risk, Hikvision takes measures such as disabling the Telnet and FTP interface, and adopting the security activation mechanism.

Note: This document is written as a general guideline. Measurements should be taken into consideration depending on the application scenarios.

Passwords

How to create a strong password?

We all know the common guidelines for choosing a strong password:

- Include numbers, symbols, uppercase and lowercase letters.
- Password should be more than eight characters long.
- Avoid any password based on repetition, dictionary words, letter or number sequences, usernames, relative or pet names, or biographical information (birthday).

The Password Phrase Method:

The phrase method is an easy way to remember complicated passwords that are hard to crack.

Use the Password Phrase Method:

- Choose a phrase that has numbers.
- Use only the first letter in each word.
- Use the proper case for each letter, just as it appears in the phrase.
- Use actual numbers whenever possible. Use “2” for “two” or “to” and “4” for “four” or “for.”
- Include punctuation.

Let’s take the following phrase as an example:

"My flight to New York will leave at three in the afternoon!"

Using the Password Phrase method explained above, the password becomes:

"MftNYwla3ita!"

Some general password/security tips

- Avoid using dictionary words in any language.
- Avoid sequences or repeated characters.
- Change your password on a schedule.
- Do not allow Internet Explorer to store passwords.
- Do not type passwords on computers that you do not control.
- Never provide your password via email.
- Never respond to an email asking for personal information. (Banks will never ask you for your personal information in an email.)
- Patch and update the software you use on a regular basis.
- Use caution when opening email attachments.
- Limit the amount of personal information you post about yourself.

What is a firewall?

The short answer is this: A firewall intercepts all communications between you and the Internet, and decides if the information is allowed to pass through to you.

Most firewalls, by default, will block all traffic both in and out. This is what we call “Deny all by Default.” In this default state, it is as if your computer is not even connected to the Internet. While this is a very safe state to be in, it is not very useful. So, we have to create a set of rules to tell the firewall what we consider safe.. Everything else is, by default, considered not safe.

As you create rules to allow traffic in and out, you are creating tiny holes in your firewall for the traffic to flow through. That is why many Internet users call “creating rules pinholing your firewall.” The more pinholes you create in your firewall, the less secure your network becomes. You should only create as many pinholes, or rules, as you need.

Standard Configuration

This is the standard configuration for homes, office or small business.

Configurations will be different based on the network the size of the system you are installing.

This is the minimum recommended for small monitoring system.

Activate the device by setting a strong password

You are required to activate the device first by setting a strong password for it before you can use the device.

Activation via web browser, Activation via SADP, and Activation via client software are all supported.

Activate via web browser

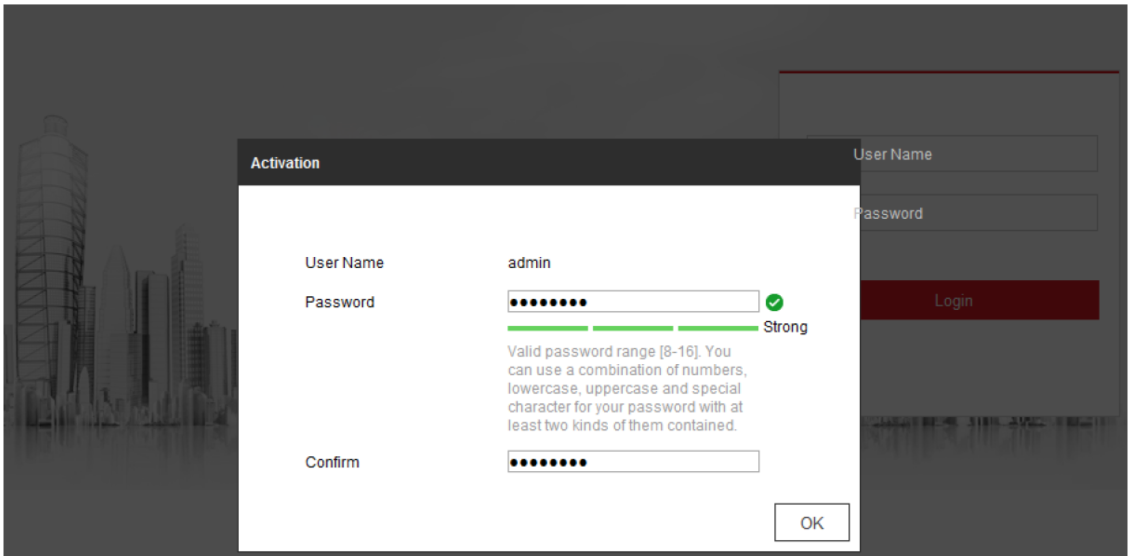
Steps:

1. Power on the device, and connect the device to the network.

2. Input the IP address into the address bar of the web browser, and click **Enter** to enter the activation interface.

Notes:

- The default IP address of the device is 192.168.1.64.
- The device enables the DHCP by default, the IP address is allocated automatically. It is necessary to activate the device via SADP software. Please refer to the following chapter for Activation via SADP.



User Name admin

Password ••••••••

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.

Confirm ••••••••

3. Create a password and input the password into the password field.

STRONG PASSWORD RECOMMENDED– We highly recommend you create a strong password of your own choosing (using a minimum of eight 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. Resetting the password monthly or weekly can better protect your product.

4. Confirm the password.

5. Click **OK** to save the password and enter the live view interface.

Activate via SADP software

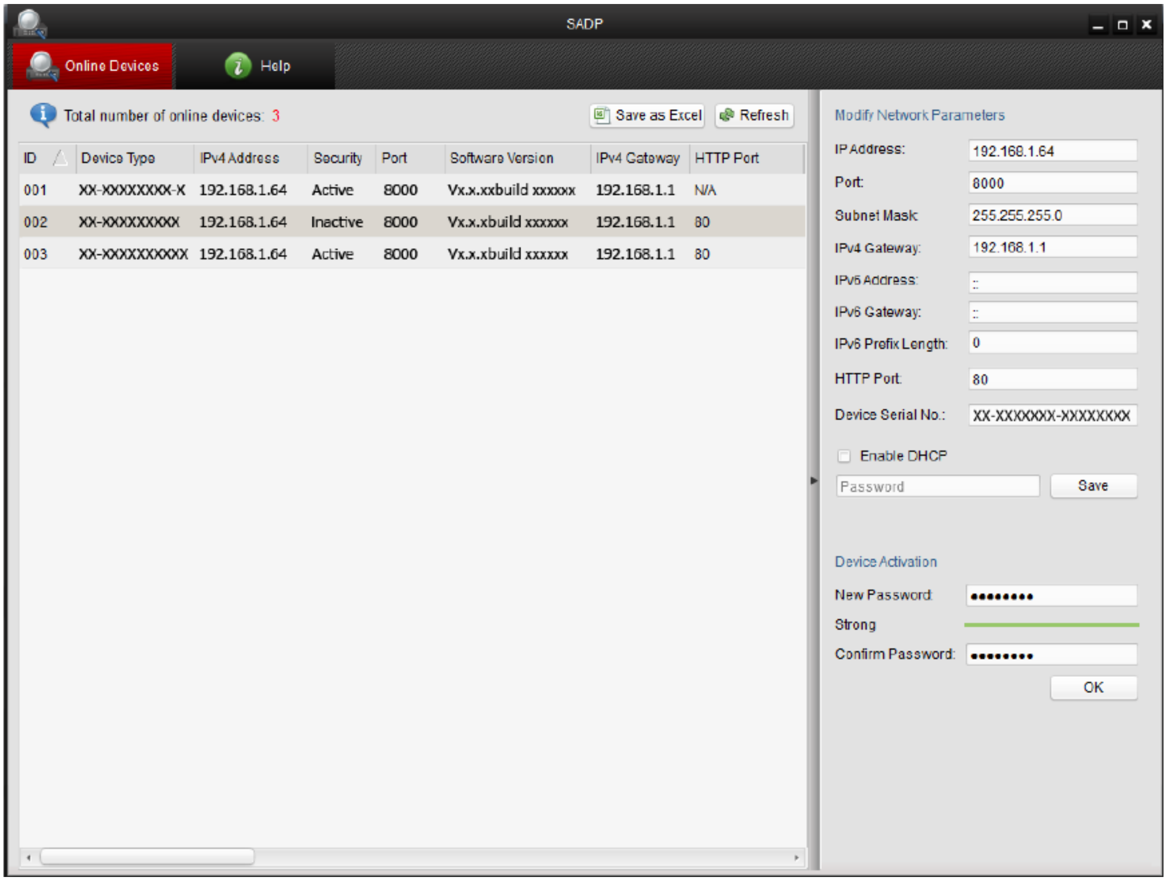
SADP software is used for detecting the online device, activating the device, and resetting the password.

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.

Steps:

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

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



Total number of online devices: 3

ID	Device Type	IPv4 Address	Security	Port	Software Version	IPv4 Gateway	HTTP Port
001	XX-XXXXXXXX-X	192.168.1.64	Active	8000	Vx.x.xxbuild xxxxxx	192.168.1.1	N/A
002	XX-XXXXXXXXX	192.168.1.64	Inactive	8000	Vx.x.xbuild xxxxxx	192.168.1.1	80
003	XX-XXXXXXXXXX	192.168.1.64	Active	8000	Vx.x.xbuild xxxxxx	192.168.1.1	80

IP Address: 192.168.1.64
Port: 8000
Subnet Mask: 255.255.255.0
IPv4 Gateway: 192.168.1.1
IPv6 Address: ::
IPv6 Gateway: ::
IPv6 Prefix Length: 0
HTTP Port: 80
Device Serial No.: XX-XXXXXXX-XXXXXXXX

New Password: ••••••••
Strong
Confirm Password: ••••••••

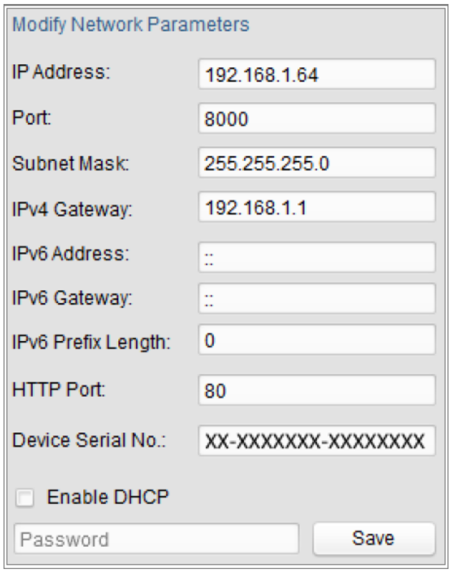
3. Create a password and input the password in the password field, and confirm the password.

STRONG PASSWORD RECOMMENDED– We highly recommend you create a strong password of your own choosing (using a minimum of eight characters, including at least three of the following categories: uppercase letters, lowercase letters, numbers, and special characters) in order to increase the security of your product. And we recommend you reset your password regularly. Resetting the password monthly or weekly can better protect your product.

4. Click **OK** to save the password.

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.

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

IP Address:	192.168.1.64
Port:	8000
Subnet Mask:	255.255.255.0
IPv4 Gateway:	192.168.1.1
IPv6 Address:	::
IPv6 Gateway:	::
IPv6 Prefix Length:	0
HTTP Port:	80
Device Serial No.:	XX-XXXXXXX-XXXXXXXX

□ Enable DHCP

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

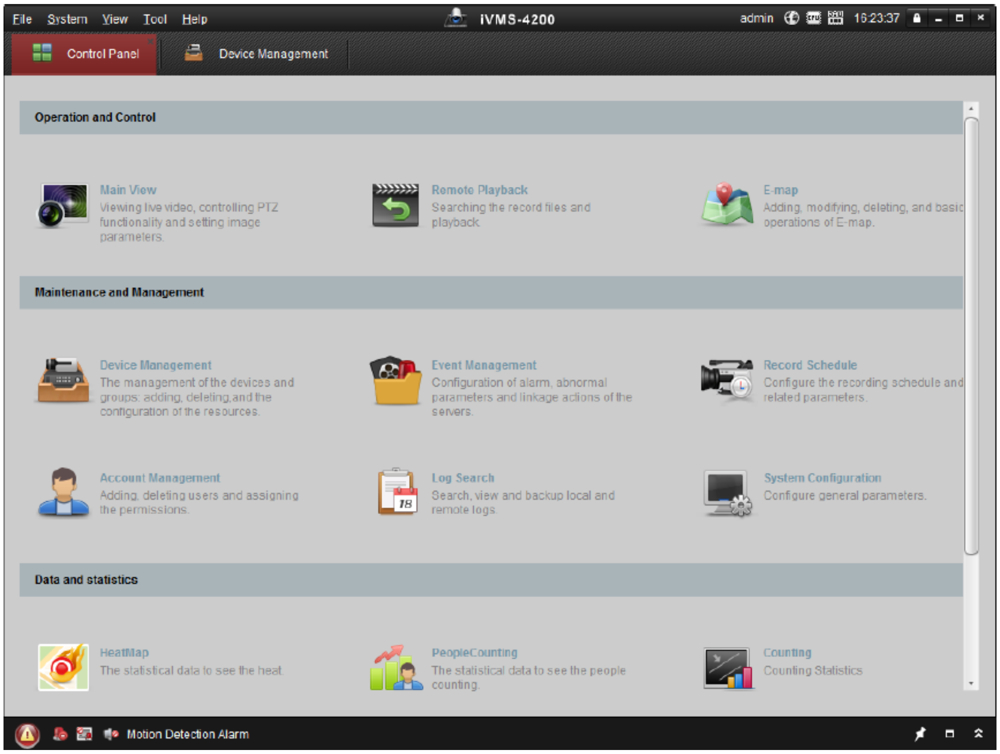
Activate via client software

The client software is versatile video management software for multiple kinds of devices.

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

Steps:

1. Run the client software and the control panel of the software pops up, as shown in the figure below.



Operation and Control

Main View
Viewing live video, controlling PTZ functionality and setting image parameters.

Remote Playback
Searching the record files and playback.

E-map
Adding, modifying, deleting, and basic operations of E-map.

Maintenance and Management

Device Management
The management of the devices and groups: adding, deleting,and the configuration of the resources.

Event Management
Configuration of alarm, abnormal parameters and linkage actions of the servers.

Record Schedule
Configure the recording schedule and related parameters.

Account Management
Adding, deleting users and assigning the permissions.

Log Search
Search, view and backup local and remote logs.

System Configuration
Configure general parameters.

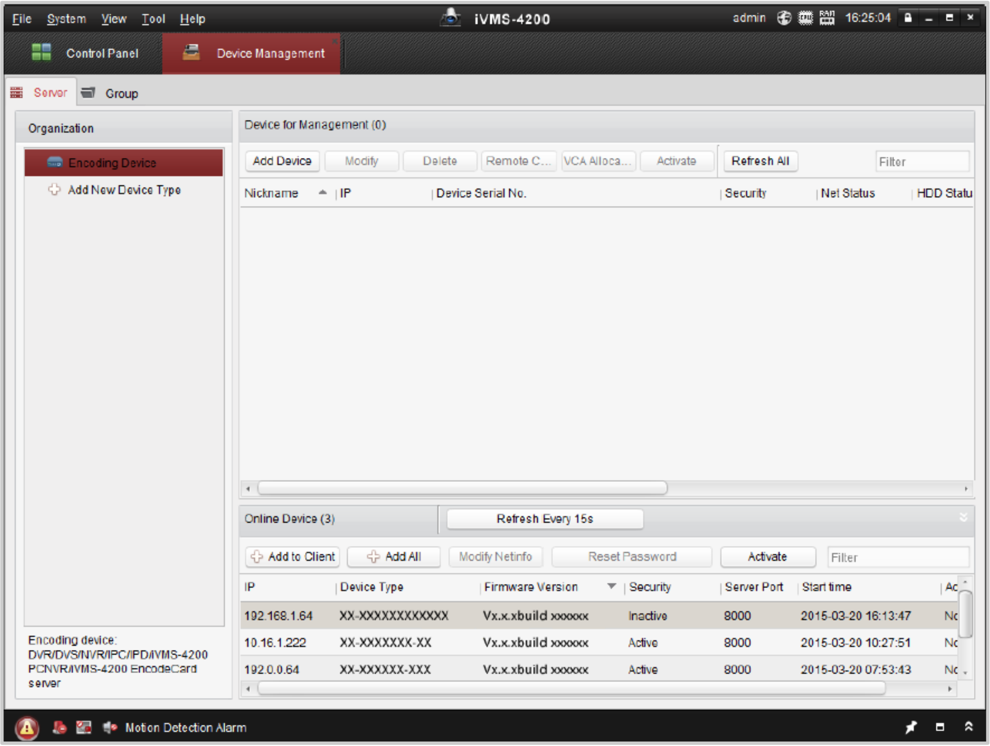
Data and statistics

HeatMap
The statistical data to see the heat

PeopleCounting
The statistical data to see the people counting.

Counting
Counting Statistics

2. Click the **Device Management** icon to enter the Device Management interface, as shown in the figure below.



Encoding device: DVR/DVS/NVR/IPC/IPD/iVMS-4200 PCNVR/iVMS-4200 EncodeCard server

IP	Device Type	Firmware Version	Security	Server Port	Start time	Ac
192.168.1.64	XX-XXXXXXXXXXXX	Vx.x.xbuild xxxxxx	Inactive	8000	2015-03-20 16:13:47	Nc
10.16.1.222	XX-XXXXXXX-XX	Vx.x.xbuild xxxxxx	Active	8000	2015-03-20 10:27:51	Nc
192.0.0.64	XX-XXXXXX-XXX	Vx.x.xbuild xxxxxx	Active	8000	2015-03-20 07:53:43	Nc

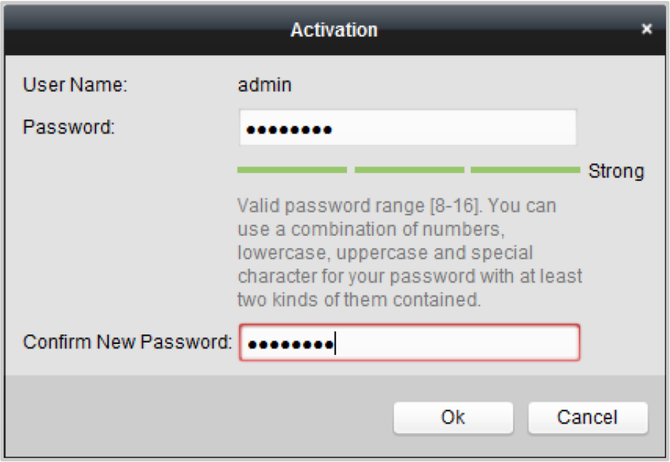
3. Check the device status from the device list, and select an inactive device.

4. Click the ***Activate*** button to pop up the Activation interface.

5. Create a password and input the password in the password field, and confirm the password.

STRONG PASSWORD RECOMMENDED– We highly recommend you create a strong password of your own choosing (using a minimum of eight characters, including at least three of the following categories: uppercase letters, lowercase letters, numbers, and special characters) in order to increase the security of your product. And we recommend you reset your password regularly. Resetting the password monthly or weekly can better protect your product.

4. Click ***OK*** to save the password.



Activation

User Name: admin

Password: ••••••••

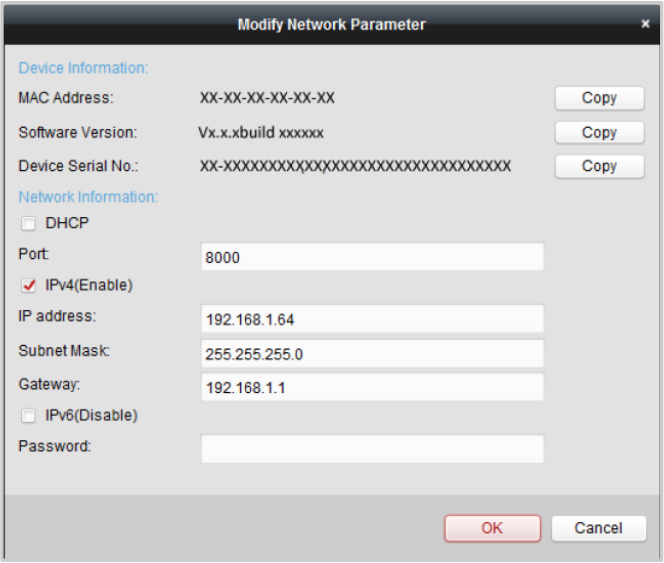
Strong

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.

Confirm New Password: ••••••••

6. Click ***OK*** button to start activation.

7. Click the ***Modify Netinfo*** button to pop up the Network Parameter Modification interface, as shown in the figure below.



Modify Network Parameter

Device Information:

MAC Address: XX-XX-XX-XX-XX-XX

Software Version: Vx.x.xbuild xxxxxx

Device Serial No.: XX-XXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXX

Network Information:

□ DHCP

Port: 8000

☑ IPv4(Enable)

IP address: 192.168.1.64

Subnet Mask: 255.255.255.0

Gateway: 192.168.1.1

□ IPv6(Disable)

Password:

8. 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.

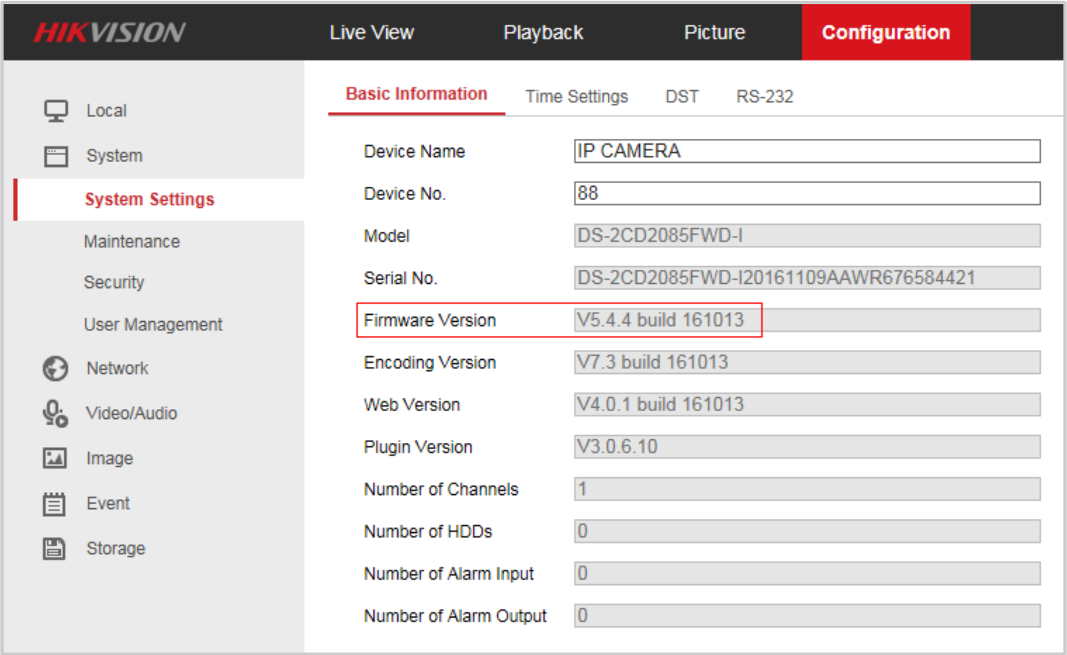
9. Input the password to activate your IP address modification.

System restoring and upgrading

Firmware is the software that enables and controls the functionality of network devices. Always use the latest firmware so that you get all possible security updates and bug fixes.

Check the current firmware

Check the current firmware version in page: ***Configuration > Maintenance > Upgrade & Maintenance***



Device Name	IP CAMERA
Device No.	88
Model	DS-2CD2085FWD-I
Serial No.	DS-2CD2085FWD-I20161109AAWR676584421
Firmware Version	V5.4.4 build 161013
Encoding Version	V7.3 build 161013
Web Version	V4.0.1 build 161013
Plugin Version	V3.0.6.10
Number of Channels	1
Number of HDDs	0
Number of Alarm Input	0
Number of Alarm Output	0

Upgrade the device to a certain version

Steps:

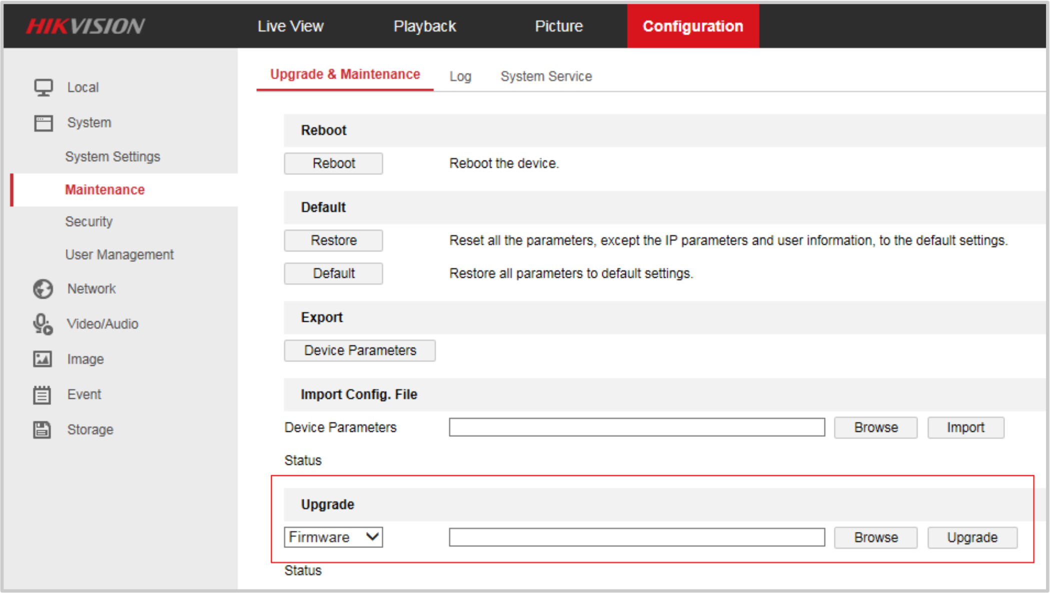
1. Select Firmware or Firmware Directory to locate the upgrade file.

Firmware: Locate the exact path of the upgrade file.

Firmware Directory: Only the directory the upgrade file belongs to is required.

2. Click Browse to select the local upgrade file and then click Upgrade to start remote upgrade.

Note: The upgrading process will take 1 to 10 minutes. Please don't disconnect power of the device during the process. The device reboots automatically after upgrade.



Reboot the device.

Reset all the parameters, except the IP parameters and user information, to the default settings.

Restore all parameters to default settings.

Restore default settings

If you are not sure about what has been changed to the device, you can always set it to the default settings to make it in a known status.

Steps:

Enter the Maintenance interface: ***Configuration > System > Maintenance > Upgrade & Maintenance.***

- **Restore**: Reset all the parameters, except the IP parameters and user information, to the default settings.
- **Default**: Restore all the parameters to the factory default.

Note: After restoring the default settings, the IP address is also restored to the default IP address, please be careful with this action.

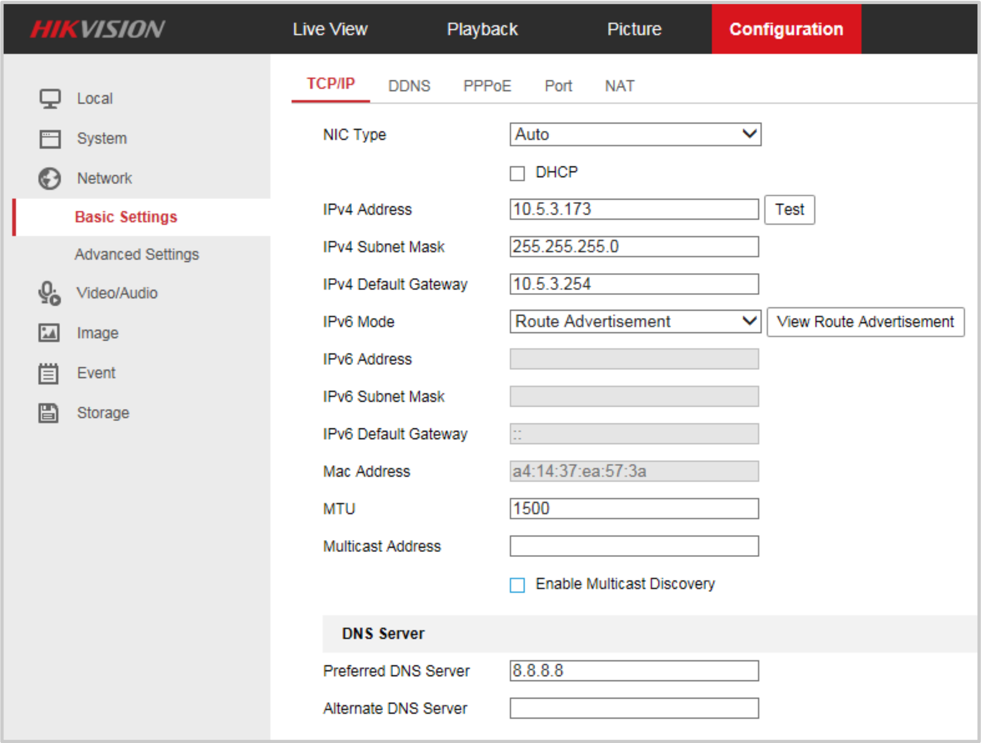
Configure basic network settings

Steps:

1. Go to ***Configuration > Network > Basic Settings > TCP/IP.***

2. Specify the IP address, subnet mask and Default Gateway.

3. Save parameters.



NIC Type	Auto
	□ DHCP
IPv4 Address	10.5.3.173
IPv4 Subnet Mask	255.255.255.0
IPv4 Default Gateway	10.5.3.254
IPv6 Mode	Route Advertisement
IPv6 Address	
IPv6 Subnet Mask	
IPv6 Default Gateway	::
Mac Address	a4:14:37:ea:57:3a
MTU	1500
Multicast Address	
	□ Enable Multicast Discovery

DNS Server

Preferred DNS Server	8.8.8.8
Alternate DNS Server	

Enable encryption

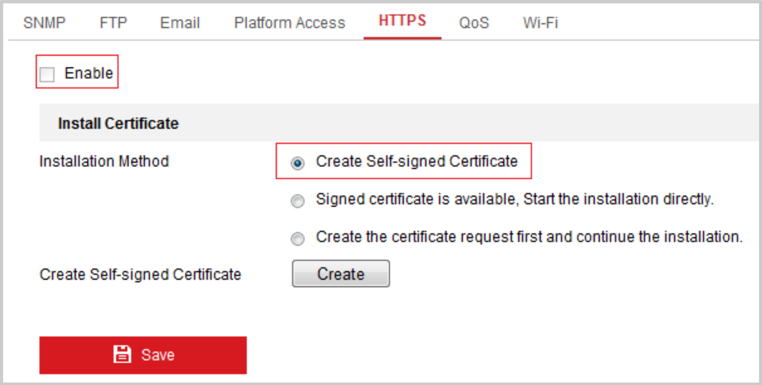
HTTPS provides authentication of the website and its associated web server, which protects against man-in-the-middle attacks. Perform the following steps to set the port number of HTTPS.

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.

Steps:

1. Enter the HTTPS settings interface. ***Configuration > Network > Advanced Settings > HTTPS.***

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

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*** button to enter the creation interface.

(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

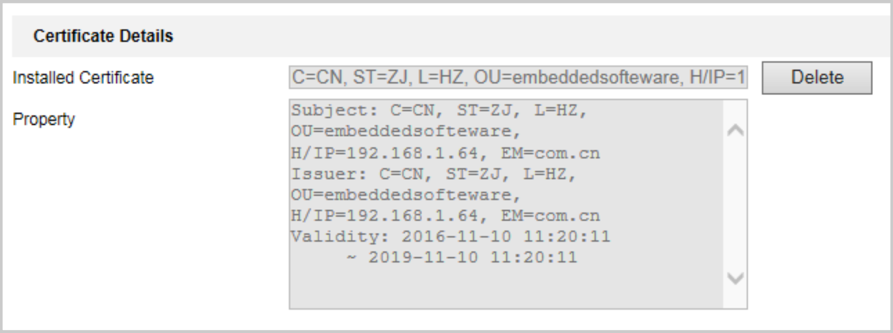
(1) Select ***Create the certificate request first and continue the installation as the Installation*** Method.

(2) Click ***Create*** button 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.

4. There will be the certificate information after you successfully create and install the certificate.



Certificate Details

Installed Certificate: C=CN, ST=ZJ, L=HZ, OU=embeddedsofteware, H/IP=1

Property:

```
Subject: C=CN, ST=ZJ, L=HZ,
OU=embeddedsofteware,
H/IP=192.168.1.64, EM=com.cn
Issuer: C=CN, ST=ZJ, L=HZ,
OU=embeddedsofteware,
H/IP=192.168.1.64, EM=com.cn
Validity: 2016-11-10 11:20:11
     ~ 2019-11-10 11:20:11
```

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

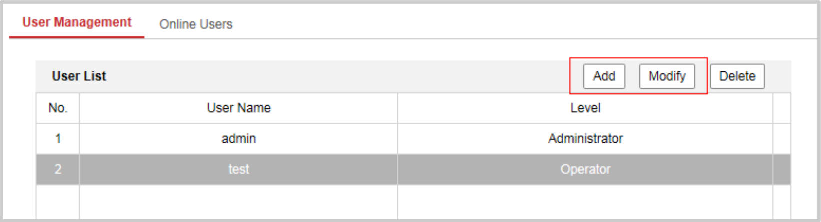
User access control

Set permission level to users

When you add and modify user settings, you can set the permission level for each user to set limitations on the device control.

Steps:

1. Go to ***Configuration > System > User Management.***



User List

No.	User Name	Level
1	admin	Administrator
2	test	Operator

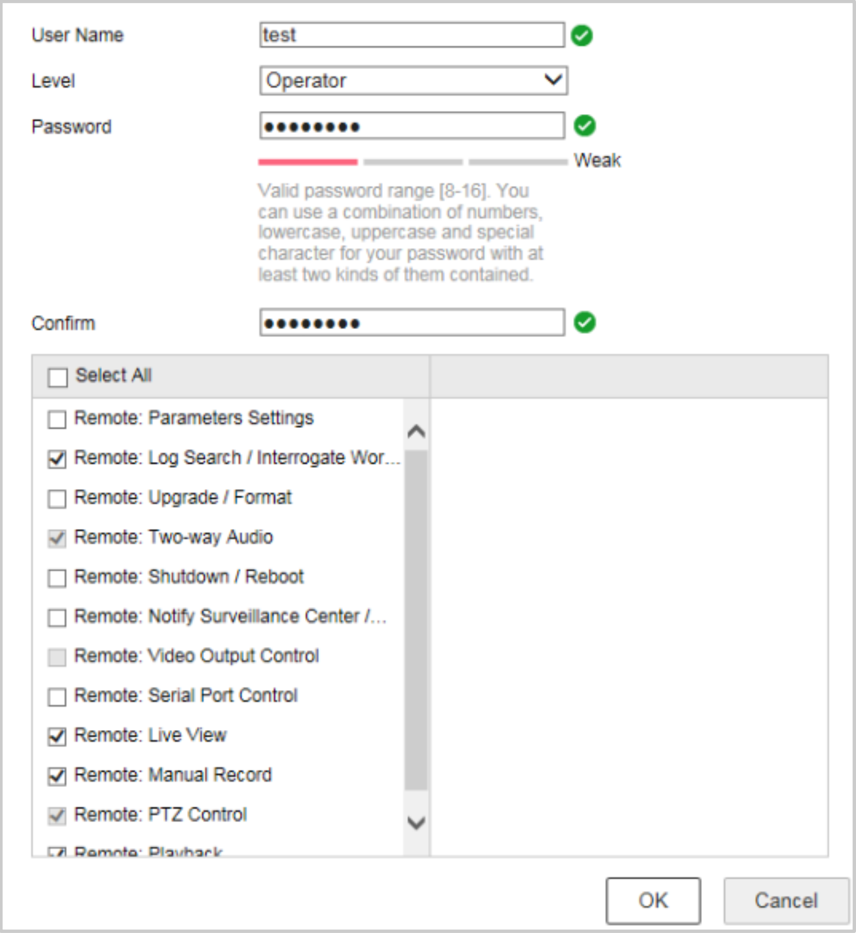
User Management Interface

2. Click ***Add*** or ***Modify*** to add a user or modify a user.

3. Set ***User Name, Level*** and ***Password.***

4. Check or uncheck the permissions.

5. Click ***OK*** to finish the user addition.



User Name: test ✓

Level: Operator

Password: •••••••• ✓

Weak

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.

Confirm: •••••••• ✓

☐ Select All

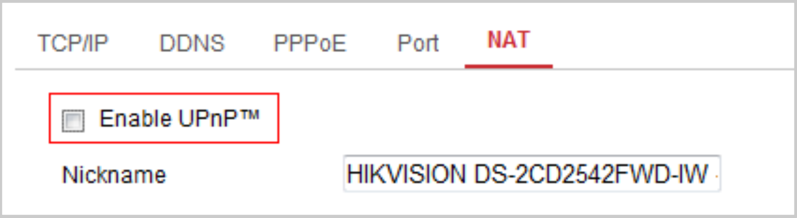
☐ Remote: Parameters Settings
☑ Remote: Log Search / Interrogate Wor...
☐ Remote: Upgrade / Format
☑ Remote: Two-way Audio
☐ Remote: Shutdown / Reboot
☐ Remote: Notify Surveillance Center /...
☐ Remote: Video Output Control
☐ Remote: Serial Port Control
☑ Remote: Live View
☑ Remote: Manual Record
☑ Remote: PTZ Control
☑ Remote: Playback

Disable 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. **If the device is not connected to a hosted video service, disable UPnP**.

Steps:

1. Go to ***Configuration > Network > Basic Settings > NAT.***



☐ Enable UPnP™

Nickname: HIKVISION DS-2CD2542FWD-IW

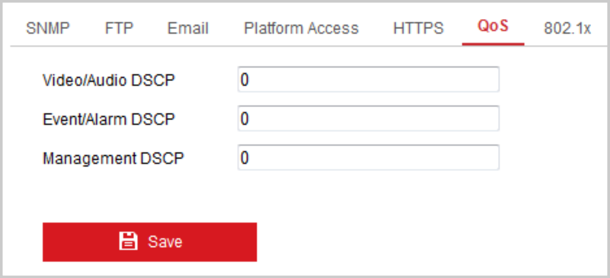
2. Uncheck the checkbox to disable the UPnP™ function.

Disable QoS

QoS is suggested to be disabled, if Quality of Services is not being used.

Steps:

1. Go to ***Configuration > Network > Advanced Settings > QoS***



Video/Audio DSCP 0

Event/Alarm DSCP 0

Management DSCP 0

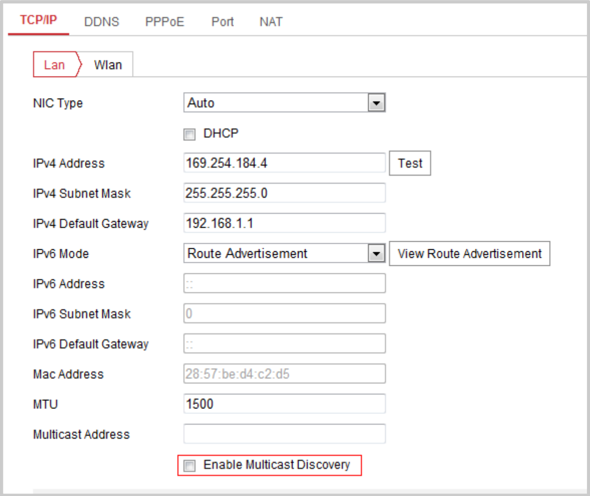
2. To disable QoS, enter the value zero in the QoS DSCP Settings fields.

Disable multicast video

If multicast is not being used, it should be disabled.

Steps:

1. Go to ***Configuration > Network > Basic Settings > TCP/IP***



NIC Type Auto

☐ DHCP

IPv4 Address 169.254.184.4

IPv4 Subnet Mask 255.255.255.0

IPv4 Default Gateway 192.168.1.1

IPv6 Mode Route Advertisement

IPv6 Address ::

IPv6 Subnet Mask 0

IPv6 Default Gateway ::

Mac Address 28:57:be:d4:c2:d5

MTU 1500

Multicast Address

☐ Enable Multicast Discovery

2. Clear ***Enable Multicast Discovery***

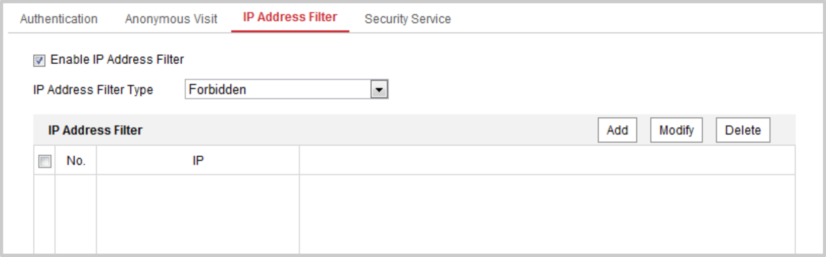
3. Click ***Save***

Set IP address filter

Enabling IP filtering for authorized clients will prevent the device from being accessed by any other unauthorized clients.

Steps:

1. Go to ***Configuration > System > Security > IP Address Filter***



☑ Enable IP Address Filter

IP Address Filter Type: Forbidden

2. Check the checkbox of ***Enable IP Address Filter***.

3. Select the type of IP Address Filter in the drop-down list, ***Forbidden*** and ***Allowed*** are selectable.

4. Set the IP Address Filter list.

Steps:

(1) Click the ***Add*** to add an IP.

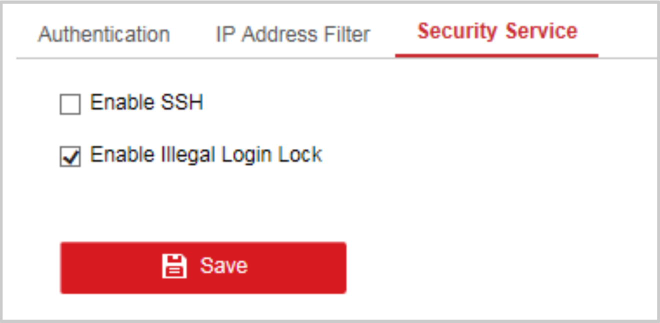
(2) Input the IP Address.

(3) Click the ***OK*** to finish adding.

Lock illegal login IP address

The IP address will be locked if the admin user performs seven failed username/password attempts (five times for the operator/user)

1. Go to ***Configuration > System> Security > Security Service.***



☐ Enable SSH

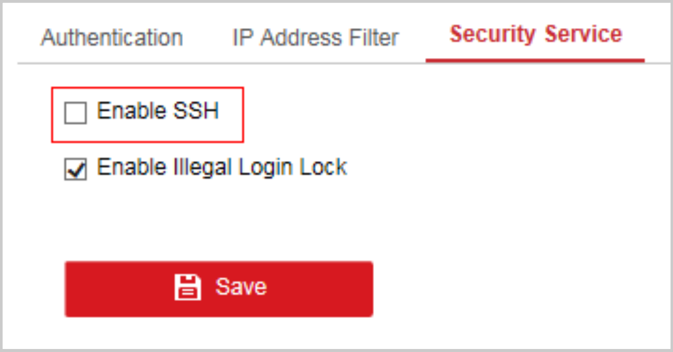
☑ Enable Illegal Login Lock

2. Check the checkbox of ***Enable Illegal Login Lock***, and then the IP address will be locked if the admin user performs seven failed username/password attempts (five times for the operator/user).

Note: If the IP address is locked, you can try to login the device only after 30 minutes.

Disable SSH

Hikvision's devices support Secure Shell and is disabled by default. Make sure it is disabled by checking the security service configuration interface: ***Configuration > System > Security > Security Service.***



□ Enable SSH

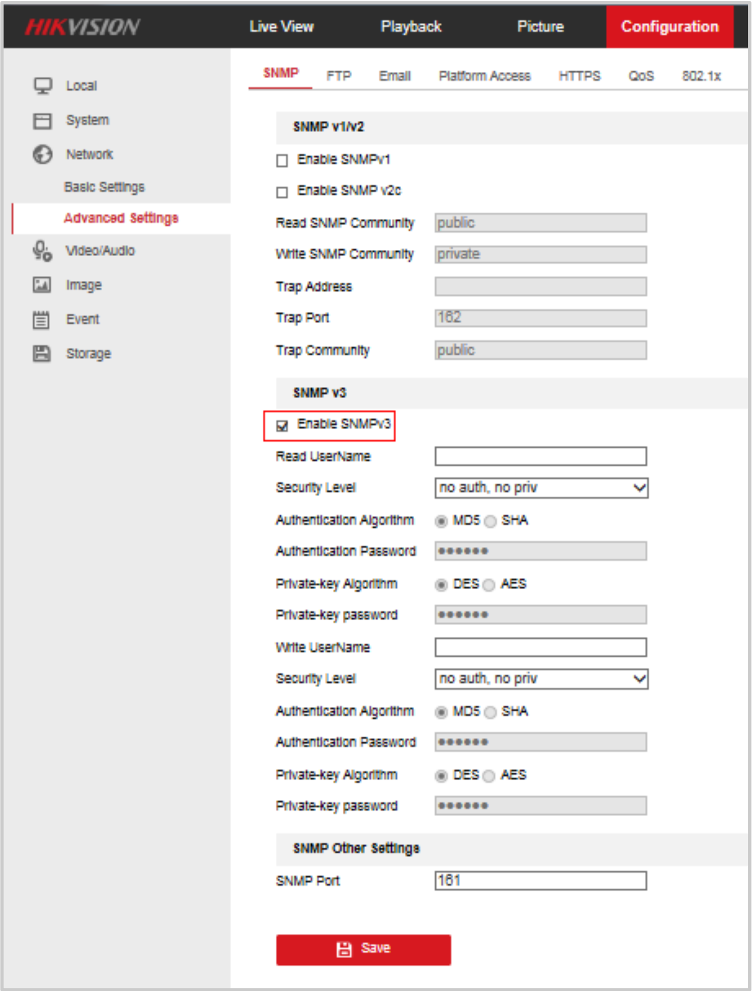
☑ Enable Illegal Login Lock

Note: For devices without this configuration interface, SHH is disabled by default.

Choose SNMP V3

Steps:

1. Go to ***Configuration > Network > Advanced Settings > SNMP.***



SNMP v1/v2

□ Enable SNMPv1

□ Enable SNMP v2c

Read SNMP Community: public

Write SNMP Community: private

Trap Address:

Trap Port: 162

Trap Community: public

SNMP v3

☑ Enable SNMPv3

Read UserName:

Security Level: no auth, no priv

Authentication Algorithm: ● MD5 ○ SHA

Authentication Password: ●●●●●●

Private-key Algorithm: ● DES ○ AES

Private-key password: ●●●●●●

Write UserName:

Security Level: no auth, no priv

Authentication Algorithm: ● MD5 ○ SHA

Authentication Password: ●●●●●●

Private-key Algorithm: ● DES ○ AES

Private-key password: ●●●●●●

SNMP Other Settings

SNMP Port: 161

2. Check the checkbox of Enable SNMPv1, Enable SNMP v2c, Enable SNMPv3 to enable the feature correspondingly.

3. Configure the SNMP settings.

Note: The settings of the SNMP software should be the same as the settings you configure here.

4. Click ***Save*** to save and finish the settings.

Notes:

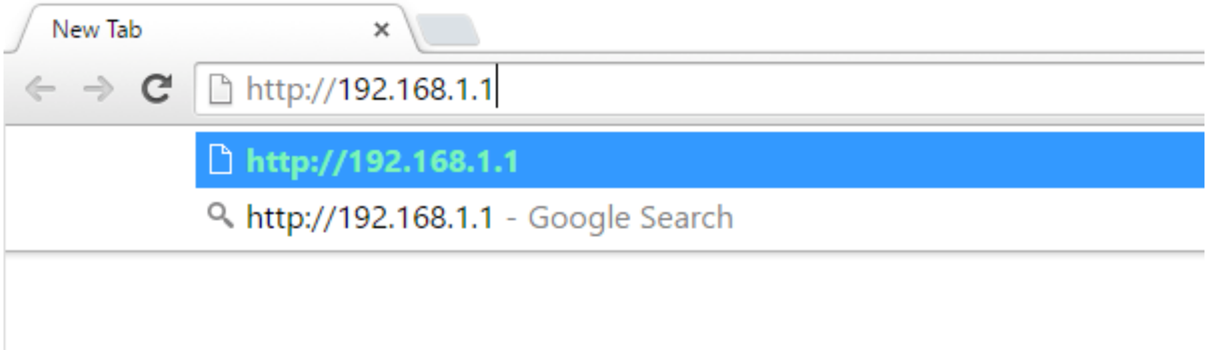
- A reboot is required for the settings to take effect.
- To lower the risk of information leakage, you are suggested to enable SNMP v3 instead of SNMP v1 or v2.

Firewall setup on router

Please keep in mind that all firewall setups are different. The examples below are intended to give a general example and overview of what ports should be setup in a firewall.

Setup:

1. Go to your router IP address

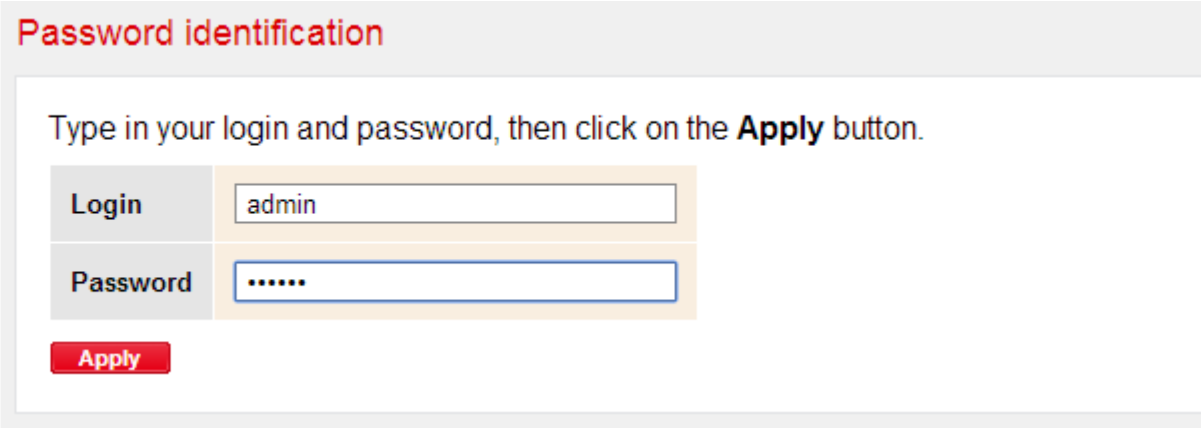


http://192.168.1.1

http://192.168.1.1

http://192.168.1.1 - Google Search

2. Login to your router

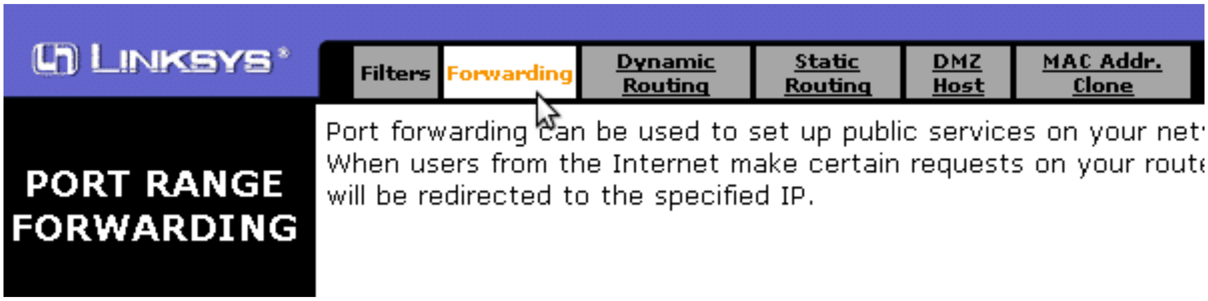


Password identification

Type in your login and password, then click on the **Apply** button.

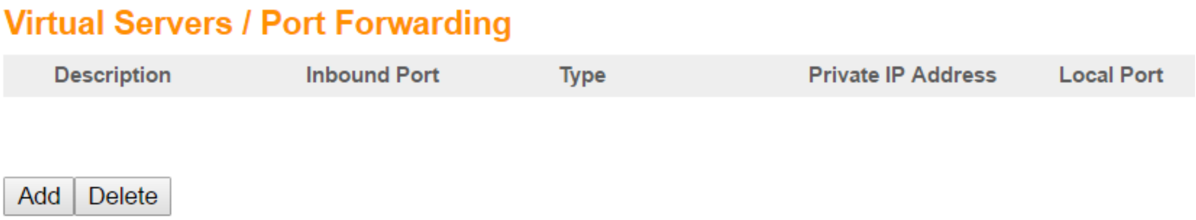
Login	admin
Password	••••••

3. Go to the port forwarding section



Port forwarding can be used to set up public services on your net
When users from the Internet make certain requests on your route
will be redirected to the specified IP.

Find the section that mentions protocols, internal and external ports, and a destination IP address or Server IP address, such as this:



Virtual Servers / Port Forwarding

Description	Inbound Port	Type	Private IP Address	Local Port

Port forwarding

Port forwarding should only be used when devices need to be accessed via the Internet. To ensure proper security configuration, please carefully follow instructions below:

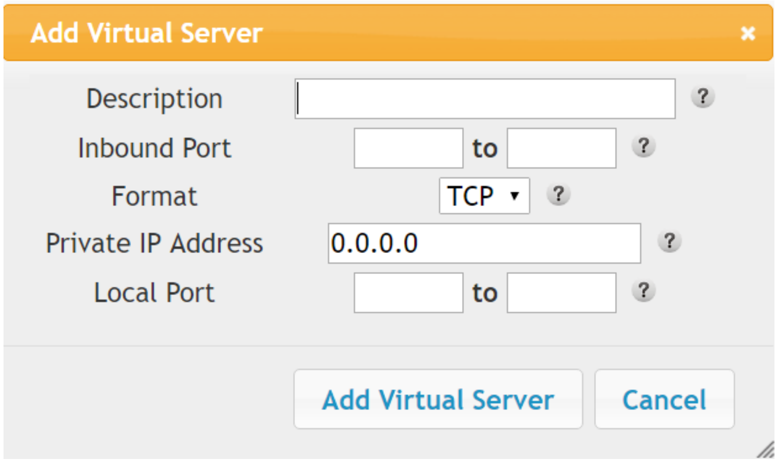
1. Minimize the port numbers exposed to the Internet. Port forwarding should only be configured when absolutely necessary. For example, to use web service, only port 443 should be forwarded.
2. Avoid common ports and reconfigure them to customized ports. For example, port 80 is commonly used for HTTP. It is recommended that the user change to a customized port on the device other than port 80 for the designated service, following TCIP/IP port rule (1 – 65535).

Create a port forwarding rule

Ports that Hikvision uses, you can change these ports to anything you want.

- 80 Web Port
- 443 Secure Web Port
- 8000, 10554 for IVMS application

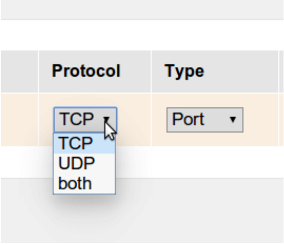
To create the port forwarding rule, firstly set a name for the rule. It's just a reminder of what type of service you are forwarding the port for.



Add Virtual Server

Description		?
Inbound Port	to	?
Format	TCP	?
Private IP Address	0.0.0.0	?
Local Port	to	?

In "protocol," select TCP, UDP, or Both depending on which application(s) need port forwarding.

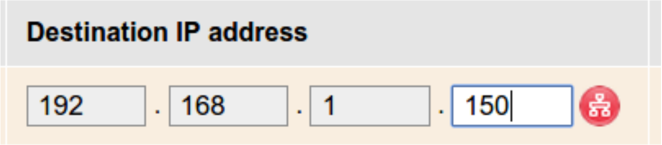


Protocol	Type
TCP	Port

For instance, you need both TCP and UDP protocols forwarding. Some routers only have a TCP or an UDP option, not both. On those routers, if both protocols are needed, two rules must be created, one for TCP and one for UDP.

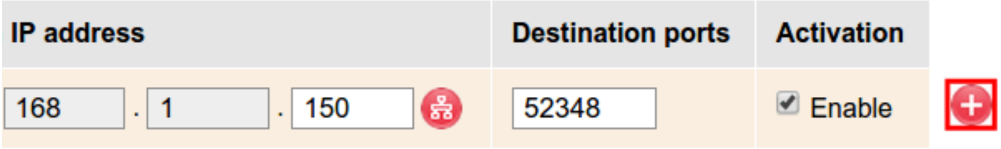
The external and destination port will be the same. Because some lower-numbered ports are being used by the system by default, or by specific applications, it's best to choose a port between 50000 and 65535.

Finally, on the destination IP address, select the static IP previously chosen for the PC.



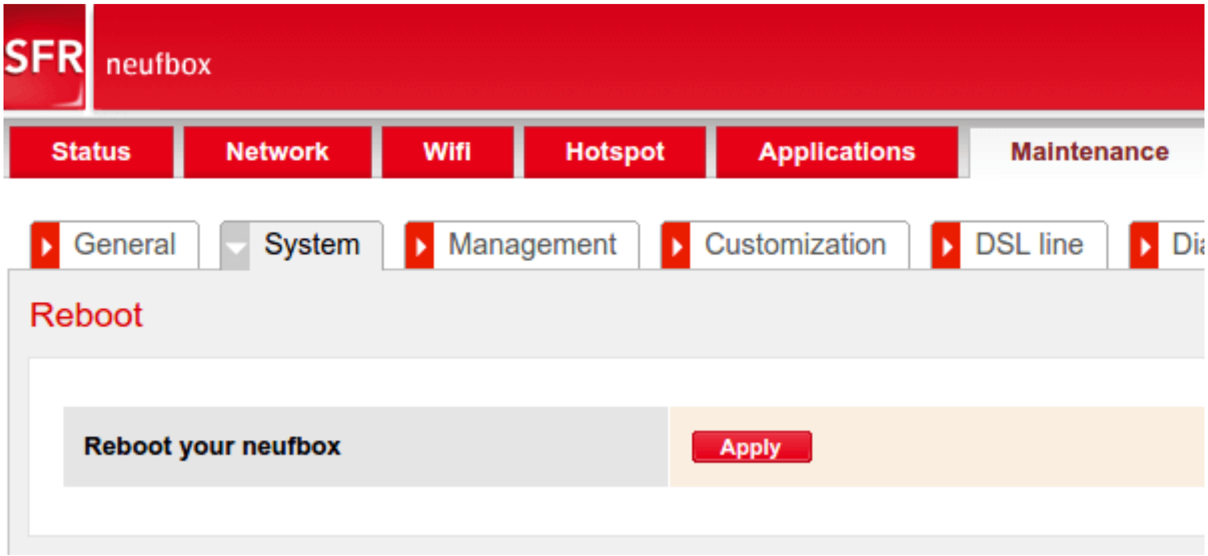
Destination IP address
192 . 168 . 1 . 150

After that, save the new rule.



IP address	Destination ports	Activation
168 . 1 . 150	52348	☑ Enable

On most routers, port forwarding activates immediately. Some routers, though, need a reboot to apply the rule.



Check Port Forwarding

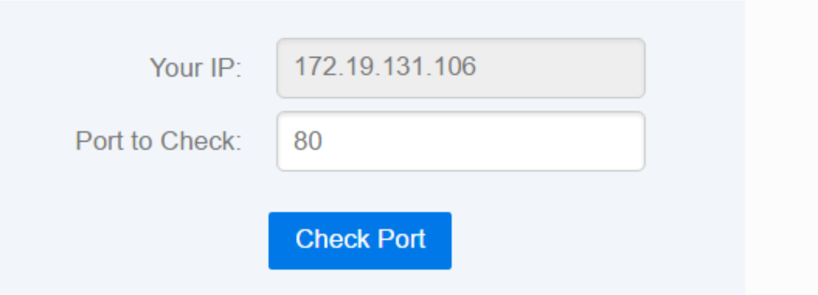
To make sure that Port Forwarding works correctly, use one of the multiple free services on the Internet.

First, ensure that the program or device that needs port forwarding is up and running, and uses the proper port.

Then, navigate to canyouseeme.org

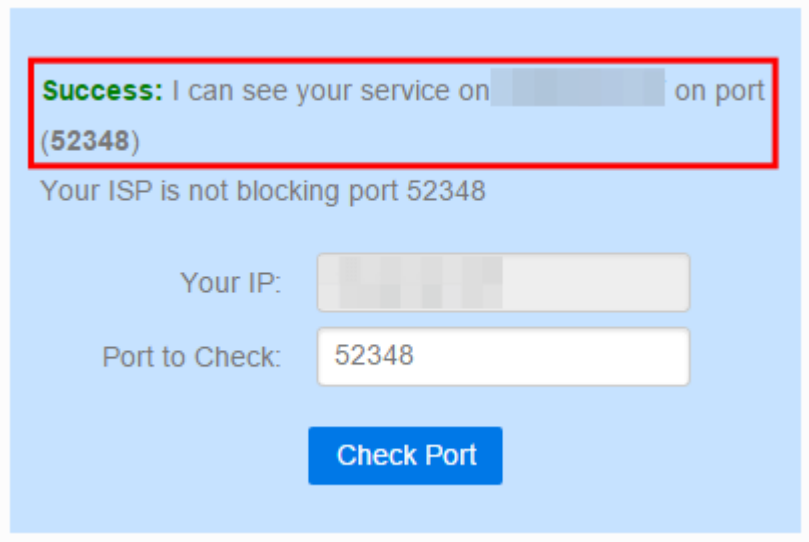
Add the proper port and select "Check Port."

This is a free utility for remotely verifying if a port is open or closed. It is useful to users who wish to verify port forwarding and check to see if a server is running or to determine if a firewall or ISP is blocking certain ports.



Your IP: 172.19.131.106

Port to Check: 80



Success: I can see your service on [redacted] on port (**52348**)

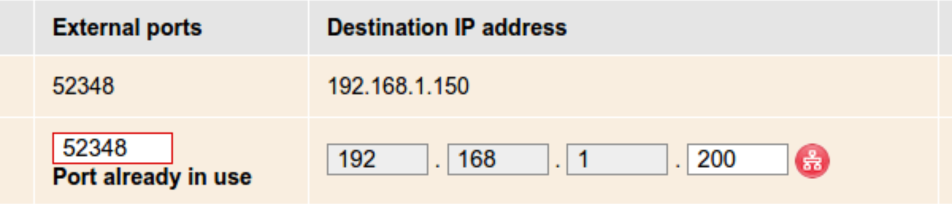
Your ISP is not blocking port 52348

Your IP: [redacted]

Port to Check: 52348

Can two devices on the same LAN use the same port forwarding?

Port forwarding is set up on a unique IP address, and can't set up a rule for the same port with two or more IP addresses.



External ports	Destination IP address
52348	192.168.1.150
52348 **Port already in use**	192 . 168 . 1 . 200

To set up the same program on two different devices, it is necessary to create two rules for two separate ports, one for each device.

Conclusion

This hardening guide is intended to be a living document and will be updated regularly to reflect the most up-to-date cybersecurity best practices. It is one of the many industry-leading cybersecurity resources provided by Hikvision. Please visit the Hikvision Security Center on our website http://www.hikvision.com/us/SecurityCenter_10636.html to learn about other available cybersecurity resources. If you have questions, please contact your Hikvision representative or contact Security.USA@hikvision.com