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  
**About the protection levels** .........................................................................................................................6  
**Default protection** .......................................................................................................................................7  
**Standard protection** ....................................................................................................................................8  
  
  Activate the device by setting a strong password ..........................................................................................8  
  System restoring and upgrading .....................................................................................................................14  
**Enterprise protection** .................................................................................................................................17  
  
  Enable encryption ...........................................................................................................................................17  
  User access control .........................................................................................................................................18  
  Disable UPnP ..................................................................................................................................................19  
  Disable QoS ....................................................................................................................................................20  
  Disable multicast video .................................................................................................................................20  
  Set IP address filter ......................................................................................................................................20  
  Lock illegal login IP address .........................................................................................................................22  
  Disable SSH ...................................................................................................................................................22  
**Managed enterprise protection** ...................................................................................................................23  
  
  Access to IEEE 802.1x network .....................................................................................................................23  
  Choose SNMP V3 ..........................................................................................................................................23  
  Firewall setup on router .................................................................................................................................25  
  Create a port forwarding rule .......................................................................................................................26  
**Conclusion** ......................................................................................................................................................30
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. The appropriate measures may differ depending on the application scenario.

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 it “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.
About the protection levels

This guide uses different protection levels depending on system size and needs. Each level assumes that the previous level’s recommendations are followed.

<table>
<thead>
<tr>
<th>Protection level</th>
<th>Recommended for</th>
<th>Procedures</th>
</tr>
</thead>
<tbody>
<tr>
<td>0 Default protection</td>
<td>Only recommended for demo purposes and test scenarios.</td>
<td>N/A</td>
</tr>
<tr>
<td>1 Standard protection</td>
<td>Minimum recommended level of protection. This level is adequate for small businesses or office installations where, typically, the operator is also the administrator.</td>
<td>Activate the device by setting a strong password. System restoring and upgrading Configure basic network settings</td>
</tr>
<tr>
<td>2 Enterprise protection</td>
<td>Recommended settings for corporations that have a dedicated system administrator.</td>
<td>Enable encryption User access control Disable UPnP Disable QoS Disable multicast video Set IP address filter Lock illegal login IP address Disable SSH</td>
</tr>
<tr>
<td>3 Managed enterprise protection</td>
<td>Large network infrastructure with an IT/IS department. For environments where devices may need to be integrated into an enterprise network infrastructure.</td>
<td>Access to IEEE 802.1x network Configure SNMP monitoring Firewall setup on router Create a port forwarding rule</td>
</tr>
</tbody>
</table>
Default protection

Network devices are delivered with predefined default settings and a default password. Adjust the settings to meet the challenges from the network environment and the result of a risk analysis.
Standard protection

The standard protection level is the minimum recommended level of protection. This level is adequate for small businesses or office installations where, typically, the operator is also the administrator.

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

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.

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.

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

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.

![Device Maintenance Interface]

**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.
Enterprise protection

The enterprise protection level is about minimizing risks by reducing the possible attack area of the network device.

Enable encryption

Access the network device using HTTPS, which encrypts the traffic between the client and the device. 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.

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 your successfully creating and installing the certificate.

![Certificate Details](image)

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 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 Management Interface](image)

**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.**

![NAT Configuration](image)

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

**Disable QoS**

If Quality of Services is not being used, QoS should be disabled

**Steps:**

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

![QoS Configuration](image)

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

**Disable multicast video**

To prevent the device from multicasting video by default, disable multicast video streaming. The device can still multicast video upon request.

**Steps:**

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

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 user name/password attempts (five times for the operator/user)


2. Check the checkbox of Enable Illegal Login Lock, and then the IP address will be locked if the admin user performs seven failed user name/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.

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

Managed enterprise networks are systems that typically have additional management tools and services that the devices need to be aligned with.

Access to IEEE 802.1x network

The IEEE 802.1X standard is supported by the network devices, and when the feature is enabled, the device data is secured and user authentication is needed when connecting the device to the network protected by the IEEE 802.1X.

Steps:
1. Go to Configuration > Network > Advanced Settings > 802.1x.

![Configuration Screen]

2. Click Enable IEEE 802.1x.
3. Input User Name, Password and then confirm.
4. Click Save.

Choose SNMP V3

Steps:
1. Go to Configuration > Network > Advanced Settings > SNMP.
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

2. Login to your router

Password identification

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

<table>
<thead>
<tr>
<th>Login</th>
<th>admin</th>
</tr>
</thead>
<tbody>
<tr>
<td>Password</td>
<td>*****</td>
</tr>
</tbody>
</table>

3. Go to the port forwarding section

Port forwarding can be used to set up public services on your network. When users from the Internet make certain requests on your router, they 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

<table>
<thead>
<tr>
<th>Description</th>
<th>Inbound Port</th>
<th>Type</th>
<th>Private IP Address</th>
<th>Local Port</th>
</tr>
</thead>
</table>

Add  Delete

Create a port forwarding rule

Ports that need to be used for Hikvision

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

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.

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

After that, save the new rule.

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.
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.

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