Network Security Hardening Guide

About This Document

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

Trademarks Acknowledgment

Contact Information

3830 SW 30 Avenue,
Ft. Lauderdale, Florida, 33312

Tel: (305) 937 - 2000
Email: sales@govcomm.us
Website: www.Govcomm.us

Table of Contents

Introduction

GovComm network devices, like any other network devices, may be exposed to cybersecurity risks. To protect the network from the risk, GovComm 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. Recommendations should be taken into consideration depending on the application scenarios.

The Role of GovComm

Preventing Vulnerabilities

GovComm utilizes the following procedures to prevent vulnerabilities:

- Regular in-person and online meetings with IT staff and contract manufacturer(s) to discuss known and potential vulnerabilities
- Follow security notifications
- Work with IT staff and contract manufacturer(s) to update firmware
- Regular testing with hacking software
- Publish and discuss cybersecurity and best practices with customers

GovComm's tracking of identified vulnerabilities:

GovComm keeps track of identified vulnerabilities by using a simple spreadsheet. The risk is identified by date, type of vulnerability, a rating is assigned (e.g. moderate or critical), corrective action and an implementation date are noted.

GovComm's defensive measures to minimize risk or exploitation of vulnerabilities is as follows:

STRONG PASSWORD RECOMMENDED

GovComm ITS cameras come with a default IP address and password. This is done because of specialized functions that need to be installed in the camera. That is why the first thing the end-user should do if the camera is directly exposed to the Internet is to change the default password. Passwords should be reset regularly to better protect equipment.

How to create a strong password?

Follow our acceptable guidelines for the creation of strong passwords:

- 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

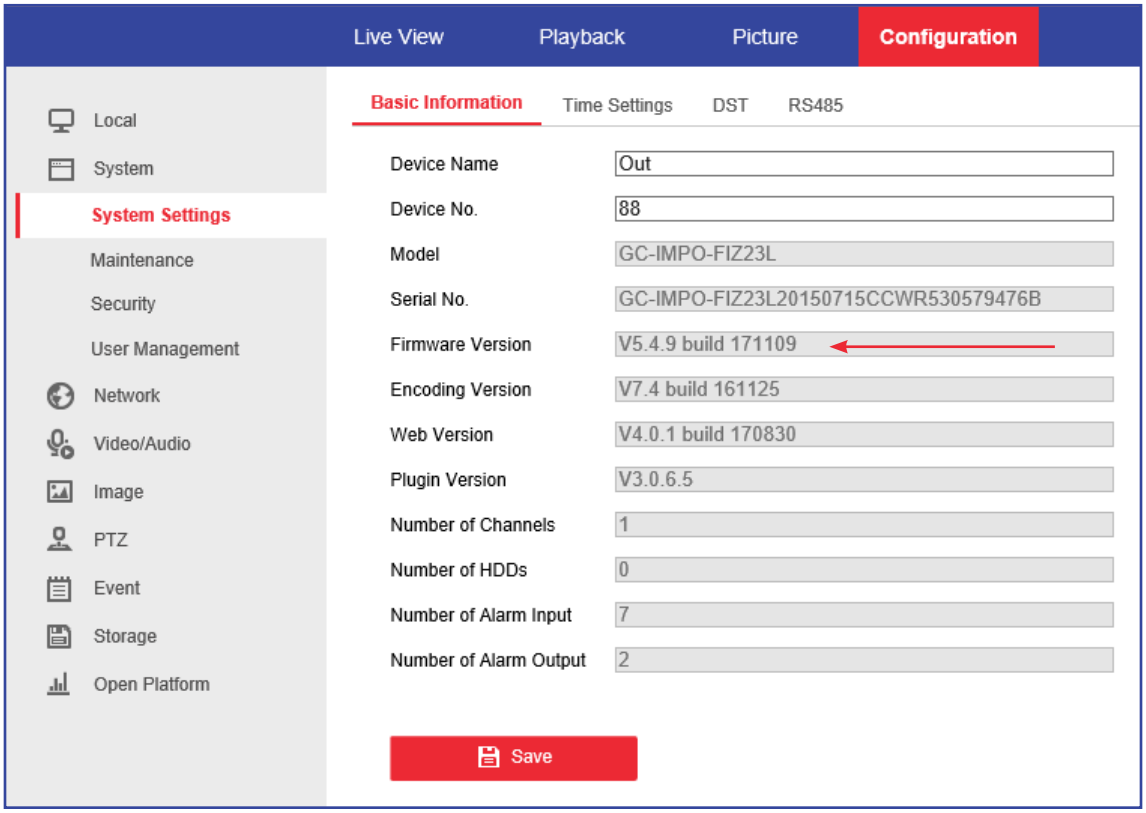
- Avoid using dictionary words in any language.
- Avoid sequences or repeated characters.
- Change your password on a schedule.
- Do not allow Internet Explorer to store passwords.
- Do not type passwords on computers that you do not control.
- Never provide your password via email.
- Never respond to 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.

UPDATE FIRMWARE

Firmware is the software that enables and controls the functionality of network devices. GovComm recommends our customers use the latest firmware to take advantage of all possible security updates and bug fixes.

Check the current firmware

Check the current firmware version in the page: ***Configuration > System Settings > Basic Information***



Upgrade the device to a certain version

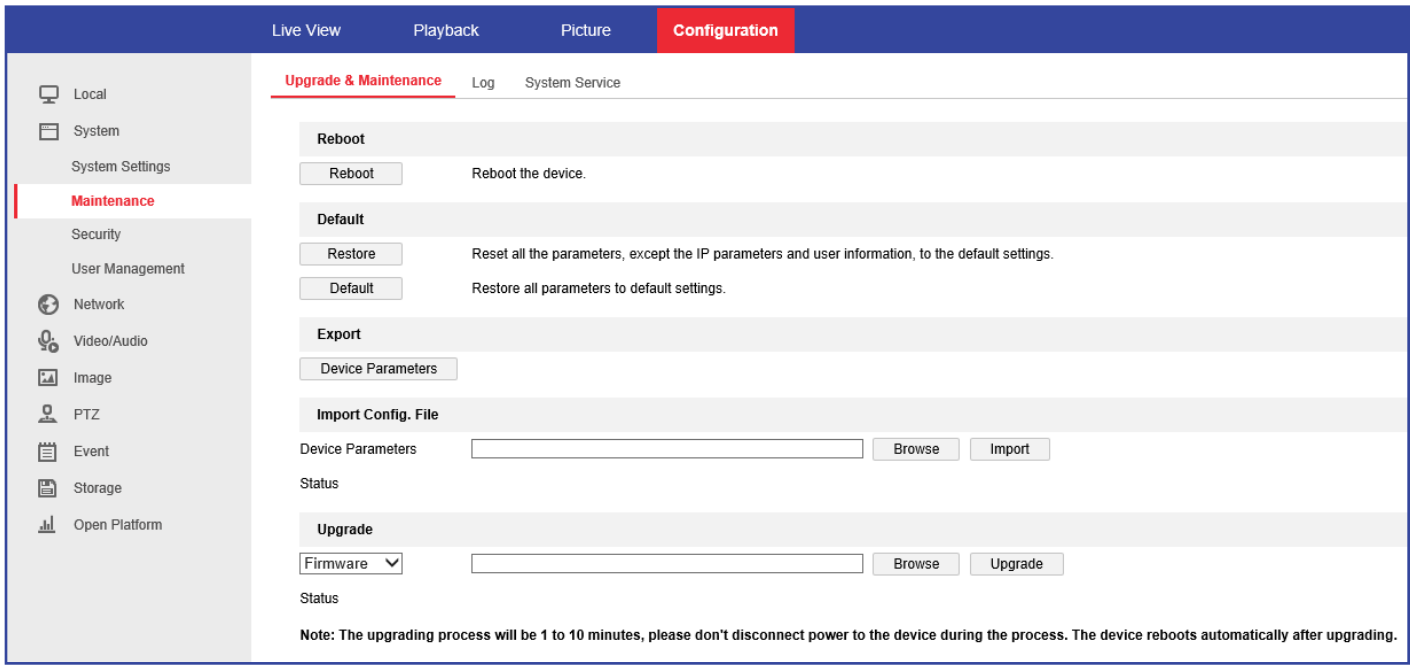
Steps:

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 can take up to 10 minutes. Please don't disconnect power of the device during the process. The device reboots automatically after upgrade.



Restore default settings

If you are not sure about what has been changed with the device, you can always set it to the default settings to restore it to 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. So, 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.

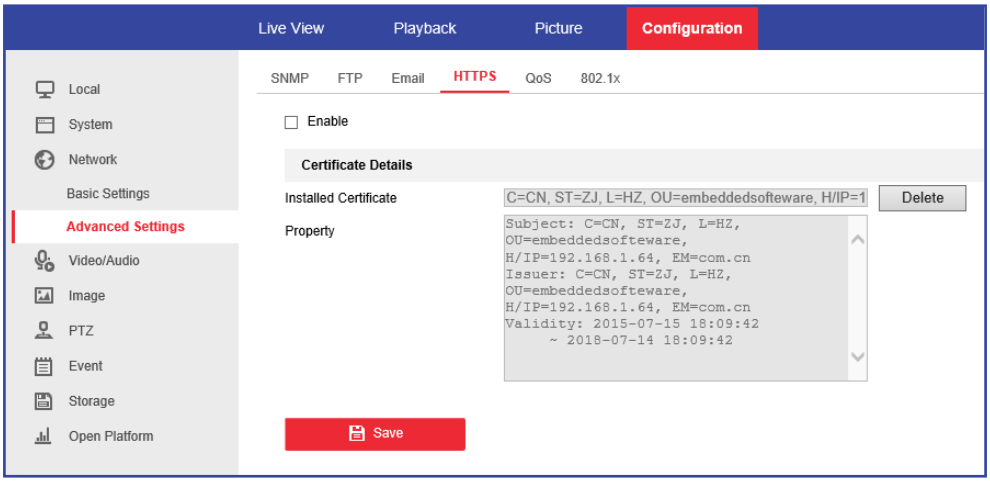
Enable Encryption

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.

For example, 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. C**reate 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, valid**ity a**nd other information.
(4) Click OK to save the settings.

Note: If you already had a certificate **installed, the Create Self-signe**d Certificate is grayed out.

- Create the authorized certificate

(1) Select create the certificate request and continue the installation normally.
(2) Click Create button to create the certificate request. Fill in the required information in the pop-up 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. The certificate information will appear after you successfully create and install the certificate.
5. Click the Save button to save the settings.

User access control

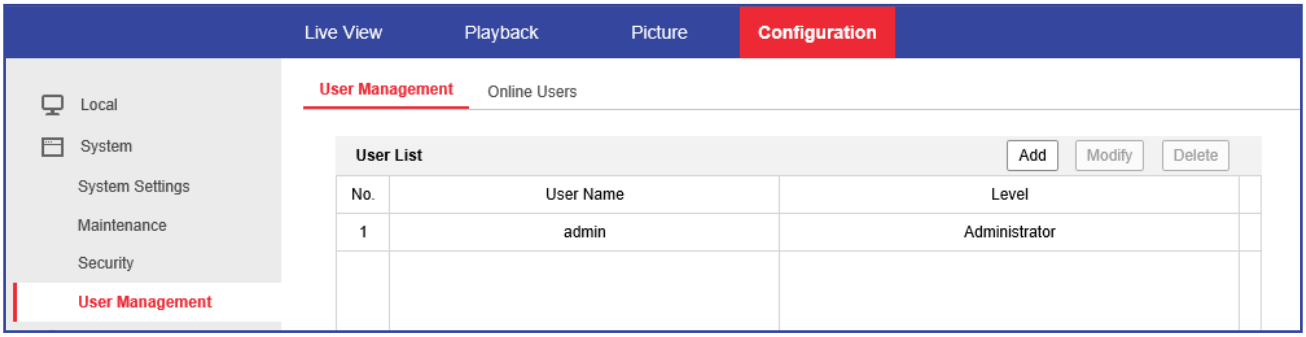
Create unique user names for each user and set individual permission levels for each user to establish limitations on each device.

Set permission level to users

Add and modify user settings to set limitations on the device control

Steps:

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



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.

Set IP address filter

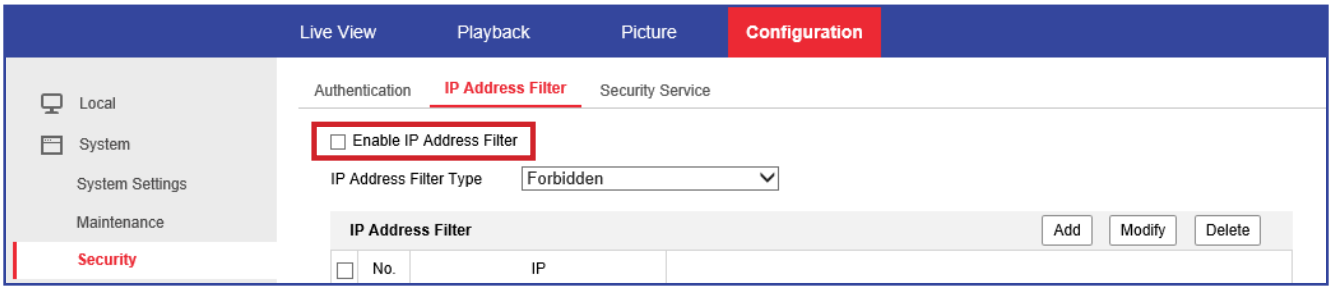
Enabling IP filtering for authorized clients will prevent the device from being accessed by any other unauthorized clients.

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 Add to add an IP.
(2) Input IP Address.
(3) Click 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.

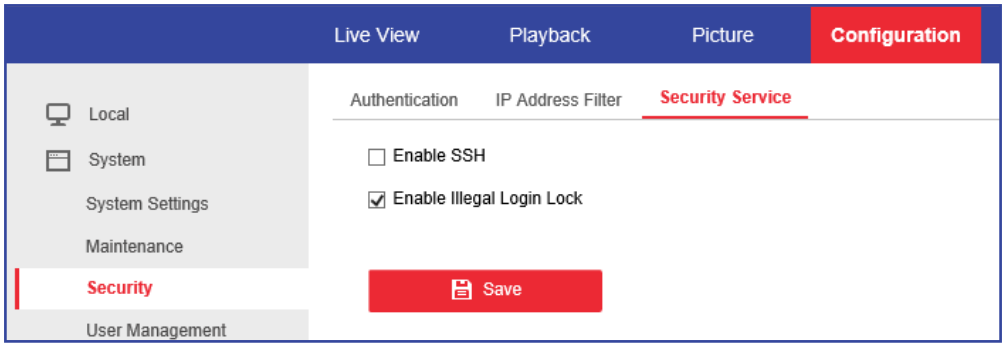
1. Go to ***Configuration > System> Security > Security Service.***
2. Check the checkbox of ***Enable Illegal Login Lock***, and then the IP address will be locked if the admin user performs seven failed username/password attempts (five times for the operator/user).

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

Disable SSH

GovComm 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.



Authentication

GovComm recommends always enabling authentication on RTSP.

Steps:

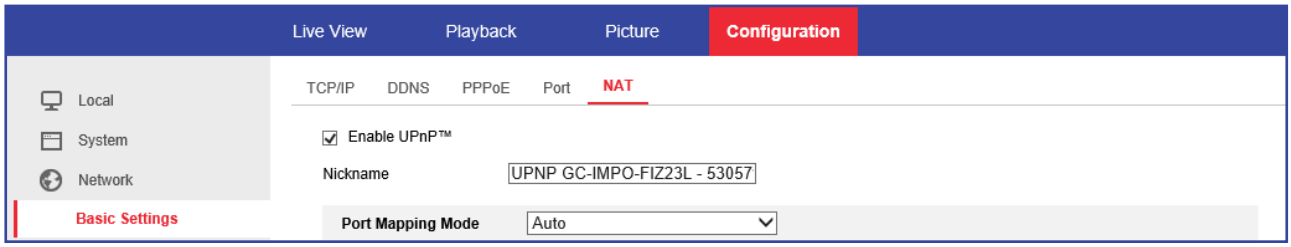
1. Go to ***Configuration > System > Security > Authentication***
2. Click in the drop down and select Basic.
3. Click Save

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.***



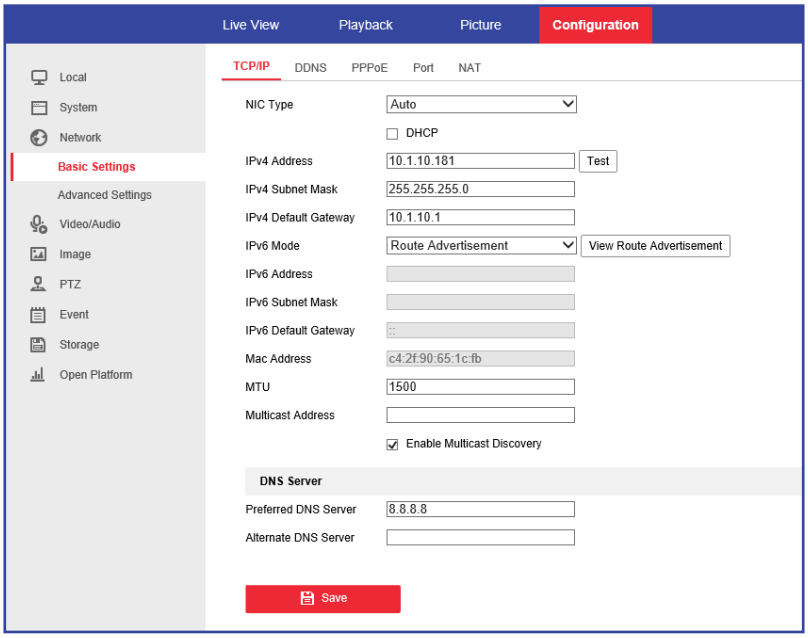
2. Uncheck the checkbox to disable the UPnP™ function.

Disable Multicast video

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

Steps:

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



2. Clear Enable Multicast Discovery
3. Click Save.

GovComm's response plan to identified vulnerabilities is as follows:

- Make an initial assessment.
- Communicate the incident.
- Contain the damage and minimize the risk.
- Identify the type and severity of the compromise.
- Protect evidence.
- Notify external agencies if appropriate.
- Recover systems.
- Compile and organize incident documentation.
- Assess incident damage and cost.
- Review the response and update policies.

Conclusion

This hardening guide is intended to be a living document (Version 2.0) 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 GovComm, Inc. If you have questions, please contact GovComm, Inc. at sales@govcomm.us.