Hanwha Techwin

White Paper

Guidelines for secure use of SNMP

22 09, 2020

Contents

Revision history

Version	Date	Content	Remarks
v1.0	20200922	Initial creation	

1. Occurrence of denial-of-service attacks

Denial-of-service (DoS) attacks using the SNMP service were recently launched against our cameras exposed to a public network. The attacks did not affect cameras installed on internal or local networks. Cameras that are connected to a public network with the SNMP service disabled are not affected by the attack. Additional safeguards can be taken such as placing the camera behind a router with Network Address Translation and blocking unnecessary ports and services. The use of a router can prevent this type of attack from occurring by limiting external access to the camera, and can prevent the need to disable the SNMP protocol.

The SNMP service in question is knows as SNMP v1 and SNMP v2c, which are versions provided for backward compatibility. Users should take precautions even if they have no intention of using the service as SNMP v2c is activated by default in old camera models/old firmware revisions and attackers can abuse the service to launch DoS campaigns.

Against this backdrop, Hanwha Techwin is distributing this "Guidelines for secure use of SNMP" to help users better understand and utilize the security features of the SNMP service in our products.

2. Secure use of the SNMP service

2.1. Introduction of the "SNMP service"

Simple Network Management Protocol (SNMP) is a protocol widely used in network management for monitoring and configuring devices on networks. Network managers can use SNMP to perform tasks such as:

Network architecture management

Identify network hosts and manage architecture.

Performance and device management

Users can analyze performance statistics such as network usage, errors, processing speed, and response time as well as system information (CPU, MEMORY, DISK usage) of certain devices.

Security management

The service offers functions to control and protect information. The latest version SNMP v3 provides enhanced information protection features.

2.2. Secure use of the SNMP service when connecting to a public network

Although the SNMP service offers convenience for network management, the incorrect use of the service can cause issues such as DoS attacks or the unauthorized disclosure of information.

For these reasons, the SNMP service is disabled by default in Hanwha Techwin’s latest cameras and firmware, while providing options to select activation of the service. The SNMP v3 version is provided for secure use of the SNMP service and recommended if the service is to be used.

In order to prevent security breaches that abuse the SNMP service, check if the following measures are applied in your installations.

2.2.1 Update firmware

It is crucial that cameras are running the latest software to ensure that the Operating System, including the SNMP service has the latest version. Please update to the latest firmware by checking on the Hanwha Security website, or by using the Wisenet Device Manager. The Wisenet Device Manager provides an easy method to download the firmware and update cameras in bulk. After the firmware update, please reset to factory default to apply the latest default security settings of the latest firmware, which includes disabling the SNMP service.

1) Search the model name in Hanwha Techwin website and download the latest firmware. After downloading the firmware, extract the camera firmware IMG file from within the ZIP file archive.

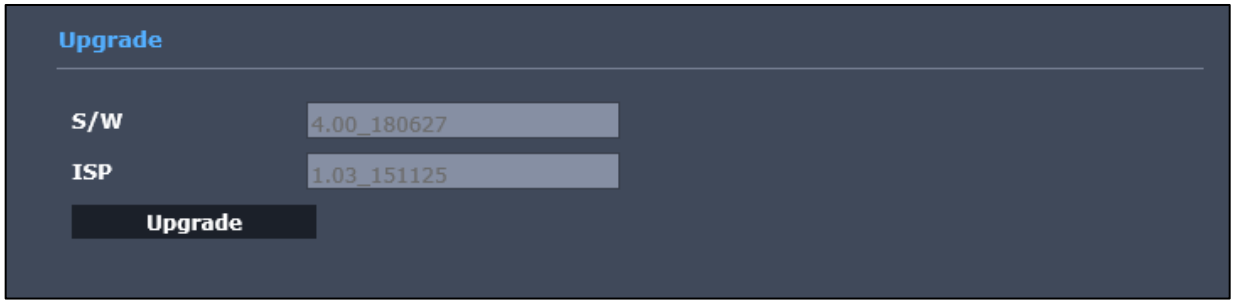
   https://www.hanwha-security.com

2) Upgrade firmware in the camera's menu or with the Wisenet Device Manager.

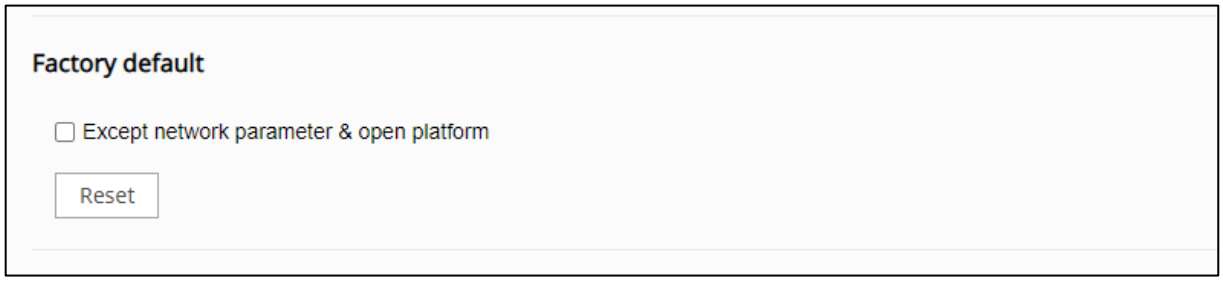
   Menu: Setting → System → Upgrade

3) After the upgrade is complete, reset to factory default. (**Uncheck** "Except network parameter & open platform")

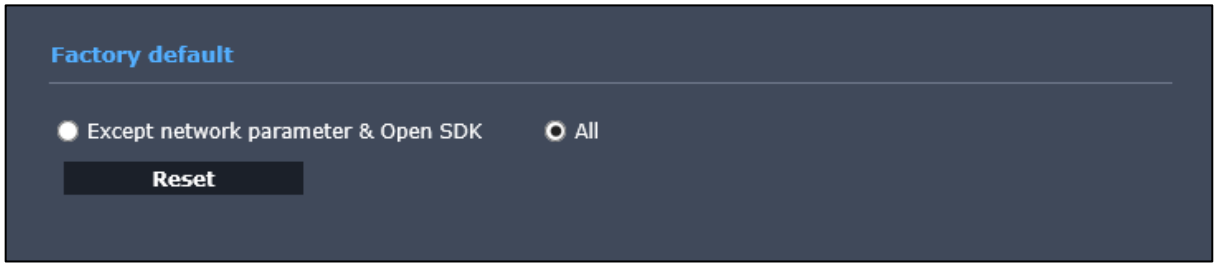
[Firmware upgrade]



[Firmware upgrade of old platform cameras]



[Uncheck “Except network parameter & open platform” during factory default]



[Uncheck “Except network parameter & open platform” during factory default for old platform cameras]

FAQ

Q: Do I need to change the SNMP settings after upgrading firmware?

A: Our devices are designed to keep the previous user settings after a firmware upgrade. For a strong security configuration, please factory default the camera (with the Except network & open platform unselected) or change/verify the SNMP settings after firmware upgrade.

(Remark: Apply 2.2.2 SNMP service inactivation)

FAQ)

Q: What is "Except network parameter & open platform" option in factory default?

A: During factory default, this option maintains the network settings previously configured in the camera (IP, ports, SNMP setting, etc.). If "Except network parameter & open platform" option is selected, the previous configuration, including SNMP settings are maintained. For more thorough security settings, disable "Except network parameter & open platform" option and reset to factory default.

FAQ

Q: Do I need to factory default the camera after upgrading firmware?

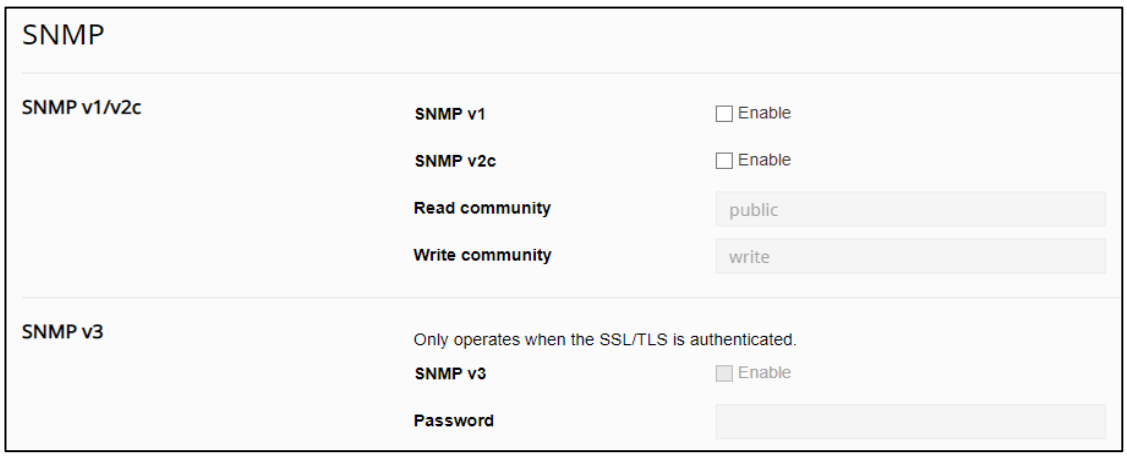
A: It is recommended to factory default the camera to apply the "Secure by Default" settings, including disabled SNMP. However in cases where it is not feasible to factory default the camera, please verify the SNMP settings after performing a firmware upgrade to ensure the SNMP service is disabled or only using the secure v3.

2.2.2 Disabling the SNMP service

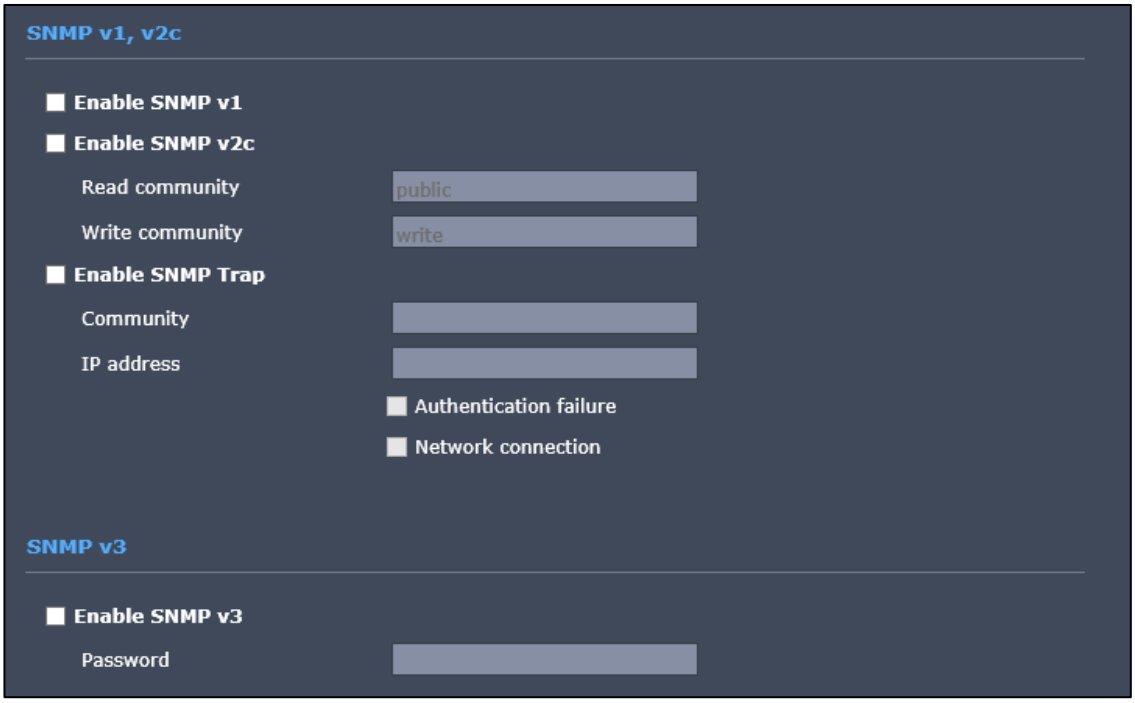
It is recommended to check if the SNMP service is activated. Please disable the service if not used to prevent attackers from abusing the SNMP service. This setting can also be configured in bulk using the Wisenet Device Manager.

1) Menu: Setting → Network → SNMP

2) Disable all SNMP v1, v2c and v3 options



[SNMP service disabled]



[SNMP service disabled in old platform cameras]

FAQ

Q: Why can't I disable SNMP.

A: In devices using firmware released before 2017, users cannot disable the entire SNMP service. In such cases, please upgrade to the latest firmware released from the website to disable the service, or use the Wisenet Device Manager.

2.2.3. Using SNMP v3

To use the SNMP service securely, the SNMP v3 is recommended. SNMP v3 offers secure access through packet authentication and encryption technologies. SNMP v3 supports the following security approaches.

• Message integrity – to ensure a packet has not been tampered while in transit.

• Authentication – to verify the message is from a valid source.

• Confidentiality – to encrypt packets to prevent snooping by an unauthorized source.

To use the SNMP service for network management, we recommend that SNMP v3 is used with the following settings.

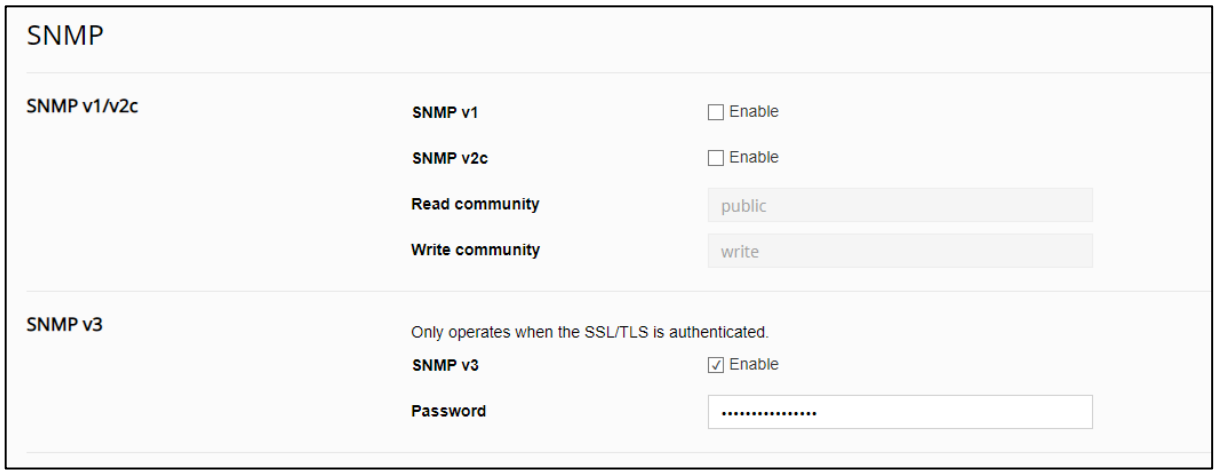
1) Activate HTTPS mode setting (Menu: Setting → Network → HTTPS or SSL). SNMP v3 will not activate until HTTPS mode is enabled.

2) Activate SNMP v3 and configure a password (Menu: Setting → Network → SNMP)

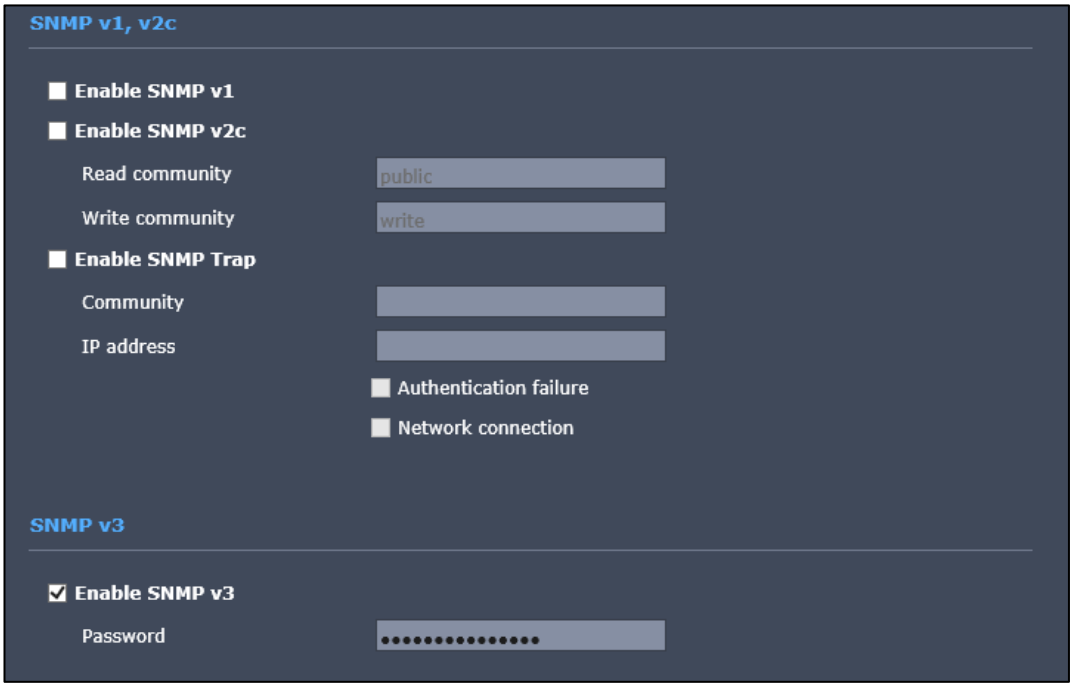
※ Passwords shall be at least 8 characters in length including alphabets and numbers.

3) Ensure that SNMP v1 and 2c are disabled

Note that these settings can also be configured in bulk with the Wisenet Device Manager. Please verify compatibility with your NVR/VMS/CMS with HTTPS mode after configuration, and ensure that your recording solution and network can support the increased load from using HTTPS communications.



[Only SNMP v3 service activated]



[Only SNMP v3 service activated in old platform cameras]

2.2.4. Change the SNMP Community String

If users have no choice but to use SNMP v1 or v2c, they shall change the SNMP's default community string from "public" to create a new one that is strong and difficult to decipher by unauthorized third parties. This can ensure a secure network management environment. It is recommended to use v2c over v1 due to the addition of the community strings.

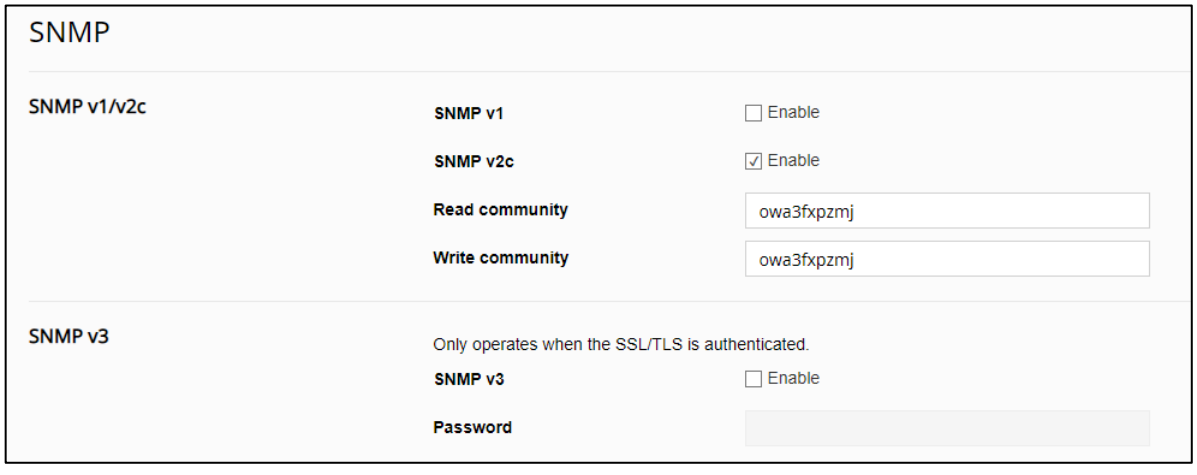
※ Use a community string that is at least 8 characters in length including numbers and letters including uppercase and lowercase.

Example : oWa3fxPzmJ

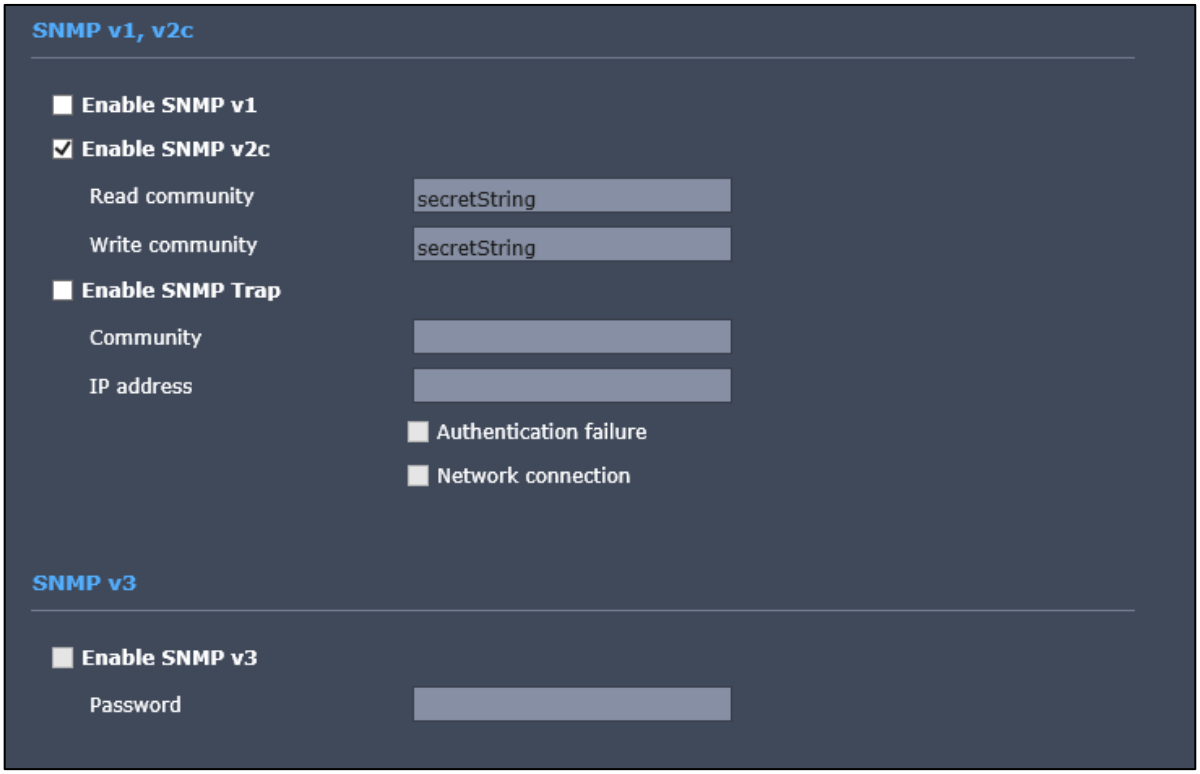
1) Menu: Setting → Network → SNMP

2) Set the Read, Write, & Traps Community Strings to a complex string that is difficult to decipher

3) Apply SNMP v1 and SNMP v2c



[Change the Community String]



[Change the Community String in old platform cameras]

WISENET

Hanwha Techwin Co.,Ltd.
Hanwha Techwin R&D Center
13488 Pangyo-ro 319 Beon-gil 6, Sampyeong-dong, Bundang-gu, Seongnam, Gyeonggido
TEL 070.7147.8771-8
FAX 031.8018.3715
http://hanwha-security.com

Hanwha Techwin