Hikvision Network Camera Series

Security Guidance

Version 0.7

Document history

Version	Date	Comment	Author
0.1	2018-04-06	First draft	XCAS
0.2	2018-04-11	SDK removed and new ISAPI interface added	XCAS
0.3	2018-04-23	Update according evaluation's comments	XCAS
0.4	2018-04-24	Update Hikvision comments	XCAS
0.5	2018-05-03	Updated bibliography	XCAS
0.6	2018-06-28	Tamper seal images added	XCAS
0.7	2018-07-19	Correct version of AGD_UM	XCAS

Contents

1 Introduction

This documents describes the secure preparation steps to set up the TOE in the evaluated TOE configuration.

This document must be only used by users having an Administrator once the courier company delivers the package containing the TOE to the final user.

Although the TOE implements the ISAPI interface that can be used by different software applications, it is mandatory to follow the secure preparation steps using the web application.

2 TOE Secure Acceptance

2.1 Secure Acceptance of the Delivered TOE

This section described the acceptance procedure since Hikvision delivers the TOE until the user receives it and verifies that it is correct.

2.1.1 Delivery

The TOE must be shipped in a carton box with tamper evident seal, in such a way that any tampering attempt would be visible.

2.1.2 Package acceptance

Hikvision will provide all the following documentation to the user:

- Hardware and software identification details. This information will be provided before the shipment and by an alternative communication channel (e.g. e-mail).
- Delivery details of the shipment.

The user must track the package and verify that the shipping details are coherent with the information provided by Hikvision once the package is received. If any inconsistency between the information sent by Hikvision and the actual delivery is detected, the user must not accept the package.

Figure 1 Tamper seal sample

Figure 2 Tamper seal sample after a tampering attempt

The user must check that the tamper evident tape. If any irregularity is found, the user must not accept the package and must contact Hikvision in case of any issue happens during the delivery process to return the TOE. Hikvision will provide a replacement of the TOE.

The package contains a box with the TOE (see Figure 3). The user must verify that the information of the box is consistent to the HW and SW details provided by Hikvision.

Figure 3 TOE box containing the TOE

2.1.3 Hardware acceptance

Once the second package is properly validated, the hardware must be checked. Each TOE has a label on it. It is the responsibility of the user to check that the model printed in the label is the same as it was ordered.

The user must contact Hikvision in case of any tampering attempt is detected in the TOE hardware. Hikvision will provide a replacement of the TOE.

Figure 4 shows an example of a label for a specific model of network camera.

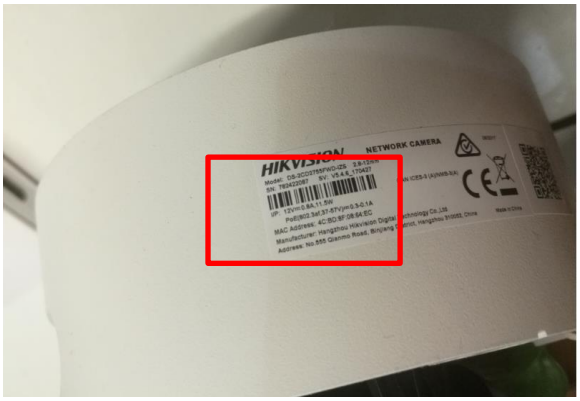

Figure 4 TOE label

2.1.4 Software acceptance

2.1.4.1 Through the web management application

Chapter 1 of this document describes the steps needed to configure the TOE in the network and activate it. Once the user is logged in the TOE, the software details must be checked to be consistent with the information provided by Hikvision.

Device Name	IP CAMERA
Device No.	88
Model	DS-2CD2755FWD-IZS
Serial No.	DS-2CD2755FWD-IZS20170703AAWR782422087
Firmware Version	V5.5.0 build 171116
Encoding Version	V7.3 build 170725
Web Version	V4.0.1 build 170711
Plugin Version	V3.0.6.26
Number of Channels	1
Number of HDDs	1
Number of Alarm Input	1
Number of Alarm Output	1
Firmware Version Property	B-R-G1-0

Figure 5 TOE identification on the web GUI

2.1.4.2 Through the website

The user must go to Hikvision's web page and download the correct version of the firmware for the TOE. The integrity of the downloaded image must be checked to be the same as it is in the web page.

If the integrity is correct, the user must install the proper firmware version in the TOE. In case of detecting any integrity inconsistency, it is recommended to repeat the downloading process and integrity verification again. If the error persists, the user must contact Hikvision, which will take the necessary actions to provide a correct version of the firmware.

2.2 Secure Preparation of the TOE environment

The evaluated scenario consists of a LAN network which is totally isolated from other networks (e.g. other LANs or Internet). The LAN network must be set up in a manner preventing the connection of unauthorized devices by unauthorized users. The TOE network may contain the following components: one or multiple TOEs, video recording devices (such as NVR) and management computers via ISAPI. All the network components coexisting with the TOE must be free of potentially harmful software, particularly any software that might be used to perform DoS attacks to the TOEs in the LAN. Figure 4 illustrates the environment where the TOE is intended to be used:

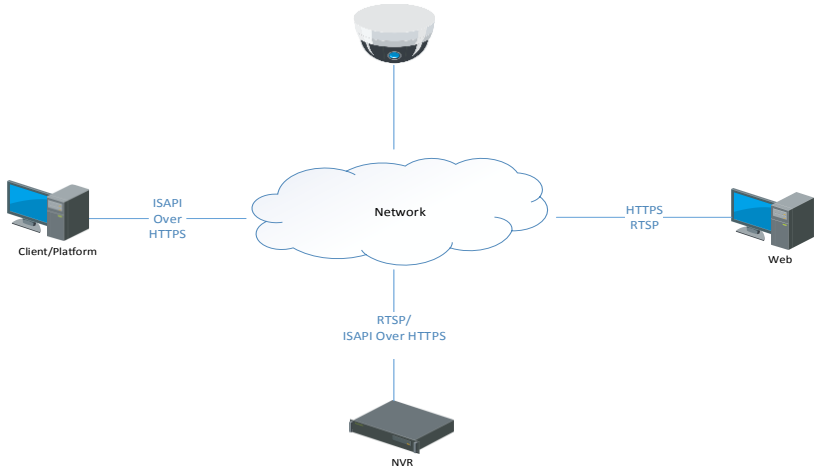

Figure 6 Evaluated scenario

The usage scenarios in scope of the evaluation are:

- TOE's management interface being accessed from a browser or a client/platform software using ISAPI over HTTPS. ISAPI is an HTTP-based application programming interface that enables the TOE to communicate with IP media devices. Web application and client/platform programs must implement this API.
- Video data distribution to a network recording device or to a web browser using the following the RTSP protocol.

The TOE does not provide confidentiality protection of the video data when distributing it to external entities through the TOE network.

3 Secure Preparation

3.1 SD card installation

It is **mandatory** to install a SD card in the TOE. The SD card storage size must be at least 128Gb. This card stores the logs of the camera.

3.2 Browser security

The administrator and all trusted users of the TOE must configure their browser (Internet Explorer) to only accept TLS versions 1.1 and 1.2.

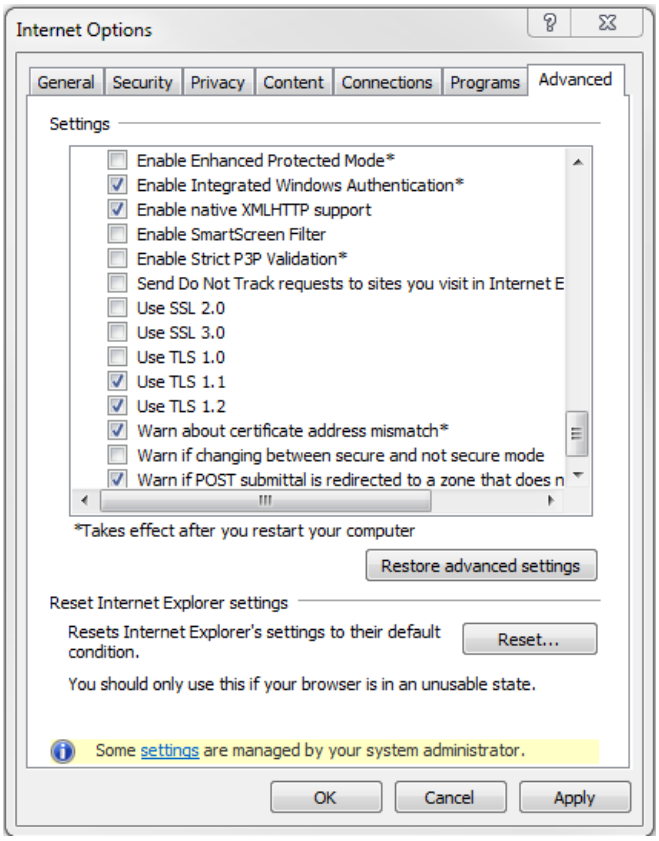

Figure 7 Web browser TLS configuration

3.3 Network Connection

3.3.1 Setting the TOE over the LAN

3.3.1.1 Wiring over the LAN

The TOE **can only be used** in a LAN network totally isolated from other networks (e.g. other LANs or Internet). The TOE network may contain the following components: one or multiple TOEs, video recording devices (such as NVR) and management computers via ISAPI.

Details of the environment preparation are detailed in Section 2.2.

3.3.2 Activating the Camera

Follow the steps described in Section 2.1.2 of [AGD_UM] taking into consideration the following **mandatory** requirements:

- For both web browser, it is mandatory to create a strong password of your own choosing (using a minimum of 8 characters, including at least two of the following categories: upper case letters, lower case letters, numbers, and special characters) in order to increase the security of your product.

Note that only the section “Activation via Web Browser” **must be applied**. Steps described in “Activation via SADP Software” **must not be used**.

3.3.3 Setting the Network Camera over Wi-Fi

Wi-Fi interface is not in the scope of the certified configuration. Therefore, it **must not be used**. Details of the environment preparation are detailed in Section 2.2.

3.3.4 Setting the Network Camera over the WAN

WAN interface is not in the scope of the certified configuration. Therefore, it **must not** be used. Details of the environment preparation are detailed in Section 2.2.

3.4 Access to the TOE

The TOE **can only be managed** by the web interface. The steps to be followed in both cases are described in Section 3.1 of [AGD_UM].

3.5 Network Camera Configuration

TOE configuration is described in Chapter 6 of [AGD_UM]. Following sections describe mandatory requirements for the secure TOE configuration that **must be taken into account** when following the user manual instructions.

3.5.1 Configuring Time Settings

In section 6.2.2 of [AGD_UM], the NTP interface **must be disabled**. The reason is that it is out of the scope of the certified configuration.

3.5.2 Configuring RS232 Settings

In section 6.2.3 of [AGD_UM], the RS232 port **must not be used**. The reason is that it is out of the scope of the certified configuration.

3.5.3 Configuring RS485 Settings

In section 6.2.4 of [AGD_UM], the RS485 port **must not be used**. The reason is that it is out of the scope of the certified configuration.

3.5.4 Configuring External Devices

In section 6.2.6 of [AGD_UM], external devices **must not be used**. The reason is that they are out of the scope of the certified configuration.

3.5.5 Security Settings

In section 6.4.3 of [AGD_UM], the "Enable Illegal Login Lock" option **must be enabled** in order to set the limits of unsuccessful login attempts.

3.5.6 User management

In section 6.5 of [AGD_UM], the following mandatory security requirements must be taken into consideration:

- When adding a new user or modifying an existing user (section 6.5.1 of [AGD_UM]), it is **mandatory** to create a strong password of your own choosing (using a minimum of 8 characters, including at least two of the following categories: upper case letters, lower case letters, numbers, and special characters) in order to increase the security of your product.

3.5.7 IP configuration

In Section 7.1.1 of [AGD_UM], the IPv6 **must not be used** since it is out of the scope of the evaluated configuration.

3.5.8 DDNS

In Section 7.1.2 of [AGD_UM], the DDNS service must not be used since it is out of the scope of the evaluated configuration.

3.5.9 PPPoE

In Section 7.1.3 of [AGD_UM], the PPPOE interface **must not be used** since it is out of the scope of the evaluated configuration.

3.5.10 SNMP

In Section 7.2.1 of [AGD_UM], all versions of the SNMP service **must be disabled** since it is out of the scope of the evaluated configuration.

3.5.11 FTP

In Section 7.2.2 of [AGD_UM], the FTP service **must not be used** since it is out of the scope of the evaluated configuration.

3.5.12 E-mail

In Section 7.2.3 of [AGD_UM], the email service **must not be used** since it is out of the scope of the evaluated configuration.

3.5.13 Platform Access

In Section 7.2.4 of [AGD_UM], the Platform Access service **must be disabled** since it is out of the scope of the evaluated configuration.

3.5.14 Wireless Dial

In Section 7.2.5 of [AGD_UM], the Wireless Dial service **must not be used** since it is out of the scope of the evaluated configuration.

3.5.15 HTTPs configuration

As described in Section 6.2.6 of [AGD_UM]:

- Follow the steps to install a CA signed certificate. **DO NOT INSTALL** self-signed certificates.
- HTTPs (port 443) **must be enabled**.
- HTTP (port 80) **must be disabled** (Check HTTPS navigation only).

Until these steps had been successfully completed, the TOE is NOT in the secure operational state.

3.5.16 QOS

In Section 7.2.7 of [AGD_UM], the QOS functionality **must not be used** since it is out of the scope of the evaluated configuration.

3.5.17 802.1X

In Section 7.2.8 of [AGD_UM], the 802.1X standard **must not be used** since it is out of the scope of the evaluated configuration.

4 Secure Operation of the TOE

The security requirements described in this Chapter supersedes the security recommendations described in the User Manual for the web application [AGD_UM].

4.1 Password policy

The TOE allows to add new users as it is described in Section 6.5.1 of [AGD_UM]. For all the possible roles it is **mandatory** to use a strong password of your own choosing (using a minimum of 8 characters, including at least two of the following categories: upper case letters, lower case letters, numbers, and special characters) in order to increase the security of your product.

5 Abbreviations and glossary

[CC]	Common Criteria
[CIFS]	Common Internet File System
[DDNS]	Dynamic DNS
[DNS]	Domain Name server
[FTP]	File Transfer Protocol
[IP]	Internet Protocol
[ISAPI]	IP Surveillance Application Interface Programming
[LAN]	Local Area Network
[NAS]	Network Attached Storage
[NFS]	Network File System
[NTP]	Network Time Protocol
[NVR]	Network Video Recorder
[OS]	Operating System
[PPPoE]	Point-to-Point Protocol over Ethernet
[SNMP]	Simple Network Management Protocol
[ST]	Security Target
[RTSP]	Real Time Streaming Protocol
[TOE]	Target of Evaluation
[UPNP]	Universal Plug and Play

6 References

[AGD_UM] Network Camera User Manual UD09650B

[ISAPI-IMG] Hikvision IP Surveillance API, Image Service Specification, v2.1 rev.1, 2014-05

[ISAPI-PTZ] Hikvision IP Surveillance API, PTZ Service Specification, v2.2 rev1, 2014-07

[ISAPI-RACM] Hikvision IP Surveillance API, (RaCM Part) User Guide, v2.0 rev1, 2014-01

[ISAPI-GUIDE] Hikvision IP Surveillance API User Guide, v2.6

[ISAPI-MANUAL] Hikvision Open ISAPI Protocol User Manual Core, v18.03