יום חמישי 10 מרץ 2022

Camera Report

-

Rhodium RDO5372-FPC

Network Camera

Table of Contents

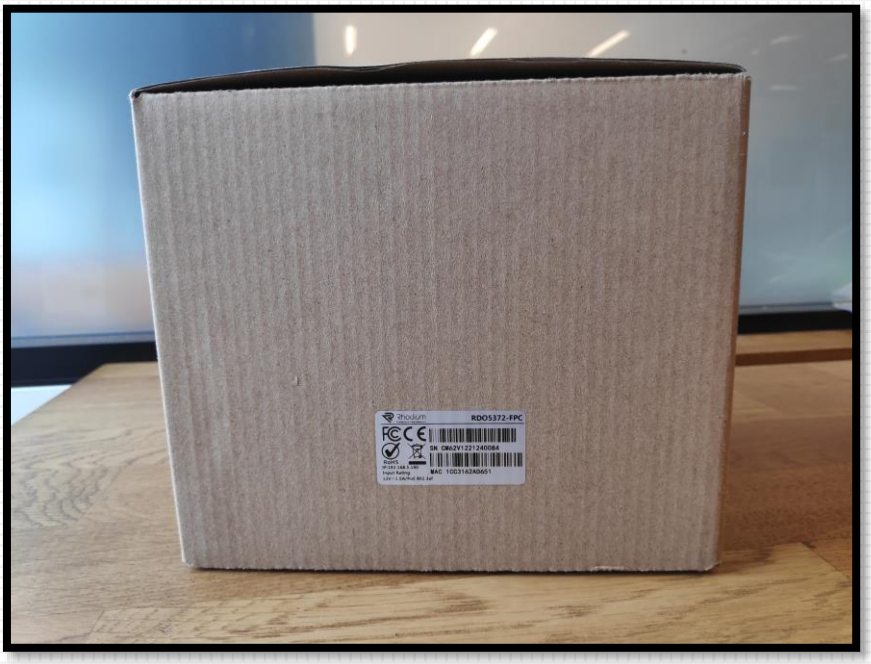
1 Product Details

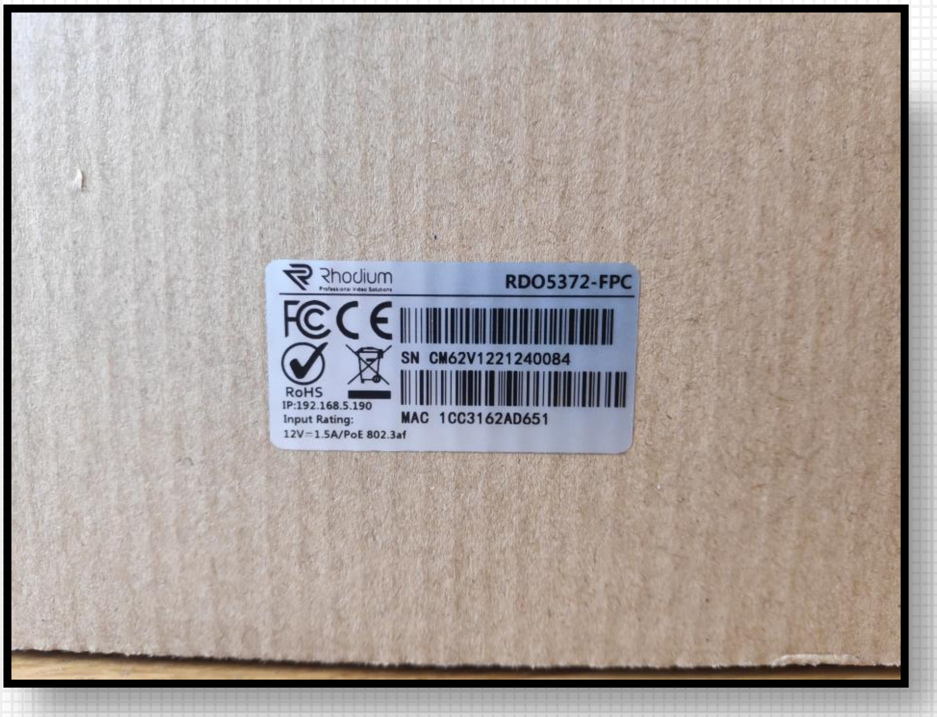
1.1 RHODIUM Dome Camera

RHODIUM NETWORK CAMERA

PRODUCT MODEL:	RDO5372-FPC
SERIAL NUMBER:	CM62V1221240084
SOFTWARE VERSION:	45.7.1.79-r17
MAC ADDRESS:	1C:C3:16:2A:D6:51

1.2 Photos of Test Product




Rhodium
Professional Video Solutions
RDO5372-FPC
SN CM62V1221240084
RoHS
IP:192.168.5.190
Input Rating:
12V⎓1.5A/PoE 802.3af
MAC 1CC3162AD651

Network Camera

2 System Compliance with Security Standards

Security Requirements:	Results:
Three Levels of Access	fulfils requirement
Password Strength	fulfils requirement
Signed firmware files	fulfils requirement *
Blocking of Third Party Software	fulfils requirement
SSL/TLS	fulfils requirement
Access Control	fulfils requirement
Encryption Standards	fulfils requirement **
Firewall	fulfils requirement
Tamper Detection	fulfils requirement **

* Provided User compliance with supplied procedures (procedures supplied in supplemental documentation).

** Requires User Actions. (See Below).

Summary: This Device meets the security requirements for this section.

Note: This applies only if the outlined security procedures are followed (as provided to the client). Device's default protocols contain known security vulnerabilities and exploits. Certain functions must be enabled before secure usage is possible.

3 Procedural Details and Findings

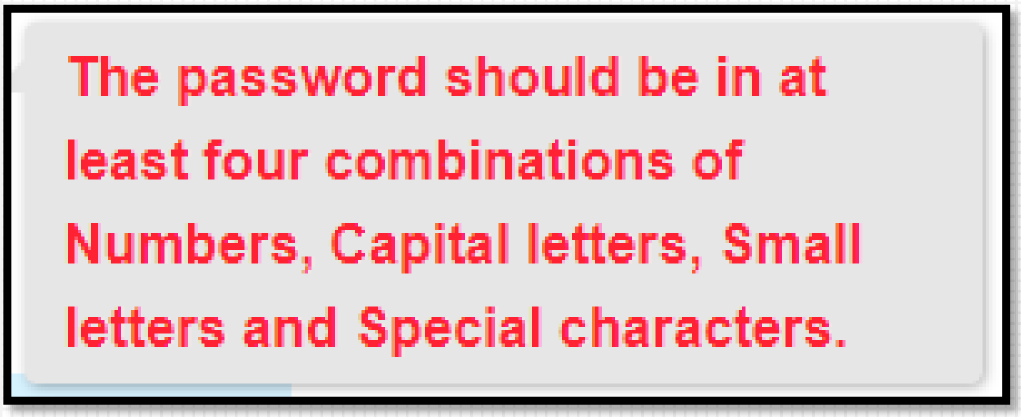
3.1 Test Details

- Testing of existing Access Levels for Device.
- Testing strength of the Minimum Password requirements for Device.
- Testing requirements for Signatures of Firmware files.
- Testing for 3rd Party Software installation on Device (Permitted/Blocked).
- For SSL Devices: Testing of Device Connections/Communications.
- Checking for existence of an access list to the Device.
- Testing for the existence (and standards/levels) of encryption on the Device.

3.2 Examination of Default Settings and Processes

- Upon initial activation, a password is required for the Admin User. This User will have Administrator-level access to the Device.
- As part of this password-setting process the Device asks the User to enter a password of between 9 and 32 characters. This password must include the following:
    1. Uppercase English characters.
    2. Lowercase English characters.
    3. Numerical Digits.
    4. Special Characters.

For this test the password was set as: **AAAaaa123!@#**

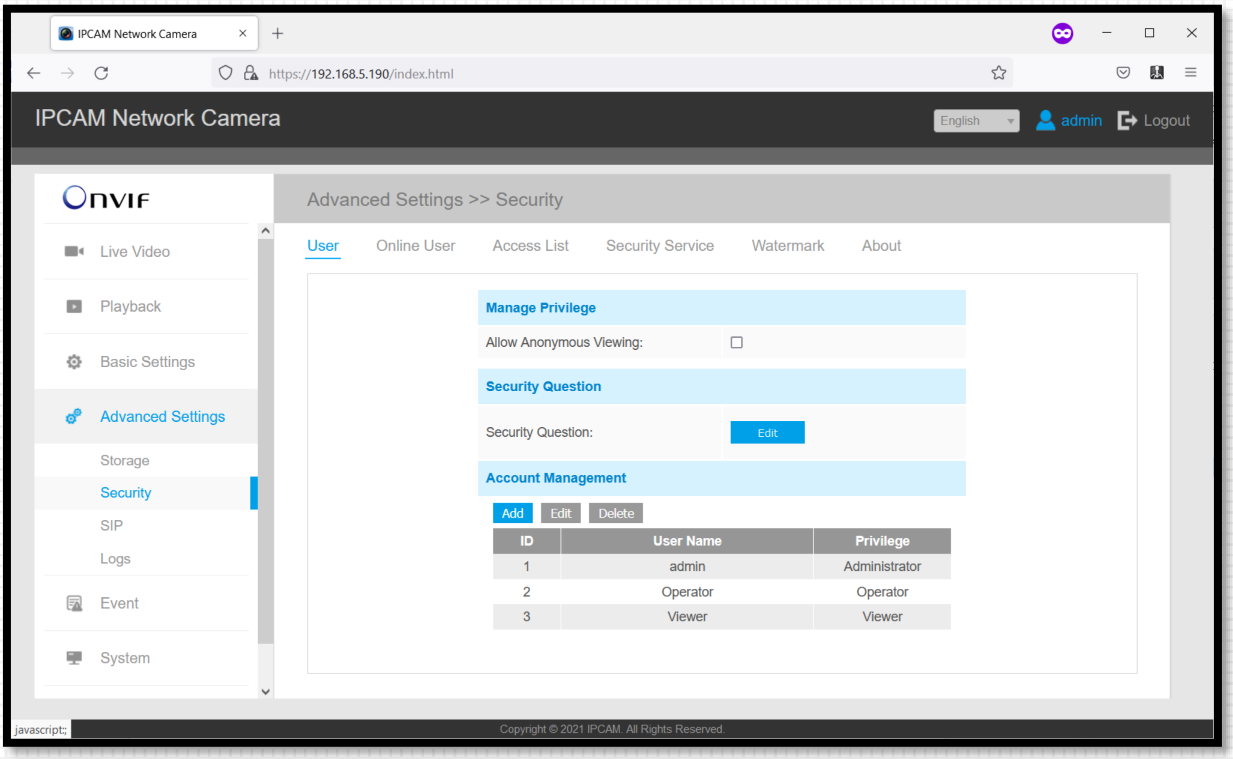


The password should be in at least four combinations of Numbers, Capital letters, Small letters and Special characters.

- By default, the Device will limit the number of incorrect password entries to 4 attempts.
- After entering the password, the user will be asked to set three security questions. This step can be skipped.

3.3 Access Levels for Device

This Device permits three levels of access: Administrator, Operator, and Viewer.



Manage Privilege

Allow Anonymous Viewing: ☐

Security Question

Security Question: Edit

Account Management

Add Edit Delete

ID	User Name	Privilege
1	admin	Administrator
2	Operator	Operator
3	Viewer	Viewer

- The default User ('admin') is the sole Administrator-level User. With full access and privileges. It cannot create another User with similar levels of access.

- The username of the 'admin' cannot be changed.

- Each level of access privileges has its own default settings. The individual, specific privileges can be individually changed manually.

The required access levels for a Device such as this are as follows:

1. Watch live video only. (Uses 'Viewer' level permissions).
2. Watch live video, watch recordings, and have Control options. (Uses 'Operator' level permissions).
3. Authorization of a configuration and adding new "Operator" and "Viewer" level User. (Requires 'Administrator' level permissions).

Summary: This Device meets the section requirements.

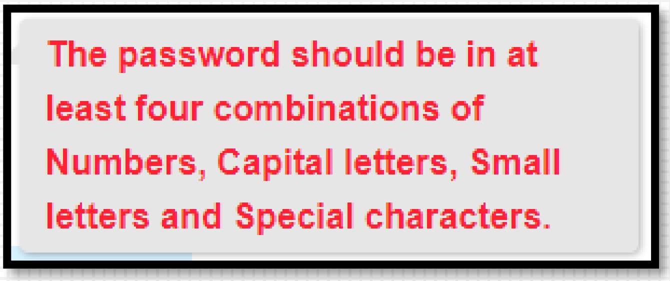
3.4 Minimum Password Strength

The Device requires the User to enter a password of between 9 and 32 characters.

This password must include three of the following.

1. Uppercase English characters.
2. Lowercase English characters.
3. Numerical Digits.
4. Special Characters.

For this test the password was set as: **AAAaaa123!@#**



The password should be in at least four combinations of Numbers, Capital letters, Small letters and Special characters.

The password strength requirements for a Device such as this are as follows:

- The Device must require all of the following conditions:

  a. Password length longer than 9 characters.

  b. Password must contain at least 1 Uppercase English character.

  c. Password must contain at least 1 Lowercase English character.

  d. Password must contain at least 1 Numerical digit.

  e. Password must contain at least 1 Special character.

Summary: This Device meets the section requirements.

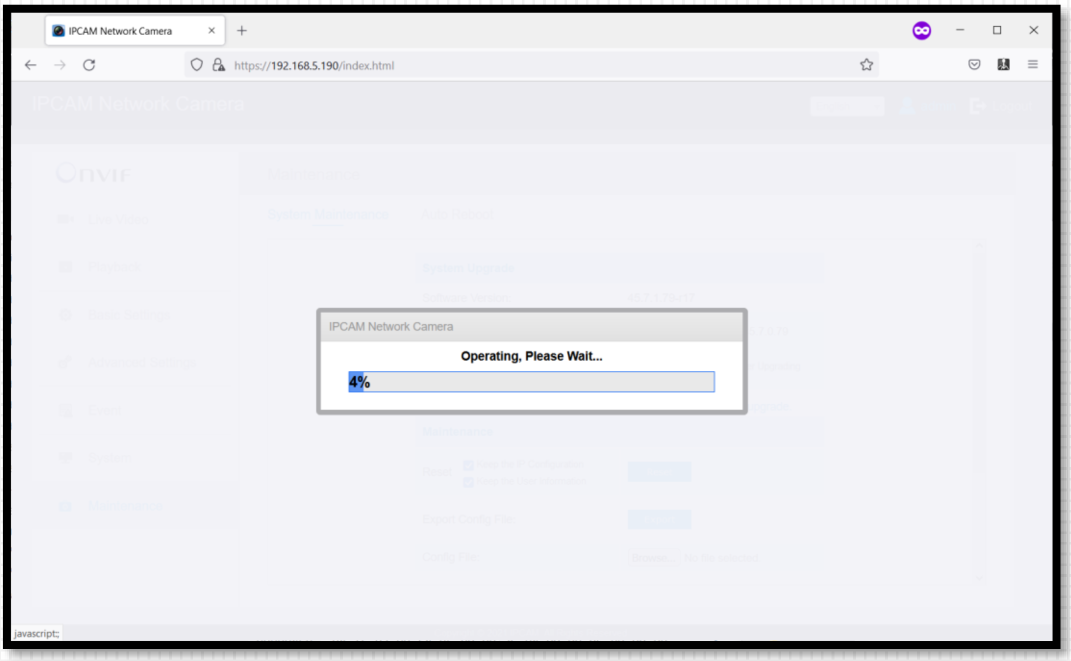
3.5 Signature Requirements for Signing of Firmware Files

The Device arrived with firmware version: 45.7.1.79-r17 installed.
On 12/23/21, our company received a firmware version: 45.7.1.79-r17, identical to the firmware currently already running on the Device.

For the test, the file received from the company was used (45.7.1.79-r17), along with an old firmware file received from the client (version 45.7.0.79).

A copy was created for each firmware file in which a change was made to the code.

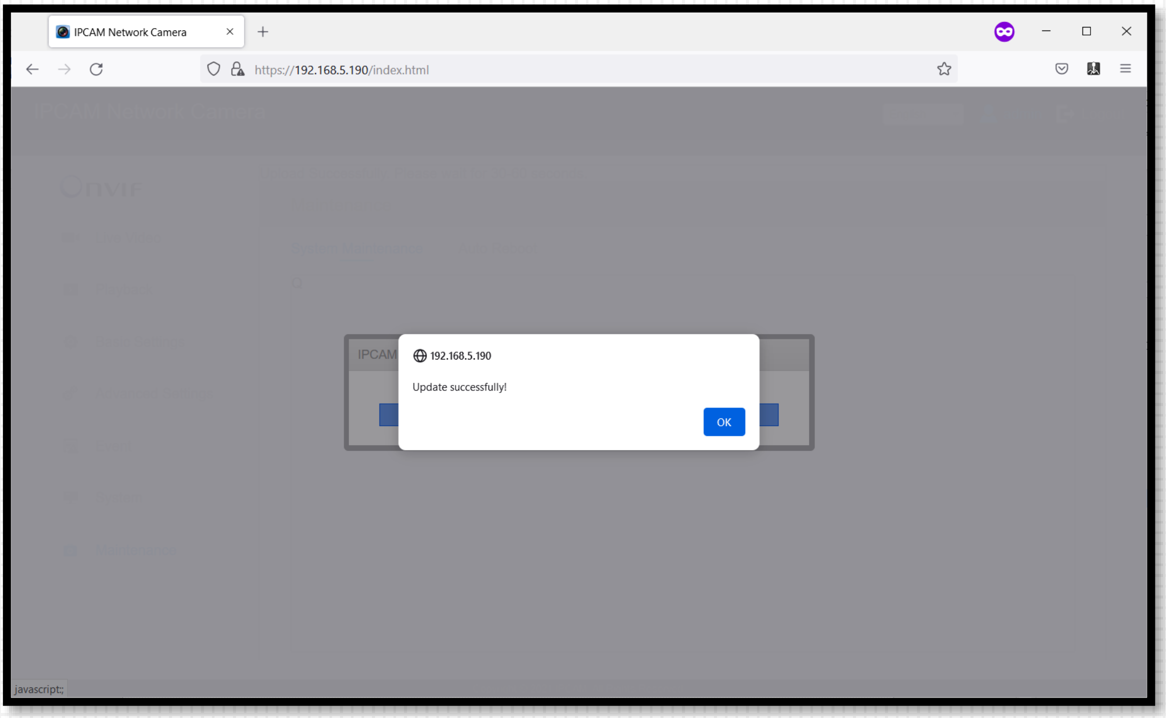
An attempt was then made to update the device with the edited file. The update attempt on the (earlier) version of the firmware (45.7.0.79) was not blocked by the system.
The later version of the firmware (45.7.1.79-r17) was similarly modified and the update was successfully applied.



IPCAM Network Camera

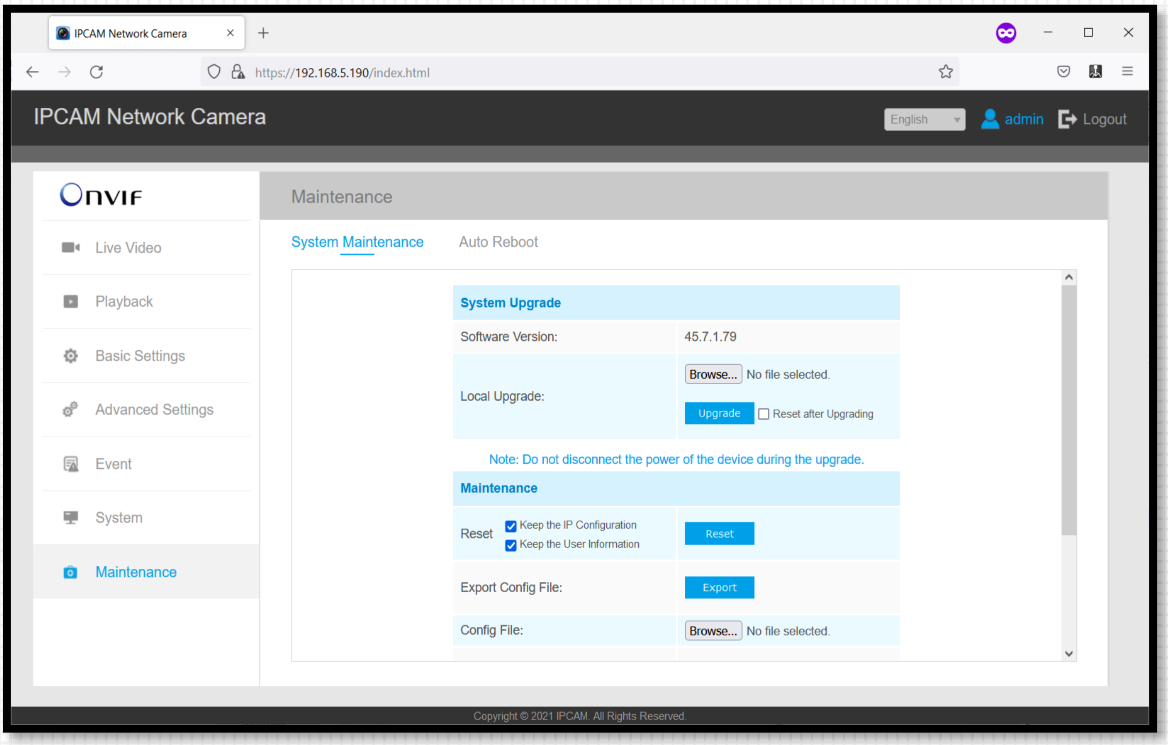
Operating, Please Wait...

4%



192.168.5.190

Update successfully!



System Upgrade

Software Version:	45.7.1.79
Local Upgrade:	Browse... No file selected. Upgrade □ Reset after Upgrading

Note: Do not disconnect the power of the device during the upgrade.

Maintenance

Reset ☑ Keep the IP Configuration ☑ Keep the User Information	Reset
Export Config File:	Export
Config File:	Browse... No file selected.

The security requirements for a Device such as this are as follows:

- The (default) Firmware installation settings must require a firmware file signed by the production company.

Summary: This Device meets the section requirements.*

*(provided User compliance with supplied procedures (procedures supplied in supplemental documentation).

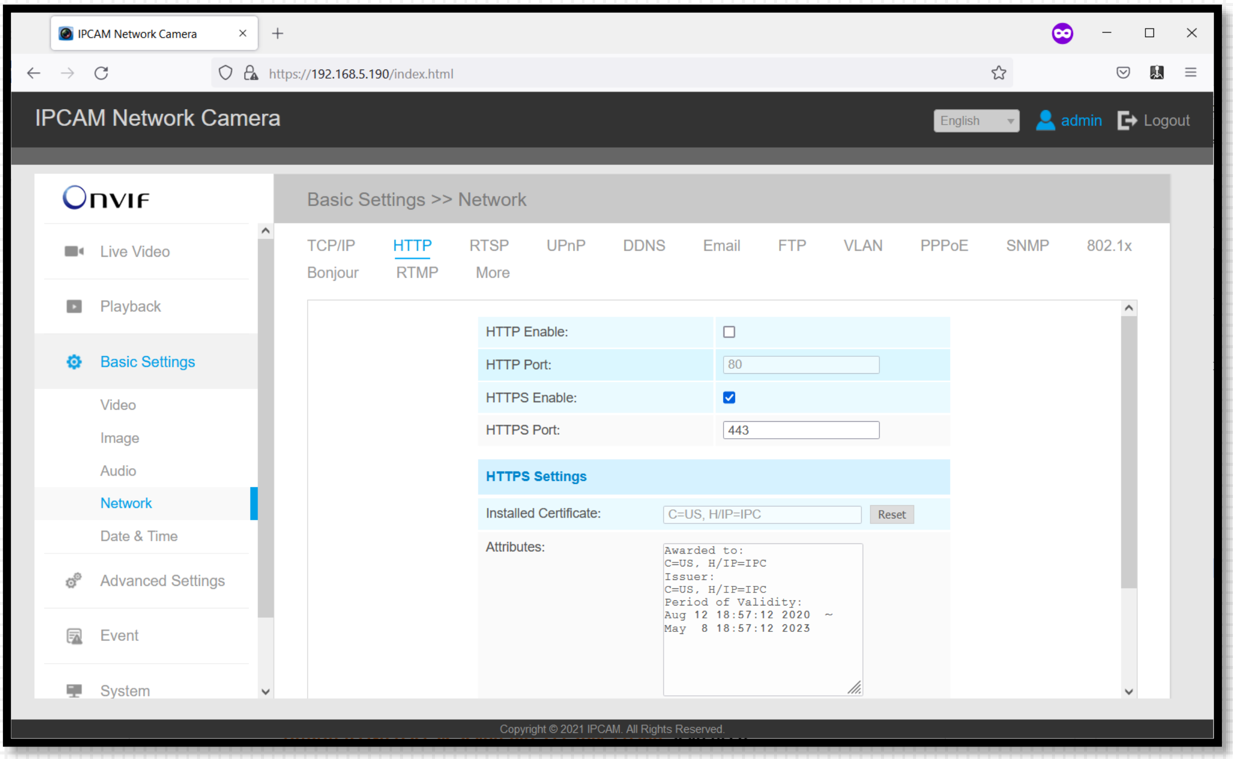
3.6 Blocking of Third Party Programs

- Attempts were made to install Third-Party software on the Device.
- The User Interface does not contain an option to install third-party software.
- Attempts to use the interface to install third-party software were unsuccessful.
- This Device does not permit the installation of third-party software.

Summary: **This Device meets the section requirements.**

3.7 SSL/TLS

The Device allows the use of HTTPS (via the HTTP protocol and on the SSL/TLS layer).



HTTP Enable: ☐

HTTP Port: 80

HTTPS Enable: ☑

HTTPS Port: 443

HTTPS Settings

Installed Certificate: C=US, H/IP=IPC

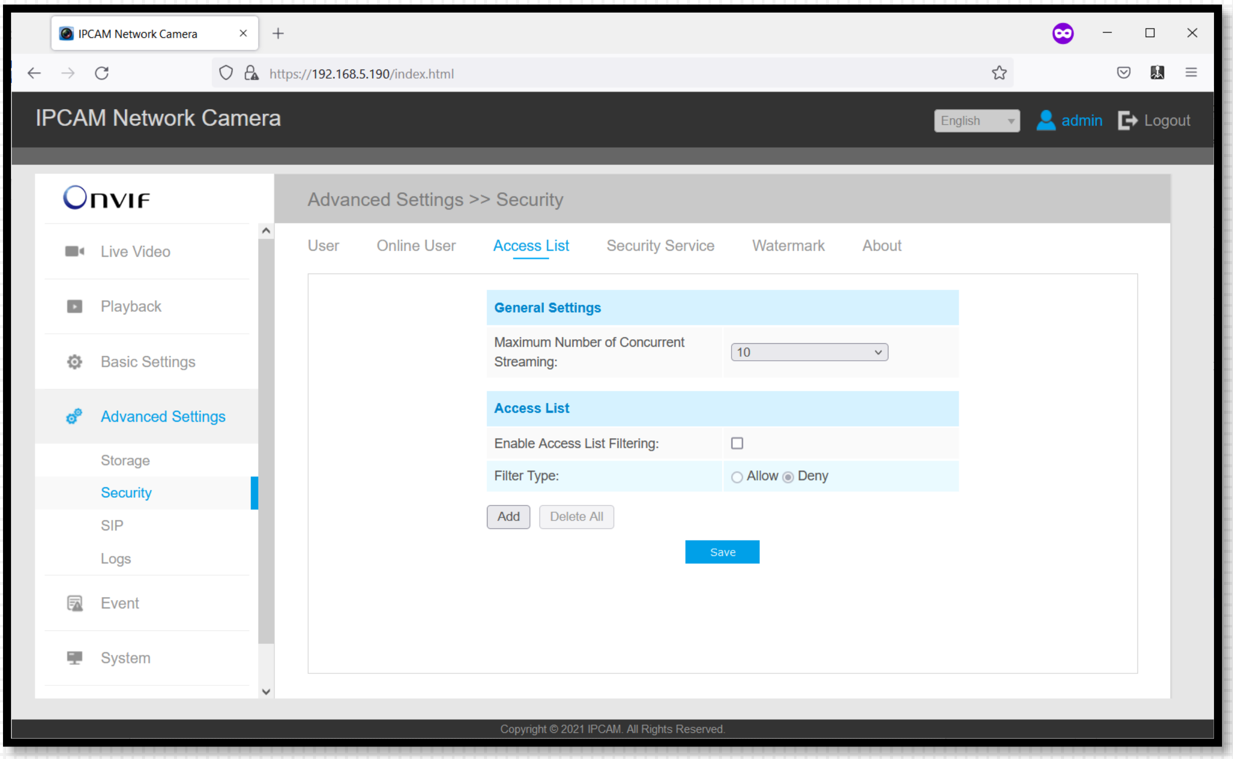
Attributes:

```
Awarded to:
C=US, H/IP=IPC
Issuer:
C=US, H/IP=IPC
Period of Validity:
Aug 12 18:57:12 2020  ~
May  8 18:57:12 2023
```

<u>Summary:</u> **This Device meets the section requirements.**

3.8 Access Control

The Device permits access-list management as required.



General Settings

Maximum Number of Concurrent Streaming: 10

Access List

Enable Access List Filtering: □

Filter Type: ○ Allow ● Deny

Add Delete All

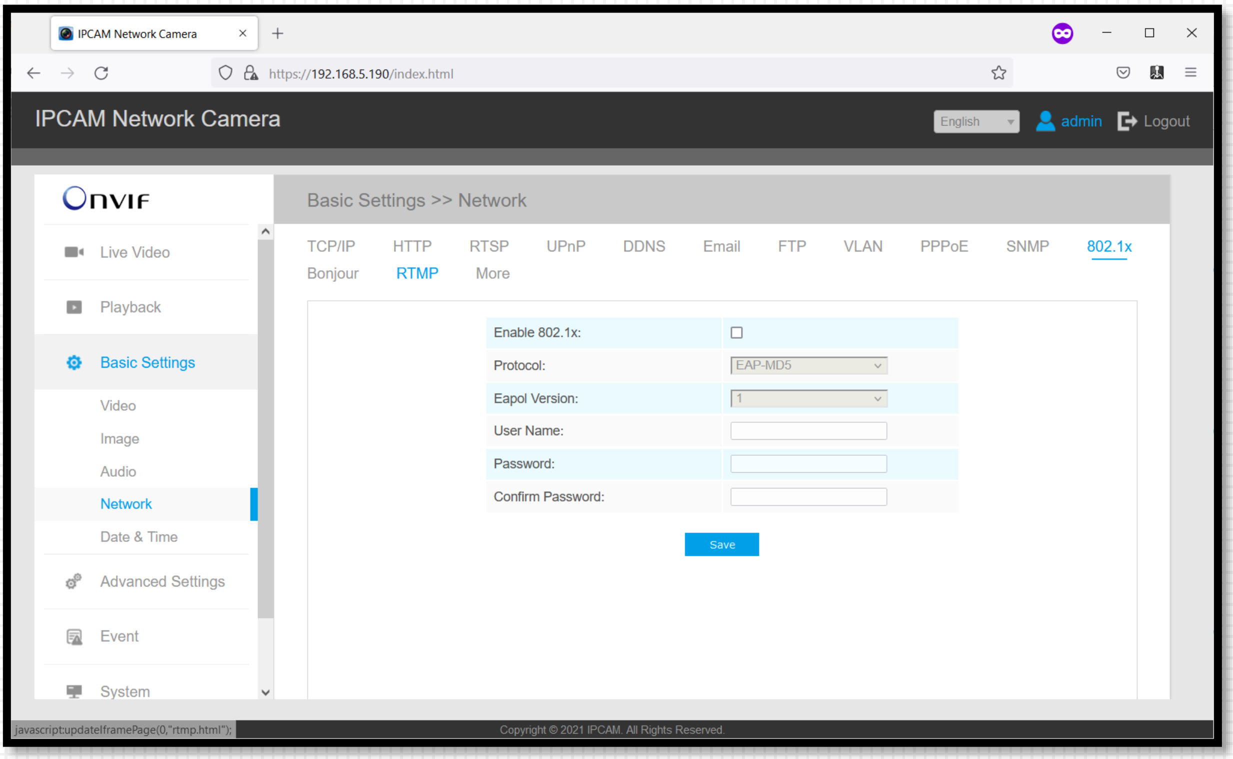
Save

Summary: **This Device meets the section requirements.**

3.9 Encryption Standards

This Device supports several encryption methods. Most of them are disabled by default settings.

Upon startup of the Device, User must ensure that at least one of the supported methods is selected and enabled.

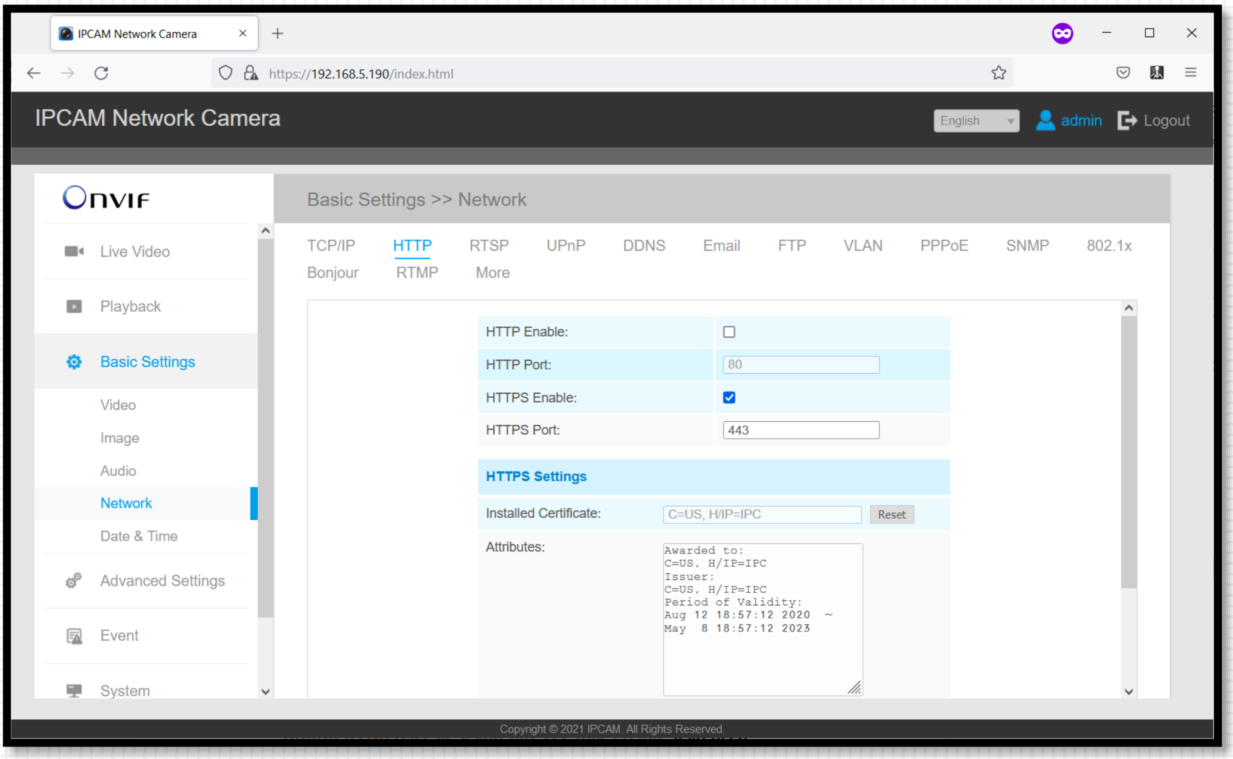


Enable 802.1x:	□
Protocol:	EAP-MD5
Eapol Version:	1
User Name:	
Password:	
Confirm Password:	

Summary: **This Device meets the section requirements. (Upon User fulfillment of required setup procedure before use).**

3.10 Firewall

The Device contains a firewall system that blocks access to unauthorized ports.



HTTP Enable:	☐
HTTP Port:	80
HTTPS Enable:	☑
HTTPS Port:	443

HTTPS Settings

Installed Certificate: C=US, H/IP=IPC

Attributes:

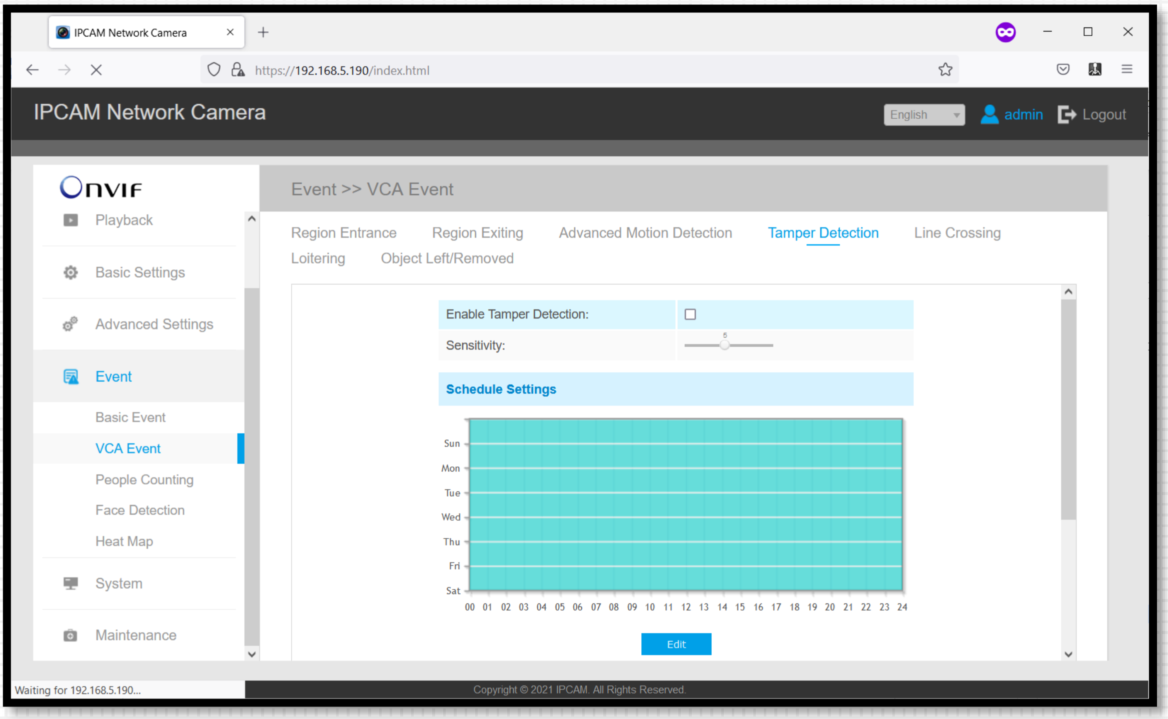
```
Awarded to:
C=US, H/IP=IPC
Issuer:
C=US, H/IP=IPC
Period of Validity:
Aug 12 18:57:12 2020  ~
May  8 18:57:12 2023
```

Summary: **This Device meets the section requirements.**

3.11 Tamper Detection

The Device contains a Tamper Detection system for damage detection.

This system is disabled by default settings.



IPCAM Network Camera

https://192.168.5.190/index.html

Event >> VCA Event

Enable Tamper Detection: □

Sensitivity: 5

Schedule Settings

Copyright © 2021 IPCAM. All Rights Reserved.

Summary: **This Device meets the section requirements. (Upon User completing required setup procedures and activation before use).**

בברכה,

יגאל גויטע,

מנכ"ל

סקדהסודו בע"מ.

משרד ייעוץ ותכנון פתרונות סייבר