iVMS-4200 Device Online Upgrading

User Instruction

Mar, 2018

COPYRIGHT © 2017 Hangzhou Hikvision Digital Technology Co., Ltd.

ALL RIGHTS RESERVED.

Any and all information, including, among others, wordings, pictures, graphs are the properties of Hangzhou Hikvision Digital Technology Co., Ltd. or its subsidiaries (hereinafter referred to as "Hikvision"). This user manual (hereinafter referred to be "the Manual") cannot be reproduced, changed, translated, or distributed, partially or wholly, by any means, without the prior written permission of Hikvision. Unless otherwise stipulated, Hikvision does not make any warranties, guarantees or representations, express or implied, regarding the Manual.

About This document

This document provides instructions for device online upgrading, and provides information on how to securely configure and use the device.

Contents

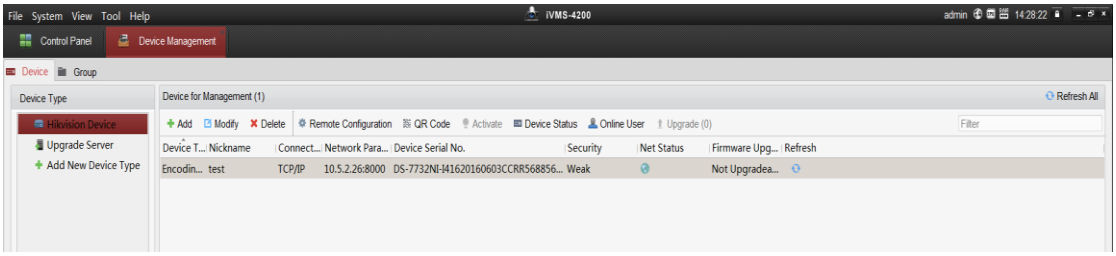
1 Summary

In order to assure the security of your devices in utmost and meet the best practices of information security requirement, we recommend that administrators should try to upgrade the device's firmware to the latest version. To facilitate the administrator to do so, we have added device online upgrading function into the surveillance client software iVMS-4200 V2.7.0.6. The Client will connect to upgrade server and detect the available firmware package automatically when connecting to the external network. Once matched, the upgrade package will be downloaded to the PC, and prompt the user to upgrade.

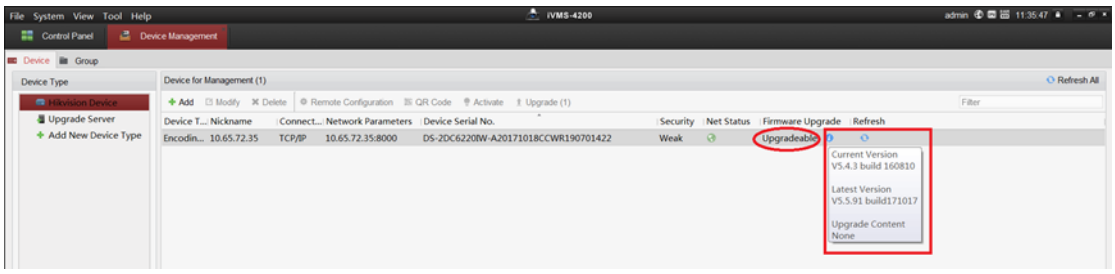
2 Operation Procedure

a) Install and Run IVMS-4200 v2.7.0.6. The Client is available from Hikvision official website, please click Here.

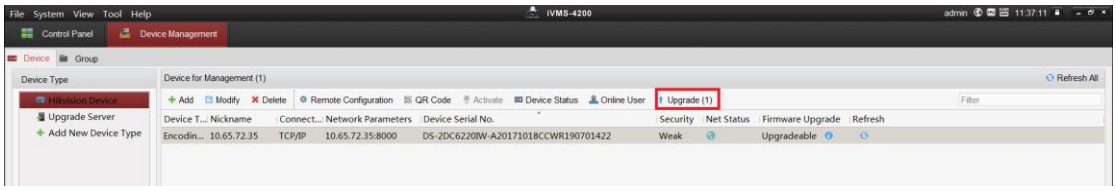
b) Add the device to the Client in Device Management module, and the device initial state is “Not Upgradeable”.



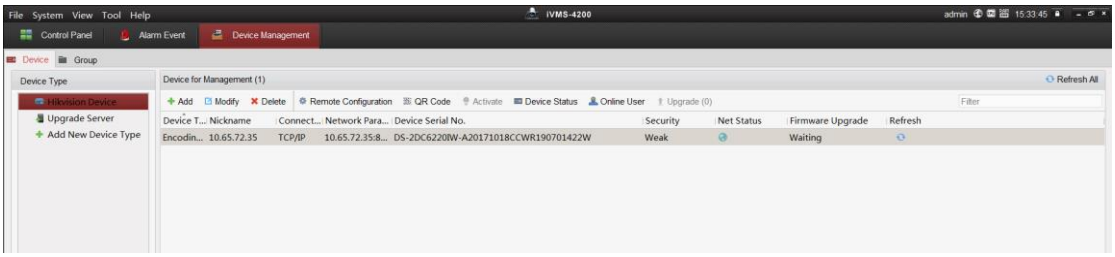
c) The Client detects the available firmware package automatically. If there is an available package on upgrading server, the client will download it to PC, and then prompt the user to upgrade. Meanwhile, the user can check the current firmware version and the latest version of the device.

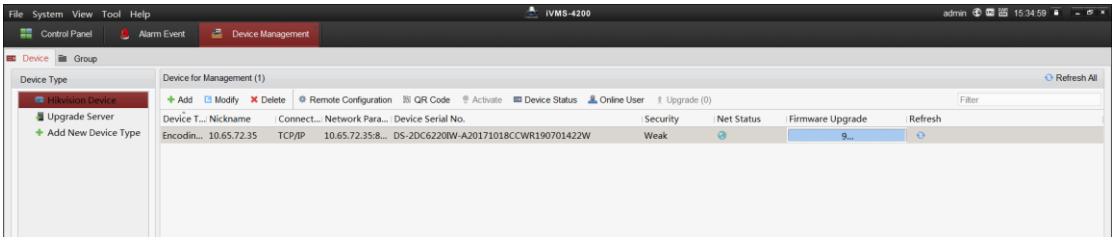


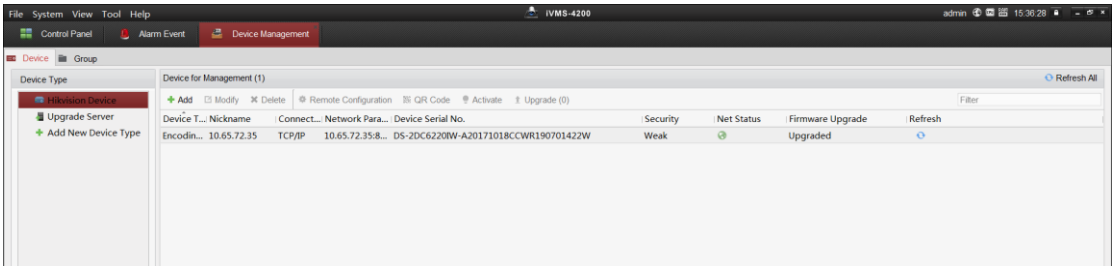
d) Choose the device prepared to be upgraded, and click “upgrade” to start.



e) The progress bar of the firmware upgrade allows you to view the real-time update progress. The upgrading status will initially be" waiting", and then shows the real-time percentage by progress bar. Once finished, the status will turn to be "upgraded".







3 Security Suggestion

Security management is an important element in product security. In order to achieve information security, we should not only conduct necessary security design to ensure the product security, but also pay high attention to security management. Therefore, the following security recommendations are made to maintain device security:

a) It is recommended that you do not disable the automatic upgrade function. You are advised to check whether there is new upgrade package or not. If there is a new upgrade package, upgrade it immediately to keep the latest version of the firmware of the device, so as to get the latest security patches.

b) It is recommended to set a strong password for the device to avoid the device being in a high-risk state due to the weak password.

c) It is recommended to make necessary security protection on the network edge of the video surveillance system, such as deploying a firewall.

4 Security Commitment

Hikvision is committed to using leading privacy and security technologies to help customers protect their personal information and to adopt a holistic approach to protect users' data.

Hikvision applies a unified integrated security infrastructure throughout the video IOT application ecosystem, and has a professional security team providing supports for all Hikvision products. They provide security audits and tests for developing and publishing products, and also provide security training and proactively monitors reports of new security issues and threats.