



Как активировать устройство

Краткое руководство

(Как активировать устройства HIKVISION IPC/DVR/NVR с повышенной безопасностью)

Ведущий инженер компании HIKVISION

Лео Тан

Версия: 1.01

2015-07

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 be “Hikvision”). This ‘How to activate device’ document (hereinafter referred to be “the Document”) 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 to the Document.

LEGAL DISCLAIMER

TO THE MAXIMUM EXTENT PERMITTED BY APPLICABLE LAW, THE PRODUCT DESCRIBED, WITH ITS HARDWARE, SOFTWARE AND FIRMWARE, IS PROVIDED “AS IS”, WITH ALL FAULTS AND ERRORS, AND HIKVISION MAKES NO WARRANTIES, EXPRESS OR IMPLIED, INCLUDING WITHOUT LIMITATION, MERCHANTABILITY, SATISFACTORY QUALITY, FITNESS FOR A PARTICULAR PURPOSE, AND NON-INFRINGEMENT OF THIRD PARTY. IN NO EVENT WILL HIKVISION, ITS DIRECTORS, OFFICERS, EMPLOYEES, OR AGENTS BE LIABLE TO YOU FOR ANY SPECIAL, CONSEQUENTIAL, INCIDENTAL, OR INDIRECT DAMAGES, INCLUDING, AMONG OTHERS, DAMAGES FOR LOSS OF BUSINESS PROFITS, BUSINESS INTERRUPTION, OR LOSS OF DATA OR DOCUMENTATION, IN CONNECTION WITH THE USE OF THIS PRODUCT, EVEN IF HIKVISION HAS BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES. REGARDING TO THE PRODUCT WITH INTERNET ACCESS, THE USE OF PRODUCT SHALL BE WHOLLY AT YOUR OWN RISKS. HIKVISION SHALL NOT TAKE ANY RESPONSIBILITIES FOR ABNORMAL OPERATION, PRIVACY LEAKAGE OR OTHER DAMAGES RESULTING FROM CYBER ATTACK, HACKER ATTACK, VIRUS INSPECTION, OR OTHER INTERNET SECURITY RISKS; HOWEVER, HIKVISION WILL PROVIDE TIMELY TECHNICAL SUPPORT IF REQUIRED. SURVEILLANCE LAWS VARY BY JURISDICTION. PLEASE CHECK ALL RELEVANT LAWS IN YOUR JURISDICTION BEFORE USING THIS PRODUCT IN ORDER TO ENSURE THAT YOUR USE CONFORMS THE APPLICABLE LAW. HIKVISION SHALL NOT BE LIABLE IN THE EVENT THAT THIS PRODUCT IS USED WITH ILLEGITIMATE PURPOSES. IN THE EVENT OF ANY CONFLICTS BETWEEN THIS DOCUMENT AND THE APPLICABLE LAW, THE LATER PREVAILS.



Содержание

Предисловие	3
Методы активации	4
Активация через Веб браузер.....	4
Активация через программу SADP	4
Активация через софт iVMS-4200	5
Активация камеры посредством видеорегистратора.....	6
Приложение	8
Подключение сторонних устройств	8
Правила создания пароля.....	8
Причины блокировки устройства.....	9



Предисловие

Все недавно изготовленные устройства HIKVISION (т.е., IP-камеры (IPC), поворотные камеры (PTZ), цифровые видеорегистраторы (DVR) и сетевые видеорегистраторы (NVR)) с последней прошивкой (IPC и PTZ версия V5.3.0, DVR / NVR версия V3.3.0) больше не используют пароль по умолчанию. При использовании этих устройств в первый раз, пользователю необходимо активировать устройство путем принудительной установки пароля. Уровень пароля должен быть намного выше, чем уровень пароля находящийся в группе "риска" (правила и уровень паролей будут описаны в приложении).

Примечание

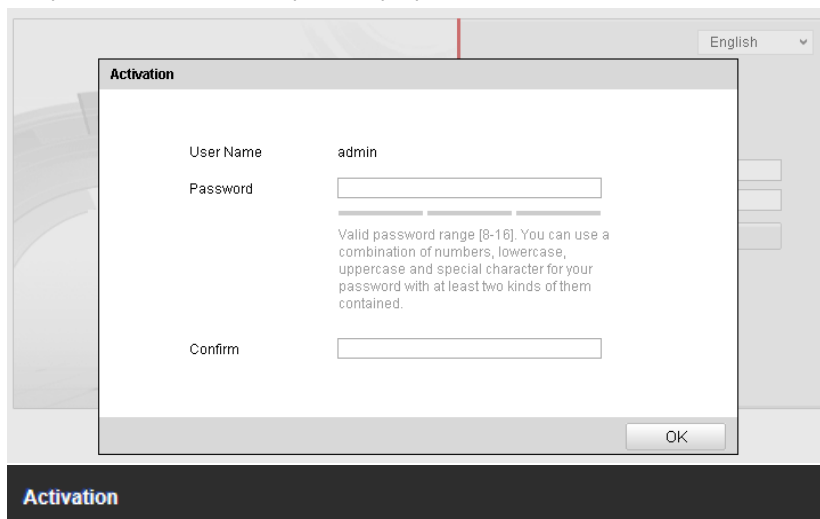
- 1. Если устройство со старой прошивкой использует пароль находящийся в группе "риска", то после обновления прошивки до версии V5.3.0, старое имя пользователя / пароль остается действителен и устройство не будет требовать активации. Тем не менее, устройство будет напоминать пользователю, что пароль находится в группе "риска";**
- 2. Если устройство сбросить на настройки по умолчанию, то после перезагрузки устройство будет в неактивном состоянии.**





Методы активации

Активация через Веб браузер:

Камеры с версией прошивки V5.3.0 и выше, также видеорегистраторы DVR/NVR с версией прошивки V3.3.0 и выше могут быть активированы в веб-браузере Internet Explorer (IE). Перед входом в устройство, пользователям необходимо установить пароль для входа и нажать кнопку **[OK]**, чтобы активировать устройство.



User Name	admin
Password	<input type="password"/> 
	 Strong
	Valid password range [8-16]. You can use a combination of numbers, lowercase, uppercase and special character for your password with at least two kinds of them contained.
Confirm	<input type="password"/>
	<input type="button" value="OK"/>

Интерфейс активации через веб-браузер IE

Активация через программу SADP:

Пользователи могут активировать устройства с новой прошивкой используя программу SADP. Для этой процедуры пользователям потребуется версия программы SADP не ниже V2.2.3.6.

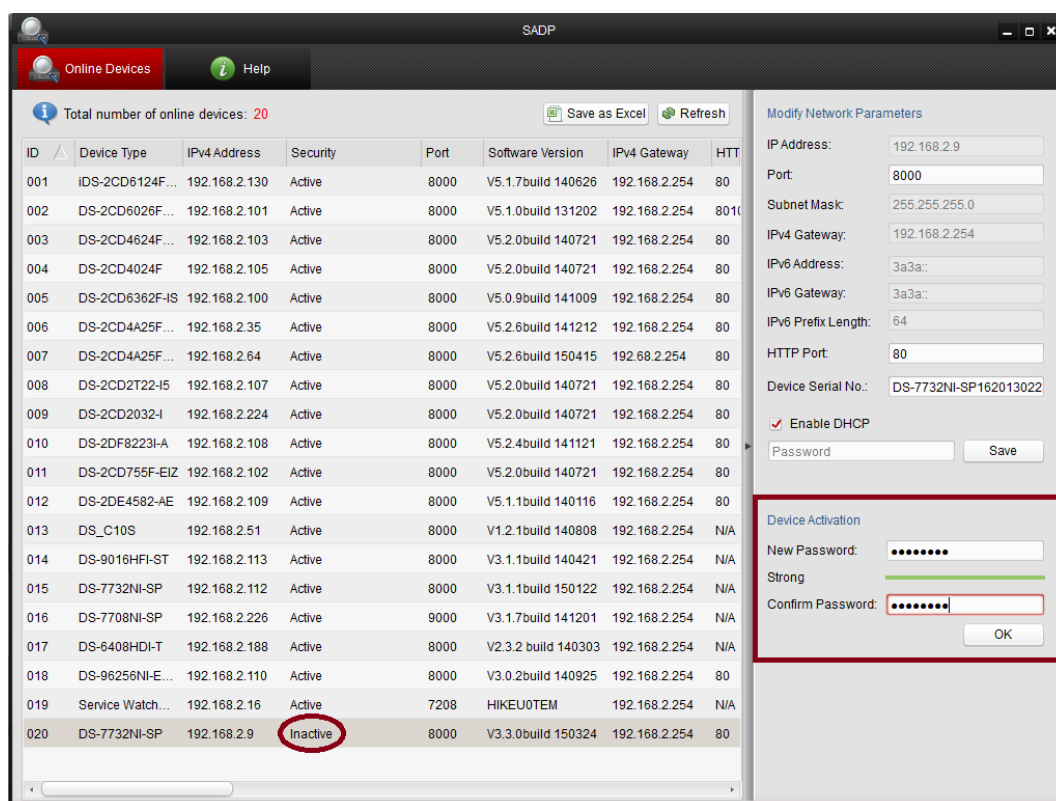




Версия программы SADP

Шаги по правильной активации устройства через программу SADP:

- Выбрать устройство, которое нужно активировать в списке "Онлайн устройств";
- Установить новый пароль в поле "Device Activation";
- Подтвердить новый пароль;
- Нажать на кнопку [OK], чтобы активировать устройство.



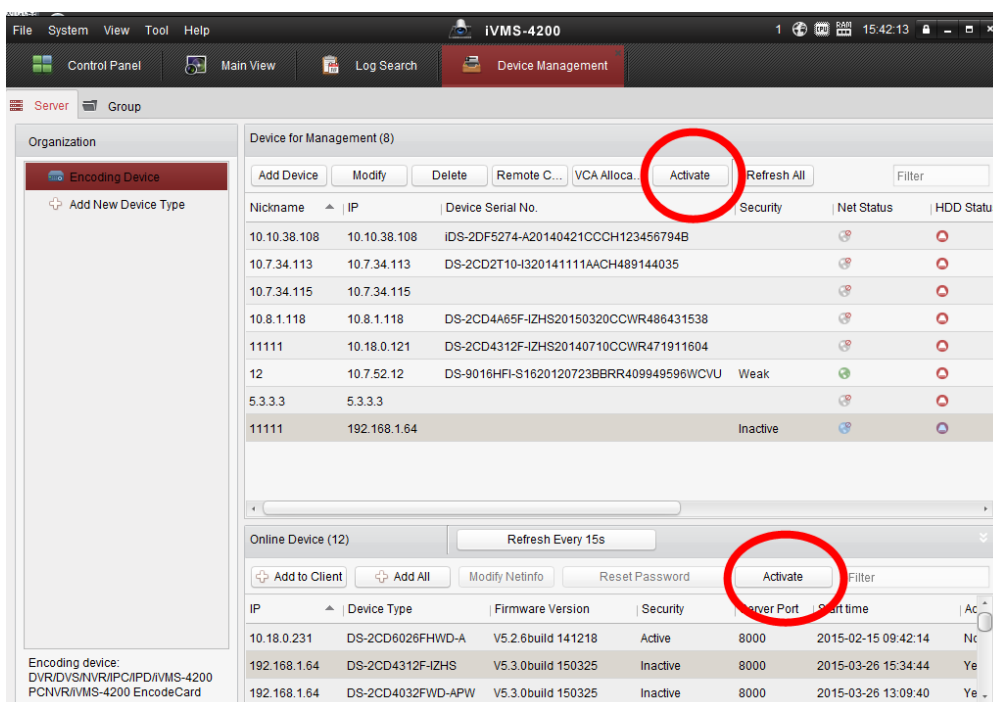
Интерфейс активации устройств в программе SADP

Активация через софт iVMS-4200:

Пользователи могут активировать устройства с новой прошивкой используя софт iVMS-4200. Для этой процедуры пользователям потребуется софт iVMS-4200 версии не ниже V2.3.1.3.



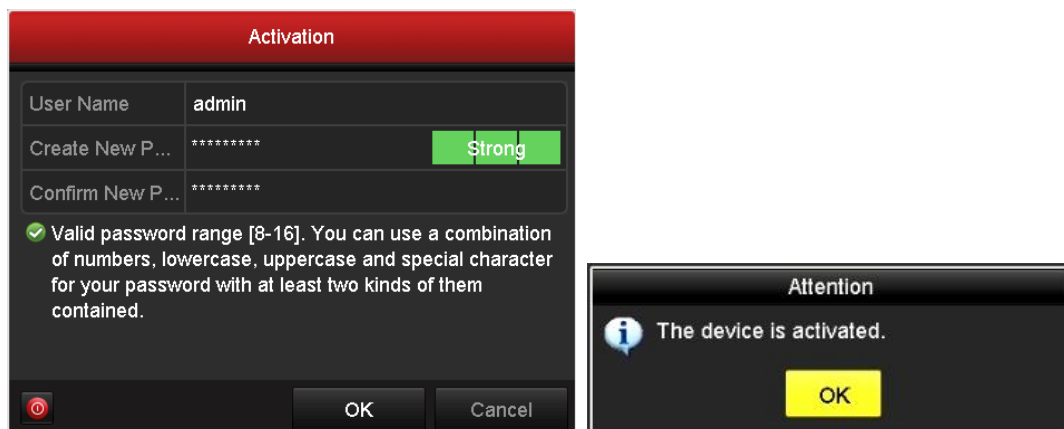
Версия iVMS-4200



Интерфейс активации устройств в iVMS-4200

Активация камеры посредством видеорегистратора

Видеорегистраторы с версией прошивки не ниже V3.3.0 могут активировать камеры, только при условии, если сам видеорегистратор уже был активирован.



Локальный интерфейс по активации видеорегастратора

Пользователи могут использовать видеорегастратор с версией прошивки не ниже V3.3.0, чтобы активировать камеры с версией прошивки V5.3.0 и выше. Имеются четыре способа:

- *Добавление в одно касание:* В интерфейсе устройства видеорегастратора, пользователи могут использовать "добавление в одно касание", чтобы добавить все камеры в локальной сети. Все добавленные камеры будут автоматически активированы с паролем как на видеорегастраторе;
- *Активация в одно касание:* В интерфейсе устройства видеорегастратора, пользователи могут активировать все камеры в локальной сети с использованием само-определенным паролем или с присваиванием пароля от видеорегастратора.
- *Ручное добавление '+':* Добавить вручную одну камеру с присваиванием пароля от видеорегастратора.
- *Plug & Play:* Подключить камеру к видеорегастратору через PoE интерфейс с присваиванием пароля от видеорегастратора.

Примечание:

1. Камера, которая была обновлена со старой прошивки (логин и пароль admin/12345) поддерживает Plug & Play нормально;
2. Перед подключением к видеорегастратору со старой прошивкой, неактивная камера обязательно должна сначала быть активирована.
3. PoE порт видеорегастратора со старой прошивкой не будет распознавать камеру с новой прошивкой. NVR необходимо обновить на самую новую прошивку.



Приложение

Подключение сторонних устройств

Подключение сторонних камер к видеорегистратору Hikvision:

Перед подключением сторонних камер к видеорегистратору HIKVISION, видеорегистратор обязательно сначала должен быть активирован.

Подключение HIKVISION камер к сторонним видеорегистраторам:

HIKVISION камеру сначала необходимо активировать, а после камеру можно добавить к стороннему видеорегистратору.

Сторонняя VMS платформа:

HIKVISION устройства должны быть активированы перед подключением. Также мы можем предоставить интерфейс SDK и протокол ISAPI для интеграции.

Правила создания пароля

Оценка уровня пароля

Есть четыре вида символов, которые могут быть использованы: цифры/заглавные(большие) английские буквы/строчные(маленькие) английские буквы/специальные символы

- Уровень 0 (группа "риска"): Длина пароля менее 8 символов, пароль состоит только из одного вида символов, пароль такой же как и логин, пароль зеркальное написание имя пользователя. Пример паролей из группы "риска": 12345, ABCDEFGH и т.д.
- Уровень 1 (слабый): Пароль содержит два вида символов. Комбинация пароля состоит из цифр + строчных букв или цифр + заглавных букв, длина пароля должна быть не меньше 8 символов. Пример: 12345abc, 12345ABC и т.д.
- Уровень 2 (средний): Пароль содержит два вида символов. Комбинация: номер + специализированный символ, строчные буквы + специализированный символ или заглавные буквы + специализированный символ, длина пароля должна быть не меньше 8 символов. Пример: 1234567+, abcdefg/, GFEDCBA), ABCDEFGh, и т.д.
- Уровень 3 (безопасный): Пароль содержит более двух видов символов и длина пароля должна быть не менее 8 символов. Пример: 1234abc + и т.д.

Примечание: Уровень пароля должен быть выше, чем уровень 0. Использование пароля из группы "риска" запрещено.



Причины блокировки устройства

Попытки входа:

Пользователь admin: разрешается 7 попыток ввода пароля

Прочие пользователи: разрешается 5 попыток ввода пароля

Если число ошибочных попыток превысит допустимое количество, то устройство будет заблокировано по текущему IP адресу или по пользователю.

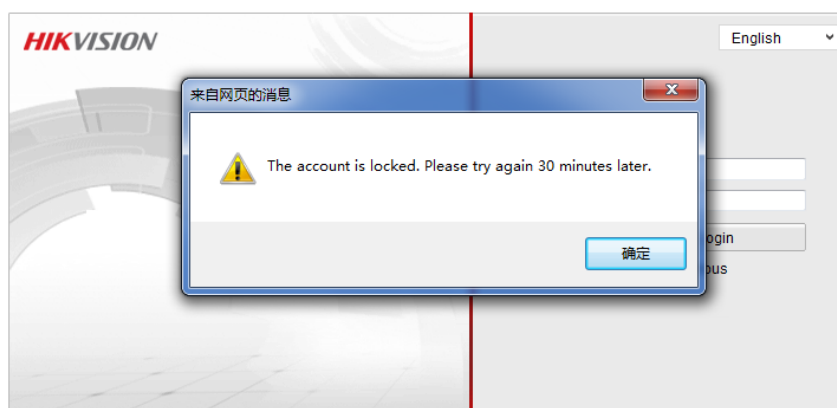
Продолжительность блокировки устройства:

Дистанционный вход: 30 минут (IP адрес клиента будет заблокирован)

Локальный вход: 1 минута (пользователь будет заблокирован);

Примечание:

1. Пользователи, которые уже зашли не будут заблокированы;
2. Пользователь Admin может быть разблокирован другим пользователем через SDK



IE интерфейс блокировки

