

| | | | | | |
|-----------------|-----------------------------|-----------------|--------|--------------|----------|
| Title: | How to Reset Password | Version: | v1.0 | Date: | 3/9/2017 |
| Product: | HIKVISION baseline products | Page: | 0 of 8 | | |

How to set a **STRONG** password

Introduction

HIKVISION products take password protection mechanism to protect customers' privacy. For IP cameras (IPC), PTZ cameras, digital video recorders (DVR) and network video recorders (NVR) with the latest firmware (IPC and PTZ from V5.3.0, DVR/NVR from V3.3.0) there would no default password. The previous user name/password would still be valid when some old devices with a week password upgrade to new firmware version. However, it will remind users that this is a 'weak' password.

When using the device for the first time, users need to activate the device through a compulsory password setting procedure. And the device would tell the password intensity according to the combination of number as well as letters you take.

We strongly recommend you set a **STRONG** password.

Different Methods to Set Password

HIKVISION different devices share different password setting strategies which provide customers with flexible choices.

At this stage you can set your password by **SADP tool**, **iVMS-4200 client**, or **NVR/DVR local GUI**, or you can set device password via **web browser**. No matter which method you take, there would always have a password intensity hint.

- **Using Web Browser:**

| | | | | | |
|-----------------|-----------------------------|-----------------|--------|--------------|----------|
| Title: | How to Reset Password | Version: | v1.0 | Date: | 3/9/2017 |
| Product: | HIKVISION baseline products | Page: | 1 of 8 | | |

- 1) Front-end device such as IPC (from V5.3.0) and back-end device such as NVR and DVR (from V3.3.0) can be activated by Internet Explorer (IE) or other web browser. Before logging into the device, users need to set a login password and click [OK] to proceed.
- 2) After device activation, we can also go to Configuration->System->User Management to change new device password.

Web browser Interface

● Using SADP Software:

- 1) Users can activate devices and set a password via SADP tool. For this procedure users will need version V3.0.0.100 (SADP).

Click here to download: http://overseas.hikvision.com/en/Tools_82.html



- 2) Just run SADP tool, find your device and check it, set a STRONG password for it and then confirm.



| | | | | | |
|-----------------|-----------------------------|-----------------|--------|--------------|----------|
| Title: | How to Reset Password | Version: | v1.0 | Date: | 3/9/2017 |
| Product: | HIKVISION baseline products | Page: | 2 of 8 | | |

Total number of online devices: 18

| ID | Device Type | Security | IPv4 Address | Port | Software Version | IPv4 Gateway | HTTP Port | Device Serial No. |
|-----|--------------------|----------|--------------|------|---------------------|--------------|-----------|-------------------|
| 002 | DS-M7508HNI/GW | Active | 10.5.2.201 | 8181 | V4.1.1build160803 | 10.5.2.254 | 90 | DS-M7508HNI/GW |
| 003 | DS-MP7504 | Active | 10.5.2.222 | 8000 | V4.0.3build160127 | 10.5.2.254 | 80 | DS-MP7504012016 |
| 004 | iDS-2CD6024FWD-A/F | Active | 192.0.0.3 | 8000 | V5.3.0build 1501... | 10.5.2.254 | 80 | iDS-2CD6024FWD |
| 005 | DS-6408HDI-T | Active | 10.5.2.234 | 8000 | V3.5.1 build 161... | 10.5.2.254 | 80 | DS-6408HDI-T012 |
| 006 | DS-7616HUHI-F2/N | Active | 10.5.2.20 | 8000 | V3.4.80build 161... | 10.5.2.254 | 80 | DS-7616HUHI-F2/N |
| 007 | Service WatchDog | Active | 10.5.2.220 | 7208 | 94CT7XFOLUQC... | 10.5.2.254 | N/A | |
| 008 | DS-2CD4585F-IZH | Active | 10.5.2.2 | 8000 | V5.4.0build 1604... | 10.5.2.254 | 80 | DS-2CD4585F-IZH |
| 009 | DS-2CD4032FWD-APW | Active | 192.0.0.5 | 8000 | V5.4.0build 1604... | 0.0.0.0 | 80 | DS-2CD4032FWD- |
| 010 | DS-2CD4535F-IZ | Active | 192.0.0.7 | 8102 | V5.4.0build 1604... | 0.0.0.0 | 91 | DS-2CD4535F-IZ2 |
| 011 | DS-2CD2142FWD-IWS | Active | 10.5.2.202 | 8180 | V5.4.1build 1605... | 10.5.2.254 | 89 | DS-2CD2142FWD-I |
| 012 | DS-2CD2512F-IS | Active | 192.0.0.6 | 8189 | V5.3.0Pbuild 1... | 10.5.2.254 | 96 | DS-2CD2512F-IS2 |
| 013 | DS-TCP335 | Active | 10.5.2.116 | 8000 | V5.2.1build 1606... | 10.5.2.254 | 80 | DS-TCP335201610 |
| 014 | DS-9616NI-ST | Inactive | 192.0.0.64 | 8000 | V3.4.3build 1608... | 0.0.0.0 | 80 | DS-9616NI-ST162 |
| 015 | | Inactive | 192.0.0.2 | 8000 | V5.4.0build 1608... | 10.5.2.254 | 80 | 20141202CCCH123 |
| 016 | DS-2CD2120F-I | Active | 192.0.0.8 | 8103 | V5.4.3build 1607... | 0.0.0.0 | 92 | DS-2CD2120F-I201 |
| 017 | iVMS_6200_SMD | Active | 10.5.2.104 | 8000 | V2.3.0 build 150... | 10.5.2.254 | N/A | iVMS-6200SMD750 |
| 018 | DS-2CD4A25FWD-IZ | Active | 192.0.0.4 | 8000 | V5.3.6build 1512... | 10.5.2.254 | 80 | DS-2CD4A25FWD- |

The device is not activated.

You can modify the network parameters after the device activation.

Activate Now

New Password:

Strong

Confirm Password:

Activate

SADP Interface

● Using iVMS-4200 Software:

- 1) Users can activate devices and set device password via iVMS-4200 Software as well. For this procedure users will need version V2.5.1.7 (iVMS-4200).

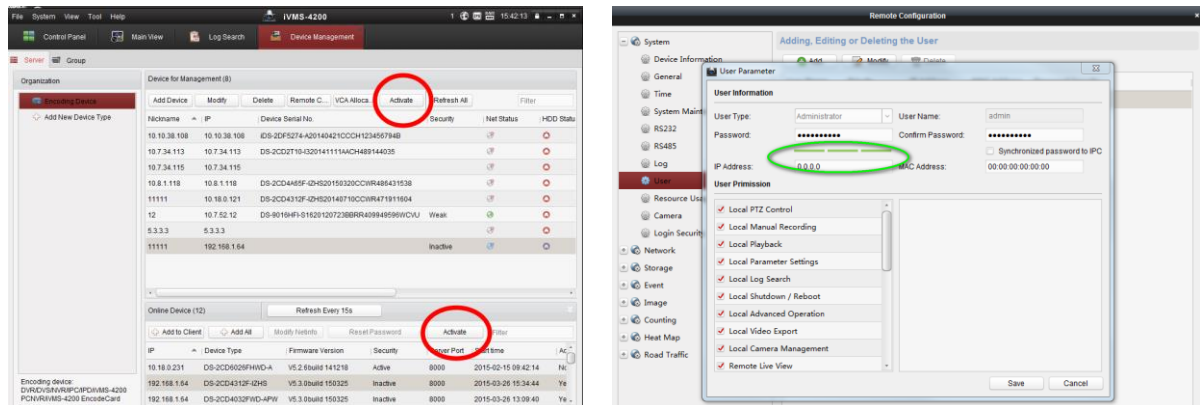
Click here to download: http://overseas.hikvision.com/en/Tools_84.html



iVMS-4200 Software Version

| | | | | | |
|-----------------|-----------------------------|-----------------|--------|--------------|----------|
| Title: | How to Reset Password | Version: | v1.0 | Date: | 3/9/2017 |
| Product: | HIKVISION baseline products | Page: | 3 of 8 | | |

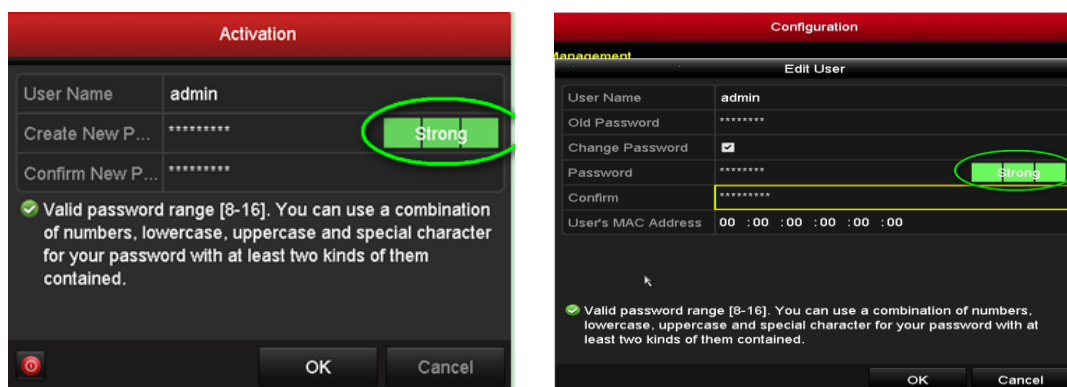
- 2) After device activation, we can also go to Remote Configuration->System->User to change new device password.




iVMS-4200 Interface

● Front-End Device Activation by Back-End Device

A back-end device (from V3.3.0) can activate a front-end device (from V5.3.0) and set a password there, only if the back-end device has already been activated.



Back-End Device Local Interface

Find your camera then click **Manual Activation** , and then you can activate one front-end device manually with the self-defined passwords or back-end device password.





Back-End Device Local Interface for activating Front-End Device

The other ways to activate IPC are:

1. **One-touch adding:** In the back-end device interface, users can use ‘One-touch adding’ to add all front-end devices on the LAN. At the same time, the devices will be automatically activated with the back-end device password.
2. **One-touch activation:** In back-end device interface, users can activate all front-end devices in LAN with the self-defined passwords or back-end device password;
3. **Manual addition ‘+’:** Add one front-end device manually with the back-end device password;
4. **Plug & Play:** Connect a front-end device to a back-end device’s PoE interface with the back-end device password.

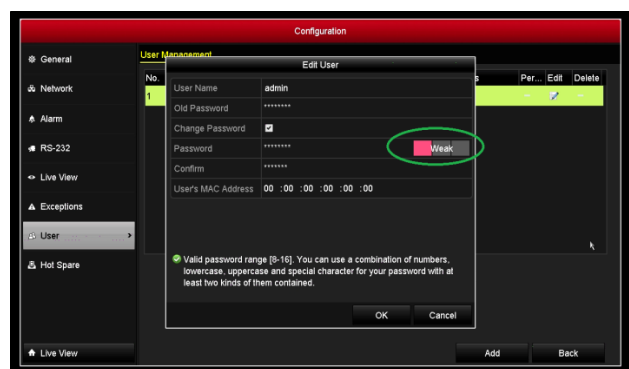
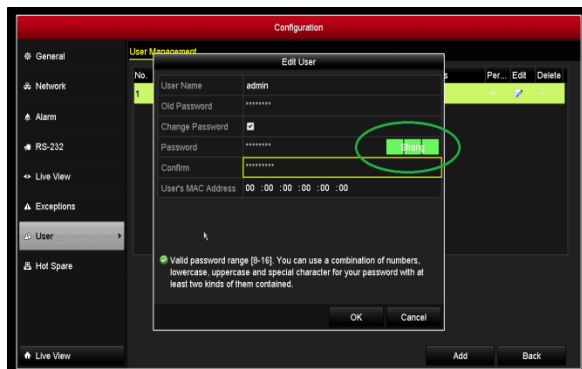
NOTES:

The method of activating front-end devices by back-end device is highly recommended.

Password intensity

No matter which methods you take, it would always tell you the password intensity according to the combination of number and letters you take. Below is a comparison of strong password and week password.

| | | | | | |
|-----------------|-----------------------------|-----------------|--------|--------------|----------|
| Title: | How to Reset Password | Version: | v1.0 | Date: | 3/9/2017 |
| Product: | HIKVISION baseline products | Page: | 5 of 8 | | |



Appendix

Password Rules

Password Level Judgment

There are four kinds of characters that can be used for password: numbers/uppercase letters/lowercase letters/ special characters:

- Level 0: Password length is fewer than eight characters; password contains one kind of character; password is the same as user name; password is the mirror writing of user name. (Example: 12345, abcdefgh)
- Level 1 (weak): Password contains two kinds of characters. The combination is number + lowercase letter or number + uppercase letter, and the password length must be no fewer than eight characters. (Example: 12345abc, 12345ABC)
- Level 2 (medium): Password contains two kinds of characters. The combination is NEITHER number + lowercase letter NOR number + uppercase letter, and the password length must be no less than eight characters. (Example: 1234567+, abcdefg/, GFEDCBA), ABCDEFGh,)
- Level 3 (strong): Password contains more than two kinds of characters and the password length must be no less than eight characters. (Example: 1234abc+)

NOTE:

Password level should be higher than 0.



| | | | | | |
|-----------------|-----------------------------|-----------------|--------|--------------|----------|
| Title: | How to Reset Password | Version: | v1.0 | Date: | 3/9/2017 |
| Product: | HIKVISION baseline products | Page: | 6 of 8 | | |

Lockout Rules

Login Attempts:

Admin Account: 7 password input attempts are allowed

Other Account: 5 password input attempts are allowed

After login error attempts reach the limitation, the device will lock the current IP or account;

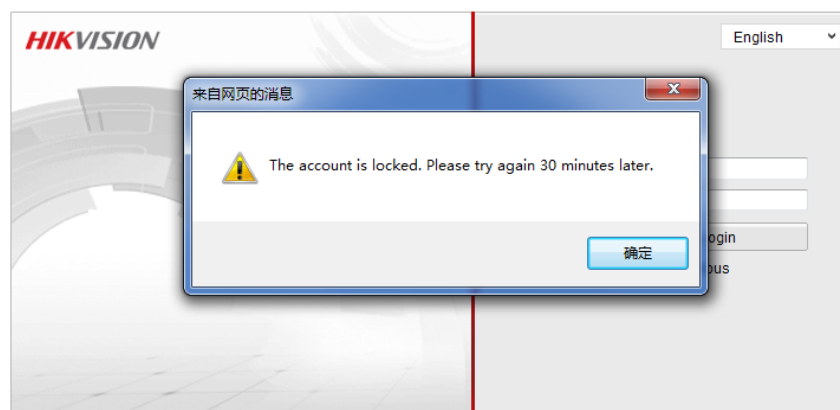
Device Lockout Duration:

Remote login: 30 minutes (the client's IP will be locked)

Local login: 1 minutes (the account will be locked);

NOTES:

1. Users who have already logged in will not be locked out;
2. Admin account can unlock the other accounts by SDK



IE Lockout Interface

Downloading Sites:

SADP Tool: http://overseas.hikvision.com/en/tools_82.html

iVMS-4200 client: http://overseas.hikvision.com/en/Tools_84.html



| | | | | | |
|-----------------|-----------------------------|-----------------|--------|--------------|----------|
| Title: | How to Reset Password | Version: | v1.0 | Date: | 3/9/2017 |
| Product: | HIKVISION baseline products | Page: | 7 of 8 | | |



First Choice for Security Professionals

***HIKVISION* Technical Support**

