HIKVISION USA

How to Reset Passwords Quick Guide

(New Secure Password Reset Strategy)

7/15

www.hikvision.com

Introduction

To reset passwords with the new Hikvision Secure Password Strategy, you must use SADP Tools software (*v2.2.3.5 Build 20150408*) or later (Figure 1). It can be downloaded from our website at www.hikvision.com. It can be used on front-end and back-end devices with firmware shown in the following table:

Device Firmware with Secure Activation

Device Type	Model Number	Firmware Version
Value Series IP Camera	DS-2CD2xxx	V5.3.0
Smart Series IP Camera	DS-2CD4xxx	V5.3.0
NVR/Hybrid	DS-9016HWI-ST DS-96xxNI-ST DS-7716NI-SP/16	V3.1.5
Plug-n-Play NVR	DS-76xxNI-EI(E2)/P	V3.1.0
Turbo DVR	DS-72xxHGHI-SH DS-73xxHQHI-SH	V3.1.6
Super NVR	DS-96128NI-E24/H DS-96256NI-E24/H	TBD

Figure 1 You need to download a new version of the SADP Tool software (v2.2.3.5 Build 20150408)

NOTE: Once you update your DVR/NVR or camera firmware, it ***cannot*** be downgraded to a previous version; the upgrade ***is not*** reversible.

By using the new SADP Tool you can determine if the front-end device is using **OLD** or **NEW** firmware. If your device has old firmware v3.1.0 (Figure 2), you'll need to reset the password by using the old procedure. With the new firmware v3.3.0 (Figure 3), the default username and password (*admin, 12345*) are no longer applicable. The user will be prompted to assign a new password during the initial password reset attempt.

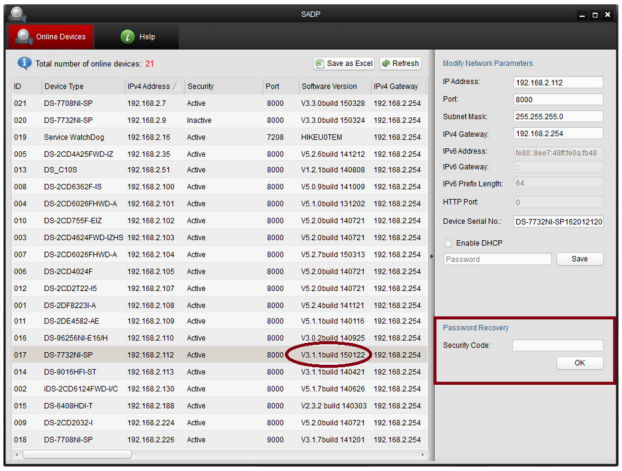

Figure 2 New SADP Tool lets you determine if front-end device is using OLD firmware (V3.1.1build 150122 shown)…

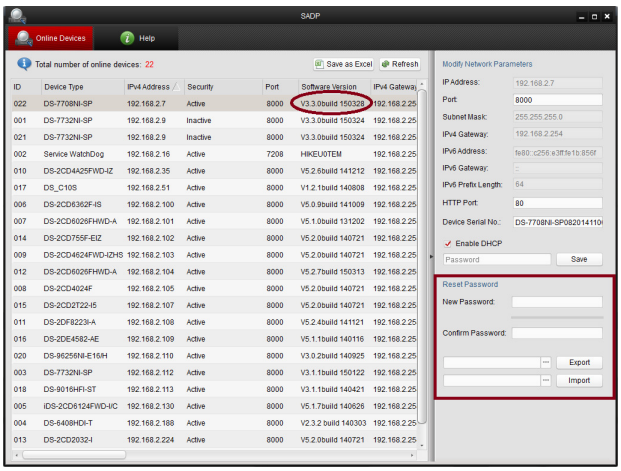

Figure 3…or NEW firmware (V3.3.0build 150328 shown)

Resetting Password

1. To request a password reset code, create a folder on your PC (Figure 4) into which to export the *.XML file.

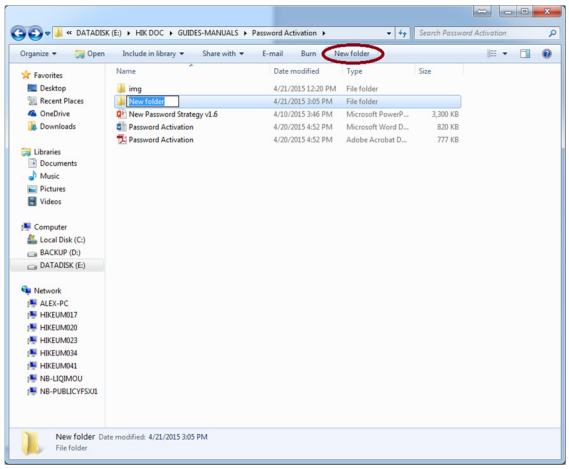

Figure 4 Create a new folder into which to export the *.XML file

2. Open the SADP Tool and highlight the device for which you need a recovery code. Click the **[Browse]** (…) button (Figure 5).

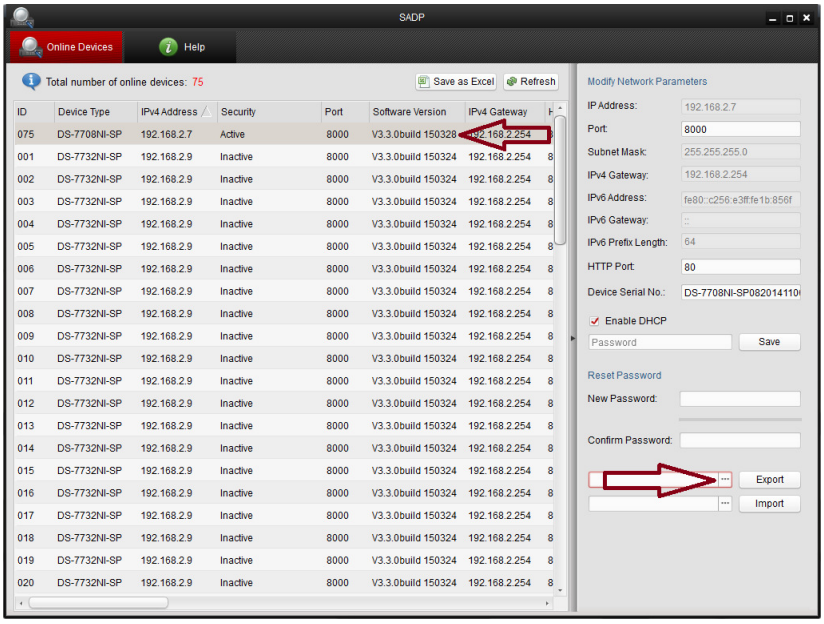

Figure 5 Click the **[Browse]** (…) button

3. Select the directory path to the folder you've created and click **[Choose]** (Figure 6).

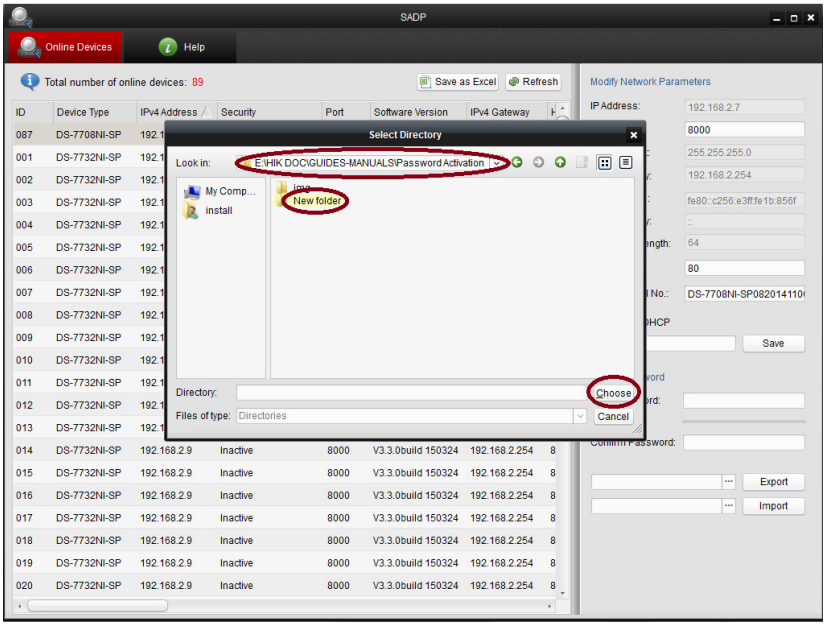

Figure 6 Select directory path and click **[Choose]**

4. Click **[Export]** (Figure 7) and a file named "*DeviceKey.xml*" will be generated.

5. Send this "DeviceKey.xml" file to helpdesk.usa@hikvision.com as an e-mail attachment.

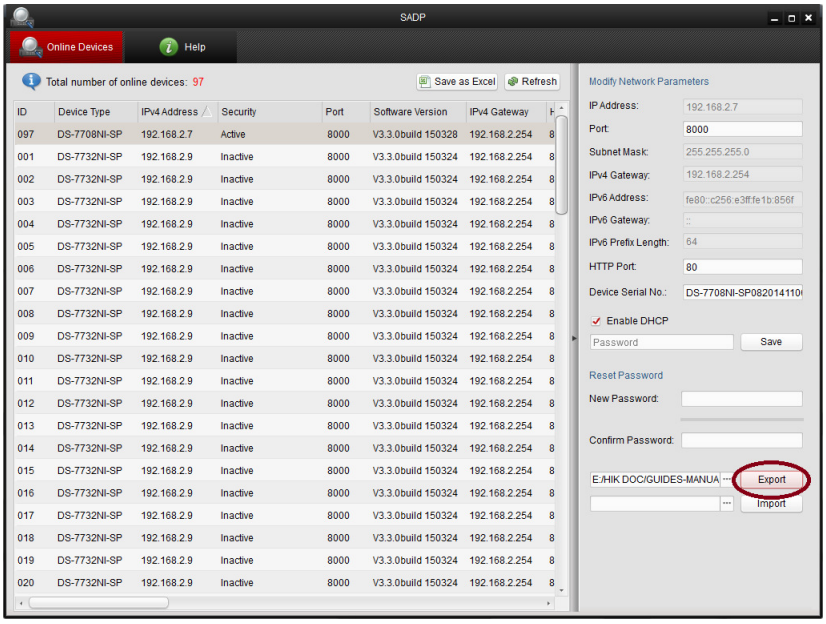

Figure 7 Click **[Export]** and a file named "*DeviceKey.xml*" will be generated

6. Once you send the "*DeviceKey.xml*" file, you'll receive an encrypted file named '*Encrypt.xml*' back via e-mail in approximately 24 hours. Save this file in the same folder you've previously saved the "*DeviceKey.xml*" (Figure 8). You'll need the path to import the encrypted key later on.

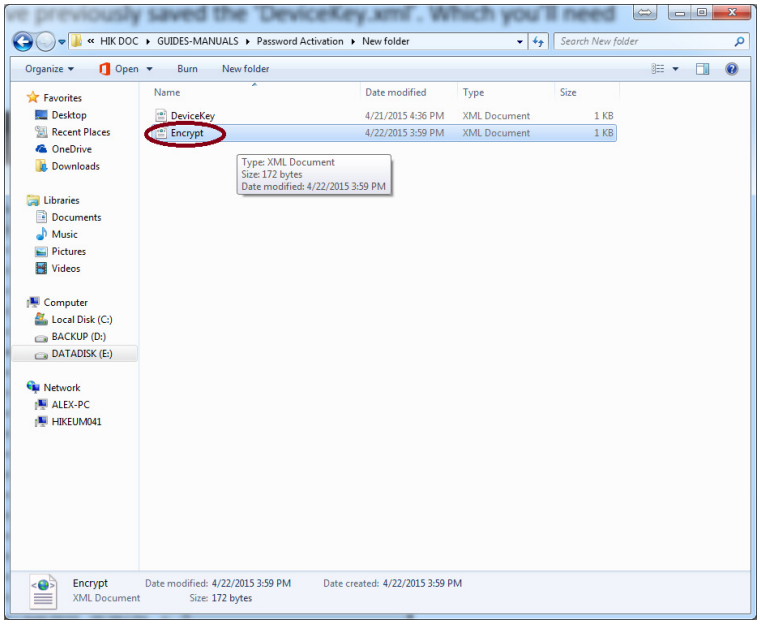

Figure 8 Save this file in same folder where you've saved "*DeviceKey.xml*"

7. In the SADP Tool, highlight the device again, click **[Browse]** (…), and select the path where you saved the "*Encrypt.xml*" file (Figure 9).

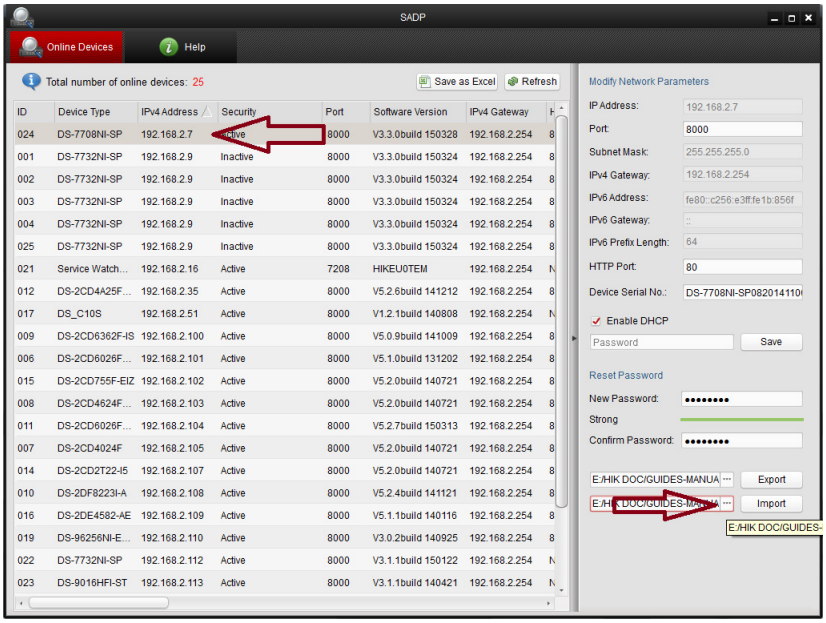

Figure 9 Select device again and click [*Browse*] to locate the path where you saved the "*Encrypt.xml*" file

8. Create a password of your choice by entering a new password into the "New Password" field on the bottom right of the screen (Figure 10). See "Reference" section on page 8 for guidelines.

9. Retype the password into the "Confirm Password" field.

10. After the password has been entered and confirmed, click **[Import]** (Figure 10) to import the "*Encrypt.xml*" file you received and saved from Hikvision Technical Support.

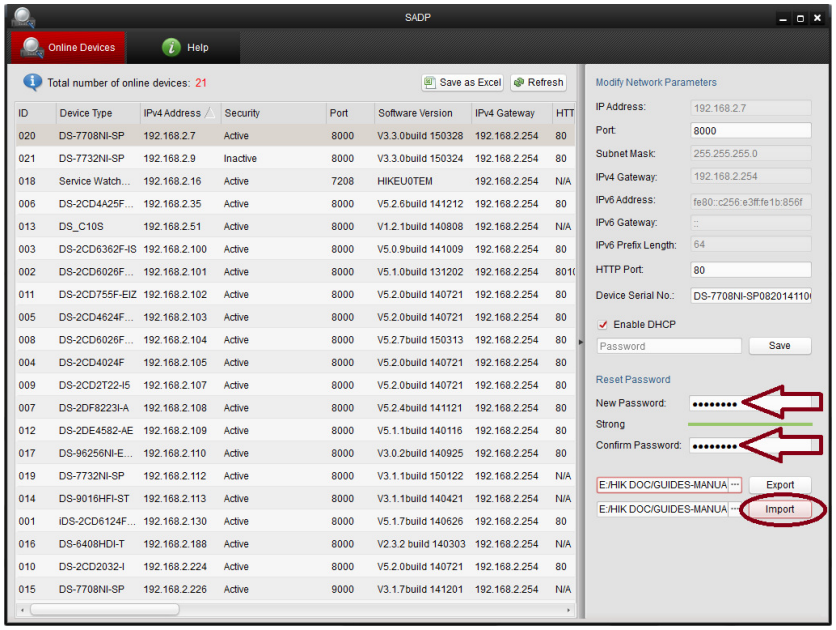

Figure 10 Set up a password by clicking **[New Password]** and **[Confirm Password]**, then click **[Import]**

11. A "Reset password succeed" message will appear (Figure 11).

12. Press the "X" in the top right corner of the pop-up confirmation window to dismiss the window.

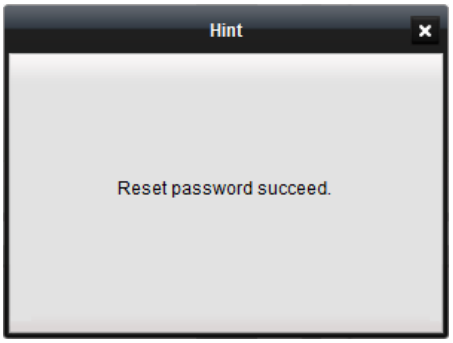

Figure 11 "*Reset password succeed*" message will appear

Reference

Password Strength Requirements

Hikvision's new login procedure requires users to create a new password for the **admin** account upon the first login to all devices. The password must contain 8 to 16 characters, combining numbers, lowercase letters, uppercase letters, and special characters. At least two types of the above-mentioned characters are required. The system will check the password strength; "Risky" passwords will not be accepted.

NOTE: Technical bulletins are available to explain password strength requirements in detail.

- The password strength will be displayed, accompanied by a color indicator*:
  - Level 0–*Risky* (no indicator): Not acceptable
  - Level 1–*Weak* (pink indicator): Acceptable
  - Level 2–*Medium* (yellow indicator): Acceptable
  - Level 3–*Strong* (green indicator): Acceptable
- Bar length indicates strength level.
- Activation will not be allowed unless the password is of acceptable strength ("Weak," "Medium," or "Strong,"). If the password is of unacceptable strength ("Risky,"), a warning box will be displayed.

Password Strength Levels

STRENGTH LEVEL	DESCRIPTION
Level 0 (Risky) Cameras ***will not*** accept a Level 0 password	Password length is fewer than eight characters, contains only one type of character, is the same as the user name, and/or is the mirror writing of the user name. This type of password ***will not*** be accepted.
Level 1 (Weak) Cameras ***will*** accept a Level 1 password	Password contains two types of characters. The combination is number + lowercase letter or number + uppercase letter, and the password length is at least eight characters. This type of password ***will*** be accepted.
Level 2 (Medium) Cameras ***will*** accept a Level 2 password	Password contains two types of characters. The combination is **neither** number + lowercase letter *nor* number + uppercase letter, and the password length is at least eight characters. This type of password ***will*** be accepted.
Level 3 (Strong) Cameras ***will*** accept a Level 3 password	Password contains more than three types of characters, and the password length is at least eight characters. This type of password ***will*** be accepted.

NOTE: Types of characters are lowercase letters, uppercase letters, numbers, and special characters. Only ASCII characters are allowed.

*__NOTE:__ The strength level indicator colors can vary by activation process, model number, and device type.