SONY®

Network Video Management System

Enterprise Edition

Device Pack

Release Note

Software Version:

Regular 9.8a

Legacy 1.0a

Revision 1 (Last Modified: September 30, 2018)

© 2018 Sony Corporation

Revision History

Revision	Date	Description
Revision 1	September 30, 2018	First release (Regular 9.8a + Legacy 1.0a)

Index

1 IP Camera and Video Server Compatibility Overview

This release note lists the changes in Device Pack 9.8a that are supported in the following systems:

- Network VMS Enterprise Edition   version 2016-2018

2 Device Pack changes

Legacy Device Pack:

Device drivers are now split into two device packs: the regular device pack with newer drivers and the legacy device pack with older drivers. You need to install both the legacy device pack and the regular device pack to enable full support for hardware devices on Network VMS. The legacy device pack is a separate installer and not included in a Network VMS installer.

Regular Device Pack updates:

- Added support for Sony's new devices and/or firmware. Refer to the NVMS Supported Device List. For details, visit
  `https://www.sony.net/Products/CameraSystem/NVMS/technical_doc/`
- New firmware support for devices for the following partners:
  Sony, Bosch, Axis, Canon, Edesix Ltd., Hanwha Techwin, Mobotix, Pelco, Siqura, Vivotek, Zepcam
- Additional support for specific features for the following partners and drivers:
  - ✓ Added support for corridor mode for Bosch.
  - ✓ Added support for SD-card events for Bosch
  - ✓ Added support for SRTP (unicast and multicast) for Axis
  - ✓ Added support for analytics events for Mobotix and Siqura
  - ✓ Added support for audio on edge for the ONVIF multichannel driver
  - ✓ Align Device Pack Dependency Versions (CorePlatform, gSoap, OpenSSL)
  - ✓ Fixed ONVIF driver crashes related to customer cases

New device support for:

3S Pocketnet Technology Inc.

N3011-E, N6033-E, N6047-EC, N1011-C, N9031-C & N3072-EC

American Dynamics
Illustra Pro 2MP PTZ 30x outdoor, Illustra Pro 2MP PTZ 30x indoor, Illustra Pro Feature Plus 2MP PTZ 30x outdoor, Illustra Pro Feature Plus 2MP PTZ 30x indoor & Illustra Pro 12MP Fisheye

Axis
P1280-E, Q6125-LE, M3058-PLVE, M3057-PLVE & C8033

Dahua
DHI-NVS0104HDC, DHI-NVS0204HDC, DHI-NVS0404HDC, DH-XVR4108C-X, DH-XVR4108HS-X, DHXVR4116HS-X, DH-XVR4216AN-X, DH-XVR5104C-X, DH-XVR5108C-X, DH-XVR5104H-X, DH-XVR5108H-X, DH-XVR5104HE-X, DH-XVR5108HE-X, DH-XVR5104HS-X, DH-XVR5108HS-X, DH-XVR5104C-4KL-X, DHXVR5104H-4KL-X, DH-XVR5104HS-4KL-X, DH-XVR7104HE-4KL-X, DH-XVR5108H-4KL-X, DH-XVR5108HS-4KL-X, DH-XVR5116H-X, DH-XVR5116HE-X, DH-XVR5116HS-X, DH-XVR5208AN-4KL-X, DH-XVR5216A-X, DHXVR5216AN-X, DH-XVR7104E-4KL-B-X, DH-XVR7104E-4KL-X, DH-XVR7108E-4KL-B-X, DH-XVR7108E-4KL-X, DH-XVR7108HE-4KL-X, DH-XVR7208A-4KL-X, DH-XVR5116H-4KL-X, DH-XVR5216AN-4KL-X, DH-XVR7108HE-4K-X, DH-XVR7116HE-4KL-X, DH-XVR7208A-4K-X & DH-XVR7216A-4KL-X

D-Link
DCS-6517B, DCS-7517B, DCS-4633EV & DCS-4605EV

Hanwha Techwin
QNB-6000, QNB-7000, LND-6010R, LND-6020R, LND-6030R, LND-6070R, LNV-6010R, LNV-6020R, LNV-6030R, LNV-6070R, LNO-6010R, LNO-6020R, LNO-6030R, LNO-6070R, XNP-6371RH, PNM-7000VD, QNP-6230/H, QNP-6320, TNO-4030T, TNO-4040T, TNO-4041T, TNO-4050T & TNO-4051T

Hikvision
DS-2CD451MF-IZ, DS-2CD453MF-IZ & DS-2CD455MF-IZ

Honeywell

HMBL8GR1, HM4L8GR1, HCL2GV, HBL2GR1V, H4L2GR1V, HCW2GV, H3W2GR1V, H3W4GR1V, H4W2GR1V, H4W4GR1V, HBW2GR1V, HBW2GR3V & H2W2GR1

Interlogix
TVC-5401, TVC-5402, TVC-5403, TVB-5401, TVB-5402, TVB-5403, TVB-5404, TVB-5405, TVD-5401, TVD-5402, TVD-5403, TVD-5404, TVD-5405, TVD-5406, TVD-5407, TVD-5408, TVB-5501, TVB-5502, TVD-5501, TVD-5502, TVT-5501 & TVT-5502

Panasonic
WV-S2250L, WV-S2550L & WV-S1550L

Pelco
S6230-EG0

Siqura
BC820v2H3, HSD820v2H3-E, HSD820v2H3-I & HSD820v2H3PRH

Uniview
IPC6222ER-X30P-B

Vivotek
IP9191-HP, IP9165-HP, IP9165-LPC, IP9167-HP, IP9167-HT, FD9391-EHTV, IB9391-EHT, FD8365-HTV-v2 & IB8365-HT-v2

Replace Hardware Remarks:

Be aware that after using Replace Hardware and changing the license, the license should always be checked to verify that it is activated.

4K Remarks:

Due to the nature of 4K and the high resolution at high frame rates, this will increase the demand for high performing network, CPU, graphic adaptors and monitors. Unless all components in the hardware infrastructure is prepared for a high load, there might be limitations seen as latency, stutter etc.
4K - Recommended Network VMS version 2016 or newer, supporting HW accelerated

decoding using the GPU

Axis Remarks:

The Axis M, P and Q drivers (except P8221) have been replaced with four new dynamic drivers that also supports the new Axis Events handling. This means that all new devices added to a system will automatically be detected on one of the new drivers.

Note: If your devices are using firmware 5.20 or lower then Events and I/O will not work with the new drivers. You should either upgrade to a newer firmware or manually select the driver to add the device. Be aware if you add the device manually and later upgrade the firmware you will need to do a Replace Hardware to change to the new driver.

Note: Before Replacing Hardware to only change the driver and not the hardware please contact Support on how to do this correctly.

AVHS: Due to a limitation in the firmwares only 9 socket connections can be open on an AVHS device at any time. JPEG video streams, Audio In streams, Audio Out and Output streams use 1 socket connection each. H.264 video streams, Events, Inputs and Edge Storage use 2 connections each. This also means that when upgrading from a previous Device Pack to 7.3 all Channels should be disabled before the upgrade.

AVHS: Audio Out does not work properly with firmwares before 5.50 when running the 2013 or older versions. To get Audio Out to work in the 2013 or older versions with a firmware before 5.50 you need to either enable anonymous login or disable all authentication on the device. Audio Out will work with firmwares before 5.50 on the new 2014 versions.

Hikvision remarks:

Due to the new security policy introduced by Hikvision with the 5.3.x baseline firmware, adding Hikvision cameras may cause temporary lockout of devices, even if the correct username and password have been predefined. This can be avoided by disabling the 'Enable Illegal Login Lock' option on the camera's webpage, if it is available in the firmware.

Firmware versions supporting the 'Enable Illegal Login Lock':

    v5.3.8 build 150722

    v5.3.0 build 150513

    v5.3.8 build 151224

    v5.3.10 build 150917

Firmware versions without the 'Enable Illegal Login Lock':

    v5.3.8 build 150707

v5.3.9 build 150910

Recommended installation steps:

For devices that have the ability to control the Illegal Login Lock:

It is recommended to disable the Illegal Login Lock from camera's web page prior adding the device to Network VMS software.

Enabling it afterwards will not affect the functionality of this camera.

If disabling this feature is not an option please mind the following:

1. Avoid using express scan. If this is not an option please specify the username and password on top of the credentials' list.

2. When using IP range don't define more than 1 password and username.

3. If you need to add a lot of cameras with different credentials it is recommended using CSV file method.

4. Use manual add method (auto discovery).

For devices without Illegal Login Lock control in their webpage:

1. Avoid using express scan. If this is not an option please specify the username and password on top of the credentials' list.

2. When using IP range don't define more than 1 password and username.

3. If you need to add a lot of cameras with different credentials it is recommended using CSV file method.

4. Use manual add method (auto discovery).

Using firmware 5.5.0 and later versions:

With firmware 5.5.0 Onvif will no longer be enabled by default.

To enabled it, you need to use the Hikvisions tool which is found on their webpage or do it directly on the cameras homepage.