Release Notes – Milestone XProtect® Device Pack Version 8.9

It is with great pleasure that Milestone Systems as of December 15th, 2016 is shipping

Milestone XProtect Device Pack Version 8.9

IP Camera and Video Server Compatibility Overview

This release note lists the changes in Device Pack 8.9 that are supported in the following systems:

- XProtect Corporate 1.5 – 6.0 versions, 2013-2016 version
- XProtect Expert 2013-2016 version

Please note that support for Audio, Multi-streams and Pre-alarms requires XProtect Corporate 2.0a or newer.
Please note that support for H.264 requires XProtect Corporate 2.0b or newer.
Please note that support for Interlaced field-encoded H.264 requires XProtect Corporate 4.1a or newer.
Please note that support for GOP and more precise presets requires XProtect Corporate 5.0a or newer.

Device Pack changes

Changes from Device Pack 8.8 to 8.9

- Added support for new devices and firmware. Refer to the supported hardware list. See http://www.milestonesys.com/Support/Technical-Support/supportedhardware/allotherxprotectproducts/ for details.
- Added support for HTTPS for Axis audio devices.
- Added support for EdgeVis for Digital Barriers.
- Fixed issue with upgrading Device Pack using Pelco Ix2x cameras.
- Fixed PTZ issue for Hanwha Techwin SNP-6320RH.

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 XProtect version 2016 or newer, supporting HW accelerated decoding using the GPU

ONVIF upgrade from DP 6.2 or earlier remarks:

After upgrade some ONVIF devices might not work. The new version of ONVIF now only shows features that a responding correctly through the ONVIF interface. Since XProtect Corporate does not allow things like e.g. Audio, Input or similar to be removed, the ONVIF device will not be upgraded properly and hence not work. A work-around is to do replace hardware.

After upgrade Video Stream 1 and 2 might not correctly reflect the actual settings on those profiles. This is due to the ONVIF driver only used to have two video streams, where you selected a profile, where it now will have a video stream for each profile. XProtect Corporate "copies" the settings for

each video stream when the driver is upgraded, so if Video Stream 1 or 2 did not have the correct profile that is now mapped to the stream it will show the same settings as before the upgrade even though the mapped profile might actually have other settings. The streams should work with the new settings unless some of these are not supported on the profile.

Some settings can be missing because the driver now only looks for the different type of settings in the places they should be according to standard.

Some features might not work any longer because the driver now only looks for the features and corresponding settings in the places and in the format they should have according to the standard.

Profile names might get changed after the upgrade because we now use the names given by the device for the profiles. These will not always correspond to what was previously used.

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. So 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.

Stretch Remarks:

To accommodate requests that the Stretch cards can run in a machine that has no Network card, the Stretch cards will from Device Pack 7.1 use a new scheme to retrieve a serial number. This means that when updating from a previous device pack, you need to run a Replace Hardware and get a new license for the Stretch cards to work.

Digital Barriers Remarks:

For the driver made for Digital Barriers TVI server there is a limit of 64 cameras connected per server. To support this new innovative mobile technology, Milestone will run a campaign offering the Digital Barriers connected cameras with a Milestone device license model similar to our encoder license setup – one license per TVI server. This time limited offering will run for 2016.

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 XProtect 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).

Upgrade from DP 6.7 or earlier remark:

If you are upgrading from a device pack prior to Device Pack 6.7 and using XProtect Enterprise 8.x, XProtect Professional 8.x, XProtect Express, XProtect Essential 2.x or XProtect Go 2.x versions, it is important that you do not uninstall the previous Device Pack first.