MAKE THE
WORLD SEE

Date: 26 April 2024

Manual

Milestone Custom Development Actions v1.3

milestone

Table of Content

Target audience for this document **4**

Copyright, trademarks & disclaimer **5**

Copyright 5

Trademarks 5

Disclaimer 5

General description **6**

Introduction 6

Installation **7**

Prerequisites 7

Hotfix installers 7

Hotfix installation steps 7

Plug-in installer 21

Plug-in installation steps 21

License 25

Configuration **26**

Enable <device> 26

Disable <device> 26

Enable <hardware> 26

Disable <hardware> 26

Start recording on <cameras> 27

Stop recording on <cameras> 27

Move <hardware> to <storage> 27

Add live permissions from <roles> on <hardware> 28

Remove live permissions from <roles> on <hardware> 28

Add <user> to <role> 28

Remove <user> from <role> 30

Add <evidence lock> to recording on <cameras> 31

Activate <rules> 33

Deactivate <rules> 34

Raise alarm via <alarm definitions> using throttling mechanism 35

Take snapshots of <cameras> from live feed 36

Example for rule Take snapshots of <cameras> from live feed 37

Example for a rule which performs Disable <hardware> action 37

Operation 43

Verify the Disable <hardware> action rule is working 43

Troubleshooting 44

MIP Logs 44

Limitations 46

Move <hardware> to <storage> 46

Add <user> to <role> 46

Remove <user> from <role> 46

Add <evidence lock> to recording on <cameras> 46

Activate <rules> / Deactivate <rules> 46

Loading issue 46

Known issues 46

Target audience for this document

The installation and configuration part of this document is aimed at system administrators of the Milestone XProtect.

The operation part of this document is aimed at system administrators and also system operators with basic knowledge of Milestone XProtect.

As this manual contains specific details about the solution, it is recommended for system administrators to check the following sources of information:

- Milestone XProtect (XProtect Management Client and XProtect Smart Client)

and for system operators to check at least:

- Milestone XProtect (XProtect Smart Client)

Copyright, trademarks & disclaimer

Copyright

Trademarks

XProtect is a registered trademark of Milestone Systems A/S.

Microsoft and Windows are registered trademarks of Microsoft Corporation.

All other trademarks mentioned in this document are trademarks of their respective owners.

Disclaimer

This document is intended for general information purposes only, and due care has been taken in its preparation.

Any risk arising from the use of this information rests with the recipient, and nothing herein should be construed as constituting any kind of warranty.

Milestone Systems A/S reserve the right to make adjustments without prior notification.

All names of people and organizations used in this document's examples are fictitious. Any resemblance to any actual organization or person, living or dead, is purely coincidental and unintended.

This product may make use of third party software for which specific terms and conditions may apply. When that is the case, you can find more information in the file *3rd_party_software_terms_and_conditions.txt* located in your Milestone surveillance system installation folder.

General description

Introduction

The Custom Development Actions plug-in extends the Actions list in the rule creation/configuration. You can create rules based on events. The rules can perform these new actions:

- Enable <device>
- Disable <device>
- Enable <hardware>
- Disable <hardware>
- Start recording on <cameras>
- Stop recording on <cameras>
- Move <hardware> to <storage>
- Add live permissions from <roles> on <hardware>
- Remove live permissions from <roles> on <hardware>
- Add <user> to <role>
- Remove <user> from <role>
- Add <evidence lock> to recording on <cameras>
- Activate <rules>
- Deactivate <rules>
- Raise alarm via <alarm definitions> using throttling mechanism
- Take Snapshots of <cameras> from live feed

The activities of these rules are tracked into the MIP logs of the XProtect Event Server.

An example for creating a rule which performs **Disable <hardware>** action can be found in subchapter Configuration > Example for a rule which performs Disable <hardware> action. Examples for the logging feature can be found in subchapter Troubleshooting > MIP Logs.

Installation

Prerequisites

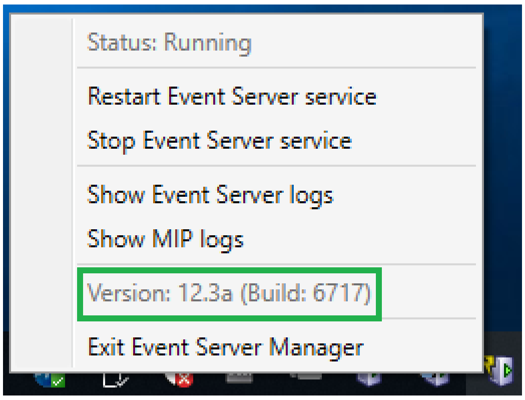
The Custom Development Actions plug-in is compatible with Milestone XProtect Corporate 2018 R3 or newer.

Hotfix installers

Several hotfixes must be installed, but only in case of Milestone XProtect Corporate 2018 R3:

- ***Milestone.Hotfix.201810250552.MC.12.3a.8563.exe*** must be installed where the XProtect Management Client is installed.
- ***Milestone.Hotfix.201810301135.MS.12.3a.8575.exe*** must be installed where the XProtect Management Server is installed.
- ***Milestone.Hotfix.201810301135.RS.12.3a.8575.exe*** must me installed where the XProtect Recording Server is installed.
- ***MilestoneEventServerInstaller_x64.exe (v12.3.13877.1)*** must be installed where the XProtect Event Server is installed.

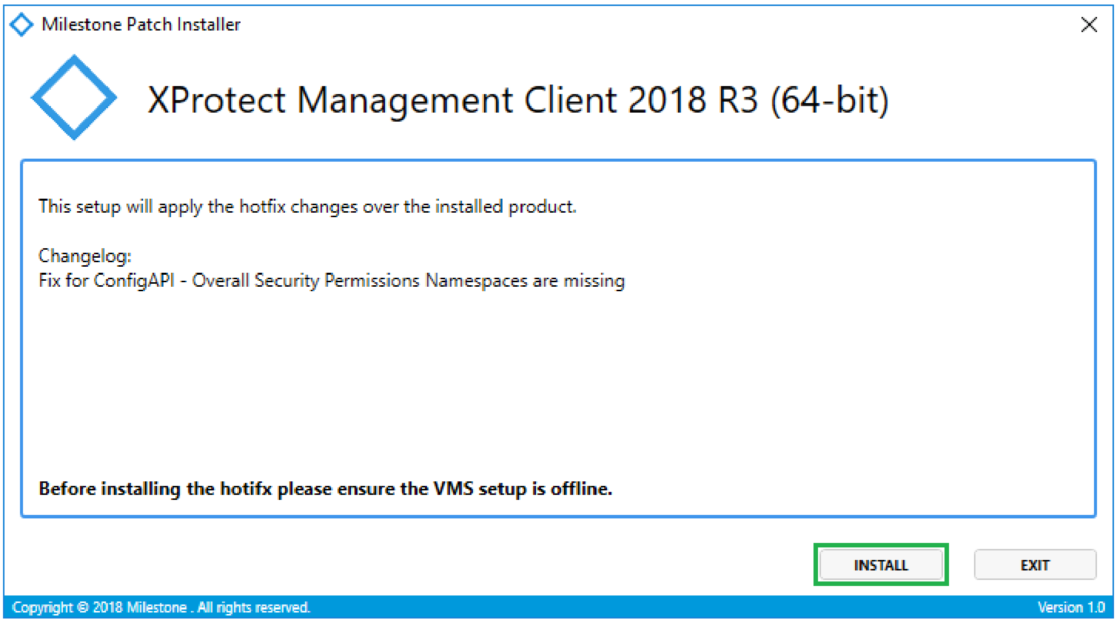
  Note: *Check the installed version of the XProtect Event Server and do not install the XProtect Event Server hotfix if the version is 12.3a (Build:6717) or higher.*


Status: Running
Restart Event Server service
Stop Event Server service
Show Event Server logs
Show MIP logs
Version: 12.3a (Build: 6717)
Exit Event Server Manager

Hotfix installation steps

Milestone.Hotfix.201810250552.MC.12.3a.8563

1. Close the XProtect Management Client.
2. Start the installation by executing ***Milestone.Hotfix.201810250552.MC.12.3a.8563.exe***.
3. Click **Install**.



Milestone Patch Installer

XProtect Management Client 2018 R3 (64-bit)

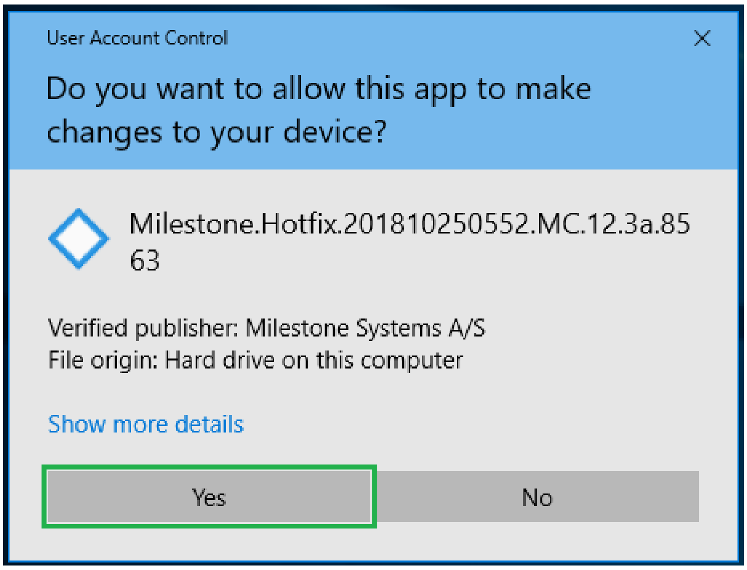
This setup will apply the hotfix changes over the installed product.

Changelog:
Fix for ConfigAPI - Overall Security Permissions Namespaces are missing

Before installing the hotifx please ensure the VMS setup is offline.

INSTALL
EXIT
Copyright © 2018 Milestone . All rights reserved.
Version 1.0

4. Click **Yes**, in case the following message appears on the screen:



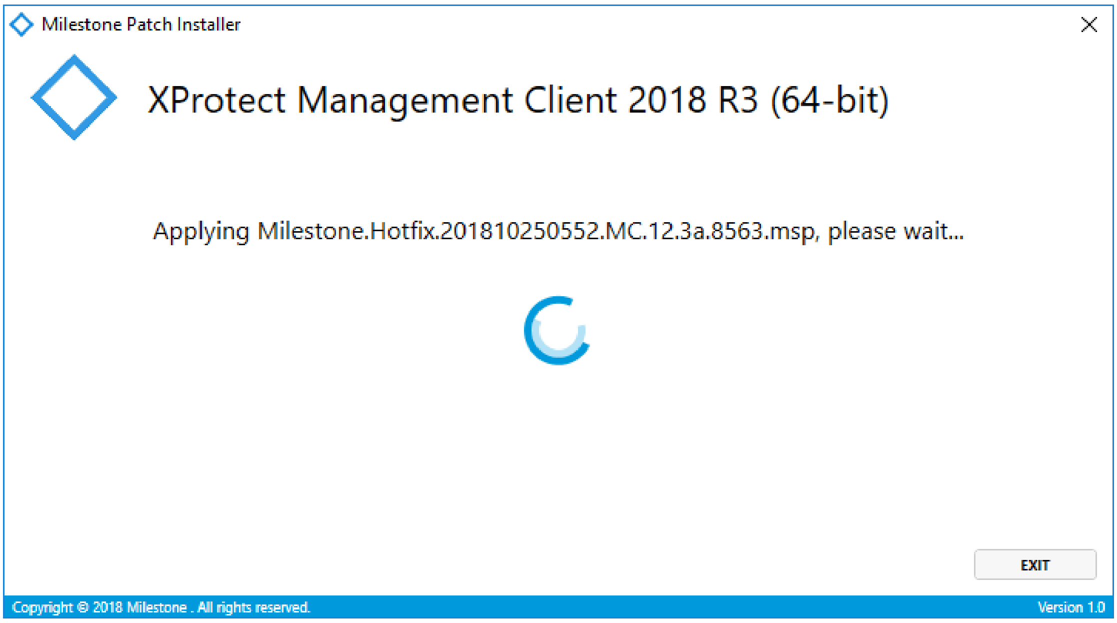
User Account Control

Do you want to allow this app to make changes to your device?

Milestone.Hotfix.201810250552.MC.12.3a.8563

Verified publisher: Milestone Systems A/S
File origin: Hard drive on this computer

5. The next steps are executed automatically.

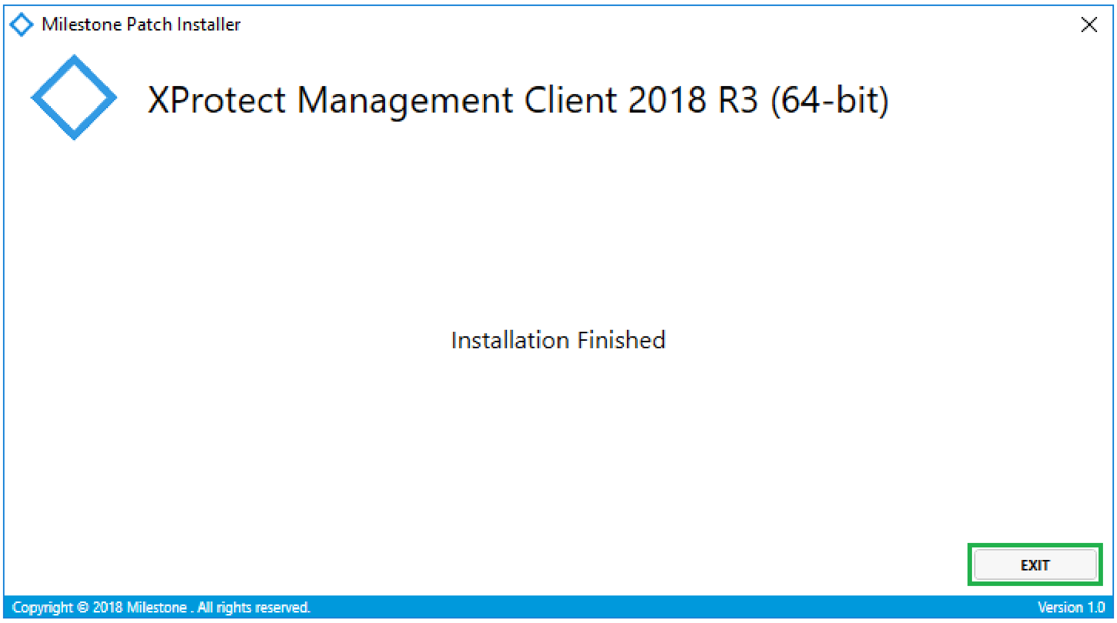


Milestone Patch Installer

XProtect Management Client 2018 R3 (64-bit)

Applying Milestone.Hotfix.201810250552.MC.12.3a.8563.msp, please wait...

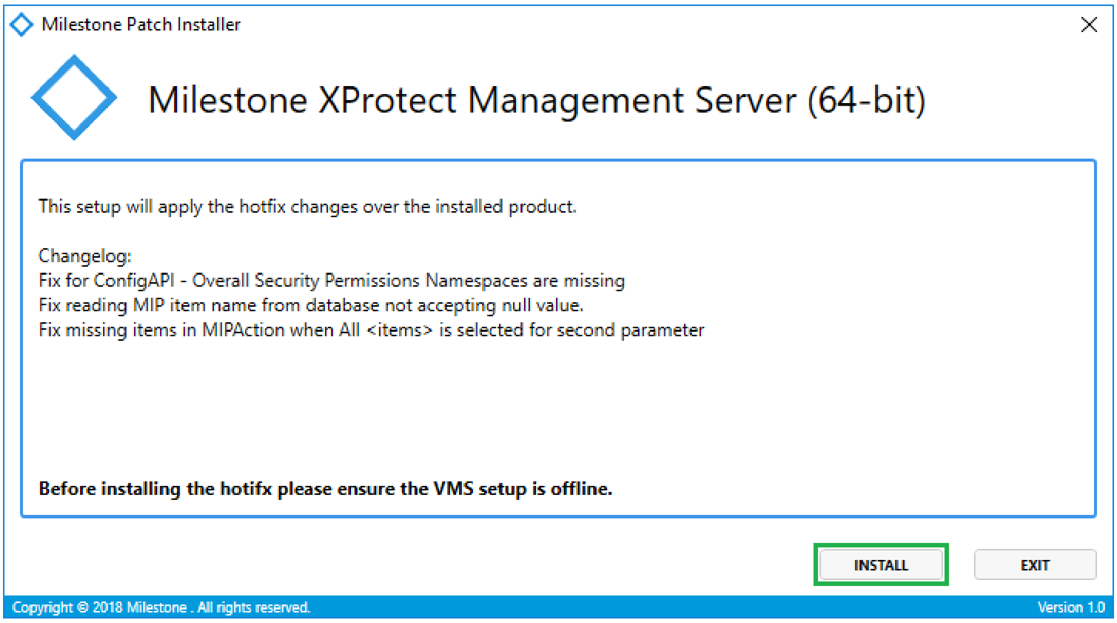
6. Click **Finish**.


Milestone Patch Installer
XProtect Management Client 2018 R3 (64-bit)
EXIT
Copyright © 2018 Milestone . All rights reserved.
Version 1.0

Installation Finished

Milestone.Hotfix.201810301135.MS.12.3a.8575

1. Stop the XProtect Management Server.
2. Start the installation by executing *Milestone.Hotfix.201810301135.MS.12.3a.8575.exe*.
3. Click **Install**.

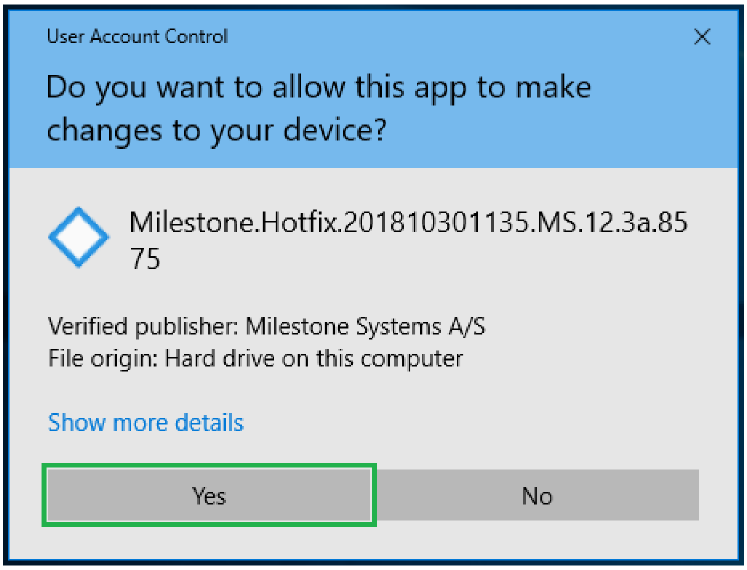

Milestone Patch Installer
Milestone XProtect Management Server (64-bit)
INSTALL
EXIT
Copyright © 2018 Milestone . All rights reserved.
Version 1.0

This setup will apply the hotfix changes over the installed product.

Changelog:
Fix for ConfigAPI - Overall Security Permissions Namespaces are missing
Fix reading MIP item name from database not accepting null value.
Fix missing items in MIPAction when All <items> is selected for second parameter

Before installing the hotifx please ensure the VMS setup is offline.

4. Click **Yes**, in case the following message appears on the screen:



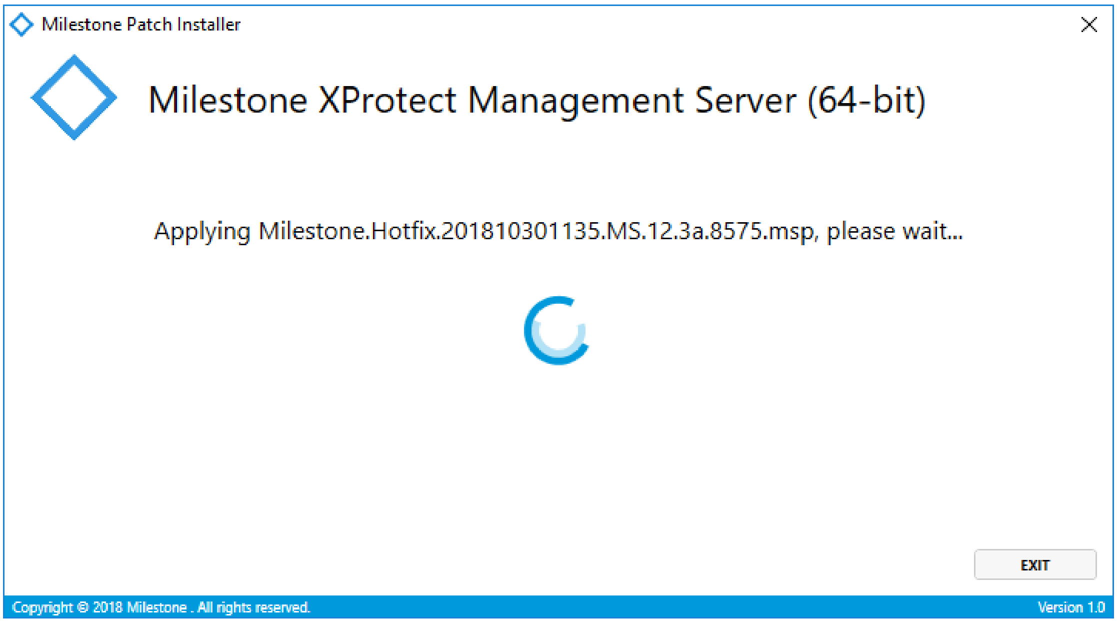
User Account Control

Do you want to allow this app to make changes to your device?

Milestone.Hotfix.201810301135.MS.12.3a.8575

Verified publisher: Milestone Systems A/S
File origin: Hard drive on this computer

5. The next steps are executed automatically.

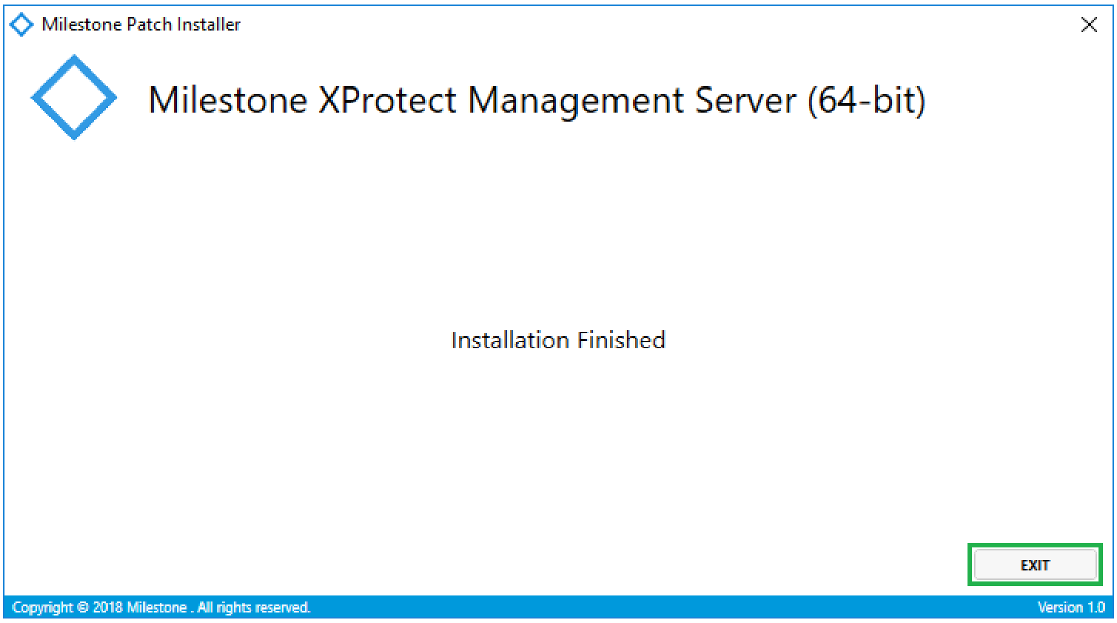


Milestone Patch Installer

Milestone XProtect Management Server (64-bit)

Applying Milestone.Hotfix.201810301135.MS.12.3a.8575.msp, please wait...

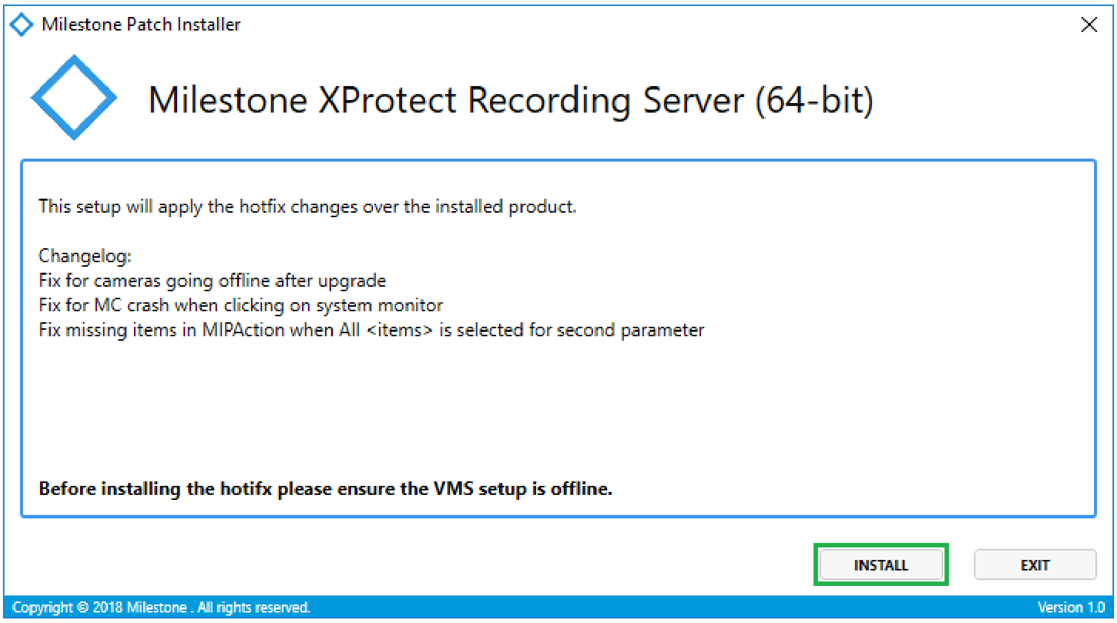
6. Click **Finish**.


Milestone Patch Installer
Milestone XProtect Management Server (64-bit)
EXIT
Copyright © 2018 Milestone . All rights reserved.
Version 1.0

Installation Finished

Milestone.Hotfix.201810301135.RS.12.3a.8575

1. Stop the XProtect Recording Server.
2. Start the installation by executing *Milestone.Hotfix.201810301135.RS.12.3a.8575.exe*.
3. Click **Install**.

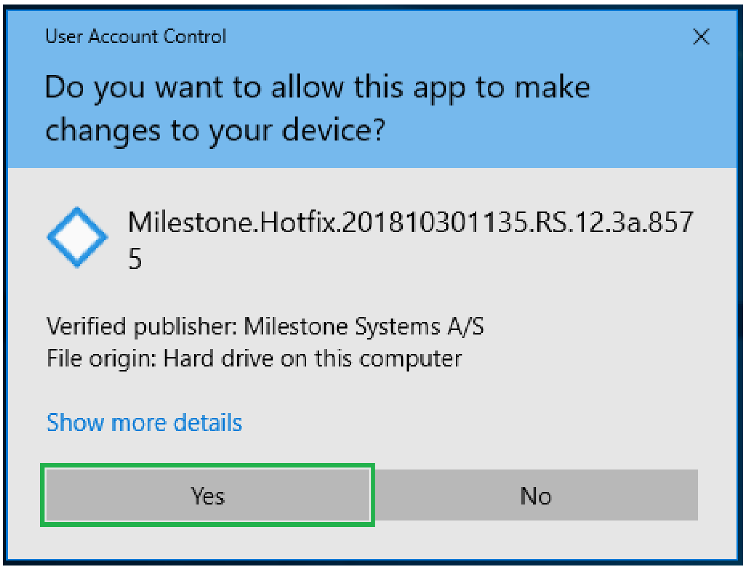

Milestone Patch Installer
Milestone XProtect Recording Server (64-bit)
INSTALL
EXIT
Copyright © 2018 Milestone . All rights reserved.
Version 1.0

This setup will apply the hotfix changes over the installed product.

Changelog:
Fix for cameras going offline after upgrade
Fix for MC crash when clicking on system monitor
Fix missing items in MIPAction when All <items> is selected for second parameter

Before installing the hotifx please ensure the VMS setup is offline.

4. Click **Yes**, in case the following message appears on the screen:



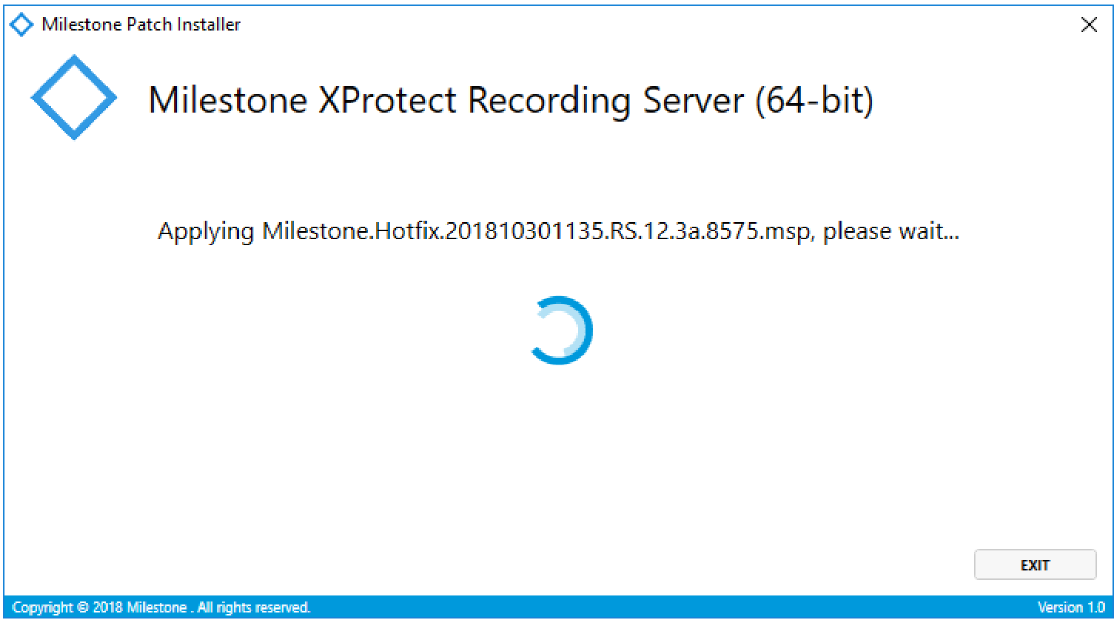
User Account Control

Do you want to allow this app to make changes to your device?

Milestone.Hotfix.201810301135.RS.12.3a.857
5

Verified publisher: Milestone Systems A/S
File origin: Hard drive on this computer

5. The next steps are executed automatically.



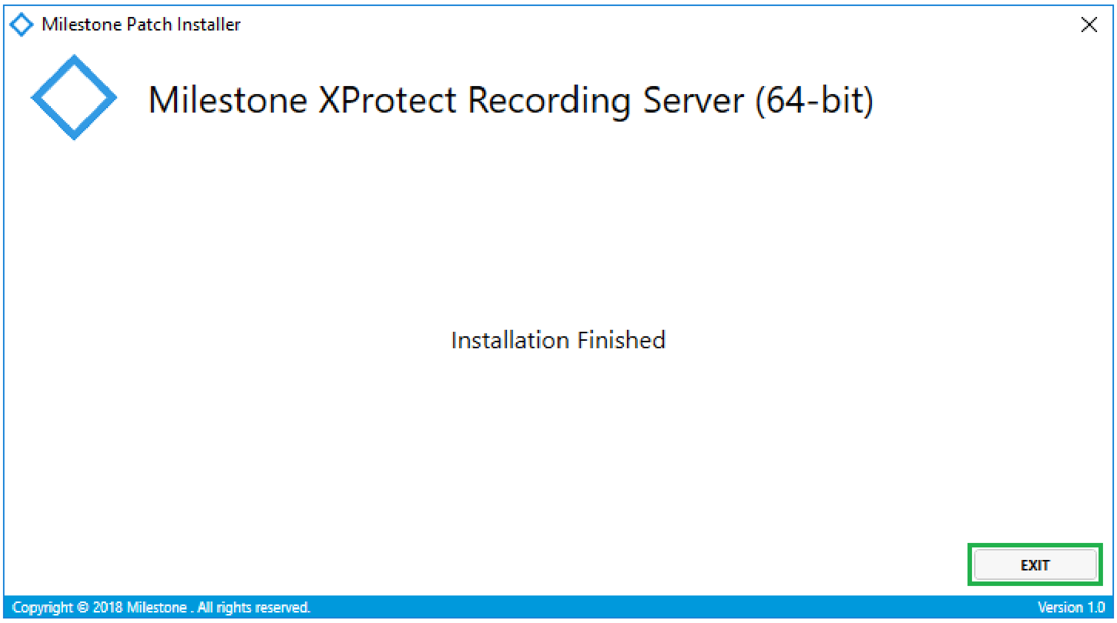
Milestone Patch Installer

Milestone XProtect Recording Server (64-bit)

Applying Milestone.Hotfix.201810301135.RS.12.3a.8575.msp, please wait...

Copyright © 2018 Milestone . All rights reserved. Version 1.0

6. Click **Finish**.



Milestone Patch Installer

Milestone XProtect Recording Server (64-bit)

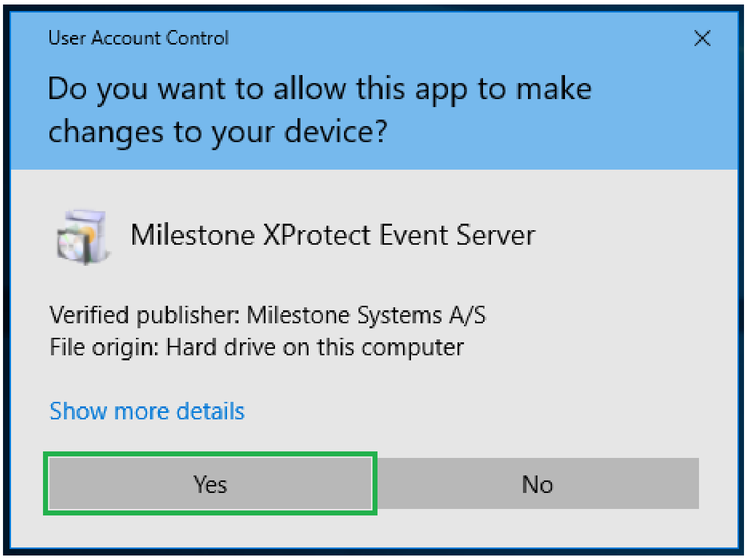
Installation Finished

Copyright © 2018 Milestone . All rights reserved.

Version 1.0

MilestoneEventServerInstaller_x64 (v12.3.13877.1)

1. Start the installation by executing *MilestoneEventServerInstaller_x64.exe*.
2. Click **Yes**, in case the following message appears on the screen:



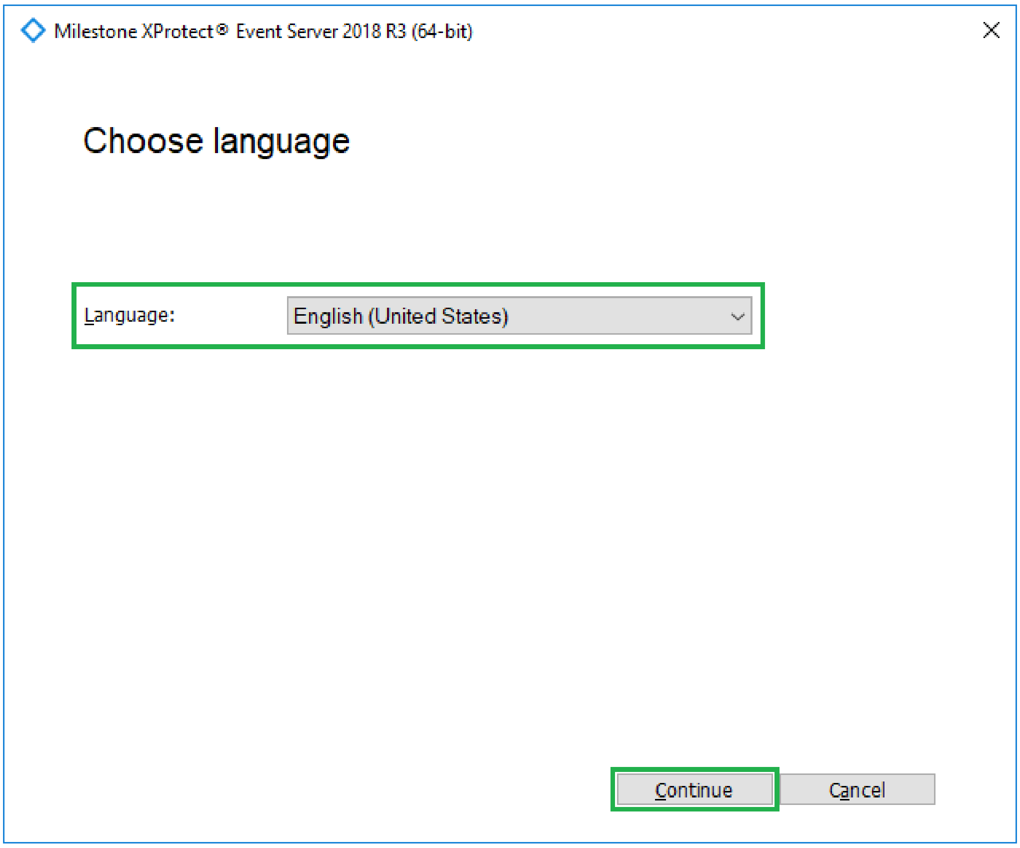
User Account Control

Do you want to allow this app to make changes to your device?

Milestone XProtect Event Server

Verified publisher: Milestone Systems A/S
File origin: Hard drive on this computer

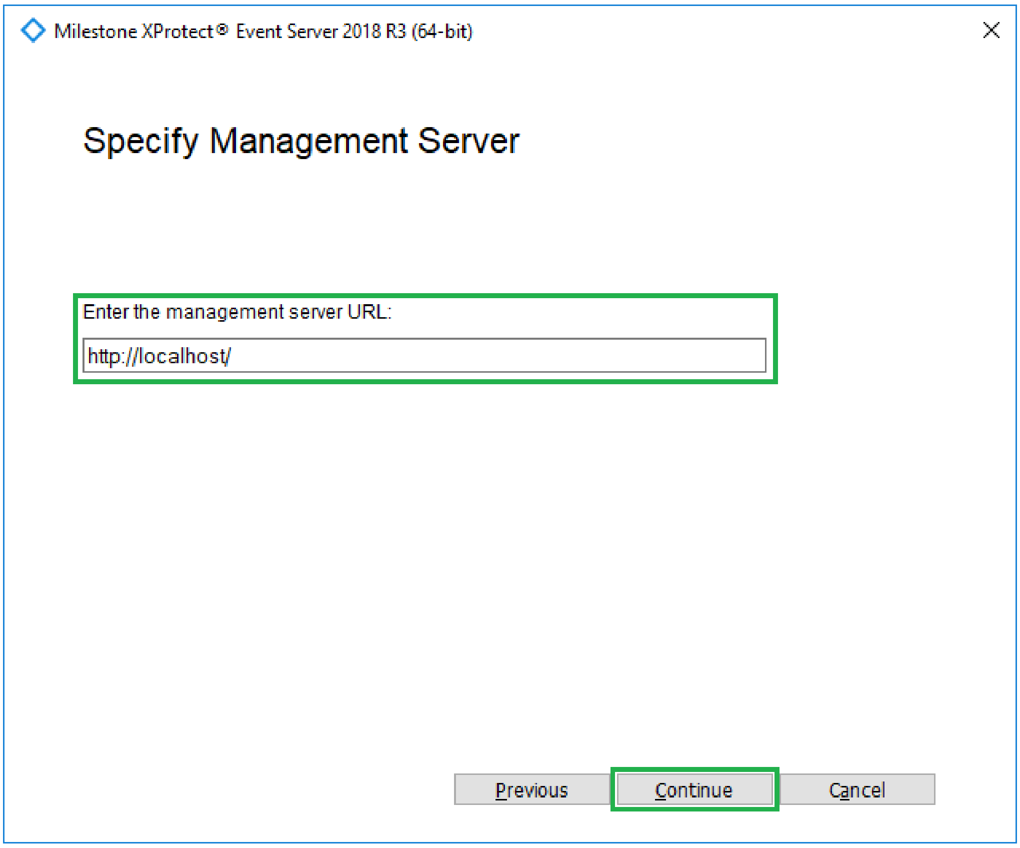
3. By default the installer will choose Language > **English (United States).** Choose any other language according to your preferences. Click **Continue**.


Milestone XProtect® Event Server 2018 R3 (64-bit)

Choose language

Language: English (United States)

4. The installer will choose for **server URL** the host where the XProtect Management Server is currently installed. In this case it is **http://localhost**.



Milestone XProtect® Event Server 2018 R3 (64-bit)

Specify Management Server

Enter the management server URL:

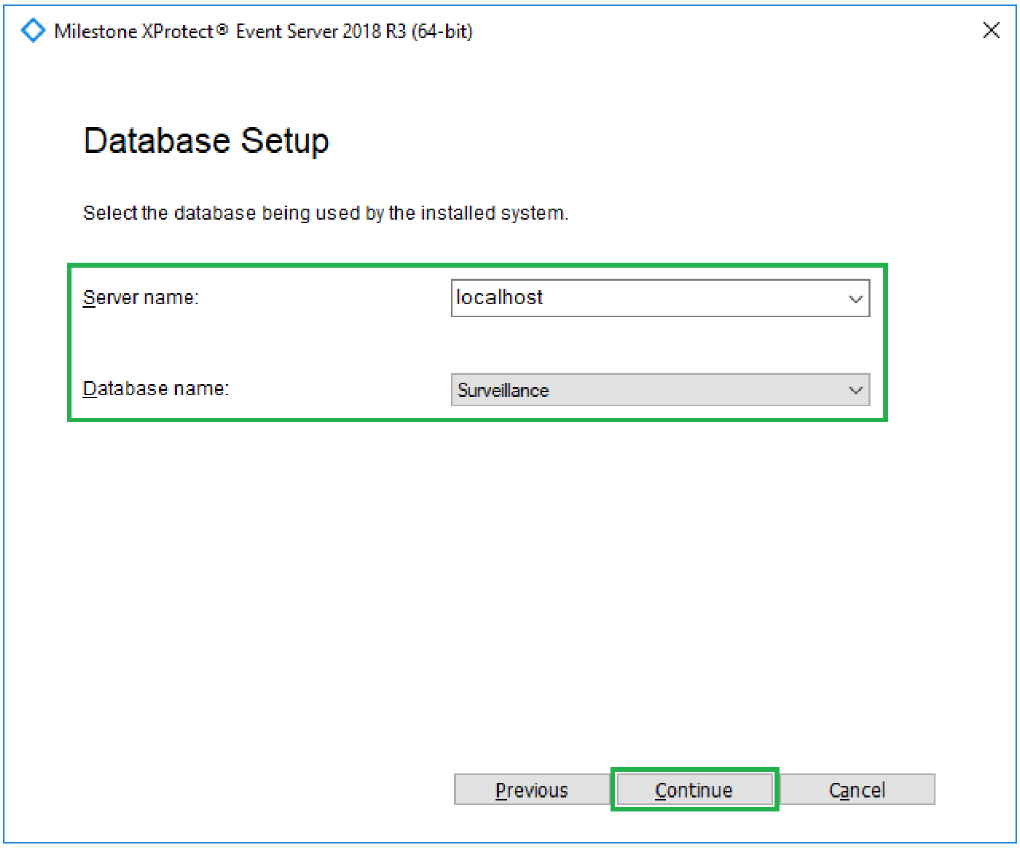
http://localhost/

5. The installer will choose the **Server name** and **Database** name based on the configuration of the current installation. In this case it is:

   Server name: **localhost**

   Database name: **Surveillance**

   Click **Continue**.



Milestone XProtect® Event Server 2018 R3 (64-bit)

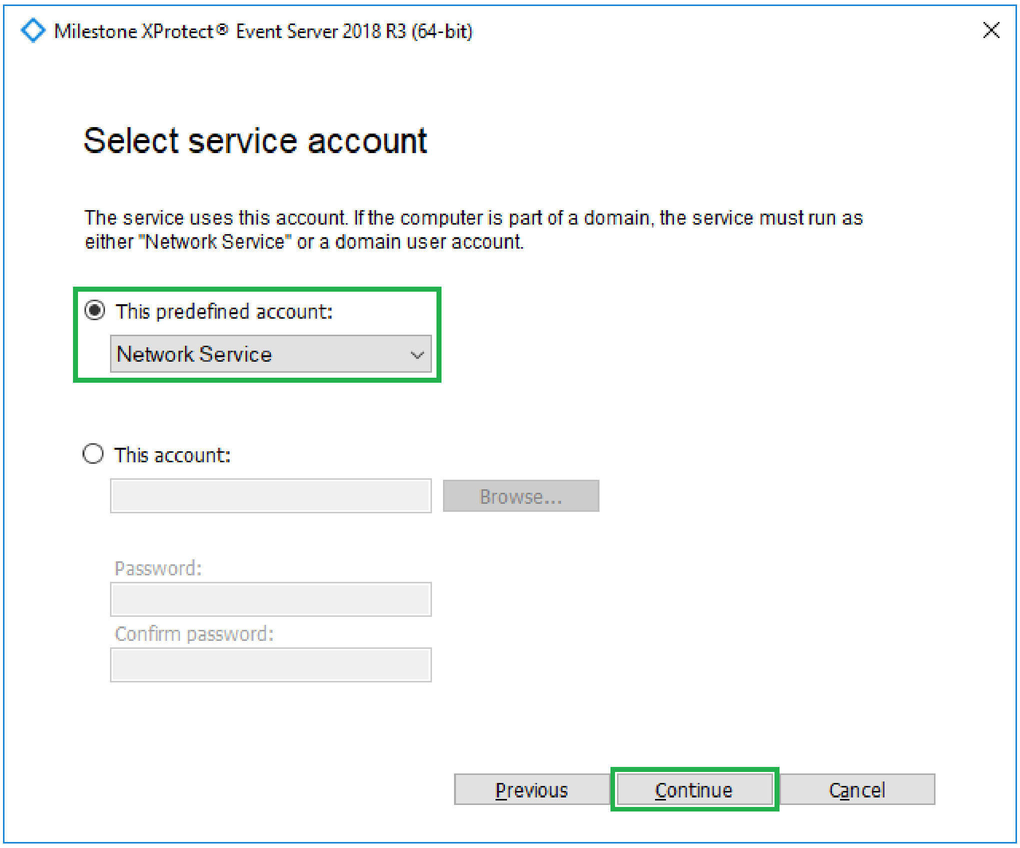
Database Setup

Select the database being used by the installed system.

Server name: localhost

Database name: Surveillance

6. The installer will choose the **service account** based on the configuration of the current installation. In this case it is **Network Service.** Click **Continue**.



Milestone XProtect® Event Server 2018 R3 (64-bit)

Select service account

The service uses this account. If the computer is part of a domain, the service must run as either "Network Service" or a domain user account.

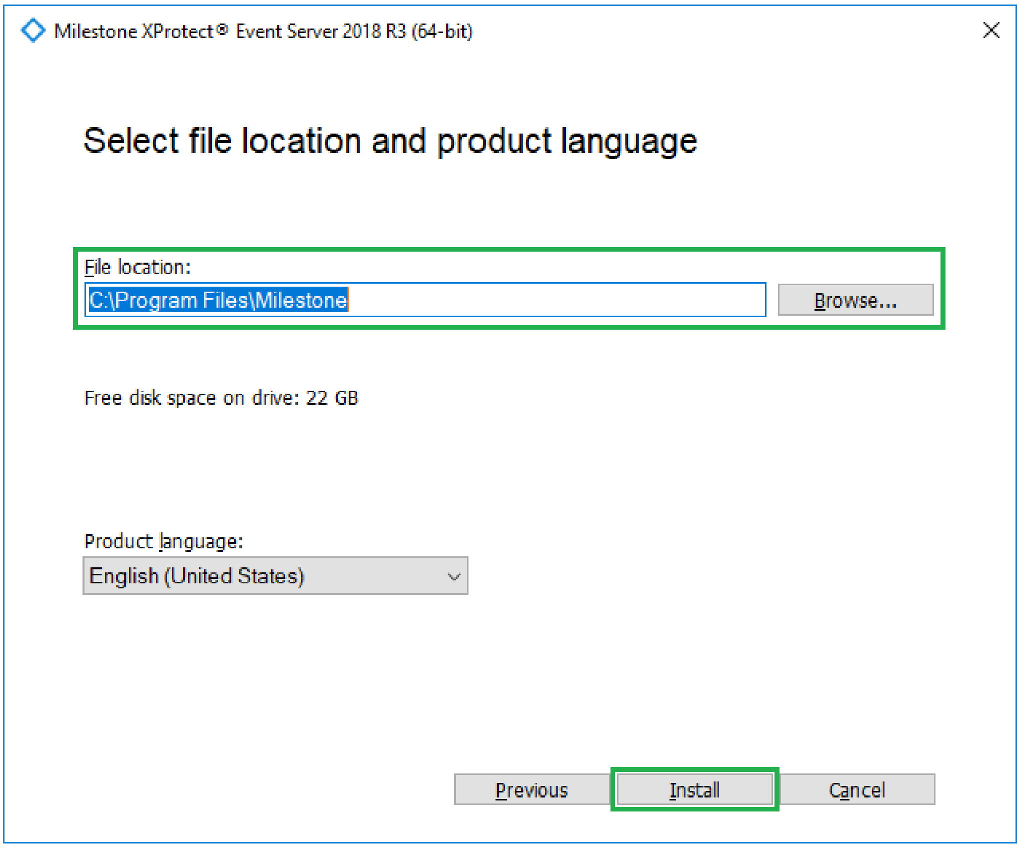
● This predefined account: Network Service

○ This account:

Password:

Confirm password:

7. The installer will choose the **File location** based on configuration of the current installation**.** In this case it is **C:\Program Files\Milestone**. Click **Install**.



Milestone XProtect® Event Server 2018 R3 (64-bit)

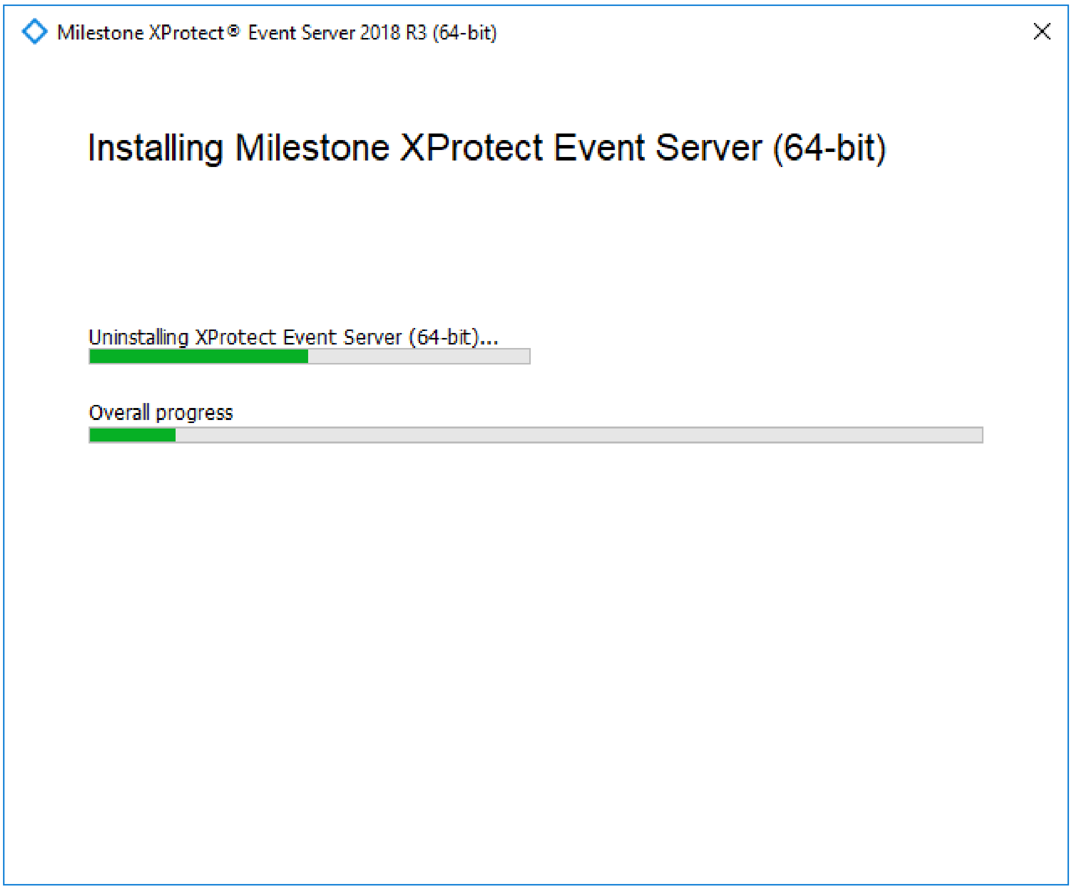
Select file location and product language

File location: C:\Program Files\Milestone

Free disk space on drive: 22 GB

Product language: English (United States)

8. The next steps are executed automatically.



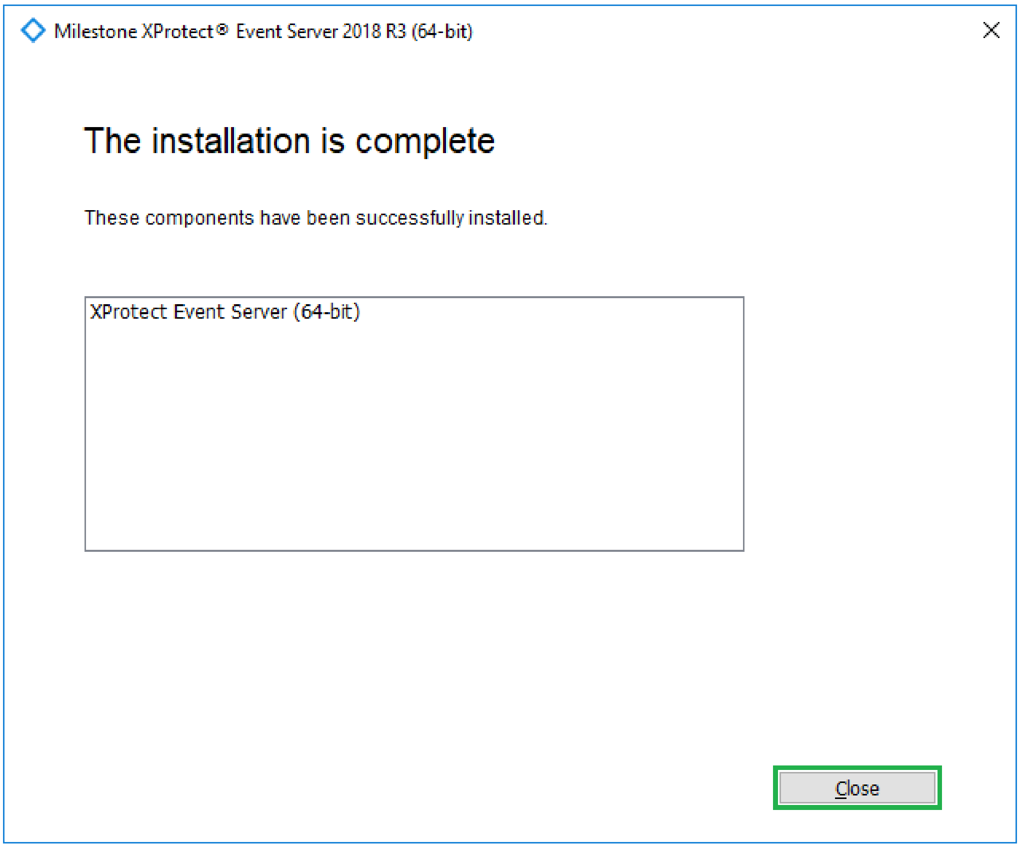
Milestone XProtect® Event Server 2018 R3 (64-bit)

Installing Milestone XProtect Event Server (64-bit)

Uninstalling XProtect Event Server (64-bit)...

Overall progress

9. Click **Close**.



Milestone XProtect® Event Server 2018 R3 (64-bit)

The installation is complete

These components have been successfully installed.

XProtect Event Server (64-bit)

10. Restart the computer in order the changes to be applied.

Plug-in installer

The Milestone Custom Development Actions plug-in consists of one installation file supporting Windows 64-bit only:

- *MilestoneCustomDevelopmentActionsInstaller_x64_v1.2.XX.X.msi*

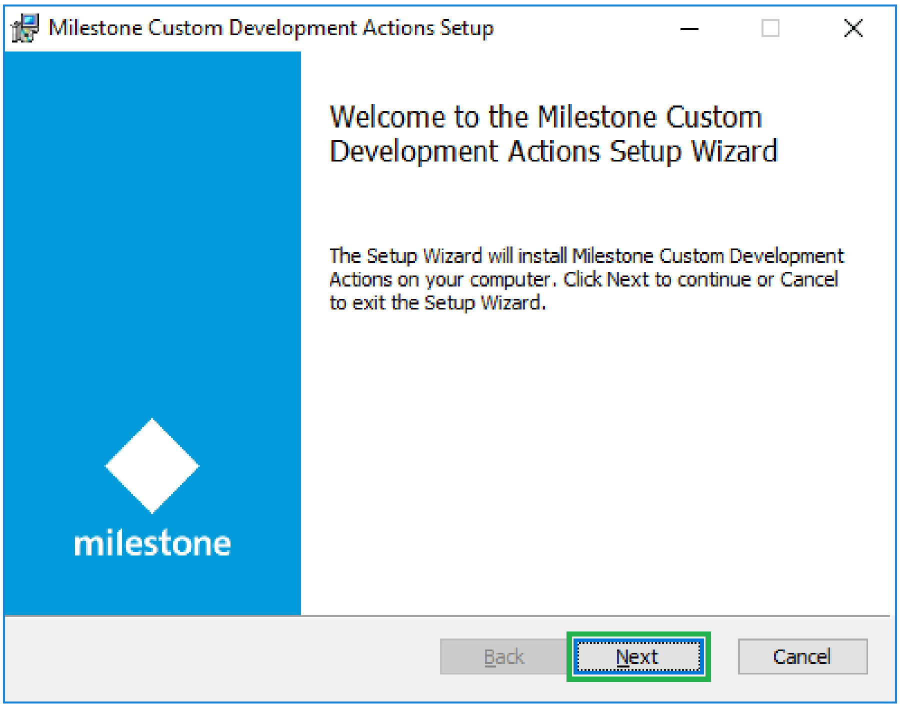
The Milestone Custom Development Actions plug-in must be installed on the following computers:

- On the computer where the XProtect Event Server is installed
- On the computer where the XProtect Management Client is installed

Plug-in installation steps

1. Start the installation by executing *MilestoneCustomDevelopmentActionsInstaller_x64_v1.2.XX.X..msi*.

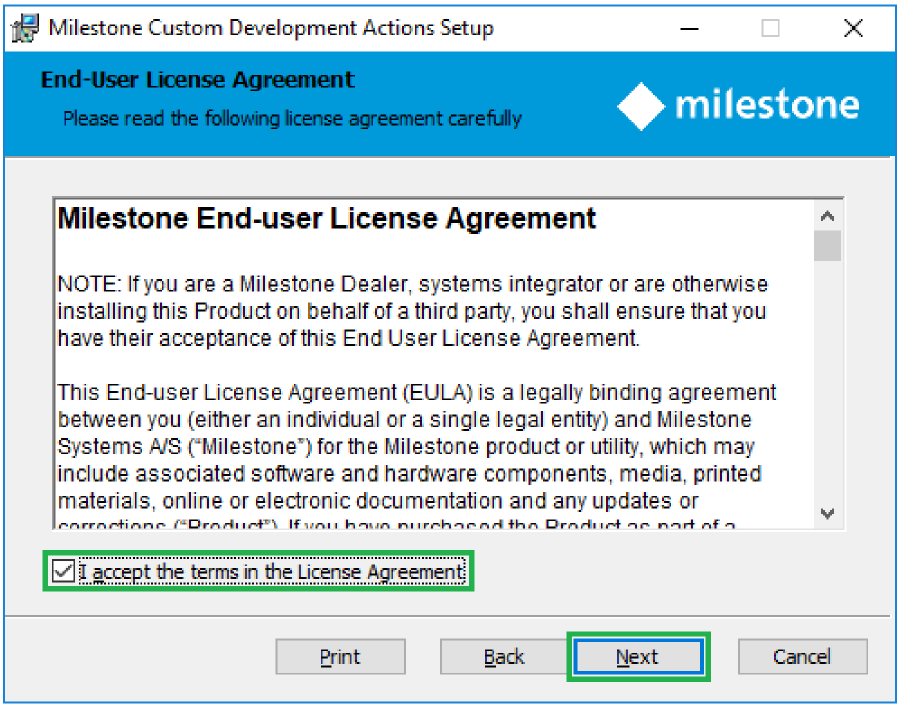
2. Click **Next**.


Milestone Custom Development Actions Setup

Welcome to the Milestone Custom Development Actions Setup Wizard

The Setup Wizard will install Milestone Custom Development Actions on your computer. Click Next to continue or Cancel to exit the Setup Wizard.

3. Read the license agreement carefully and select the **I accept the terms in the License Agreement** box. Click **Next**.


Milestone Custom Development Actions Setup

End-User License Agreement

Please read the following license agreement carefully

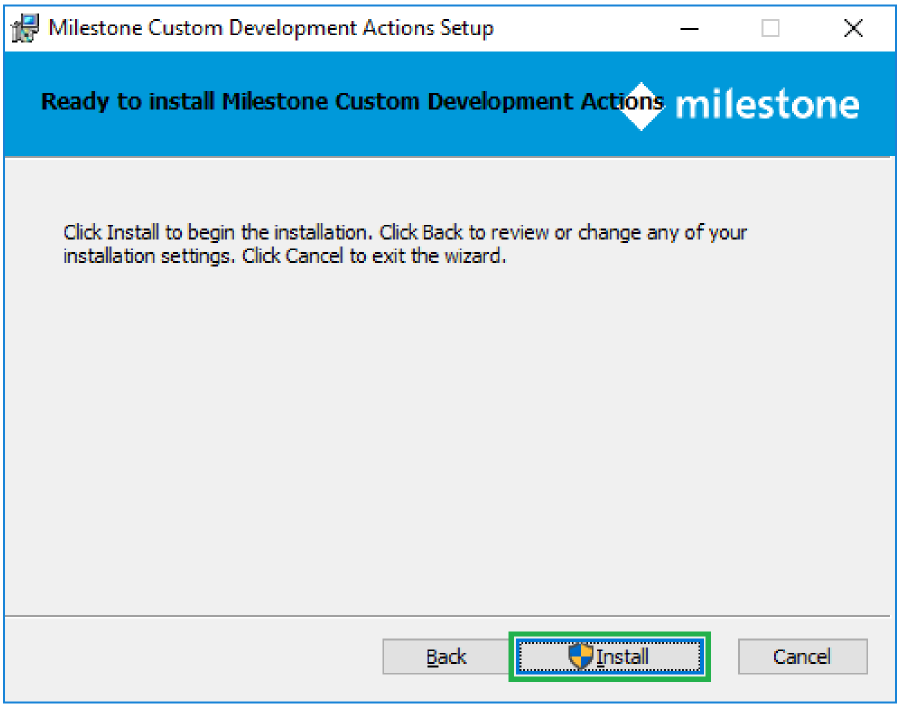
Milestone End-user License Agreement

NOTE: If you are a Milestone Dealer, systems integrator or are otherwise installing this Product on behalf of a third party, you shall ensure that you have their acceptance of this End User License Agreement.

This End-user License Agreement (EULA) is a legally binding agreement between you (either an individual or a single legal entity) and Milestone Systems A/S ("Milestone") for the Milestone product or utility, which may include associated software and hardware components, media, printed materials, online or electronic documentation and any updates or corrections ("Product"). If you have purchased the Product as part of a

☑ I accept the terms in the License Agreement

4. Click **Install**.

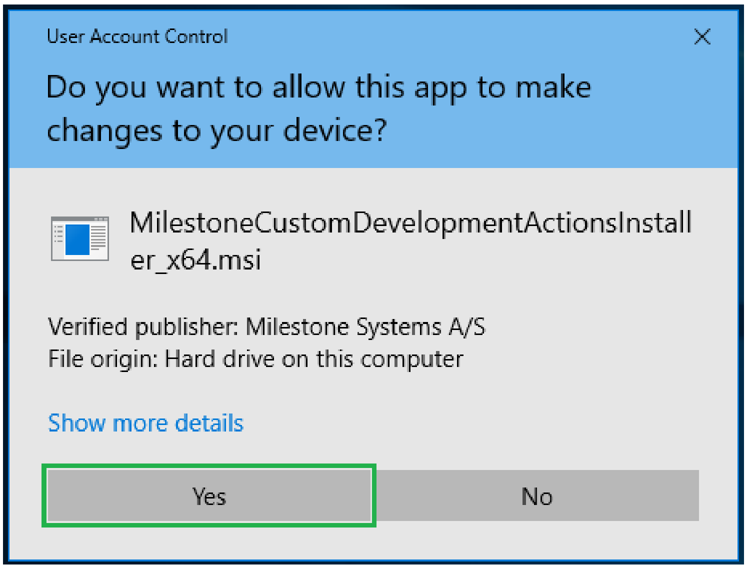


Milestone Custom Development Actions Setup

Ready to install Milestone Custom Development Actions

Click Install to begin the installation. Click Back to review or change any of your installation settings. Click Cancel to exit the wizard.

5. Click **Yes**, in case the following message appears on the screen:



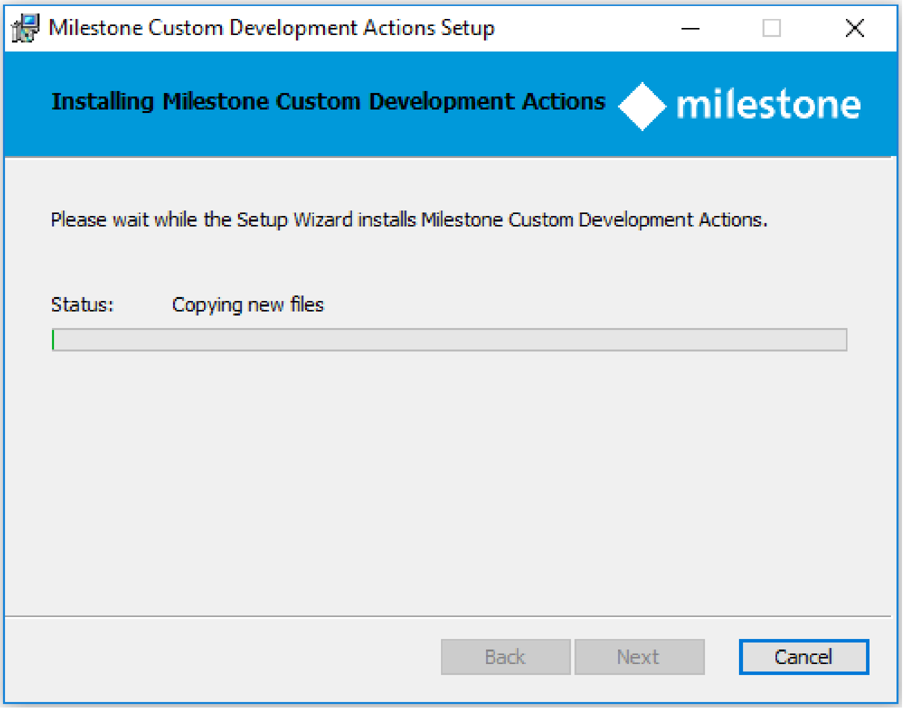
User Account Control

Do you want to allow this app to make changes to your device?

MilestoneCustomDevelopmentActionsInstaller_x64.msi

Verified publisher: Milestone Systems A/S
File origin: Hard drive on this computer

6. The next steps are executed automatically.

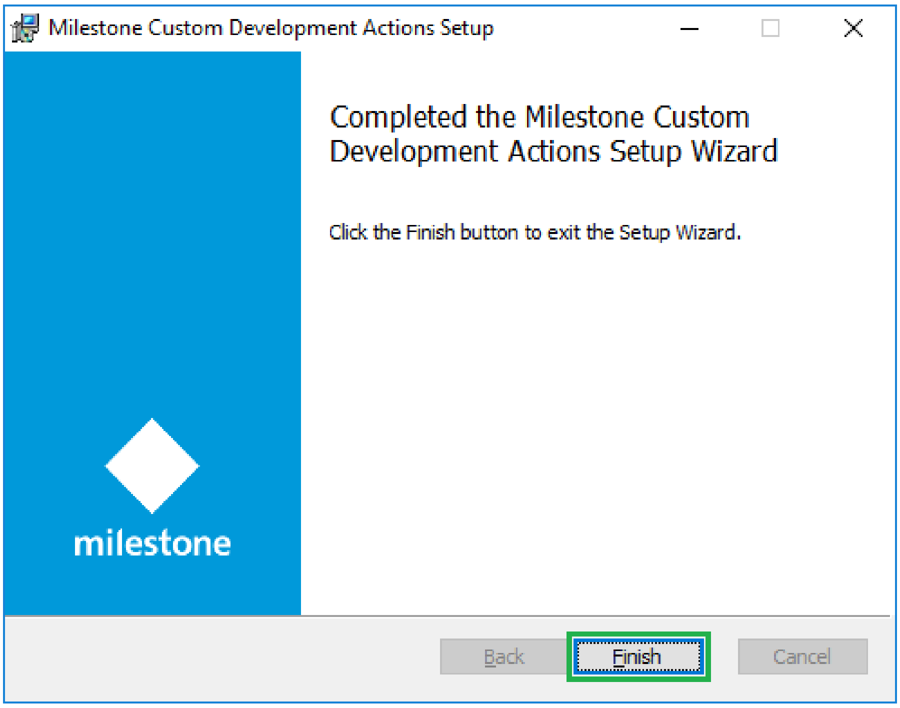


Milestone Custom Development Actions Setup
Installing Milestone Custom Development Actions
milestone

Please wait while the Setup Wizard installs Milestone Custom Development Actions.

Status: Copying new files

7. Click **Finish**.



Completed the Milestone Custom Development Actions Setup Wizard

Click the Finish button to exit the Setup Wizard.

8. Restart the XProtect Event Server.

License

This solution does have a build-in **MIP** license check that is locked to the software license code (SLC) of the XProtect installation of which it is a part.

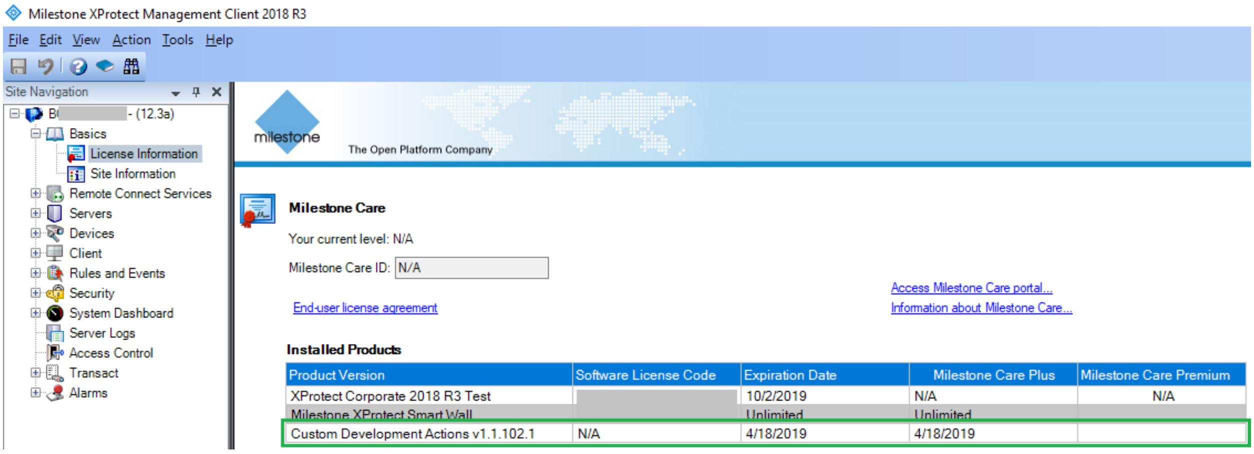
It automatically comes with a 30 day grace period which starts from the date when the plug-in is installed. After the grace period expires, a permanent **MIP** license is needed.

The permanent **MIP** licenses are provided by the distributor. In order to generate a permanent **MIP** license, the distributor must know the SLC of the XProtect system where the solution has been installed. Collect the SLC and send it to the distributor, preferably via email.

When the permanent **MIP** license is acquired, the XProtect system must be reactivated, either online or offline.
If **MIP** license check fails, the following error message will be displayed in the MIP logs and the solution will have a reduced functionality:

Example:
2021-10-11 12:54:12.873 UTC+03:00 Error CustomActionManager There is a problem with the license.(System.Collections.ObjectModel.Collection`1[VideoOS.Platform.License.LicenseInformation])

The license information can also be checked in the XProtect Management Client > **Site Navigation** > **Basics** > **License Information** > **Installed Products** > **Custom Development Actions v1.3.XX.1**.



Milestone Care

Your current level: N/A

Milestone Care ID: N/A

Installed Products

Product Version	Software License Code	Expiration Date	Milestone Care Plus	Milestone Care Premium
XProtect Corporate 2018 R3 Test	[redacted]	10/2/2019	N/A	N/A
Milestone XProtect Smart Wall	[redacted]	Unlimited	Unlimited	
Custom Development Actions v1.1.102.1	N/A	4/18/2019	4/18/2019	

Configuration

Enable <device>

Description	
This is an action which changes the state of the selected device (Cameras, Inputs, Metadata, Microphones, Outputs and/or Speakers) in the available Recording Servers from Not **Enabled** (Disabled) to **Enabled.**	
Parameters	
<device>	You need to select one, many or **All Cameras**, **All Inputs**, **All Metadata**, **All Microphones**, **All Outputs** and/or **All Speakers** from list.

Disable <device>

Description	
This is an action which changes the state of the selected device (Cameras, Inputs, Metadata, Microphones, Outputs and/or Speakers) in the available Recording Servers from **Enabled** to Not **Enabled** (Disabled).	
Parameters	
<device>	You need to select one, many or **All Cameras**, **All Inputs**, **All Metadata**, **All Microphones**, **All Outputs** and/or **All Speakers** from list.

Enable <hardware>

Description	
This is an action which changes the state of the selected hardware in the available Recording Servers from Not **Enabled** (Disabled) to **Enabled**.	
Parameters	
<hardware>	You need to select one, many or **All Hardware** from the list.

Disable <hardware>

Description	
This is an action which changes the state of the selected hardware in the available Recording Servers from **Enabled** to Not **Enabled** (Disabled).	
Parameters	
<hardware>	You need to select one, many or **All Hardware** from the list.

Start recording on <cameras>

Description	
This is an action which starts the recording (via sending MIP message "Start recording") for the selected cameras.	
Parameters	
<cameras>	You need to select one, many or **All Cameras** from the list.

Stop recording on <cameras>

Note: *This action can be used to stop the recording in case it is started by the action* ***Start recording on <cameras>****.*

Description	
This is an action which stops the recording (via sending MIP message "Stop recording") for the selected cameras.	
Parameters	
<cameras>	You need to select one, many or **All Cameras** from the list.

Move <hardware> to <storage>

Description	
This is an action which moves hardware to a specific storage of another Recording Server which belongs to the same site. After a move, the hardware and its devices run on the new Recording Server and all new recordings are stored into this specified server storage.	
Parameters	
<hardware>	You need to select one, many or **All Hardware** from the list. Each hardware does have a name in format **<Recording Server name> - <Hardware name>**. After a move, the hardware is renamed with the new **<Recording Server name>** as a prefix, but only in terms of rule configuration for the new actions.
<storage>	You need to select a storage from the list. ***Note***: *Only one storage must be selected in the rule configuration.*

Notes: *After a move, the rule is no longer valid, because the hardware is renamed (only in terms of rule configuration for the new actions) and the prefix contains the new* ***<Recording Server name>****.*

A hardware cannot be moved to the same or different storage on the Recording Server to whom it initially belongs.

Only hardware from one and the same Recording Server (does have the same ***<Recording Server name>*** *as a prefix) must be selected in the rule configuration.*

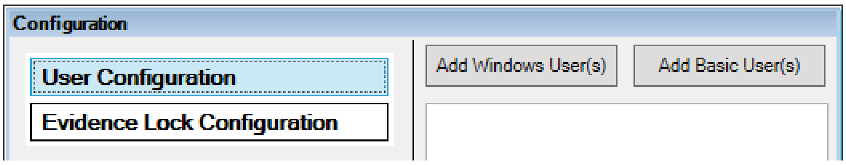
Add live permissions from <roles> on <hardware>

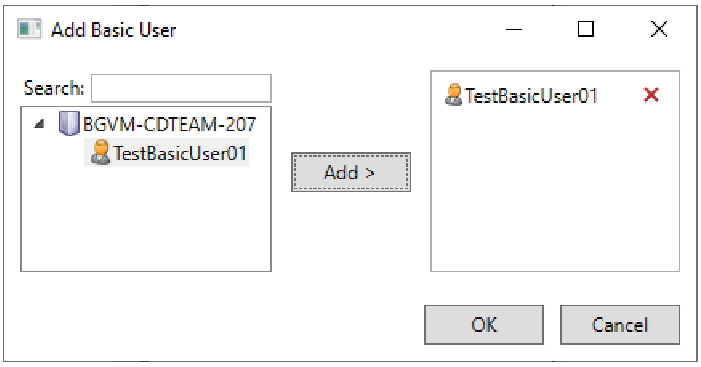
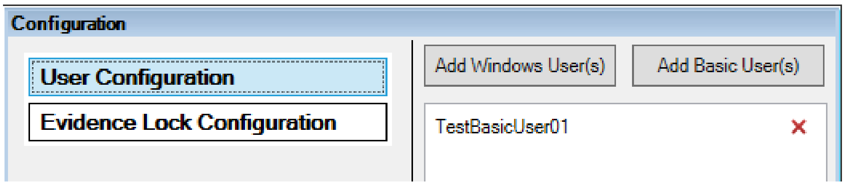
Description	
This is an action which adds **Live** permissions to selected roles for Cameras and Metadata and **Listen** permissions for Microphones, Speakers for the selected hardware.	
Parameters	
<roles>	You need to select one, many or **All Roles** from the list.
<hardware>	You need to select one, many or **All Hardware** from the list.

Remove live permissions from <roles> on <hardware>

Description	
This is an action which removes **Live** permissions from selected roles for Cameras and Metadata and **Listen** permissions for Microphones, Speakers for the selected hardware.	
Parameters	
<roles>	You need to select one, many or **All Roles** from the list.
<hardware>	You need to select one, many or **All Hardware** from the list.

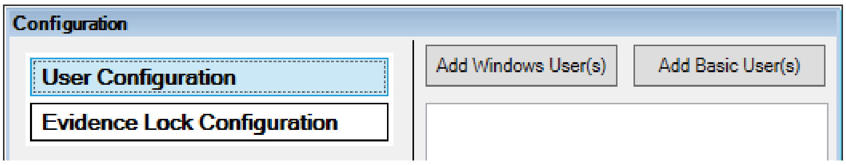
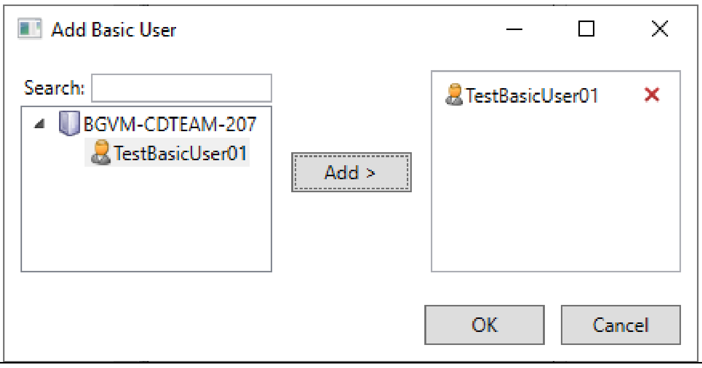
Add <user> to <role>

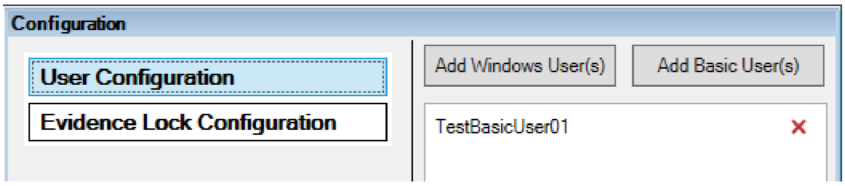
Description	
This is an action that adds a pre-defined user to a role.	
Preconditions	
Add Windows or basic user(s)	Windows or basic users must be configured before creating a rule with that action: 1. Open XProtect Management Client > **Site Navigation** > **MIP Plug-ins** > **Custom Development Actions** > **Custom Development Actions** > **User Configuration**.  Configuration User Configuration Evidence Lock Configuration Add Windows User(s) Add Basic User(s) 2. Add users based on your requirements.

	Add Windows User(s) I. Click **Add Windows User(s)**. In the **Select Users** dialog window insert one or many, Windows local and/or domain user(s). Click **OK**. II. The user(s) is added to the **User Configuration**. III. Click **Save** in the toolbar to save the configuration. **Add Basic User(s)** I. Click **Add Basic User(s)**. In the **Add Basic User** dialog window select one or many basic user(s) and click **Add >**. The **Search** option can be used to filter the results. **Example**:  Add Basic User Search: BGVM-CDTEAM-207 TestBasicUser01 Add > TestBasicUser01 OK Cancel Click **OK**. II. The user(s) is added to the **User Configuration**. **Example**:  Configuration User Configuration Evidence Lock Configuration Add Windows User(s) Add Basic User(s) TestBasicUser01 III. Click **Save** in the toolbar to save the configuration. User(s) are now available for selection when using the action **Add <user> to <role>**.
Delete user	1. Click the red cross for the selected user. 2. Click **Save** in the toolbar to confirm the deletion.
	Parameters
<user>	You need to select one user from the list.

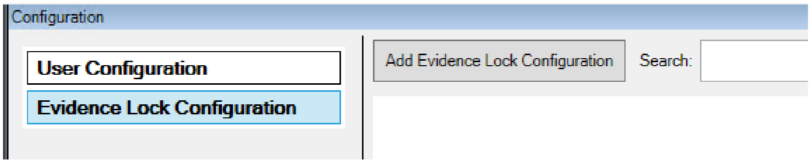
	***Note*:** *Only one user must be selected.*
<role>	You need to select one, many or **All Roles** from the list.

Remove <user> from <role>

Description	
This is an action that removes a pre-defined user from a role.	
Preconditions	
Add Windows or basic user(s)	Windows or basic users must be configured before creating a rule with that action: 1. Open XProtect Management Client > **Site Navigation** > **MIP Plug-ins** > **Custom Development Actions** > **Custom Development Actions** > **User Configuration**.  Configuration User Configuration Evidence Lock Configuration Add Windows User(s) Add Basic User(s) 2. Add users based on your requirements. **Add Windows User(s)** IV. Click **Add Windows User(s)**. In the **Select Users** dialog window insert one or many, Windows local and/or domain user(s). Click **OK**. V. The user(s) is added to the **User Configuration**. VI. Click **Save** in the toolbar to save the configuration. **Add Basic User(s)** IV. Click **Add Basic User(s)**. In the **Add Basic User** dialog window select one or many basic user(s) and click **Add >**. The **Search** option can be used to filter the results. **Example**:  Add Basic User Search: BGVM-CDTEAM-207 TestBasicUser01 Add > TestBasicUser01 OK Cancel

	Click **OK**. V. The user(s) is added to the **User Configuration**. **Example**:  Configuration User Configuration Evidence Lock Configuration Add Windows User(s) Add Basic User(s) TestBasicUser01 ✕ VI. Click **Save** in the toolbar to save the configuration. User(s) are now available for selection when using the action **Add <user> to <role>**.
Delete user	1. Click the red cross for the selected user. 2. Click **Save** in the toolbar to confirm the deletion.
Parameters	
<user>	You need to select one user from the list. ***Note***: *Only one user must be selected.*
<role>	You need to select one, many or **All Roles** from the list.

Add <evidence lock> to recording on <cameras>

Description	
This is an action that creates an **evidence lock** to a recording for specific camera(s).	
Preconditions	
Add Evidence Lock Configuration	An Evidence Lock Configuration must be created before creating a rule with that action: 1. Open XProtect Management Client > **Site Navigation** > **MIP Plug-ins** > **Custom Development Actions** > **Custom Development Actions** > **Evidence Lock Configuration**.  Configuration User Configuration Evidence Lock Configuration Add Evidence Lock Configuration Search:

2. Click **Add Evidence Lock Configuration**. This will open a dialog window with several parameters to be filled in:

   Name: Name of the evidence lock.

   Description: Description of the evidence lock.

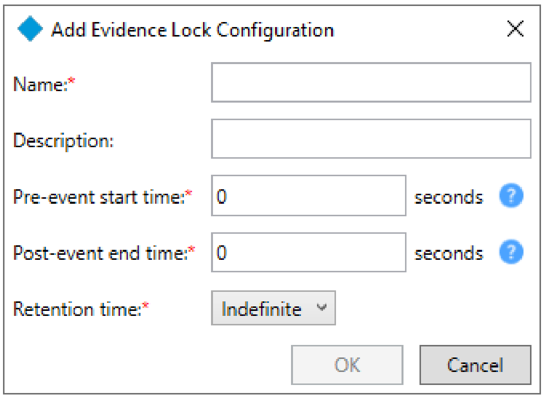
   Pre-event start time *(in seconds, min 1 / max 600)*: Select time before recording to include in the evidence lock.

   Post-event end time *(in seconds, , min 1 / max 600)*: Select time after recording to include in the evidence lock

   Retention time: Specify how long should the evidence lock be saved for. Two options are available.

   Indefinite: Select this option to save the evidence lock for indefinite period of time.

   Days: Select this option and insert value for the number of days, so the evidence lock is saved for the specified number of days.



Add Evidence Lock Configuration

Name:*

Description:

Pre-event start time:* 0 seconds

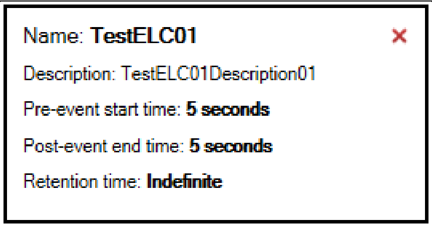
Post-event end time:* 0 seconds

Retention time:* Indefinite

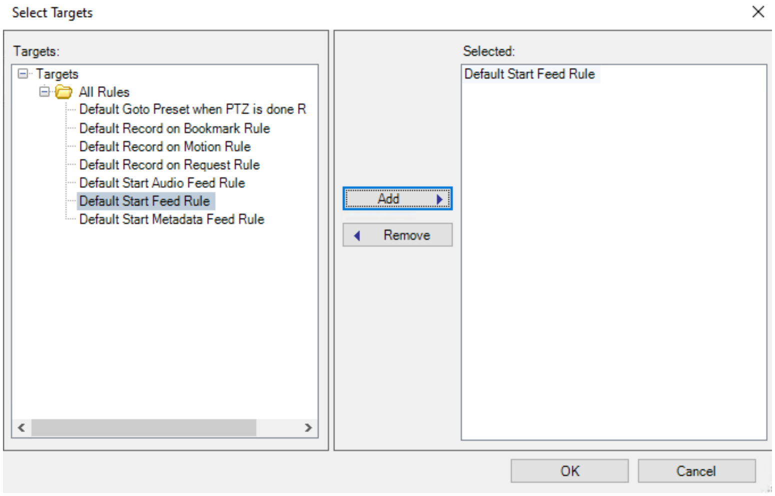
Click **OK.**

The evidence lock configuration in created.

Example:

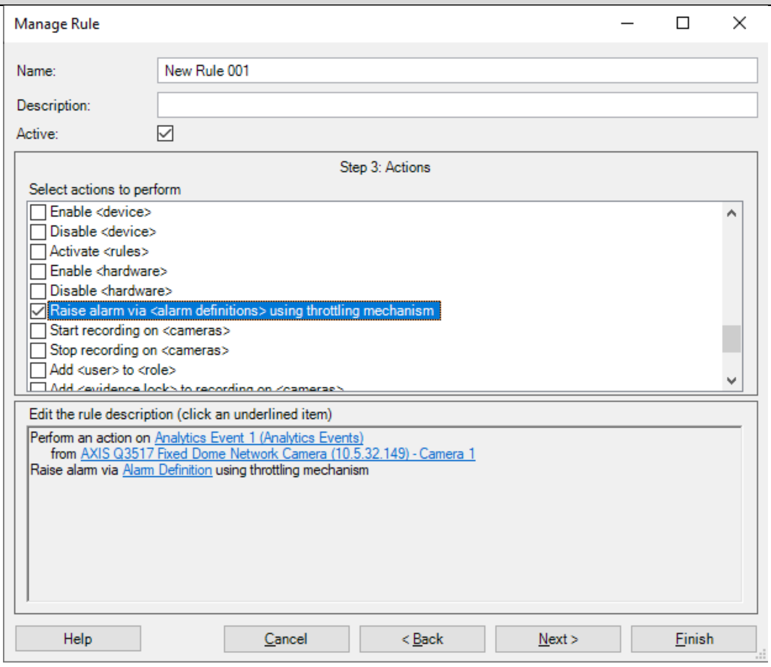
	 Name: **TestELC01** Description: TestELC01Description01 Pre-event start time: **5 seconds** Post-event end time: **5 seconds** Retention time: **Indefinite** 3. Click **Save** in the toolbar to save the configuration.
Delete Evidence Lock Configuration	1. Click the red cross in the right upper corner of the selected configuration. 2. Click **Save** in the toolbar to confirm the deletion.
Search	Type a string in the **Search** bar to filter the results.
Parameters	
<evidence lock>	Select Evidence Lock Configuration. ***Note***: *Only one Evidence Lock Configuration must be selected.*
<cameras>	You need to select one, many or **All Cameras** from the list.

Activate <rules>

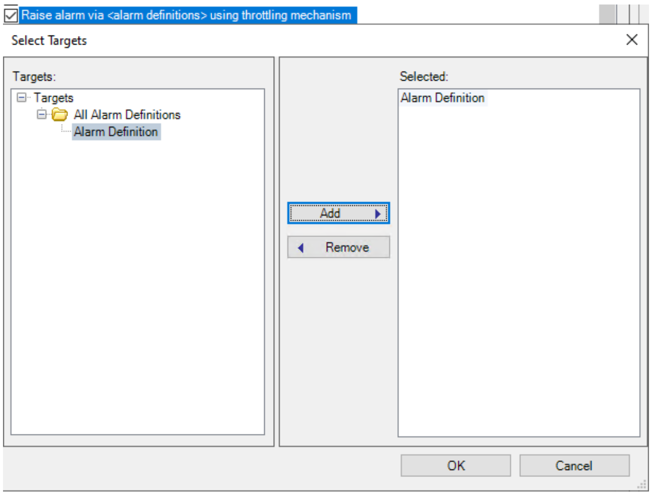
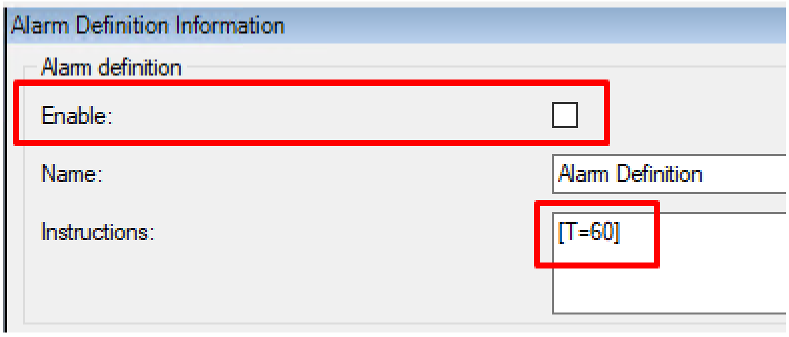
Description	
This is an action which activates another rule	
Parameters	
<rules>	Clicking on rule opens a Selected Targets window.  Selected: Default Start Feed Rule Select the rule you wish to Activate > Add > OK (rules you wish to activate must be created before the Activate <rules> rule.

Select Targets
Targets:
Targets
All Rules
Default Goto Preset when PTZ is done R
Default Record on Bookmark Rule
Default Record on Motion Rule
Default Record on Request Rule
Default Start Audio Feed Rule
Default Start Feed Rule
Default Start Metadata Feed Rule
Add
Remove
OK
Cancel

Deactivate <rules>

Description	
This is an action which deactivates another rule	
Parameters	
<rules>	 Manage Rule Name: New Rule 001 Description: Active: ☑ Step 3: Actions Select actions to perform ☐ Enable <device> ☐ Disable <device> ☐ Activate <rules> ☐ Enable <hardware> ☐ Disable <hardware> ☑ Raise alarm via <alarm definitions> using throttling mechanism ☐ Start recording on <cameras> ☐ Stop recording on <cameras> ☐ Add <user> to <role> ☐ Add <evidence lock> to recording on <cameras> Edit the rule description (click an underlined item) Perform an action on Analytics Event 1 (Analytics Events) from AXIS Q3517 Fixed Dome Network Camera (10.5.32.149) - Camera 1 Raise alarm via Alarm Definition using throttling mechanism Select the alarm which 1. Trigger and event (triggering event for the rule) Depending on the [T=20] value the throttling will not create an alarm in this period after the last created alarm.

Raise alarm via <alarm definitions> using throttling mechanism

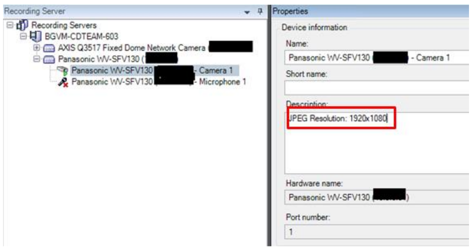
Description	
This is an action which allows the user to setup a rule that suppresses alarm	
Parameters	
<rules>	Select an alarm definition which is configured with time throttling (in seconds)  ☑ Raise alarm via <alarm definitions> using throttling mechanism Select Targets Targets: Targets All Alarm Definitions Alarm Definition Selected: Alarm Definition Add Remove OK Cancel  Alarm Definition Information Alarm definition Enable: ☐ Name: Alarm Definition Instructions: [T=60]

Preconditions for alarm throttling

Before configuring the rule Raise alarm via <alarm definitions> using throttling mechanism, the operator must configure alarm definitions in the XProtect Management Client > Alarm Definitions section, with the desired throttling time. This is done by typing the throttle interval in the description field of the alarm definition.
The format for the throttling interval is [T=60]. This format must be used.
- T - time
- 60 – value is in seconds. The value used is an example. The operator may type in any number as long as it is not a negative one.

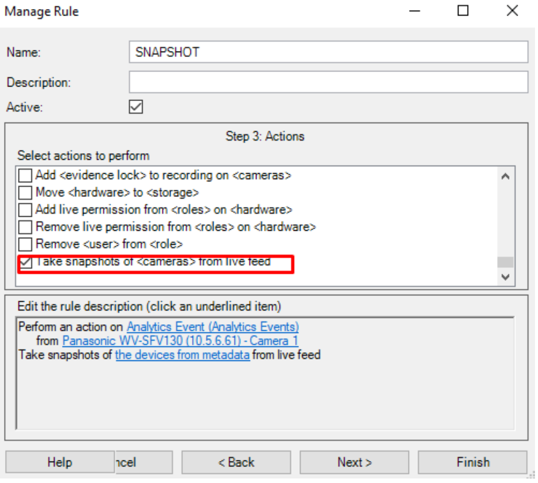
Note* It is **very important** the operator removes the checkmark next to **Enabled** in the alarm definition.
This is required only for alarms that will use throttling.

Take snapshots of <cameras> from live feed

Description	
This is an action which allows the user to setup a rule that takes a snapshot of cameras live feed	
Parameters	
<rules>	One or more cameras and at least 1 event shout be created before hand to ease the setup of the snapshot rule. Default resolution for a snapshot is 1920x1080. Take in mind that the system will upscale or downscale resolutions to keep the aspect ratio of the camera. If the user wishes to change this default resolution a string must be input in the Devices' Description field under Recording Server. It is important to note that the string is case sensitive and must be input in this exact order.  Recording Servers BGVM-CDTEAM-603 AXIS Q3517 Fixed Dome Network Camera [redacted] Panasonic WV-SFV130 ([redacted] Panasonic WV-SFV130 [redacted] - Camera 1 Panasonic WV-SFV130 [redacted] - Microphone 1 Device information Name: Panasonic WV-SFV130 [redacted] - Camera 1 Short name: Description: JPEG Resolution: 1920x1080 Hardware name: Panasonic WV-SFV130 [redacted]) Port number: 1 - If privacy masking is enabled the taken screenshot will display it. - Changing the name of the camera device may not be reflected in the following screenshots if the event server is not restarted. - Placing special characters in the camera device's name will be replaced with underscore on screenshot creation. - Default JPEG format of generated screenshot *{cameraName}_{frameTime.ToString("yyyyMMdd'T'HHmmss")}.jpg* - Default location for generating screenshots is *C:\ProgramData\Milestone\Custom Development Actions\LiveSnapshots.* - If the user wishes to change the default location for generating screenshots a SYMLINK must be done between the default location and the new one.

Example for rule Take snapshots of <cameras> from live feed

Configuration using an analitics event as the trigger to take a snapshot from the listed camera. Take in mind that all cameras group can be selected here instead of a single camera.



Manage Rule

Name: SNAPSHOT

Description:

Active: ☑

Step 3: Actions

Select actions to perform

- □ Add <evidence lock> to recording on <cameras>
- □ Move <hardware> to <storage>
- □ Add live permission from <roles> on <hardware>
- □ Remove live permission from <roles> on <hardware>
- □ Remove <user> from <role>
- ☑ Take snapshots of <cameras> from live feed

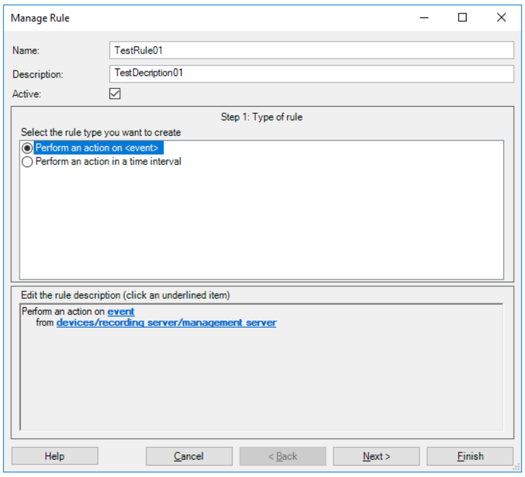
Edit the rule description (click an underlined item)

Perform an action on Analytics Event (Analytics Events)
from Panasonic WV-SFV130 (10.5.6.61) - Camera 1
Take snapshots of the devices from metadata from live feed

NOTE* If you have a failover Recording Server setup the action will function.

Example for a rule which performs Disable <hardware> action

1. Open XProtect Management Client > **Site Navigation** > **Rules and Events** > **Rules**.
2. Right click on the **Rules** > **Add Rule.**
3. In the **Manage Rule** dialog box enter valid **Name** and **Description** (not a mandatory field). Leave the **Active** checkbox enabled if you want the current rule to be created as active.



Manage Rule

Name: TestRule01

Description: TestDecription01

Active: ☑

Step 1: Type of rule

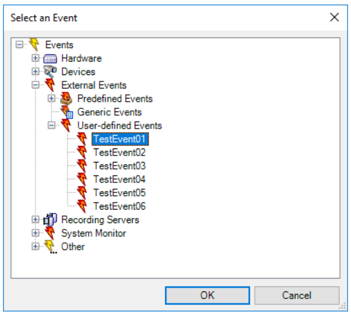
Select the rule type you want to create

- ● Perform an action on <event>
- ○ Perform an action in a time interval

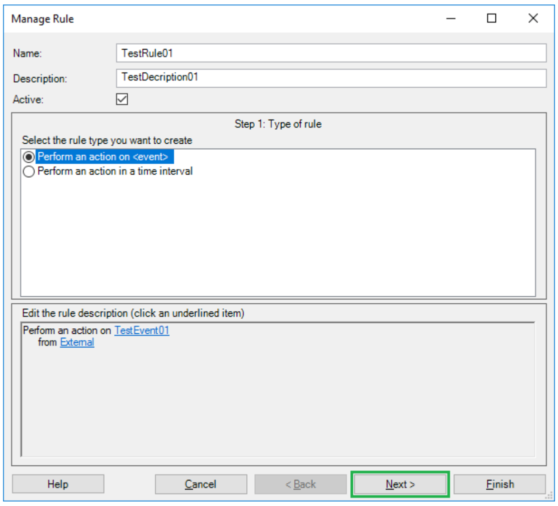
Edit the rule description (click an underlined item)

Perform an action on event
from devices/recording server/management server

4. In the **Step 1: Type of rule section**, select **Perform an action on <event>**.
5. In the **Edit the rule description section (click an underlined item)**, click **event**.
6. In the **Select an Event** dialog box that appears, expand **External Events** > **User-defined Events** and select **TestEvent01**. Click **OK**.



Click **Next**.



Name: TestRule01

Description: TestDecription01

Active: ☑

Step 1: Type of rule

Select the rule type you want to create

● Perform an action on <event>

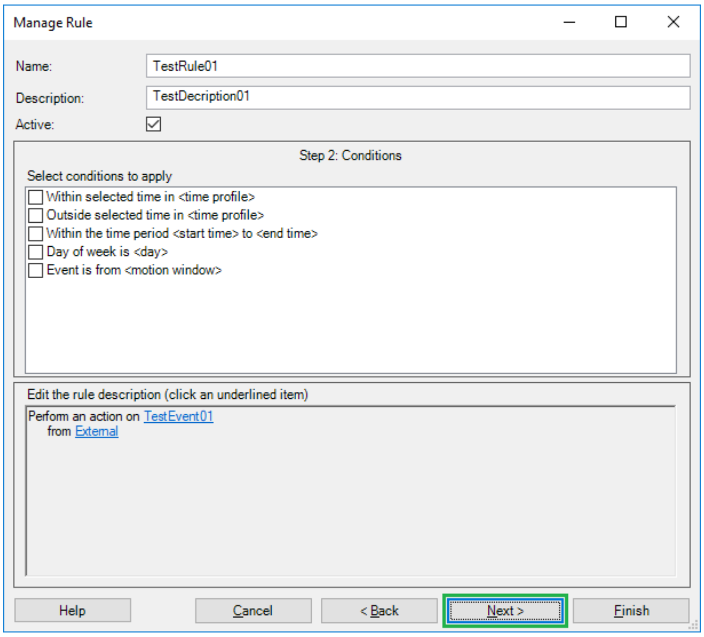
○ Perform an action in a time interval

Edit the rule description (click an underlined item)

Perform an action on TestEvent01
from External

Note*: *TestEvent01* is already created event in *Site Navigation* > *Rules and Events* > *User- defined Events.

7. In the **Step 2: Conditions sections**, you can apply any conditions. In this scenario conditions will not be applied. Click **Next.**



Name: TestRule01

Description: TestDescription01

Active: ☑

Step 2: Conditions

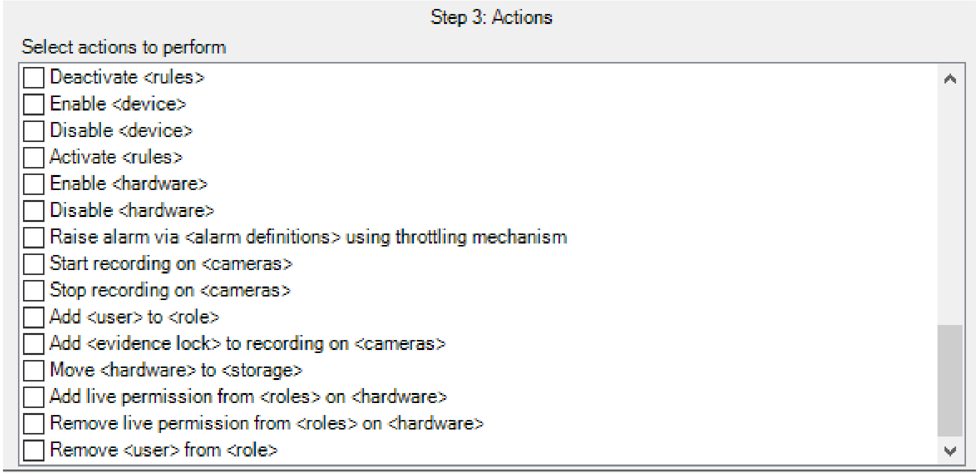
Select conditions to apply

□ Within selected time in <time profile>
□ Outside selected time in <time profile>
□ Within the time period <start time> to <end time>
□ Day of week is <day>
□ Event is from <motion window>

Edit the rule description (click an underlined item)

Perform an action on TestEvent01
from External

8. In the **Step 3: Actions** section, you will see the list with available actions, including the new actions which can be selected:
Enable <**device**>
Disable <**device**>
Enable <**hardware**>
Disable <**hardware**>
Start recording on <**cameras**>
Stop recording on <**cameras**>
Move <**hardware**> to <**storage**>
Add live permissions from <**roles**> on <**hardware**>
Remove live permissions from <**roles**> on <**hardware**>
Add <**user**> to <**role**>
Remove <**user**> from <**role**>
Add <**evidence lock**> to recording on <**cameras**>
Activate <**rules**>
Deactivate <**rules**>
Raise alarm via <**alarm definitions**> using throttling mechanism
Take snapshots of <cameras> from live feed

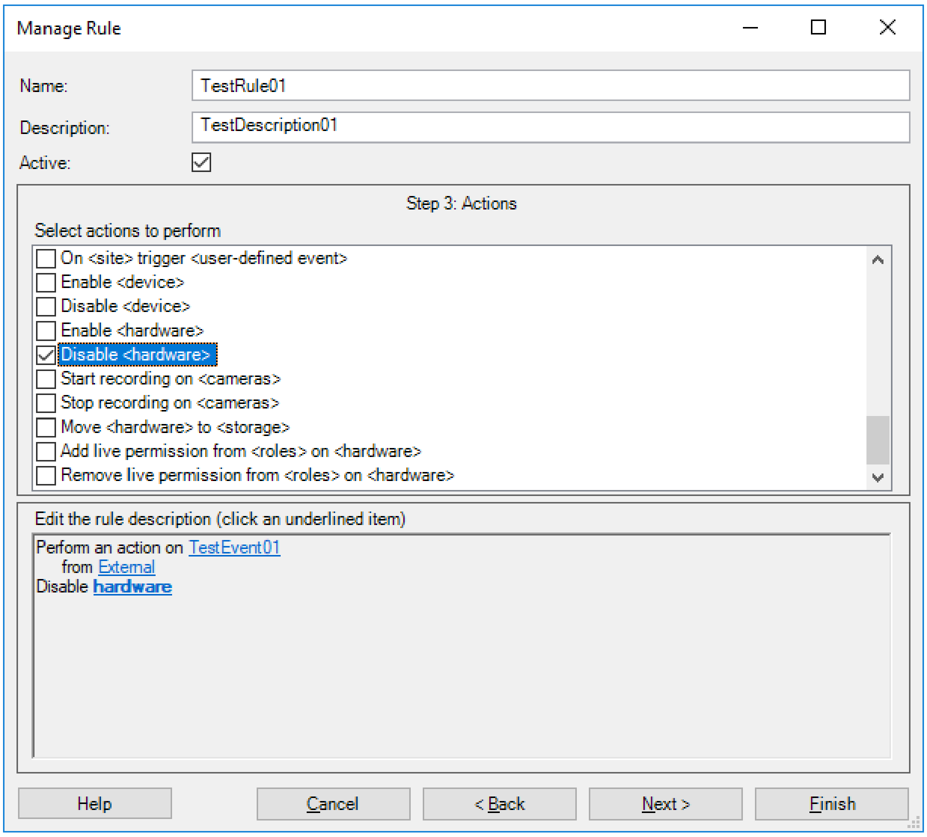


Step 3: Actions

Select actions to perform

- □ Deactivate <rules>
- □ Enable <device>
- □ Disable <device>
- □ Activate <rules>
- □ Enable <hardware>
- □ Disable <hardware>
- □ Raise alarm via <alarm definitions> using throttling mechanism
- □ Start recording on <cameras>
- □ Stop recording on <cameras>
- □ Add <user> to <role>
- □ Add <evidence lock> to recording on <cameras>
- □ Move <hardware> to <storage>
- □ Add live permission from <roles> on <hardware>
- □ Remove live permission from <roles> on <hardware>
- □ Remove <user> from <role>

9. Select **Disable <hardware>**.



Manage Rule

Name: TestRule01

Description: TestDescription01

Active: ☑

Step 3: Actions

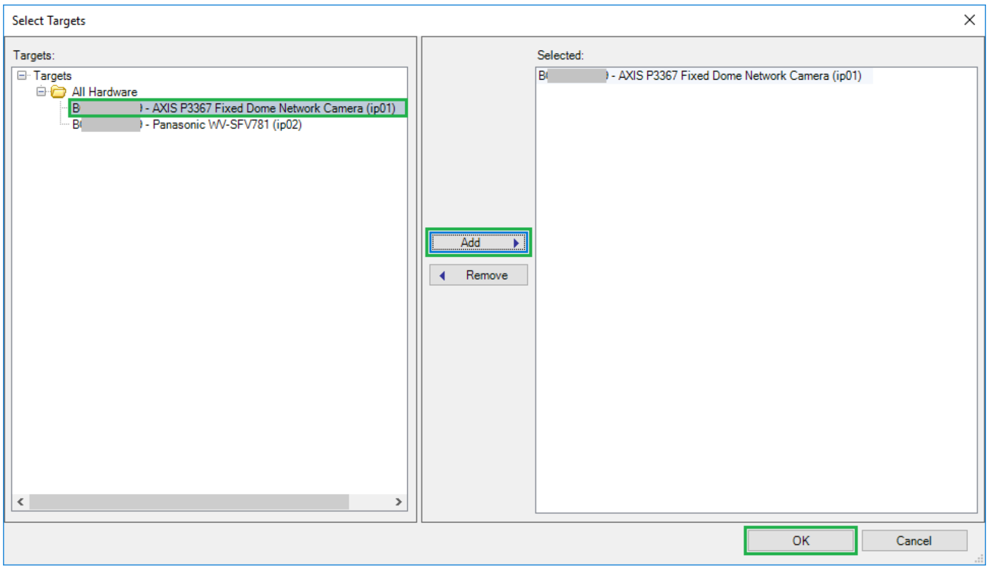
Select actions to perform

- □ On <site> trigger <user-defined event>
- □ Enable <device>
- □ Disable <device>
- □ Enable <hardware>
- ☑ Disable <hardware>
- □ Start recording on <cameras>
- □ Stop recording on <cameras>
- □ Move <hardware> to <storage>
- □ Add live permission from <roles> on <hardware>
- □ Remove live permission from <roles> on <hardware>

Edit the rule description (click an underlined item)

Perform an action on TestEvent01
from External
Disable hardware

10. In the **Edit the rule description section (click an underlined item)**, click **hardware**.
11. In the **Select Targets** dialog box, select the hardware which need to be disabled. In this scenario **BXX1 - Axis P3367 Fixed Dome Network Camera (ip01)** will be disabled. Click **Add**. Click **OK**.


Select Targets

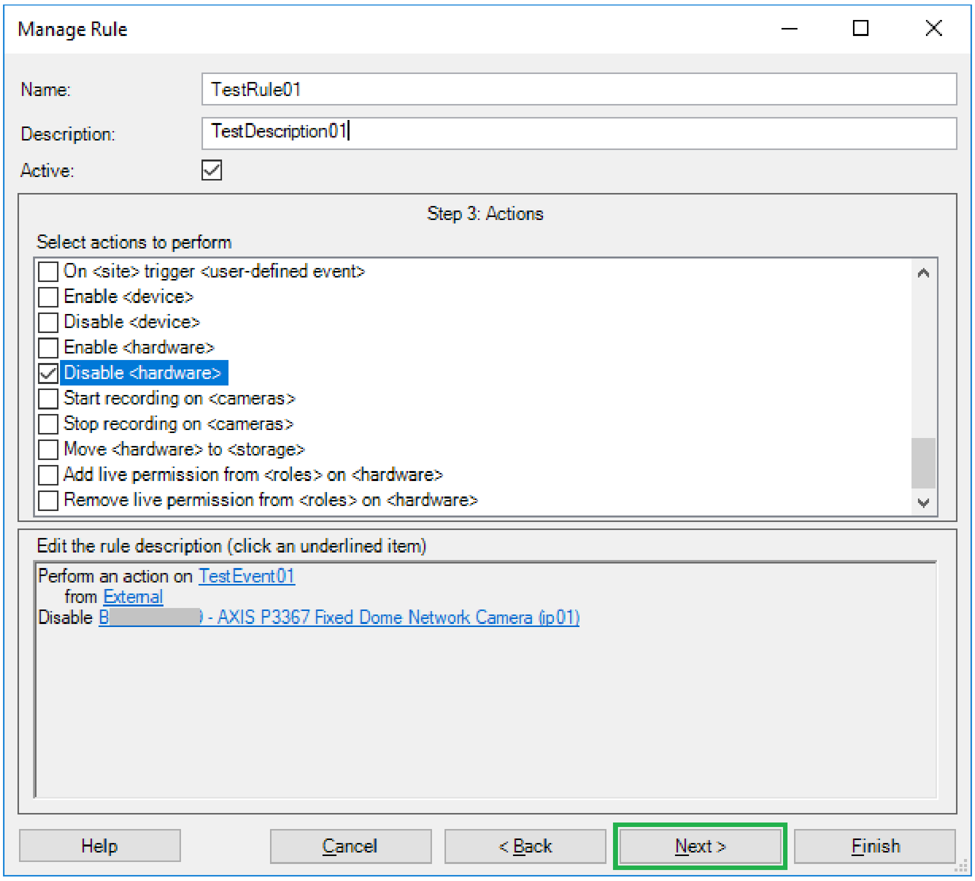
Targets:

- Targets
  - All Hardware
    - B[redacted]) - AXIS P3367 Fixed Dome Network Camera (ip01)
    - B[redacted]) - Panasonic WV-SFV781 (ip02)

Selected:

B[redacted]) - AXIS P3367 Fixed Dome Network Camera (ip01)

12. In the **Manage Rule** dialog box click **Next**.


Manage Rule

Name: TestRule01

Description: TestDescription01

Active: ☑

Step 3: Actions

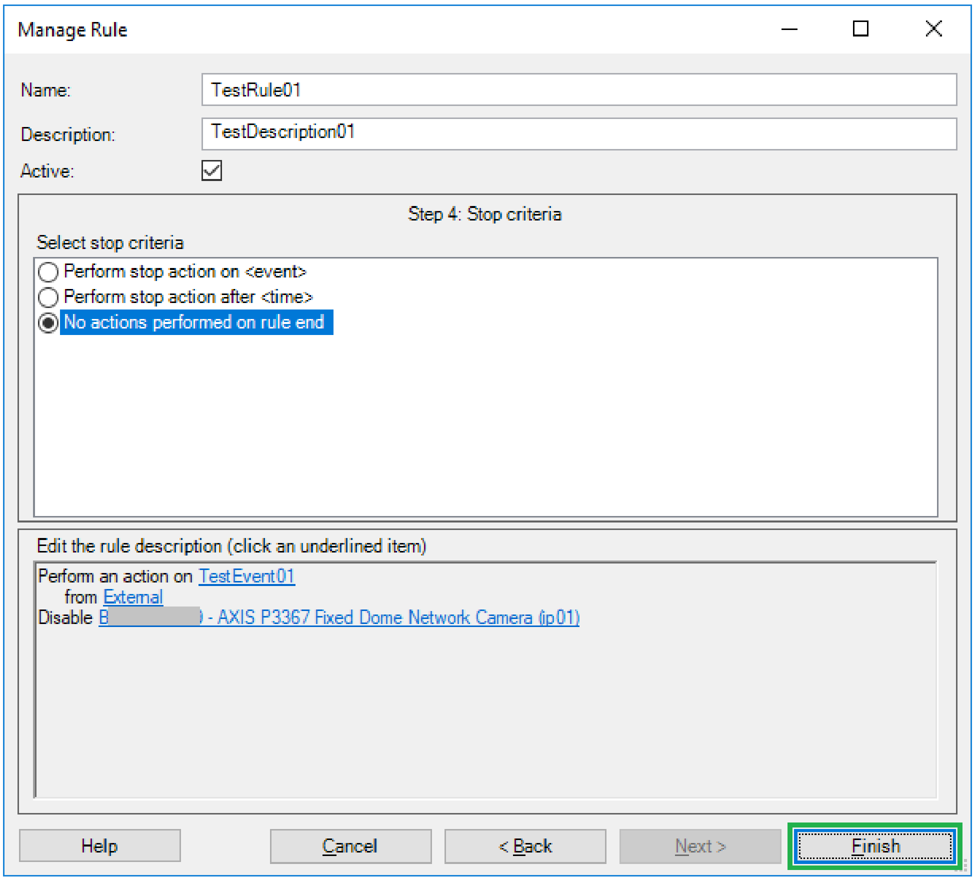
Select actions to perform

- ☐ On <site> trigger <user-defined event>
- ☐ Enable <device>
- ☐ Disable <device>
- ☐ Enable <hardware>
- ☑ Disable <hardware>
- ☐ Start recording on <cameras>
- ☐ Stop recording on <cameras>
- ☐ Move <hardware> to <storage>
- ☐ Add live permission from <roles> on <hardware>
- ☐ Remove live permission from <roles> on <hardware>

Edit the rule description (click an underlined item)

Perform an action on TestEvent01
from External
Disable B[redacted]) - AXIS P3367 Fixed Dome Network Camera (ip01)

13. In the **Step 4: Stop criteria** you can apply a criterion. It is selected **No actions performed on rule end** by default. Click **Finish**.



Manage Rule

Name: TestRule01

Description: TestDescription01

Active: ☑

Step 4: Stop criteria

Select stop criteria

○ Perform stop action on <event>

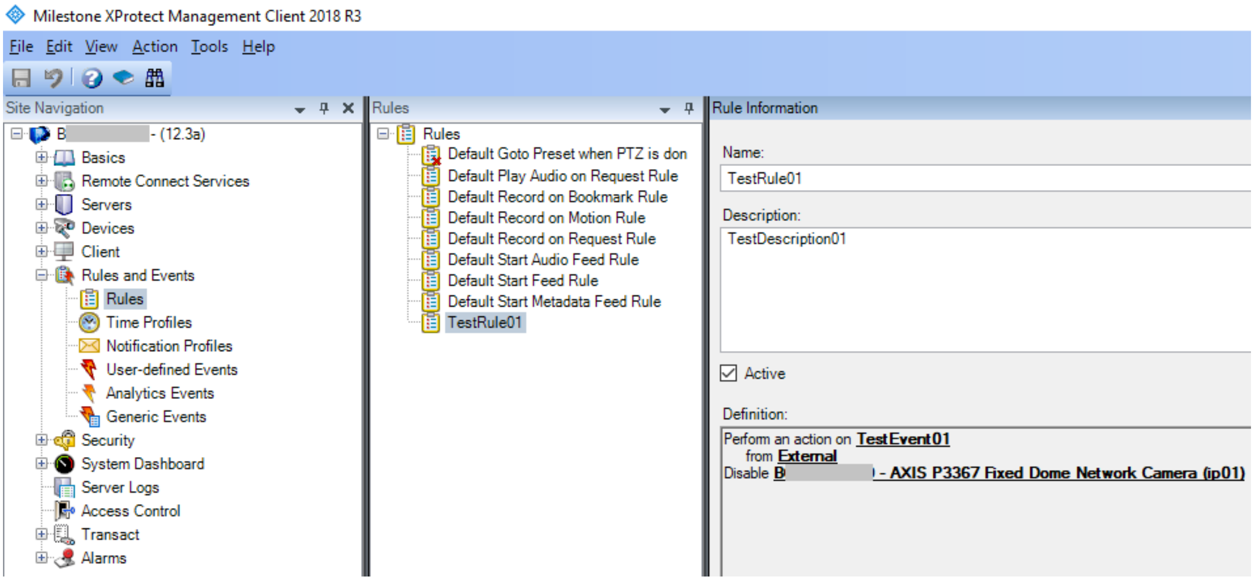
○ Perform stop action after <time>

● No actions performed on rule end

Edit the rule description (click an underlined item)

Perform an action on TestEvent01
from External
Disable B[redacted]) - AXIS P3367 Fixed Dome Network Camera (ip01)

14. Verify your new rule has the following syntax.



Milestone XProtect Management Client 2018 R3

Name: TestRule01

Description: TestDescription01

☑ Active

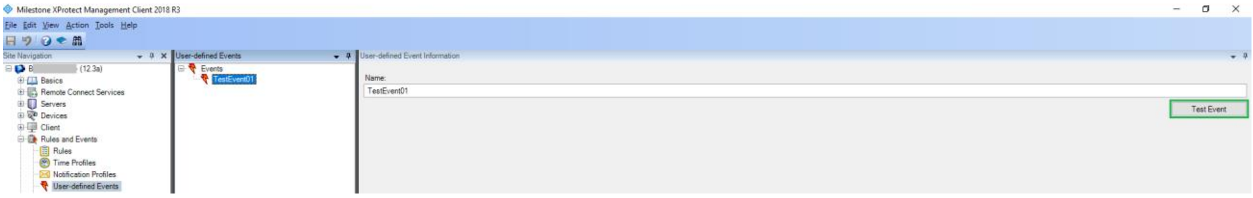
Definition:

Perform an action on **TestEvent01**
from **External**
Disable **B**[redacted] **- AXIS P3367 Fixed Dome Network Camera (ip01)**

Operation

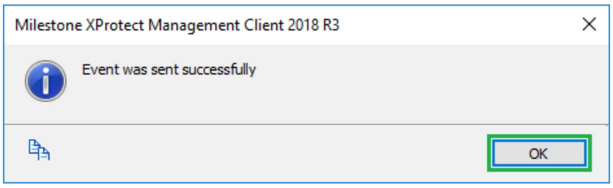
Verify the Disable <hardware> action rule is working

1. Open XProtect Management Client > **Site Navigation** > **Rules and Events** > **User-defined Events**.
2. Select **TestEvent01** from the list and click **Test Event**.



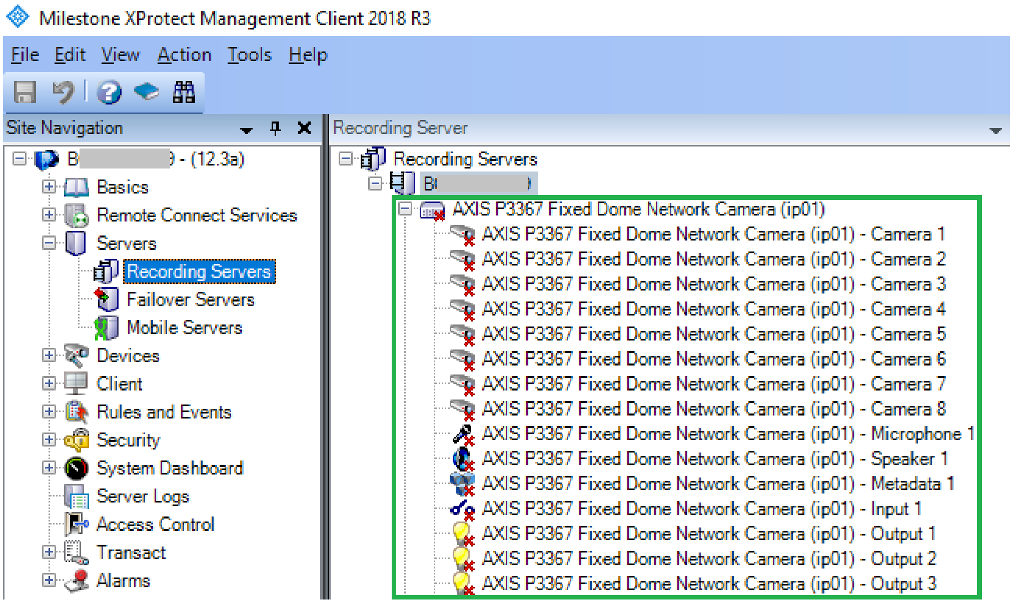
Name: TestEvent01

3. Following message will be displayed. Click **OK**.



Event was sent successfully

4. Open XProtect Management Client > **Site Navigation** > **Servers** > **Recording Servers**. In the Recording Server pane expand the current recording server and its hardware.
5. Verify that the **BXX1 - AXIS P3367 Fixed Dome Network Camera (ip01)** hardware and all its devices are in disabled state.


Milestone XProtect Management Client 2018 R3
File Edit View Action Tools Help
Site Navigation
B[redacted] - (12.3a)
Basics
Remote Connect Services
Servers
Recording Servers
Failover Servers
Mobile Servers
Devices
Client
Rules and Events
Security
System Dashboard
Server Logs
Access Control
Transact
Alarms
Recording Server
Recording Servers
B[redacted]
AXIS P3367 Fixed Dome Network Camera (ip01)
AXIS P3367 Fixed Dome Network Camera (ip01) - Camera 1
AXIS P3367 Fixed Dome Network Camera (ip01) - Camera 2
AXIS P3367 Fixed Dome Network Camera (ip01) - Camera 3
AXIS P3367 Fixed Dome Network Camera (ip01) - Camera 4
AXIS P3367 Fixed Dome Network Camera (ip01) - Camera 5
AXIS P3367 Fixed Dome Network Camera (ip01) - Camera 6
AXIS P3367 Fixed Dome Network Camera (ip01) - Camera 7
AXIS P3367 Fixed Dome Network Camera (ip01) - Camera 8
AXIS P3367 Fixed Dome Network Camera (ip01) - Microphone 1
AXIS P3367 Fixed Dome Network Camera (ip01) - Speaker 1
AXIS P3367 Fixed Dome Network Camera (ip01) - Metadata 1
AXIS P3367 Fixed Dome Network Camera (ip01) - Input 1
AXIS P3367 Fixed Dome Network Camera (ip01) - Output 1
AXIS P3367 Fixed Dome Network Camera (ip01) - Output 2
AXIS P3367 Fixed Dome Network Camera (ip01) - Output 3

***Note: Refresh** the Recording Servers if you do not see the changes.*

Troubleshooting

This section provides information, which helps the administrator solve cases where the solution fails working. For detailed troubleshooting the MIP logs should be inspected.

Case: A rule with custom action is not triggered successfully.

Cause	Action
MIP License has expired or is not activated.	First, consider re-activation of the license either online or offline. Check the license details in XProtect Management Client.

MIP Logs

Examples:

Note: BXX1 *and* ***BXX2*** *are the names of the two Recording Servers used in the examples.*

- **Enable <device >**
  2019-03-18 14:06:22.506 UTC+02:00 Info SetCamerasEnabledState Enabled state for cameras BXX1 - AXIS P3367 Fixed Dome Network Camera (ip01) - Camera 1 is set to True.

- **Disable <device>**
  2019-03-18 14:01:11.566 UTC+02:00 Info SetCamerasEnabledState Enabled state for cameras BXX1 - AXIS P3367 Fixed Dome Network Camera (ip01) - Camera 1 is set to False.

- **Enable <hardware>**
  2019-03-18 14:51:12.175 UTC+02:00 Info SetHardwareEnabledState Enabled state for hardware BXX1 - AXIS P3367 Fixed Dome Network Camera (ip01) is set to True.

- **Disable <hardware>**
  2019-03-18 14:45:41.652 UTC+02:00 Info SetHardwareEnabledState Enabled state for hardware BXX1 - AXIS P3367 Fixed Dome Network Camera (ip01) is set to False.

- **Start recording on <cameras>**
  2019-03-20 19:26:55.489 UTC+02:00 Info StartRecording Recording of cameras(BXX1 - AXIS P3367 Fixed Dome Network Camera (ip01) - Camera 1) was started.

- **Stop recording on <cameras>**
  2019-03-18 16:00:25.138 UTC+02:00 Info StopRecording Recording of cameras(BXX1 - AXIS P3367 Fixed Dome Network Camera (ip01) - Camera 1) was stopped.

- **Move <hardware> to <storage>**
  2019-03-19 14:05:23.543 UTC+02:00 Info MoveHardware Hardware BXX1 - AXIS P3367 Fixed Dome Network Camera (ip01) was moved to BXX2 - Local Default.

- **Add live permissions from <roles> on <hardware>**
  2019-03-18 18:09:36.023 UTC+02:00 Info SetHardwareLivePermission Live permission for Roles(TestRole01) is set to True for Hardware(BXX1 - AXIS P3367 Fixed Dome Network Camera (ip01))

- **Remove live permissions from <roles> on <hardware>**
  2019-03-18 18:15:12.638 UTC+02:00 Info SetHardwareLivePermission Live permission for Roles(TestRole01) is set to False for Hardware(BXX1 - AXIS P3367 Fixed Dome Network Camera (ip01))

- **Add <user> to <role>**
  2021-07-22 13:08:51.365 UTC+03:00 Info Add/RemoveUserFromRole User: TestUser01 was added to Role: TestRole01

- **Remove <user> from <role>**
  2021-07-22 13:02:25.885 UTC+03:00 Info Add/RemoveUserFromRole User: TestUser01 was removed from Role: TestRole01

- **Add <evidence lock> to recording on <cameras>**
  2021-08-16 091227.866 UTC+0200 Info EvidenceLockHelper Adding evidence lock TestELC01 resulted in Success
- **Activate <rules>**
  2023-01-30 14:18:25.231 UTC+02:00 Info SetRuleEnabledState Enabled state for Default Start Feed Rule changed to True
- **Deactivate <rules>**
  2023-01-30 14:24:15.138 UTC+02:00 Info SetRuleEnabledState Enabled state for Default Start Feed Rule changed to False
- **Take snapshots of <cameras> from live feed**
  2024-04-26 11:54:35.587 UTC+03:00 Info CreateLiveSnapshot New job for creation of live snapshots for 1 received.
  2024-04-26 11:54:35.714 UTC+03:00 Info CreateLiveSnapshot Successfully saved snapshot of camera Panasonic WV-SFV130 (10.5.6.61) - Camera 1 at C:\ProgramData\Milestone\Custom Development Actions\LiveSnapshots\Panasonic WV-SFV130 (10.5.6.61) - Camera

Limitations

Move <hardware> to <storage>

- Only one storage must be selected in the rule configuration.
- After a move, the rule is no longer valid, because the hardware is renamed (only in terms of rule configuration for the new actions) and the prefix contains the new <Recording Server name>.
- A hardware cannot be moved to the same or different storage on the Recording Server to whom it initially belongs.
- Only hardware from one and the same Recording Server (does have the same <Recording Server name> as a prefix) must be selected in the rule configuration.

Add <user> to <role>

- Only one user must be selected when creating/configuring the rule.

Remove <user> from <role>

- Only one user must be selected when creating/configuring the rule.

Add <evidence lock> to recording on <cameras>

- Only one Evidence Lock Configuration must be selected when creating/configuring the rule.

Activate <rules> / Deactivate <rules>

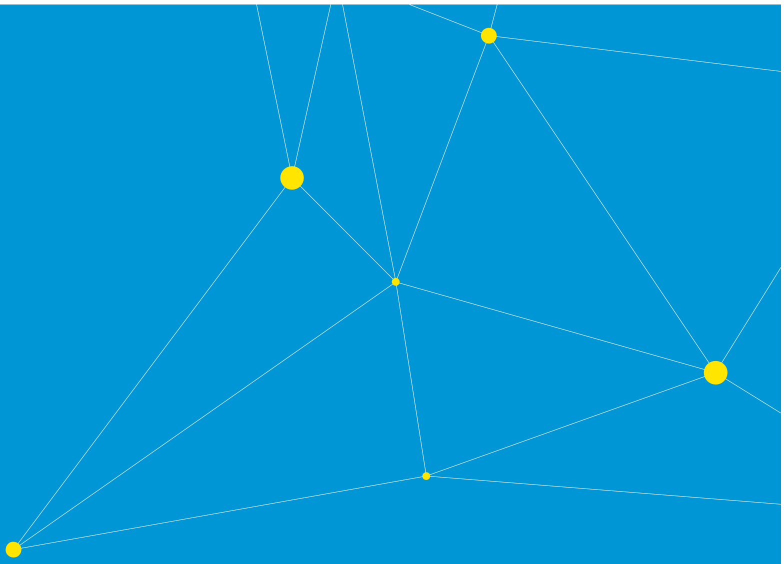
- will only be able to list and show Rules which are using built-in Actions and NOT Custom Development Actions.

Loading issue

- In rules selection list. When selecting a newly created rule, there might me delay in displaying that new event. Refresh Management Client

Known issues

There are no known issues at the time of the release.



Milestone Systems is a leading provider of open platform video management software; technology that helps the world see how to ensure safety, protect assets and increase business efficiency. Milestone enables an open platform community that drives collaboration and innovation in the development and use of network video technology, with reliable and scalable solutions that are proven in more than 150,000 sites worldwide. Founded in 1998, Milestone is a stand-alone company in the Canon Group.