

MAKE THE
WORLD SEE

Milestone Systems

XProtect® Hospital Assist

Installation and Configuration



Contents

- Copyright, trademarks, and disclaimer** 4
- Introduction** 5
 - XProtect Hospital Assist 5
 - What's new 5
- Licenses** 6
 - License overview 6
 - Activating licenses 6
- Setting up the features on the Hospital Assist node** 7
 - Associate cameras with XProtect Hospital Assist 7
 - Configure the Privacy Blur timer 7
 - Set up Sticky Note categories 8
- Setting up Fall Detection** 9
 - Setting up the Fall Detection app 9
 - The Fall Detection app 10
 - The Processing Server 10
 - Secure the connections between the XProtect VMS and the Processing Server 10
 - Install a self-signed CA certificate 11
 - Running the Fall Detection deployment scripts 11
 - Create a basic user for the Processing Server 12
 - Prerequisites for running the deployment scripts 13
 - Script 1: Creating and provisioning a virtual machine and install the Ubuntu Server software 16
 - Script 2: Configuring the system and deploying the Processing Server on the Ubuntu Server computer 21
 - Connecting the Processing Server to XProtect 25
 - Using Portainer 25
 - Monitor the health of the Processing Server 26
 - Preparing the Fall Detection app for use in XProtect 26
 - Configuring the Fall Detection app 27
 - Enable the Fall Detection app 27
 - Setting up exclusion zones 27
 - Adjusting person and fall detection confidence 28

Enabling the analytics from the Fall Detection app and disabling service mode	30
Create an alarm based on a fall detection event	30
Test the fall detection event in XProtect Smart Client	30
Enable desktop and sound notifications in XProtect Smart Client	30
Troubleshooting	32

Copyright, trademarks, and disclaimer

Copyright © 2023 Milestone Systems A/S

Trademarks

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

Microsoft and Windows are registered trademarks of Microsoft Corporation. App Store is a service mark of Apple Inc. Android is a trademark of Google Inc.

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

Disclaimer

This text 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 reserves the right to make adjustments without prior notification.

All names of people and organizations used in the examples in this text 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 system installation folder.

Introduction

This guide details and explains how to install and configure XProtect Hospital Assist as an add-on to your Milestone XProtect VMS installation.

The guide also includes a detailed description of how to deploy and set up the Fall Detection app as part of the XProtect Hospital Assist installation and configuration.

XProtect Hospital Assist

XProtect Hospital Assist is designed exclusively for hospital units caring for patients in need of 24/7 or situational observation.

This add-on to the main XProtect VMS products is a dedicated solution to remotely monitor patients which allows the hospital to:

- Increase staff efficiency.
- React to incidents rapidly.
- Provide high-quality patient care.

XProtect Hospital Assist is compatible with XProtect VMS 2023 R1 or later.

What's new

In this initial release, XProtect Hospital Assist includes:

- Sticky Notes with associated Sticky Note categories to allow hospital staff to add non-sensitive patient information to cameras in XProtect Smart Client that monitors patients and create different categories for the Sticky Notes.
- Privacy Blur in XProtect Smart Client to give patients privacy for a fixed number of minutes. A Privacy Blur timer counts down the time when the Privacy Blur is lifted.
- Fall Detection which can detect when people have fallen and send alarms to XProtect Smart Client. Two scripts help you configure and deploy Fall Detection.

Licenses

XProtect Hospital Assist and its features are not visible in XProtect VMS until you activate its licenses.

Read this section to learn which license types you need and in what order you need to activate them.

License overview

To use XProtect Hospital Assist and all its features, you must have the following licenses:

License	Description
A base license for your XProtect VMS	This base license activates the XProtect VMS product.
Device licenses for all devices to use in XProtect VMS	One device requires one device license. All camera devices that you want to use with your system must have a device license. Speakers, microphones, or input and output devices attached to your cameras do not require device licenses.
A base license for the XProtect Hospital Assist add-on	This base license activates XProtect Hospital Assist on top of your XProtect VMS product.
Camera licenses for all cameras associated with XProtect Hospital Assist	To use Sticky Notes, Privacy Blur, and Fall Detection on cameras that monitor patients, you must activate camera licenses on the cameras that you are associating with XProtect Hospital Assist. Similar to the general device licenses, one camera license is required for one XProtect Hospital Assist camera.

Activating licenses

Your license file includes all the license types mentioned in the table above. You must activate this license to enjoy all features of XProtect Hospital Assist. If you leave your system and devices in grace period, you cannot use the XProtect Hospital Assist features.

Similar to other XProtect products, you can activate the license online or offline. For more information about license activation, see the Licensing section in the [XProtect VMS Administrator manual](#).

Setting up the features on the Hospital Assist node

When you have activated your XProtect Hospital Assist license, you see the **Hospital Assist** node on the **Site Navigation** pane in XProtect Management Client.

On the **Hospital Assist** node, you can:

- Associate cameras with XProtect Hospital Assist camera licenses.
- Configure the Privacy Blur timer used for Privacy Blur in XProtect Smart Client.
- Add, edit, or delete Sticky Note categories for Sticky Notes in XProtect Smart Client.

Associate cameras with XProtect Hospital Assist

When you have activated your software license for XProtect Hospital Assist, you must add the cameras to associate with the XProtect Hospital Assist licenses. Milestone recommends that you add all cameras that you want to associate with XProtect Hospital Assist to a camera group. This allows you to associate all the relevant cameras at the same time instead of associating them with the licenses individually. Each camera takes up a separate camera license.

To add the cameras to associate with XProtect Hospital Assist:

1. On the **Hospital Assist** tab, click **Add**.
2. In the **Select camera** window, click through the folder structure to locate the camera group, then click **OK**. The selected cameras on the camera group is now activated for XProtect Hospital Assist.



You can keep adding cameras, provided that you have unassigned licenses available. You can always remove cameras that have already been added, then add a new camera again. Removing a camera frees up its license and you can use it to add a different camera.

By default, the available cameras are divided into groups, indicated in the folder structure. To add cameras one-by-one, clear the **Group Hierarchy** check box in the **Select camera** window to view the full list of available cameras.

Configure the Privacy Blur timer

You can use Privacy Blur on activated XProtect Hospital Assist cameras.

Privacy Blur is a feature that users of XProtect Smart Client can use to give patients privacy by blurring the camera image halfway or entirely for a specific amount of time. An example can be blurring the camera image at the same time as a patient uses the restroom.

On the **Privacy Blur** tab, you can configure how long time the Privacy Blur can be active in XProtect Smart Client until it is removed automatically:

- In the text field on the **Privacy Blur** tab, click the up or down arrows to add or reduce the number of minutes Privacy Blur can be active before it is automatically removed.

You can select values from one to 9999 minutes. By default, the Privacy Blur timer is set to five (5) minutes.

Set up Sticky Note categories

You can use Sticky Notes on activated XProtect Hospital Assist cameras.

Sticky Notes is a feature where users of XProtect Smart Client can add information as an overlay to the camera image, for example, to provide non-sensitive patient information.

To give XProtect Smart Client users a way to present different types of Sticky Notes, you can create Sticky Note categories. You must give each Sticky Note category its own name and a unique color, so that the XProtect Smart Client users can tell the different categories apart from each other.

To add Sticky Note categories:

1. On the **Sticky Notes** tab, in the right-side column, click **Add**.

In the **Add new category** window that opens, type a **Name** for the sticky note category.

2. Choose a color for the new sticky note category, then click **Add**. The new category is now added to the **Category** list.

When you add a new Sticky Note category, the category is enabled by default. Clear the **Enabled** check box if you want to disable it.



XProtect Hospital Assist includes two default Sticky Note categories: **General** and **Warning**. You can edit or remove the **Warning** category if you want to, but you cannot remove the **General** category.



You can have up to seven sticky note categories.

Setting up Fall Detection

Setting up the Fall Detection app

To install and configure the Fall Detection app, and connect it to your XProtect VMS, you must complete a number of steps.

What	Why
Activate all the cameras that you want to associate with XProtect Hospital Assist	The Fall Detection app only works on cameras that you have associated with an XProtect Hospital Assist license. See Licenses on page 6
Check the prerequisites to running the scripts	Before you run the deployment scripts, consult the Prerequisites for running the deployment scripts on page 13 to see if your system is ready to run the scripts.
Run deployment script 1: provision-hyper-v-machine.ps1	This script creates a new virtual machine with Ubuntu Server 22.04. Use this virtual machine as your Processing Server for the Fall Detection app. See Script 1: Creating and provisioning a virtual machine and install the Ubuntu Server software on page 16 .
Run deployment script 2: configure-system-and-deploy-processing-server.ps1	This script sets up the Processing Server on the Ubuntu Server computer and to the Fall Detection app on the Processing Server. See Script 2: Configuring the system and deploying the Processing Server on the Ubuntu Server computer on page 21 .
Configure the Fall Detection app on cameras in XProtect Management Client	Enable and configure the Fall Detection app on each camera that you have associated with XProtect Hospital Assist. See Preparing the Fall Detection app for use in XProtect on page 26 .
Set up events and alarms in XProtect Management Client	Configure the events and alarms so that when the system detects a fall, it triggers an alarm to the healthcare staff in the Alarm Manager in XProtect Smart Client. See Configuring events .
Activate all the cameras that you want to associate with XProtect Hospital Assist	The Fall Detection app only works on cameras that you have associated with an XProtect Hospital Assist license.

The Fall Detection app

The Fall Detection app is designed to observe people's movement in a hospital environment. You can use it to detect when people are lying down in hospital wards and to inform XProtect Smart Client operators of the falls.

The purpose of using the Fall Detection app is to help hospital staff respond fast when people have fallen in hospital wards, and to ensure the safety and comfort of the people who are being monitored.



Milestone has done extensive testing to ensure the accuracy and reliability of the Fall Detection component of XProtect Hospital Assist. However, Milestone makes no guarantee, express or implied, that this product will detect a patient fall. As with any other AI-based technology, the performance of the fall detection alerts depends on a number of factors, including, but not limited to, the environment, light, camera angle, and distance of the camera to the object.

The Processing Server

The Processing Server acts as a bridge between installations of XProtect Video Management Software (VMS) and the Fall Detection app. It enables the communication and exchange of information between the two types of applications.

The Processing Server forwards video streams from cameras added to the Fall Detection app and enables this application to send the analytics results back to the XProtect VMS as data (events, metadata, and video).

The Processing Server sends continuous video streams from the cameras in your XProtect system to the Fall Detection app. The Fall Detection app analyzes the streams and, if a person has fallen over, triggers an event in XProtect. You have the option to configure alarms that appear in XProtect Smart Client.

When you have installed the Processing Server, you can configure and set up the Fall Detection app from the XProtect Management Client's **Processing servers** node.



You see the **Processing servers** node in XProtect Management Client when you have successfully added the Processing Server to the XProtect VMS and installed the Processing Server plugin for XProtect Management Client.

Secure the connections between the XProtect VMS and the Processing Server



You can run XProtect Hospital Assist on an encrypted or non-encrypted connection. This section is only relevant if you want to run your system on an encrypted connection.

Before encrypting the connection to and from the Processing Server, you must have already enabled encryption and installed the necessary certificates on the management server.

To connect securely to the Processing Server:

1. Install the public Certificate Authority (CA) certificate on the Ubuntu Server computer.
2. Create an SSL certificate for the Processing Server.
3. Install the SSL certificate on the Processing Server.

During the deployment of the Processing Server, you must connect to the management server through HTTPS and upload the public CA certificate and the SSL certificate for the Processing Server.

Related resources:

- To enable encryption on the management server, see the [XProtect Administrator manual](#)
- To generate and install certificates manually, see the [XProtect VMS certificates guide](#)

Install a self-signed CA certificate

When you run the script, it deploys a self-signed Certificate Authority (CA) certificate. This certificate encrypts the connection between the Processing Server services.



The script generates the self-signed certificate regardless of the communication protocol used between the Processing Server and the management server.

1. Copy the **public-authority-[Ubuntu Server IP].cer** file from your computer to the computers that will use XProtect Management Client to manage the Processing Server.
2. Right-click the server certificate and select **Install Certificate**.
3. In the **Certificate Import** wizard, select **Local Machine** as the certificate store.
4. Select **Next** to continue.
5. Select **Place all certificates in the following store** and specify a folder.
6. Select **Browse**, and then **Trusted Root Certification Authorities**.
7. Select **OK** and **Next**.
8. When in the **Certificate Import Wizard** window, select **Finish**.
 - If you receive a security warning that you are about to install a root certificate, select **Yes** to continue.
 - If the import has succeeded, a confirmation window is displayed.
9. Verify that the server certificate is listed in the center view of the **Trusted Root Certification Authorities** subtree.

Running the Fall Detection deployment scripts

To set up Fall Detection for your XProtect Hospital Assist installation, you must run two PowerShell scripts in the sequence which will:

- Create a virtual machine on the host machine (through Hyper-V)
- Assign a GPU from the host machine to the virtual machine
- Install Ubuntu Server 22.04 on the virtual machine
- Install the Processing Server on the virtual machine
- Install the Fall Detection functionality.

Name	Details
provision-hyper-v-machine.ps1	<p>Run this script to create a new virtual machine with Ubuntu Server 22.04.</p> <p>The virtual machine takes ownership of one or more Graphic Processing Units (GPU)s from the host machine . The GPU allows the Processing Server to do video analytics.</p>
configure-system-and-deploy-processing-server.ps1	<p>Run this script to set up the Processing Server on the virtual machine and to set up and configure the Fall Detection app on the Processing Server.</p>



Run the **provision-hyper-v-machine.ps1** PowerShell script before you run the **configure-system-and-deploy-processing-server.ps1** script.


Create a basic user for the Processing Server

You must create a new basic user for the Processing Server to use when logging in to the XProtect VMS. Milestone recommends that the new basic user is only used for your Fall Detection setup.



You must add the basic user to the Administrator role in XProtect Management Client.

1. Select **Site Navigation > Security > Basic Users**.
2. In the **Basic Users** pane, right-click and select **Create Basic User** and specify a user name and password.

 The password must meet the complexity defined in the appsettings.json file for your XProtect VMS. See [Configure login settings for basic users](#). See the section about creating basic users in your [XProtect VMS administrator manual](#).

3. Clear the **Force Basic User to change password on next login** check box because the Processing Server cannot change the password when logging in.
4. Keep the **Enabled** status of the basic user and select **OK** to create the basic user.
5. To add the basic user to the Administrator role, select **Site Navigation > Security > Roles**.
6. Select the **Administrators** role and then the **User and Groups** tab.
7. Select **Add** and then **Basic user**.
8. Select the user you just created and select **OK**.

Now you can configure the Processing Server to log in to your XProtect VMS.

Prerequisites for running the deployment scripts

The deployment scripts help you install, set up, and configure the Processing Server and the Fall Detection app in your XProtect Hospital Assist setup.

This page lists a number of necessary steps to complete/consider before you run the installation scripts.

BIOS

What	Details
Enable virtualization and GPU passthrough in BIOS	Enable the following settings: <ul style="list-style-type: none"> • Intel VT for Directed I/O (VT-D) • Trusted Execution Technology (TXT) • ASPM (Active State Power Management) or PCI Express Native Power Management (to increase system performance) • Single root I/O virtualization (SR-IOV)
Disable Secure Boot (recommended)	Secure Boot may prevent the NVIDIA GPU driver from running. To disable Secure Boot, see https://learn.microsoft.com/en-us/windows-hardware/manufacture/desktop/disabling-secure-boot

Hardware

What	Details
Memory	You must allocate at least 12 GB of RAM to the virtual machine for optimal performance on the virtual machine. You decide on how much RAM to allocate when you run the scripts.
Hard disk space	You must allocate at least 100 GB of hard disk space to the virtual machine. You decide on how much hard disk space to allocate when you run the scripts.

NVIDIA Graphics Processing Unit (GPU)

What	Details
NVIDIA GPU Model	<p>You must have an NVIDIA GPU on the host machine. Milestone recommends that you use an NVIDIA RTX A2000 12 GB GPU, which can host 10 cameras running fall detection.</p> <p>Your host machine must have an NVIDIA GPU with capability 6.0 (Pascal) or later installed.</p>
NVIDIA driver installation	<p>Install the NVIDIA drivers on the host machine before you run the script. The script does include NVIDIA drivers, so you can include those.</p> <p>If you do not install the driver supplied by the script or have a valid NVIDIA driver installed, the script will fail and exit the process.</p>

Network

What	Details
Internet connection	As part of the deployment script process, you install Ubuntu Server 22.04 on a virtual machine. If you have internet access on this server, the script can download the Ubuntu installer automatically.

What	Details
	<p>If the server does not have internet access, you must download the installer yourself from the Ubuntu website, then copy it to the host machine before running the script.</p>

Operating system

What	Details
Windows Server version	<p>The scripts can only run on Windows Server 2019 or 2022.</p>
Install Hyper-V on your Windows Server 2019 or 2022 installation	<p>You need Hyper-V to create the virtual machine running the Processing Server.</p> <p>To learn how to install Hyper-V on your computer, go to https://learn.microsoft.com/en-us/windows-server/virtualization/hyper-v/get-started/install-the-hyper-v-role-on-windows-server.</p>
Download Ubuntu Server 22.04 (optional)	<p>The Processing Server runs on Ubuntu Server 22.04. During the configuration, you can choose the script to download the image file for the operating system or browse for the image file on your computer.</p> <p>The Ubuntu Server 22.04 image file is available at https://ubuntu.com/download/server</p>

User rights in XProtect VMS

What	Details
Create a basic user with administrator rights	<p>You must create a basic user in XProtect VMS and give this basic user administrator rights.</p> <p>The basic user must have access to the cameras that you have associated with XProtect Hospital Assist.</p>

What	Details
	User names can contain spaces but not special characters such as , @.
Install certificates for the Processing Server (optional)	If you want to encrypt the connection between the management server and the Processing Server, you need certificates. See Secure the connections between the XProtect VMS and the Processing Server on page 10
Create a device group (optional)	If you have a large installation and want to limit the number of cameras that you want to use with the Fall Detection app, you can create a device group. You specify the name of the device group during the deployment of the Processing Server.


XProtect Management Client

What	Details
Install the Microsoft Edge WebView2 application to view web pages inside XProtect Management Client	Install the Microsoft WebView2 application on all computers using XProtect Management Client to manage the Processing Server. You can download the installer from https://developer.microsoft.com/en-us/microsoft-edge/webview2/ .

Script 1: Creating and provisioning a virtual machine and install the Ubuntu Server software

When you run the **provision-hyper-v-machine.ps1** PowerShell script, you must first make some initial selections before the rest of the installation completes automatically.

Find a description of the installation steps in the table below.

What	Description	Options/results
<p>Are you running the script as a system administrator?</p>	<p>You need to run the script as an administrator to complete the steps in the script.</p>	<p>If you run the script as an administrator, you can proceed to the script's welcome text.</p> <div data-bbox="946 454 1386 813" style="border: 1px solid #c00; background-color: #f9cb9c; padding: 10px; margin: 10px 0;">  <p>If you have not run the script as an administrator, you cannot proceed and the script stops running.</p> </div> <p>To run the script as an administrator, exit the window, then in the folder where you have saved the script files, right-click the script file, and select Run as Administrator to run the script again.</p>
<p>Which Windows Server version are you running?</p>	<p>The script checks if you have Windows Server 2019 or 2022 installed. You must run one of these versions of Windows Server for the script to continue.</p>	<ul style="list-style-type: none"> • If you have a valid Windows Server version, the PowerShell script continues to the next step. • If you do not have a valid Windows server version, the script stops running, and you cannot proceed.
<p>Have you enabled Hyper-V?</p>	<p>You must enable Hyper-V on your Windows Server computer to create the virtual machine.</p>	<ul style="list-style-type: none"> • If you have enabled Hyper-V on your Windows Server computer, the script continues to the next step.

What	Description	Options/results
		<ul style="list-style-type: none"> If you have not enabled Hyper-V on your Windows Server computer, the script stops running, and you cannot proceed. Enable Hyper-V, then run the script again.
<p>Do you have an existing Processing Server?</p>	<p>The script checks if you have already created a Processing Server.</p> <ul style="list-style-type: none"> If you have no existing Processing Server, the script continues to the next step. If you have an existing Processing Server, you are asked if you want to overwrite it or not. 	<p>Y/N</p> <ul style="list-style-type: none"> Y = You remove the existing Processing Server and create a new one. N = You keep the existing Processing Server.
<p>How much memory do you want to allocate to the virtual machine?</p>	<p>You must assign an amount of memory to the virtual machine. Milestone recommends that you use at least 12 GB (12888 MB) of memory for the virtual machine.</p>	<ul style="list-style-type: none"> Type a whole number to specify how much memory you want to assign to the virtual machine. Press Enter to use the default value (12888 MB).
<p>How much hard disk space do you want to allocate to the virtual machine?</p>	<p>You must assign some hard disk space to your virtual machine. Milestone recommends that you use at least 100 GB of hard disk space for the virtual machine.</p>	<ul style="list-style-type: none"> Type a whole number to specify how much memory you want to assign to the virtual machine. Press Enter to use the default value (100 GB).
<p>The virtual hard disk is created</p>	<p>Your virtual hard disk is being created.</p> <p>The folder for the virtual hard disk is C > ProgramData > Microsoft > Windows > Virtual Hard Disks.</p>	<p>Wait for the step to complete.</p>

What	Description	Options/results
<p>Select a virtual switch to connect to the network</p>	<p>You must select the virtual switch that you want to use to connect to the network.</p> <p>You see only external switches on the list. The script lists the names of the switches as a numbered list.</p>	<ul style="list-style-type: none"> • If the script cannot detect any virtual switches, you cannot proceed and the script exits the installation process. • If the script detects at least one virtual switch, you must select which virtual switch to use. Type the number that corresponds to the virtual switch or press Enter to use the default script's virtual switch. • If you type an invalid number or something that is not a whole number, the script shows an error message.
<p>Download Ubuntu Server to your computer or install an offline version</p>	<p>Depending on your system setup, you must choose to either download an .iso image file of Ubuntu Server 22.04 or install an offline .iso image file.</p>	<p>Y/N</p> <ul style="list-style-type: none"> • If you type Y, the script downloads the .iso image file from the Ubuntu website. The image file is around 1.5 GB in size, so the download takes a few moments to complete. • If you type N, the script prompts you for a path to the offline .iso file.
<p>The new virtual machine is created</p>	<p>The script allocates the Graphic Processing Unit (GPU) to the virtual machine.</p> <p>In addition, it runs a number of commands to complete the setup of the virtual machine:</p> <ol style="list-style-type: none"> 1. Set-VM -Name \$VMName -AutomaticStopAction Turnoff 	<p>The script configures the settings that are necessary to set up the virtual machine for use.</p>

What	Description	Options/results
	<ol style="list-style-type: none"> 2. Set-VM -Name \$VMName - GuestControlledCacheTypes \$true 3. Set-VM -Name \$VMName - LowMemoryMappedIoSpace 3Gb 4. Set-VM -Name \$VMName - HighMemoryMappedIoSpace 33280Mb 5. Set-VMDvdDrive -VMName \$VMName ControllerNumber 1 -Path \$ISOPath 6. Set-VMProcessor -VMName \$VMName -Count 4 -Reserve 10 -Maximum 65 -RelativeWeight 500 7. Set-VMemory -VMName \$VMName - DynamicMemoryEnabled \$false 	<ol style="list-style-type: none"> 1. TurnOff turns off the Automatic Stop Action setting on the virtual machine to prevent Hyper-V from going into a Save state which does not work when you enable GPU passthrough. 2. Enables Write-Combining on the CPU. 3. Defines the 32-bit memory mapped I/O (MMIO) space. 4. Defines the greater than 32-bit MMIO space. 5. Defines the path to the Ubuntu installation ISO file. 6. Define the number of CPUs to use for the virtual machine. 7. Turns off Dynamic Memory on the virtual machine.
<p>Choose a GPU for the virtual machine step 1: Do you have any NVIDIA drivers installed?</p>	<p>You must assign at least one GPU from the Windows Server computer to the virtual machine to make it the Processing Server and to use the Fall Detection's video analytics.</p> <p>The script first checks if you have at least one NVIDIA GPU driver installed on your Windows Server computer.</p>	<p>If you do not have at least one NVIDIA GPU driver installed on your Windows Server computer, the script stops running. Install an NVIDIA driver for your GPU, then run the script again.</p>
<p>Choose a GPU to use for the virtual machine step 2: NVIDIA driver</p>	<p>If the script has found at least one NVIDIA GPU driver on your Windows Server computer, the script displays a list of available drivers.</p>	<ul style="list-style-type: none"> • The script suggests using the first NVIDIA GPU driver on the list.

What	Description	Options/results
status	The script runs a check to look for available GPU drivers to assign to the virtual machine.	<ul style="list-style-type: none"> If no driver is available, an error message is displayed and the installation is aborted.
Choose a GPU to use for the virtual machine step 3: Assigning the devices to the virtual machine	The selected devices are assigned to the virtual machine from the Windows Server computer.	Wait for the step to complete.
The virtual machine is started	The virtual machine is started and Ubuntu Server 22.04 is installed on that machine. The installation completes and the virtual machine has been rebooted, you have reached the end of the script.	<p>An installation window for Ubuntu Server opens.</p> <p>Follow the instructions on the screen.</p>
Ubuntu Server is installed	<p>You must enter the user name and password for the virtual machine's administrator account, then configure the network connection settings.</p> <p>All additional steps of the Ubuntu Server software installation takes place automatically.</p>	<p>The installation of the Ubuntu Server software on the virtual machine has completed.</p> <p>You can now run the second installation script.</p>


You are now ready to run the **configure-system-and-deploy-processing-server.ps1** script to configure the system and set up the Processing Server.

Script 2: Configuring the system and deploying the Processing Server on the Ubuntu Server computer

You can run the **configure-system-and-deploy-processing-server.ps1** PowerShell script on any computer that meets the system requirements. To learn more about system requirements, see [Prerequisites for running the deployment scripts on page 13](#).

Milestone recommends that you run the script on the computer where you deployed the Ubuntu Server computer.

Find a description of the installation steps in the table below.

What	Description	Options/results
<p>Are you running the script as a system administrator?</p>	<p>You need to run the script as an administrator to complete the steps in the script.</p>	<p>If you run the script as an administrator, you can proceed to the script's welcome text.</p> <div data-bbox="887 454 1386 734" style="border: 1px solid #ccc; background-color: #f9e79f; padding: 10px; margin: 10px 0;">  <p>If you have not run the script as an administrator, you cannot proceed and the script stops running.</p> </div> <p>To run the script as an administrator, exit the window, then in the folder where you have saved the script files, right-click the script file, and select Run as Administrator to run the script again.</p>
<p>Connect to the Ubuntu Server computer</p>	<p>Specify the address, user name, and password of the Ubuntu Server computer.</p>	<p>When you connect to the Ubuntu Server computer successfully, you see information about that computer, such as host name, operating system, architecture, and other details.</p>
<p>Which NVIDIA GPU drivers do you want to use with XProtect Hospital Assist?</p>	<p>The script detects the GPUs on the Ubuntu Server computer and shows a list of compatible drivers.</p>	<p>Select a driver to install on the Ubuntu Server computer that is compatible with your NVIDIA GPU. Milestone recommends that you select the NVIDIA-525-server driver.</p> <p>If the driver is recognized, the script moves to the next step.</p>
<p>Deploy the Processing Server</p>	<p>The script installs Ansible and copies the Ansible playbook to the Ubuntu Server computer.</p>	<p>If you have selected a new driver, the Ubuntu Server computer restarts. When the process is complete, the script prepares the</p>

What	Description	Options/results
	<p>The Ansible playbook contains instructions to:</p> <ul style="list-style-type: none"> • Stop the Processing Server and the Fall Detection services in case they have been installed before • Upload the Processing Server and the Fall Detection images to the Ubuntu Server computer • Start Docker Compose using the uploaded images • Start the Processing Server and Fall Detection services • Install Portainer 	<p>Processing Server and the Fall Detection app for configuration.</p> <p>Then, the script moves to the next step.</p>
<p>Which NVIDIA GPUs do you want to use?</p>	<p>Select one or more NVIDIA GPUs to use for the Fall Detection app.</p> <p>You can select multiple NVIDIA GPUs to share the load of the Fall Detection app's streams.</p>	<p>When you select the NVIDIA GPUs, the script moves on to the next step.</p>
<p>What is the address of the management server?</p>	<p>Enter the address of the management server in the format http://[computer name].[domain name] or https://[computer name].[domain name], depending on the level of encryption needed on the</p>	<p>When you provide the address of the management server and import the certificates, the script moves to the next step.</p>

What	Description	Options/results
	<p>system.</p> <p>If you have selected HTTPS, you must provide the public CA certificate for the VMS and an SSL certificate for the Processing Server.</p>	
<p>Where do you want to save the self-signed CA certificate?</p>	<p>The script generates a self-signed CA certificate to encrypt the connection between the Processing Server services.</p> <p>Press any key to save the self-signed CA certificate to your computer.</p> <p>You must install this certificate on all computers using XProtect Management Client to manage the Processing Server. See Install a self-signed CA certificate on page 11.</p>	<p>The script saves the certificate at the selected location and moves to the next step.</p>
<p>Which user do you want the Processing Server to use to connect to the XProtect VMS?</p>	<p>Specify the user name and password of a user that belongs to the Administrator role in XProtect.</p>	<p>If the credentials are correct, the script continues to the next step.</p>
<p>Which device group do you want to use with XProtect Hospital Assist? (optional)</p>	<p>Specify the name of the device group you created for XProtect Hospital Assist or leave it blank to include all cameras.</p>	<p>Once you press Enter, the script moves to the next step.</p>
<p>What password do you want to use for</p>	<p>The script installs Portainer and</p>	<p>The script creates the Portainer account and finishes the configuration of the</p>

What	Description	Options/results
Portainer?	<p>creates a user name 'admin'. You set the option for this user name.</p> <p>The password must be at least 12 characters long and meet the listed password requirements.</p>	<p>Processing Server.</p> <p>A Hospital Assist server appears under Processing Servers in XProtect Management Client.</p>

If you experience any errors or you want to change your selections, you can run the script again at any time.

You are now ready to go to XProtect Management Client to configure the Fall Detection app for XProtect Hospital Assist.

Connecting the Processing Server to XProtect

When the deployment scripts are run, you must log in to the XProtect Management Client with the basic user you created earlier in the setup process. A Processing servers node should be visible from the XProtect Management Client's **Site Navigation** pane.

You can now access [Portainer](#) to monitor the status of your Processing Server or move directly to [configuring the Fall Detection app](#) through the **Processing servers** node.

Using Portainer

Portainer is a container management system from which you can manage the Processing Server services. You can learn more about Portainer at <https://www.portainer.io/>

XProtect Hospital Assist uses the Community Edition of Portainer.

Use Portainer to:

- Monitor the health of the services.
- Restart the services.
- Obtain logs.

During the deployment of the **Processing Server**, the script installs Portainer and creates the user name **admin**. You must set the password for this user name.

Portainer does not need an internet connection to be able to run.

- To open Portainer, go to the **Servers** node in XProtect Management Client and select **Processing Servers > Hospital Assist**.

Monitor the health of the Processing Server

The Processing Server consists of services called containers. If one or more containers stop running, the Fall Detection app may not work properly.

You can monitor the status of the containers from XProtect Management Client using Portainer. To learn more about Portainer, see [Using Portainer on page 25](#).

1. Expand **Processing Servers** and select **Hospital Assist**.
2. Log in with your user name and password for Portainer.
3. On the **Home** page, under **Environments**, select **primary**.
4. Select **Containers**. If all containers have a state **running**, your Processing Server is working as expected. If any of the containers has stopped, contact Milestone support.

Preparing the Fall Detection app for use in XProtect

This section details what you must do inside the XProtect Management Client when both scripts have run, the Processing Server has been created, and the Fall Detection app has been deployed.

To finalize the setup of the Fall Detection app:

Step	Name	Description
1	Configure the Fall Detection app	Set up detection zones on your cameras and decide on the confidence level for detecting people and people who have fallen.
2	Create an alarm and a triggering event in XProtect Management Client.	Create an alarm that triggers the fall detection event. The event is only available in the system when all previous configurations have been done.
3	Send test events to XProtect Smart Client	Before you release the AI-based Fall Detection to the healthcare staff, you can test that you can send a successful event to XProtect Smart Client.
4	Enable desktop and sound notifications in XProtect Smart Client	Enabling desktop and sound notifications will help alerting healthcare staff about detected falls.

Configuring the Fall Detection app

You can enable and use the Fall Detection app immediately after the script has installed this app to your system. However you should spend some time to configure the app and optimize its settings to fit the use on each camera that you are running Fall Detection on.

The app contains a number of threshold value sliders to help you determine how confident the Fall Detection app's settings must be before it detects that a person is a person, a fall is a fall, and the time between when fall detection events are sent to XProtect.

There are default settings for the threshold values, but you should test out the threshold values before you start using the app in XProtect Smart Client.

Remember that you must adjust the Fall Detection app's settings separately for each camera associated with XProtect Hospital Assist.

Enable the Fall Detection app

1. In the XProtect Management Client, on the Site Navigation tab, go to **Servers > Recording Servers**, then select the relevant camera in the **Recording Server** window.

Remember that you must have activated the camera with an XProtect Hospital Assist camera license to use it with the Fall Detection app.

2. In the **Properties** window, under the **Processing settings** sections, under **App subscriptions**, select the **Hospital Assist subscription**, then go to the **Processing server** tab located in the bottom right-hand corner.

Next, you should set up and adjust the configuration of the Fall Detection app before enabling it to send streams. **Stream status** should say **Waiting** and **Analytics status** should say **Disabled**. The camera image shown is bordered by a blue outline.


Setting up exclusion zones

Below the camera image, you can set up exclusion zones for areas where you don't want any fall detection to take place. This can, for example, be areas where people normally do not appear.

You can add up to 10 exclusion zones of up to 14 vertices. When you mark these exclusion zones, the analytics from the Fall Detection app do not analyze data in these areas. You can remove exclusion zones again if you do not need them.

There are four buttons you can use to define the exclusion zones:

Button	Description
Draw	Manually draw the exclusion zones on the camera image. In this mode, you can also drag and drop specific exclusion zones in a different window. To do that, you must click on an area and then drag the selection to the other window.
Select	Allows you to delete a specific highlighted exclusion zone.
Remove selected	Removes the selected exclusion zones.
Remove all	Deletes all exclusion zones, including existing zones (if they have already been saved).


 Every time you create or remove existing exclusion zones, you must save by clicking the **Save** button located in the bottom area of the view.


Adjusting person and fall detection confidence

The fall detection app's analytics analyzes the camera image to recognize people and people falls in the areas of the camera image that have not been added to an exclusion zone.

Below the buttons where you define the exclusion zones, you can adjust the threshold values for **Analytics thresholds** and **Event timers**.

The **Analytics thresholds** determine when the analytics should detect people and people having fallen in the camera image.

Name	Description
Person Detection Confidence	<p>Sets the minimum required trust necessary for the analytics to detect an object as a person.</p> <div style="background-color: #e6f2ff; padding: 10px; border: 1px solid #0070c0;">  The lower you set the value, the greater the risk of getting a false positive, for example, detecting an inanimate object as a person. </div>

Name	Description
Fall Detection Confidence	<p>Sets the minimum required confidence level for the analytics to determine that a person has fallen.</p> <div style="border: 1px solid #0070C0; padding: 5px; background-color: #E6F2FF;">  <p>The lower you set the value, the greater the risk that a person has not fallen over but is instead in a different body position.</p> </div>

Clicking the **Set recommended threshold values** button moves the sliders to the recommended values at which the sliders should be most efficient to not trigger too many false positives/negatives.

- If you get too many false positives, consider increasing the confidence value or the sliders.
- If you get too many false negatives, consider lowering the confidence value for the sliders.

The **Event Timer** threshold values determine the time that must pass before a fall is reported and the interval between fall detection events.

Name	Description
Delay Time	<p>The minimum amount of time in seconds needed for the event state to be maintained in order for it to be reported.</p> <p>For example, if you set Delay Time threshold values to two seconds and the Fall Detection app detects a fall, the fallen state need to be maintained for two seconds before the system reports a fall detection event.</p>
Cooldown Time	<p>The minimum amount of time in seconds between reported events.</p> <p>For example, if you set Cooldown Time threshold values to three seconds, the system can report a next fall three seconds after the previous fall detection event.</p>



Every time you update the **Analytics** threshold values or change the events timers, you must save by clicking the **Save** button located in the bottom area of the view.

Enabling the analytics from the Fall Detection app and disabling service mode

When you have set up the fall detection's threshold values, the next step is to disable service mode.

- Click the blue button to disable service mode.

When service mode is disabled, the analytics from the Fall Detection app are now enabled and the streams will be sent to the Processing Server.

The next step is test the fall detection event in XProtect Smart Client.

Create an alarm based on a fall detection event

1. On the **Site Navigation** pane in the XProtect Management Client, go to **Alarms > Alarm Definitions**.
2. Right-click on **Alarm Definitions**, then select **Add New** to open the **Alarm Definition Information** window.
3. Select **Enable** to enable the alarm on your system.
4. Give the alarm a name, for example, Fall Detection.
5. In the **Triggering Event** fields in the **Trigger** section, select **Analytics Event** and **Fall Detection**.
6. In the **Sources** fields, select the cameras where the notifications can be sent from.
7. Save the event.

Test the fall detection event in XProtect Smart Client

To test that you have set up the event properly, you must first open XProtect Smart Client to set it up for the test, then return to the Fall Detection app:

1. Open and log in to XProtect Smart Client
2. Go to the **Alarm Manager** tab, then enter setup mode by clicking the **Setup** button on the upper-right side.
3. In the **Quick Filters** section of the **Alarm Manager** tab, click **All Events**.
4. In the **Data Source** drop-down list, select the fall detection event.
5. Return to the **Fall Detection** app in the XProtect Management Client and click **Send Test Event** button.
6. Go to XProtect Smart Client to see if a fall detection event is triggered.

Enable desktop and sound notifications in XProtect Smart Client

When you are satisfied with the event, you should enable desktop notifications for the healthcare staff so that they receive notifications on their desktop and a sound notification is played when a fall detection event has triggered.

1. In the Management Client **Site Navigation** pane, go to **Alarms > Alarm Data Settings**.
2. On the **Alarms Data levels** tab in the **Configuration** window, select the alarm data level you want desktop notifications for.
3. Then, go to **Alarms > Sound Settings** and enable sound notifications.
4. In the **Site Navigation** pane, go to **Smart Client profiles**, then locate the Smart Client profile for your healthcare staff.
5. On the **Alarm Manager** tab, select **Yes** for the properties **Show desktop notifications for alarms** and **Play sound notifications for alarms**.

A desktop notification is now displayed when a Fall Detection event has been triggered and a sound notification will also be played.

Troubleshooting

Issue	Solution
<p>I cannot add any cameras on the Hospital Assist tab in the Healthcare node</p>	<p>You haven't activated your license file. When your XProtect VMS and its devices are running in a grace period, you can't access any of the XProtect Hospital Assist features. Activate your license, then try again.</p>
<p>I can't see the current GPU and CPU load on the Processing Server in the XProtect Management Client. Where can I find this information?</p>	<p>To see the loads on CPU and GPU, you must log in to your host machine and run commands from Command Prompt in Windows.:</p> <ul style="list-style-type: none"> • The current CPU load: <pre>ssh abcd@IP address "top -b -n 1 -o %CPU head -n 20"</pre> • The current GPU load: <pre>ssh abcd@IP Address "nvidia-smi -q -d UTILIZATION"</pre> <p>In the above, "abcd" represents the user name and "[IP address]" is the IP address of the Processing Server.</p> <p>Both commands prompt you for a password when you run them.</p>
<p>I can't complete all steps in one of the PowerShell script used for installing/deploying the components needed for the Fall Detection app. What has gone wrong?</p>	<p>All steps in the scripts are detailed in these two topics, including what may make the script stop running before it is complete. See</p> <ul style="list-style-type: none"> • Script 1: Creating and provisioning a virtual machine and install the Ubuntu Server software on page 16 <p>or</p> <ul style="list-style-type: none"> • Script 2: Configuring the system and deploying the Processing Server on the Ubuntu Server computer on page 21.
<p>Why is the Processing server node and tab not available?</p>	<p>You have connected the Processing server to your XProtect VMS and you have installed the XProtect Processing Server Admin Plugin, but there is still no Processing Server node and tab in XProtect Management Client.</p> <p>The Processing Server and your computer with XProtect Management Client are likely not on the same network or domain.</p> <p>To fix it, add the IP address and the host name of the Processing Server to the hosts file on the computer with XProtect Management Client.</p>

Issue	Solution
<p>Where do I find log files for the Processing Server?</p>	<p>During the installation, upgrade, or uninstallation of the XProtect Processing Server Admin Plugin for XProtect Management Client (VideoOS.ProcessingServer.Plugin.Admin.Installer.exe), log entries are written to the XProtect Processing Server PluginI.log file that you can find in the C:\ProgramData\Milestone\Installer folder.</p>
<p>I can't see the current GPU and CPU load on the Processing Server in the XProtect Management Client. Where can I find this information?</p>	<p>To see the loads on CPU and GPU, you must log in to your host machine and run commands from Command Prompt in Windows.:</p> <ul style="list-style-type: none"> • The current CPU load: <code>ssh abcd@IP address "top -b -n 1 -o %CPU head -n 20"</code> • The current GPU load: <code>ssh abcd@IP Address "nvidia-smi -q -d UTILIZATION"</code> <p>In the above, "abcd" represents the user name and "[IP address]" is the IP address of the Processing Server.</p> <p>Both commands prompt you for a password when you run them.</p>



helpfeedback@milestone.dk

About Milestone

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 Systems 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 Systems is a stand-alone company in the Canon Group. For more information, visit <https://www.milestonesys.com/>.

