**AN-242**

# Protege GX XProtect Video Integration

Application Note

Last Published: 27-Feb-26 10:09 AM

# Contents

# Introduction

The Protege GX XProtect Video Integration provides a seamless integration between Protege GX and a Milestone XProtect system, enabling you to control cameras and view live and historical video footage from a single, easy-to-use interface.

Cameras can be linked to doors, inputs, outputs and areas, allowing you to easily retrieve footage based on any change of status, such as when a PIR is triggered or a door is opened. An automatic popup can display a live video stream on any door event, allowing you to see when someone is at the door or when a door has been forced open.

The included high level interface (HLI) enables the communication of PTZ triggers and alarm interfaces back to the VMS, providing bi-directional exchange of information. If desired, VMS events such as 'Motion Detected' can be monitored directly in Protege GX.

The following instructions outline how to install the Protege GX XProtect Video Integration and configure the DVRs, cameras, and doors within Protege GX.

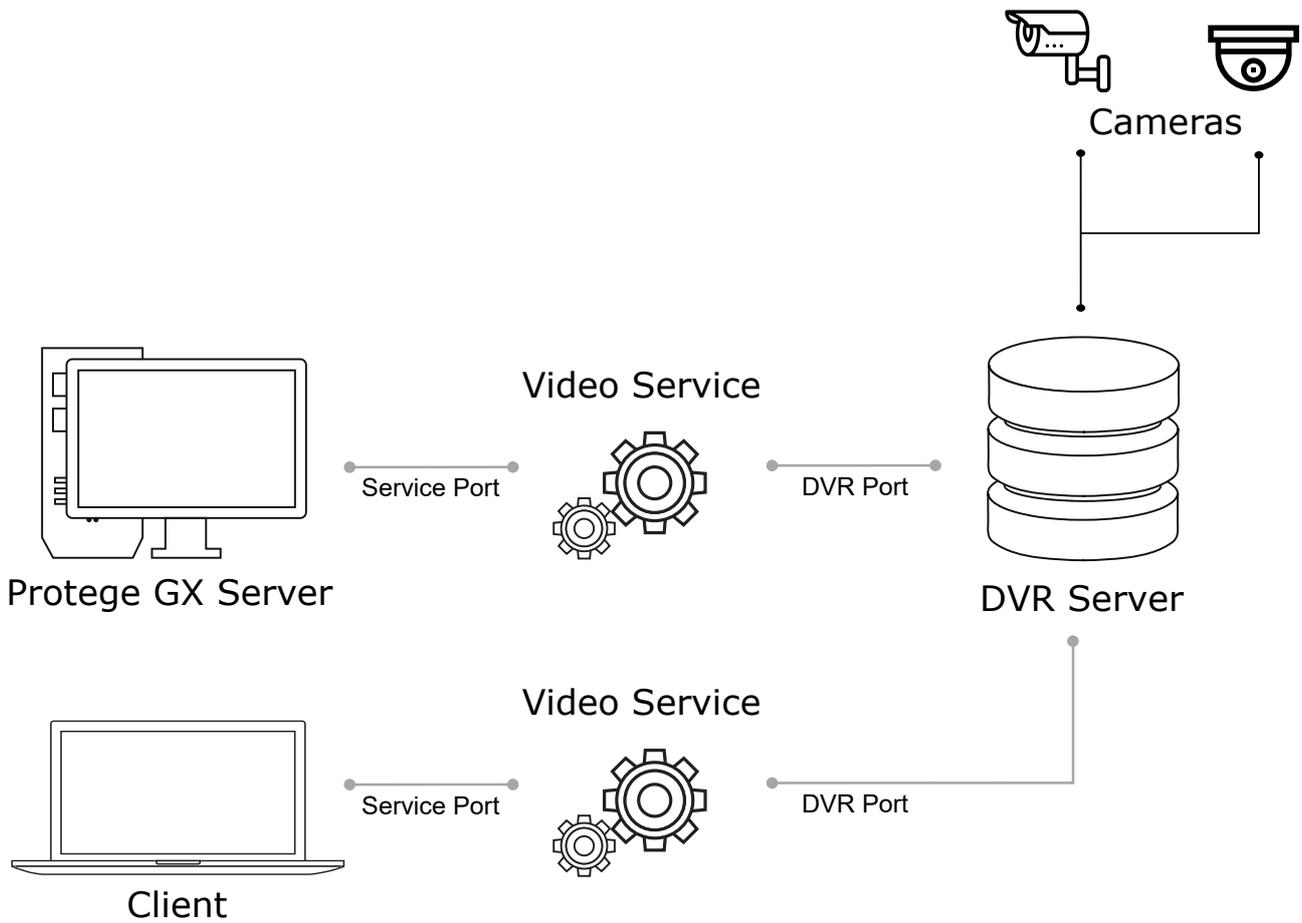## Milestone XProtect Integration Comparison

ICT offers two different integrations between Milestone XProtect and Protege GX which have different architecture and capabilities.

|  | Protege GX XProtect Video Integration | Protege GX Milestone XProtect Bidirectional Integration |
|---|---|---|
| Architecture | A middleware service connects the two systems | An MIP plugin installed on the XProtect server connects to the Protege GX SOAP Service |
| Main User Interface | Protege GX Client | XProtect Smart Client |
| Synchronization | Cameras and events are synchronized from XProtect to Protege GX | Access control devices, events and cardholders are synchronized from Protege GX to XProtect. |
| Commands | PTZ commands are sent from Protege GX to XProtect | Manual commands (e.g. lock, unlock) are sent from XProtect to Protege GX |
| Application Note | AN-242 Protege GX XProtect Integration Service | AN-358 Milestone XProtect Bidirectional Integration with Protege GX |

It is possible to run both integrations at the same time, enabling operators to use either Protege GX or XProtect as their user interface. These must be installed and configured separately following their respective application notes.

## Integration Architecture

In this integration Protege GX communicates with the DVR server via the integration's video service. This service monitors the two systems and sends any camera commands from Protege GX to the DVR server, and continuously transfers any events triggered in the DVR system to Protege GX.

Cameras

Video Service

Service Port

DVR Port

Protege GX Server

DVR Server

Video Service

Service Port

DVR Port

Client

## Ports

As shown in the diagram above, the video service communicates with Protege GX via the **Service Port**, and with the DVR server via the **DVR Port**. These ports are configured in the Protege GX DVR programming.

The DVR port is determined by the third-party VMS. If required, the service port can be customized when installing the video service. It is recommended to use the default ports where possible.

The default ports can be found in the Port Settings section of the Protege GX DVR programming instructions.

# Feature Support

This integration allows you to:

- View live video footage from programmed cameras.
- View historic and archived video footage.
- Embed cameras into a status page.
- Link a camera to a door, input, output or area.
- View live or archived video footage directly from an event associated with a camera.
- Automatically launch a camera view window when specific types of events occur.
- Send PTZ preset commands to the VMS in response to a Protege GX event filter.
- View and report on motion detection events in Protege GX.

# Prerequisites

Before you begin, ensure that you have the following information about your XProtect system:

- The HTTPS port that the XProtect VMS server uses to communicate with external systems. This is port 443 by default, but may be configured differently in your system.
- If you wish to use PTZ presets in this integration these must first be programmed in XProtect. Make a note of the **Name** of any preset position that will be used by Protege GX.

For more information, see the Milestone XProtect documentation.

## Software Requirements

All software must be installed and operational unless otherwise specified.

| Software | Version | Notes |
|---|---|---|
| Protege GX | 4.3.298.1 or higher | |
| Protege GX XProtect Video Integration | 1.2.0.1 or higher | This service must be installed on the Protege GX server and every client machine that will use this integration.<br>This document includes instructions for installing this service (see page 8). |
| Milestone XProtect | 2025 R2, 2024 R3, 2023 R3 | These are the **only** tested and supported versions for this integration.<br>The following variants are supported:<br>• Corporate<br>• Expert<br>• Professional+<br>• Express+ |
| Microsoft .NET Framework | 4.6.2 or higher | |

Supported cameras are determined by the XProtect system.

> It is the responsibility of the installation professional to verify the version of the proposed third-party system and supported components with the version listed in this document. ICT will not accept responsibility for the failure to verify integrated system versions and requirements.

## Protege GX Services

XProtect and the Protege GX SOAP Service and Web Client cannot be installed on the same server. If your Protege GX system uses these features, you **must** install them on a separate server from the XProtect software.

> **Installing these software components on the same server will cause XProtect to become unusable.** If this happens, contact ICT Technical Support.

## Protege GX Licensing Requirements

| License | Order Code | Notes |
|---|---|---|
| Protege GX Camera License | PRT-GX-CAM-10 | 1 license required per camera programmed in Protege GX. A single camera is included with the Protege GX standard license. |
| | PRT-GX-CAM-50 | The base Protege GX license includes an unlimited number of DVRs and DVR HLIs. HLIs allow bi-directional communication between Protege GX and the VMS. Note that this is separate to the live and archived video display that is covered by a camera license. |

## Time Settings

VMS integrations rely on the time being accurately configured for both the hardware and the operating systems used in a site.

To ensure the system is keeping precise time, all devices should be set to synchronize with the same NTP time server. NTP servers work by sending accurate time information periodically to the system. Many corporate organizations have an NTP server running on the internal network, allowing you to simply enter the relevant IP address. Alternatively, you could use any public NTP server. Finding an NTP server relevant to your region is usually as simple as a quick web search.

**The same time server must be used for all workstations, servers and controllers within the site.** You can configure the time server for each computer in the Windows **Date and Time** settings, and set a time server for the controller in the **Sites | Controllers | Time update** settings in Protege GX.

# HTTPS Certificate

The Protege GX XProtect Video Integration can communicate with XProtect using either the HTTPS or HTTP protocols. We recommend using HTTPS communications to ensure that data is encrypted. The default **DVR port** for HTTPS is 443.

To use HTTPS, there must be an HTTPS certificate installed on the XProtect server. The HTTPS certificate needs to be trusted by both the XProtect server and the computer with the video service installed. Otherwise, the video service will refuse the connection. This may be a third-party certificate or a certificate issued from internal Public Key Infrastructure (PKI).

The XProtect system may already have a trusted certificate installed for communication between different XProtect servers. Discuss what is available with the VMS installer. If the system is not already configured for encrypted communications, you may need assistance from the VMS installer or the site's IT team. For more information and instructions for installing a certificate on an XProtect system, see the Certificates Guide in the Milestone XProtect Help.

To set up and test the system, you may use the HTTP protocol. This is not recommended for live installations, as messages are not encrypted. The default **DVR port** for HTTP is 80.

# Installing the Video Service

The Protege GX XProtect Video Integration service must be installed on the server and each client machine that uses the integration. You must have administrator rights on each computer to complete the installation.

1. Run the Protege GX XProtect Video Integration.exe file to launch the installation wizard. Click **Next**.
2. Select **Complete** for the installation type then click **Next**.
3. Click **Install**.
4. Enter the **Service Port Number** to be used for the integration (8070 is the default) and click **Next**.
5. Click **Finish**.
6. If the Windows Defender Firewall is on, you will see a Windows Security Alert popup indicating that some features of the integration service have been blocked.

   To allow the service to function, check the boxes to allow the service to communicate on **Domain networks** and **Private networks** (or as appropriate for your installation). Then click **Allow Access**.

## Check the Services are Running

The services used by the integration must be running so that Protege GX can communicate with XProtect.

1. Open **Services** as an administrator:
   - Press the **Windows + R** keys.
   - Type **services.msc** into the search bar.
   - Press **Control + Shift + Enter**.
2. Scroll down to locate the **Protege GX XProtect Video Integration**.
3. Ensure the service has started automatically (check the **Status** column to confirm that it's 'Running'). If not, right-click the service and select **Start**.
4. Ensure the **Protege GX DVR Service B** is running.

# Programming Cameras in Protege GX

## Port Settings

To configure the DVR in Protege GX you will need to enter the DVR port and service port settings, as described in the Integration Architecture section. It is recommended to use the default ports where possible.

- Default **DVR Port**: 443 (HTTPS) or 80 (HTTP) (see page 7)
- Default **Service Port**: 8070

## Adding the DVR

From the main menu, navigate to **Monitoring | Setup | DVRs**. Add a DVR record and configure the following options:

1.  Enter the **IP address** and **DVR port** of the DVR server.

    The DVR port is determined by the third-party VMS and will depend on the configuration of the DVR itself.

2.  Set the **DVR type** to Custom.

3.  Set the **Service port** that was configured during the video service installation. This option is only visible once the **DVR type** is set to Custom.

    The service port must be defined for the integration to work correctly. If necessary, it can be changed in the config file for the service.

4.  Enable the **Monitor events from this DVR/NVR** option to start logging HLI events from the DVR in Protege GX. The operator can right click any HLI event to view the footage archived at the time the event was logged.

    For camera motion events, the **Monitor events** option must be enabled in the camera settings in Protege GX. Note that motion detection must also be enabled for that camera in the VMS.

5.  If required, enable the **Connect to this DVR/NVR on start up** option. When this option is enabled, Protege GX will send a login request to the DVR when the client starts up. Otherwise, Protege GX will not connect to the DVR until it needs to request a camera list or footage.

6.  If logging in to the VMS requires authentication, enable **Login required** and enter the **Username** and **Password** required to access the VMS.

    The pipe character | is not supported in these fields.

## Adding the Camera(s)

Once the DVR has been configured, you can add a record for each of the installed cameras, enabling you to view live and historical (archived) video feeds directly from a status page or floor plan.

1.  From the main menu, navigate to **Monitoring | Setup | Cameras**. Add a new camera with a descriptive name.

2.  Set the **Type** to DVR and select the **DVR** you created earlier.

3.  On the **DVR camera name** row, select the **[...]** button to open the **Select camera** window.

    The pipe character | is not permitted in the **DVR camera name**. You may need to change the camera's name in the third-party system.

4.  The window will display a list of cameras connected to the selected DVR. Highlight the camera you want to use and click **Select**.

5.  Set the required display options:

- **Show sidebar controls in status page**: When this option is enabled, PTZ controls are displayed by default when the camera feed is viewed on a status page. When this option is disabled the control sidebar can be opened but will not be displayed by default.
- **Stretch image**: When this option is enabled the camera image will be stretched to fill the tile where it is displayed. This may not preserve the aspect ratio.
- **Floor plan**: The floor plan the camera belongs to. This allows you to right click on a camera event in the event log and open the floor plan associated with the camera.

6. Enable the **Monitor events** option if you wish to log HLI events from the DVR system.

This setting must be used in conjunction with the **Monitor events from this DVR** option of the DVR record. It enables certain camera events, such as motion detected, to be logged from the DVR/NVR. The operator can then right click the event and select the camera to view the footage archived from the time the event was logged.

## Linking a Camera to a Record

Linking a camera to a record enables you to view a live or archived feed by right clicking a record or any associated event. Cameras can be linked to doors, inputs, outputs or areas, allowing you to track any status changes, such as when a PIR is triggered or an area is disarmed.

If an event has a camera associated with it, a small yellow camera icon appears to the left of the event. Right-clicking the event allows you to view the archived footage from the camera at the time the event was logged.

If the door auto camera popup settings are enabled, Protege GX will automatically display a window with the live camera feed whenever a door event is triggered, or if a door is forced open.

1. Select the door, input, output or area you wish to link the camera to (from the appropriate **Programming** menu).

2. In the **General** tab, scroll down to **Graphics**. Set the **Camera** which is monitoring that physical space.

   For doors, you can set a **Camera (entry)** and **Camera (exit)**. Depending on where the camera is located, you may wish to use the same camera for both entry and exit, or select a different camera for each.

3. For doors, you can set the following **Auto popup options**:
   - **Auto camera popup on any door event**: When enabled, displays a popup window showing a live camera feed when any door event is triggered.
   - **Auto camera popup on door forced event**: When enabled, displays a popup window showing a live camera feed when a forced door event is triggered.
   - Select the **Camera** to be displayed in the popup window.

4. Save your changes.

5. To view the camera feed, right click on the record in the programming window or status list and click the **Camera** button. Right click any events associated with that record to view either live footage or archived footage from the time of the event.

## Including a Camera in a Status Page

A camera can also be included in a status page for live viewing of video footage while monitoring a site.

1. Open the **Status page editor** (**Monitoring | Setup | Status page editor**). Select an existing status page to update, or create a new status page by clicking **Add** and choosing a layout.

2. Select the panel where you wish to display the camera and set the **Type** to Camera.

3. For the **Record**, select the camera that you wish to display.

4. Save your changes.

5. Navigate to **Monitoring | Status page view** to view the camera feed on your status page. Click the arrow button on the upper right of the panel to display PTZ arrows, which can be used to pan, tilt and zoom a PTZ camera.

You can also include camera HLI events on a status page. You can do this by including a panel that displays All Events. Alternatively, you can create an event report that displays only camera HLI events, and display that on the status page:

1. Navigate to **Events | Event filters** and create a new event filter which will filter for camera HLI events.

2. In the **Event types** tab, disable **Include all event types**.

3. Click **Add** and expand the **All PC events** section. Scroll down to the Camera events, select the desired HLI events and drag and drop them onto the main window. **Save** the event filter.

4. Navigate to **Reports | Setup | Event** and create a new event report to display the HLI events.

5. **Add** the event filter created above.

6. Finally, to display the event report on a status page, navigate to **Monitoring | Setup | Status page editor**. Select an existing status page to update or create a new status page.

7. Select a panel and set the **Type** to Event windows. Set the **Record** to the event report created above.

8. Save your changes and navigate to **Monitoring | Status page view** to view the events on your status page. You can right click the events to open the camera window to the time of the event.

**Note**: Some HLI events require the corresponding camera feature to be enabled in the VMS (such as motion detection).

# Programming Camera Actions

Actions in Protege GX are triggered in response to particular events, as defined by an event filter. There are two actions related to cameras: sending PTZ commands and popping up a camera feed window.

## Send PTZ Command on Event

Through the HLI, Protege GX can send PTZ commands to connected cameras in response to particular events. This allows the system to physically move PTZ cameras to preset positions to get the best view of the situation.

Before you begin, ensure that any cameras have PTZ enabled and the PTZ preset commands are programmed in the VMS. Note down the **Command String** for each PTZ preset that you wish to use. This is the **Name** of the PTZ preset in XProtect.

See the documentation for your VMS for information on programming PTZ presets and viable command strings. These cannot be programmed directly in Protege GX.

1. Navigate to **Monitoring | Setup | PTZ commands** and create a new PTZ command.

2. Under **Configuration**, select the **Camera** that the command will be sent to.

3. Enter the **Command string** that represents the PTZ preset.

4. Navigate to **Events | Actions** and create a new action.

5. Set the **Event filter** to define the events that will trigger the action. If required, click the ellipsis **[...]** button to break out the event filter programming window and create a relevant event filter.

6. Select the **PTZ command** created above.

7. Click **Save**.

8. Open the Windows Services Manager and restart the Protege GX XProtect Video Integration.

## Pop Up Camera Window on Event

Actions can be used to automatically trigger a live popup window when specific events occur, such as when a door is left open or when an area alarm is triggered.

1. Navigate to **Events | Actions** and create a new action.

2. Set the **Type** to Popup camera window.

3. Set the **Event filter** to define the events that will trigger the action. If required, click the ellipsis **[...]** button to break out the event filter programming window and create a relevant event filter.

4. Select which camera to use. You can choose from:
   - Default camera associated with event
   - Door entry camera
   - Door exit camera
   - Select camera from list

5. Click **Save** to create the action.

## Enabling Camera Popups on Alarm

Operator alarms send a popup window to Protege GX operators (such as security guards) when selected events occur in the system. Along with the event information, you can also include a camera popup window which displays footage from the camera associated with the relevant door, area, input or output.

This approach is similar to using the Popup camera window action but has the additional benefit that the camera popup obeys alarm routing rules, allowing it to be routed to particular workstations and passed on if it is not acknowledged. It may also be more efficient to program if the alarms are already being used in the system.

For more information on programming alarms, see Application Note 332: Setting up Event Notifications in Protege GX.

1. Assign cameras to doors, areas, inputs and outputs as required (see page 10).

2. Navigate to **Events | Alarms** and create a new alarm.

3. Set the **Event filter** to define the events that will trigger the alarm. If required, click the ellipsis **[...]** button to break out the event filter programming window and create a relevant event filter.

4. Enable **Allow camera popup**.

5. Click **Save**.

Now when an alarm popup appears, if any device associated with the alarm has a camera assigned to it that camera window will pop up as well.

## The Camera Window

The camera window displays a split view showing archived and live camera footage. It can be opened by right clicking on a record or event associated with a camera.

- The **top left pane** displays a 5 second looping video centered 2 seconds either side of the time of the event.
- The **top right pane** displays a 30 second controllable window centered 15 seconds either side of the time of the event. Drag the slider to adjust the image to any point within the 30 second period.
- The **main lower pane** displays the live camera view.
  - The **Archive view controls** allow you to select any date and time in the past.
  - The **Live view controls** provide PTZ camera control buttons, allowing you to physically control a PTZ enabled camera.

- The options on the **right** provide control over the main view:

  Select the tab on the side to switch between the two views as required.

# XProtect Events in Protege GX

Protege GX can generate three types of events based on events from XProtect:

- Camera Motion Detected
- Camera Motion Ceased
- Camera Generic Event

The 'Camera Generic Event' is used for a number of different events that may be received from XProtect. These events can be found on the Events Overview page in the XProtect help, under the following headings:

- **Devices - Configurable Events**: Specific events for each device.
- **Devices - Predefined Events**: Events related to devices, including communication loss, start/end of recording, PTZ commands and output activations. Motion started and motion stopped events have unique event types, as noted above.
- **System Monitor - Camera**: Camera issues, such as FPS drops and storage warnings.

Because the 'Camera Generic Event' has a range of causes, you will need to investigate the event details in the XProtect client.

Do not connect automated responses such as actions to the 'Camera Generic Event'. Many actions will generate another 'Camera Generic Event', causing the action to be triggered again in an infinite loop.

# Troubleshooting

**While upgrading the service, I receive the error message "The setup was unable to automatically close all requested applications". The installer does not proceed through the upgrade.**

For some upgrades, you need to stop the existing video service manually before running the installer. If you receive this error message, do the following:

1. Close the installer.
2. Open **Services** as an administrator:
   - Press the **Windows + R** keys.
   - Type **services.msc** into the search bar.
   - Press **Control + Shift + Enter**.
3. Locate the **Protege GX XProtect Video Service**.

   Older versions are called **Protege GX Milestone Video Service**.

4. Right click the service and select **Stop**.
5. Run the installer again. This error should no longer occur.

**Protege GX does not connect to XProtect**

Windows Firewall may be preventing the video service from connecting to XProtect. To check and update the firewall settings:

1. Open the **Control Panel** and select **Windows Defender Firewall**.
2. Select **Allow an app or feature through Windows Defender Firewall**.
3. Click **Change settings** and enter your administrator details to allow editing.
4. Locate the Protege GX XProtect Video Integration.

   If it is not already in the list, click **Allow another app**. Use **Browse** to select the service from its installation directory. This is typically:

   C:\Program Files (x86)\Integrated Control Technology\GXVideoService_Milestone

5. Check the boxes under **Domain** and **Private** to allow the service to communicate.

   Do not enable **Public** unless required for your network.

**I can select XProtect cameras in Protege GX, but some camera streams are not working**

XProtect installations consist of one management server and one or more recording servers. If the installation has recording servers that are on different subnets/VLANs from the management server, the video service may not be able to resolve the hostnames of those recording servers and so will not be able to retrieve the camera streams.

There are two methods for resolving this issue. The simplest method involves enabling a public IP address on the recording server.

1. In the XProtect Management Client, navigate to **Servers > Recording Servers**.
2. Select the recording server that needs to be updated.
3. In the Properties window, select **Network**.
4. Check the **Enable Public Access** option.
5. Set the **Public Address** to the IP address that the Protege GX XProtect Video Integration will use to connect to this recording server.
6. Set the **Public Port** to the port that the video service will use to communicate with this recording server. The default port is 7563.

> The XProtect management server supplies the IP address and port information for each recording server to the video service. There is no need to program these settings in the DVR record in Protege GX.

7. Save your settings.

If the public address on the recording server is not available, alternatively you can manually update the static hosts on the Protege GX client machines. This must be done on every machine that uses the video service.

1. Open Notepad or another text editor as an administrator.

2. Select **File > Open**, then browse to **C:\Windows\System32\drivers\etc**

3. Open the **hosts** file (no file extension).

4. At the end of the file, start a new line and enter the following:

   ```
   x.x.x.x recording.server.hostname
   ```

   Replace these values with the IP address and hostname of the XProtect recording server.

   > Include a space or tab between the IP address and the hostname.

5. Save the file.

6. Repeat on each Protege GX client workstation that uses this integration.

# Video Service Logs

MIPSDK logs are generated on the XProtect server. You can view the logs in the following directory: **C:\ProgramData\Milestone\MIPSDK**

By default, the logging is optimized to prevent it from filling too much space on the server. If you need to capture detailed logs for troubleshooting purposes, edit the video service settings as follows:

1. On the computer where the video service is installed, open the installation folder. This is typically:

   C:\Program Files (x86)\Integrated Control Technology\GXVideoService_Milestone

2. Open **MIPSettings.xml**.

   > Files in this directory require administrator permissions to edit. You may need to open the file as an administrator using an application like Notepad++, or make a copy in a different directory to edit and replace the original.

3. Immediately below the **TraceFunctionCalls** line, add the following code:

   ```
   <DebugLogging>True</DebugLogging>
   ```

4. Save the XML file.

5. In the Windows Services Manager, restart the Protege GX XProtect Video Integration.

Once you have captured the logs you need, change **DebugLogging** to **False** and restart the service again. This will prevent excessive logs from filling up storage on the XProtect server.

# Release History

**Version 1.2.0.1**

- This integration has been validated against XProtect version 2025 R2.
- Updated the name of the service from Protege GX Milestone Video Service to Protege GX XProtect Video Integration.
- Updated the Milestone SDK to version 25.2.2.
- Improved performance of the camera popup window in Protege GX.
- The integration now maintains the correct camera links when cameras are removed from XProtect.
- Resolved an issue where the **Field time** for XProtect events in Protege GX was displayed in UTC instead of local time.
- Resolved an issue where excessive MIPSDK logs were created on the XProtect server. Logging levels are now configurable (see previous page).