Milestone Systems

Milestone Diagnostics Tool 2022 R3

User manual

milestone

Copyright, trademarks, and disclaimer

Copyright © 2022 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.

Contents

Introduction

Milestone Diagnostics Tool (explained)

Introduction

Milestone Diagnostics Tool is a system diagnostics tool that gathers and displays detailed information about your system setup. This information includes, but is not limited to, ports, camera drivers, software versions and hardware information. You can also find a list of all cameras that have been added to the system, including the specific device model and camera manufacturer, no matter the size of the system setup.

Milestone Diagnostics Tool is provided free of charge with any installation and without any restrictions. Milestone Diagnostics Tool is compatible with all XProtect VMS products:

XProtect Advanced products:

- XProtect® Corporate

- XProtect® Expert

- XProtect® Professional+

- XProtect® Express+

- XProtect® Essential+

XProtect Professional products:

- XProtect® Enterprise

- XProtect® Professional

- XProtect® Express

Where to find Milestone Diagnostics Tool

For XProtect versions before 2017 R1 (11.a), you must download the Milestone Diagnostics Tool and place it on a server that is connected to your system.

If you are using XProtect versions from 2017 R1 (11.1a) or later, you can find the Milestone Diagnostics Tool in one of the following locations in your installation:

- XProtect Advanced products

    - XProtect Management Server— install location

    {Drive letter}:\Program Files\Milestone\XProtect Management Server\Tools\DiagnosticsTool\

    - XProtect Recording Server— install location

    {Drive letter}:\Program Files\Milestone\XProtect Recording Server\Tools\DiagnosticsTool\

- XProtect Professional products

    - Product installer — install location

    {Drive letter}:\Program Files (x86)\Milestone\Milestone Surveillance\Diagnostics\

- Other components

    - XProtect Event Server— install location

    {Drive letter}:\Program Files\Milestone\XProtect Event Server\Tools\Diagnostics Tool\

    - XProtect LPR Server — install location

    {Drive letter}:\Program Files (x86)\Milestone\XProtect LPR Server\Tools\Diagnostics Tool\

    - XProtect Smart Client— install location

    {Drive letter}:\Program Files\Milestone\XProtect Smart Client\Tools\DiagnosticsTool\

Running Diagnostics

Diagnostics report (explained)

The diagnostics report provides information about the environment the VMS is operating on. It consists of nine tabs: **System**, **Hardware Information**, **Software**, **Services**, **IIS**, **Ports**, **Drivers**, **Test**, and **Firewall**.

> ✅ If you want to learn more about each tab, see .

You can use the report to:

- See the version of your operating system

- See the VMS-related services and their statuses

- See the ports in use

- See a list of all cameras that are added to your system

- Test your configuration against the Milestone-recommended settings

You can share the report with a Milestone Technical Support representative as part of the troubleshooting process.

> ⚠️ The diagnostics report does not contain any log messages. To view the VMS installation and system logs, see or .

Create a diagnostics report

To create the report:

1. On a relevant server that is connected to an XProtect server, for example the management server, open the **Diagnostics Tool.exe** from the relevant file location.

2. From the main screen of Milestone Diagnostics Tool, select **Logs & Diagnostics**. Then, select **Run diagnostics** to start the wizard.

3. When the analysis of your system is completed, the **Diagnostic report** page is displayed. The system information is divided into a number of tabs that all include different information about the site's system setup.

4. Click **Save** to export the analysis as an.MCLOG file. The default location of the files is {System drive}:\ProgramData\VideoOS

> ✅ By default, this directory is hidden. Make sure to enable **Hidden items** in **Windows Explorer** in your system drive to navigate to the VideoOS folder.

Use Milestone Diagnostics Tool to list all cameras added to your system

1. On a relevant server that is connected to an XProtect server, for example the management server, open the **Diagnostics Tool.exe** from the relevant file location.

2. From the main screen of Milestone Diagnostics Tool, select **Logs & Diagnostics**. Then, select **Run diagnostics** to start the wizard.

3. When the analysis of your system is completed, the **Diagnostic report** page is displayed. The system information is divided into a number of tabs that all include different information about the site's system setup.

4. In the top bar of the **Diagnostic report** page, select the **Drivers** tab.

5. On the **Drivers** tab, all cameras detected in your system are displayed. Initially, the cameras that have been detected are sorted alphabetically in the **Name** column.

> ✏️ You cannot rely on the naming information that is shown in the **Name** column to display the exact model and manufacturer of your cameras. The system administrators can change the name of cameras in the administration applications at any time.

6. To save a log file of the diagnostic analysis and the cameras that were found, click **Save.** To open a previous diagnostics report, select a diagnostics report from the **Logs & Diagnostics** page.

Open an existing diagnostics report

Diagnostic reports are saved as .MCLOG files in {System drive}:\ProgramData\VideoOS. You can view them with the Milestone Diagnostics Tool.

If you want to create a new diagnostics report, see Create a diagnostics report on page 6.

With the diagnostics report you can:

- Get an overview of the VMS installation at a particular point of time

- Compare current and previous VMS installations

- Compare VMS installations on different machines

To open a diagnostics report:

1. On a relevant server that is connected to an XProtect server, for example the management server, open the **Diagnostics Tool.exe** from the relevant file location.

2. From the main screen of Milestone Diagnostics Tool, select **Logs & Diagnostics**. A list of saved diagnostics reports opens.

3. Select a diagnostics report to view it.

If you want to learn more about the report tabs, see .

Diagnostics report (properties)

The Diagnostic report consists of nine tabs: **System**, **Hardware Information**, **Software**, **Services**, **IIS**, **Ports**, **Drivers**, **Test**, and **Firewall**.

System

On this tab, you can find information regarding a number of components in your VMS environment:

Group name	Contains information about
Operating system	**OS Language, Architecture, Localization, Version**
Memory	**Used, Free, Total**
Processor	**Number of logical processors,CPU(%), Last error, Current speed, No of cores/ processors, Enabled cores, Number of physical processors**
Domain and user information	**Machine, Role, Current user, Domain name**
GPU	**Name**
Installed system components	A list of Windows components that the VMS requires to operate.

Hardware Information

On this tab, you can find information regarding the computer's hardware.

Group name	Contains information about
Computer system product	**ID Number**, **Version**, **Vendor**
Computer system	**SKU Number**
BIOS	**Release Date**
Baseboard	**Serial Number**, **Product**
Physical disc	Model and SKU of the hard drives *Click on the arrow to learn more. You can see **Index**, **Interface Type**, **Model**, **Partitions**, and **Size**.
Logical drive	Windows partitions *Click on the arrow before the drive letter to learn more about each drive. You can see **Description**, **Free space**, **Size**, and **Volume name**.

Software

On this tab, you can find detailed information regarding your VMS components.

Group name	Contains information about
Software license	The **SLC** (Software License Code) in use
VideoOS software products	Installed VMS components. Can be sorted by **Software**, **Version** or **Release**
Installed VideoOS patches	Installed cumulative patches with information about the **Product**, **Patch**, and **Version**
Installed MIP Plugins	**Installed MIP SDK plugins** with information about the **Product**, **Patch**, and **Version**

Services

On this tab, you can find information about the VMS services, their **Name**, **Status**, **Condition**, **Startup Type**, and **Log On As** status.

IIS

The management server communicates with the remote computers through the Internet Information Services (IIS). On this tab, you can see if the application pools are running under the same identity.

Ports

On this tab, you can see the ports that are currently in use. For more information, see Ports used by the system.

> ✅ If a required port is missing, you must manually open the port to allow communication.

Drivers

On this tab, you can see all cameras that your system has detected. The following camera details are displayed:

- **Name** of the device (chosen by the Administrator)
- **Address**
- **Port**
- **Firmware** version
- **Hardware ID**
- **Driver Name**

Test

The **Diagnostics report** performs 19 tests against Milestone-recommend settings and displays the results in either red, yellow, or green color, each of which color indicate a different state:

- Green - the test result matches the expected outcome
- Yellow - the VMS can still operate, but you may experience issues with this particular setting at some point
- Red - action is required, see details from more information

Test	Passed when
Antivirus Software	Antivirus software is disabled.
Hardware Acceleration	Hardware Acceleration is enabled.
Proxy Enabled Status	No proxy is enabled.
Cluster	Cluster status is found.
Windows Firewall	Windows Firewall is disabled.
Hostname	The hostname has less than 15 characters.
Application pool account "Administrator" role membership	Identities in the IIS Application Pool have Administrator rights in XProtect Management Client.
Service account "Administrator" role membership	The Service account has Administrator rights in XProtect Management Client.
Windows Updates	There are no pending updates.

Test	Passed when
Application Pool Status	IIS Application Pools for the VMS are running.
Default Hardware Password	Cameras' passwords are not set to default.
Duplicate devices	There are no duplicate devices in the SQL database.
IIS AppPool/Management server identities	The identities used by the VMS in the IIS Application pool match with the identities in the Management Server.
SQL Server location and cluster status	The SQL Server location and cluster status are found.
SQL database compatibility level	The SQL database compatibility level is found and is set to highest level (current level is 150).
Resolve Recorder hostname to IP	The recorder's hostname is resolved to an IP address.

Test	Passed when
Resolve Registered Services hostnames to IP	The Registered Services' hostnames are resolved to IP addresses.
Disk cluster size test	The Allocation unit size is 64 kilobytes.
Recorder storage location	The recording server is not installed on the System drive.

✅ You can click on **Details** for each test to learn more.

Firewall

On this tab, you can find:

- The current status of your **Windows Firewall**

- A list of **Allowed Service and Applications**

- Additional **Firewalls, Antivirus, and Antispyware Software** that are installed on the computer

Collecting logs

Collect custom logs

You can use Milestone Diagnostics Tool to collect logs and additional site information for all VMS components from a single place. You can choose what information to extract, depending on your specific need.

> ⚠ If you want to collect a predefined set of logs, see Collect default logs on page 17.

From the **Collect logs** menu, you can collect:

- Logs from all VMS components

- Site analysis report

- Windows event logs

- Product Minidumps (process captures generated by the VMS components)

- Process dumps (Windows process captures)

- SQL tables

> ✎ Milestone Diagnostics Tool saves the report into a .ZIP file.

> ✓ You can include additional files in the report file such as screenshots, topology diagrams and more.

You can:

- Collect logs on page 14

- Collect logs using command line arguments on page 15

Collect logs

You can use the user interface to create and export logs. If you want to use the Command prompt instead, see Collect logs using command line arguments on page 15.

1. On a relevant server that is connected to an XProtect server, for example the management server, open the **Diagnostics Tool.exe** from the relevant file location.

2. From the main screen of Milestone Diagnostics Tool, select **Logs & Diagnostics**. Then, select **Collect logs** to start the wizard.

3. Enter your **Case Number** (example: MSCxxxxxx).

4. Select the **Save to** location.

5. (Optional) Check the **Collect site analysis** box to include a diagnostics report.

6. Select the time range for the logs. You can choose between one day, one week, two weeks, one month or custom.

7. (Optional) If you want to include **Product Minidumps**, select this check box.

8. (Optional) If you want to include Windows Event logs, select one or more of the check boxes under Event Viewer. You can choose to include logs from the following areas:

    - Application - shows events logged by the software installed on your computer

    - Security - contains events related to the security of your computer

    - Setup - refers to domain control events

    - System - collects events logged by the operating system

    - All Files - includes Application, Security, Setup and System logs

9. (Optional) If you want to include **Process dumps**, select the **Process dump type** and **Processes** name.

> ⚠️ Some process dumps types can take a lot of memory and slow the report generating process. Use this feature only if the technical support representative has instructed you so.

10. Select if you want to backup an SQL database:

    - **SQL data not included**

    - **Full SQL database backup**. You can optionally select to include the log server backup.

    - **SQL table export**. You can select different tables from different databases and schemes. After selecting the database and the schema, you can check the boxes of the tables that you want to include. Once you are done with a database, you can switch to another one. The previous selection will be saved.

11. (Optional) If you want to add additional files, such as screenshots, topology diagrams or other, click **Browse** in the **Additional files** field.

12. Click **Collect**. Milestone Diagnostics Tool starts preparing the files.

13. A message informs you when the process is completed. The report is saved as a .ZIP file on your desktop. You can close the window by selecting **OK**.

Collect logs using command line arguments

The Milestone Diagnostics Tool also supports command line arguments.

To create logs using command line arguments:

1. Open Windows Command Prompt. The easiest way to do this is to click on Windows Start menu and type cmd.

2. Navigate to the Milestone Diagnostics Tooldirectory and press **Enter**. Example:

```
cd "C:\Program Files\Milestone\XProtect Management
Server\Tools\DiagnosticsTool"
```

3. Type "**Diagnostics Tool.exe**" to open the program.

4. Add the commands and associated arguments for the types of logs. You can use some or all commands to generate a report. To find an overview of available commands and arguments, see Milestone Diagnostics Tool commands (explained) on page 16.

   The example below will collect logs from the past four weeks, minidumps, Event Viewer logs from Application, Security, Setup and System, and a copy of the Surveillance SQL database.

```
C:\Program Files\Milestone\XProtect Management
Server\Tools\DiagnosticsTool>"Diagnostics Tool.exe" /logs:4w
/includeminidumps:yes /eventviewer:all /db:yes
```

5. Press **Enter** to run the program with the selected parameters. A message is displayed when the file is ready. The logs are saved as a .ZIP file on your desktop.

Milestone Diagnostics Tool commands (explained)

Milestone Diagnostics Tool supports the following Command Prompt commands:

Command	Description	Arguments
/logs	Collects logs for a specified time period (in days, weeks or months).	1d, 1w, 1m
/includeminidumps	Collects process minidumps.	true, false
/eventviewer	Collects Windows Event Viewer logs. Select the Event Viewer logs, separated by commas with no spaces or choose all to include all logs.	application, security, setup, system, all

Command	Description	Arguments
/db	Collects a copy of the Surveillance SQL database.	yes, no
/includelist	Specifies the path to a plain text document containing file or folder paths that should be included in the collection.	location of the .TXT file
/?	Displays the Milestone Diagnostics Tool command line help in a pop-up window.	none

Collect default logs

With Milestone Diagnostics Tool, you can quickly collect the most important details and present them to Milestone Technical Support when necessary. With the Collect default logs option, you can:

- Extract logs from all VMS components for the past month
- Create a diagnostics report on page 6

🖊	If you want to modify the logs selection, see Collect custom logs on page 14.

To create a **Collect Defaults** report:

1. On a relevant server that is connected to an XProtect server, for example the management server, open the **Diagnostics Tool.exe** from the relevant file location.

2. From the main screen of Milestone Diagnostics Tool, select **Logs & Diagnostics**. Then, select **Collect default logs** to start the wizard.

3. A message informs you that the process is completed. The report is saved as a .ZIP file on your desktop. You can close the window by selecting **OK**.

Monitor debugging

Enable debug logging

Debug logs are used to identify flaws in the system and the configuration. By default, all logs levels are set to **Information**, but you can change the level to **Debug** from Milestone Diagnostics Tool.

You can manage the log levels for:

- VMS
- VMS drivers
- Windows Registry (limited).

To enable debug-logging for a component:

1. On a relevant server that is connected to an XProtect server, for example XProtect Management Server, open the **Diagnostics Tool.exe** from the relevant file location.

2. From the main screen of Milestone Diagnostics Tool, select the **Log Levels** tab.

3. A new window will notify you that changing VMS component settings might require a restart of the related services. Click **OK** to continue.

4. Select the check box next to each component to enable debug-level logging for that component. You can enable debug logging for as many components as you want to.

   Then, select **Save**. A new window opens, informing you about the services that require a restart.

5. If you want to apply the changes on the selected services, select **Yes**.

6. Milestone Diagnostics Tool restarts the services. Once the services restart, you can close the window. You have changed the log level for the selected services.

Monitor debugging

Use **Monitor Debugging** to monitor debug output between the recording server and the hardware devices in real time. You can use the monitor to:

- Find a failed device
- Check for dropped camera events
- Troubleshoot camera stream issues

> ⚠ To see the detected messages, make sure you have enabled debug logging for the VMS drivers before you start. See .

To create a **Debug Monitor report**:

1. On the recording server computer, open the **Diagnostics Tool.exe** from the relevant file location.

2. From the main screen of Milestone Diagnostics Tool, click on the **Debug monitor** tab. A message informs you if you have not enabled debug logging for the VMS drivers. Select **OK** to close the window. Enable debug logging for the VMS drivers before you start detecting.

3. Click **Start detecting** to initiate the capture process. During this time, you can trigger your issue and collect the messages that are exchanged between the server and the devices.

4. (Optional) Click **Clear messages** to remove the collected messages.

5. Click **Stop detecting** to stop the capture process.

6. Click **Save** to save the report. The **Debug Monitor** reports are saved at {System drive}:\ProgramData\VideoOS.

> ✅ By default, {System drive}:\ProgramData\VideoOS directory is hidden. Make sure to enable **Hidden items** in **Windows Explorer** in your system drive to navigate to the VideoOS folder.

You can now attach the file to your support case for further investigation.

View debug messages

The **Monitor Debugging** option monitors the debug output between the recording server and the devices in real time. You have the option to save the debug messages as an .MDDM file and view them later.

To view previously saved debug messages:

1. On the recording server computer, open the **Diagnostics Tool.exe** from the relevant file location.

2. From the main screen of Milestone Diagnostics Tool, select the **Monitor Debugging** tab.

3. Select a report with debug messages. You have the option to:

   - Search for specific messages

   - Select a proxy type

   - Filter messages from a specific time period

Searching the SQL database

Search for entries in the SQL database

The management server, the event server and the log server store, for example, the system configuration, alarms, events and log messages in SQL databases on one or more SQL Server installations.

You can look for entries in the SQL database that is running on your current computer with the Milestone Diagnostics Tool when you need to:

- Check for log messages

- Look for events related to a particular device

- Search for other information.

To start searching the SQL Database:

1. On a relevant server that is connected to an XProtect server, for example XProtect Management Server, open the **Diagnostics Tool.exe** from the relevant file location.

2. From the main screen of Milestone Diagnostics Tool, select the **SQL Database** tab.

3. Type the words that you want to match entries in the database and click **Search**. A list of the results is displayed.

> ✅ The SQL Database search is not case-sensitive. You can look for strings of words without special characters.