Milestone Systems

Milestone Diagnostics Tool 2022 R2

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

The 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.

The Milestone Diagnostics Tool is provided free of charge with any installation and without any restrictions. The 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\XProtectSmart 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, Firewall**, **Drivers**, and **Test**.

> ✅ If you want to learn more about each tab, see Diagnostics Report (properties) on page 9.

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 Collect custom logs on page 14 or Collect default logs with Milestone Diagnostics Tool on page 17.

Create a Diagnostics Report

To create the report:

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, click **Run Diagnostics** to open the **Run Diagnostics** wizard.

3. On the first page of the **Run Diagnostics** wizard, select the sites that you want to include in the system diagnostics. You can search for specific sites in the search bar or click **Select all** to make sure that every camera on all sites are included in the diagnostics.

> ✅ You must select the check box for each individual site for it to be included in the system diagnostics analysis.

When you have selected the sites that you want to include, click **Run** in the top-right corner to start the analysis of your system. Depending on the size of the system's setup, the analysis may take up to five minutes to complete.

4. When the analysis of your system has completed, the **Diagnostic Report** page is displayed. On this page, you can see system information for each site that you included in the analysis. The system information is divided into a number of tabs that all include different information about the site's system setup. The site that comes first alphabetically is shown first when the page opens. You can change the site by selecting another site in the **Sites** pane on the left-side of the page.

5. 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.

You can now upload the file to your support case.

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 XProtect Management Server, open the **Diagnostics Tool.exe** from the relevant file location.

2. From the main page of Milestone Diagnostics Tool, click **Run Diagnostics** to open the **Run Diagnostics** wizard.

3. On the first page of the **Run Diagnostics** wizard, select the sites that you want to include in the system diagnostics. You can search for specific sites in the search bar or click **Select all** to make sure that every camera on all sites are included in the diagnostics.

> ✅ You must select the check box for each individual site for it to be included in the system diagnostics analysis.

When you have selected the sites that you want to include, click **Run** in the top-right corner to start the analysis of your system. Depending on the size of the system's setup, the analysis may take up to five minutes to complete.

4. When the analysis of your system has completed, the **Diagnostic Report** page is displayed. On this page, you can see system information for each site that you included in the analysis. The system information is divided into a number of tabs that all include different information about the site's system setup. The site that comes first alphabetically is shown first when the page opens. You can change the site by selecting another site in the **Sites** pane on the left-side of the page.

5. In the top bar of the **Diagnostic Report** page for the relevant site that you want to view information about, click **Drivers** to open the **Drivers** tab.

6. 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. However, because system administrators can change the name of cameras in the administration applications, either when they are added and set up in the system or at any point after that, for example to name cameras according to their physical location, you cannot rely on the naming information that is shown in the **Name** column to display the exact model and manufacturer of your cameras.

7. Instead, you must look for the **Device Model** column. Click this column to sort the listed cameras alphabetically, according to the device model. If you click the column, an arrow pointing upwards or downwards is added to the column to indicate that sorting has been enabled.

8. To save a log file of the diagnostic analysis and the cameras that were found, click **Save**. To open a log of a previous diagnostics analysis, click **Open**.

Open an existing Diagnostics Report

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

If you want to create a new diagnostics report, see .

> ✅ 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.

With this feature 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 XProtect Management Server, open the **Diagnostics Tool.exe** from the relevant file location.

2. From the main page of Milestone Diagnostics Tool, click on the **Open Existing Report** button.

3. Locate the .MCLOG file from the folder where you have saved it and select **OK** to open it.

If you want to learn more about the report tabs, see Diagnostics Report (properties) on page 9.

Diagnostics Report (properties)

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

System

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

Group name	Contains information about
Operating system	**Version**, **Architecture**, **OS Language**, **Localization**
Memory	**Used**, **Free**, **Total**
Processor	**Name, Number of physical processors, Number of logical processors, No of cores/ processor, Enabled cores, CPU(%), Current Speed, Last Error**
Domain and user information	**Domain name, Current user, Role, Machine**
GPU	**Name**, **Memory**, **Video processor**, **Video mode**, **Driver version**
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 each icon to learn more. You can see **Index**, **Media Type**, **Interface Type**, **Model**, **Size**, **Partitions**, and **Last Error of the selected physical disc**.
Logical drive	Windows partitions *Click on each icon to learn more about each drive. You can see **Description**, **Provider Name**, **Free space**, **Size**, and **Volume name of the logical driver**.

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**

Group name	Contains information about
Installed VideoOS patches	Installed cumulative patches with information for the **Product**, **Patch name**, **Version**, and **Install Date**
Installed MIP Plugins	**Installed MIP SDK plugins** with **Name**, **Version**, and **Install Date**

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 can communicate with remote machines through the 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**
- **Device Model.**

Test

The **Diagnostics report** performs 18 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 the XProtect Management Client.
Service account "Administrator" role membership	The Service account has Administrator rights in the XProtect Management Client.
Windows Updates	There are no pending updates.
Application Pool Status	IIS Application Pools for the VMS are running.
Default Hardware Password	Cameras' passwords are not set to default.
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	The SQL Server location and cluster status are found.

Test	Passed when
status	
SQL database compatibility level	The SQL database compatibility level is found and is set to highest level (currently that level is 150).
Resolve Recorder hostname to IP	The recorder's hostname is resolved to an IP address.
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 machine.

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 .

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 with the Milestone Diagnostics Tool

You can use the user interface to create and export logs. If you want to use the Command prompt instead, see .

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, click **Collect logs**.

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

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

5. (Optional) Check the **Collect site analysis** box to run a System Diagnostics report.

6. Select the time range for the logs. You can choose between one day, week, 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. (Optional) If you want to include a complete or partial SQL database export, select one of the buttons:

    - **Full SQL database 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 include the Log Server backup, select the **Include Log Server backup** check box.

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

13. Click **Collect**.Milestone Diagnostics Tool to will start preparing the files.

14. A message is displayed to inform you when the process is completed. The report is saved as a .ZIP file on your Desktop. You have the options to:

   - Close the window by selecting **OK**

   - Copy the location path by selecting **Copy location**

   - Open the containing folder by selecting **Open folder**

   - Upload the file to Milestone through FTP, by selecting **Upload to FTP**. To learn more, see Share reports on page 23.

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 Diagnostics Tool directory 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)

The 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
/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 Diagnostics Tool command line help in a pop-up window.	none

Collect default logs with Milestone Diagnostics Tool

With Milestone Diagnostics Tool, you can quickly collect the most important details and present them to Milestone Technical Support when necessary. With the Collect Defaults 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 XProtect Management Server, open the **Diagnostics Tool.exe** from the relevant file location.

2. From the main page of Milestone Diagnostics Tool, click the **Collect Defaults** tab to start the process.

3. A message is displayed, informing you that the process is completed. The report is saved as a .ZIP file on your desktop. You have the options to:

   - Close the window by selecting **OK**

   - Copy the location path by selecting **Copy location**

   - Open the containing folder by selecting **Open folder**

   - Upload the file to Milestone through FTP, by selecting **Upload to FTP**. To learn more, see Share reports on page 23

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 machine 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, click on the **SQL Database search** 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.

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 click the **Configuration and Logging** tab.

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

4. Click on one of the three tabs. You can choose between **VMS Log Level**, **VMS Drivers** or **Registry**.

5. Find the component you want to enable debug-logging for and click on its toggle button to enable **Debug**.

> You can enable debug-logging for as many components as you want to. A pop-up window will notify you if the select service requires a restart.

6. When you are done, click **Save** to apply the changes.

Run Debug Monitor

Use the **Debug Monitor** to monitor debug output between the Recording Server and the devices in real time. You can use the monitor to:

- Find a failed device

- Check for dropped camera events

- Troubleshoot camera stream issues.

To create a **Debug Monitor report**:

1. On the XProtect Recording Server, 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.

3. Click **Run Debug Monitor**.

4. Click **Start** 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.

> ✏ **Debug Monitor** changes the log level to Debug for the VMS Drivers.

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

6. Click **Stop** to stop the capture process.

7. 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.

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

Open a Debug Monitor report

The **Debug Monitor** monitors debug output between the Recording Server and the devices in real time. You can view an existing **Debug Monitor report** in Milestone Diagnostics Tool. To create a **Debug Monitor report**, see .

To open an existing **Debug Monitor report**:

1. On the XProtect Recording Server, 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.

3. Select **Open Report**.

4. Browse for an .MMDM file.

5. Click **Open** to view the file. You have the option to:

    - Filter messages from a specific time period

    - Search for messages

    - Include or exclude processes.

Sharing reports

Share reports

Logs and diagnostic reports can help you to determine a root cause of a failure. To share a report with a Milestone Technical Support representative, you can use File Transfer Protocol (FTP).

You can attach the report to an existing support case:

- From the Milestone Diagnostics Tool after reports' collection. See Upload reports to a Milestone FTP server from Milestone Diagnostics Tool on page 23.

- By using a third-party FTP client such as FileZilla. See Upload reports to a Milestone FTP server using FileZilla on page 23.

Upload reports to a Milestone FTP server from Milestone Diagnostics Tool

After you run the **Collect Logs** or **Collect Defaults** report, you have the option to upload the gathered information to an existing support case using FTP.

1. Select **Upload to FTP**. The **FTP Server Credentials** window opens.

2. In the **FTP Server Credentials** window, type in the following information:

   - **MSC Number**: Enter your Milestone Support case number (example: MSCxxxxxx)

   - **FTP address.:** From the drop-down list, select the region that is closer to you (EMEA or US) unless you are instructed otherwise

   - **Username**: Enter the username that was given to you by the Milestone Technical Support representative

   - **Password**: Enter the password that was given to you by the Milestone Technical Support representative

3. Select **OK**. The upload process starts. You receive confirmation upon completion.

You can see the ZIP file in your support case under the **Related** tab.

Upload reports to a Milestone FTP server using FileZilla

> Before uploading, rename your ZIP file, so that it starts with the Milestone Support case number (example MSCxxxxxx - Diagnostics - [site name] - [date] [time].zip).

If you cannot upload your diagnostics report with FTP through the Milestone Diagnostics Tool, you can manually send it with a third-party FTP client. The example below describes the process with the FileZilla FTP Client, however you can upload to FTP using any FTP client.

1. Start FileZilla.

2. Under the toolbar, type in the FTP credentials that were given to you by the Milestone Technical Support representative. The port number is added automatically (the default FTP port is 21).

3. Click **Quickconnect**. An **Insecure FTP connection** window opens. Click **OK** to continue.

4. Browse through the file-tree on the left-side pane to locate your ZIP file and select it.

5. Right-click on the file and choose **Upload**. The transfer of the file starts immediately. If the transfer is successful, a log entry is shown under the **Successful transfers** tab.

You can see the ZIP file in your support case under the **Related** tab.