



MIRASYS 9.9.2 RELEASE NOTES

Release date 7 April 2025

Important Notes

1. Mirasys VMS V9 is only available as a 64-bit version.
2. A V9 Master Server (Management Server) can handle 64-bit V8 and V9 servers.
3. The Complete Installer will automatically install the SQL Server Express 2019 or upgrade an earlier SQL installation to 2019 on 64-bit systems.
4. A 32-bit (x86) SQL Server Express 2008 version will not be upgraded to the 64-bit (x64) SQL Server Express 2014. Update SQL manually before updating from an old 32-bit V7 to the latest 64-bit version!

Supported OS

- Windows 10 IOT/Pro
- Windows 11 (V9.4 or later)
- Windows Server 2016
- Windows Server 2019
- Windows Server 2022 (since V9.5.0)

Free 12-month SMA

Free 12-month SMA offer for new licenses and licenses acquired until December 31st, 2025.



Tel +358 (0)9 2533 3300



Email info@mirasys.com



<https://www.mirasys.com>



VMS V9.9.2 Enhancements

System Manager installer

Mirasys VMS provides a new installer that installs the System Manager application on a dedicated client workstation without the need to install any services. The main server is defined during the System Manager installation.

List Management

Mirasys List Management is optimized to work with up to 5000 identities. The CSV file import and export for the identities and identity lists in the System Manager List Management settings are optimized to support up to 5000 identities.

SMServer API

A new integration HTTP API is available in the SMServer. This API can be used to query the system information, connected VMS servers, and their devices. The API also provides endpoints to query Watchdog events and listen to them in real time.

Separated storage limits for normal and alarm footage

The VMS Server file system storage supports storing alarm and normal footage using different storage retention times. This allows configuring the VMS server to store the alarm footage, including the pre- and post-recordings, longer than the normal footage.

Renewed event mechanism

Mirasys VMS main server provides events to the VMS clients through a NATS event queue, allowing for a more fluent and scalable solution for event delivery. The NATS service is installed with the main server, and the communication uses port 4222. The firewall exceptions for the port to the installed machine are added by the VMS installers automatically if the setting of the firewall exceptions is enabled in the VMS installer.

Component updates

The Chromium browser and email components have been updated to the latest versions. The hardware temperature monitoring library was refactored to use a new library.





VMS V9.9.2 Fixes

System

- Memory usage optimizations are done for servers and clients.
- The VMS server address and port are included correctly in the audit trail log data.
- The DVMS installer repair option does not remove firewall rules.
- The Spotter and SpotterWeb installers work correctly when installed on the same machine.
- The default text data channel name is used correctly throughout the system.
- The Export service handles database access error as intended.
- The DVMS installer doesn't install VCA and SystemManagement service files if the recorder is not selected to be installed.

Spotter

- The Spotter log does not contain errors on the VMS server reconnection.
- Profile search is optimized.
- Access to plugins works as intended after the user is switched and the plugin user rights have changed.
- A clip file is opened without any errors.
- Identities and identity lists are ordered by the identity name and the list name in Smart Recognition, Smart Search, and Smart List Management.
- PTZ camera controls work as intended from a PTZ camera in a plugin placed in a grid.
- The Watchdog event search works as intended when communication encryption is enabled.
- Joystick drivers are cleaned up on the Spotter shutdown as intended.
- The user name is shown correctly in the storage locker history.
- Profile loading works as intended in the Spotter without errors in the log.
- The keyboard shortcuts for selecting and removing cameras work as intended.
- A minor memory leak is fixed when the Spotter window is closed.
- Archive playback works as intended.
- Metadata streaming optimization to avoid unnecessary data copying.
- An image can be exported to the Storage Locker when "Save to Storage Locker" has been selected in the user role image export settings.
- The opening of the Camera Carousel plugin works as intended.

Spotter Web

- 2FA is working as intended with the Spotter Web login.
- Streaming is working as intended based on changes in profile settings.
- User login, layouts, and views work as intended on the first login.





- Streaming in a desktop browser using mobile UI works as intended.
- Tab name saving works as intended.
- Take PTZ control works as intended.
- When clicking the alarm from the alarm list, the video related to the alarm is opened as intended.
- The alarm list is not cleaned up after a tab change or clicking on an alarm.
- The VMS server name is saved in the audit trail log where applicable.
- Video streams work as intended when the user switches tabs.
- Closing SpotterWeb works as intended without any errors.
- SpotterWeb works as intended when a lot of clients are logged in.

System Manager

- The conflicting AI settings are automatically resolved when the camera settings are saved.
- When disabling the RTSP stream in System Manager RTSP settings and keeping the RTSP camera enabled, the settings are saved as intended.
- LPR, FR, and OR settings work as intended with all RTSP stream types.
- LPR, FR, and OR settings work as intended when camera streams are enabled or disabled.
- Adding and removing alarm triggers from the System Manager works as intended.
- Audit trail search works as intended even with large databases.
- Font color is shown correctly in the multi-stream settings.
- Configured List Management lists are shown correctly in the Spotter role Smart List Management settings.
- The profiles list is shown correctly in user group settings when there are a lot of profiles.
- The password is not shown as plain text in the MoxaIO driver settings.
- Setting all user role properties on for the Spotter role works as intended.
- The identities and lists are imported only if the name field is not empty.
- The identity lists are imported correctly from the CSV file.
- After clean installation, the testing of the email settings works as intended.
- Identities and identity lists are ordered by the identity name and the list name in the List Management settings.
- Logging is done at the INFO level by default.
- The exported camera data in CSV format has correctly encoded UTF8 symbols.
- The audit trail search works as intended when filtered by the specified application.
- The face detection region of interest is set to the whole picture when a new identity is added.
- The audit trail log search works as intended when communication encryption is enabled.
- The identities and identity list import from the CSV file work correctly with invalid data input.
- Identity and identity list information input field validation works as intended.
- VMS search works as intended when the user types search text and the system contains failover servers.





System Monitor

- System Monitor log writing works as intended.
- The log export works as intended.
- Logging is done at the INFO level by default.

System Manager Server

- If a parameter does not exist in Database.xml, the SMServer updates the Database.xml file by adding a default value at startup.
- System data update works as intended when 2FA is used.
- Establishing connections from the System Management server to VMS servers and clients is optimized.
- Audit trail data deletion works faster when a lot of audit trail data is removed.
- The re-login and login to the System Manager work as intended.
- The local VMS server's automatic network address change is off by default. You can enable it by configuring the "HandleNetworkAddressChanging" parameter in the SMServer configuration file.
- Look and feel configuration file update works as intended.
- Encrypted communication between SMServer and WDServer works as intended.
- The VMS server and failover server count check works as intended when the servers are connected.
- Storing the Watchdog events from the local VMS server works as intended when the server is removed and readadded to the system.

VMS Server

- Adding and removing alarm triggers from the Alarm Triggering API works as intended.
- The external one-shot alarm triggers work as intended.
- The "moxaiodb.xml" file is included in the settings backup.
- The external alarm trigger channel number is limited to 0 - 32767.
- The Bosch IVA proxy configuration file "BoschIVA.xml" was updated to contain the newest functionalities.
- The VMS server log contains information about all network adapters.
- DatabaseConfigurationFailover.xml file is created by default on the VMS server startup.

Gateway SDK

- The video clip export works as expected.
- The VMS server alarms with an external trigger are handled correctly in the Gateway service and Gateway SDK library.





Spotter Web API

- Sample application can be compiled and executed.

Drivers

AxisIPCapture v2.9.9.0.

- Vaxtor LPR black and white lists work as intended using the AxisIPCapture Driver.
- The “radar” video channel of the AXIS Q1656-DLE camera is working as intended with all supported compression formats.

EHIPCapture driver v2.1.18.0

- The PTZ type for the Hikvision cameras is detected correctly.

WisenetIPCapture Driver v1.2.16.1

- The WisenetIPCapture Driver works as intended with the latest Vaxtor app installed on the Hanwha camera.
- The multichannel devices can be added to VMS if some channels are not configured.
- Support for Hanwha HRX-385 NVR.
- Edge storage works as intended by receiving all recorded material intervals.

EHIPCapture Driver v2.1.19.0

- Hikvision IP Encoder can be added to Mirasys VMS, and video and I/Os work as intended.





OnvifIPCapture Driver v1.9.14.1

- When a camera is added to the VMS server, the video encoder with the highest resolution for the recording stream is selected.
- The H.265 video stream is smooth using the ONVIF driver (the driver handles I and P frames correctly) for the Pelca IBE238-1ER camera.
- The audio stream from the DeskCamera application works as intended.
- All event topics are parsed correctly when users add a camera with profile M support.
- The ONVIF profile M events that are unrelated to any video source work as intended.
- VCA Core service can be added as an ONVIF device to VMS in the “passive” mode.

PanasonicIPCapture v1.6.3.0

- Easy LPR and Smart LPR work as intended with the latest Vaxtor ANPR application installed on the i-PRO camera.
- The timestamp is set correctly for streaming and edge storage.
- Smart Coding features are disabled by default.





Legal Notice for Mirasys Video Management Software Release Notes

Copyright © 2025 Mirasys Oy All rights reserved.

License Agreement: This software and its documentation are provided to the licensed client under the Mirasys License Agreement terms and conditions. By installing, copying, downloading, accessing, or otherwise using the Mirasys Video Management Software, you agree to be bound by these terms. If you do not agree to the terms of this agreement, do not install or use this software.

Copyright Notice: This software and accompanying documentation are copyrighted works of Mirasys Oy. Unauthorized reproduction, distribution, or use of this software and/or documentation may result in severe civil and criminal penalties and will be prosecuted to the maximum extent possible under law.

Disclaimer of Warranty: Mirasys Video Management Software is provided "as is" without warranty of any kind, either express or implied, including but not limited to the implied warranties of merchantability, fitness for a particular purpose, or non-infringement. The entire risk arising out of use or performance of the software remains with you.

Limitation of Liability: In no event shall Mirasys Oy or its suppliers be liable for any damages whatsoever (including, without limitation, damages for loss of business profits, business interruption, loss of business information, or any other pecuniary loss) arising out of the use of or inability to use this Mirasys product, even if Mirasys Oy has been advised of the possibility of such damages.

Third-Party Notices: This software may contain third-party software components that are subject to open-source and third-party license terms. Your use of these components is subject to the terms and conditions of the respective license agreements, which can be found in the documentation or provided with the software package.

Use Restrictions: This software is licensed to the client and is not sold. The software may be used only by the licensed client and its authorized users within the organization. Sharing this software with individuals outside of the organization, or allowing its use by unauthorized users, is strictly prohibited and may result in termination of the license agreement.

Export Control: You agree to comply with all applicable international and national laws that apply to the software, including the export control laws of your jurisdiction as well as the United States.

Changes to Terms: Mirasys Oy reserves the right to make changes to this legal notice and the terms of the license agreement at any time without prior notice. Your continued use of the software will be considered acceptance of such changes.

Governing Law: This notice shall be governed by and construed in accordance with the laws of Finland without giving effect to any principles of conflicts of law.

Contact Information: For any questions regarding this legal notice or the licensing of the software, please contact Mirasys Oy at: <https://support.mirasys.com>



Tel +358 (0)9 2533 3300



Email info@mirasys.com



<https://www.mirasys.com>