Video Management System Security Introduction

Mirasys Oy

12/05/2026

1. Contents

Executive Summary

A video surveillance system is a critical part of an organization's safety infrastructure: these systems are complex and require considering a multitude of factors related to keeping the system safe and secure. The system components themselves, such as the cameras, software, and network, require proper hardening measures. In addition to this, other considerations must also be accounted for, such as laws and regulations.

This whitepaper covers extensive safety documentation for the Mirasys Video Management System. The purpose of this document is to provide customers with the needed information regarding the security of the system. The paper includes descriptions of how safety measures are implemented in the system, how the system complies with standards and regulations, and how end users can ensure the safety of the system when it is in use.

This document starts with an introduction to the Mirasys VMS by covering the system architecture, applications and services, and with an introduction to the most common attack vectors that are used to exploit video surveillance systems. The next topics covered are physical safety considerations, identity and access management, and network security, moving on to camera hardening and video data integrity and protection. Lastly, the document includes sections for AI usage, resiliency and high availability, compliance with standards and regulations, and maintenance and lifecycle management. The contents of this document are based on industry best practices and standard VMS Security frameworks.

This document is for customers of Mirasys who are actively using the Mirasys VMS in their organization or are planning to start using it. The target audience for this documentation is the organization's personnel, such as security officers, system architects, and IT managers.

The information provided in this document is intended to complement, not replace, any legal or regulatory requirements that may be applicable to the organization. It is the responsibility of each organization to ensure compliance with all relevant laws, regulations, and industry standards, as well as to adopt the recommendations in this document to suit their unique environment and risk profile.

2. Introduction to Mirasys and VMS Security

Mirasys software is a distributed digital video management system (VMS) used for video and audio surveillance applications. Mirasys's solutions are designed to seamlessly integrate with existing security infrastructures while offering flexibility, scalability, and ease of use.

The Mirasys software can monitor both real-time video and recorded video, audio, and text data. It can be used to control PTZ cameras, I/O devices, and IP cameras. The software implements an alarm mechanism that utilizes both internal and external event triggers to initiate and terminate an alarm, and performs actions defined by the user. The software supports systems consisting of digital surveillance cameras and the creation of analog, digital, or hybrid (consisting of both analog and digital surveillance cameras) surveillance systems. A centralized surveillance system domain can consist of a network of up to 150 local or remote VMS Servers.

In this document, the Mirasys Video Management System will be referred to with the term VMS, or simply "the system".

Defining the Video Management System architecture

Mirasys Video Management System has two main parts: Mirasys applications and Mirasys VMS server hardware. The software runs on a Windows platform. The VMS servers and client applications communicate with each other over the network. The system architecture is visualized in Figure 1.

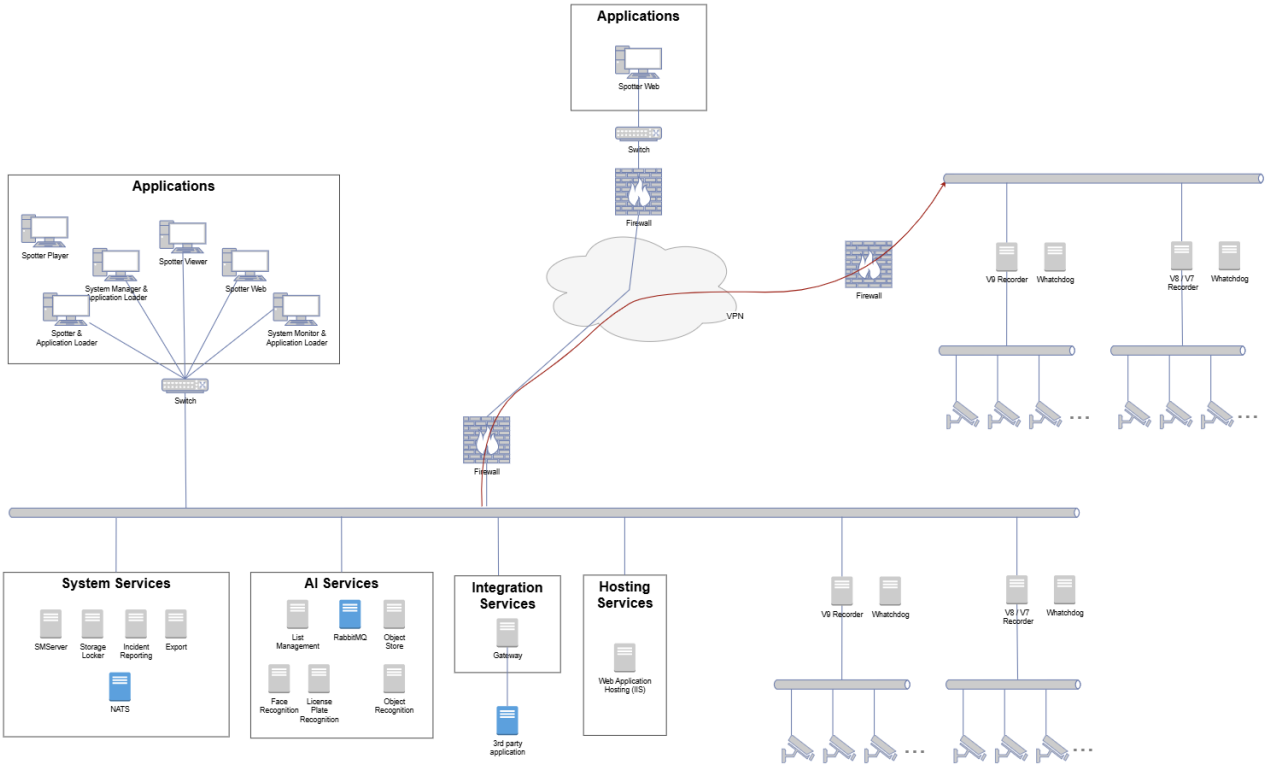

Figure 1

The Mirasys VMS system architecture includes several applications and services, which are briefly introduced in the following sub-sections.

Applications

Spotter

Spotter is the primary desktop monitoring application. A Spotter client contacts the SMServer and the DVRServer services of the VMS, and accesses the connected devices, allowing it to access live and recorded surveillance data.

System Manager

System Manager is the primary system management and configuration application. It contacts the SMServer and the DVRServer services of the VMS to access information about the system. The application allows a user to add, modify, and remove servers, cameras, and other devices to the service, manage alarm conditions and actions, and more.

Spotter Web

Spotter Web is an HTML5-based client application that can be used on a web browser from any computer on the Internet. Supported browsers for Spotter Web are Edge, Chrome, and Firefox.

Spotter Player

Spotter player is a single executable file and can be run without installing any other components on a Windows machine. Spotter player can be used to open and playback archives, SEF, and ASF clips. Spotter Player is installed with Spotter.

System Monitor

System Monitor is a desktop application for system administrators to monitor the state of the VMS system. The application can also export recorder, client, and system management logs.

VAU (VMS Application Updater)

VAU is used to automatically update user applications to the latest versions from the main SMServer. VAU is installed during application installation, and the application is started automatically when System Manager, System Monitor, or Spotter is run.

Spotter Viewer

Spotter Viewer is a client application for viewing streams from Spotter, available for VMS version 9.10.0. The Spotter view sharing functionality makes it possible for operators to share their Spotter view, allowing workers without surveillance rights or device access to see the shared view in the Spotter Viewer application.

System Services

SMServer

SMServer is the main server service. SMServer is used to assign a server in the system as a main server that acts as the focal point in communicating with the client applications and the other servers in the system.

DVRServer

DVRServer is the service installed on servers set up as recording devices in the VMS network. This sets them up to store data sent by the devices.

WDServer

Watchdog server is a service that functions as a system monitor. It monitors local DVRServer and SMServer services and is responsible for seeing that both services are running and operating normally.

GatewayServer

Gateway server can be used to integrate 3rd party systems with Mirasys VMS.

Incident reporting service

Incident reporting is a Spotter plugin for accessing incident reporting services and storing incident report data in the incident report database.

Storage Locker

The Spotter Storage Locker is a Spotter plugin for accessing storage locker content. It can be used to search, edit, or delete a stored item, open a selected picture, video clip, or camera audit report PDF file for viewing, or save a file of a similar type to the disk.

Export service

The export service is a Windows service used by Spotter Web to create video exports.

AI services

AI services carry out AI-based recognition and provide functionalities based on it. AI services consist of List Management (LM), Face Recognition (FR), License Plate Recognition (LPR), Object Recognition (OR), and Object Data Store (ODS).

3. Identifying Major Attack Vectors for Security Camera Systems

Vulnerabilities and Attack Vectors

Video surveillance systems can generally have various vulnerabilities that expose them to different threats. Common vulnerabilities include the following:

Application-Level Vulnerabilities: The software itself can contain security vulnerabilities, such as insufficient authentication methods and session management threats.

Camera Hardware and Firmware Issues: There are several issues regarding the physical cameras in the system setup. Common issues include using weak/default passwords, outdated firmware, poorly managed access control, and possible memory corruption.

Network Security Weaknesses: Weaknesses related to network security include unprotected data transmission, use of vulnerable communication protocols, insufficient encryption, and compromised network devices.

Protocol Vulnerabilities: Protocol vulnerabilities include the use of outdated TLS versions, insecure DNS configuration, HTTP security gaps, and RTSP weaknesses.

Storage System Risks: Risks related to storage systems include unsecured backup systems, poor storage footage encryption, insufficient access control for stored data, and unprotected physical storage devices.

System vulnerabilities can be used as attack vectors by hackers. There are several ways to infiltrate the system that are made possible by different vulnerabilities arising from security flaws. Common attack vectors include the following:

Dictionary-based password attacks: Dictionary attacks are commonly used as a way to automate password guessing. A dictionary attack is especially effective when default passwords or otherwise commonly used passwords are used. Passwords will be easier to guess also when the system's password requirements are not complex enough.

Backdoor exploitation: Hidden system access points are exploited by attackers in backdoor attacks when, for example, developer testing interfaces are left active in production, maintenance access points are left undocumented, or firmware vulnerabilities enable remote code execution.

Man-in-the-Middle attacks: This type of attack occurs when a hacker intercepts data transmission between the components of the surveillance system. This attack makes it possible to capture live video streams, modify transmitted data, inject false information, redirect communication paths, and collect system credentials.

Network-based exploits: Network vulnerabilities can be exploited by redirecting network traffic, DNS poisoning attacks, TCP/IP exploitation, wireless network infiltration, or port scanning and exploitation.

Social engineering techniques: With this technique, the attacker takes advantage of the human element of the system. Social engineering methods include phishing emails to system administrators, impersonation of personnel, and false maintenance requests.

Measures for Protection

For the best protection of the system, several security measures should be implemented. The most important recommended measures can be briefly summarized as follows:

Updating the system regularly, including hardware and software across all system components: Updates often come with patching security issues, which helps with reducing vulnerabilities in the system. Updates should be completed immediately after release.

Implementing strong authentication protocols and password policies for the system: Multi-factor authentication is recommended for enhanced protection of user accounts. Passwords will be more difficult to crack if the system requires them to be complex, and strong authentication protocols make third-party intrusion more challenging.

Encrypting data transmission for all network components: Proper data encryption is required so outsiders can't access sensitive data.

Continuously monitoring the system to catch any suspicious activity early on: Having a proactive mode of operation is crucial in protecting the system against attacks.

Comprehensive training for staff on security practices: Staff training is important for security breach prevention and keeping the system safe. All staff must have a

clear understanding of basic cybersecurity, and training for staff members who have access to the VMS should be emphasized.

Use full hard drive encryption: For additional security, hard drives should be protected with full encryption. Full encryption can be enabled for Windows systems used by organizations with the BitLocker Drive Encryption feature.

Implementing the security measures in practice for the Mirasys VMS will be discussed in the later sections of this white paper.

4. Physical & Infrastructure Security

Servers (physical and virtual), network, software applications, and cameras are key VMS components that require protection. This section describes hardening measures for physical VMS components to ensure a high standard of system security.

Mirasys recommends following the physical and environmental protective measures described in Security and Privacy Controls for Information Systems and Organizations (NIST Special Publication 800-53 Revision 5). The hardening measures described in this measure are based on this publication.

Server Hardening

Overview

Server hardening is a general system hardening process that involves securing a server's data, ports, components, functions, and permissions using advanced security measures at the hardware, firmware, and software layers.

These general server security measures include, but are not limited to:

- Keeping a server’s operating system patched and updated.
- Regularly updating third-party software essential to the operation of the server and removing third-party software that doesn’t conform to established cybersecurity standards.
- Using strong and more complex passwords and developing strong password policies for users.
- Locking user accounts if a certain number of failed login attempts are registered, and removing needless accounts.
- Disabling USB ports at boot.
- Implementing multi-factor authentication.
- Using self-encrypting drives or AES encryption to conceal and protect sensitive information.
- Using firmware resilience technology, memory encryption, antivirus and firewall protection, and advanced cybersecurity suites specific to your operating system.
- Restrict access to servers. Keep servers in locked rooms and make it difficult for intruders to access the network and power cables.

Hardening Measures

1) *Use physical access controls and monitor the server room*

Mirasys recommends placing the hardware with the servers installed in a designated server room and using physical access controls. In addition, you should maintain access logs to document who has had physical access to the servers. Surveillance of the server room is also a preventive precaution.

Mirasys supports the integration of access control systems and their information. For example, you can view access logs in System Manager with the audit log search.

2) *Use encrypted communication channels*

Mirasys recommends that you use a VPN for communication channels for installations where servers are distributed across untrusted networks. This is to prevent attackers from intercepting communications between the servers. Even for trusted networks, Mirasys recommends using HTTPS to configure cameras and other system components.

3) *Run services with service accounts*

Mirasys recommends that you create service accounts for services related to Mirasys VMS instead of using a regular user account. Set up the service accounts as domain users and only give them the permissions required to run the relevant services. For example, the service account should not be able to log on to the Windows desktop.

5) *Run components on dedicated virtual or physical servers*

Mirasys recommends that you run the components of Mirasys VMS only on dedicated virtual or physical servers without any other software or services installed.

6) *Restrict the use of removable media on computers and servers*

Mirasys recommends that you restrict the use of removable media, for example, USB keys, SD cards, and smartphones, on computers and servers where components of Mirasys VMS are installed. This helps prevent malware from entering the network. For example, allow only authorized users to connect removable media when you need to transfer video evidence.

7) *Use individual administrator accounts for better auditing*

Mirasys recommends using individual accounts for administrators instead of shared administrator accounts. This lets you track who does what in the VMS to help prevent malware from entering the network. You can then use an authoritative directory such as Active Directory to manage the administrator accounts. You assign administrator accounts to roles in System Manager\User group\System Manager Enterprise role.

8) *Use subnets or VLANs to limit server access*

Mirasys recommends that you logically group different types of hosts and users into separate subnets. This can have benefits in managing privileges for hosts and users as members of a group with a given function or role.

Design the network so that there is a subnet or VLAN for each function (for example, one subnet or VLAN for surveillance operators and one for administrators). This allows you to define firewall rules by group instead of individual hosts.

Management Server

Mirasys recommends enabling only the ports used by the management server and blocking all other ports, including the default Windows ports (see detailed information on ports in section 6: VMS Communication and Ports). This guidance is consistent for the server components of Mirasys VMS.

Recording Server

Mirasys recommends using multiple network interface cards (NICs) to separate communication between recording servers and devices from the communication between recording servers and client programs. Client programs do not need to communicate directly with devices, except for ThruCast, for which the Spotter Client needs direct access to devices.

Camera Hardening

Cameras are a key part of the surveillance system. Mirasys has several recommendations for VMS camera hardening.

1) *HTTPS encryption and certificates*

Mirasys recommends using HTTPS to configure cameras and other system components, even in trusted networks. HTTPS encryption requires creating an access certificate. Whenever possible, use a certificate (SSL) to protect camera authentication and communication.

2) *Camera communication*

Connect the camera subnet only to the recording server subnet. The cameras and other devices need to communicate only with the recording servers, apart from when ThruCast is used by Spotter.

3) *Wireless cameras and location considerations*

Don't use wireless cameras in mission-critical locations. Wireless cameras are easy to jam, leading to video loss.

4) *Separate VLANs*

Set the cameras on separate VLANs and use HTTPS for the camera-to-recording server communication.

5) *Firmware updates*

Use the latest firmware to minimize the possibility of vulnerabilities being present. The latest firmware versions typically include patches for known vulnerabilities that attackers may try to exploit.

6) *Physical protection*

Use camera enclosures to physically protect the cameras from damage and tampering attempts.

Note that in addition, it is always recommended to follow hardening guidelines provided by the camera manufacturer for the specific camera model in use.

Protection of Network Cabling

Along with a clear topology, planning the routes of physical connections through a building or site can save a lot of time. Mapping the devices and cabling in a site, even if it's a three-room section of a floor, can help in selecting the cabling that will be used as well as the placement of the devices.

With cabling, the appropriate length cabling should be used to reduce the chance of interference or overheating coming from coiled cables or straining them when they're slightly too short for the required distance. Distances between the ports on networked devices need to be pre-planned or measured to ensure the correct cable is obtained for it.

Cable labelling can be done with taped labels or with cable colors. Colors will help with grouping the cables to the connection groups they're a part of. Cables should also be bunched or guided to make sure they do not get tangled. Using cable trays can keep them out of the way and prevent any tripping or snagging hazards. The actual cables themselves should be planned based on the estimated amount of interference they might face on their routes.

Electromagnetic interference (EMI) affecting cables can lead to image quality deterioration or even complete image loss. Standard cables are UTP (Unshielded

Twisted Pair) cables. When interference is expected or encountered, STP (Shielded Twisted Pair) cables should be used.

Elements that cause EMI:

- **High Voltage Wiring**: Power wiring can interfere with data transmission even when run parallel to each other. Even wiring running a compliant distance apart within a grounded raceway can be a source of video interference. The best practice is that any data cabling sharing the same raceway with power cables, regardless of how either is contained, must be run using an STP cable.
- **Inductive Sources**: Data cabling near common electromechanical components like electric motors, power transformers, magnetic coils, or solenoids can introduce significant EMI.
- **Radio sources**: Common low-powered communication radios disrupt data transmission. High-powered repeaters or transmitters necessitate the use of STP to eliminate problems.
- **Fluorescent Lights**: Fluorescent lights are prone to light fixtures and can cause interference to cable bundles in overhead cable runs. Cable trays or STP cables should then be used.

Infrastructure Protection

Mirasys recommends following the environmental protective measures described in Security and Privacy Controls for Information Systems and Organizations (NIST Special Publication 800-53 Revision 5):

> *Fire and water damage protection:* Employ and maintain fire detection and suppression systems that are supported by an independent energy source. Protect the system from damage resulting from water leakage by providing master shutoff or isolation valves that are accessible, working properly, and known to key personnel.
>
> *Environmental controls:* Maintain organization-defined environmental controls such as temperature, humidity, pressure, or radiation levels within the facility where the system resides at organization-defined acceptable levels and monitor environmental control levels at organization-defined frequency.
>
> *Safe location of system components:* Position system components within the facility to minimize potential damage from organization-defined physical and

environmental hazards and to minimize the opportunity for unauthorized access.

Emergency shutoff, power, and lighting: Provide the capability of shutting off power to the system in emergency situations. Provide an uninterruptible power supply to facilitate an orderly shutdown of the system or transition of the system to long-term alternate power in the event of a primary power source loss. Employ and maintain automatic emergency lighting for the system that activates in the event of a power outage or disruption and that covers emergency exits and evacuation routes within the facility.

Software Application and OS Hardening

Software Application Hardening

Software application hardening, or just application hardening, involves updating or implementing additional security measures to protect both standard and third-party applications installed on your server.

Unlike server hardening, which focuses more broadly on securing the entire server system by design, application hardening focuses on the server's applications, specifically including, for example, a spreadsheet program, a web browser, or a custom software application used for a variety of reasons.

At a basic level, application hardening involves updating existing or implementing new application code to secure a server further and implementing additional software-based security measures.

Examples of application hardening include, but are not limited to:

- Patching standard and third-party applications automatically
- Using firewalls
- Using antivirus, malware, and spyware protection applications
- Using software-based data encryption
- Using CPUs that support Intel Software Guard Extensions (SGX)
- Using an application (eg. LastPass) to manage and encrypt passwords for improved password storage, organization, and safekeeping
- Establishing an intrusion prevention system (IPS) or intrusion detection system (IDS)

Spotter Hardening

1*) Restrict physical access to any computer running Mirasys Spotter:* Mirasys recommends that you restrict physical access to computers running Mirasys Spotter. Allow only authorized personnel to access the computers. For example, keep the door locked, and use access controls and surveillance.

2*) Always use a secure connection by default, particularly over public networks:* If you need to access the VMS with Mirasys Spotter over a public or untrusted network, Mirasys recommends using a secure VPN connection. This helps protect communication between Mirasys Spotter and the VMS server.

3) *Create a customer Mirasys Spotter Enterprise role:* Turn on only required features and turn off features that a surveillance operator does not need. The point is to limit opportunities for misuse or mistakes.

4) *Use separate names for user accounts:* Mirasys recommends creating a user account for each user and using a naming convention that makes it easy to identify them personally, such as their name or initials. This is the best practice for limiting access to only what is necessary and reducing confusion when auditing.

5) *Prohibit the use of removable media:* For video exports, establish a chain of procedures that are specific to evidence. Mirasys recommends that the security policy allows only authorized Mirasys Spotter operators to connect removable storage devices such as USB flash drives, SD cards, and smartphones to the computer where Mirasys Spotter is installed. Removable media can transfer malware to the network and subject video to unauthorized distribution. Alternatively, the security policy can specify that users can export evidence only to a specific location on the network or to a media burner only. You can control this through the Mirasys Spotter Enterprise Plus role.

System Manager Hardening

1) Allow administrators to access relevant parts of the VMS: If a setup requires multiple administrators, Mirasys recommends configuring different administrator rights for administrators who use the System Manager.

2) *Run the System Manager on trusted and secure networks:* If you access the System Manager over HTTP, the plain text communication can contain unencrypted system details. Mirasys recommends that you run the System Manager only on trusted and known networks. Use a VPN to provide remote access.

OS Hardening

Each version of the Mirasys VMS software is tested and supported on a specific set of Windows operating systems. Please always refer to the Installation Guide of your specific Mirasys VMS software release to check the supported operating system and other system software module versions. Mirasys VMS V9 supports the following operating systems (as of 04/2026):

Operating System	Server with analogue camera support via encoders	Server with only IP cameras or connected video servers (encoders)	Gateway server	System Manager application	Spotter application
Windows 11	**-**	**X**	**X**	**X**	**X**
Windows Server 2016	**-**	**X**	**X**	**X**	**X**
Windows Server 2019	**-**	**X**	**X**	**X**	**X**
Windows Server 2022	**-**	**X**	**X**	**X**	**X**
Windows Server 2025	**-**	**X**	**X**	**X**	**X**

Ensuring that the operating system on which the VMS is installed is configured safely is crucial. Some general guidelines that can be applied to many different system components are also useful when it comes to securing the OS:

1) *Remove or disable unnecessary services*
To help avoid unauthorized access or information disclosure, Mirasys recommends that you stop unused services and protocols on devices. Deactivating or deleting unnecessary services makes it more difficult for attackers to get access to your system.

2) *Firewall configuration*
Set up your firewall so that only the needed traffic that can be verified to be legitimate is allowed.

3) *Implementation of access controls*
Only authorized users should be allowed to access the system. It is recommended to follow the principle of least privilege (i.e. only the rights required to take care of necessary tasks are provided to the user).

4) *Use authentication mechanisms*
Users should be required to use a password that fulfills the criteria for a strong password. Multi-factor authentication is recommended for extra protection.

5) *Data encryption*
Data should be protected both at rest and in transit. This should be done with secure encryption methods to guarantee that data is kept safe.

The Center for Internet Security (CIS) has the following recommendations specifically for hardening the Windows OS (CIS Microsoft Windows 10 Enterprise (Release 1803) Benchmark v1.3.0 – 10-30-2017 & CIS Microsoft Antivirus Benchmark v1.0.0 – 02-20-2026):

- Using Microsoft Defender Antivirus with the proper configurations (For more detailed information, see CIS Microsoft Antivirus Benchmark v1.0.0)
- Password policy
    - User Accounts Shall Use Long Passwords - Where multi-factor authentication is not supported, user accounts shall be required to use long passwords on the system (longer than 14 characters)
    - All Accounts Have A Monitored Expiration Date - Ensure that all accounts have an expiration date that is monitored and enforced.
    - Encrypt/Hash All Authentication Files and Monitor Their Access - Verify that all authentication files are encrypted or hashed and that these files cannot be accessed without root or administrator privileges. Audit all access to password files in the system.
- Account lockout
    - Configure Account Lockouts - Use and configure account lockouts such that after a set number of failed login attempts the account is locked for a standard period of time.
    - Ensure Workstation Screen Locks Are Configured - Configure screen locks on systems to limit access to unattended workstations.
- Local policies / User rights assignment

    - Minimize And Sparingly Use Administrative Privileges - Minimize administrative privileges and only use administrative accounts when they are required. Implement focused auditing on the use of administrative privileged functions and monitor for anomalous behavior.
    - Perform Regular Account Reviews - Review all system accounts and disable any account that cannot be associated with a business process and owner.
- Windows Firewall
    - Leverage Host-based Firewalls - Apply host-based firewalls or port filtering tools on end systems, with a default-deny rule that drops all traffic except those services and ports that are explicitly allowed.

CIS also has other benchmarks available for different operating systems (eg. specific Windows OS's). Mirasys recommends referring to guidelines that are specifically tailored for the operating system in use.

5. Identity & Access Management (IAM)

Two-Factor Authentication

Strong authentication protocols are essential in ensuring system security. The VMS software supports two-factor authentication (2FA), which can be enabled for chosen user groups. Two-factor authentication improves your security by requesting the username and password upon login and a code from an external physical device. Among other things, this provides an added layer of security and should prevent users from sharing their credentials.

When 2FA has been enabled for a user group and a user in that group logs in for the first time, the user is requested to use or install the 2-factor authentication client (eg. Authy, Google Authenticator, MS Authenticator) on their mobile device. The VMS and the authentication client are synchronized with the VMS: this is done by transferring the secret key generated by the VMS to the authentication software via QR code or by directly typing it into the software. The authentication client automatically generates new one-time passwords. The passwords also change periodically and are kept in sync as the VMS clocks and the authentication app have the same time (note that this does not require any direct data communication link between the software).

If a user forgets their 2-factor secret key, the administrator can reset it from the System Manager. After the 2-factor secret key reset, the user needs to update the private key the next time they log in.

Role-Based Access Control (RBAC)

Mirasys recommends that you only allow access to functionality for a select user set that needs this permission, or in other words, apply the principle of least privilege (PoLP). Only the system administrator can access the system and perform tasks by default. All new roles and users that are created have no access to any functions until an administrator deliberately configures them.

It is also recommended to set up permissions for all functionality, including viewing live video and recordings, listening to the audio, accessing metadata, controlling PTZ cameras, accessing and configuring, removing privacy zones on the client, working with exports, saving snapshots, and so on.

Access should be granted only to the cameras that the specific operator needs to access, and it is recommended to restrict access to recorded video, audio, and metadata for operators, either completely or grant access to only the video, audio, or metadata recorded in the past few hours or less.

Regularly assess and review roles and responsibilities for operators, investigators, system administrators, and others with access to the system.

The system supports the following types of user roles (defined through user groups):

- **System Manager role:** Administrators are allowed to log in to System Manager and change all settings, such as changing camera settings or adding new profiles or user accounts.
- **Monitoring role:** Users with monitoring rights are allowed to log in to System Manager and monitor the system on the **System** tab, but they are not allowed to change the settings.
- **Gateway role:** If this role is active, the user group can access the DVMS gateway.
- **Mirasys Spotter Enterprise role:** End users can log in to Spotter but not to System Manager.
- **Spotter Web role:** End users with this role can log in to Spotter Web.

Mirasys recommends limiting the number of users with a System Manager role. Suppose you need to create multiple Administrator roles: in that case, you can restrict their access by creating Administrator roles that can manage only select parts of the system, such as certain devices or functions.

Mirasys also recommends that the VMS administrator does not have full administrator rights. Mirasys VMS allows setting different kinds of permissions in the following areas:

- System
- VMS Servers - Profiles
- Users

Domain-Based User Groups (LDAP)

The system supports domain-level user rights integration (Microsoft Active Directory, LDAP), enabling users to be synchronized from domain groups. Domain-based users can log into the VMS with their domain usernames and passwords. By default, user group rights are synchronized with their parent domain every 30 minutes (if you need to change the default interval, please contact your system supplier). This feature requires a license update.

Password Policies

Default Passwords and Securing Transmission

One of the key aspects of cybersecurity is to configure all needed devices and to use non-default passwords. Default logins and passwords are always the first to be tried in an attack. Always set new passwords for cameras and other devices and change your devices' passwords regularly.

Another important part when it comes to passwords is to have them secured when transmitted over a network. Password transmissions between VMS clients and servers are secured with public key encryption. However, if you do not use a password at all, attackers snooping the network connection are able to see this.

Second Password

It is possible to configure the system to require two separate passwords for all users. This is done by activating the "Second password in use" option in the general system settings. When this mode is selected, users are required to give two passwords. The default second password is empty. This feature ensures that no single person can review videos alone: if one password is known to one person and the other password is known to another person, both persons must be present when reviewing videos.

Password Strength

A strong password is at least 8-10 (recommended 12-14+) characters long, has both upper- and lower-case letters, and has special characters and numbers in it. Even if your password is strong, the best practice is to change it regularly.

One should avoid words and phrases that are easily guessed (such as password12345), as crackers can test dictionary words in passwords along with brute force cracking, in which each possible character combination is tried one by one. Computers can also harness graphics cards (GPUs, Graphics Processor Units) to number-crunch the passwords and try each one.

Moore's law dictates that computing power doubles every two years. With multiple GPUs per computer, newer GPUs becoming available, distributed computing and botnets, computer systems with unrestricted login attempts could face significant attempts at breaking through.

If your password is to be made of a phrase or certain words, they should be as obscure as you can think of, and they need to be turned into a form that is as complex as it can be through character substitution and spelling corruption. User-defined passwords

made primarily through word generation can be strengthened through character swapping. Character substitution is a simple way of increasing password complexity. Randomly generated passwords also use the same character ranges.

Session Management

Session timeout can be configured for a specific user or a user group in the VMS. The system is locked after a certain time of user inactivity has passed, and the user must re-enter their user credentials if they wish to continue using it. The timing for session timeout can be configured to be between 1 minute and 24 hours.

It is also possible to enable automatic log-off, which will close the software. Similar time configuration options are available for this option as for automatic locking. If the System Manager Enterprise Role is activated, the users with this role have the setting available to enable logging other users off on login.

6. Network Security & Data Transmission

Network Topology Recommendations

A clear network topology is useful in narrowing down network bottlenecks, failure points, and sections that could be improved or expanded. A network topology should map the whole network that the system will encompass. This includes cameras, recording devices running DVRServer and other servers, decoders, connection types, network switches, and any workstations with Spotter for Windows and System Administrator applications installed and connected to the network. Also, if the VMS network is connected to the Internet, firewalls or gateway servers should be included in the topology.

Networks the devices have been assigned to should also be marked, as well as device IPs on the relevant connections. Switches and routers should have their interfaces marked as well, either on the topology itself or on a list close to the devices. If VLANs have been assigned, these need to be marked as well. The software contained within the end devices doesn't need to be marked, but should still be recorded in the documentation as well.

Example Network Topology

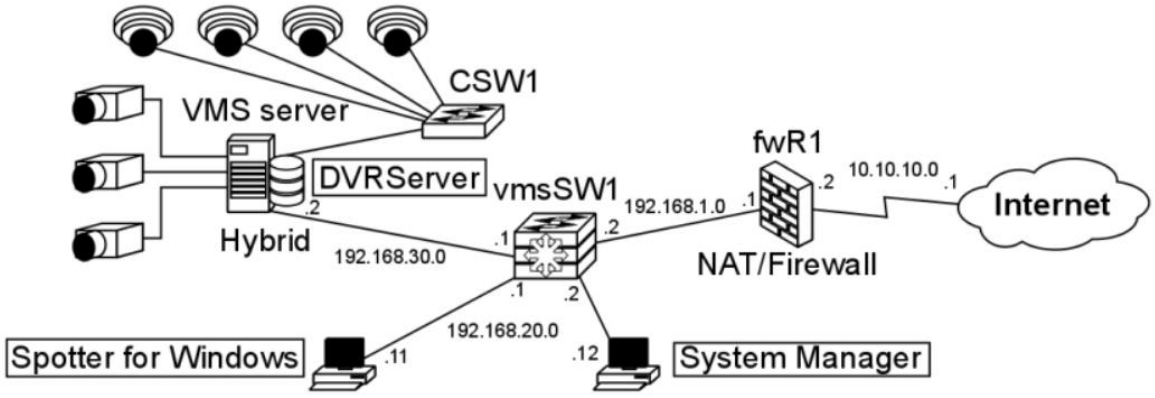

Figure 2

The example topology in Figure 3 has the VMS network connected to the Internet through a firewall running NAT. The clients and the hybrid recording VMS server (running SMServer) are connected to the firewall through a Layer 3 switch, so the connections within the network can be segmented into their own subnets.

There are several analogue cameras connected to the VMS via encoders. The camera network is connected to the DVRServer through an unmanaged Layer 2 switch, so their

packets are switched by MAC addresses alone. Segments of the VMS are placed under their own subnets for easier navigation and possible expansion, e.g., with more users or more servers. These subnets can be placed under VLANs in the Layer 3 switch's configuration.

Camera Isolation

The best practice for system security and network performance is to have the cameras separated from the rest of the network so that there is less chance for camera signals to face interference from other traffic in the system, and to improve system security as a safeguard against unwanted connections. This can be done in two ways: having cameras physically separated or having them logically separated. Physically separating cameras would involve connecting them to their own local network switch and having the switch connect to a recording server's network adapter assigned to the camera network. An example topology of this network principle is presented in Figure 4.

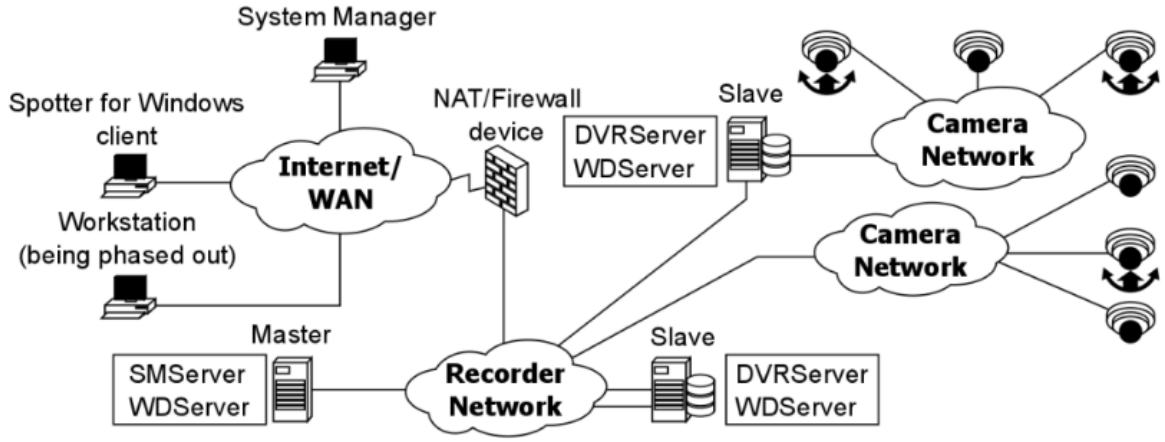

Figure 3

Another method of separating the cameras in the network would be to use VLANs (Virtual LAN) on the switch to logically separate them into their own virtual network. This manner of networking should be left for smaller operators and isolated surveillance sites with their own ICT workers. An example of this network principle is presented in Figure 5.

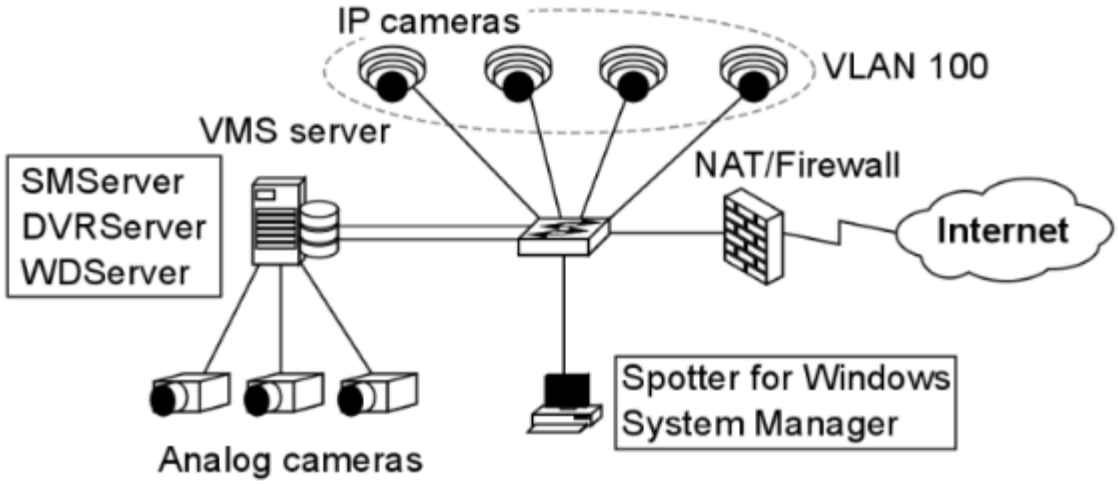

Figure 4

VLAN Configuration

VLANs are configured on switches to segment the device's ports for enhanced data traffic control. Setting up a VLAN is an alternative to setting up physical segmentation for a network. It is recommended that you consult an ICT expert or your IT department before planning and configuring VLANs on your VMS network's networking devices.

Layer 2 switches forward data based on device MAC addresses, and any VLANs configured on the switch would shunt data from certain ports to named trunk ports. This can be used in isolating the camera network to communicate with only a VMS server's network card. Any VLANs configured on a Layer 2 switch cannot communicate with each other without the device being connected to a Layer 3 network device and the VLANs trunked to it through the interface connecting it.

Layer 3 switches with IP routing can support multiple VLANs that can communicate with each other, as data is routed based on target IP addresses.
Each VLAN could also oversee its own subnet, and IP addresses need to be assigned for them.

One example of a VLAN setup in the VMS would have (if all system devices are ultimately connected to the same Layer 3 switch) a VLAN for the camera network, a VLAN for the recorder network's camera network NICs, a VLAN for the recorder network's server-server/server-client network NICs along with the SMServer's NIC and a VLAN for local computers running Spotter for Windows and System Manager.
Ports should be reserved for these purposes as needed. Layer 2 switches can be used to allow more devices to be connected to the network if these are connected to the VLAN-configured ports.

VLANs can be used across multiple switches. Having multiple VLANs in the network will necessitate having routing capabilities in the network to route IP packets between the VLANs. This can be done with a Layer 3 switch, a router, or a router-on-a-stick, where you have a routing device with a single LAN connection to the Layer 2 switch. The device routes between the VLANs, allowing traffic between them.

With VLAN segregation, the exact physical location of each system device is largely irrelevant to the network. To the network, VLANs are their own local networks that the router routes traffic between. With multiple VLANs, each device needs to have an IP address configured, so the Layer 3 device can route the traffic between them.

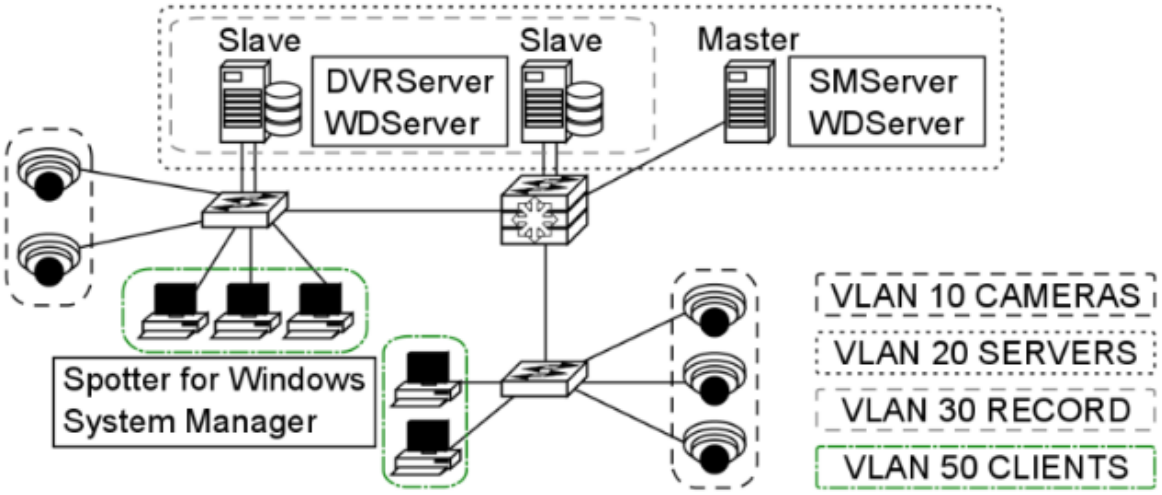

Figure 5

Inter-VLAN routing requires configuring the Layer 3 switch and enabling routing on it. Specific actions and commands are dependent on the manufacturer of the device, but usually, the procedure is as follows:

1. Enable IP routing
2. Assign addresses to the VLANs (e.g. VLAN 10 would have 192.168.10.1/24)
    - These will be the default gateways for the end devices in the VLANs
3. Configure a default route for the switch

VMS Communication and Ports

Applications are used to open communication with and between the system's servers, and to send connection requests to servers. Servers accept connection requests from applications or from other servers. Communication between the system components is implemented with TCP/IP protocol through TCP ports 5008-5011.

Mirasys recommends that you use secure connections and the following additional steps:

- Use secure device authentication
- Use TLS
- Use device whitelisting to authenticate devices
- Use firewalls to limit network communication between servers and client computers and programs.

Ports used by the VMS components are listed in the following tables.

Management Server (Main server)

TCP	inbound/outbound	
4222	in	C:\Program Files\DVMS\SystemManagement\NATS\nats-server.exe
5008	in	C:\Program Files\DVMS\SystemManagement\SMServer.exe
5009	out	C:\Program Files\DVMS\SystemManagement\SMServer.exe
5010	out	C:\Program Files\DVMS\SystemManagement\SMServer.exe
8082	in	C:\Program Files\DVMS\SystemManagement\SMServer.exe
8086	in	C:\Program Files\DVMS\IncidentReporting\ADVIncidentReporting.exe
8087	in	C:\Program Files\DVMS\StorageLocker\ADVStorageLocker.exe
8088	in	C:\Program Files\DVMS\Export\ADVExportService.exe

VMS Server (Recording Server)

TCP	inbound/outbound	
5009	in	C:\Program Files\DVMS\DVR\DVRServer.exe
5010	in	C:\Program Files\DVMS\DVR\WDServer.exe
5011	in	C:\Program Files\DVMS\DVR\DVRServer.exe
5013	in	C:\Program Files\DVMS\DVR\DVRServer.exe
554	out	C:\Program Files\DVMS\DVR\DVRServer.exe
80	out	C:\Program Files\DVMS\DVR\DVRServer.exe
443	out	C:\Program Files\DVMS\DVR\DVRServer.exe
7001 -> RTSP Server Streaming	out	C:\Program Files\DVMS\DVR\DVRServer.exe
UDP	**inbound/outbound**	
3556-4556	out	C:\Program Files\DVMS\DVR\DVRServer.exe

Client Applications

TCP	inbound/outbound	
4222	out	C:\Program Files\DVMS\VAU\Vau.exe C:\Users\<user>\AppData\Roaming\DVMS\spotter\<versionnumber>\<master server>\spotter.exe C:\Users\<user>\AppData\Roaming\DVMS\systemmanager\<versionnumber>\<master server>\systemmanager.exe C:\Users\<user>\AppData\Roaming\DVMS\systemmonitor\<versionnumber>\<master server>\systemmonitor.exe
5008	out	-"-
5009	out	-"-
5011	out	-"-
5013	out	C:\Users\<user>\AppData\Roaming\DVMS\systemmanager\<versionnumber>\<master server>\systemmanager.exe
UDP	**inbound/outbound**	
40000 - 50000	in	Thrucast streaming

Spotter Web

TCP	inbound/outbound	
443	in	C:\Windows\System32\inetsrv\w3wp.exe
4222	out	-"-
5008	out	-"-
5009	out	-"-
5011	out	-"-

Gateway

TCP	inbound/outbound	
5008	out	C:\Program Files\DVMS\Gateway\ServiceLauncher.exe

5009	out	-"-
5011	out	-"-
9000	in	-"-

List Management

TCP	inbound/outbound	
5432	in	C:\Program Files\PostgreSQL\XX\bin\postgres.exe
5672	in	C:\Program Files\Erlang OTP\erts-XX.X\bin\erl.exe
8082	out	C:\Program Files\DVMS\AdvLmService\AdvLmService.exe
8089	in	-"-

Smart LPR

TCP	inbound/outbound	
5672	out	C:\Program Files\DVMS\AdvLprService\AdvLprService.exe
8082	out	-"-
8090	In	-"-

Smart FR

TCP	inbound/outbound	
5672	out	C:\Program Files\DVMS\AdvFrService\AdvFrService.exe
8082	out	-"-
8091	In	-"-

Smart ODS

TCP	inbound/outbound	
5432	in	C:\Program Files\PostgreSQL\XX\bin\postgres.exe
5672	in	C:\Program Files\Erlang OTP\erts-XX.X\bin\erl.exe
8082	out	C:\Program Files\DVMS\AdvOdsService\AdvOdsService.exe
8093	In	-"-

Smart OR

TCP	inbound/outbound	
5672	out	C:\Program Files\DVMS\AdvOrService\AdvOrService.exe
8082	out	-"-
8092	In	-"-

Protocols

UDP

UDP (User Datagram Protocol) is a transport-layer protocol used to stream the video feeds from the connected cameras. The protocol is connectionless and lightweight, so it is often used to discover connectivity issues in a network. In the VMS, any connection difficulty is immediately noticed as a loss in the video feed. For streaming to function properly, the network for the system needs to be well constructed, and the connections need to be reliable.

RTSP

RTSP (Real-Time Streaming Protocol) is used to control video streams over a network. RTSP communications between a client and a recording VMS server send instructions on playback and play speed. As with UDP, RTSP is a stateless communication protocol that requires a solid network to function reliably. Usually, the interaction between VMS and the camera goes in the following order:

1. VMS sends a DESCRIBE request to the camera
2. Camera answers with a DESCRIBE response containing information about supported video/audio streams in SDP (Session Description Protocol) format
3. VMS sends a SETUP request to the camera
4. Camera answers with SETUP response needed to create a new RTSP session for a specific stream
5. VMS sends a PLAY request to the camera
6. The camera answers with a PLAY response after this camera starts video/audio sending to VMS – usually, RTP (Real-Time Protocol) over UDP protocol is used for data sending
7. Periodically, the VMS sends a KEEPALIVE request – if no camera stops video stream sending
8. VMS sends TEARDOWN request when the video should be stopped

RTSPS

RTSP (Real-Time Streaming Protocol over TLS) is a secure version of RTSP, similar to how HTTPS is a secure version of HTTP. The protocol uses TLS (Transport Layer Security) to secure communications, requiring a stable connection for TCP traffic.

TCP

TCP (Transfer Control Protocol) is used for signaling between the devices and components of the VMS network and the Internet at large. TCP is an ordered, error-checked, and reliable signaling protocol that can function even if there are some minor faults in the network, at the cost of latency.

HTTP

HTTP (Hypertext Transfer Protocol) is used to communicate control signals for IP cameras in the system. Many drivers use HTTP/HTTPS for setting and retrieving parameters to/from the cameras. In a direct connection, a user contacts the camera GUI (Graphical User Interface) with HTTP/HTTPS. Some drivers may also use HTTP to receive motion detection data and video streams. Some camera drivers traffic PTZ signaling through HTTP.

HTTPS

HTTPS (Hypertext Transfer Protocol over TLS) is a secure version of HTTP. The protocol uses TLS to secure communications.

Quality of Service (QoS)

Quality of Service is a set of strategies usually standardized with network device manufacturers. QoS is used to ensure a certain standard of quality in the transmissions configured on a managed device that is serving as a part of a shared network.

When QoS is configured on VLANs, it prioritizes their bandwidth so it is not as readily consumed by other traffic, and the information going through switches does not degrade. While QoS can be used with any application connection or by users, using it with VLANs is easier to manage and configure. QoS is generally not needed on dedicated networks, as there's no need to prioritize the traffic the network is dedicated to transmitting. In larger, shared networks, however, it becomes vital in preventing performance fluctuations.

Network Hardening

Network Infrastructure

Network hardening involves securing the basic communication infrastructure of multiple servers and computer systems operating within a given network.

Two main ways to carry out network hardening are through establishing an intrusion prevention or intrusion detection system, which are usually software-based. These applications automatically monitor and report suspicious activity in a network and help administrators prevent unauthorized access to the network.

Network hardening techniques include properly configuring and securing network firewalls, auditing network rules and network access privileges, disabling certain network protocols and unused or unnecessary network ports, encrypting network traffic, and disabling network services and devices not currently in use or never in use.

In case of a distributed denial of service (DDoS) threat towards the VMS infrastructure, consider implementing protection for exposed parts of the infrastructure.

Hardening Measures for The Network

If left unprotected, cameras and their network connections represent a significant risk of compromise, potentially giving intruders further access to the system. To prevent this, utilize the following guidelines:

1) *Use secure and trusted network connections*.

Mirasys recommends selecting cameras that support HTTPS. Network communications must be secure, regardless of whether the network is closed or not. By default, secure communications should be used when accessing the VMS. For example:

- VPN tunnels or HTTPS by default
- The latest version of the Transport Layer Security with valid certificates that meet industry best practices, such as from Public-Key Infrastructure (X.509) and CA/Browser Forum.

Otherwise, credentials may be compromised, and intruders might use them to access the VMS. Configure the network to allow client computers to establish secure HTTPS sessions or VPN tunnels between the client devices and the VMS servers.

2) *Use firewalls to limit access to servers and computers*

Mirasys recommends that you use secure connections and the following additional steps:

- Use secure device authentication
- Use TLS
- Use device whitelisting to authenticate devices
- Use firewalls to limit network communication between servers and client computers and programs.

Please refer to the list of VMS components and the ports needed by them that was presented earlier in this section. To ensure, for example, that the firewall blocks only unwanted traffic, you need to specify the ports that the Mirasys VMS uses. You should only enable these ports.

3) *Use a firewall between the VMS and the Internet*

The VMS should not connect directly to the Internet. If you expose parts of the VMS to the Internet, Mirasys recommends that you use an appropriately configured firewall between the VMS and the Internet. If possible, expose only the Mirasys Gateway component to the Internet, and locate it in a demilitarized zone (DMZ) with firewalls on both sides.

4) *Connect the camera subnet to the recording server subnet only*

Mirasys recommends that you connect the camera subnet only to the recording server subnet. The cameras and other devices need to communicate only with the recording servers, except for when ThruCast is used by Spotter.

5) *Use secure wireless protocols*

If you use wireless networks, Mirasys recommends that you use a secure wireless protocol to prevent unauthorized access to devices and computers. For example, use standardized configurations. The NIST guidance on wireless local area networks provides specific network management and configuration details. For more information, see SP 800-48 revision 1, Guide to Securing Legacy IEEE 802.11 Wireless Networks (Guide to Securing Legacy IEEE 802.11 Wireless Networks).

6) *Use port-based access control*

Use port-based access control to prevent unauthorized access to the camera network. The port should become blocked if an unauthorized device connects to a switch or router port. Information about how to configure switches and routers is available from the manufacturers.

Please see NIST SP 800-128 (Guide for Security-Focused Configuration Management of Information Systems) for information about configuration management of information systems.

7) *Run the VMS on a dedicated network*

Mirasys recommends that, whenever possible, you separate the network where the VMS is running from networks with other purposes. For example, a shared network such as the printer network should be isolated from the VMS network. In addition, Mirasys VMS deployments should follow a general set of best practices for system interconnections.

8) *Restrict unused services and protocols*

To help avoid unauthorized access or information disclosure, Mirasys recommends that you stop unused services and protocols on devices (for example, Telnet, SSH, FTP, UPnP, and Ipv6. If UPnP is disabled, then the camera discovery will not work for all cameras.) Using strong authentication on any services that access the VMS, network, or devices is also important. For example, use SSH keys instead of usernames and passwords and certificates from a Certificate Authority for HTTPS.

For more information, see the device manufacturer's hardening guides and other guidance.

9) *Use the IEEE 802.1X authentication protocol*

For devices that are attached to the network, it is advisable to use the 802.1X authentication method. This ensures that an attacker cannot infiltrate the network by, e.g., smuggling a hacking device into the building that they then plug into the network to gain full access.

10) *Other recommendations*

- Use a VPN-encrypted network or similar if using Mirasys Spotter from a remote location.

- Mirasys recommends that customers use data encryption between the VMS server and clients.

Port Forwarding

Automatic router configuration

This feature is not enabled by default, but can be enabled during the installation process or later using the instructions in the text below.

When a VMS Server starts up, it tries to discover UPnP devices from the network. The router needs to support UPnP (Universal Plug and Play), which must be enabled on the device. The server has continuous UPnP device discovery when running, so if any network changes are made, the server will automatically detect new routers and do port forwarding to them. Only UPnP devices with external (WAN) addresses are detected. Note that UPnP is disabled by default, so if this feature is needed, the user needs to first enable it in the VMS Server settings in System Manager.

If the user wants to remove port forwarding automatically, they can do this in System Manager. After this, the server will remember that the settings were removed and not port forward to this router. The software does not allow deleting port forwarding mapping if the server is added to the system with an external address. Deleting the port forward mapping would disconnect the system, and no further configuration would be possible.

If forward port settings are changed, and the connection to the server has not returned after a while, it might be necessary to reboot the router. Servers need four ports for server-to-server communication. The first server that does port forwarding will claim ports 5008, 5009, 5010**,** and 5011. The second server will claim ports 5012-5015, the third server ports 5016-5019, and so on, assuming all the ports are available.

The first port is used for SMServer communication (5008, 5012, 5016...). The second port is used for DVRServer process communication (5009, 5013, 5017...). When connecting to a Main Server, the port is typically 5008. When adding new servers to the main server, the port is typically 5009. If there is more than one server on-site, then the ports are 5009 +4, 5009 + 8, and so forth.

Risks related to port forwarding

The basic idea of port forwarding is that access is provided to one or more VMS Servers or Main Servers behind a router that does Network Address Translation (NAT). Typically,

this situation happens when the client is outside the network and needs to access servers inside a company network.

Port forwarding makes the network more vulnerable to intrusions as open ports provide access to the network, which could be exploited by malicious actors. Therefore, it is recommended to carefully consider whether port forwarding is needed. Generally, you should use port-based access control to prevent unauthorized access to the camera network. The port should become blocked if an unauthorized device connects to a switch or router port.

External Networks and Public Internet Connection

The recommended way to use Spotter from external networks or through a public Internet connection is to establish a VPN connection to the company intranet. This way, the Spotter application outside the firewall can use the intranet IP address of the Main Server and the video recording VMS Servers.

It is also possible to use the VMS system without a VPN. In this case, the user should connect to the Main Server with the outside IP address and port combination. If the user is using Spotter from multiple networks, then the DNS name must be used instead of the static IP address on the VMS server side. This can be done in System Manager by entering the DNS name as the new VMS server address.

Virtual Private Network (VPN)

VPN (Virtual Private Network) can be used to establish secure connections between two or more LANs or to have a well-protected point-to-point connection over the Internet. VPN uses encryption and authentication protocols, preventing unknown computers from accessing data delivered between two or more local network sites.

VPN tunnels for LAN-to-LAN connections can be created using hardware-to-hardware connections, usually with routers that can be used as firewalls or dedicated VPN devices. VPN tunnels for point-to-point connections are typically created with the combination of a hardware firewall functioning as a VPN server and software VPN client connections. After the VPN is configured, Mirasys VMS can be installed and used as if it were in a closed network. Do note that the use of a VPN connection might reduce available bandwidth and consume other resources used by the VMS, which may have a negative impact on the performance of the system or its network. A data packet can have an MTU (Maximal Transmission Unit) size of 1500 bytes (12 kilobits) before it’s fragmented by a Layer 3 device for delivery over IP networks.

VPN adds additional information to the packet header, so the packet is fragmented. This fragmentation could lead to packets arriving in the wrong order and not playing the video properly on some end applications. It is recommended to set the cameras in the system to have their TCP and UDP MTUs set to 1300 bytes.

VPN Methods

VPNs can be set up with a certain variety of methods afforded by the ICT networking industry. Routers can be set up to create Layer 3 VPN tunnels between them, connecting large sites to each other. A site can have dedicated hardware for VPNs, or a server can be configured through software settings to manage VPN tunnels. It is recommended to consult an ICT expert or your IT department for in-depth details on how to set up VPNs and what type of solution is best.

Layer 2 Tunneling Protocol

L2TP (Layer 2 Tunneling Protocol) is a tunnelling protocol used to support VPNs. The protocol itself doesn't provide any encryption or data confidentiality but relies on an encryption protocol that it passes within the tunnel to provide privacy. IPSec is often used to secure L2TP packets by providing confidentiality, authentication and integrity. The combination is generally known as L2TP/IPSec.
When a VPN connection has been established in an L2TP/IPSec VPN tunnel, L2TP packets are encapsulated by IPSec, so no data about the private network can be ascertained from the secured packets. Also, it is not necessary to open UDP port 1701 on firewalls between the tunnel endpoints, since the secured packets are not acted upon until after IPSec data has been decrypted and stripped at the endpoints. L2TP allows the creation of a VPDN (Virtual Private Dialup Network) to connect remote clients to their corporate network by using a shared infrastructure, such as the Internet or the ISP WAN. Desktops and laptops using Microsoft Windows Vista and later operating systems can form remote L2TP VPN connections with a private network.

Layer 3 VPNs

VPN tunnelling between Layer 3 devices is used to connect LANs. This is commonly done between routers connected to a WAN such as the Internet. Routers and routing hardware firewalls (e.g. Cisco ASA or SonicWall devices) can maintain IPSec VPNs between each other over the Internet.

VPN Concentrators

VPN concentrators are networking devices specialized in providing secure VPN connections and message delivery between VPN nodes.
Its capabilities are realized by adding data and network security to the communications that it routes. It is meant to create and manage many individual VPN tunnels. A VPN concentrator is typically used for creating site-to-site VPN connections. Their tasks include:

- Establishing and configuring VPN tunnels
- Authentication of users
- Assigning tunnel/IP addresses to users
- Encryption and decryption of data
- Insurance of end-to-end data delivery

VPN Servers

VPN servers come in two general types: hardware servers and software-based servers. Hardware VPNs are purpose-built networking devices that connect to an Internet connection from within a service site and provide improved VPN capabilities when compared to application-based servers. Usually, these devices can support multiple simultaneous connections. Servers are normally managed through web browsers contacting their IP addresses. Software-based VPN servers can be made from stripped-down or bare-bones desktop computers with the appropriate VPN software application or server operating system installed and network connections configured. There are numerous applications available through a myriad of providers that can form a stand-alone VPN server on a desktop/server operating system environment. Some server operating systems come with built-in capabilities to function as VPN servers. The number of supported connections depends on the running server software and the number of ports on the computer's NICs. Note that some VPN server applications may be incompatible with other VPN standards.

Bandwidth Usage

Mirasys VMS system components are optimized for effective bandwidth usage.
The amount of bandwidth used by the system is determined by the system's component structure and functional requirements. In case of network bandwidth problems, the system can automatically prioritize presentation functions and restrict image display rates to avoid network load problems. The total bandwidth consumption by cameras in the network needs to be noted and considered when planning and implementing the

VMS network. As each camera consumes bandwidth on its connection, the cameras in the system have a sum of bandwidth that they consume. Each connection with multiple cameras should be planned with this in mind.

The system administrator can view and edit system settings through the System Manager application. Through the application, the administrator can add and remove recording servers as well as individual devices, such as cameras and microphones, from the system. In addition, the administrator can define and edit functions affecting bandwidth requirements, such as the video quality of specific cameras. For example, the administrator can temporarily lower or raise the quality of video recorded from a camera, and the change will directly affect the network load created in video playback or real-time presentation from the specific camera.

For bandwidth estimation, these questions should normally be addressed:

- How much bandwidth does each camera use?
- How many simultaneous users are connected to the Mirasys VMS?
- How many simultaneous video and audio streams will the users access?
- What is the minimum acceptable video resolution and quality required by users?
- What is the maximum amount of bandwidth required by users?

You can calculate this by multiplying the number of users by the maximum number of streams consumed simultaneously.

An important consideration that often goes overlooked is the concept of scene complexity, where different or changing scenes may require many times more bandwidth, even if viewed through the same camera. Scene complexity denotes activities and details contained within the viewed scene, but this factor is not a straightforward thing to evaluate. Understanding bandwidth is critical because it impacts network load and storage use, both of which incur their own costs.
These can be kept down by influencing the recorded scene's complexity by keeping the factors of it in check.

An important consideration beyond the physical attributes of setting up an image is that the more an image is processed or compressed on one end of video transmission, the more CPU resources are consumed on the other end to "unpack" the video and make it presentable. It is recommended to test and measure different camera models to find an acceptable balance between performance and bandwidth consumption before any wide-scale deployment. All performance properties have their own impacts on bandwidth. A quick way of estimating basic video bandwidth is to calculate a figure based on a single frame file size and the frame rate.

The following factors can impact bandwidth usage:

- Resolution
- Frame rate
- Color
- Compression
- Codec
- Intra – and inter-frames
- Gain control
- Lighting levels
- Field of view
- Aspect ratio
- Camera placement
- Sharpness
- WDR (Wide Dynamic Range)
- Camera Driver Solutions
- Motion detection
- Streaming options

To size a video surveillance network, you will need to know:

- How much bandwidth each camera consumes, depending on the models you have or plan to have
- How many cameras do you plan to use and in how many locations
- The distance (administrative or physical) of the DVRServer to the cameras connected to it, presuming they need an IP network
- What the bandwidth of those network connections is, and what pre-existing load those networks must also support
- What cameras must be viewed live, and where/how many viewing stations are in the system
- How many servers will there be in the network

Video surveillance consumes network bandwidth in two general routes, in some cases at the same time on some networking devices:

- IP camera/encoder to server: Video is generally produced in devices different than what they are recorded on (e.g., a camera generates video; a VMS server running DVRServer records it).
    - The video needs to be transmitted between the end devices. If it goes over an IP network (e.g., IP cameras to a VMS server running DVRServer), bandwidth is required.

- Server to the client: Statistically, a very low percentage of video is watched by humans. Often, a user is viewing the footage on a device that is connected to a different IP network than the server.
    - For example, the server might be in a rack in a server cabinet, but the client is operated on a laptop, mobile phone or an AVM setup.
    - The connections between these devices require bandwidth every step of the way.

Because of these design realities, the overwhelming majority of bandwidth needed in surveillance systems is dictated by (A) camera type and (B) the relative placement of cameras and servers. In terms of the camera type, analogue cameras do not normally consume bandwidth unless the video is being streamed to clients from DVRServer, as each camera has a cable directly connected to said server. However, analogue cameras can be connected to an encoder that converts analogue transmissions into digital signals in their own channels, with each having its own IP address in the network to which the encoder is connected. Signals from the encoder produce network traffic and consume bandwidth. For all camera types, the relative physical placement of the server near the camera significantly impacts bandwidth needs.

A simple scenario, as presented in Figure 6, has three sites with their own camera network connected to a recording VMS server. Each camera has its own bandwidth, and each server receives the camera network's combined bandwidth. The main server receives bandwidth from the three other servers.

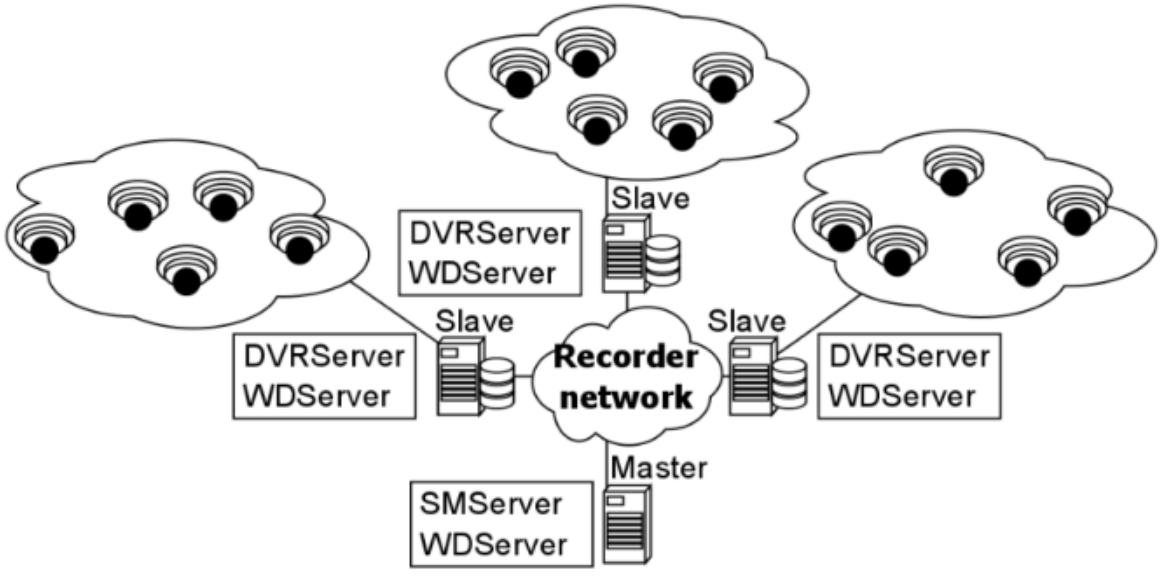

Figure 6

In Figure 7, the number of cameras is the same, but they're connected to only one recording VMS server as a single combined camera network.
The bandwidth received by the sole server is three times greater than what the main server would receive from the three other servers.

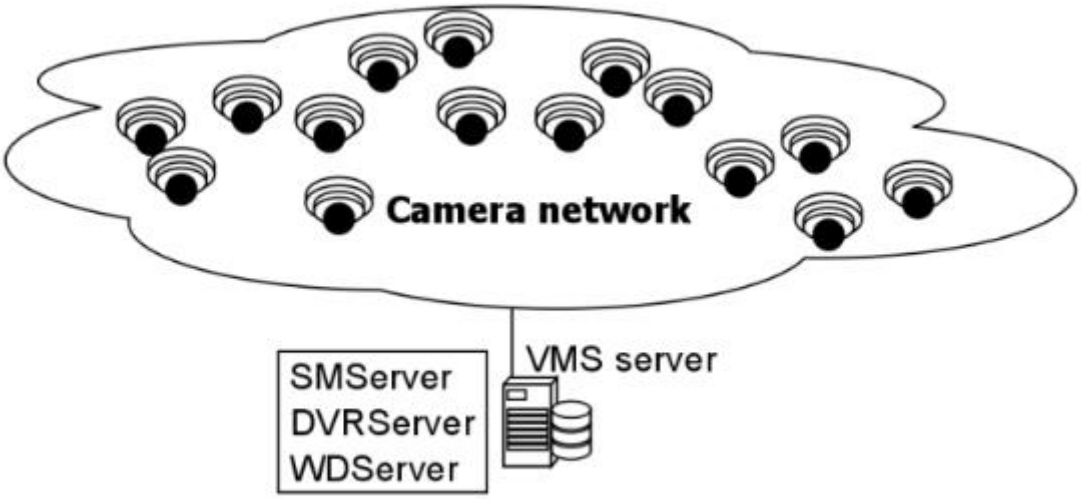

Figure 7

Any networking approach carries with it its own pros and cons, and these must be weighed and balanced before arriving at a solution.

7. Data Integrity & Protection

The Critical Role of Video Data as Evidence

Video data is commonly used as evidence in court, provided that the material is of high quality and trustworthy. Mirasys VMS provides video data that can be exported in high-quality encoding, as well as be verified to be authentic in legal proceedings. In addition, details related to the chain of custody can be reviewed from audit trail logs (see section 10: Audit Trails and Logging of All User Activities). In this section, we discuss how proper encryption, authenticity verification, and privacy protection of surveillance video material and other data are ensured in Mirasys VMS.

Communication Encryption and Certificates

Mirasys VMS supports various encryption methods for securing communication in different parts of the system.

Mirasys sees communication encryption as an essential tool for protecting sensitive information, maintaining privacy, and ensuring the security and integrity of communication.

There are several reasons why one might want to use communication encryption:

1. *Confidentiality*: Communication encryption can ensure that only the intended recipient can read the message, thus preventing unauthorized access and maintaining confidentiality.
2. *Privacy*: Using encryption can protect personal information from being intercepted by hackers, cybercriminals, or unauthorized third parties, protecting your privacy.
3. *Integrity*: Encryption can ensure that the message has not been altered during transit, ensuring message integrity.
4. *Compliance*: Encryption can be required by law or regulations for certain types of communication for example in the healthcare or finance industries.
5. *Reputation*: Using encryption can improve a company's reputation and build trust with customers, partners, and stakeholders who are concerned about privacy and security.
6. *Security*: Encryption can protect against hacking, data breaches, and other cyber-attacks, reducing the risk of data loss or theft.

Communication Between Cameras and The Recorder

Communication between cameras and the recorder service depends on the camera manufacturer. Mirasys VMS supports encryption for the following manufacturers:

Axis

- Uses the root CA public certificate to validate the device's certificate and verify the device.
- TLS 1.2 is used.

Bosch

- Uses the root CA public certificate to validate the device's certificate (signed by the root CA certificate) and verify the device.
- TLS 1.2 is used.

Dahua

- Mirasys uses Dahua's own encryption (implemented inside Dahua SDK) for encrypting the signaling and streaming.

Hikvision / Hanwha (Wisenet) / ONVIF

- HTTPS-encrypted streaming (RTSP over HTTPS tunneling) is supported in the following way: when an RTSP connection over TLS is made, a device shares its public certificate during the handshake procedure, and thus the client does not need to store or have the device's public certificate. The certificate's errors are ignored.
- TLS 1.2 is used

Please refer to the manufacturer's documentation for more detailed information on specific camera models.

Certificate for Spotter Web

A certificate from an approved certificate authority (CA) is required for using the system. An approved certificate can be any RFC8555-compliant CA certificate. A company using the Mirasys VMS can establish its own CA solution for enabling certificates for the VMS infrastructure. There are several free CA solutions to choose from.

One option for obtaining a CA certificate is Let's Encrypt. Let's Encrypt is a free, automated, and open certificate authority (CA), run for the public's benefit. It is a service provided by the Internet Security Research Group (ISRG). You can create a Let's

Encrypt certificate for Spotter Web.
The requirements for a Let's Encrypt certificate are:

- Windows 2016 server or newer
- Domain/subdomain
    - Certificates are domain-bound
- Win-acme tool (available for free on the Win-acme website)

When the certificate has been created, it can be added to Spotter Web in the Internet Information Services Manager.

Streaming between the recorder and clients

Video, audio, text data, and metadata streaming over TCP socket is encrypted using symmetric encryption (Rijndael algorithm is used for encryption (256bit key and 128bit IV values)).

Signaling Between Services and Applications

Genuine Channels (GC) is used for remoting communication and events between services and applications. GC supports various methods for communication encryption, and Mirasys VMS uses ZPA (Zero Proof Authorization). Each VMS system service implements its own ZPA service.

ZPA

The Zero Proof Authorization Security Provider provides authentication, encryption, and content integrity checking services. The client ZPA Key Provider is initialized with a login and a password. The server ZPA Key Provider is initialized with the password provider returning passwords for the requested logins.

- Encryption: 256-bit Rijndael in the CBC chaining mode
- Authorization: Based on a custom password provider
- Integrity Checking: A choice between two algorithms based on MAC-3DESCBC (64 bit) and HMAC-SHA1 (160 bit)

The following algorithm is executed by each Security Session:

1. The client or the server initiates establishing a Security Session.
2. The server generates an arbitrary salt sequence of variable length and sends it to the client. The length of the sequence varies between 128 and 256 bytes.

3. The client receives the sequence and calculates the HMAC-SHA1 (160-bit) keyed hash sum based on the password and the received sequence. The result and the serialized login are sent to the server.
4. The server calculates the same hash sum and compares the calculated value with the received sequence. If both byte sequences are equal, the client is considered to have proved its password knowledge.
5. Both the client and the server generate a 256-bit key and a 128-bit IV vector based on the salt and the password for symmetric encryption (Rijndael encryption) and a 192-bit key for content integrity checking.

As a result, we have a Security Provider which:

1. Does not send open passwords through the network. Only salt and salt-based hash sums are sent. The salt is unique for each established connection and Security Session.
2. Performs 256-bit Rijndael symmetric encryption in CBC or EBC chaining modes depending on the requested encryption functionality. Keys are unique for every connection and Security Session. Note that keys are not sent through the network.
3. Performs content integrity checking based on either the MAC-3DES-CBC (64-bit) keyed hash algorithm or based on the HMAC-SHA1 (160-bit) keyed hash algorithm, depending on the requested functionality. Note that keys are not sent through the network.
4. Provides the client login during every invocation.

Video Encryption

The streaming data between the VMS server and clients can be encrypted by turning on the encryption in System Manager (VMS server's general settings, where it can also be turned off). Data streamed from the VMS server to clients is not encrypted. Encryption is used with the following protocols:

- TCP
- RTP Unicast
- RTP Multicast

Encryption is used with the following stream types:

- Video

- Audio
- Text data
- Metadata

If encryption is used, the VMS server encrypts data before sending it to clients, and clients decrypt the received data.

- All video, audio, etc. data is encrypted
- Some header data is not encrypted
- Commands coming from clients to the VMS server are not encrypted

Encryption can be used only if both the VMS server and client support it, i.e., both must be 8.3.0 or newer versions.

Technical details:

- Encryption is done with AES (used in V9.10.0)
- Rijndael algorithm is used for encryption (256bit key and 128bit IV values) in VMS versions older than 9.10.0
- VMS server generates a password needed for encryption and decryption
- .NET remoting is used for transferring passwords from the VMS server to clients. The password is encrypted too.

Mirasys employs robust encryption techniques to safeguard exported video data. AES encryption with a 256-bit key encrypts image data, layout data, bookmarks, and storyboard data. This selective encryption ensures that critical components of the video and its metadata are secured against unauthorized access or tampering. AES is a widely recognized encryption standard that provides a high level of security, making it suitable for protecting sensitive video data in SEF files.

SHA1 (Secure Hash Algorithm 1) is used for hashing. While SHA1 is not an encryption technique per se, it complements the encryption process by ensuring data integrity and authenticity, allowing the system to detect any alterations to the data.

HTTPS consists of communication over HTTP within a connection encrypted by Transport Layer Security (TLS). Network encryption protects communication between the client, VMS, and the network device. It prevents information from being extracted by network traffic sniffing, and it prevents data from being altered during transfer. The default port 443 for HTTPS traffic is used to securely communicate with a camera's system.

You have the option to password-protect SEF clips during the export process. If password protection is selected, the password will be requested in a separate dialog. When the correct password is entered, the clip is opened.

Decryption occurs dynamically when a password-protected SEF clip is accessed in the Spotter system. For image data, decryption is performed on the fly, meaning it is decrypted in real time as it is accessed without storing decrypted data on the disk. This approach enhances security by ensuring that sensitive decrypted data is not left vulnerable on storage media.

Tamper Detection

Mirasys VCA (Video Content Analytics) has a tamper detection feature that detects if cameras are tampered with. The feature can be enabled in a camera's VCA settings. The following types of tampering are detected:

- Spray painting
- Drastic light change
- Complete or partial obstruction
- Camera defocus
- Camera movement

An alarm can be configured to notify the user if tampering is detected by the system.

Authenticity Verification

Content authentication, as it relates to video authentication, is the examination of digital video evidence to determine potential visual changes to the encoded streams within the digital video file container. An essential feature of the Mirasys system is the use of digital watermarks to verify the authenticity of exported video material. The watermark is a digital signature confirming the video content's originality and integrity.

The Spotter system automatically verifies the authenticity of media files when they are played back using Spotter Player or Spotter. This process checks for the presence of the digital watermark to ascertain if the media file is authentic.

Upon verification, the system informs the user of the authenticity status of the media file through notifications. If the media file is authentic, a notification stating "Media file authenticity verified" is shown.

Videos can be exported in SEF format from Spotter. SEF supports exported videos with subtitles, audio, and text data in an authenticity-protected format. The use of digital watermarks for authenticity verification is particularly associated with the SEF2 format,

which is an extension of the original SEF format with additional security and privacy features. SEF2 supports exported videos with subtitles, audio, and text data in an authenticity-protected format, and enables the following:

- Protecting the video material with a password
- Software side privacy zones in the export
- Face blurring (needs to be enabled on the camera side to be included in the export)
- Mask moving objects

Another essential feature for creating content that can be authenticated is the Storyboard. With Spotter's Storyboard feature, it is possible to create a movie-like video export that makes it easy for the recipient of the clip to view and understand instantly and accurately the chain of events. Storyboard solves the problem of a video's authenticity being compromised when putting together clips in external video editing software, as clips can be compiled inside Spotter with Storyboard. Storyboards can be viewed with the regular Spotter client application or the separate, standalone Spotter Player executable that is exported as the default player for exported video.

Privacy Masking for Sensitive Areas in Live and Recorded Footage

In the context of a surveillance camera, a relevant example of privacy by design is a feature that digitally allows the user to restrict image capture to a specific perimeter, preventing the camera from capturing any imagery outside this perimeter that would otherwise be captured.

Recognizable people are the main issue of video surveillance systems. Personal data is any data related to the identified person in the video. It is illegal to record or photograph people in cases where this would violate their privacy. Thus, the company or people cannot record anyone at places where there is a reasonable expectation of privacy. Such places include e.g. washrooms, homes, toilets, and hotel rooms. Recording people on videos when they are in such locations may cause a violation of privacy, which is protected by Section 10 of the Finnish Constitution (please refer to your country's legislation regarding this issue).

A company or person can record videos of people in a public place since a person has no reasonable expectation of privacy when they are in a public place. However, it is not always obvious which place is public, and which has privacy properties that cannot be violated by video camera filming. A public place is typically defined as a place that is generally open and accessible to people, such as public squares, streets, parks, roads, and beaches. Nevertheless, public places can include pieces of private territories or

objects. Thus, the private territories and objects that could be viewed in public spaces should be defined before choosing the camera angle location and recording the video view. Then, if private objects are defined in the video overview, the camera should be positioned so as not to record private spaces or objects. In case the installation of such a position is impossible, the organization of a video surveillance system should obtain the official consent of the objects' owners. Examples of private spaces are private houses, house entrances and gardens, common neighbor areas, and spaces inside personal cars. Note that you should always refer to and follow your local legislation when it comes to filming in private and public places.

Another way to protect privacy zones on web application streams and recorded videos is to create a special feature inside the application when installing a camera. This feature allows choosing a part of the camera view that must not be recorded or sent to the web application when the video is streaming. These zones can be black squares or have another form; the private zone can also be blurred. Administrators can set up private zones and user permissions regarding these private zones.

The controller also must implement technical or organizational measures which, by default, ensure the least privacy intrusive processing of the personal data in question. GDPR refers to this as privacy by default.

In the Mirasys VMS, it is possible to create privacy zones for a camera to keep a sensitive area within the view of the camera private. Privacy zones can be implemented for the client only or for a camera. It is recommended to use privacy zones to help eliminate surveillance of areas irrelevant to your surveillance target. This can be done by setting a privacy zone in sensitive areas and places where personal identification is not allowed. Create a second role that can authorize the mask to be removed.

There is support for privacy masking for cameras in two forms: a privacy zone on the camera that cannot be removed, and a privacy zone on the camera that (with the right permissions) can be removed to reveal the image behind the mask. For the client only, privacy zones are implemented only on the viewing client. This allows the complete video to be recorded and exported, but the privacy-screened areas are only accessible to users who have the needed user rights.

The content of the privacy functionalities is available (for the user) only if they are defined for the camera (i.e., if the camera does not have e.g. the facial blurring defined, this camera shall not have the faces blurred – even if the user group of the end-user would have permission level set to view only unblurred materials). This also applies when exporting the materials.

It should also be noted that different purposes require different image qualities. When identification is unnecessary, the camera resolution and other modifiable factors should be chosen to ensure no recognizable facial images are captured. In the VMS,

“Blur faces” and “Blur moving objects” settings are available to be set up for additional privacy. Blurring is included in live, recording, and exported material.

System Monitoring

Camera Audit

Camera Health Audit is a plugin that allows the operators to ascertain that every camera of the system works appropriately, and that the cameras have not been turned/tampered/blocked. The main report page provides the following information:

- Name of the camera
- Footage start time
- Footage end time
- Footage Days/Hours
- Current status of the camera
- No signal time period
- Reference image
- Current image
- Audit status
- Comments

When cameras are audited, the following information is displayed:

- Playback view from the camera
- Real-time view from the camera
- Number of frames received from the camera
- Possibility to add a comment to the camera audit report

The camera audit report can be exported in PDF format.

Diagnostics

VMS Server Diagnostics shows information about the server, CPU, and network usage.

The Diagnostics tab shows this information:

- Software version
- Model

- Number of cameras, audio channels, digital inputs, digital outputs, and video outputs
- The name of the computer and the time zone
- Operating system information
- Processor information
- Installed drivers, for example, capture drivers, video output drivers, digital output drivers, and PTZ drivers.

The *Log files* tab shows a list of log files.

To see the contents of a log file:

- Select the file from the drop-down list. The contents are shown in the **Contents of the selected log file**.

On the *Performance* tab, you can monitor the following:

- CPU usage
- Usage of physical memory
- Usage of virtual memory
- Network traffic
- Used disk space

On the *Storage* tab, you can monitor disk and file properties. For example, you can examine free disk space or monitor saved data by the camera and audio channel.

- General
    - **Total recording capacity:** Shows the total storage capacity that is reserved for the recordings.
    - **Used space**: The quantity of space that the recordings have used.
    - **Free space**: Free space is available for recordings.
    - **% used**: The percentage of the disk's capacity that is used.
    - **Average saving speed**: Calculated by dividing the quantity of data saved since the server was last started by the uptime.
    - **VMS Server uptime**: Shows the time that the server has been operating since it was last started.
      The counter shows the difference between the current time and the start time in days, hours, and minutes.
- Disks

    - **Total recording capacity**: Shows the storage capacity that is reserved for the recordings on the selected disk.
    - **Used space**: Used recording space on the selected disk.
    - **Free space**: Free space is available for recordings on the selected disk.
    - **% used**: The percentage of space used of the total capacity reserved for the recordings.
    - **Total recording cache:** Shows the total capacity of the cache that is used for the temporary storage of data before it is permanently written on a disk. Because of the cache, video and audio can be recorded immediately when the server is started. The cache is also used for pre-event recording. The system automatically calculates how much cache space it must have and allocates space accordingly.
    - **Used recording cache**: Temporary space that is currently in use.
    - **Free recording cache**: Temporary space that is currently free.
- Cameras/Video
    - **Oldest time**: The date and time of the oldest image in the store.
    - **Newest time**: The date and time of the newest image in the store.
    - **Total no. of images**: The total number of images in the store.
    - **Average image size**: The average image size.
    - **Used space**: This value shows how much space the images and metadata files from this camera use.
    - **% used**: This value shows what percentage of space this camera has used of the total capacity reserved for the recordings.
- Audio channels
    - **Oldest time:** The date and time of the oldest audio sample in store.
    - **Newest time**: The date and time of the newest sample in store.
    - **A total number of samples**: The total number of audio samples in store.
    - **Average sample size**: The average audio sample size.
    - **Used space**: This value shows how much space the audio samples and metadata files from the audio channel use.
    - **% used**: This value shows what percentage of space the audio channel has used of the total capacity reserved for the recordings.
- Text channels
    - **Oldest time:** The date and time of the oldest text data sample in store.
    - **Newest time**: The date and time of the newest sample in store.
    - **A total number of samples**: The total number of text data samples in store.
    - **Average sample size**: The average text data sample size.
    - **Used space**: This value shows how much space the text data samples and metadata files from the text channel use.

- **% used**: This value shows what percentage of space the text channel has used of the total capacity reserved for the recordings.

SMServer Diagnostics

SM Server Diagnostics shows information about the System Management Server that runs on the Master Server. In SMServer Diagnostics, you can examine this information:

- SM Server version
- Computer name and time zone
- Operating system information
- Major version
- Minor version
- Build
- Platform ID
- CSD version
- Service pack major version
- Service pack minor version
- Suite mask
- Product type
- Framework version

If there is a problem with the system, you can access the system log files on the *Log Files* tab.

Watchdog

The system has a software watchdog (system monitoring service) that monitors the system and performs specific actions if problems occur.

In the Watchdog tool, you can select the events for which the notification list is notified through e-mail and access Watchdog logs, which contain the events that have occurred and the actions that have taken place. All event types are written to the Watchdog logs, regardless of the e-mail settings.

More information about specific Watchdog events can be found on the public Mirasys documentation portal.

Audit Trails and Logging of All User Activities

The Audit trail log can be used to search for VMS user activity information. It can be accessed in System Manager at the System tab tree under Monitoring. In the audit trail log dialog admin can search for audit trail events using several search parameters. Results are listed in the result list ordered by time. Found audit trail events can be sorted by other audit trail event information by clicking the list headers.

The found audit trail events are listed in the search result list. The list contains information about each audit trail event.

- **Time** - Time of the user action.
- **User** - Username who did the user action.
- **Application** - Application where the user action was taken.
- **Event** - Name of the user action. When the event is related to camera audit, and the operator needs to add a comment before accessing playback material, the event contains the comment.
- **Event status** - Whether the operation was successful or not.
- **Object** - The object depends on the operation itself. For example, if you open a camera, the name of that camera is shown.
- **VMS Server** - Displays on which VMS server the operation occurred.

Listed audit trail events can be exported to a PDF file as an audit trail. The location and the name of the exported file and the comments for the report can be given on the save report dialog. The audit trail log report title includes the export time and the user who exported the report. The report contains all the audit log entries with the same information that is listed in the audit trail event result list.

Retention time for audit trail logs can be modified in the Database.xml file. The user can insert the desired number of days for retention. Maximum day limits are checked periodically: the first check is done 1 minute after SMServer is started, and from then on, every 30 minutes. If the maximum days limit is exceeded, then rows older than the maximum days are deleted. However, not more than 10 000 rows are deleted at a time.

8. AI & Analytics

This section covers the AI features available for the Mirasys VMS. Note that all AI features are disabled by default, as the use of AI plugins requires separate installation and licenses that must be activated for each service.

Mirasys Object Recognition

Object Recognition Search allows operators to search recordings for attributes for both persons and vehicles. The Object Recognition search conducts searches with the following criteria: where (which cameras), when (time frame), and what (humans or vehicles and their attributes).

For persons, searchable attributes are upper body clothing color, lower body clothing color, if the person is carrying a bag, and if the person is wearing headwear. Vehicles can be searched by type and by color.

Mirasys List Management

List Management (LM) is used to process Face Recognition (FR) and License Plate Recognition (LPR) events by matching detected faces and license plates to an identity and identity list. LM service is used to store identities and identity list information, receive and save LPR and FR events, send LPR and FR events to clients, do searches in saved events, and send LPR and FR events to the VMS server for processing.

LM service has the following abilities:

- Store identities and identity lists in the database
- Receive and store LPR and FR events in the database
- Match detected license plates and faces to defined identities and identity lists
- Search LPR and FR events from the database using search parameters
- Send real-time LPR and FR events for clients and recorders
- Send LPR and FR events to the VMS server for processing
- Notify clients and recorders about changes in identities and identity lists
- Enable integration to License Plate and Face recognition

Mirasys Face Recognition

Face Recognition (FR) is used to identify a human face. It is used in the VMS to get events when faces are detected from selected video streams and to detect when specific people are seen in the video. Together with the Mirasys List Management, this allows you to, for example, create an automatic detection system for a person's access to the premises.

The FR service receives video streams, processes images, detects faces, and sends notifications with detection data to the LM service for identity and list matching.

If any client privacy masks are defined for the camera, the FR service draws privacy masks to input images before inference. No face can be detected inside the privacy zone, and thumbnail images have privacy zones.

Mirasys License Plate Recognition

License Plate Recognition (LPR) is used to identify a car using its license plate. It is used in the VMS to get events when license plates are detected from selected video streams and to detect when specific cars are seen in the video. Together with Mirasys List Management, this allows you to, for example, create an automatic detection system for cars' access to the parking hall.

The LPR service receives video streams, processes images, detects license plates, and sends notifications with detection data to the List Management (LM) service for identity and list matching.

If any client privacy masks are defined for the camera, then the LPR service draws privacy masks to input images before doing inference. No license plate can be detected inside the privacy zone, and privacy zones are included in thumbnail images.

LPR includes country detection as an optional feature, but in some countries, it is recommended to be used; plate number detection accuracy can be improved when the country is known. Plate number detection is available for Eurasia and the Americas. If country detection is enabled, then license plate type can sometimes be detected. License plate type can be undefined or one of these:

- antique
- diplomatic
- export
- military
- provisional

- rental
- taxi
- test
- work

Mirasys VCA

Mirasys Video Content Analytics (VCA) comprises a set of real-time video analytics solutions that utilize advanced image processing algorithms to turn video into actionable intelligence. The product's core is an advanced object recognition and tracking engine that continually tracks moving and stationary targets. The tracking engine features built-in robustness to environmental nuisance conditions such as changing illumination, moving foliage, rippling water, and more.

Mirasys VCA is a generic name for a suite of video analytics add-on product options that include functionality such as:

- Ability to detect aggressive behavior.
- Ability to detect falls.
- Ability to detect directional crossing.
- Ability to detect repeated behavior.
- Ability to detect persons with their hands up.
- Deep learning object tracker classes are person, bus, motorcycle, bicycle, car, van, truck, forklift, and bag for triggering alarms
- Support for different event state possibilities: start (default), on, stop. Note that the states on and stop are only available if defined in the VCA Core config files.

Other features include:

- *Motion object tracking*: Motion-data-based object highlighting and tracking, auto-zoom functionality. The motion data is produced by server-based, hermeneutic motion detection.
- *Tripwire counting*: In addition to motion object tracking functionality, line counting for overhead installed cameras and Spotter client-based counter visualization.
- *Object behavior/attributes detection*: To continuously track and classify moving and stationary targets and features, a full suite of rule-based filters including enter, exit, appear, disappear, stopped objects, directionality constraints, object

counting, loitering, object type, and object speed. Multiple filters and rules are supported on any combination of multiple overlapping detection zones, in addition to an advanced people-tracking engine optimized for tracking people in cluttered indoor scenes such as retail scenarios. Includes specific high-accuracy counting functions optimized for use in busy scenes.

The following are available as separate applications, products, or through project-based integrations:

- Camera-based (built-in, edge) analytics support selected camera manufacturers and their functionality through manufacturer-specific integration connectors.
- Audio analytics technologies refer to software for extracting information and meaning from audio signals, such as detecting sounds of breaking glass, etc.
- Facial recognition technologies refer to software or camera features for automatically identifying or verifying the identity, age, gender, etc., of a person from video footage.
- Number plate recognition technologies (ANPR/LPR) refer to software or camera features for automatically identifying vehicle or container numbers.

9. System Resilience & High Availability

Resiliency and availability are central issues in a robust VMS. This section focuses on how the Mirasys VMS handles resiliency and availability issues when it comes to recording surveillance material.

Disaster recovery and Scalability considerations

Disaster recovery refers to the process of maintaining or re-establishing vital infrastructure and systems following a disaster. In disaster recovery, the basic assumption is that the primary site is not immediately recoverable and data and services are restored to a secondary site.

Organizations should create an action plan for disaster situations and set desired limits for eg. Recovery Time Objective and Recovery Point Objective. Recovery Time Objective (RTO) is the targeted duration of time and a service level within which a business process must be restored after a disruption to avoid a break in business continuity. Recovery Point Objective (RPO) is the maximum acceptable interval during which transactional data is lost from an IT service.

A video management system is a critical part of organizational infrastructure, and therefore organizations should aim for high availability when it comes to disaster recovery. This can be done by employing the recovery features included in the VMS (such as failover and edge storage) and having a clear internal plan for disaster situations. It should be noted that the larger and more extensive the system is, the more extensive the measures for disaster recovery should be.

Failover Strategies for Recording Servers

Mirasys VMS supports failover video servers as a Mirasys VMS option. Failover servers are VMS servers on a passive standby until the system recognizes that one of the active video recording VMS servers has broken down; at this point, a failover server takes the place of the broken server. The failed server can be repaired and replaced as a new failover server, while the failover server that took its place can continue operating as an active server. Failover events are available in failover logs if the user role for the function has been enabled.

Recording and failover servers should be of a similar hardware setup and share drive letter assignments and version numbers. Analog cameras connected to encoders will not be transferred to the failover server. Only previously assigned IP cameras are reassigned during the switch.

When adding a new server to the system, the administrator can select whether the added server is a standard server or a failover server. There can be any number of failover servers (0-n). If the server is the standard server, the administrator can choose if that server will be added to the failover monitoring, i.e., in case of server failure (hardware or software), this server will migrate to the available failover server. It is important to note that the main server needs to be installed on hardware separate from those operating with recording licenses or failover licenses. The minimum hardware setup consists of three servers: one main server, one video recording VMS server, and one standby failover server.

Failover migration will be triggered in the following conditions:

- The main server has lost the connection to a VMS server, and the timeout set by the administrator has been reached
- A VMS Server has informed the main server that the connection to all the material disks (recording storage) on the server has failed
    - Manual data recovery from server hard drives can be attempted if the disks are still functional
- A server's Watchdog service has informed the main server that it cannot initialize the recording service

A recording continues after the failover server has taken over to keep the system operational. The only exception is the timeout between disconnect and the failover trigger. The administrator configures this. After a failover server has assumed the recording role of a failed server, a system backup will automatically be created to set a new baseline.

During the failover restore process and the following system backup:

- Users cannot perform manual backup operations
- Any following broken servers are added to a failover queue

The failover queue is handled after the failover restore has been completed.

When failover is started (triggered manually by the user, by network connection loss, or by critical recorder failure), SMServer will do the following operation:

1. Check if there is a failover server available that belongs to the same failover group as the failed recorder, and there is a connection to the failover server
2. Creates a failover log entry about the failover
3. Get settings, masks, and schedules of the failed recorder from the recorder settings cache

4. Saves failed recorder settings to the failover server
5. Makes changes to system data that the failover server has taken the tasks of the failed server
6. Makes changes to the system data that the failover server is now acting as a normal recorder, and the failed recorder is in a broken state
7. Sets the failover progress result to the failover log
8. Sends system change notification to clients

The user can trigger manual failover in the System Manager in recorder settings. Manual failover is possible if

- There is a connection to a failover server that belongs to the same failover group as the selected recorder
- Selected recorder has failover enabled
- User has a role that allows triggering failover manually

Failback

Failback can be done either automatically or manually, and there is no need to use settings backup to revert the failover. The failback uses the same functionality as failover, but in reverse order by moving server functionality from the failover server back to the failed server. Manual failback can be triggered from the failover log. Automatic failback will trigger failback when automatic failback is enabled, and the connection to the failed server is restored successfully.

When failback is triggered (manually or automatically):

1. Check that there is a valid failover log entry and the failover state in the log is correct
2. Check that the failover server is still acting as a normal recorder
3. Check that the failed server is still in a broken state
4. Check that failover is enabled in the license
5. Check that there is no ongoing failback process running for the failed recorder
6. Update the failover log that failback is started

7. Get failover server recorder settings, configuration files, masks, and schedules from the recorder settings cache
8. Set failed recorder settings
9. Mark the failover server to act as a failover server again, and mark the failed recorder to be in ok state
10. Update the failover log that failback has been performed
11. Send system change notification to clients

Edge Storage

The Edge storage functionality enables uninterrupted recording during network blackouts. In practice, in a network blackout, the video feed can be stored on an SD memory card in the camera. Once the network connection has been re-established, video is transmitted from the camera's SD card to the server. Please refer to the camera manufacturer's documentation to see which cameras support the feature. Edge storage must be enabled in the device settings. This feature is configured solely through the camera's configuration utility. Please refer to the camera's documentation for instructions on enabling Edge storage.

When Edge storage fetching for offline periods is enabled, the Mirasys VMS transfers recordings from the camera SD card only from the time of the period, when the connection has been lost between the Mirasys VMS and the IP camera.

Settings Backup and Restoration

The user can back up system settings to be able to restore them if the hard disk that contains the settings fails:

- You can back up system settings and server settings.
- System settings contain data about the servers, profiles, and user accounts.
- VMS Server settings contain data about the devices connected to the servers and their parameters.
- You can save the backup copy to a hard disk, network drive, CD/DVD, floppy disk, or another removable or non-removable device.
- Backup files have the file extension ".vbk".

If you have created a backup file of the system and server settings, you can restore the settings if a problem occurs**.** Doing automatic settings backup after successful settings

restore is recommended, especially when restoring the system after failover has occurred. This option can be enabled when doing a settings restore.

The automatic backup to HDD feature makes an automatic backup to the local HDD every night at 2 AM if there have been any changes on the system side. The default location for this is: C:\ProgramFiles\DVMS\SystemManagement\SMData\RecoveryStore\Backups.

Automatic backup can also be done to USB, but using this feature requires a separate license.

It is recommended to take care of the backup files with the following measures:

- Encryption: Files should be encrypted after backup by e.g. using ZIP password protection. Tools like VeraCrypt can also be used for encryption, as they make the file contents unreadable without the key.
- Offsite storage: It is recommended to store a copy of the backup in a separate physical location. This helps protect the data against e.g. fire or theft.
- Offline/disconnected backups: Disconnect external drives when not in use to avoid, e.g. ransomware encrypting your backup.
- Using secure cloud services: For storing the backup, you should use a trusted cloud service (e.g. Google Drive, OneDrive, Backblaze) with 2-Step verification enabled.
- Immutable backups: Consider cloud storage options that offer immutable storage, which prevents files from being modified or deleted for a set period, protecting against ransomware

Redundant Storage Configurations (RAID)

RAID stands for “Redundant Array of Independent Disks" or "Redundant Array of Inexpensive Disks". RAID is an orchestrated approach to data storage in which data is written to more than one secondary storage device. Instead of storing all data in a single hard disk drive, RAID coordinates two or more such devices into a disk array. When the computer writes data to secondary storage, the RAID system distributes the data across the array. There are several possible ways of doing this, and these various configurations are called RAID levels.

While most RAID levels can provide good protection against and recovery from hardware defects or defective sectors/read errors (*hard errors*), they do not provide any protection against data loss due to catastrophic failures (fire, water) or *soft errors* such as user error, software malfunction, or malware infection. For valuable data, RAID is

only one building block of a larger data loss prevention and recovery scheme – it cannot replace a backup plan.

A RAID storage unit can be connected to a VMS server.

10. Compliance & Standards

ONVIF Compliance for Multi-vendor Interoperability

Currently supported Onvif profiles are the following:

- Profile G: Profile G is designed for IP-based video systems. A Profile G device (e.g., an IP network camera or video encoder) can record video data over an IP network or on the device itself. A Profile G client (e.g., a video management software) can configure, request, and control recording of video data over an IP network from a Profile G conformant device. Profile G also includes support for receiving audio and metadata stream if the client supports those features.
- Profile M: Mirasys software supports ONVIF Profile M, enabling it to respond to alerts triggered by camera analytics. Thus, the VMS system can effectively respond to camera alerts, which opens new opportunities to enhance site security or utilize video analytics for other purposes. To ensure seamless integration and compliance, this feature has been tested with Axis, Bosch, and Hanwha camera brands.
- Profile S: Profile S is designed for IP-based video systems. A Profile S device (e.g., an IP network camera or video encoder) can send video data over an IP network to a Profile S client. A Profile S client (e.g., a video management software) can configure, request, and control video streaming over an IP network from a Profile S device. Profile S also covers ONVIF specifications for PTZ control, audio in, multicasting, and relay outputs for conformant devices and clients that support such features.
- Profile T: Profile T is designed for IP-based video systems. Profile T supports video streaming features such as the use of H.264 and H.265 encoding formats, imaging settings, and alarm events such as motion and tampering detection. Mandatory features for devices also include onscreen display and metadata streaming, while mandatory features for clients also include PTZ control. Profile T also covers ONVIF specifications for HTTPS streaming, PTZ configuration, motion region configuration, digital inputs and relay outputs, and bidirectional audio for conformant devices and clients that support such features.

Adherence to Regulations and Standards

GDPR

Mirasys VMS products are designed to deliver secure end-to-end communication, as well as to protect privacy and secure data. Data protection is always an important issue,

including when it comes to being General Data Protection Regulation (GDPR) compliant in the EU.

According to GDPR, when processing such data, the controller of personal data must implement technical or organizational measures designed to implement the data protection principles set out in GDPR. GDPR refers to this as privacy by design. In the context of a surveillance camera, a relevant example of privacy by design would be a feature that digitally allows the user to restrict image capture to a certain perimeter, preventing the camera from capturing any imagery outside this perimeter that would otherwise be captured. For more information about privacy masking in the Mirasys VMS, see section 7: Privacy Masking for Sensitive Areas in Live and Recorded Footage.

According to Article 4(1)(e) of the GDPR, recordings must not be retained longer than necessary for the specific purposes for which they were made. Mirasys recommends that you set the retention time according to regional laws and requirements, and in any case, set the retention time to a maximum of 30 days. In System Manager's storage settings, you can set the storage time of the recorded video, audio, text data, and alarm data. Alarm and normal recordings can use different storage limits. Video, audio, text data, and alarm recordings are kept until their defined maximum date has been exceeded or until the allocated storage space has run out.

GDPR also imposes restrictions on transferring personal data outside of the EEA (European Economic Area) countries. Mirasys does not transfer any personal data abroad, as the VMS does not use public cloud services. All data is stored on the servers of the owner/administrator of the system, meaning that the data never leaves the possession of the owner/administrator unless they share the data themselves.

Automatic Deletion of Video, Audio, and Text Data

After exceeding the defined maximum storage time, stored video, audio, text, and alarm data are automatically deleted -- the maximum storage time for data is checked daily.

As the size of a stored data stream can vary significantly due to movement in the video image, changes in audio levels, or the number of text data events, it may be hard to predict storage space requirements accurately. Thus, sometimes the system may deem it necessary to ensure free storage space by automatically deleting old material regardless of the maximum storage time.

If data needs to be deleted to ensure free storage space, the deletion process proceeds through the following pattern:

1. Check alarm quota, if alarm material files count in more than set in quota (% from all data), cleanup the oldest alarm file and reuse it

2. Check min settings for alarm data - if alarm channels have data that exceeds min alarm settings – we take the oldest file from those, clean it up, and reuse
3. Check min settings for all material channels (video, audio, data) - if some channels have data that exceeds min settings, take the oldest file from those, clean it up, and reuse
4. Check the oldest file from channels with auto min settings if they are present; if so, take the oldest file from those, clean it up, and reuse
5. If still nothing is found, take the oldest file from all channels (material and alarm), clean it up, and reuse

In addition, there is a background task that cleans up material files according to max settings.

Data Subject Rights

According to the General Data Protection Regulation (GDPR), data subjects have the right to have access to their data. Video material of a specific subject can be located by selecting a camera or cameras in the VMS and entering the specified date/time to go to the needed time. Playback controls are also available for viewing the playback. Footage can be exported in a secure format (see section 7: Video Encryption).

NDAA

The Mirasys VMS software is NDAA (National Defense Authorization Act)-compliant and can be deployed in an entirely NDAA-compliant configuration.

Manufacturers who sell NDAA-compliant cameras and whose cameras are compatible with the Mirasys VMS include:

- Axis
- Bosch
- Hanwha
- Mobotix
- Panasonic / iPro
- Pelco
- Vivotek

Note that in some cases, NDAA compliance applies only to certain camera models produced by a manufacturer. This means that while the manufacturer offers NDAA-

compliant cameras, not all their cameras necessarily fulfill compliance criteria. You can check NDAA-compliance for a specific camera model from the manufacturer.

NIS2

NIS2 is an EU Security Directive applied to each EU member country via the national legislation. This means that the legislation in each EU country can vary, but the content of the legislation should generally be the same.

NIS2 aims to strengthen the common EU and national cybersecurity level for sectors and actors considered critical for the functioning of society. The NIS2 Directive affects the business management, technology, and partner selection, and operational control of organizations in all EU Member States.

The requirements of the law apply to the organisation's production processes and the relevant communication networks and information systems: ensuring the confidentiality, integrity, and availability of information at an acceptable level of risk.

The requirements in NIS2 are related to the following areas:

- Roles & processes
- Risk management & leadership
- Asset, change, and configuration management
- Identity & access management
- Threat & situation picture
- Event & incident management
- Supply chain & external dependency management
- Staff management
- Cybersecurity architecture

NIST

Mirasys adheres to the guidelines presented in various NIST publications. NIST CSF provides organizations with best practices for cybersecurity that can help them identify, assess, and prioritize their cyber risks. The framework also helps to improve communication between different organizational departments by providing an integrated approach to cybersecurity planning across all areas of an organization.

OWASP

The OWASP Top 10 is a standard awareness document for developers and web application security. It represents a broad consensus about the most critical security risks to web applications.

Each organization must assess security controls periodically. This assessment determines whether the controls are effective in the application. Corrections in the implementation should be made if they are found to be lacking.

Mirasys VMS has certification from Prime Infoserv LLP. Prime Infoserv LLP is a solution and service-centric organization in Kolkata, West Bengal, with a range of technology and cybersecurity solutions. This certification proves that the Mirasys VMS is free from vulnerabilities as per the OWASP Top 10 benchmark and is safe for hosting.

Threat Modeling

Threat modeling is a family of activities for improving security by identifying threats and then defining countermeasures to prevent or mitigate the effects of threats to the system. A threat is a potential or actual undesirable event that may be malicious (such as DoS attack) or incidental (failure of a Storage Device). Threat modeling is a planned activity for identifying and assessing application threats and vulnerabilities.

Mirasys implements threat modelling in its Software Development Lifecycle (SDLC). Threat modelling is integrated in three different stages of the SDLC: development, testing, and deployment.

11. Maintenance & Lifecycle Management

Updating The Firmware

NIST SP 800-193 provides the following information on firmware update mechanisms:

One or more authenticated update mechanisms anchored in the RTU (Root of Trust for Update) shall be the exclusive means for updating device firmware, absent unambiguous physical presence through a secure local update -- Authenticated update mechanisms shall meet the following authentication guidelines:

1) Firmware update images shall be signed using an approved digital signature algorithm -- with security strength of at least 112 bits in compliance with SP 800-57, Recommendation for Key Management – Part 1: General [8].

2) Each firmware update image shall be signed by an authorized entity – usually the device manufacturer, the platform manufacturer or a trusted third party - in conformance with SP 800-89, Recommendation for Obtaining Assurances for Digital Signature Applications [9].

3) The digital signature of a new or recovery firmware update image shall be verified by an RTU or a CTU (Chain of Trust for Update) prior to the non-volatile storage completion of the update process. For example, this might be accomplished by verifying the contents of the update in RAM and then performing an update to the active flash. In another example, it could also be accomplished by loading the update into a region of flash, verifying it, and then selecting that region of flash as the active region.

Decommissioning Procedures for Old Hardware

NIST SP 800-88r1 describes three main methods for data sanitization, depending on the sensitivity of the data and the type of equipment:

- *Clear: This method applies logical techniques to sanitize data in all user addressable storage locations of an ISM (Information Storage Media) for protection against simple, non-invasive data recovery techniques using the same interface that is available to the user (e.g., host interface). Clear sanitization techniques are typically applied through the standard read and write commands to the ISM, such as by rewriting with a new value or using a menu option to reset the ISM to the factory state if rewriting is not supported. Clear sanitization techniques typically have no impact on the usability of the ISM.*

- *Purge: Using advanced techniques, such as degaussing (magnetic field) or special built-in security features in the device, to make the data inaccessible. This method is useful for higher-security needs.*
- *Destroy: Physically damaging the device so it can no longer be used. This is typically reserved for devices that stored highly sensitive information and are no longer needed.*

Mirasys provides a standard 5-year manufacturer's warranty for all machines bought from Mirasys. For any support required, you can contact Mirasys hardware provider.

Vulnerability Monitoring and Security Advisories

API Security testing

Security testing against the APIs is performed with automated tests for the Mirasys VMS. The testing tool simulates more than a thousand hacking and penetration scenarios to test whether HTTP requests are safe from cyber attacks. The following tests are performed:

- *Boundary Scan:* The Boundary scan checks if the service handles unexpected input values correctly. The goal is to check if the service is sensitive to values that fall outside of the normal range, and if its vulnerabilities are therefore exposed.
- *HTTP Method Fuzzing Scan:* The HTTP Method Fuzzing scan finds weaknesses in the service by generating semi-random input through HTTP methods. The scan reveals if the service responds to undocumented methods, indicating instabilities or vulnerability to iterative HTTP method requests.
- *Sensitive Files Exposure Scan:* The Sensitive Files Exposure scan verifies that any files that cause security problems are not accessible through the service. The scan shows if the service leaves sensitive files unprotected.
- *Weak Authentication:* The Weak Authentication scan checks the authorization method against several standard rules for authorization security. The scan specifies if the service uses inefficient authorization schemes and is vulnerable to impersonation and other authentication-based security breaches.
- *Invalid Types Scan:* The Invalid Types scan checks how the service behaves when you are getting values of unexpected types. The scan will alert whether the service is vulnerable to unexpected value types and exposes sensitive information.

- *Cross-Site Scripting Scan:* The Cross-Site Scripting (XSS) scan checks how the service handles potentially harmful injections into web pages. It shows if the service is vulnerable to scripts sent from the browser side.
- *Fuzzing Scan:* The Fuzzing scan checks how the service behaves when getting random input. The output of the scan demonstrates if there are instabilities in the service, or if iterative requests cause security problems or reveal sensitive data.
- *SQL Injection Scan:* The SQL Injection scan checks how the service handles incorrect or malicious SQL statements. The goal is to check if the service is vulnerable to SQL attacks or cannot handle the authorization routines correctly.
- *XPath Injection Scan:* The XPath Injection scan checks how your service handles incorrect or malicious XPath queries. The scan will indicate if the service is vulnerable to XPath attacks or cannot handle authorization routines correctly.
- *Groovy:* The Custom Script scan uses the Groovy script to check for vulnerabilities in the service.
- *Malformed XML:* The Malformed XML scan checks how the service behaves when it gets malformed XML snippets. The scan is performed to determine if the server can handle malformed XML snippets correctly.
- *Malicious Attachment Scan:* The Malicious Attachment scan generates corrupted files to check how the service behaves when receiving malicious files.
- *XML Bomb Scan:* The XML Bomb scan checks if the service has efficient protection against an XML bomb.

According to NIST SP 800-218, organizations should identify residual vulnerabilities in their software releases and respond appropriately to address them and prevent similar ones from occurring. The following actions are recommended:

- *Identify and Confirm Vulnerabilities on an Ongoing Basis*
    - *Help ensure that vulnerabilities are identified more quickly so that they can be remediated more quickly in accordance with risk, reducing the window of opportunity for attackers.*
- *Assess, Prioritize, and Remediate Vulnerabilities*
    - *Help ensure that vulnerabilities are remediated in accordance with risk to reduce the window of opportunity for attackers.*
- *Analyze Vulnerabilities to Identify Their Root Causes*
    - *Help reduce the frequency of vulnerabilities in the future.*

Vulnerability Disclosure and Patching Policy

Whenever Mirasys delivers VMS updates for its customers, the updates utilize the newest components and provide better functionality. The safety precautions described in this document enhance the security to a high degree so that separate security patch deliveries are not used. The reason for this is that the VMS generally utilizes services that are specific to the VMS itself, making the attack surface of the system notably small.

Camera manufacturers and operating systems typically provide security updates, and it is important to install these updates for the devices that are linked to the VMS. Mirasys also posts release notes for new updates on the public documentation portal, which provide information on, e.g., what new fixes and features the update contains.

12. Conclusion

Summary of Cybersecurity Best Practices

Securing a VMS is an extensive process with a high number of factors to consider, and this whitepaper presents multiple specific and general security measures for the VMS. On a general level, the central steps for hardening a VMS can be summarized as follows:

1. Understand the components to protect
2. Harden the surveillance system components
3. Document and maintain security settings on each system
4. Train and invest in people and skills, including your supply chain

Hardening is a continuous process of identifying and understanding security risks and taking appropriate steps to counter them. The process is dynamic because threats and the systems they target are continuously evolving. Hardening establishes actions that mitigate threats for each phase in the threat lifecycle. Hardening can and should be done for the following components:

- Network
- Software applications and OS
- Physical components (eg. cameras, network cables, servers)

In addition to hardening the system itself, an important part of security is to be aware of and follow legislation and regulations that affect the system (eg. GDPR). The system provider and the user both have the responsibility of avoiding violations.

This document provides information on the most important security topics for the VMS. It is recommended to refer to security standards by e.g. NIST and CIS to get more information on both general system security and more specific topics (CIS, for example, has benchmarks on different operating systems and network devices, among other topics, available for free online). When questions regarding specifically e.g., hardware and firmware arise, the best option is to check the manufacturer's documentation and/or be in contact with their support department. With questions regarding the VMS specifically, customers can contact Mirasys.

Future trends in VMS security

It should be noted that VMS security and the technology related to it are developing and improving all the time, and new solutions can be integrated into VMS products for an enhanced user experience. One of the current trends in this field is the use of AI analytics, which have already been incorporated into the Mirasys VMS to a great extent.

However, the evolution of AI technology will provide even more opportunities to improve VMS products with AI features later on. Another upcoming VMS security trend is the Zero Trust Architecture (ZTA), which is a cybersecurity architecture based on zero trust principles and designed to prevent data breaches and limit lateral movement from cyber attackers. As technologies continue to develop, security practices and recommendations must develop with them and be updated on a regular basis.

Sources

Attacks and Preventative Measures on Video Surveillance Systems: A Review
https://www.mdpi.com/2076-3417/11/12/5571

AXIS Camera Station 5 – System hardening guide - AXIS

https://help.axis.com/en-us/axis-camera-station-system-hardening-guide - axis-camera-station-software-update-policy

Best Practices for Digital Video Authentication - SWGDE

https://www.swgde.org/documents/published-complete-listing/23-v-001-best-practices-for-digital-video-authentication/

Bosch NDAA Compliant - A1 Security Cameras

https://www.a1securitycameras.com/bosch/ndaa-compliant/

CCTV Hacking: Understanding Vulnerabilities and Strengthening Surveillance Security

https://mikuz.hashnode.dev/cctv-hacking-understanding-vulnerabilities-and-strengthening-surveillance-security

CIS Microsoft Antivirus Benchmark v1.0.0 – 02-20-2026

CIS Microsoft Windows 10 Enterprise (Release 1803) Benchmark v1.3.0 – 10-30-2017

Compliance | i-PRO Products

https://i-pro.com/products_and_solutions/en/surveillance/compliance

Government Security Cameras and Solutions - NDAA Compliant - Hanwha Vision

https://hanwhavisionamerica.com/markets/government/

A guide to secure file storage and transfers for UK businesses – InitialIT

https://initialit.co.uk/post/a-guide-to-secure-file-storage-and-transfers/

High availability - Wikipedia

https://en.wikipedia.org/wiki/High_availability

How to back up your files and devices – Australian Signals Directorate

https://www.cyber.gov.au/protect-yourself/securing-your-devices/how-back-up-your-files-and-devices

International data transfers | European Data Protection Board

https://www.edpb.europa.eu/sme-data-protection-guide/international-data-transfers_en

IT disaster recovery - Wikipedia

https://en.wikipedia.org/wiki/IT_disaster_recovery - Recovery_Time_Objective

MOBOTIX video technology 100 percent NDAA compliant - Mobotix

https://www.mobotix.com/en/node/16372

National Defense Authorization Act – Pelco's Position Statement

https://www.pelco.com/cybersecurity/ndaa

NDAA/TAA Compliance - Vivotek

https://www.vivotek.com/company/about_us/ndaa_and_taa

ONVIF Profiles - ONVIF

https://www.onvif.org/profiles/

OWASP Top 10:2025- OWASP

https://owasp.org/Top10/2025/

Platform Resiliency Guidelines, NIST Special Publication 800-193

https://doi.org/10.6028/NIST.SP.800-193

Port forwarding - Wikipedia

https://en.wikipedia.org/wiki/Port_forwarding

A Practical Guide to NIST (SP 800-88r1) for Handling Decommissioned IT Equipment - SEAM | Secure Data Destruction & Electronics Recycling

https://seamservices.com/blog/a-practical-guide-to-nist-sp-800-88r1-for-handling-decommissioned-it-equipment/

Principle of least privilege - Wikipedia

https://en.wikipedia.org/wiki/Principle_of_least_privilege

Rights of the data subject | Data Protection Ombudsman's Office

https://tietosuoja.fi/en/rights-of-the-data-subject

Secure Software Development Framework (SSDF) Version 1.1: Recommendations for Mitigating the Risk of Software Vulnerabilities, NIST Special Publication 800-218

https://doi.org/10.6028/NIST.SP.800-218

Security and Privacy Controls for Information Systems and Organizations, NIST Special Publication 800-53 Rev. 5

https://doi.org/10.6028/NIST.SP.800-53r5

Standard RAID levels - Wikipedia

https://en.wikipedia.org/wiki/Standard_RAID_levels

Technical and procurement compliance | Axis Communications

https://www.axis.com/en-us/solutions/government/compliance - ndaa-compliance

Zero Trust Architecture, NIST Special Publication 800-207

https://doi.org/10.6028/NIST.SP.800-207

Glossary

Alarm	Alarms in the Mirasys VMS are configured in the System Manager and can be assigned to user profiles. Alarms have a trigger, action, and calendar that can be activated based on the hour.
API	The application programming interface is a set of programming routines, protocols, and tools for building software applications.
Bandwidth	The maximum possible data transfer rate of a network or internet connection.
Camera	IP camera with its address and user interface for configuration.
Closed network	An information network of computers or other digital devices not connected to an internetwork, e.g. the Internet.
CTU	Chain of Trust for Update, used to authenticate firmware updates.
DNS	Domain Name System, a method of converting IP addresses to hostnames.
Domain	A shared network of computers and the user accounts for them in a corporate environment.
DDoS	Distributed denial-of-service refers to an attack aiming to flood a network or a machine where the incoming traffic originates from multiple sources
DoS	Denial-of-Service is a digital attack aimed at flooding a network or networked device with connection requests, drowning out legitimate requests or overloading a connected device's capabilities.

Driver	A software component used to interact with hardware devices.
DVRServer	VMS recording server service.
Export	This functionality of the Spotter application provides the possibility to save video and audio data into files for any period.
Failback	Failback uses the same functionality as failover but in reverse order by moving recorder functionality from the failover server back to the failed Recorder. Manual failback can be triggered from the failover log. Automatic failback will trigger failback when automatic fallback is enabled and connected to the failed Recorder is restored successfully.
Failover	Failover servers are VMS Servers on a passive standby until the system recognizes that one of the active video recording VMS Servers has broken down; at this point, a failover server takes the place of the broken server. This function grants an automatic switch from a production server to a spare (=failover) server. The switch will start when the slave server is unavailable for a configured period. By default, this threshold time is 10 minutes to avoid the process from starting on temporary network problems.
Firewall	The network security measure, screening incoming and outgoing network traffic and blocking unauthorized or harmful packets.

Gateway	Gateway is an optional service that can be installed to grant users access via web browser, mobile applications or Gateway SDK integrations.
GPU	Graphics Processing Unit, a processor chip specialized in calculating, generating and outputting images from data. Can be harnessed for other complex computational tasks, such as distributed computing.
High Availability	This technology is used for master servers to grant an automatic switch within milliseconds from the production master server to a master server in standby mode. This function is typically provided by Hyper-V or VMware systems.
HTTP	Hypertext Transfer Protocol, an application layer Internet protocol used for sending requests from a web client (e.g. a web browser) to a web server, returning web content (web pages) from the server back to the client.
HTTPS	Hypertext Transfer Protocol over TLS, an application layer Internet protocol used for sending requests from a web client (e.g. a web browser) to a web server, returning web content (web pages) from the server back to the client over TLS-secured communications.
ICT	Information and Communications Technology, the term for fields relating to telecommunications and information networking.
Incident Reporting	Incident Reporting is a service that takes care of creating daily reports and incident reports, which can contain video clips or images as evidence.

I/O device	Hardware that is used to communicate with a computer
IP	Internet Protocol, an OSI Layer 3 networking protocol.
IPSec	Internet Protocol Security Architecture, security suite used to secure packets between routers, forming VPN tunnels over IP networks.
LAN	Local Area Network, a small, usually home or office-level networked area.
Layer 2	2nd layer (Data Link) of the OSI model, transfers data between adjacent network nodes in a WAN or between nodes on the same local area network segment.
Layer 3	3rd layer (Network) of the OSI model, used for packet forwarding, including routing through intermediate routers.
License	Every VMS server (master or slave) has its license, which provides features to this one server. Example: Number of channels, integration connectors, special plugins, etc.
Load	Network traffic through or on network components, such as connections or devices.
MAC Address	Media Access Control address, a physical-layer identifier composed of six pairs of hexadecimal characters for network interfaces of digital devices. The first three pairs identify the device/interface manufacturer.

Master	VMS server device with the Mirasys SMServer service installed on it.
Main server	Central server with typically no recording functionality. This server manages alarms, user access, profiles and system configuration.
Metadata	Separated into two groups: 1. Event metadata describes attributes of an object/scene/event in the context of a preconfigured rule on the metadata source/device. Face detection, ANPR and tripwire are specific events. 1. Continuous object attributes like bounding box coordinates, speed, and size… on every frame of video footage. These metadata are described in text from the activity of objects in video footage.
Multicast	Transmission of an audio or video stream from one computer to others selected to be the targets. In computer networking, multicast is group communication where data transmission is simultaneously addressed to a group of destination computers.
NAT	Network Address Translation, translation of an internal network's IP addresses to outside IP addresses.
Network	Logical structure between a collection of interconnected digital devices. All active and passive network components enable the application to communicate.
NIC	Network Interface Controller, a computer device's LAN adapter card.

OS	Operating System, system software managing hardware and software resources, and provides common services for computer programs.
Person search	The person search is the Mirasys Spotter plugin, which uses Person/Vehicle/Bike detector SSD detection architecture, RMNet backbone, and learnable image downscale block. The model is intended for security surveillance applications and works in various scenes and weather/lighting conditions.
Plugin	A spotter is expandable with plugins. Built-in plugins are currently enabled functionality, and available plugins depend on the product version and licensed features.
Port	Software construct serving as a network communications endpoint for a computer or other digital device.
Port forwarding	Application of NAT that redirects communications from one address and port number combination to another while the packets are traversing a network gateway.
Principle of Least Privilege (PoLP)	Users should only be given the minimum access rights that are required to perform their needed tasks.
PTZ	“Pan, Tilt, Zoom,” two-axis remote-controlled camera.
QoS	Quality of Service, a description of the general performance of a service (often network performance).

RAID	Redundant Array Of Independent Disks, a method of saving data across multiple disks. RAID levels are used to categorize readiness of data integrity and redundancy.
Router	Active network component to control, filter and direct network traffic. Typically Layer-2 or 3.
RTP	Real-time Transport Protocol, a networking protocol used for delivering audio and video over IP networks.
RTSP	Real-Time Streaming Protocol, a connectionless networking protocol used to control video streaming between a viewing client and a video source.
RTSPS	Real-Time Streaming Protocol over TLS, a secure networking protocol used to control video streaming between a viewing client and a video source.
RTU	The Root of Trust for Update (RTU) is responsible for authenticating firmware updates and critical data changes to support platform protection capabilities.
SMServer	System Manager Server, VMS master controller service The service name of the master server. This service is installed on every system but is only required on the master server for system configuration, alarm handling or user/profile management.
Spotter	Spotter is the leading Windows application to access the system as a user. Find more details in the Spotter User Guide for your version.

Spotter Web	Spotter Web is an HTML5 client in which communication is automatically encrypted using IIS certificates.
Storage Locker	Storage Locker is Mirasys VMS service which takes care of video clips, images, and incident reports in a centralized location.
Storyboard	This functionality of the Spotter application allows exporting of data with comments provided in a storytelling format.
Stream	Continuous audio or video transmission over a network A stream is the data send by a device or system to a receiver. We typically use this term for video streams.
Subnet	A network segment sharing a range of IP addresses. Subnet size is represented with a prefix signifying the number of bits (most significant first) reserved for a subnet.
System Manager	System Manager is the Windows application to configure the installation. This application is installed on every VMS server by default. In multi-server installations, the system administrators should use only the System Manager of the Master server to configure elements.
TCP	Transmission Control Protocol, a networking protocol.
Text channel	Receiving point for text messages in the VMS.
ThruCast	A proprietary direct video streaming feature that streams video directly to a Spotter client in case of a recording VMS server disconnect or for the purpose of network optimization.

TLS	Transport Layer Security, formerly known as SSL (Secure Sockets Layer), is a cryptographic protocol that provides secure communication over an IP network.
Tunnel	A channel that allows untouched packets of one network to be transported over another network.
UDP	User Datagram Protocol, a connectionless networking protocol.
Update	Going from lower to higher minor software version, eg. v9.9 -> v9.10.
Upgrade	Going from lower to higher major software versions, eg. v8.x -> v9.x.
UPnP	Universal Plug and Play, is a set of networking protocols that permits networked devices to discover each other's presence on the network and establish functional network services.
VCA	Video Content Analysis is AI model-based image processing to describe video footage in text form.
VLAN	Virtual Local Access Network, a logical method of partitioning a layer-2 network by assigning Ethernet ports to virtual networks.
VMS	Video Management System. This describes all software components required for a complete system functionality to configure, administer, process, view, record, stream and store data from devices.

VPN	Virtual Private Network, secure communication line between end devices over a larger network.
WDServer	The service name of the WatchDog service. This service is installed on every system to monitor and restart the other services and report hardware problems.
WLAN	Wireless LAN, wireless local networking. Also known as Wi-Fi.
ZPA	Zero Proof Authorization, an authentication method.