MIRASYS
DEEP VISION DATA COMPANY

Hardening Guide

English version published on 11 July 2023

Mirasys Ltd – Espoo, Finland
Tel +358 (0)9 2533 3300 • Email info@mirasys.com • www.mirasys.com
documentation.mirasys.com

Hardening Guide

Cyber Security, Best Practices, and Incident Response

Introduction

Security continues to increase in importance when we see increasing attempts to compromise critical IT infrastructure at corporations.

This guide describes Mirasys' security, physical security measures, and best practices that can help secure your Mirasys VMS against cyber-attacks. This includes security considerations for the hardware and software of a video surveillance system's servers, clients, and network device components.

The guide adopts standard security and privacy controls. It maps them to each of the recommendations, which makes it a resource for compliance across industry, government security, and network security requirements.

The guide provides two different levels of information:

- Basic information with general insights into security in the company and the product (VMS systems)
- The advanced information in the form of IT-specific technical guidance on hardening Mirasys VMS products.

Scope and applicability

This guide is relevant for organizations of all sizes, from small businesses to large enterprises and government agencies, that utilize the Mirasys VMS for their video surveillance needs. It primarily aims at people using Mirasys' software, system integrators, and component manufacturers. It also applies to all employees, contractors, and other third-party vendors working with or for Mirasys Oy.

The Guide covers all aspects of the Mirasys VMS, including servers, clients, network devices, and camera components. The policies and best practices outlined in this guide are applicable to the design, development, deployment, maintenance, and operation of the Mirasys VMS.

The information provided in this guide 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 adapt the recommendations in this guide to suit their unique environment and risk profile.

Glossary

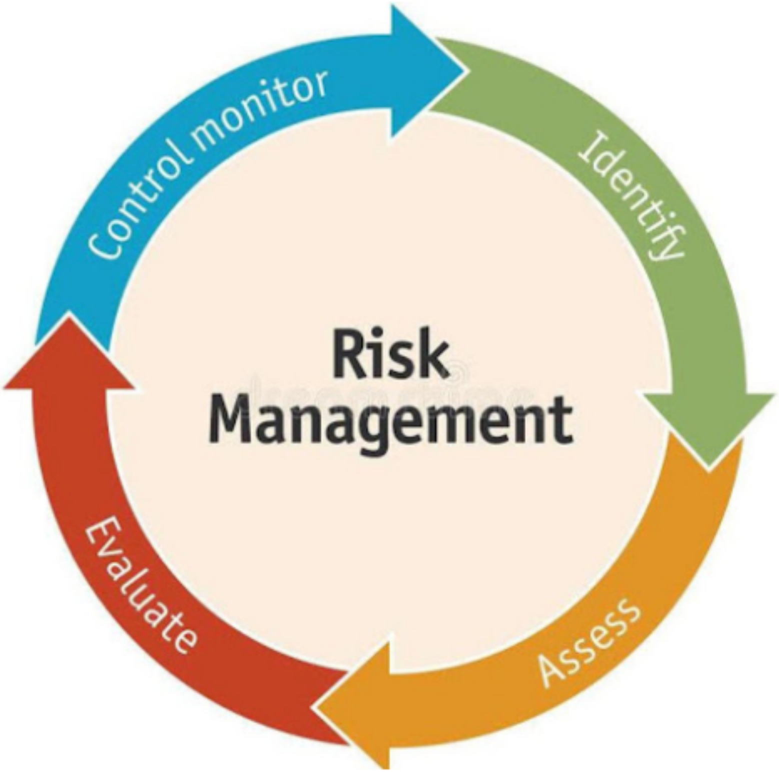
Buyer	**The people or organizations that consume a given product or service.**
Critical Infrastructure	Systems and assets, whether physical or virtual, so vital to the country that the incapacity or destruction of such systems and assets would have a debilitating impact on cybersecurity, national economic security, national public health or safety, or any combination of those matters.
Cybersecurity	The process of protecting information by preventing, detecting, and responding to attacks.
Cybersecurity Incident	A cybersecurity event that has been determined to have an impact on the organization prompting the need for response and recovery.
Framework	A risk-based approach to reducing cybersecurity risk composed of three parts: the Framework Core, the Framework Profile, and the Framework Implementation Tiers. Also known as the “Cybersecurity Framework.”
Framework Core	A set of cybersecurity activities and references that are common across critical infrastructure sectors and are organized around particular outcomes. The Framework Core comprises four types of elements: Functions, Categories, Subcategories, and Informative References.
Framework Implementation Tier	A lens through which to view the characteristics of an organization’s approach to risk—how an organization views cybersecurity risk and the processes in place to manage that risk.
Framework Profile	A representation of the outcomes that a particular system or organization has selected from the Framework Categories and Subcategories.
Risk	A measure of the extent to which an entity is threatened by a potential circumstance or event, and typically a function of: (i) the adverse impacts that would arise if the circumstance or event occurs; and (ii) the likelihood of occurrence.
Risk Management	The process of identifying, assessing, and responding to risk.
Supplier	Product and service providers used for an organization’s internal purposes (e.g., IT infrastructure) or integrated into the products of services provided to that organization’s Buyers.

Security Concepts

Cyber threats and risks

Cybersecurity refers to the technologies, processes, and practices designed to protect an organization's intellectual property, customer data, and other sensitive information from unauthorized access by cybercriminals.

The frequency and severity of cybercrime are on the rise and there is a significant need for improved cybersecurity risk management as part of every organization's enterprise risk profile. It's one of the top risks to any business.



The threat lifecycle is important for risk assessment because it shows where you can mitigate threats. The goal is to reduce the number of vulnerabilities and to address them as early as possible. For example, discouraging an attacker who is probing a system for vulnerabilities can eliminate a threat.

The risk and threat assessment process includes the following steps:

- Identify information and security risks
- Assess and prioritize risks
- Implement policy, procedures, and technical solutions to mitigate these risks

The overall process of risk and threat assessment, and the implementation of security controls, is referred to as a risk management framework. This document refers to NIST security and privacy controls and other publications about risk management frameworks.

Importance of NIST standards

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

Hardening

Developing and implementing security measures and best practices are known as "hardening."

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. For example, during the reconnaissance phase, an attacker scans to find open ports and determine the status of services that are related to the network and the VMS. To mitigate this, the hardening guidance is to close unnecessary system ports in Mirasys VMS and Windows configurations.

While most of the information in this guide focuses on IT settings and techniques, it is important to remember that physical security is also a vital part of hardening. For example, use physical barriers to servers and client computers, and make sure that things like camera enclosures, locks, tamper alarms, and access controls are secure.

The following are the actionable steps for hardening a VMS

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

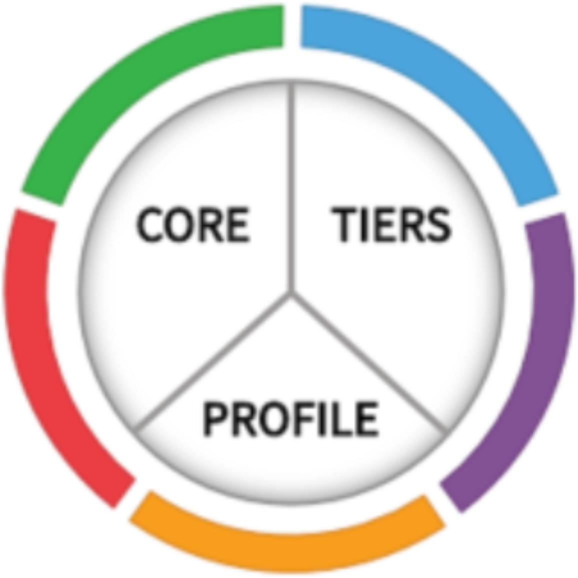
Cybersecurity Framework

The Framework is voluntary guidance, based on existing standards, guidelines, and practices for organizations to better manage and reduce cybersecurity risk. In addition to helping organizations manage and reduce risks, it was designed to foster risk and cybersecurity management communications amongst both internal and external organizational stakeholders.

Framwork information:

1. NIST Framework for Improving Critical Infrastructure Cybersecurity
2. Related link with Cybersecurity framework description

The Cybersecurity Framework consists of three main components: the Core, Implementation Tiers, and Profiles.



Framework Core

The Core is **a set of desired cybersecurity activities and outcomes organized into Categories and aligned to Informative References**. The Framework Core is designed to be intuitive and to act as a translation layer to enable communication between multi-disciplinary teams by using simplistic and non-technical language.

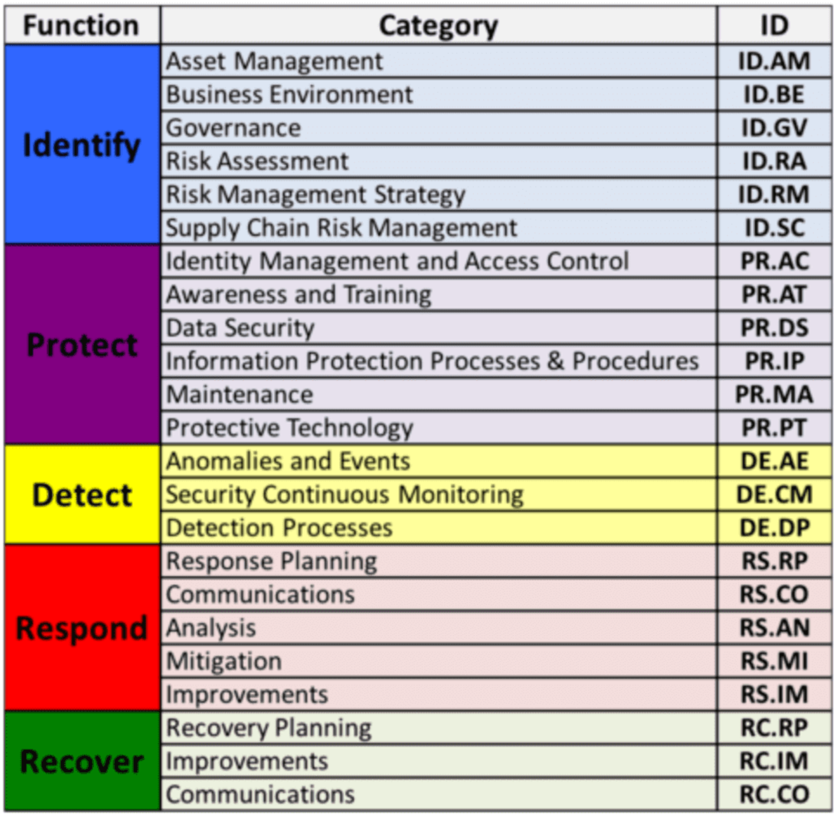
The Core consists of three parts:

1. Functions
2. Categories
3. Subcategories.

The Core includes five high-level functions:

1. Identify
2. Protect
3. Detect
4. Respond
5. Recover

These 5 functions are not only applicable to cybersecurity risk management but also to risk management at large. The next level down is the 23 Categories that are split across the five Functions. The image below depicts the Framework Core's Functions and Categories.



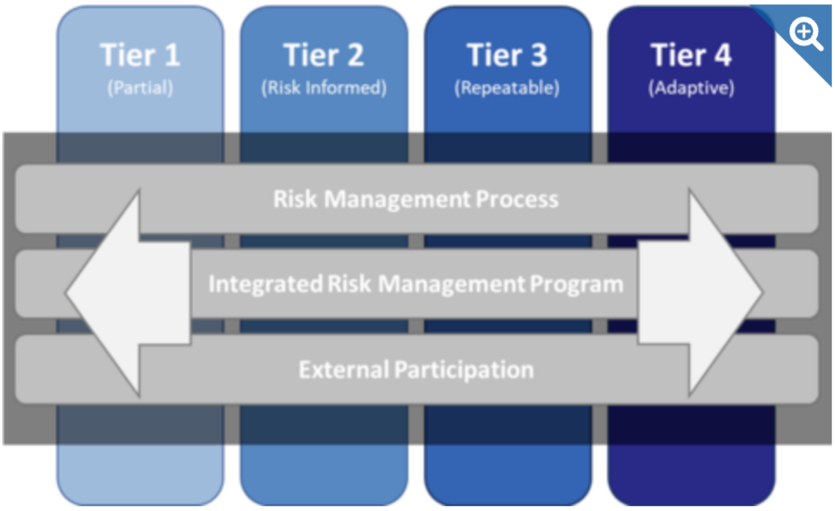
Function	Category	ID
Identify	Asset Management	ID.AM
	Business Environment	ID.BE
	Governance	ID.GV
	Risk Assessment	ID.RA
	Risk Management Strategy	ID.RM
	Supply Chain Risk Management	ID.SC
Protect	Identity Management and Access Control	PR.AC
	Awareness and Training	PR.AT
	Data Security	PR.DS
	Information Protection Processes & Procedures	PR.IP
	Maintenance	PR.MA
	Protective Technology	PR.PT
Detect	Anomalies and Events	DE.AE
	Security Continuous Monitoring	DE.CM
	Detection Processes	DE.DP
Respond	Response Planning	RS.RP
	Communications	RS.CO
	Analysis	RS.AN
	Mitigation	RS.MI
	Improvements	RS.IM
Recover	Recovery Planning	RC.RP
	Improvements	RC.IM
	Communications	RC.CO

The Categories were designed to cover the breadth of cybersecurity objectives for an organization, while not being overly detailed. It covers topics across cyber, physical, and personnel, with a focus on business outcomes.

Framework Implementation Tiers

Tiers describe **the degree to which an organization's cybersecurity risk management practices exhibit the characteristics defined in the Framework**.

The Tiers range from Partial (Tier 1) to Adaptive (Tier 4) and describe an increasing degree of rigor, how well-integrated cybersecurity risk decisions are into broader risk decisions, and the degree to which the organization shares and receives cybersecurity info from external parties.

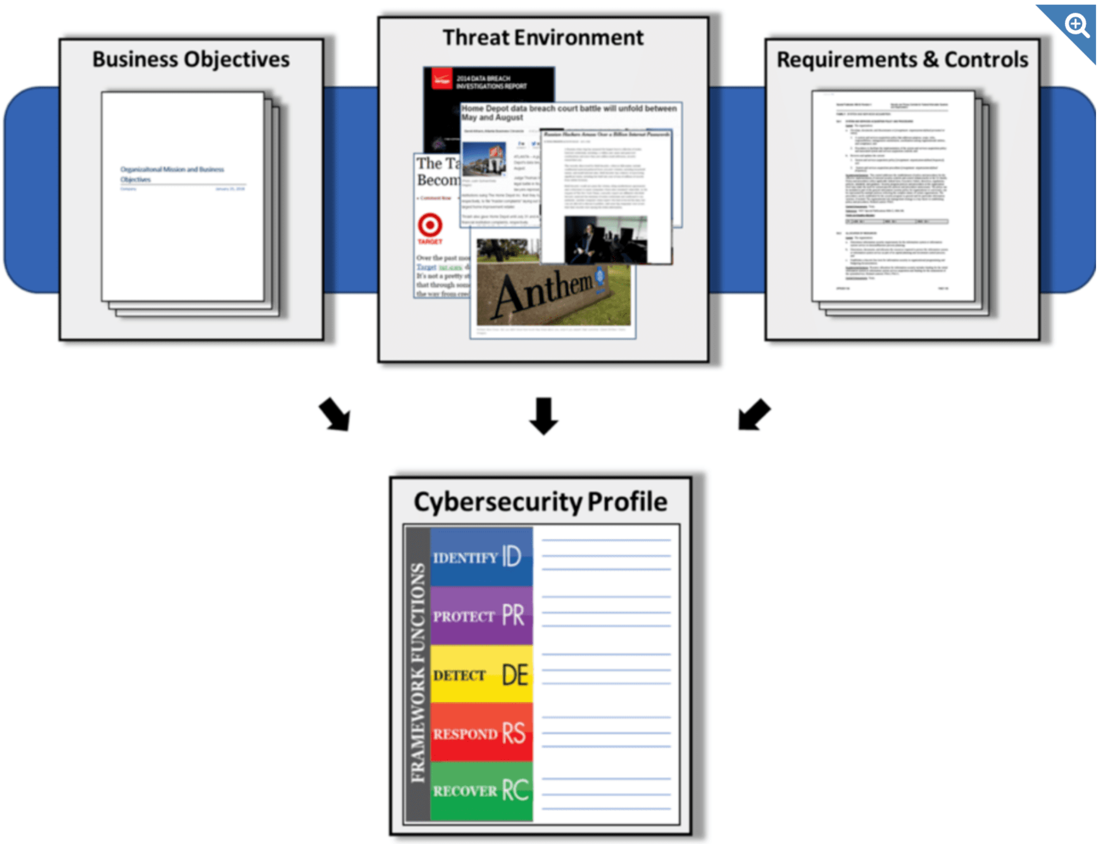


Tiers do not necessarily represent maturity levels. Organizations should determine the desired Tier, ensuring that the selected level meets organizational goals, reduces cybersecurity risk to levels acceptable to the organization, and is feasible to implement, fiscally and otherwise.

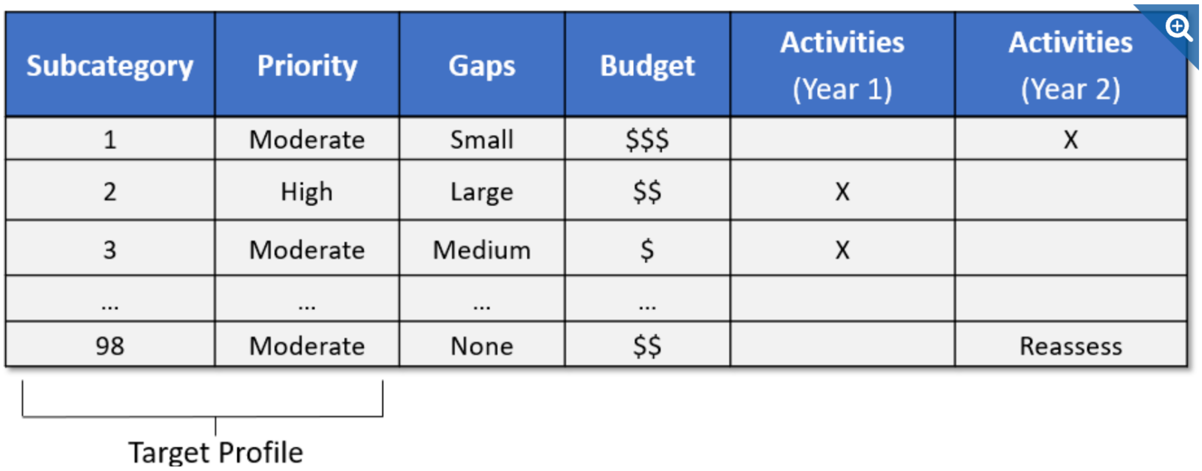
Framework Profiles

Profiles are **an organization's unique alignment of its organizational requirements and objectives, risk appetite, and resources against the desired outcomes of the Framework Core**.

Profiles can be used to identify opportunities for improving cybersecurity posture by comparing a “Current” Profile with a “Target” Profile.



Profiles are about optimizing the Cybersecurity Framework to best serve the organization. The Framework is voluntary, so there is no 'right' or 'wrong' way to do it. One way of approaching profiles is for an organization to map its cybersecurity requirements, mission objectives, and operating methodologies, along with current practices against the subcategories of the Framework Core to create a Current-State Profile. These requirements and objectives can be compared against the current operating state of the organization to gain an understanding of the gaps between the two.



Subcategory	Priority	Gaps	Budget	Activities (Year 1)	Activities (Year 2)
1	Moderate	Small	$$$		X
2	High	Large	$$	X	
3	Moderate	Medium	$	X	
...	...	...	...		
98	Moderate	None	$$		Reassess

Target Profile

The creation of these profiles and the gap analysis allows organizations to create a prioritized implementation plan. The priority, size of the gap, and estimated cost of the corrective actions help organizations plan and budget for cybersecurity improvement activities.

Hardening VMS Components

Components to protect

1. Servers (physical and virtual)
2. Network
3. Software applications
4. Cameras

Configure the VMS with roles that control access to the system, and designate tasks and responsibilities. (AC2, AC3, AC6, AC16, AC25, AU6, AU9, CM5, CM11, IA5, PL8, PS5, PS7, SC2, SI7, in Appendices D and F in NIST SP 800-53 Rev4).

Hardening servers (physical and virtual)

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 a strong password policies for users. *(See password policy in Appendices)*

- 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, such as Titanium Linux
- Restrict access to servers. Keep servers in locked rooms, and make it difficult for intruders to access network and power cables. (PE2 and PE3 in Appendices D and F in NIST SP 800-53 Rev4 (http://nvlpubs.nist.gov/nistpubs/specialpublications/nist.sp.800-53r4.pdf) (PE Physical and Environment Protection).)

Mirasys VMS servers

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 Mirasys Spotter.

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. See Kerberos authentication (explained). 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 Mirasys 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 these hosts and users as members of a group with a given function or role.

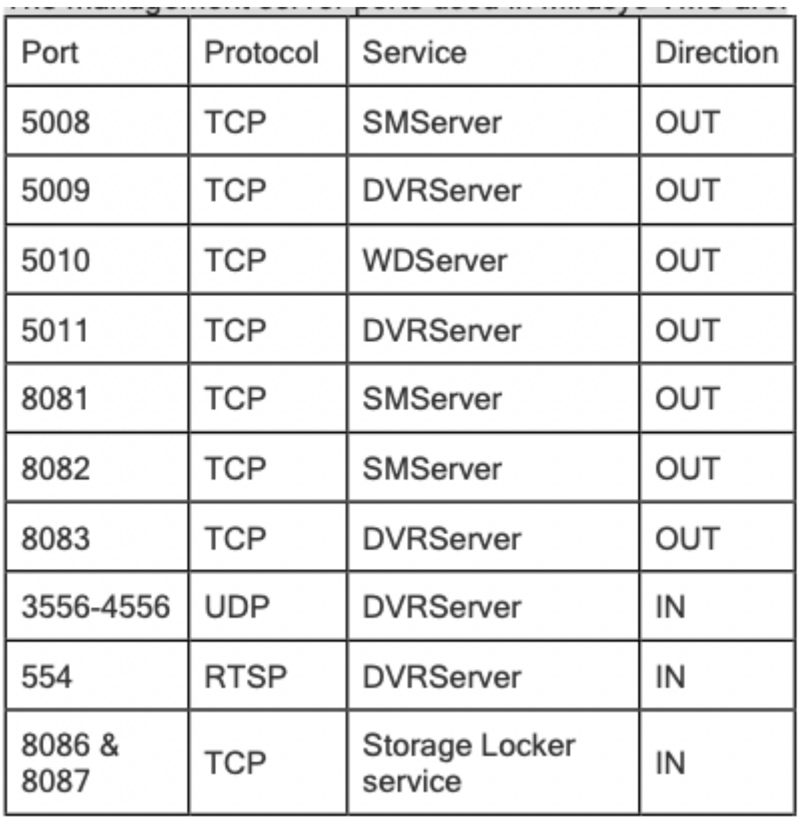
Design the network so that there is a subnet or VLAN for each function. For example, one subnet or VLAN for surveillance operators and one for administrators. This allows you to define firewall rules by group instead of individual hosts.

Management Server

> Enable only the ports used by the management server. Documenting and maintaining security settings on each system.

Mirasys recommends enabling only the ports used by the management server and blocking all other ports, including the default Windows ports. This guidance is consistent for the server components of Mirasys VMS.

The management server ports used in Mirasys VMS are:



Port	Protocol	Service	Direction
5008	TCP	SMServer	OUT
5009	TCP	DVRServer	OUT
5010	TCP	WDServer	OUT
5011	TCP	DVRServer	OUT
8081	TCP	SMServer	OUT
8082	TCP	SMServer	OUT
8083	TCP	DVRServer	OUT
3556-4556	UDP	DVRServer	IN
554	RTSP	DVRServer	IN
8086 & 8087	TCP	Storage Locker service	IN

The ports used depend on the deployment. If in doubt, contact Mirasys Support.

Recording Server

Use separate network interface cards.

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

Hardening the network

Network Infrastructure

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

Network hardening
If left unprotected, cameras and their network connections represent a significant risk of compromise, potentially giving intruders further access to the system.

1) Use secure and trusted networks connection.
Mirasys recommends selecting cameras that support HTTPS. Network communications must be secure, whether or not you are on a closed network. 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 (https://datatracker.ietf.org/wg/tls/charter/) (TLS, currently 1.2) with valid certificates that meet industry best practices, such as from Public-Key Infrastructure (X.509) (https://datatracker.ietf.org/wg/ipsec/documents/) and CA/Browser Forum (https://cabforum.org/).

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:

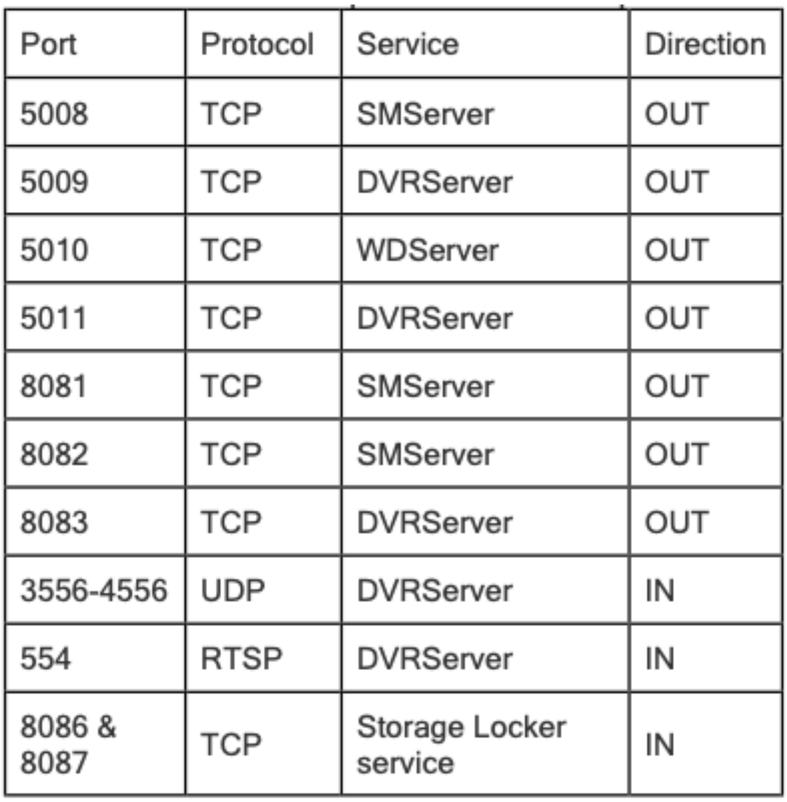
- Use secure device authentication
- Use TLS
- Use device whitelisting to authenticate devices
- Use firewalls to limit network communication between servers and client computers and programs.

All Mirasys VMS components and the ports needed by them are listed in individual sections below.

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.

The lists also include the ports used for local processes.



Port	Protocol	Service	Direction
5008	TCP	SMServer	OUT
5009	TCP	DVRServer	OUT
5010	TCP	WDServer	OUT
5011	TCP	DVRServer	OUT
8081	TCP	SMServer	OUT
8082	TCP	SMServer	OUT
8083	TCP	DVRServer	OUT
3556-4556	UDP	DVRServer	IN
554	RTSP	DVRServer	IN
8086 & 8087	TCP	Storage Locker service	IN

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, with the exception of when TruCast 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).
Additionally, Mirasys recommends **not** using wireless cameras in mission-critical locations. Wireless cameras are easy to jam, leading to video loss.

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 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 user names and passwords and certificates from a Certificate Authority for HTTPS.
For more information, see the device manufacturer's hardening guides and other guidance.

9) Other recommendations

- It is recommended that Mirasys Spotter is on the same VLAN as the servers.
- 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

Software application hardening

All software applications

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 like LastPass to manage and encrypt passwords for improved password storage, organization, and safekeeping
- Establishing an intrusion prevention system (IPS) or intrusion detection system (IDS)

Client programs

The sections below provide guidance about how to protect the Mirasys client programs. The client programs are:

- Mirasys System Manager
- Mirasys Web Client
- Mirasys Spotter
- Spotter Mobile

> Always run clients on trusted hardware on trusted networks

Mirasys recommends that you always run Mirasys clients on hardware devices with the proper security settings.

Specific guidance for mobile devices is available in SP 800-124 (SP 800-124).

These settings are specific to the device.

Hardening cameras

It is recommended to set the cameras on separate VLANs and use HTTPS for the camera to Recording Server communication.

Mirasys Spotter

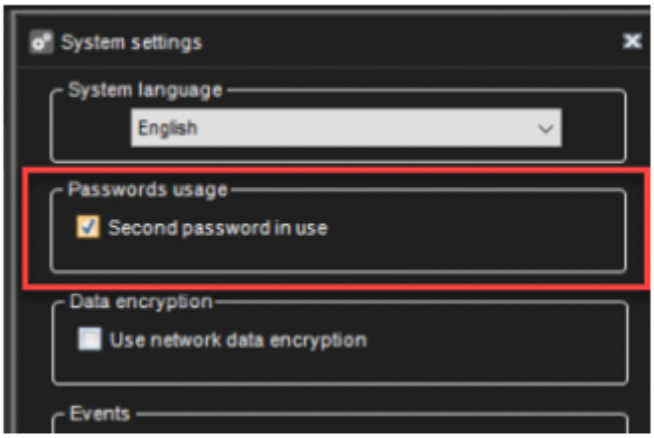
1) Restrict physical access to any computer running Mirasys Spotter

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) Enable a Second password in use



System settings

System language: English

Passwords usage: ☑ Second password in use

Data encryption: □ Use network data encryption

Events

4) 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.

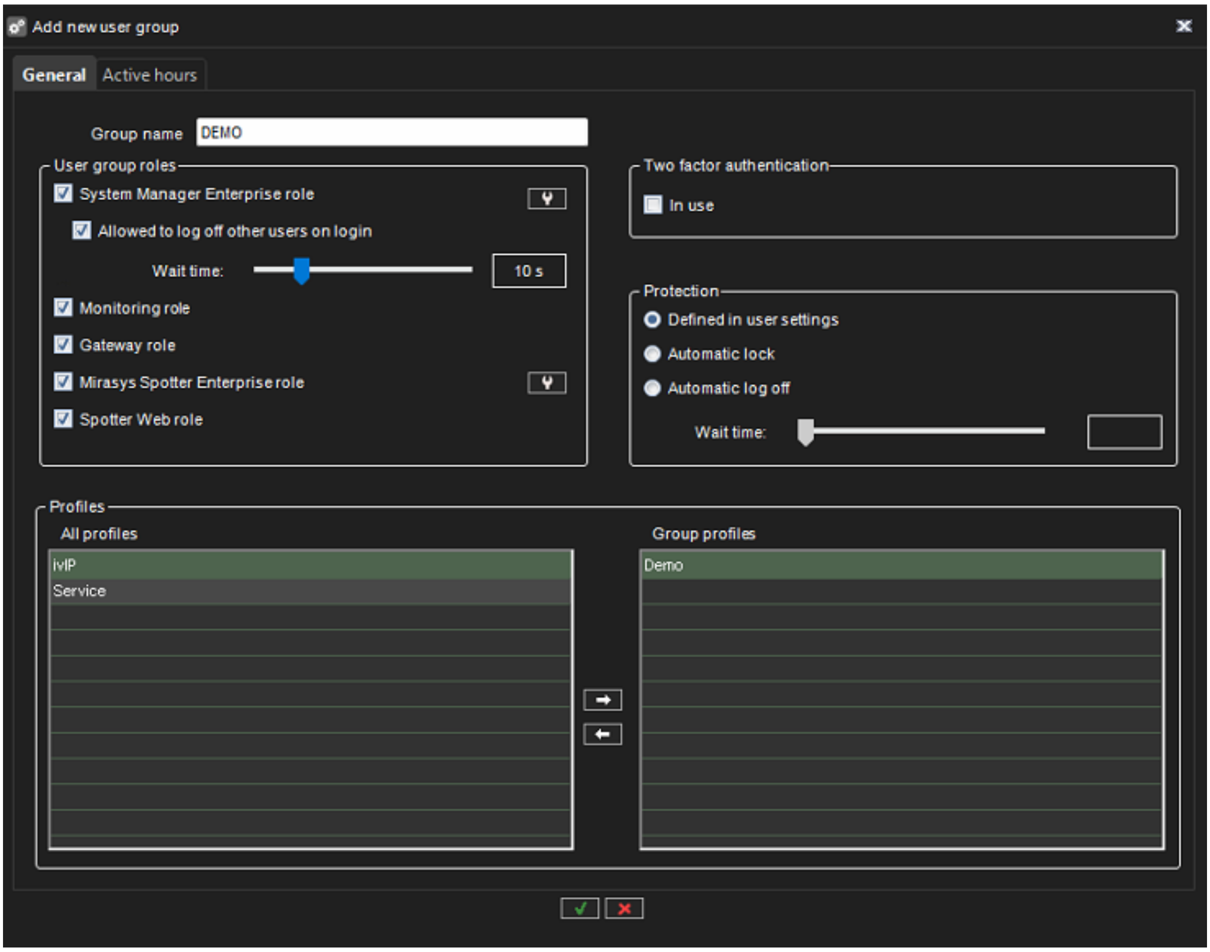
5) Use separate names for user accounts
Mirasys recommends creating a user account for each user and using a naming convention that makes it easy to identify them personally, such as their name or initials. This is a best practice for limiting access to only what is necessary and reducing confusion when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

6) 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.

4. System Manager

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.



Add new user group

General | Active hours

Group name: DEMO

User group roles
- ☑ System Manager Enterprise role
  - ☑ Allowed to log off other users on login
  - Wait time: 10 s
- ☑ Monitoring role
- ☑ Gateway role
- ☑ Mirasys Spotter Enterprise role
- ☑ Spotter Web role

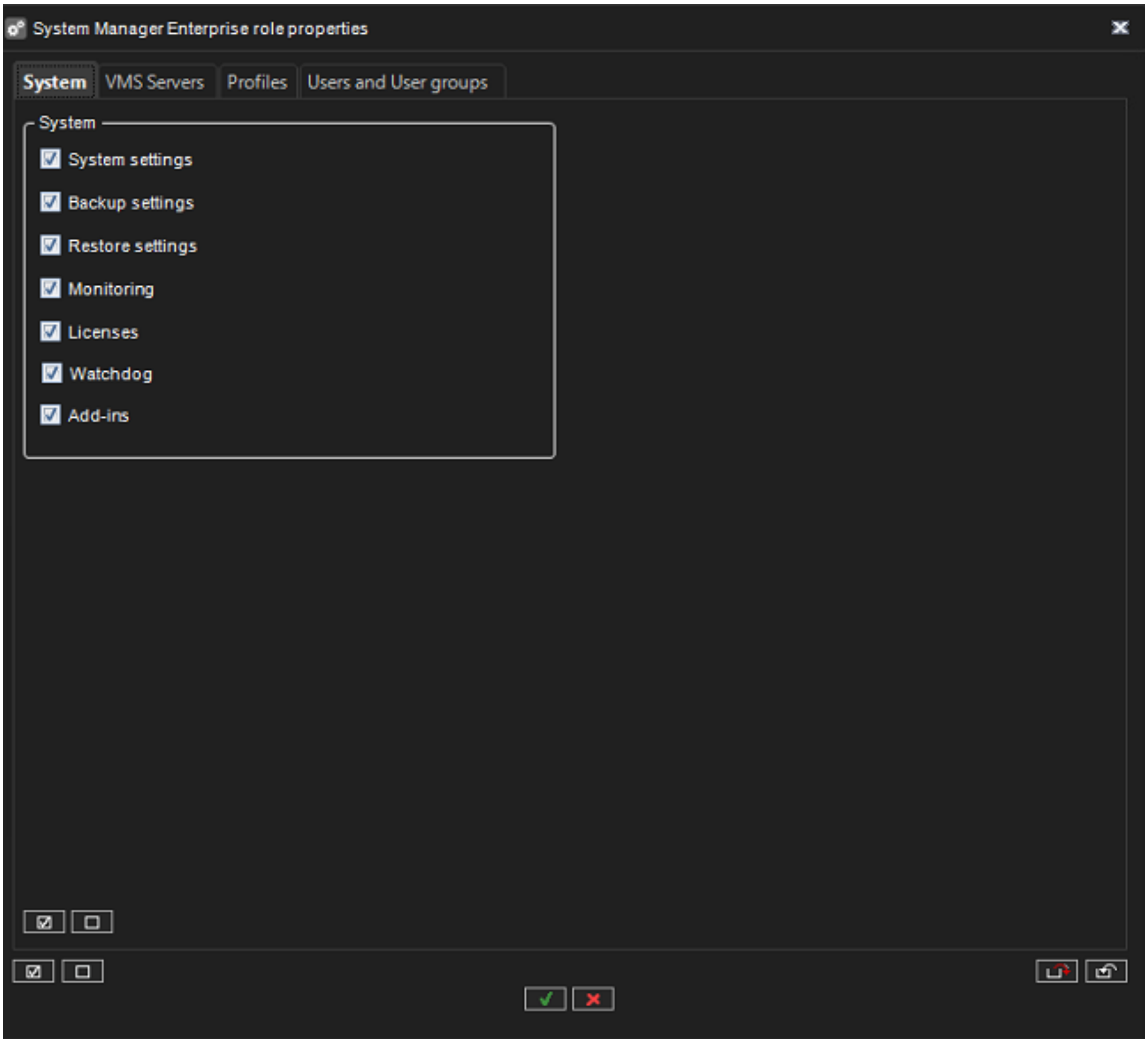
Two factor authentication
- □ In use

Protection
- ● Defined in user settings
- ○ Automatic lock
- ○ Automatic log off
- Wait time:

Profiles

All profiles:
- iVIP
- Service

Group profiles:
- Demo



System Manager Enterprise role properties

System | VMS Servers | Profiles | Users and User groups

System

- ☑ System settings
- ☑ Backup settings
- ☑ Restore settings
- ☑ Monitoring
- ☑ Licenses
- ☑ Watchdog
- ☑ Add-ins

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.

Physical security considerations

1. Use of physical barriers to servers and client computers
2. Camera enclosures, locks, tamper alarms, and access controls

Application build-in security features

Mirasys VMS products are designed to deliver secure, end-to-end communication. Mirasys products are designed to protect privacy and secure data.
Data protection is always important, especially if you intend to be 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.

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 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 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.

A company or person can record videos of people in a public place since that person has no reasonable expectation of privacy when he is located 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. According to the definition, a public place is a place that is generally open and accessible to people—examples of public places: public squares, streets, parks, roads, and beaches. Nevertheless, public places can include pieces of private territories or objects. Thus, the private territories and an object that could be viewed in the public spaces should be defined before choosing the camera angle location and recording the video view. Then, if private objects were defined in the video overview, the camera should be positioned in order 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 get 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.
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 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 squire or have another form; the private zone can also be blurred. Administrators can set up private zones and user permissions regarding these private zones.

In Mirasys VMS, there is support for privacy masking 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.
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 context of a camera, a relevant example of privacy by default could be using privacy masking to keep a sensitive area within the view of the camera private.

1. GDPR - Privacy zones

Use privacy zones to help eliminate surveillance of areas irrelevant to your surveillance target.
Mirasys recommends setting a privacy zone for clients in sensitive areas and places where personal identification is not allowed. Create then a second role that can authorize the mask to be removed.

2. GDPR - Retention time

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.

3. Resolution of different points

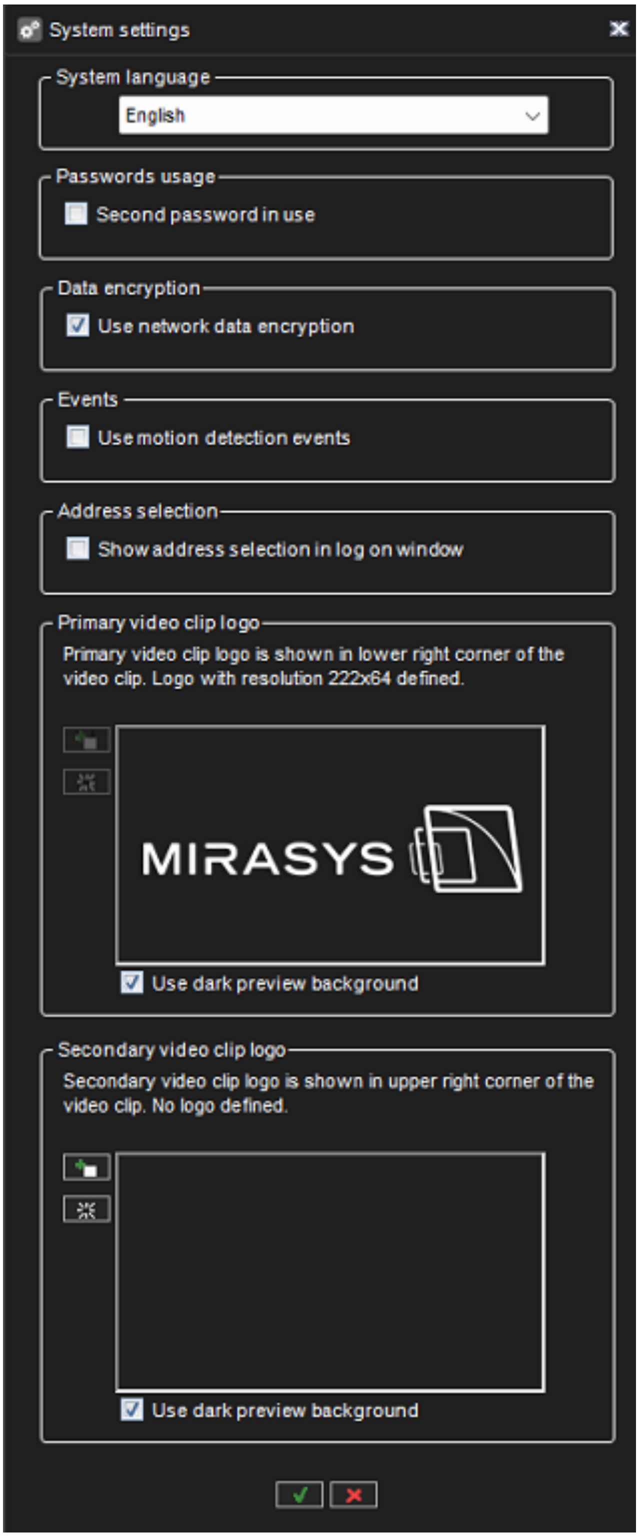
Different purposes require different image qualities.
When identification is unnecessary, the camera resolution and other modifiable factors should be chosen to ensure no recognizable facial images are captured.

4. Secure material export

Mirasys recommends allowing access to export functionality for a select set of users needing this permission.
Mirasys also recommends only changing the Mirasys Spotter Enterprise Plus role to allow export in SEF Format.
AVI and JPEG exports should not be allowed because they can not be made secure.
This makes the export of any evidence material password-protected, encrypted, and digitally signed, making sure forensic material is genuine, untampered with, and viewed by the authorized receiver only.

5. Client Data encryption functionality

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



System settings

System language
English

Passwords usage
□ Second password in use

Data encryption
☑ Use network data encryption

Events
□ Use motion detection events

Address selection
□ Show address selection in log on window

Primary video clip logo
Primary video clip logo is shown in lower right corner of the video clip. Logo with resolution 222x64 defined.

☑ Use dark preview background

Secondary video clip logo
Secondary video clip logo is shown in upper right corner of the video clip. No logo defined.

☑ Use dark preview background

6. Two-Factor Authentication (2FA)

Mirasys recommends that you specify an additional login step for users of Mirasys System Manager.

7. User roles
Apply the principle of least privilege (PoLP).

Mirasys recommends that you only allow access to functionality for a select user set that needs this permission. 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.

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. Grant access to only the cameras that the specific operator needs to access, and 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.

8. Functionality to restrict administrator permissions with user roles
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