Hardening Guide for OnSSI's Ocularis 5 Video Management System

Date: April 9, 2018

Rev: 00040620181703

Table of Contents

Hardening Guide for Video Surveillance Systems

Introduction

Cybersecurity for Video Surveillance Systems

Over the past two decades, video surveillance technology has evolved from analog closed-circuit television (CCTV) technology to networked digital video cameras and recording technology. Cameras are now embedded computers with video capture sensors and intelligent analytics algorithms that optimize video, create digital scene models, and provide metadata about scene activity and other information. As with all networked computer systems, protecting the systems from cyberattacks is of critical importance.

System hardening is the development and application of cybersecurity measures to a networked computer system to protect it against attacks from potential threats. Secure video surveillance systems are not a luxury – they are a necessity. However, research by the Center for Internet Security® (CIS) gives us the following good news:

> **Most cyber attacks are not the sophisticated, complex activity shown on television and in movies – in fact, attacks often rely on simply misconfigured or outdated systems . . . the vast majority of cybersecurity problems that plague us today could be prevented by action, technology, and policies that are already known or exist in the marketplace.** [1]

The CIS is a forward-thinking, non-profit entity whose mission it is to safeguard private and public organizations against cyber threats.[2] As cyber risks evolve, the CIS updates its critical security controls list, based on new attacks that are identified and analyzed by leading security research firms, and also based on technology advances and trends. The CIS Controls list was updated in March of 2018 from version 6.1 to version 7, just before this hardening guide was written. This guide is based on the field-proven recommendations of the Center for Internet Security and its CIS Controls™ guidance version 7.

OnSSI's Approach to Product Cybersecurity

Most organizations focus strongly on the security of their networks and expect application vendors to focus on the security of their applications. Research has shown that 84% of

[1] "Auditing, Assessing, Analyzing: A Prioritized Approach using the Pareto Principle", Center for Internet Security, 20 Mar. 2018, p.3. Download: https://www.cisecurity.org/white-papers/auditing-assessing-analyzing-a-prioritized-approach-using-the-pareto-principle/

[2] "About Us", Center for Internet Security, 20 Mar. 2018, https://www.cisecurity.org/about-us/

cyberattacks happen on the application layer.[3] This means two things: applications must be kept updated with the latest patches, and deployed systems need to be hardened to reduce their attack surface (the points at which an application's attackers can insert or remove data). Thus, two key areas of focus for the OnSSI software development team have been patch distribution and system hardening.

Patch Distribution

How fast and effectively can OnSSI distribute patches to its many thousands of customers, who have tens of thousands of video servers, without having security systems integrators needing to "drop everything" just to perform system updates in a timely manner? That has been the former approach within the security industry, which is not scalable and not cost effective, especially for large-scale deployments.

Thus, OnSSI updates Ocularis servers with security patches overnight, with no user or security technician involvement required. Just like smartphone apps, a new patch is pushed overnight to tens of thousands of online servers or distributed to isolated networks that are not Internet-connected.

Additionally, Ocularis Client software checks for updates. Ocularis 5 can be configured to prompt users to update Client software upon login, if the Ocularis Base software version is found to be newer than the Client software.

Ocularis updates itself to ensure that Ocularis customers remain protected at the lowest cost of maintenance possible.

System Hardening

Ocularis itself contains application security features, including encryption and strong user credential management, to reduce the attack surface of the application. The release of this system hardening guide facilitates the further hardening of Ocularis deployments using field-proven best practices.

Addressing Product Security Vulnerabilities

OnSSI works hard to provide software that our customers can trust and rely on for their video surveillance system deployments. That includes improving and upgrading the cybersecurity features of Ocularis and addressing discovered security vulnerabilities in our applications. To do that we actively monitor sources of vulnerability reports relating to the operating systems and third-party software libraries that our applications rely on, and we regularly test our applications for security vulnerabilities as part of our software development process, which

[3] Gloge, Andreas, podcast, "Final Security Frontier: Application Layer." Aired on VoiceAmerica.com, 5 Feb. 2015, 57:57 mins. https://news.sap.com/guestspeaker/andreas-gloege/

we keep improving. We welcome feedback from application security researches who report discovered security vulnerabilities to us.

Security vulnerabilities should be reported to cybersecurity@onssi.com. We will respond quickly to reports of security vulnerabilities, keep vulnerability reporters apprised of our remediation efforts, and promptly provide patches to customers and system service providers as they are released.

About This Guide

This guide presents three video surveillance system cybersecurity profiles, which are sets of numbered recommendations for deployed video surveillance systems cyber defense. They are listed below along with a description of the type of deployment they apply to.

- **Basic:** Simple single-site deployments on a closed local area network (LAN).
- **Advanced:** Site deployments whose LAN is accessible from a wide area network (WAN) and/or the Internet.
- **Enterprise:** Multi-site/multi-LAN deployments running on a corporate IT infrastructure, maintained by an internal and/or external service group following IT Service Management (ITSM) practices within a corporate data governance framework.

All the Basic hardening recommendations apply to Advanced and Enterprise deployments, and all the Advanced recommendations apply also to Enterprise deployments. However, Basic deployments at high-risk facilities should consider implementing Advanced recommendations that make sense based on the deployment's cybersecurity risks, and should also consider the monitoring practices listed in the Enterprise cybersecurity profile.

The differences between Basic, Advanced and Enterprise deployments are typically: (a) the size and scale of deployments, (b) the extent of technology infrastructure management, and (c) the maturity of cyber risk governance frameworks. The Basic Security Profile recommendations apply to all video surveillance deployments. The remaining recommendations are applicable based upon the specifics of each deployment.

Although this guide has been written for video surveillance systems based on OnSSI's Ocularis video management system software, it provides hardening recommendations that are applicable for most security video surveillance systems.

Each numbered hardening recommendation is followed by a listing of the one or more CIS Controls applicable to the recommendation.

In each cybersecurity profile the recommendations are grouped by these classes of computers and devices, because each group has its own typical deployment or usage environments, with attendant cybersecurity risks:

- Cameras
- Servers, Workstations and Laptops
- Mobile Devices
- Networks

This guide labels as “cameras” both “IP cameras” (also known as “digital video cameras” or ”network cameras”) and analog cameras connected to the Oculars video management system via network video encoders (also known as a “media encoders”). Video encoders give analog cameras an IP address and provide additional functionality typically found in IP cameras.

Appendix A contains password guidance based on the significantly revised password recommendations released by the National Institute of Standards and Technology (NIST) in its NIST 800-63-3 publication. **Appendix B** contains the Ocularis network port usage list. **Appendix C** contains references to sections in OnSSI product manuals and guides that refer to specific hardening recommendations.

Applying This Guide

Many organizations have already realized that protecting an organization from cyber-attacks has become a necessary cost and effort associated with using technology as a business tool, and that includes the protection of security video surveillance systems and the data that they produce, both video image data and metadata about video scene activity. This awareness has been heightened by media publicity focusing on the high-profile 2016 and 2017 botnet attacks involving networked video cameras and video recorders.

The continuing advancement of video technology, along with the evolving threats against it, make hardening a video surveillance system an ongoing process rather than a one-time action. The full scope of system hardening involves an appropriate combination of security measures that include people, process and technology elements. Which measures to apply to a deployed system depends on that system’s exposure to likely threats, as well as the criticality, size and complexity of the system.

Organizations must make several conscious decisions regarding their approach to video surveillance system hardening. The larger the organization is, the more important the following questions are:

- Who within the organization will be overall responsible for establishing and maintaining video surveillance system cybersecurity?

- Who should develop and get approved the phased implementation plan for system cybersecurity hardening?

- What coordination will be needed with the organization’s IT, HR, and Legal functions to ensure that policies, procedures, software tools and service contracts are aligned with the organization’s risk governance and technology infrastructure management?

The CIS Controls are widely known and understood, and mappings have been defined for the CIS Controls for all major security standards. Thus, basing this hardening guide on the CIS controls makes it feasible to identify points of commonality between existing organizational technology protections and those desired for video surveillance systems. It also makes it easier to take advantage of existing organizational technology management resources, or to parallel the types of cybersecurity measures the organization uses.

CIS Sub-Controls

For each control, the CIS Controls documentation contains a chart of sub-controls that organizations should take to implement the control. The recommendations in this guide are based on many of the CIS sub-controls. Refer to the original CIS Controls documentation[4] for more information, especially if you are working to identify existing cybersecurity resources that may be available within your organization. The CIS Controls were written to address the entire landscape of an organization’s technology infrastructure, and your organization may already have people, process or technology controls in place that could be utilized for security video surveillance systems.

Additional CIS Guidance

Additional cybersecurity guidance is provided on the CIS website. It includes the best practices that leading organizations and their IT functions have found highly effective. It also includes thoughtful white papers that provide perspectives and case study examples that can be helpful in preparing to plan for, collaborate on, or explain the rationale for cybersecurity measures and tools.

Cybersecurity Profiles

In the following cybersecurity profiles, the first time a CIS Control is listed, a description of the control is provided. Later listings of the control omit the control description.

Note that a few of the recommendations require an additional software or hardware component to be added to the video surveillance system. However, most recommendations are video device or system configuration actions, or changes affecting people or processes.

[4] “CIS Controls Version 7”, Center for Internet Security, 19 Mar. 2018, p.3. Downloadable from: https://www.cisecurity.org/controls/

Basic Security Profile

Cameras

1. **Inventory and Control All Cameras.**

CIS Control 1: Inventory and Control of Hardware Assets

Actively manage (inventory, track, and correct) all hardware devices on the network so that only authorized devices are given access, and unauthorized and unmanaged devices are found and prevented from gaining access.

CIS Control 2: Inventory and Control of Software Assets

Actively manage (inventory, track, and correct) all software on the network so that only authorized software is installed and can execute, and that unauthorized and unmanaged software is found and prevented from installation or execution.

Cameras are hardware devices with embedded computers, operating systems, web servers and other application software. Thus, both hardware and software controls are warranted.

Utilize an active discovery tool to identify devices connected to the video network and update the hardware asset inventory. Your organization may have a tool of choice already in use on the business network, or you may choose to use a security industry tool specifically made for camera discovery, such as the Axis Device Manager software if you only use Axis cameras, or Viakoo.

Ensure that the camera inventory records the network address (IP address), hardware address (MAC address), as well as the camera name, firmware version, date of installation, physical location, target area or scene being covered, and manufacturer and/or systems integrator warranty period.

If add-on or third-party analytics or other software is being run on the camera, inventory that software as well, including manufacturer name, software name and version number.

2. **Begin camera configuration from a known factory default state.**

CIS Control 5: Secure configuration for hardware and software on Mobile Devices, Laptops, Workstations and Servers

Establish, implement, and actively manage (track, report on, correct) the security configuration of mobile devices, laptops, servers, and workstations using a rigorous configuration management and change control process in order to prevent attackers from exploiting vulnerable services and settings.

Before beginning camera configuration, make sure that the camera is in a known factory default state. Follow the manufacturer's instructions to return the camera to its factory default state if you are not sure of its state.

3. **Document and back up camera configurations.**

   CIS Control 10: Data recovery capabilities

   The processes and tools used to properly back up critical information with a proven methodology for timely recovery of it.

Document and back up camera configuration. Update the documentation when service technicians change camera configurations.

If available, use an automated tool to back up camera configurations, such as Axis Device Manager. Other methods of backing up configuration data include:

a. Screen shots or photos of screens containing configuration data plus appropriate notes saved in a word processing document.

b. Typed configuration data and notes saved in a spreadsheet file.

c. Typed configuration data and notes in tool made for system design and documentation, such as System Surveyor.

Some camera configuration settings cannot be set or displayed within video management system software. This makes it important to document such settings independently of the surveillance system software.

Before performing camera firmware updates, obtain the backed-up device configuration information, or document the configuration before updating if current documentation can't be found. When updating, verify that camera configuration settings have not been changed the first time a different model of camera is updated. If the update changed the configurations, return them to their intended values and do the same for other similar cameras as they are updated.

4. **Use the latest camera firmware.**

   CIS Control 2: Inventory and Control of Software Assets

Apply camera firmware updates as they are released, following the manufacturer's instructions, and after testing the firmware update on at least one of each model of camera. Note that not all security-related updates may be identified as such in firmware release notes.

5. **Use strong camera passwords.**

   CIS Control 4: Controlled use of administrative privileges

   The processes and tools used to track/control/prevent/correct the use, assignment, and configuration of administrative privileges on computers, networks, and applications.

   Use strong passwords and keep them secure. When there are many camera passwords to track, use a secure password management software program to keep passwords accessible but still secure. For example, the Axis Device Manager software includes user password management for Axis cameras.

   See Appendix A, which contains password management advice based upon the new 2017 NIST password guidance, plus cautions about poor password practices that are commonly found in use with security video surveillance systems.

6. **Properly manage camera user accounts.**

   CIS Control 4: Controlled use of administrative privileges

   CIS Control 14 Controlled Access Based on the Need to Know

   The processes and tools used to track/control/prevent/correct secure access to critical assets (e.g., information, resources, systems) according to the formal determination of which persons, computers, and applications have a need and right to access these critical assets based on an approved classification.

   Ensure that when a new camera is configured, or an existing camera is reconfigured, default factory passwords have not been left in place. Also make sure that user privileges have been assigned consistent with the approved scheme for camera user account management. See Appendix A.

   If possible, use multi-factor authentication and encrypted channels for all administrative account access.

   Apply the following account management practices:

   a. *Disable anonymous or "guest" viewing of camera video.*

   b. *Set a strong primary account password.* Replace the factory default user account with a new username and strong password. Where possible, delete high level user accounts such as root, admin, service, supervisor and so on.

   c. *Set up dedicated user accounts for the video management system software.* This helps create important troubleshooting information, as the camera's device logs can help determine whether an individual or a surveillance system server accessed the camera, and when. Using an individual account for each camera caries the lowest risk but a higher management burden. Using the same account across all cameras carriers a much higher risk but does lower the management burden.

d. *Forbid service technician universal credentials.* Forbid human users to share logon credentials for accounts of any kind.

e. *Apply the principal of least privilege.* This principle requires giving a user account only those privileges that are essential for the user to perform his or her job. Even for small systems with a single user, the user should have two accounts: an administrative account reserved for infrequently performed administrative tasks, and an operator account with limited privileges appropriate for daily operations. Provide view-only privileges for users who have no need perform configuration changes.

f. *Require human video access via the surveillance system software, not via cameras.* Use the surveillance system software for operations access to camera video and audio. Don't allow direct network access to camera via a computer's web browser. The use of the surveillance system software for accessing camera configuration options, and a camera's web pages if needed, provides a system-level audit trail as well as a single point of user lock-out if needed.

g. *Don't reuse human camera logon credentials, such as for service personnel, within a video management system.* This weakens password management control.

7. Use the same time source, or set of synchronized time sources, for all cameras.[5]

CIS Control 5: Secure configuration for hardware and software on Mobile Devices, Laptops, Workstations and Servers

CIS Control 6: Maintenance, monitoring and analysis of audit logs

> Collect, manage, and analyze audit logs of events that could help detect, understand, or recover from an attack.

Logging and synchronized time stamps are typically underutilized in physical security systems. Timestamps are vital for investigation purposes and real-time incident response, for example, for tracking activity across multiple camera fields of view.

The CIS Controls documentation explains the cybersecurity reasons why CIS Control 6 is critical:

> Deficiencies in security logging and analysis allow attackers to hide their location, malicious software, and activities on victim machines. Even if the victims know that their systems have been compromised, without protected and complete logging records they are blind to the details of the attack and to subsequent actions taken by the attackers.

[5] CIS Sub-Control 6.1 recommends the use of three synchronized time sources: Use at least three synchronized time sources from which all servers and network devices retrieve time information on a regular basis so that timestamps in logs are consistent.

Without solid audit logs, an attack may go unnoticed indefinitely and the particular damages done may be irreversible.

Sometimes logging records are the only evidence of a successful attack. Many organizations keep audit records for compliance purposes, but attackers rely on the fact that such organizations rarely look at the audit logs, and they do not know that their systems have been compromised. Because of poor or nonexistent log analysis processes, attackers sometimes control victim machines for months or years without anyone in the target organization knowing, even though the evidence of the attack has been recorded in unexamined log files.

All camera, alarm, event system and operator activity must correlate to the same timeline, to have a forensic quality audit trail.

To maintain consistency across camera and recorder logs, configure the cameras for the same Network Time Protocol (NTP) server used by its surveillance system server. For each camera, manually initiate the initial retrieval from the time server. Ensure that time zones are correctly set. Ensure that the camera is configured to automatically update the time at an appropriate interval (such as hourly) using the time server.

Do not connect each camera to the Internet for time server access. Instead, use a small GPS NTP network time server device that does not require an outdoor antenna.

Ensure that other integrated systems, such as such as cash register or point-of-sale systems, use the same time server source.

8. **Disable camera audio not in use.**

CIS Control 9: Limitation and Control of Network Ports, Protocols, and Services

Manage (track/control/correct) the ongoing operational use of ports, protocols, and services on networked devices in order to minimize windows of vulnerability available to attackers.

Disable camera audio features that are not in use. Audio is enabled by default in most cameras that support it. There are privacy and regulatory considerations related to the use of audio. In some locales it is permissible to use audio for live monitoring, such as for alarm verification, but not for recording. In the U.S. check federal, state and local regulations before using camera audio.

9. **Disable unused protocols.**

CIS Control 9: Limitation and Control of Network Ports, Protocols, and Services

Disable the following functions and protocols if supported by the camera but not in use:

- FTP (File Transfer Protocol) Server
- IPv6 or IPv4 (whichever is not in use)

- Multicast
- Network discovery protocols: Bonjour, UPnP, and Zeroconf
- QoS (Quality of Service)
- SNMP (Simple Network Management Protocol) or use only SNMPv3, as the previous versions are not secure.
- SOCKS
- SSH (Secure Shell)

10. Encrypt camera edge storage.

CIS Control 13: Data protection

The processes and tools used to prevent data exfiltration, mitigate the effects of exfiltrated data, and ensure the privacy and integrity of sensitive information.

If camera SD Card capabilities will be used for recording purpose, enable the strongest level of encryption that the camera supports for SD card video storage. If an unauthorized individual removes the SD card, the encryption will prevent access to the recorded video.

If a local Network Attached Storage (NAS) device is used for recording, enable the strongest level of encryption supported, secure it in a locked area and ensure that the device's user accounts are properly configured.

11. Encrypt communication between the camera and the recording server.

CIS Control 13: Data protection

Establish an HTTPS connection between the cameras and the recording servers.

Ocularis Note: As of Ocularis 5.5, the streaming of audio and video is always from the camera to the recorder and is dependent upon camera capabilities. The streaming method that must be supported by the camera is "RTSP over RTP over HTTPS". Ocularis will use TLS 1.2 if supported by the camera.

Servers and Workstations

12. Document and back up server and dedicated workstation configurations.

CIS Control 10: Data recovery capability.

The processes and tools used to properly back up critical information with a proven methodology for timely recovery of it.

Document, and back up, server and workstation configuration information, and update it when service technicians change configurations. Perform complete system backups initially and at appropriate intervals. Ensure that backups are properly protected via physical security or encryption when they are stored, as well as when they are moved across the network. This includes remote backups and cloud services.

13. **Use strong computer and application logon passwords**

    CIS Control 4: Controlled use of administrative privileges

    Use a strong password and keep it secure. To reduce the risk of unauthorized access, do not write passwords down, for example, on a note affixed to the monitor or a slip of paper kept under the keyboard or in an unlocked drawer.

14. **Properly manage software user accounts.**

    CIS Control 4: Controlled use of administrative privileges

    CIS Control 14: Controlled Access Based on the Need to Know

    CIS Control 16: Account Monitoring and Control

    Actively manage the life cycle of system and application accounts - their creation, use, dormancy, deletion - in order to minimize opportunities for attackers to leverage them.

    Apply the principal of least privilege. Provide view-only privileges for users who have no need perform configuration changes.

    Even for small systems with a single user, the user should have two accounts: an administrative account reserved for infrequently performed administrative tasks, and an operator account with limited privileges appropriate for daily operations.

    For systems with multiple user accounts, set account expiration dates and prior to expiration, review the accounts to ensure that unneeded accounts are deleted, and that retained accounts have appropriate privileges based upon each account-holder’s current roles and job needs.

    Encrypt or hash with a salt all authentication credentials when stored. Ensure that all account usernames and authentication credentials are transmitted across networks using encrypted channels.

    Ocularis Note: For communication between Ocularis 5 recorders and Ocularis 5 client software:

    a. Encrypted transmission is enabled by default and cannot be switched off

    b. Passwords are always transmitted from the Ocularis Client to the Ocularis 5 Recorder as "salted SHA-512 hash"

15. Activate Lockout and Logout Features.

CIS Control 4: Controlled use of administrative privileges

Activate operating system and application lockout and logout features, as appropriate, to reduce the risk of unauthorized access to surveillance system capabilities.

16. Keep operating systems current regarding all security updates.

CIS Control 5: Secure Configuration for Hardware and Software on Mobile Devices, Laptops, Workstations and Servers

Ensure that operating system software is manually kept up to date with all security updates and relevant patches. Do not enable automatic operating system updates, as that could cause the operating system to reboot while video recording is still in progress.

17. Keep applications updated to their current versions.

CIS Control 18: Application Software Security

Manage the security life cycle of all in-house developed and acquired software in order to prevent, detect, and correct security weaknesses.

Ensure that application software is kept up to date, with all security updates and relevant patches. Before performing software updates, obtain the most recent software backup and verify it, or make a new backup of the software and its data.

Ocularis Note: As of version 5.2, Ocularis includes an Update Service that automatically checks online for patches and software application upgrades to recording system components and downloads them when available, with optional automatic installation. Details are provided in the Ocularis Installation and Licensing Guide.

Ocularis Note: StayCURRENT is OnSSI's program designed to keep Ocularis software up-to-date. See the Ocularis Administrator User Manual.

Ocularis Note: As of Ocularis 5.4, Client software may be updated at login when Ocularis detects that the connecting Client software is newer than the Base software it is connecting to.

18. Close all unused network ports, stop unused operating system services and protocols.

CIS Control 9: Limitation and control of network ports, protocols, and services

Stop unused operating system services and protocols. Unused application services and protocols such as FTP, IPv6, SSH, and Telnet can be turned off upon initial installation. Discovery services such as Bonjour, UPnP, and Zeroconf can be turned off after the cameras and other networked devices have been discovered and enrolled in the video surveillance system.

Disable these Windows services that the video surveillance system does not require:

- Application Host Helper
- Application Layer Gateway
- Application Management
- Bluetooth Support
- BranchCache
- Certificate Propagation (unless computer has a smart card reader)
- Computer Browser
- Distributed Link Tracking Client (may be required for some storage architectures)
- Function Discovery Provider Host
- Function Discovery Resource Publication
- Human Interface Device Access
- Hyper-V Data Exchange (unless running on virtual machine)
- Hyper-V Guest Shutdown (unless running on virtual machine)
- Internet Connection Sharing (ICS)
- Link-Layer Topology Discovery Mapper
- Offline Files
- Remote Access Auto Connection Manager
- Remote Access Connection Manager
- Routing and Remote Access (unless using IPSec or VPN tunneling)
- Shell Hardware Detection (used by Windows AutoPlay feature for removable storage)
- Special Administration Console Helper
- Simple Services Discovery Protocol (SSDP) (provides AutoPlay feature for removable storage devices)
- Web Services Dynamic Discovery Protocol (WS-Discovery)

Close all unused ports. Refer to the Port Lists in Appendix B for Ocularis port requirements. Ensure that all unused ports are closed, that all needed ports are open, and that any software firewalls have their port configurations appropriately set.

19. Use the same time source, or set of synchronized time sources, for all servers and workstations.

CIS Control 5: Secure Configuration for Hardware and Software on Mobile Devices, Laptops, Workstations and Servers

CIS Control 6: Maintenance, monitoring and analysis of audit logs

Do not connect each camera to the Internet for time server access. Instead, use a small GPS NTP network time server device that does not require an outdoor antenna.

20. Restrict Internet browser use.

CIS Control 7: Email and Web Browser Protections

Minimize the attack surface and the opportunities for attackers to manipulate human behavior though their interaction with web browsers and email systems.

CIS Control 9: Limitation and Control of Network Ports, Protocols, and Services

Disable or remove unneeded Internet browser features and plug-ins. Apply a host-based firewall default-deny rule that drops all traffic except those services and ports that are explicitly allowed.

21. Use antimalware software on servers and workstations.

CIS Control 8: Malware defenses

Control the installation, spread, and execution of malicious code at multiple points in the enterprise, while optimizing the use of automation to enable rapid updating of defense, data gathering, and corrective action.

Deploy antimalware software on all surveillance system servers and workstations, and set the software:

a. Not to scan file folders (directories) that contain video files and recording databases

b. Not to monitor the network ports used by the surveillance system

c. Not to monitor camera-to-recorder network traffic

22. Keep mobile devices that connect to the surveillance system updated.

CIS Control 5: Secure Configuration for Hardware and Software on Mobile Devices, Laptops, Workstations and Servers

Ensure that any mobile devices that connect to the surveillance system have the latest operating systems installed and are kept current with patches.

23. Back up and encrypt server and client configuration files.

CIS Control 5: Secure Configuration for Hardware and Software on Mobile Devices, Laptops, Workstations and Servers

CIS Control 10: Data recovery capability

CIS Control 13: Data protection

Back up server and client configuration files, using a password or other encryption key to encrypt the files.

Ocularis Note: The Ocularis 5 Recorder automatically backs up its recorder configuration database nightly, by default at 1:01 am. The default backup time and destination settings may be changed by Administration users.

24. **Encrypt streaming video between video recording servers and video viewing client software.**

    CIS Control 13: Data protection

    Encrypt streaming video to protect it from interception when transmitted for viewing in client software, web browser applications, or mobile device applications.

    Ocularis Note: Streaming video transmitted for viewing is encrypted when sent to the Ocularis 5 Client Software:

    a. *To Ocularis Client 5 software:* Video streams (including audio if present) are sent over TCP or UDP to the clients and to maximize video data throughput are protected via an OnSSI proprietary transmission protocol.

    b. *To Ocularis 5 Web and Mobile clients:* Video streams are sent over RTMP to the web and mobile clients and are not encrypted. A one-time RTSP-URL for the video stream is be generated and sent over an encrypted connection. Audio streams are not delivered.

25. **Encrypt stored video recordings.**

    CIS Control 13: Data protection

    Encrypt stored video recordings.

    Ocularis Note: To maximize video data throughput, the storage of video data in the Ocularis 5 database is encrypted in an OnSSI proprietary format.

26. **Encrypt and password protect exported video recordings.**

    CIS Control 13: Data protection

    Password-protected encryption protects the video data from unauthorized access, and at the same time provides a means to prove the protected file contains the original unaltered video data.

    Ocularis Note: Exported video files are encrypted using 128-bit or 256-bit AES (Advanced Encryption Standard) encryption in Ocularis version 4.0 and later.

Network

27. Establish a network configuration that isolates the camera LAN.

CIS Control 11: Secure Configurations for Network Devices such as Firewalls, Routers, and Switches

CIS Control 12: Boundary Defense

Detect/prevent/correct the flow of information transferring networks of different trust levels with a focus on security-damaging data.

Establish a closed camera LAN. Configure firewall settings to ensure that cameras can only connect with their recording server, and that no outside connections can be made to the cameras.

Service Agreement

28. Establish an appropriate technical service response capability.

CIS Control 19: Incident Response and Management

Protect the organization's information, as well as its reputation, by developing and implementing an incident response infrastructure (e.g., plans, defined roles, training, communications, management oversight) for quickly discovering an attack and then effectively containing the damage, eradicating the attacker's presence, and restoring the integrity of the network and systems.

Establish an appropriate service response capability. Ensure that the servicing security integrator has appropriately IT-trained service personnel, and that the service contract terms establish an acceptable level of qualified response, including an appropriate response-time requirement in the event of a cyber-related problem.

Advanced Security Profile

Connecting a surveillance system to a business WAN or to the Internet exposes the surveillance system to potential threats. Apply the appropriate Basic Security Profile recommendations, and also apply the Advanced Security Profile recommendations listed below.

Cameras

29. Enable IP address filtering.

CIS Control 1: Inventory and Control of Hardware Assets.

CIS Control 12: Boundary defense

CIS Control 14: Controlled access based on the need to know

Set up IP address filtering (IP tables) only for authorized connections to prevent the cameras from responding to network traffic from any non-surveillance system software or devices.

30. Establish a VLAN configuration that isolates the camera LAN.

CIS Control 11: Secure Configurations for Network Devices such as Firewalls, Routers, and Switches

CIS Control 12: Boundary Defense

Where camera network traffic must travel over segments of a corporate network, segregate the camera network traffic using a VLAN (virtual LAN). Use network switch MAC binding and VLAN configuration to limit where video network traffic can go.

Servers and Workstations

31. Establish HTTP digest authentication or enable HTTPS.

CIS Control 5: Secure Configuration for Hardware and Software on Mobile Devices, Laptops, Workstations and Servers

CIS Control 13: Data Protection

To ensure login passwords are not sent in clear text over the network, use digest authentication (encrypted passwords) or HTTPS connections (see the following recommendation), to prevent surveillance system client software from sending

32. Enable HTTPS connections between Servers and Workstation/Mobile Clients.

CIS Control 5: Secure Configuration for Hardware and Software on Mobile Devices, Laptops, Workstations and Servers

CIS Control 13: Data Protection

Configure servers for HTTPS connections between servers and client applications on workstations and mobile devices. Follow the setup instructions for installing digital certificates and enabling HTTPS connections using TLS.

Ocularis Note: For communication between Ocularis 5 recorders and Ocularis 5 client software, encrypted transmission is enabled by default and cannot be switched off.

Network

33. Use device whitelisting, if it is the organization's standard network practice.

CIS Control 2: Inventory of Hardware Assets

CIS Control 12: Boundary defense

CIS Control 14: Controlled access based on the need to know

Use router and/or firewall device whitelisting to authenticate surveillance system equipment and connecting devices.

34. Adjust WAN network configuration as required.

CIS Control 9: Limitation and control of network ports, protocols, and services

If a surveillance system software client or web client is to be used over the WAN connection, ensure that the required ports are open on the WAN network path.

Enterprise Security Profile

Apply the Basic Security Profile and Advanced Security Profile recommendations, updating and adding to them based upon the recommendations that follow below. In applying the recommendations, collaborate with your organization's in-house or outsourced IT function.

The suitability or ease of applying specific recommendations may depend upon whether the related control technology is already in use by the organization. It can be very helpful to utilize a chart or spreadsheet that maps the CIS Controls to the controls provided in the organization's information security management framework, such as NIST 800-53, PCI DSS 3.1, ISO 27002, CSA, and HIPAA.

At the time this guide was written, CIS had not yet published a mapping reference for the Version 7 controls. However, due to the high similarity between Versions 6 and 7, the poster that provides Mappings of the CIS Controls Version 6.0 to various other frameworks is a very helpful reference.

Infrastructure Management

Managed enterprise network environments typically have cybersecurity controls in place, which is a benefit to any video surveillance system connected to the enterprise network. Such networks typically have additional management tools and services that cameras, servers, workstations, laptops and mobile devices may need to be configured for.

In most enterprise environments the organization's IT department will provide specific information to enable the video surveillance system and its local networks to participate according to the overall IT plan and the management infrastructure in place. Additionally, there will likely be firewall, router and switch configurations required to support the video surveillance system. Thus, collaboration with IT is usually required to establish the secure viewing of surveillance video across the corporate network and/or for camera streams to traverse the corporate network.

Cameras

35. Use the corporate NTP time sources for cameras.

    CIS Control 5: Secure Configuration for Hardware and Software on Mobile Devices, Laptops, Workstations and Servers

    CIS Control 6: Maintenance, monitoring and analysis of audit logs

    Configure each camera to use the Network Time Protocol (NTP) server that the corporate network uses.

36. Establish camera participation in IEEE 802.1X network access control.

    CIS Control 2: Inventory of Hardware Assets

    CIS Control 12: Boundary defense

    Set up the cameras for IEEE 802.1X network access control. For example, to participate in a network infrastructure where a Radius server is used, cameras need to have appropriate certificates and specific configuration settings. To a Radius server a surveillance camera would appear as a web server. Apply camera manufacturer instructions according to information provided by IT. Where available, utilize automated password generation provided by the Radius server or similar technology.

37. Set up SNMP Monitoring.

    CIS Control 6: Maintenance, monitoring, and analysis of audit logs

    Obtain appropriate camera MIB (Management Information Base) files from the sources designated by camera manufacturers. Examine the camera manufacturer's documentation to determine which camera events should be monitored.

38. Set up Remote System Log monitoring.

    CIS Control 3: Continuous Vulnerability Management

    CIS Control 6: Maintenance, monitoring, and analysis of audit logs

    CIS Control 16: Account monitoring and control

    CIS Control 19: Incident response and management

    Set up cameras to generate syslog messages, to the established syslog server. A syslog server collects the log messages generated by the devices being monitored. Collection of log messages simplifies audits and prevents log messages from being destroyed in the camera maliciously or unintentionally (for example, by a camera reboot, by an overwrite caused by the maximum log size being reached, or by human error during service). Follow camera manufacturer instructions for enabling syslog messaging.

39. Establish and monitor a digital inventory of servers, workstations, cameras and network equipment.

    CIS Control 2: Inventory of Hardware Assets

    CIS Control 3: Continuous Vulnerability Management

    CIS Control 6: Maintenance, monitoring, and analysis of audit logs

    CIS Control 19: Incident response and management

    Use standard IT infrastructure open source and/or commercial monitoring tools to discover and monitor authorized and unauthorized devices. Enroll the video surveillance system in the IT department's IT infrastructure management program.

Servers and Workstations

40. Use the corporate NTP time server for servers and workstations.

    CIS Control 5: Secure Configuration for Hardware and Software on Mobile Devices, Laptops, Workstations and Servers

    CIS Control 6: Maintenance, monitoring and analysis of audit logs

    Configure each server and workstation to use the Network Time Protocol (NTP) server that the corporate network uses.

41. Establish server and workstation participation in IEEE 802.1X network access control.

    CIS Control 2: Inventory of Hardware Assets

    CIS Control 12: Boundary defense

    Set up servers and workstations for IEEE 802.1X network access control, following Microsoft's instructions for installing the needed certificates and enabling the required authentication method per the information provided by the organization's IT department.

42. Set up SNMP Monitoring.

    CIS Control 6: Maintenance, monitoring, and analysis of audit logs

    Establish appropriate SNMP monitoring for servers and dedicated workstations.

    Ocularis Note: Utilize the Ocularis alerting features to provide on-screen, audio, mobile device, email and SNMP events for important system events. See the Ocularis Installation and Licensing Guide, and the Ocularis 5 Recorder Proxy Configuration Guide.

43. Set up for Remote System Log monitoring.

    CIS Control 3: Continuous Vulnerability Management

    CIS Control 6: Maintenance, monitoring, and analysis of audit logs

    CIS Control 16: Account monitoring and control

    CIS Control 19: Incident response and management

Set up servers and dedicated workstations to generate syslog messages. Utilize an available enterprise syslog server or establish a dedicated server for video surveillance systems computers and devices. A syslog server collects the log messages generated by the devices being monitored. Ocularis servers require a syslog agent to be installed in Windows.

Network

44. Configure video system LANS for WAN/Internet connectivity per corporate networking requirements

    CIS Control 2: Inventory of Hardware Assets

    CIS Control 5: Secure Configuration for Hardware and Software on Mobile Devices, Laptops, Workstations and Servers

    CIS Control 12: Boundary defense

    CIS Control 13: Data Protection

    CIS Control 14: Controlled access based on the need to know

    Obtain the corporate networking requirements that apply to LANS and to WAN/Internet connectivity. They may, for example, require that a particular antivirus application be used, or that switches and routers have specific configurations applied.

45. Provide corporate IT with network firewall, switch and router configuration requirements for security video

    CIS Control 2: Inventory of Hardware Assets

    CIS Control 12: Boundary defense

    CIS Control 14: Controlled access based on the need to know

    Provide firewall, switch and router port and protocol configuration requirements. Refer to the port lists in Appendix B for Ocularis port requirements. Ensure that all unused ports are closed, and that all needed ports are open, and that any software firewalls have their port configurations appropriately set.

Data Governance Frameworks

There may be a data governance program in place for corporate confidential, critical and privacy-restricted data, with some regulatory requirements involved. Surveillance video and audio information may become part of an investigation into an employee, contractor or visitor misconduct incident or criminal offense, and may have specific handling required due to privacy or regulatory requirements. Security video surveillance systems may need to be included into an overall computer and network acceptable use policy, or a specific acceptable use policy may need to be developed for security video surveillance systems.

46. Establish appropriate participation in the corporate data governance framework.

    CIS Control 13: Data Protection

    CIS Control 14: Controlled access based on the need to know

    Apply the appropriate the appropriate data governance policies to the management of security video and the video management system, including roles and technology measures.

    Some example privacy restrictions may include:

- Do not record video or audio of indoor and outdoor union or other types of meetings.
- Obscure the faces of union or other meeting attendees using video analytics technology.
- Obscure faces in exported video unless facial images are required for forensic purposes.
- Exclude audio from exported video unless required for forensic purposes.
- Designate an individual to be the data steward for the security surveillance video.
- Establish a published acceptable use policy for video surveillance data.
- See that servers and workstations appropriately participate in automated security controls, such as those that log the use of use of USB memory devices and CD/DVD drives, and automatically disable such devices except for authorized users.
- Create privacy masks for areas of video camera scenes that contain work areas where employees have a concern about personal privacy, and this can be done without compromising security concerns.

Ocularis Note: See the Privacy Mask section in the Ocularis Administrator User Manual for more information about configuring privacy masks.

General Guidance

Prioritization

> "Invest first in Controls that will provide the greatest risk reduction and protection against the most dangerous threat actors and that can be feasibly implemented in your computing environment."[6]

Apply Updates Promptly

After testing camera firmware updates when they are released, updates should be applied as quickly as possible, even if no security vulnerability is included in the release notes. This is because manufacturer's release notes do not always include every security related fix. Sometimes bugs can create security vulnerabilities, but the bug fix comments in the release notes don't always mention the security impact. Even if your system and devices do not appear to be affected by such a bug, an attacker may still be able to exploit the bug if the system and devices are not updated. The Ocularis software will update itself with patches as soon as the patches are delivered to the server.

Physical Security Protection

Video surveillance system equipment must be protected against physical sabotage, vandalism and tampering. Servers must be placed in properly air-conditioned access-controlled rooms, making it difficult for unauthorized individuals to access servers, network cables and power cables. Cameras should be installed using security screws (or have existing standard screws replaced). Vandal-resistant camera models or camera housings should be used as appropriate. Cable protection should be provided for outdoor or physically accessible indoor cameras, such as flexible steel conduit. The camera network ports and power connections must be kept secure.

Collaboration with IT

For organizations that have an IT department, there are usually several important points of cybersecurity collaboration relating to security video surveillance systems deployments, including the *information security triad* perspectives of *confidentiality*, *integrity* and *availability.* Example collaboration topics are:

- Computing and networking requirements for connecting a security video LAN to a business LAN, including the isolation of cameras from outside cybersecurity threats

[6] "CIS Controls – Version 7", page 5.

- Video Surveillance LAN design
- High availability computer and networking requirements for security video, including for network path redundancy
- Computer and network acceptable use policies
- System server and network monitoring
- Integration for system user authentication via the organization's existing identity and access management system
- Automated backups for servers and dedicated workstation configurations
- Aligning hardening guide recommendations with IT policies and practices, such as antivirus software and server/workstation configuration standards
- Enterprise encryption policies and requirements
- Digital certificate administration and issuance
- Service level terms for support from IT and from the system integrator, and how the two will collaborate when needed on service and maintenance
- Classification of video surveillance system data according to IT data classification policies
- Video surveillance system computer and network risk assessments
- Automated monitoring of video surveillance system cameras, computer and network devices

Collaboration with HR

The confidentiality perspective has a data privacy component, which may include regulatory requirements. Thus, for organizations that have a Human Resources or Talent Management function, there are also these points of collaboration:

- Video acceptable use policy for live and recorded video
- Camera location policy relative to privacy expectations and regulations
- Appropriate periodic training regarding the correct use of video systems and video data for security and non-security personnel
- Integration for system user authentication via the organization's existing identity and access management system

Collaboration with Legal and Corporate Governance

- Retention periods for recorded surveillance video and audio
- Video acceptable use policy for live and recorded video

- Camera location policy relative to privacy expectations and regulations
- Classification of video surveillance system data according to IT data classification policies
- Video surveillance system computer and network risk assessments
- Integration for system user authentication via the organization's existing identity and access management system

Additional Ocularis Data Security Information

For additional information on Ocularis data security see:

- February 2018 OnSSI White Paper titled, "Video Data Security"
- April 2018 document titled, "Ocularis 5 Encryption"

Appendix A – 21st Century Password Guidance

The misuse of administrative privileges is a primary method for attackers to gain access to networks and computers, spread malware inside a target network, and steal data from computers and devices. Another common technique used by attackers is elevation of privileges by guessing or cracking a password for an administrative user to gain access to a target machine or device. This is why the National Institute for Standards and Technology issued new password rules guidance in mid-2017, because research showed that previous password practices have not been as effective as originally expected. Human memory limitations that have led users to respond in very predictable ways to the requirements imposed by password composition rules. Advances in computing technology have improved the capabilities of attackers, who use common and easily-guessable password dictionaries as well as brute force attacks (trying many letter and number password combinations).

Password Length

"Password length has been found to be a primary factor in characterizing password strength. Passwords that are too short yield to brute force attacks as well as to dictionary attacks using words and commonly chosen passwords." [7]

Per the new NIST guidance, "Users should be encouraged to make their passwords as lengthy as they want, within reason . . . there is no reason not to permit the use of lengthy passwords (or pass phrases) if the user wishes."[8]

Thus, a phrase of seemingly random words that can be easily remembered makes for a hard-to-guess password, especially when the user can relate it to something visual or to an experience. For example, a good example of such a password (but now a non-usable because it's published) is: "tall buildings can make long shadows" typed without spaces (tallbuildingscanmakelongshadows). This is the maximum size password that can be used in Ocularis 5 Base (31 characters), and is a better password than those resulting from previous password rules regarding combinations of numbers, letters and special characters.

Password Guidance

The password guidance below is based upon the NIST guidance, as well as other recent password research and best practices.

- **Use Strong but easily recallable passwords.** Use an easily remembered lengthy password that's not a common sentence or phrase.

[7] Paul Grassi, James Fenton, et al., SP 800-63B, Digital Identity Guidelines, "Authentication and Lifecycle Management", National Institute of Standards & Technology, Gaithersburg, MD, 2006, p.67.

[8] Ibid., p. 68.

- **Activate lockout and logout features.**
  - **Invalid Logon Attempts.** Utilize an account lockout feature that helps defeat password guessing attacks by locking the user account after a certain number of incorrect name/password logon attempts have occurred. Require either a password reset or an administrator unlock (this is called *account lockout*), or prevent additional logon attempts until a specified time period has elapsed (called *throttling*).
  - **Automatic Logouts.** Lower the risk of unauthorized use of unattended workstations by automatically log users out after a specified period of user inactivity, or use a screen saver lock to require re-authentication. To prevent users who are at their workstations from needlessly having to reauthenticate due to inactivity, prompt users with a warning to trigger activity several minutes before an inactivity timeout would otherwise occur.
- **Use One-Time Passwords (OTP).** Utilize a system or device that generates an OTP to be presented for completion of the logon sequence. Allow at least 10 entry attempts for entry of the OTP because the longer and more complex the entry text, the greater the likelihood will be of user entry errors.
- **Use multi-factor authentication.** In addition to username and password, use multi-factor authentication, such as a fingerprint or other type of biometric scanning.
- **No hints or security questions.** Do not permit the use of a password "hint" feature or security questions, such as: "What was the name of your first pet?"
- **Use a secure password manager.** Do not permit the use of browser password storage. Turn off form autofill if the password manager application supports it; autofill is an exploitable weakness.

Avoiding Surveillance System Bad Password Practices

There are two common risky service practices that should be forbidden:

- Service technician *universal logon credentials*
- Service technician *shared logon credentials*

Forbid both practices by specific instruction as well as by service contract terms.

"Service technician *universal logon credentials*" refers to the practice of integrator service technicians using the same personal logon credentials (name and password) across all customer accounts that the technician services. This creates the risk of credentials leakage to personnel at other organizations (some of whom may be competitors), which is a magnified risk if the passwords are not strong.

*"*Service technician *shared logon credentials"* refers to the practice of using common logon credentials (name and password) that all the service technicians of a single customer share. This makes it impossible to verify which technician accessed a camera or system and performed certain actions, because all technicians use the same logon credentials.

Appendix B – Ocularis Network Ports

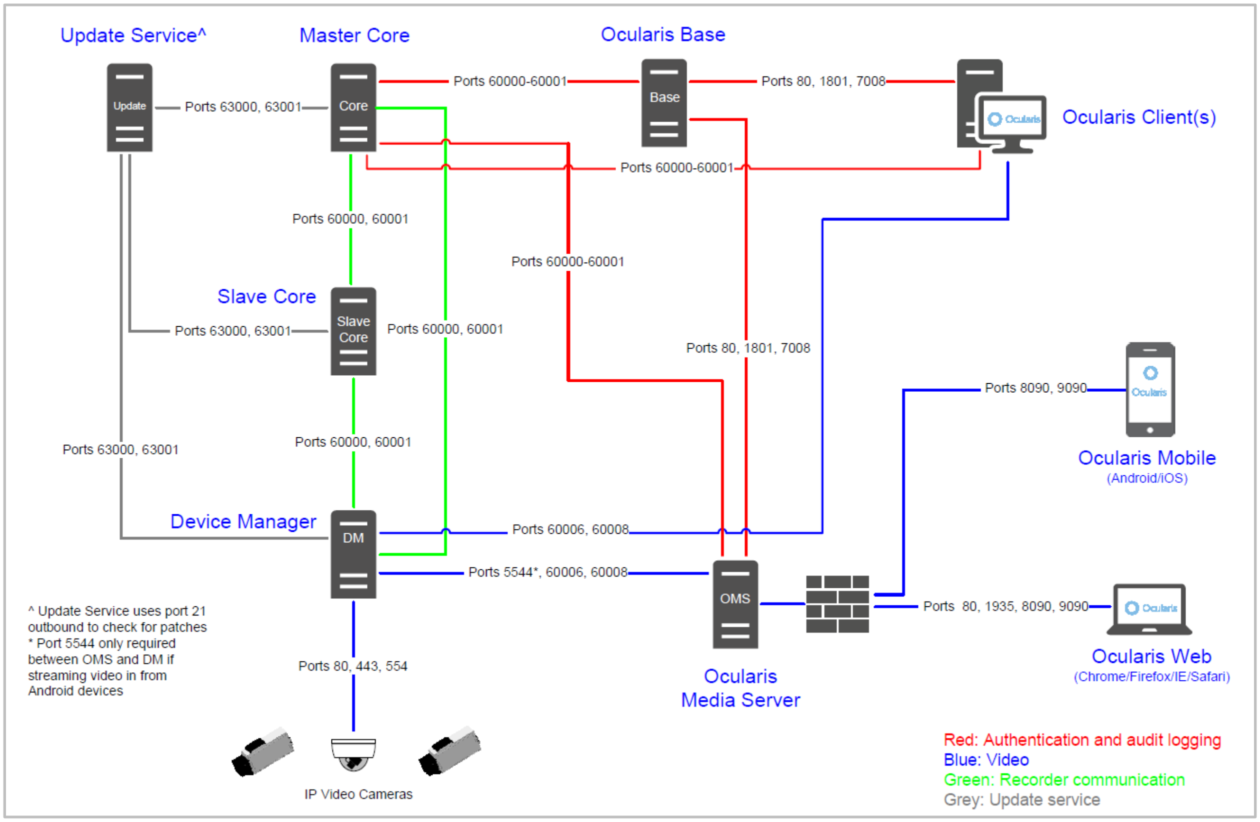
The ports listed below should be open for network data traffic when using Ocularis. *See the Ocularis Installation and Licensing Guide for additional details.*

Table 1. Ocularis Server Network Ports

Port Number (inbound and outbound)	Description
20 and 21	Used when devices use FTP for sending event messages. FTP (File Transfer Protocol) is a standard for exchanging files across networks.
25	Used when recording servers listen for SMTP information. Also, some devices use SMTP (e-mail) for sending event messages and /or for sending images to the surveillance system server via e-mail. SMTP (Simple Mail Transfer Protocol) is a standard for sending e-mail messages between servers.
80	Port 80 is typically used by the IIS (Internet Information Services) for Ocularis and Ocularis Media Server's HTTP website.
443	Port used by IIS to host the Ocularis Media Server's HTTPS website.
554	Used by some camera manufacturers.
1024 and above (outbound only)	**(Except ports listed below):** Used for HTTP traffic between cameras and servers.
1801	Used for Message Queuing.
1935	Used by Ocularis Web when connecting to Ocularis Media Server via RMTP. This is the default setting.
5432	Used when recording servers listen for alert socket/TCP information; some devices use TCP for sending event messages.
5544	Open this port on all Device Managers (DMs).
7008	Used by Ocularis.net (communication with video walls and push video).
7210	Internal port (MaxDB) - Do not open this port in your Firewall.
7563	Used for handling PTZ camera control commands and for communication with Ocularis Client.
8090	Used by HTTP.
8500 – 8600	Dynamic ports used for streaming video from Ocularis Media Server to Ocularis Mobile.
9000	Used by mobile devices to connect to the Ocularis Media Server.
9090	Used by SSL.
9100	RTSP Port.
60000 – 60008 (inbound and outbound)	Recorder Core/DM/MDS.
60021	SIP/VOIP.
63000 – 63001	Update Service.
64222	AV Export.
60601 – 60724	LPR/Analytics/Transcoding Engine.
Other port numbers you may have selected to use or are required by cameras.	Examples: If you have changed the IIS Default Web Site port from its default port number (80) to another port number.

Also see Figure 1 below, Ocularis Communication Flow, which contains identified port usage.

Figure 1. Ocularis Communication Flow



^ Update Service uses port 21 outbound to check for patches
* Port 5544 only required between OMS and DM if streaming video in from Android devices

Appendix C – Ocularis Product Information References

Recommendations for which there is relevant material in OnSSI product manuals and webinar tutorials are listed below, followed by the product manual or tutorial references.

Recommendation Items

The numbered recommendations below refer to the recommendations provided in the Security Profiles section of this document. Only recommendations that have related instructions or guidance in OnSSI documentation are listed below.

13. Use strong computer and application logon passwords.
14. Properly manage software user accounts.

- Apply password guidance for each step involving password creation and management actions in the following installation and configuration instructions:
    - Ocularis Administrator User Manual
    - Ocularis Installation and Licensing Guide
    - Ocularis Recorder Configuration Manual
    - C•CURE 9000 - Ocularis Installation & Configuration Guide
    - Ocularis Mobile User Guide
    - Technical Notes for Ocularis 5.5, Increased Security with Ocularis Recorder Proxy
    - Using NAT with Ocularis 5
- Apply password guidance for password creation and management actions in the following user manuals:
    - Ocularis Administrator User Manual
    - Ocularis Client User Manual
    - Ocularis 5 Upgrade Manual
- For more information on user account configuration, see:
    - Technical Training Webinar #4: Users, Privileges & Views
    - Technical Training Webinar #17: Ocularis 5 Multiple Administrator Accounts

Note: Although several Ocularis guides and manuals contain the earlier NIST password guidance, the 21st century password guidance provided in Appendix A can still be applied, up to a maximum password length of 31 characters on Ocularis Base and 256 characters on Ocularis Recorder.

16. Keep operating systems current regarding all security updates.

- For recommendations regarding operating system updates, see:
    - Best Practices with Ocularis 5

17. Keep applications updated to their current versions.

- For information about the Ocularis automatic update feature and OnSSI's StayCURRENT software updates program, see:
  - Ocularis Administrator User Manual
- For Client software automatic updates upon login, see:
  - Ocularis 5 Administrator Manual, Update Settings
  - Ocularis 5 Client User Manual, Automatic Update of Ocularis Client Software
- For Update Server configuration, see:
  - Best Practices Technical Training Webinar #27, at approximately 55:26

18. Close all unused network ports, stop unused operating system services and protocols.

- In addition to this document's Appendix B, check the network port usage information in the latest versions of following documents:
  - Ocularis Installation and Licensing Guide
  - Ocularis 5 Port Diagram (or later version-specific document)

23. Back up and encrypt server and client configuration files.

- For Recorder automatic backup configuration, see:
  - Ocularis 5 Recorder Configuration Manual, Configuring the backup
- For additional discussion on Recorder backup configuration, see:
  - Technical Training Webinar #27, Ocularis 5 Best Practices, at 58:52
- For discussion of the Ocularis Configuration Export Tool, see:
  - Technical Training Webinar #25, Efficiently Adding Cameras to Ocularis 5, at 54:14
  - Technical Training Webinar #27, Ocularis 5 Best Practices at 1:00:21

28. Establish an appropriate technical service response capability.

- This applies to cameras. See the following document:
  - Ocularis Installation and Licensing Guide, Ocularis Media Server, HTTP vs. HTTPS

About OnSSI

On-Net Surveillance Systems' (OnSSI) was founded in 2002 with the goal of developing comprehensive and intelligent IP video surveillance management software. By applying the same principles of voice-over IP to transfer huge amounts of data over IP lines, founders Gadi Piran and Mulli Diamant had a hand in revolutionizing video delivery. The result of their R&D work has propelled the IP surveillance system industry and placed OnSSI as a leader in physical security information management. With its worldwide headquarters in Pearl River, New York and its European headquarters in Bruchsal, Germany, plus representation in over 100 countries around the globe, OnSSI is committed to powering your surveillance system so you can truly stay one step ahead.

OnSSI's award-winning IP-based surveillance software, Ocularis, addresses complex, multi-server installations, as well as single installations. The flexibility and functionality of Ocularis suits a range of applications in education, gaming, government, healthcare, manufacturing, public safety, transportation, and utilities. With a company mission to increase security, reduce operating costs, and get operators closer to prevention, OnSSI is raising safety standards around the globe.

For more information about this document or OnSSI, email info@onssi.com.

On-Net Surveillance Systems, Inc.
One Blue Hill Plaza, 7th Floor
PO Box 1555
Pearl River, NY 10965

Tel: 845.732.7900
Web: https://onssi.com/