

---

# **VIDEO SURVEILLANCE SYSTEMS HARDENING GUIDE**

Cyber Security Measures for Deployed Video Surveillance Systems

Version 1.0

Salient Systems Corp.  
4616 W. Howard Lane  
Building 1, Suite 100  
Austin, TX 78728

## ***Table of Contents***

Video Surveillance Systems Hardening Guide .....	1
Introduction .....	1
Hardening.....	1
Effective Cyber Defense.....	1
Applying the CIS Critical Security Controls.....	2
This Guide .....	2
General Guidance .....	2
Applying Software and Firmware Security Updates .....	2
Password Management .....	3
Password Length.....	3
Password Guidance.....	3
Avoiding Security System Bad Password Practices.....	4
Physical Security Protection.....	4
Collaboration with IT.....	5
Collaboration with HR .....	5
Cyber Security Profiles .....	5
Basic Security .....	6
Cameras .....	6
Servers and Workstations.....	9
Network .....	12
Service Agreement.....	12
Advanced Security.....	12
Cameras .....	12
Servers and Workstations.....	13
Network .....	13
Enterprise Security.....	13
Infrastructure Management .....	14
Cameras .....	14
Servers and Workstations.....	15
Network .....	16
Data Governance Frameworks .....	17
Critical Infrastructure and Government Security.....	17
Standards and Regulatory Requirements.....	17
Appendix A – CompleteView Network Ports .....	19
Server Network Ports.....	19
Camera Network Ports.....	19
Appendix B – CompleteView Product Manual References.....	20

Product Manual References.....	20
Recommendation Items.....	20
Appendix C – Factory Configurations for Services, Ports and Protocols.....	22
Hardening Configuration Items.....	22
ABOUT SALIENT SYSTEMS .....	24

## ***Video Surveillance Systems Hardening Guide***

### ***Introduction***

This document provides guidance for system end users, system integrators, and security design consultants about establishing a sensible *cyber security* profile for their deployed Salient Systems security video management system products. Cyber security, also known as computer and network security or IT security, is defined as “the protection of computer systems from theft and damage to their hardware, software or information, as well as from disruption or misdirection of the services they provide.”<sup>1</sup>

### ***Hardening***

*System hardening* is a computer security term for developing and applying cyber security measures to a networked computer system, to protect it against attack from potential threats. There are several categories of computing and network technologies involved in security video surveillance deployments:

- Network cameras and network encoders for analog cameras
- Servers, workstations and mobile devices
- Computer software and device firmware
- Networking and the Internet
- Video encoding
- Data encryption
- Computer and network security

In each of these areas technology is continually advancing. Thus, every aspect of security video surveillance technology is evolving. Additionally, cyber security threats to networked computer systems continue to evolve, including malware such as [BASHLITE](#) and [Mirai](#), which primarily targeted networked security cameras and video recording servers and appliances. *Therefore, hardening a computer system is an ongoing process rather than a one-time action.* The full scope of system hardening involves a combination of appropriate people, process and technology security measures. 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.

### ***Effective Cyber Defense***

Working together, the [SANS Institute](#) and the [Center for Internet Security](#) (CIS) have taken the best-in-class cyber threat data and transformed it into actionable guidance, called the [CIS Critical Security Controls for Effective Cyber Defense](#), popularly known as the SANS Top 20. These recommended security controls also serve as the foundation for many regulations & compliance frameworks, including NIST 800-53, PCI DSS 3.1, ISO 27002, CSA, HIPAA, and others.

A principal benefit of the Critical Security Controls is that they prioritize and focus a smaller number of actions with high pay-off results. The Controls are updated based on new attacks that are identified and

---

<sup>1</sup> Wikipedia contributors. "Computer security." Wikipedia, The Free Encyclopedia. Web. 4 Dec. 2017.

analyzed by leading security research firms, to assure that the Controls continue to stop or mitigate cyberattacks.

## Applying the CIS Critical Security Controls

Based on the Critical Security Controls, this guide presents four *cyber security profiles*, which are sets of recommended actions 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 deployments on a dedicated (i.e. 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 that is maintained by IT Service Management (ITSM) practices within a corporate data governance framework.
- **Critical Infrastructure and Government:** Enterprise scale deployment environments that also have regulatory and/or government cyber security requirements to comply with.

## This Guide

This guide provides hardening recommendations that are applicable for most security video management systems, and are specifically intended to be applicable to these Salient Systems products:

- **VMS Software:** CompleteView Enterprise, CompleteView Professional, CompleteView ONE
- **Servers:** RED3 and eXtreme8 models
- **NVRs:** PowerChoice, PowerMicro, PowerPlus, PowerPro, and PowerUltra models
- **Workstations:** Guardstation models

The main body of this document contains the hardening recommendations. *Appendix A* contains the Salient Systems network port usage lists. *Appendix B* contains references to sections in Salient Systems product manuals that refer to specific hardening recommendations. *Appendix C* contains tables of factory-configured Windows service, port and protocol configurations for servers and NVRs.

In this guide, “camera” refers to an “IP camera” (also known as a “digital video camera” or a “network camera”) or to an analog camera connected to the VMS via a network video encoder. Video encoders give analog cameras an IP address and provide additional functionality typically found in IP cameras.

## General Guidance

### Applying Software and Firmware Security Updates

When a software or hardware security vulnerability is discovered, vendors will release software or firmware updates to fix the vulnerability (updates are sometimes called “fixes”) and issue a security advisory notice. If the update cannot be developed quickly enough, the vendor may issue a security advisory containing a workaround or protective steps to take, until the update can be released.

It is generally a good practice to apply software and firmware updates when they are released, whether a security vulnerability is included in the release notes or not, for two reasons. *First, release notes do not always include every security related fix.* Release notes from some manufacturers mention only critical security vulnerabilities and do not mention less critical vulnerabilities that are fixed in the update. *Second, sometimes bugs can create security vulnerabilities, but the bug fix comments in the release notes don't mention the security impact.* Even if your use of a system or device does not appear to be affected by such a bug, an attacker may still be able to exploit the bug if the system or device is not updated.

## Password Management

The National Institute for Standards and Technology issued [new password rules guidance](#) in mid-2017, due to research that shows previous password practices have not been as effective as originally expected. This is partly due to advancing technology and the growth of automated cyberattacks on systems and devices, but is also due to human memory limitations that have led users to respond in very predictable ways to the requirements imposed by password composition rules.

### 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.”<sup>2</sup>

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, “green tile trip again cement” typed without spaces (greentiletripagaincement) makes a better password than those resulting from previous password recommendations. According to 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.”<sup>3</sup>

### Password Guidance

Apply the password guidance below, which is based upon the NIST guidance and other recent password research, along with the additional protective measures listed in the Cyber Security Profiles.

- **Use Strong but easily recallable passwords.** Use an easily remembered lengthy password that’s not a common sentence or phrase.
- **Activate lockout and logout features.**
  - **Invalid Logon Attempts.** Defeat password guessing attacks by enabling a feature that, after a certain number of incorrect name/password logon attempts have occurred, locks

---

<sup>2</sup> 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.

<sup>3</sup> Ibid., p. 68.

the user account, and either requires a password reset or administrator unlock (this is called *account lockout*), or prevents additional logon attempts until a specified time period elapses (called *throttling*).

- **Automatic Logouts.** To lower the risk of unauthorized use of unattended workstations, 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 actually are at their workstations from needlessly having to reauthenticate due to inactivity, prompt users with a warning to trigger activity just before (e.g., 2 minutes) an inactivity timeout would otherwise occur.
- **Use One-Time Passwords (OTP).** In addition to username and password, 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; the longer and more complex the entry text, the greater the likelihood 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 (e.g. “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 Security 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.

### **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. 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 cyber security collaboration relating to security video surveillance systems deployment, including the *information security triad* perspectives of *confidentiality*, *integrity* and *availability*. Example topics are:

- Computing and networking requirements for connecting a security video LAN to a business LAN, including the isolation of cameras from outside cyber security threats
- 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
- Service level terms for support from IT and from the system integrator, and how the two will collaborate when needed on service and maintenance

### **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

### **Cyber Security Profiles**

Note that each numbered security profile recommendation is followed by a listing that identifies each Critical Security Control (CSC) category that applies to the recommendation. Almost half of the security profile recommendations fit into a single Critical Security Control (CSC) category, the remainder apply to two or more categories.



## Basic Security

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

### Cameras

#### 1. Begin camera configuration from a known factory default state.

CSC #3: Secure configuration for hardware and software

*Before starting camera configuration, make sure that the camera is in a known factory default state. If you are unsure of the state, follow the manufacturer's instructions to return the camera to its factory default state.*

#### 2. Document and back up camera configurations.

CSC #10: Data recovery capability

*Document and back up camera configuration information, and update it when service technicians change camera configurations. Camera configuration data can be captured and backed up in several ways: (1) place screen shots or photos of screens containing configuration data plus appropriate notes in a Microsoft® Word® document, (2) type configuration data into a Microsoft Excel® spreadsheet file, or (3) use a commercial tool for system documentation, such as [System Surveyor](#).*

Not all camera configuration settings can be set or displayed within VMS software, such as PTZ presets. This makes it important to document the settings independently of the VMS. The more cameras there are in a security surveillance system, the more likely there are to be common camera configurations for certain camera makes and models.

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

#### 3. Use the latest camera firmware.

CSC #2: Inventory of authorized and unauthorized software

*Apply camera firmware updates as they are released, following the manufacturer's instructions.*

#### 4. Use strong camera passwords.

CSC #5: Controlled use of administrative privileges

*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.

## **5. Properly manage camera user accounts.**

CSC #5: Controlled use of administrative privileges

CSC #14 Controlled Access Based on the Need to Know

*Disable anonymous or guest viewing of video.* Some cameras have anonymous viewing or guest-account viewing (no credentials needed) enabled by default. This should never be enabled.

*Set a strong primary account password.* Replace the factory default user account with a new username and strong password. The name for the highest level of user account varies by vendor, and it can be called *root*, *admin*, *service*, *supervisor* or other names.

*Set up the user accounts to be used only by the video management system software.* This could be an individual account for each camera (lowest risk but higher management burden, or the same account across all cameras (highest risk, but lowest management burden). This helps create important troubleshooting information, as the camera's device logs can help determine whether an individual or a VMS server accessed the camera, and when.

*Forbid service technician universal credentials.* Forbid shared logon credentials for human user accounts of any kind.

*Apply the principal of least privilege in the assignment of user privileges.* 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.

*Use the VMS system for operations access to camera video and audio, rather than allowing direct network access to camera via a computer's web browser.* If possible, don't use individual personal camera logon credentials. The use of the VMS system 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.

## **6. Use a single time server for all cameras.**

CSC #3: Secure configuration for hardware and software

CSC #6: Maintenance, monitoring and analysis of audit logs

*Configure the cameras for the same Network Time Protocol (NTP) server used by the VMS servers.* Use a known reputable time server. For each camera, manually initiate the first time retrieval from

the time server, then ensure that the camera is configured to automatically update the time at an appropriate interval (such as hourly) using the time server. Ensure that time zones are correctly set. This is important to establish a time correlation across all cameras and video servers. All camera, alarm, event system and operator activity must correlate to the same timeline, to have a forensic quality audit trail.

Do not connect each camera to the Internet to for time server access. Small GPS NTP network time server devices are available that do not require an outdoor antenna.

If other types of time-sensitive activity recording are being performed, such as cash register or point-of-sale system's transactions, ensure that all systems are using the same time server source.

## **7. Disable camera audio not in use.**

CSC #9: Limitation and control of network ports, protocols, and services

*Disable camera audio features unless they are 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. For example, in some locales it is permissible to use audio for live monitoring, such as for alarm verification, but not for recording. Additionally, regulations often prohibit video and audio recording in building areas with reasonable privacy expectations (restrooms, changing rooms, and sometimes individual private offices). In the U.S. check federal, state and local regulations before using camera audio.

## **8. Disable unused protocols.**

CSC #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)

## **9. Encrypt camera edge storage.**

CSC #13: Data protection

*If camera SD Card capabilities will be used for primary, backup or buffered recording, enable the strongest level of encryption that the camera supports. If an unauthorized individual removes the SD card, this will prevent access to that video. If a local Network Attached Storage (NAS) device is used for recording, secure it in a locked area and ensure that its user accounts are properly configured.*

## **Servers and Workstations**

### **10. Document and back up server and dedicated workstation configurations.**

CSC #10: Data recovery capability

*Document, and back up, server and dedicated workstation configuration information, and update it when service technicians change configurations. Configuration data can be captured and backed up in several ways: (1) place screen shots or photos of screens containing configuration data plus appropriate notes in a Microsoft® Word® document, (2) type configuration data into a Microsoft Excel® spreadsheet file, or (3) use a commercial tool for system documentation, such as [System Surveyor](#).*

### **11. Use strong computer and application logon passwords.**

CSC #5: 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 Post-It® note affixed to the monitor or a slip of paper kept under the keyboard or in an unlocked drawer.*

### **12. Properly manage user accounts.**

CSC #5: Controlled use of administrative privileges

CSC #14 Controlled Access Based on the Need to Know

CSC #16 Account Monitoring and Control

*Apply the principal of least privilege in the assignment of user privileges. This principle requires giving a user account only those privileges that are essential for the user to perform required job tasks. 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 to perform configuration changes. 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 task needs.*

### **13. Activate Lockout and Logout Features.**

CSC #5: Controlled use of administrative privileges

CSC #14 Controlled access based on the need to know

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

**14. Keep operating systems current regarding all security updates.**

CSC #3: Secure configuration for hardware and software

*Ensure that operating system software is kept up to date, with all security updates and bug fixes.*

**15. Keep applications updated to their current versions.**

CSC #18: Application Software Security

*Ensure that applications are kept up to date, with all security updates and relevant patches.*

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

CSC #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 VMS.

*Additional windows services that should be disabled unless you know the VMS requires it:*

- 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 A for CompleteView VMS port requirements, and ensure that all unused ports are closed, that all needed ports are open, and that any software firewalls have their port configurations appropriately set.

#### **17. Use a single time server for all servers and workstations.**

CSC #3: Secure configuration for hardware and software

CSC #6: Maintenance, monitoring and analysis of audit logs

Do not connect servers and workstations to the Internet solely for accessing a time server. Small GPS NTP network time server devices are available that do not require an outdoor antenna.

#### **18. Use antivirus software on all servers and workstations.**

CSC #8: Malware defenses

*Deploy anti-virus software on all VMS servers, and on workstations that connect to the VMS.* Set the antivirus applications not to scan file folders (directories) that contain video files and recording databases. Set antivirus applications not to monitor the network ports used by the VMS.

#### **19. Keep mobile devices that connect to the VMS updated.**

CSC #3: Secure configuration for hardware and software

Ensure that any mobile devices that connect to the VMS have the latest operating systems installed along with their current patches.

#### **20. Back up and encrypt server and client configuration files.**

CSC #3: Secure configuration for hardware and software

CSC #10: Data recovery capability

CSC #13: Data protection

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

## **Network**

### **21. Establish a firewall configuration that isolates the camera LAN.**

CSC #11: Secure Configurations for Network Devices such as Firewalls, Routers, and Switches  
CSC #12: Boundary Defense

*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. This is especially important given the series of distributed denial-of-service (DDoS) botnet attacks on video cameras and recording equipment occurring since 2016.

### **22. Establish a VLAN configuration that isolates the camera LAN.**

CSC #11: Secure Configurations for Network Devices such as Firewalls, Routers, and Switches  
CSC #12: Boundary Defense

*Segregate camera network traffic using a VLAN.* Use network switch MAC binding and VLAN (virtual LAN) configuration to limit where video network traffic can go.

## **Service Agreement**

### **23. Establish an appropriate technical service response capability.**

CSC #19: Incident Response and Management

*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**

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

## **Cameras**

### **24. Establish HTTP digest authentication or enable HTTPS.**

CSC #3: Secure configuration for hardware and software  
CSC #13: Data Protection.

*Allow only digest authentication (encrypted passwords) or use HTTPS connections* (see recommendation #22 below), to prevent VMS client software from sending login passwords in clear text over the network.

## **25. Enable IP address filtering.**

CSC #1: Inventory of Authorized and Unauthorized Devices

CSC #12: Boundary defense

CSC #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-VMS software or devices.

## ***Servers and Workstations***

## **26. Enable HTTPS connections between Servers and Workstation/Mobile Clients.**

CSC #3: Secure configuration for hardware and software

CSC #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.

## ***Network***

## **27. Use device whitelisting, if it is the organization's standard network practice.**

CSC #1: Inventory of Authorized and Unauthorized Devices

CSC #12: Boundary defense

CSC #14: Controlled access based on the need to know

*Use router and/or firewall device whitelisting,* to authenticate VMS equipment and connecting devices.

## **28. Adjust WAN network configuration as required.**

CSC #9: Limitation and control of network ports, protocols, and services

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

## **Enterprise Security**

Apply the Basic and Advanced recommendations, updating and adding to them based upon the recommendations that follow below. In applying the following recommendations, collaborate with the organization's in-house or outsourced IT function. The applicability of these recommendations will depend upon whether the related control technology is in use by the organization. It can be very helpful to utilize a chart or spreadsheet that maps the CIS Critical 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. Documents that provide such mappings are easily found on the Internet.

## ***Infrastructure Management***

Managed enterprise network environments typically provide good cyber security controls, which is a benefit to any physical security systems on the network. Such networks typically have additional management tools and services that cameras, servers and workstations may need to be configured for. In such a case, the organization's IT department will provide specific information to enable the video surveillance system and its network to participate according to the IT plan and the management infrastructure in place. This is usually required in order for the viewing of security video to be available across the corporate network and/or for camera streams to traverse the corporate network.

## ***Cameras***

### **29. Use the corporate NTP time server for cameras.**

CSC #3: Secure configuration for hardware and software

CSC #6: Maintenance, monitoring and analysis of audit logs

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

### **30. Establish camera participation in IEEE 802.1X network access control.**

CSC #1: Inventory of Authorized and Unauthorized Devices

CSC #12: Boundary defense

*Set up the cameras for IEEE 802.1X network access control.* To participate in a network infrastructure where, for example, a Radius server used, the cameras need to have appropriate certificates and specific configuration settings. A Radius server would treat a camera as a web server. Apply the camera manufacturer's instructions according to the information provided by IT. Utilize automated password generation provided by the Radius server or similar technology.

### **31. Set up SNMP Monitoring.**

CSC #6: Maintenance, monitoring, and analysis of audit logs

*Obtain appropriate camera MIB (Management Information Base) files from the sources designated by the camera manufacturers.*

### **32. Set up Remote System Log monitoring.**

CSC #4: Continuous vulnerability assessment and remediation

CSC #6: Maintenance, monitoring, and analysis of audit logs

CSC #16: Account monitoring and control

CSC #19: Incident response and management

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

### **33. Establish and monitor a digital inventory of servers, workstations, cameras and network equipment.**

CSC #1: Inventory of Authorized and Unauthorized Devices

CSC #4: Continuous vulnerability assessment and remediation

CSC #6: Maintenance, monitoring, and analysis of audit logs

CSC #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 organization's IT department IT infrastructure management program. Commonly used tools are:

#### **Open Source**

- [Icinga](#)
- [LibreNMS](#)
- [Nagios Core](#)
- [NeDi](#)
- [Nmap](#)
- [Observium](#)
- [OpenNMS](#)
- [Zabbix](#)

#### **Commercial**

- [Solarwinds Network Performance Monitor \(NPM\)](#)
- [Solarwinds Server and Application Monitor \(SAM\)](#)
- [PRTG Network Monitor](#)
- [WhatsUp Gold](#)
- [Zenoss Service Dynamics](#)
- [Viakoo](#) (specifically for networked video systems)

### ***Servers and Workstations***

#### **34. Use the corporate NTP time server for servers and workstations.**

CSC #3: Secure configuration for hardware and software

CSC #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.*

#### **35. Establish server and workstation participation in IEEE 802.1X network access control.**

CSC #1: Inventory of Authorized and Unauthorized Devices

CSC #12: Boundary defense

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

### **36. Set up SNMP Monitoring.**

CSC #6: Maintenance, monitoring, and analysis of audit logs

*Establish appropriate SNMP monitoring for servers and dedicated workstations.*

### **37. Set up for Remote System Log monitoring.**

CSC #4: Continuous vulnerability assessment and remediation

CSC #6: Maintenance, monitoring, and analysis of audit logs

CSC #16: Account monitoring and control

CSC #19: Incident response and management

*Set up the servers and dedicated workstations to generate syslog messages, if the IT infrastructure network has a syslog server available. A syslog server collects all the log messages generated by the devices being monitored. Linux computers have built-in syslog functionality. Windows servers will require a syslog agent to be installed.*

## **Network**

### **38. Configure video system LANS for WAN/Internet connectivity per corporate networking requirements.**

CSC #1: Inventory of Authorized and Unauthorized Devices

CSC #3: Secure configuration for hardware and software

CSC #12: Boundary defense

CSC #13: Data Protection

CSC #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.

### **39. Provide corporate IT with network switch and router configuration requirements for security video.**

CSC #1: Inventory of Authorized and Unauthorized Devices

CSC #12: Boundary defense

CSC #14: Controlled access based on the need to know

*Provide switch and router port and protocol configuration requirements. Refer to the Port Lists in Appendix A for CompleteView VMS 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. Video and audio information that may become part of an investigation into an employee, contractor or visitor misconduct incident or criminal offense, may have specific data handling requirements. The security video surveillance system 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 the security video surveillance system.

#### **40. Establish appropriate participation in the corporate data governance framework.**

CSC #13: Data Protection

CSC #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.*

For example, privacy restrictions may apply, such as a rule not to record video or audio of indoor and outdoor union meetings, or that the faces of the meeting attendees are obscured using video analytics technology. Designate an individual to be the data steward for the security surveillance video. Establish an 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/DVE drives, and disable them except for authorized users.

### **Critical Infrastructure and Government Security**

#### ***Standards and Regulatory Requirements***

Critical infrastructure facilities, and government agency facilities, have specific computer system and network cyber security requirements. Collaborate early in the VMS project with the organization's IT department to identify the applicable policies, practices and technology that should be applied to the VMS system. The IT department is likely to already have a chart or spreadsheet that maps the CIS Critical Controls to the controls and regulations that apply, such as NIST 800-53, which will provide a correlation between the organization's requirements and the recommendations of this hardening guide.

Due to the critical importance of video security systems at some critical infrastructure facilities, video system requirements can include network path redundancy and hot standby servers for assurance of high availability. To fulfill such requirements, see the Salient Systems Corporation technical paper titled, "High Availability Failover Solution", implemented using virtual machines and VMWare's High



Availability Failover (HA) approach, which requires data center deployment utilizing three or more servers, redundant networking, and virtual storage area network (vSAN) technology.

## Appendix A – CompleteView Network Ports

### Server Network Ports

The table below contains the list of CompleteView (CV) network ports, and their application or transport protocol usage. Note that additional ports may be required for integration to 3<sup>rd</sup> party systems or devices. For CompleteView to function properly, firewall exceptions for servers, workstations and router firewalls will be required for these ports. Open only the needed ports in port ranges. *See CompleteView user and installation manuals for details.*

**Table 1. CompleteView Server Network Ports**

Port or Port Range	Protocol	Usage
25	SMTP	CV Email Notifications
80	HTTP	Required for the configuration of some cameras
554	RTSP	Video Data
943	TCP	Microsoft Silverlight Admin
4242	TCP	CV Data - CV Client Server to Software Clients on the network Interface
4250	TCP	CV Config Server
4255	TCP	CV Admin Service
8080	TCP	CV Web Service (pre-CompleteView 4.6)
4502-4534	TCP	CV Web Server to Web Client (Microsoft Silverlight)
1024-49100	UDP	UDP Video Data – default UDP port range
6970-7225	UDP	UDP Video Data – optional UDP port range

### Camera Network Ports

Firewall exceptions can also be required for communication with all cameras in the system, depending upon the make and model of specific cameras. Some common ports used by camera protocols are listed below. *For specific details about individual cameras, refer to the camera manufacturer's documentation.*

**Table 2. Common Camera Firewall Exceptions**

Port or Port Range	Protocol	Usage
554	TCP	Real Time Streaming Protocol (RTSP)
554	UDP	Real Time Streaming Protocol, Unreliable (RTSPU)
1024-49100	UDP	RTP/RTCP session pool (generic stream implementation)
6970-7225	IDP	RTP/RTCP session pool (generic stream implementation)

## ***Appendix B – CompleteView Product Manual References***

### **Product Manual References**

Recommendations for which there is relevant material in Salient Systems product manuals are listed below, followed by the specific product manual references.

Salient's RED3 Integration Server, referenced below, combines a server, a network switch, and VMS application software (CompleteView Professional or CompleteView ONE) together in a single professional video surveillance appliance.

Sections referenced below are from one or more of the following CompleteView (CV) manuals:

- **CV Server Administration 4.7.4:** CompleteView Administrators User Manual (version 4.7.4)
- **CV Server Administration 4.8:** CompleteView Administrators User Manual (version 4.8)
- **CV Web Client User 4.7.4:** CompleteView Web Client User Manual (version 4.7.4)
- **CV Video Proxy:** CompleteView Video Proxy User Manual (version 4.7.4)
- **RED3 IS User:** Red3 Integrated Server User Manual

### **Recommendation Items**

☐ **11. Use strong computer and application logon passwords.**

- **CV Server Administration 4.7.4 and 4.8:** Client Configuration, Users/Groups

☐ **12. Properly manage user accounts.**

- **CV Server Administration 4.7.4 and 4.8:** Client Configuration, Users/Groups
- **CV Web Client User 4.7.4:** Initial Setup

☐ **16. Close all unused network ports, stop unused operating systems services and protocols.**

- **CV Server Administration 4.7.4 and 4.8:** Windows® Firewall, VMS System Network Communications

**Note:** See Appendix C for the hardening-related port, service and protocol factory configuration settings for CompleteView servers, workstations and NRVs.

☐ **20. Back up and encrypt server and client configuration files.**

- **CV Server Administration 4.7.4 and 4.8:** System Configuration, CompleteView™ Configuration Utility

☐ **22. Establish a VLAN configuration that isolates the camera LAN.**

- **RED3 IS User:** Conceptual Overview, Initial Startup, and Switch Management.

☐ **26. Enable HTTPS connections between Servers and Workstation/Mobile Clients.**

- **CV Server Administration 4.7.4 and 4.8:** Appendix N: Digital Certificate Management and More
- **CV Video Proxy:** Appendix A: Video Proxy Secured Communications



## ***Appendix C – Factory Configurations for Services, Ports and Protocols***

### **Hardening Configuration Items**

The tables and paragraphs below contain the factory configurations for Windows service, port and protocol settings for Salient VMS servers and NVRs.

***Table 3. Salient Factory-Configured Windows Services Settings***

<b>Service</b>	<b>Factory Configuration Setting</b>
<b>Application Host Helper Service</b>	Not Installed on Server
<b>Application Layer Gateway Service</b>	Not Running - Manual Start
<b>Application Management</b>	Not Running - Manual Start
<b>Bluetooth Support Service</b>	Not Installed on Server or Workstation
<b>BranchCache</b>	Disabled
<b>Certificate Propagation</b>	Not Running - Manual Start (unless computer has a smart card reader)
<b>Computer Browser</b>	Disabled
<b>Distributed Link Tracking Client</b>	Running – Automatically maintains shortcut links between NTFS files within a computer or across a network, by updating links when the file is moved from its original location to a different location on the computer or across a network on the same Windows network domain
<b>Function Discovery Provider Host</b>	Not Running - Manual Start
<b>Function Discovery Resource Publication</b>	Not Running - Manual Start
<b>Human Interface Device Access</b>	Not Running - Manual Start
<b>Hyper-V Data Exchange Service</b>	Not Running - Manual Start (unless running on a virtual machine)
<b>Hyper-V Guest Shutdown Service</b>	Not Running - Manual Start (unless running on a virtual machine)
<b>Internet Connection Sharing (ICS)</b>	Not Running - Manual Start
<b>Link-Layer Topology Discovery Mapper</b>	Not Running - Manual Start
<b>Offline Files</b>	Not Running - Manual Start
<b>Remote Access Auto Connection Manager</b>	Not Running - Manual Start
<b>Remote Access Connection Manager</b>	Not Running - Manual Start
<b>Remote Desktop Services</b>	Disabled
<b>Routing and Remote Access</b>	Not Running - Manual Start (unless using IPSec or VPN tunneling)
<b>Shell Hardware Detection</b>	Running - provides AutoPlay feature for removable storage devices – may be disabled if not utilized
<b>Special Administration Console Helper</b>	Not Running - Manual Start
<b>Simple Services Discovery Protocol (SSDP)</b>	Not Installed on Server

Service	Factory Configuration Setting
<b>Web Services Dynamic Discovery Protocol (WS-Discovery)</b>	Not Installed on Server

CompleteView servers and NVRs are shipped with Windows Firewall enabled, and an appropriate set of firewall rules established. Additional information on Windows Firewall configuration is provided in the [CompleteView Quick Start Guide](#).

**Table 4. Salient Factory-Configured Port and Protocol Settings**

Port or Protocol	Factory Configuration Setting
<b>FTP port 21</b>	There is no inbound Windows firewall rule set for port 21. With no inbound rule this port would be blocked with an enabled firewall.
<b>ICMPv4 and v6</b>	Disabled.
<b>IPv6</b>	Disabled. Currently CompleteView supports only IPv4 addresses, and recommends setting a static (fixed rather than dynamic) IP address for a server or NVR.
<b>Network Discovery</b>	Enabled only for the private network. The public network would not permit network discovery. This would be needed if the customer wanted to auto-discover camera or network shares during system installation and configuration.
<b>SNMP Traps – ports 161 and 162</b>	Port 162 is disabled. Port 161, SNMP management port, has no inbound firewall rule. With no inbound rule this port would be blocked with an enabled firewall.
<b>SOCKS</b>	Socks has no inbound firewall rule. With no inbound rule this port would be blocked with an enabled firewall.
<b>SSH – port 22</b>	SSH port 22 has no inbound firewall rule. With no inbound rule this port would be blocked with an enabled firewall.



### ***ABOUT SALIENT SYSTEMS***

Salient Systems is a leader in open architecture video management systems. By combining powerful, yet flexible video management software and versatile hardware platforms, Salient delivers surveillance solutions that are easy to use, flexible and scalable. As Salient's CompleteView VMS supports a wide variety of security industry applications, customers are free to choose the best available design parameters to fit their needs.

For information about this document or CompleteView, email [info@salientsys.com](mailto:info@salientsys.com).

**Salient Systems**  
4616 W. Howard Lane  
Building 1, Suite 100  
Austin, TX 78728  
512.617.4800  
512.617.4801 Fax  
[www.salientsys.com](http://www.salientsys.com)

©2017 Salient Systems Corporation. All Rights Reserved. Company and product names mentioned are registered trademarks of their respective owners.