tyco | American Dynamics

American Dynamics Video Management System (AD VMS)

Hardening guide

GPS0046-CE-EN
Version 3.00.2
Rev A
Revised 2024-05-20

Johnson Controls

Introduction

Our solution provides peace of mind to our customers with a holistic cyber mind set beginning at initial design concept, continues through product development, and is supported through deployment, including a rapid incident response to meet the comprehensive and evolving cybersecurity environments.

The Hardening Guide intends to provide cybersecurity guidance used in planning, deployment, and maintenance periods.

As cybersecurity threats have become a risk impacting all connected devices, it is important to ensure that cybersecurity is considered throughout the planning, deployment and maintenance phases associated with a solution's functional operation.

This guide provides hardening guidance for configuration and maintenance, including the operating system, release management, user accounts, backup and restore.

This Johnson Controls **American Dynamics Video Management System Hardening guide** is broken down into three main sections depicting the overall process for hardening:

1. Planning	2. Deployment	3. Maintain
Provides an introduction, general knowledge, and overall guidance for you to prepare your system for security and hardening	Guides you through the execution and hardening steps based on the products and security features of the target system components	Provides a checklist for future checkpoints to keep your system safe and secure

Appendixes are included at the end for additional literature, and acronyms used within this document.

Legal disclaimer

The cybersecurity practices described in this guide are recommended practices to facilitate the secure installation and configuration of the products described herein. However, Johnson Controls cannot guaranty that the implementation of the cybersecurity practices or recommendations described in this guide will ensure the security of the relevant product or system, or prevent, or alter the potential impact of, any unauthorized access or damage caused by a cybersecurity incident. This guide is provided “as is”, and Johnson Controls makes no representation or warranty, expressed or implied, as to the efficacy of the cybersecurity practices or recommendations described in this guide. Johnson Controls disclaims all liability for any damages that may occur because of, or despite, reliance on this guide or compliance with any cybersecurity practices or recommendations set forth herein.

Table of Contents

1 Planning

Advanced planning will ensure the installation will be hardened and more secure. The contents within this section are useful to help plan for the deployment of American Dynamics[tm] Video Management System (AD VMS) in planning stage functions such as:

- Assuring compliance with the cybersecurity criteria that governs the target environment
- Designing the deployment architecture
- Providing a reference for settings made during deployment

1.1.0 AD VMS overview

AD VMS is a software program that enables a user to perform video surveillance operation on multiple VideoEdge recorders.

AD VMS operators can customize their video settings to best fit their site's bandwidth requirements. Operators can prioritize video frame rate or video resolution, and they can select a bandwidth connection speed that ensures that data transfers fit within their network guidelines.

AD VMS is hosted on a Windows® computer.

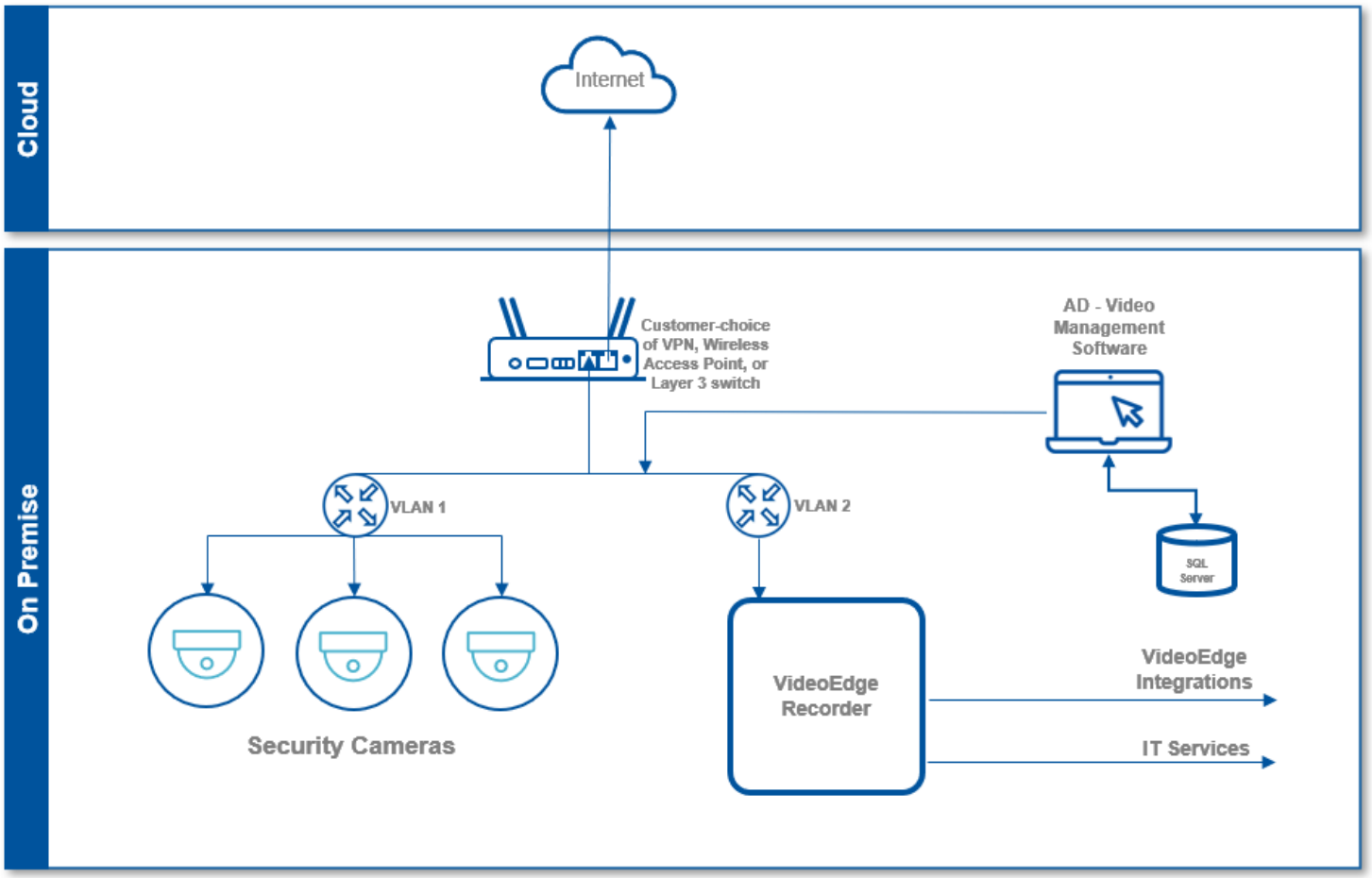
Currently supported features are:

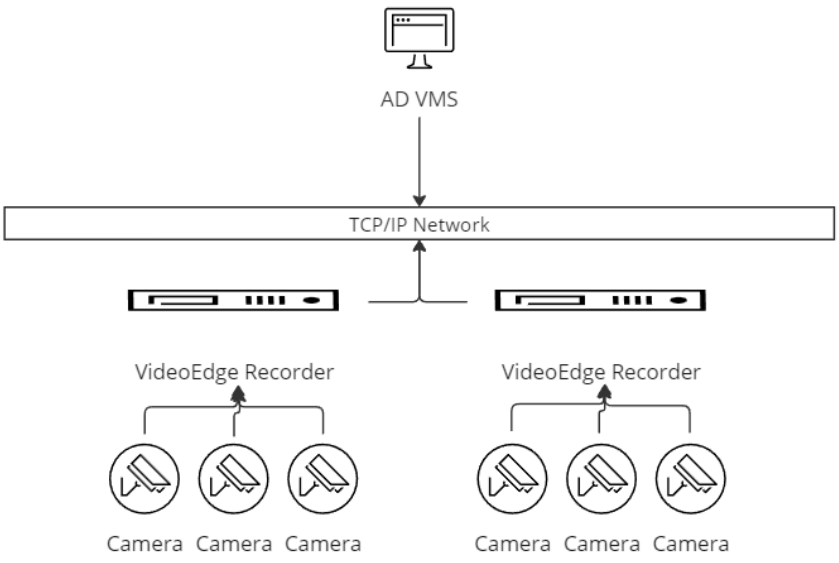
- Connect to VideoEdge recorders
- View up to 16 live cameras from 1 or more VideoEdge recorder
- View up to 16 playback videos from 1 or more VideoEdge recorder using video scrubber bar
- Retrieve recorded video using date, time, camera, or advanced search criteria
- Receive real-time alarm notification when viewing live cameras and download video snapshots
- PTZ control, Dewarp, and Virtual Presets
- Camera Tours and Saved Views
- Smart Streaming and bandwidth management

This document provides guidance on how to harden and operate an AD VMS securely.

1.1.1 AD VMS Deployment Architecture

Below is a sample architecture drawing of AD VMS





1.1.2 AD VMS Components

AD VMS. The AD VMS is standalone software designed to communicate with VideoEdge recorders over TCP/IP Network. Each installation has one or more VideoEdge recorders. Each installation supports up to 256 video cameras to any number of VideoEdge recorders.

1.1.3 AD VMS Supporting Components

VideoEdge Recorder. A device used to make and store digital video recordings, supporting a variety of search and playback functions. VideoEdge Recorders are connected to Video Camera and video surveillance applications. AD VMS streams video from VideoEdge recorder and receives alarm notifications from the VideoEdge Recorder.

Network Layer 3 Switch. A network switch with layer 3 routing capabilities provides VLAN management and connects AD VMS and the VideoEdge recorders into the network. It is best practice to segment this network to isolate VideoEdge recorders, Video Cameras on a dedicated LAN or VLAN.

1.2.0 Security Feature Set

Johnson Controls products are designed with built-in cybersecurity features out of the box. Some features are included and set by default while other features need the reader to go through steps for advanced hardening.

The following features are available in AD VMS:

Table 1.2.0.1 Security Features

Section	Type	Feature name	Feature Available
1.2.1	Configuration	Device Management	3.0.2
1.2.2	Monitor	Activity log files	3.0.2
1.2.3	Secure communications	Websockets secure and HTTPS support	3.0.2
1.2.4	Software updates	Automatic updates	3.0.2

For additional information, see the documents in Appendix A.

1.2.1 Configuration

Device management (passwords for recorders stored on the system / setting default protocol HTTPS) for the AD VMS system.

1.2.2 Monitor

AD VMS has the capability to download system activity log files (Capture Clients, pages navigated, user actions within application).

1.2.3 Secure communications

AD VMS can use WebSocket secure (WSS) and HTTPS to securely communicate with the VideoEdge server(s).

1.2.4 Software updates

AD VMS has the capability to notify the user and update itself with the latest patches and releases, to ensure the system has the latest security fixes.

1.3.0 Intended environment

The physical access to the device and physical installation of the device can impact the cybersecurity. It is recommended that AD VMS be installed in a physically secured location, such as a data center, or locked room.

1.3.1 Internet connectivity

For the highest security, internet connectivity is not recommended, and only required for the following scenarios:

- Use of the automatic updates feature (Can also manually update via website)
- Access to a VideoEdge which is accessible only through the internet

1.3.2 Integration with IT networks

The AD VMS client only needs connectivity to route to one or more VideoEdge servers. It is typical for clients to be installed on shared IT networks.

1.4.0 Patch Policy

Johnson Controls only supports the most recent version of the AD VMS Software. It is best practice to upgrade AD VMS with the latest software to install the most recent security fixes.

When we discover a critical security vulnerability, we use commercially reasonable efforts to:

- Issue a **critical update** for the current version of the product as soon as is reasonably practicable

When we discover non-critical security vulnerability, we use commercially reasonable efforts to:

- Apply fixes for **high severity** vulnerabilities in the next immediate release
- Apply fixes for **medium severity** vulnerabilities in the next major release

This policy is limited to the commercial life of the product.

1.5.0 Hardening methodology

AD VMS has many on board security safeguards, including many secure-by-default settings. However, Johnson Controls recommends that the client is hardened according to the guidance outlined in section 2 Deployment. A defence-in-depth strategy employing standard IT hardening methods and compensating controls as needed to complement the base security features of each component.

1.6.0 Communication

As stated in section 1.3.2, the AD VMS client only needs connectivity to route to one or more VideoEdge servers. This is unique in that the product has been designed to be accessed internally. Therefore, no specific ports will need to be opened for the AD VMS client.

1.6.1 Hardening the network ports

It is strongly recommended to close all ports that are unnecessarily open.

1.7.0 Network planning

Video surveillance systems transmit, collect, process and, store sensitive data that will disclose sensitive information if accessed by unauthorized users. While several security controls are inherent to the AD VMS client

to limit access to authorized users, it is best practice for the network design to provide additional layers of defense.

When designing a network for a video management system, first determine which components will be included in the full scope of the system required to provide all the planned functions for that system, for example, video cameras, network video recorders, clients, service connections, and remote access points.

With the full scope of components and functions in mind, build the appropriate level of protection into the network design to protect both the network and endpoints.

Important: The network infrastructure security is the customer's responsibility.

AD VMS is a client designed to connect to one or more VideoEdge recorders. Network planning should have been completed when VideoEdge was installed and hardened. Please review the VideoEdge hardening guide for additional details.

1.8.0 User management best practices

Following best practices for managing user accounts, account credentials and authorizations (permissions) can greatly improve the security for the system. Some guidance is presented in this section. For additional guidance, NIST standards such as SP 800-63 Digital Identity Guidelines may be consulted.

Create unique user accounts for each administrator. The proper configuration of individual user accounts assures that security best practices are followed and that all user actions cannot be repudiated.

Best practices for account management include:

1.8.1 No shared accounts

Unique accounts should be used during all phases of operation. Installers, technicians, auditors, and other deployment phase users should never share common user accounts.

1.8.2 Strong passwords

Strong passwords should be used to minimize the risk of password guessing. Automated forms of password guessing such as "dictionary attacks" and "rainbow tables" can run through commonly used passwords and can be successful if strong passwords are not used. Passwords can be strengthened by their length and complexity. The length of a password has the biggest impact on making password guessing difficult.

Passwords must be at least 8 characters long and have at least 4 characters from the following character groups:

- 1 Upper case letters
- 1 Lower case letters
- 1 Number between 0-9
- 1 Special character (such as $, !, &, #, %, ^, etc.)

NOTE: Johnson Controls strongly recommends a minimum of 15-character passwords which do not contain common dictionary words.

1.8.3 Password policy

It is important to have a password policy. Customers often have password policies that all systems must support.

2 Deployment

The contents within this section address how to initiate secure deployment for new installations, how to harden the solution and additional steps after commissioning required before turning over the solution to runtime operations.

2.1.0 Deployment Overview

Security hardening of AD VMS begins prior to deployment with careful planning as outlined in section 1 of this guide. It is a good practice to review section 1 prior to deployment to fully under the security feature set, its architecture, and requirements before physically installing and making application specific configuration changes.

In this section more details are provided to help the installer prepare for deployment:

- Physical installation considerations
- Resetting factory defaults
- Recommended knowledge level
- Other recommendations

2.1.1 Physical installation considerations

The physical access to the device and physical installation of the device can impact the cybersecurity. To prevent unauthorized access, be sure to place the device in a room, data center, cabinet or enclosure that can restrict access (for example, mechanical lock or physical access control).

2.1.2 Resetting factory defaults

There are two ways to reset AD VMS to factory default. Note that reinstalling the software over an existing AD VMS instance will retain user data. The two methods below will remove the user data:

Method 1.

- Under Windows Configuration, Settings, Apps, Uninstall AD VMS
- Reinstall AD VMS

Method 2.

- Navigate to C:\Users\%USERNAME%\AppData\Roaming\
- Delete the ADVMS directory
- Reinstall AD VMS

Notes (Next time 1-Un/Reinstall [data flushed] or 2. Delete directory[data flushed])

2.1.3 Recommended knowledge level

The person confirming that the proper hardening steps are executed in this guide must have Illustra administration and networking technologies experience.

2.1.4 Other recommendations

Applications such as AD VMS should always be launched with minimum privileges. For example, avoid launching AD VMS with 'Run as Administrator'.

2.2.0 Hardening

While AD VMS has several secure-by-default safeguards, it must be hardened to meet the security requirements of the target environment.

2.2.1 Hardening checklist

- ☐ Hardening Step 1: Apply Windows Operating System updates
- ☐ Hardening Step 2: Apply Client Software updates
- ☐ Hardening Step 3: User Account hardening
- ☐ Hardening Step 4: Backup application files

2.3.0 Operating system updates

Hardening Step 1: Apply Operating System updates

AD VMS is installed on a machine with Microsoft Windows Operating system. This operating system should be updated to the current version with all applicable patches applied during and after the commissioning process.

For further hardening, follow guidance from the Center for Internet Security (CIS) https://www.cisecurity.org/.

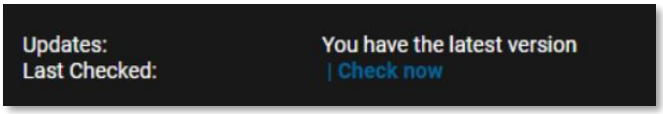
2.4.0 AD VMS Software

It is always best practice to harden AD VMS by updating to the latest release. Releases often contain fixes which strengthen the security of the application.

Hardening Step 2: Apply Client Software updates

Use one of the following methods depending on if AD VMS is connected to the internet:

- Method 1. If internet connectivity is available to AD VMS software, **Auto Updater** will automatically upgrade the latest version of the application.
  Note: To verify the system has the latest software, go to the Windows user tray, right-click the **AD VMS** icon, select the **About** option, and then select **Check now.**



- Method 2. If internet connectivity is unavailable to AD VMS software, the user must manually download the latest build and install it. To do this, navigate to the AD VMS website, and select **Software Downloads** at the following link - https://www.americandynamics.net/

2.5.0 User Accounts

When the AD VMS installation is complete, the user is guided through the account creation process. During this process, the user credentials are provided and a secret key for this account must be generated. The secret key

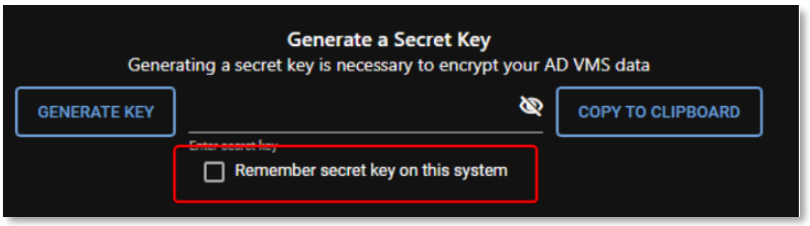
is used to securely encrypt (and decrypt) the database. User credentials tell AD VMS which user is accessing the system, assigns privileges, and grants data access.

2.5.1 All installation scenarios

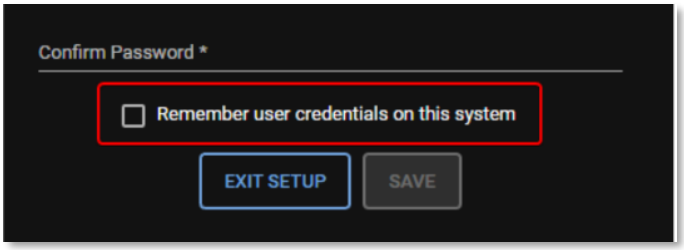
Hardening Step 3: User Account hardening

When creating the user account, be certain the following boxes are unchecked:

- Secret key – [ ] Remember secret key on this system



- User credentials – [ ] Remember user credentials on this system



Note: While this is the most secure approach towards managing an AD VMS account, it will also require the user to type in these credentials every time they launch AD VMS. Be sure to capture and securely store the secret key, username, and password in a secure document or password manager program (preferred) such as 1Password. Section 2.5.2 explains an alternative to typing in the credentials each time.

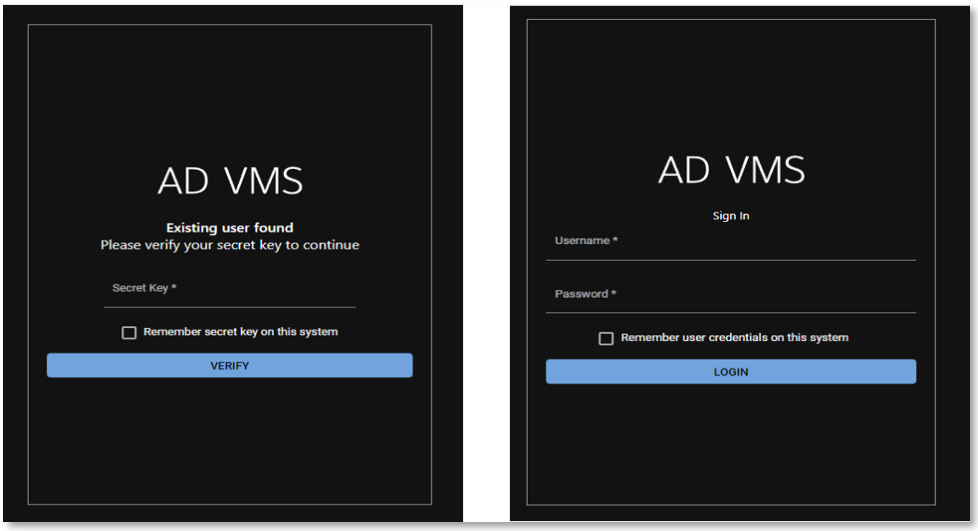
2.5.2 Secure Alternative

When a user does not want to enter the secret key and user credentials each time, then the following requirements must be satisfied before they select the appropriate boxes to make login faster:

- Only a single user has access to where AD VMS is installed
- The machine which hosts AD VMS is secured by a password and/or locked door

The next time AD VMS is started, do the following:

- Secret key
  - Enter the **Secret key**
  - Put a check in [X] Remember secret key on this system
  - Click **VERIFY**
- User credentials
  - Enter the **Username** and **Password**
  - Put a check in [X] Remember user credentials on this system
  - Click **LOGIN**



AD VMS will now automatically start each time, no longer prompting for the secret key, username, or password, after performing these steps.

2.6.0 Set a backup routine

Critical files are stored under the protected C:\Users directory of the AD VMS machine and need to be backed up in the event the machine experiences corruption or hardware failure.

Hardening Step 4: Backup application files

Follow your IT department procedures to regularly backup the following directory:

C:\Users\%USERNAME%\AppData\Roaming\advms

Restore AD VMS. In the event the AD VMS instance must be restored, select the latest backup from the hardening step 4 above, and restore those files into the “C:\Users\%USERNAME%\AppData\Roaming\advms” directory.

3 Maintain

The contents within this section address how to monitor for potential cybersecurity issues and maintain protection levels as conditions change.

An audit that produces a report indicating low cybersecurity risk is a very positive result and suggests that the deployment was conducted with a high degree of care and consideration. However, new attack vectors combined enhanced hacking tools and more advanced testing techniques may, in the future, disclose vulnerabilities with the technologies used.

The impacted technologies and their implementation may have been previously well regarded by cybersecurity experts. The discovery of vulnerabilities post the final deployment audit may not reflect the quality of the audit at the time. A higher degree of protection may be required for the environment as policies and regulations change over time.

3.1.0 Cybersecurity maintenance checklist

Continuously or periodically practice the following cybersecurity maintenance items. The frequency of their execution will depend on the policies and regulations which govern the site.

The typical maintenance periods provided are a starting point and adjusted to best suit the target conditions of the deployed environment:

Item	Description	Immediate	Base on Priority	Daily	Weekly	Monthly	Quarterly	Annual
1	*Backup application data*					✓		
2	*Test backup data*						✓	
3	*Remove inactive user accounts*	✓					✓	
4	*Disable unused features, ports, and services*						✓	
5	*Check for and prioritize advisories*				✓			
6	*Plan and execute advisory recommendations*		✓					
7	*Check and prioritize software patches and updates*				✓			
8	*Plan and execute software patches and updates*		✓					
9	*Review updates to organizational policies*							✓
10	*Review updates to regulations*							✓
11	*Conduct security audits*							✓
12	*Update password policies*							✓
13	*Update standard operating procedures*							✓
14	*Update logon banners*							✓
15	*Check for end-of-life announcements and plan for replacements*						✓	
16	*Monitor for cyber attacks*	✓		✓				

3.1.1 Backup application data

If AD VMS is to be restored or replaced, it is important to have a backup of its application data to minimize the time required to restore functionality.

Action	Details	Suggested frequency
Backup application data	Create a data backup. See section 2.6.0 – Set a backup routine.	Monthly

3.1.2 Test backup data

Test backups to provide assurance that the data backups contain the expected data and integrity.

Action	Details	Suggested frequency
Test backup data	Test the data created in step 3.1.1. See section 2.6.0 – Set a backup routine.	Quarterly

3.1.3 Remove inactive user accounts

While an employee may still be employed by an organization in which the system is owned, managed, serviced, or used by, they may not have utilized it for a long period. This suggests that independent of being authorized to use the system, they do not have a need to use the system and their user account should be removed. This is sometimes referred to as a use it or lose it policy. This best practice reduces the amount of active user accounts in the system and therefore lowers the potential attack footprint.

Action	Details	Suggested frequency
Remove inactive user accounts	Remove accounts of users immediately when known and review the list of users who have access quarterly	Quarterly

3.1.4 Disable unused features, ports, and services

If certain optional features, ports, and services are no longer required, disable them. This practice lowers the attack surface of AD VMS resulting in a higher level of protection.

Action	Details	Suggested frequency
Disable unused features, ports, and services	Review features, ports, and services.	Quarterly

3.1.5 Check for and prioritize advisories

Security advisories for AD VMS are located on the Cyber Protection website. Access is provided through a registered user account with that site. User account registration is open to Johnson Controls' customers and authorized representatives. At the bottom of the page, register to receive AD VMS product security advisories via email.

Determine if AD VMS is impacted by the conditions outlined in the advisories. Based on how the AD VMS system is deployed, configured, and used, the advisory may not be of concern. Referring to as-built documentation of the

AD VMS system will help with this assessment. A good set of as-built documentation will help identify the number of components impacted and where they are located.

While advisories call attention to a cybersecurity issue, it is not always possible to take immediate action or execute the full recommendation described in the advisories. If so, prioritization will aid in planning to ensure that any issue impacting the system is fully and appropriately addressed in order of priority. Check for advisories from third party components such as networking equipment and operating systems by consulting with the respective vendor.

Action	Details	Suggested frequency
Check for and prioritize advisories	Refer to the product advisories page. https://www.johnsoncontrols.com/cyber-solutions/security-advisories	Weekly

3.1.6 Plan and execute advisory recommendations

If AD VMS is impacted by the conditions outlined in the advisories, then action must be taken to mitigate the issues raised. The specific action is based upon the content of the advisories distributed and depends upon the environment AD VMS is deployed into. Plans for executing the advisory recommendations must consider the Hosting platform and environment.

Action	Details	Suggested frequency
Plan and execute advisory recommendations	Plan as described above and execute advisory recommendations	Based on priority

3.1.7 Check and prioritize patches and updates

While an AD VMS patch or update may or may not relate to an advisory, it is always best practice to apply the most current patches and updates. These patches and updates can include cybersecurity enhancements and fixes to known issues. Review the release notes and prioritize the benefits of the patch or update. The overall benefit should include the improved protection that lowers the cybersecurity risk. Check for updates and patches of third-party components such as networking equipment and operating systems by consulting with the respective vendor.

Action	Details	Suggested frequency
Check and prioritize software patches and updates	Explore available patches and updates each week. See section 2.4.0 AD VMS Software.	Weekly

Note: AD VMS Registration and software support is located at this link - https://www.americandynamics.net/

3.1.8 Plan and execute software patches and updates

Create a plan to apply software updates on a regular basis. This plan should include provisions for the unlikely event of service impact. Make considerations regarding schedule and deployed environment to minimize service disruptions.

Action	Details	Suggested frequency
Plan and execute software patches and updates	Plan as described above and execute update recommendations.	Based on priority

3.1.9 Review updates to organizational policies.

Organizations may update their policies which include cybersecurity requirements. Changes to these policies can impact systems which complied prior to the change. Periodically check to see if policy changes were made and re-assess compliance with those policies

Action	Details	Suggested frequency
Review updates to organizational policies	Collect most recent security policies for your organization	Annual

3.1.10 Review updates to regulations.

If AD VMS is deployed in a location that is governed by regulation, it is important to check to see if there are any updates to those regulations. In some cases, new regulations are introduced. Whether it is a review of an updated regulation to maintain compliance and a new regulation, an assessment of the changes should be conducted periodically.

Action	Details	Suggested frequency
Review updates to regulations	Collect most recent copies of regulations as applicable. Perform a gap analysis against the deployed configuration.	Annual

3.1.11 Conduct security audits.

Periodic security audits are necessary as cybersecurity guidance, organizational policies, regulations, auditing processes, system use, and configuration and threats have likely changed since the last audit. By conducting periodic security audits, the latest knowledge and conditions can be applied revealing gaps in protection previously undetected or created by changes in system use of configuration.

Action	Details	Suggested frequency
Conduct security audits	Perform the tasks listed on your Security audit checklist	Annual

3.1.12 Update password policies

Guidance on password policies has been evolving. Password policies should be re-assessed periodically to make sure the right policy in place for the target environment based on current organizational policies, regulations, and guidance from standards organizations such as NIST.

Action	Details	Suggested frequency
Update password policies	Review internal password policies and the section on passwords	Annual

Note: A password policy is not modifiable in AD VMS.

3.1.13 Update standard operating procedures

Including best practices for cybersecurity within standard operating procedures can complement the protection that the system can deliver on its own. Depending on the procedures an operator uses, a gap in protection can be created, prevented, or closed. Therefore, it is important to update standard operating procedures periodically.

Action	Details	Suggested frequency

Update standard operating procedures	Collect standard operating procedures for use of your system within the organization	Annual

3.1.14 Update logon banners

The system use policy details included on logon banners can change over time. Review and update as required.

Action	Details	Suggested frequency
Update logon banners	Review and modify the logon banner as necessary	Annual

3.1.15 Check for end-of-life announcements and plan for replacements

Review product announcements to determine if any of the components of AD VMS have a planned end-of-life announcement.

Action	Details	Suggested frequency
Check for end-of-life announcements and plan for replacements	Collect end-of-life details for all your products	Quarterly

3.1.16 Monitor for cyber attacks

Monitoring site perimeters, networks and endpoints for cyber-attacks is a part of good cybersecurity operation. Many tools are available to assist with real-time analytics-based detection.

Note: It is the customer's responsibility to verify that AD VMS continues to operate properly after any security monitoring tool has been installed.

Action	Details	Suggested frequency
Monitor for cyber attacks	Determine which security monitoring tools and services to implement	Run continuously once implemented

Appendix A - Additional AD VMS Literature

Description	Link
AD VMS User Guide:	https://docs.johnsoncontrols.com/americandynamics/r/American-Dynamics/en-US/AD-VMS-User-Guide/A/3.00.2

Appendix B - Acronyms

Acronym	Description
AD	American Dynamics
CIS	Center for Internet Security
LAN	Local Area Network
NIST	National Institute of Standards and Technology
PTZ	Pan tilt zoom
VLAN	Virtual Local Area Network
VMS	Video Management System
WSS	WebSocket secure