exacqVision
Hardening Guide v2.0

GPS0001-CE-20200420-EN

Rev A

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 exacqVision Hardening Guide provides cybersecurity guidance used in planning, deployment, and maintenance periods.

Because 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, user accounts, permissions and roles, backup and restore, redundancy, and patch management.

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, express 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 as a result of, or despite, reliance on this guide or compliance with any cybersecurity practices or recommendations set forth herein.

Contents

1 exacqVision overview

Exacq video management solution is a video management system (VMS) that includes video servers, and network video storage servers.

Use the exacqVision VMS on factory-installed hybrid, IP, and commercially available servers. Use exacqVision to manage live and recorded video, from small stand-alone systems to large enterprise applications.

Compatible with thousands of IP camera models and dozens of access control, intrusion, and point-of-sale systems, exacqVision's integrations make it one of the most robust end-to-end security solutions in the industry.

2 Deploying exacqVision securely

Use this section to initiate secure deployment for new installations, harden the solution, and complete additional steps after commissioning.

2.1.0 Server – desktop platforms

Harden the exacqVision Server on desktop platforms including Windows 10 or later, and Ubuntu 14.04 or later.

2.1.1 Hardening (Network Video Recorder) NVR or S-Series Server Service version 9.8 or earlier on Linux

To maintain all software functionality while de-elevated, upgrade to version to 19.03 or later. To harden, complete the following steps:

1. To recreate the cloud archive target, you must have your credentials for your Exacq cloud drive account.
2. Delete existing archive targets.
3. Create new archive targets. If you do not complete these steps, archive targets will not connect after transitioning to de-elevation or inversely.
4. Open the terminal.
5. In the terminal, type the following command: `sudo dpkg-reconfigure –p low edvrserver`
6. To de-elevate, select **Yes**.
7. To re-elevate, select **No**. The service automatically restarts.
8. To verify that the **core** and **exacqd** processes, are both running as the **edvrserver** user instead of the **root** user, in the terminal type the following command: `ps agux`

Note: The NVR can still record and search, and a local client running as non-administrative OS user is able to search, because 755 permissions (service has full access, all other users have read-only access) automatically apply recursively to all relevant local recording drives.

Result: Now you can create new SMB (Server Message Block), NFS (Network File System), and cloud archive target.

2.1.2 Hardening a Windows system

You can continue to use existing SMB or NFS archive targets after you transition to de-elevation or inversely. This is due to fundamental differences between the Windows security model and the Linux security model. However, this is not true for cloud archiving targets. To harden a Windows system, complete the following steps:

1. Delete existing archive targets.
2. Create new archive targets.
3. In the Windows toolbar right-click **Command Prompt** and click **Run as administrator**.
4. In the command prompt window, type the following command: `icacls d:\ /grant “Network Service:f” /t`
5. In the command prompt window, type the following command: `icacls d:\ /grant “Users:rx” /t`
6. Stop the service.
   a. To stop the service click the Windows **Start** menu and type *`Service`*.
   b. Click the Services desktop application icon.
   c. In the Service list right-click **exacqVision Server** and click **Restart**.
7. Add the following line to the `PluginList.ini` file: `deelevate=true`
8. Start the service.
9. Press CTRL+ALT+DELETE and click **Task Manager**.
10. Confirm that the following processes are both running as network service user and not SYSTEM user: **core** and **exacqd**.

Note: The NVR can still record and search because you have manually granted permission for the Network Service user to be able to read, write, and delete files on all relevant local recording drives. Local clients running as non-administrative OS users can search because you have manually granted read and execute permissions for all valid OS users to all relevant local recording drives.

Result: You can create new SMB, NFS, and cloud archive targets.

2.1.3 Enabling password strengthening and augmented authentication

This feature, introduced in exacqVision Server version 9.0, enables a more secure communication protocol between the client and server, meaning the server can enforce stricter authentication controls. When you upgrade the client and the server to version 9.0 or later you can use the **Security** tab to enable this feature. Refer to Strengthening server passwords for more information.

When you upgrade to version 9.0, machines running earlier versions of exacqVision client are no longer compatible with the server. This is acceptable because earlier client versions (9.0 or later) forces users to set strong passwords.

When this feature is enabled, the system does not store actual passwords. Instead, the system uses a strong algorithm to generate a secure identifier that combines a salt and hash with the Argon2 key extension algorithm and additional encryption. This secure identifier is stored. If you enable the secure identifier, passwords that are salted and hashed cannot be converted into cleartext. The use of a key extension algorithm makes dictionary or brute-force attacks more time-consuming for attackers.

2.1.4 Discontinue using external systems that do not require authentication

If you use the E-mail Servers tab, ensure that you use only an SMTPS server that requires password authentication and SSL.

If you use the Active Directory/LDAP integration feature, ensure that you use only an LDAP server that requires password authentication for binding and SSL.

If you connect an intrusion panel or an access control system, ensure that you connect only to systems that require password authentication or a type of secret key mechanism.

If you connect to IP cameras or encoders, ensure that you connect only to devices that require password authentication and SSL.

If you use the Archiving feature, ensure that you connect to only SMB targets that require password authentication.

2.2.0 Hardening exacqVision Web Service

Harden exacqVision Web Service on desktop platforms including Windows 7 or later, Ubuntu 10.04 or later, S-Series, and M-Series.

2.2.1 Enable TLS (HTTPS):

TLS connections require a user-specific certificate and you must manually configure them to enable them. Use TLS in all web communication because it actively prevents reading and manipulation of communication between the client and the web service. TLS connections are provided in the Web Service through two mechanisms:

- Let's Encrypt/ACME: A free service to provide TLS certificates with minor restrictions, for example, the web service must be hosted on port 80 and a domain name must be associated with the web service.
- External: User-supplied certificates for TLS. Purchase certificates from a certificate authority, such as VeriSign, DigiCert, or Network Solutions.

From the web service and end-user perspectives, there is no functional difference between the two types of configuration. To configure TLS in the web service, complete the following steps:

1. On the web service landing page, click the **Web Service Configuration** link. If this link is not displayed, the **Restrict to localhost** setting is enabled. To disable this setting access the web service directly from the machine.
2. From the navigation menu click **Configuration** and then click **HTTPS**.
3. Click **Configure**.
4. From the drop down select an encryption type, **Let's Encrypt** or **External**.
5. Enter the information and click **Apply**.
6. Restart the web service when prompted. The web service is now reachable using HTTPS.

2.2.2 Modify system settings (Windows only)

To modify system settings you must reconfigure the exacqVision Web Service to run as Local Service. The Web Service always installs as Local System, which grants unlimited OS administrative privileges to the software. This may be a security risk if the OS itself becomes compromised. The Local Service account is more secure for a long-running Windows Service that accepts incoming network connections. To modify system settings, complete the following steps:

1. Stop the exacqVision Web Service and exacqVision Web Server services.
    a. To stop the service click the Windows **Start** menu and type `Service`.
    b. Click the Services desktop application icon.
    c. In the Service list right-click **exacqVision Web Service** and click **Stop**.
2. Right-click on each service and select **Properties**.
3. Navigate to the **Log On** tab, select **This Account** and enter `Local Service`*.*
4. Clear both password controls.
5. Click **Apply**.
6. In the **Services Control** panel check if the service is **Local Service**.
7. Start the services.
8. Press CTRL+ALT+DELETE and click **Task Manager**.
9. Confirm that the following processes are both running as LOCAL SERVICE: **evws** processes and a **wfe** process.

2.2.3 Unavailable functionality after hardening

The following functions become unavailable when you apply certain hardening steps:

- Updates (Windows): If you attempt to update the web service through the service configuration the following message appears: **An error occurred while installing the update.** You must manually update the web service.
- Restarting (Windows): If you attempt to restart the web service through the service configuration, the following message appears: **There was an error during restart.** Use the Windows Services utility or Start menu shortcuts to manually restart the web service utility.

2.3.0 Enterprise Manager

This section has information on how to harden exacqVision Enterprise Manager on desktop platforms including Windows 7 or later, Windows Server 2008 or later, and Ubuntu 12.04 or later.

2.3.1 Hardening folder security in Windows 7, 8 or 10:

Refer to the following document for hardening steps: https://crm.exacq.com/kb/?crc=31399#loadAnswer~ebc3a63b-5e0c-be62-f712-5c67218d6c1f~1969ca77-8c11-92ff-fb62-52b0658f6feb

2.3.2 Hardening indexing with Solr:

Refer to the following document for hardening steps: https://crm.exacq.com/kb/?crc=41964#loadAnswer~14670fb0-54f0-292c-ac10-5c9409436b3a~1969ca77-8c11-92ff-fb62-52b0658f6feb