# victor Web vAS 5.7
# Hardening guide

GPS0022-CE-20220215-EN
Rev A

# 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, 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, 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 that your installation will be hardened and more secure.  The contents within this section are useful to help plan for the deployment of victor 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 victor Web overview

victor Servers and Workstations are developed to pair with the victor Video Management System and VideoEdge Network Video Recorders. Choose from several options based on your surveillance needs to ensure optimum performance.

Johnson Controls offers 4 different licensed client software offerings depending on your needs.

- victor Web Client
- victor Express Client
- victor Pro Client
- victor Enterprise Client

Please note that this document is focused on the first bullet point – victor Web Client

1.1.1 victor Web Client

Access and monitor a security infrastructure through the victor video management system from virtually anywhere. With browser support available on Chrome, and Firefox the victor Web Client allows users to quickly view and play back video for timely event management. Search videos from multiple recorders simultaneously and export video clips with a single click.

The victor Web Client compliments the victor software by allowing operators to utilize their system from remote locations away from the command center without additional plug-ins or system updates.

victor Web comes in two options.

- victor Web LT Client
- victor Web Client

The table below shows the features which are included in each victor Web option:

| | victor Web LT Client | victor Web Client |
|---|---|---|
| **Live monitoring, time/date playback & export** | ✓ | ✓ |
| **Real-time alerts & event management** | ✓ | ✓ |
| **Smart Search** | ✓ | ✓ |
| **Integrated user policy management** | ✓ | ✓ |
| **Video analytics support** | ✓ | ✓ |
| **Smart Streaming** | ✓ | ✓ |
| **Search videos across multiple recorders** | ✓ | ✓ |
| **Virtual PTZ** | ✓ | ✓ |
| **Health monitoring** | NVR | Enterprise |
| **TSP recorder support** | VideoEdge Only | VideoEdge Only |
| **Tyco or 3rd party integrations** | | ✓ |
| **Personnel activity monitoring** | | Add-on |
| **Swipe and Show** | | Add-on |
| **Interactive maps** | | Add-on |
| **Text Stream Search** | ✓ | ✓ |
| **Text Stream Monitor** | ✓ | ✓ |
| **Fixed/Saved Views** | ✓ | ✓ |
| **Custom Video Layouts** | | ✓ |
| **Personnel Management** | | Add-on |
| **Audit** | | ✓ |
| **Journal** | | ✓ |
| **Light or Dark User Interface** | ✓ | ✓ |
| **English, French, German, Italian, Portuguese (Brazilian), Spanish** | ✓ | ✓ |

### 1.1.2 Appliance models

VAS Servers come in two form factors, 1U (Standard) and 2U (Performance). The features of each are shown in the table below:

| | ADVC-SVRSTD | ADVC-SVRHIPERF |
|---|---|---|
| Form Factor | 1U | 2U |
| Description | Powerful performance and high availability | Offers impressive performance and large memory footprint |
| Processors | Intel Xeon E-2176G | Intel Xeon 6242 |
| Operating Systems | Windows Server 2019 | Windows Server 2019 |
| Memory | 32 GB (16 GB UDIMM x 2) | 128 GB (32 GB RDIMM x 4) |
| Hard Drive Slots | Four Front Accessible Drives Hot Swap Capable | Eight Front Accessible Drives Hot Swap Capable |
| Storage | 2 x 600 GB RAID 1 | 6 x 900 GB RAID 10 |
| Network Interface | 4 x 1 GbE NICs | 2 x 10 GbE NICs; 4 x 1 GbE NICs |
| Dimensions (W x H x D) | 17.08in x 1.7in x 23.45in (43.4cm x 4.3cm x 59.5cm) | 17.09in x 3.44in x 26.72in (43.4cm x 8.8cm x 67.8cm) |
| Power Supplies | Single 350W | Dual, redundant 750W |
| Emissions | EN55022 Class A | EN55022 Class A |
| Immunity | EN55024 | EN55024 |
| Safety | EN/IEC60950-1 | EN/IEC60950-1 |
| Environmental | RoHS | RoHS |
| Warranty and Support Services | Three-year limited warranty plus NBD onsite service | Three-year limited warranty plus NBD onsite service |
| Max BTU | 1340 BTU/hr | 2891 BTU/hr |
| DVD Drive | +/- RW SATA | +/- RW SATA |
| Included Accessories | Rack Mount Rails, USB Mouse and Keyboard | Rack Mount Rails, USB Mouse and Keyboard |

### 1.1.3 Restful API Service

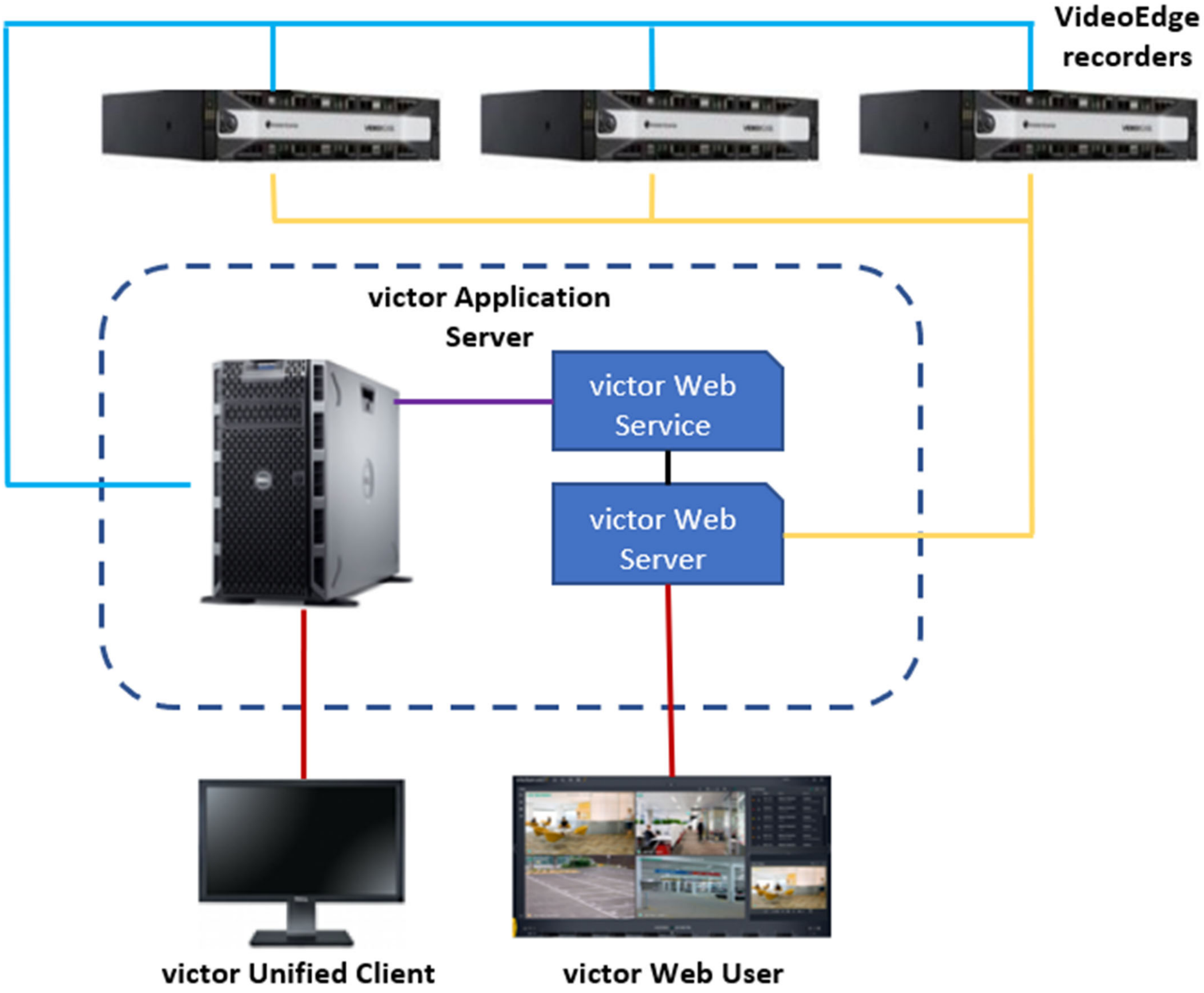
The victor Integration Driver Service (IDS) supports a pre-defined variety of services exposed as a REST API. Any authenticated source will be capable of raising events within victor providing they conform to the interface described in this document. All return values are through JavaScript Object Notation (JSON).

### 1.2.0 Deployment architecture

This section provides an overview of the deployment options for victor Web. There are four deployment options: one victor Application Server deployment and three standalone server deployments. The deployments differ, based on how you install victor Web Service and the victor Web Server. Choose one of the following deployment options:

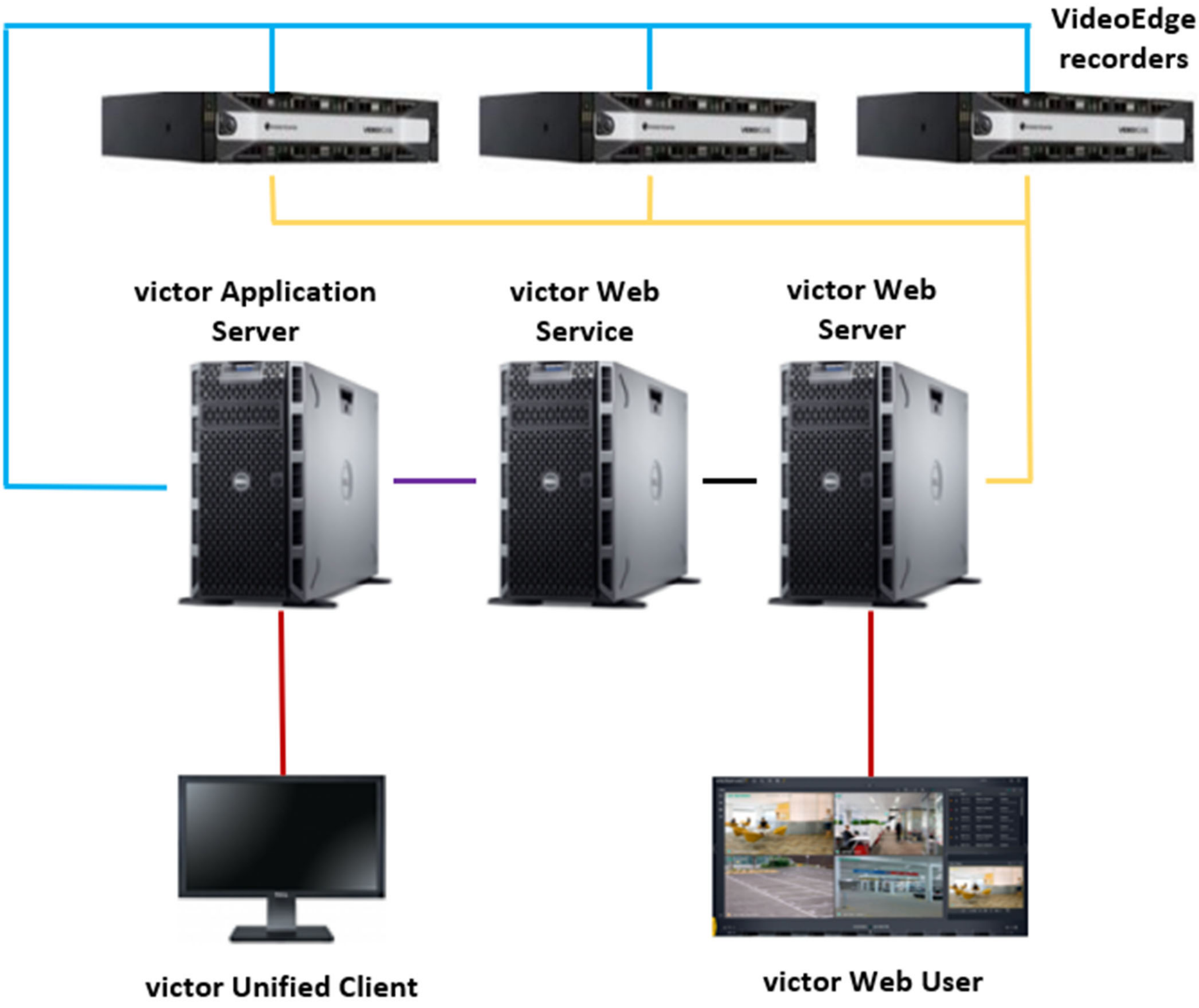
#### victor Application Server deployment

1.2.1 **Scenario 1**: Install victor Web and the victor Web Service on a single victor Application Server.

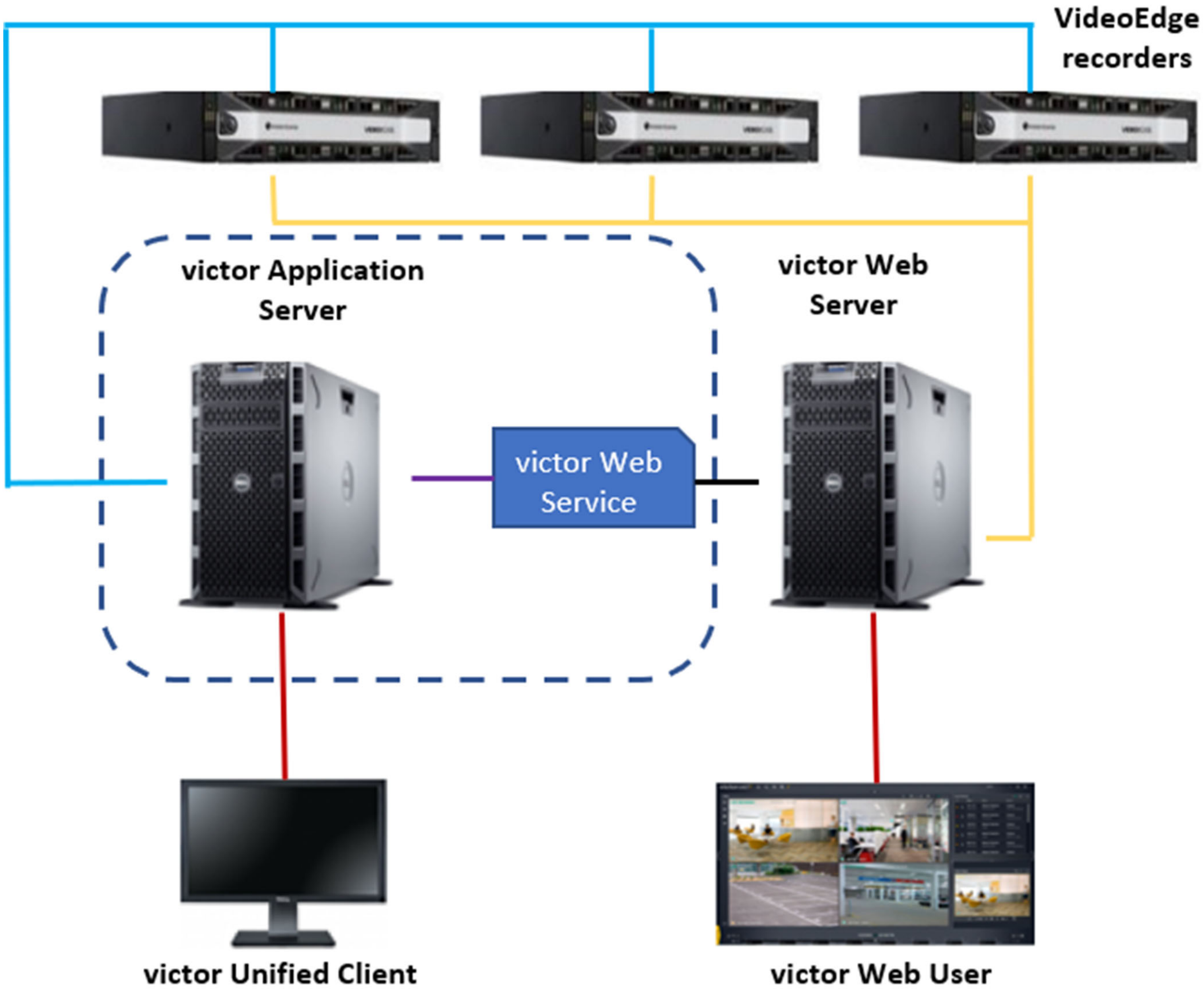


### Standalone server deployments

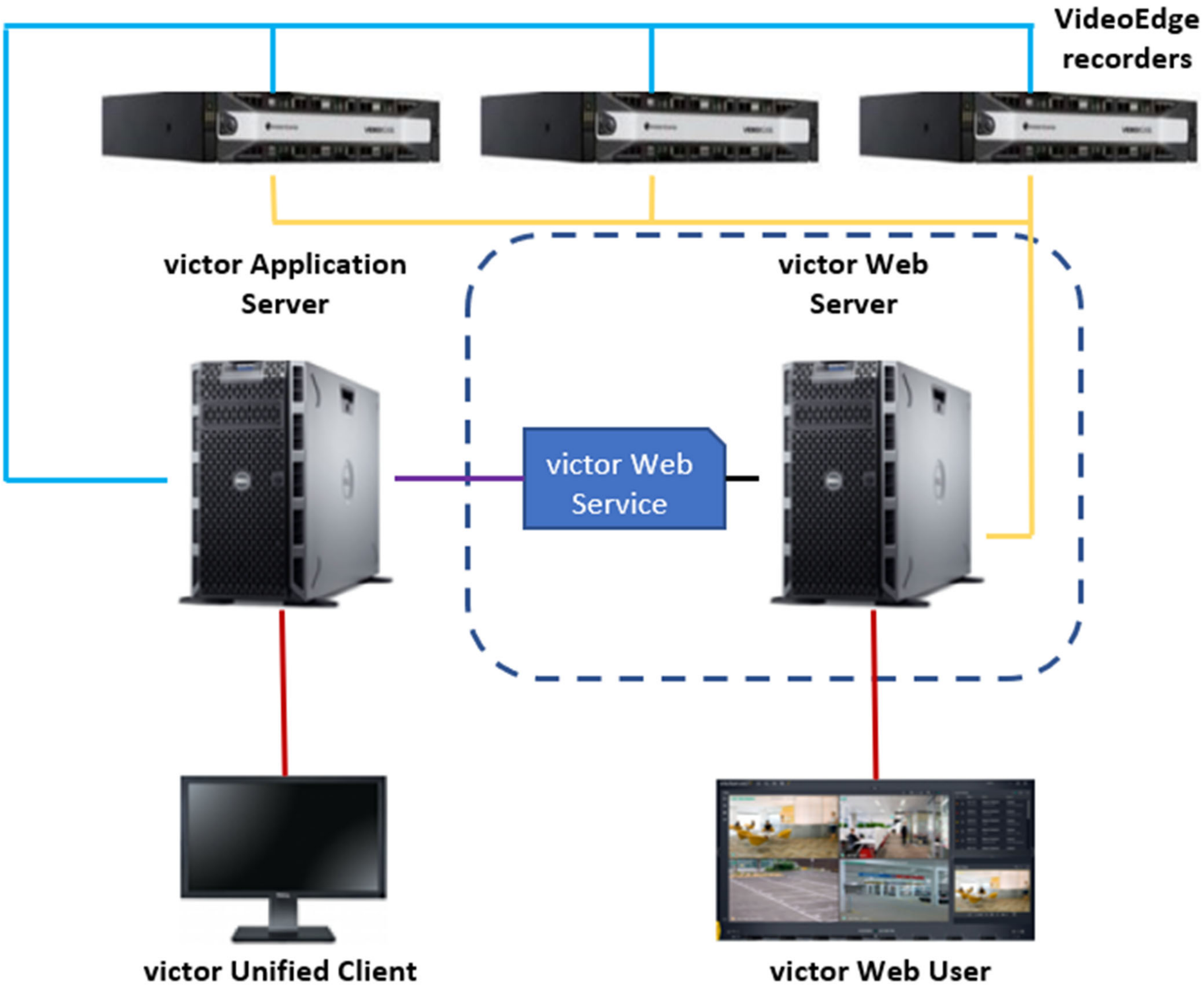
1.2.2 **Scenario 2**: Install victor Web Service and the victor Web Server on separate standalone servers.



### 1.2.3 **Scenario 3**: Install victor Web Service on a standalone server.



### 1.2.4 **Scenario 4**: Install victor Web Service and victor Web Server on a standalone server.



### 1.3.0 Core components

victor Web is not a standalone product. To use victor Web, your video Management System must have a victor Application Server, and the victor Web Service.

*victor Application Server*

victor Application server (vAS) is a dedicated, licensed version of victor. victor is part of a powerful NVMS that includes advanced policy management, health monitoring, Smart Search, instant playback, and more, ensuring the security and safety of your entire organization whether a single site, or a multi-location, globally dispersed enterprise Scalable from single-site locations to enterprise-level deployments, these servers are available in several form factors with distinct configurations to simplify ordering and installation.

*victor Web*

victor Web is a portal through which users can view live and recorded video, events and diagnostics from multiple VideoEdge recorders by logging in through a web browser. victor Web is hosted on a Windows computer and must be integrated with a victor Application Server (vAS).

*victor Web service*

Depending on your deployment scenario, you can install victor Web on the victor Application Server, or you can install victor Web on a standalone server.

*victor client*

This is the victor client software. The default victor unified client layout consists of three tabbed toolbars (Home, Build and Setup), the Device List and a 1X1 Surveillance tab. This layout can be completely customized, allowing you to create a workspace that better suits the requirements of individual operators and roles.

*victor Workstations*

Scalable from small single-site locations to enterprise-level deployments, victor Workstations are available in three distinct configurations (Standard, Performance, High Performance). These workstations are ideally suited for viewing and managing video via the pre-installed victor client for operator efficiency.

*victor Compact Workstation*

Conserve space and maximize uptime with the victor client pre-installed on small, versatile hardware that can be deployed in constrained environments. The full-featured VMS can be utilized for live viewing and playback without taking up the amount of space required by traditional PC workstations. victor Compact is ideal for active deployments in retail, healthcare, and financial industries that need to increase situational awareness quickly and efficiently.

*victor Web User*

This refers to a user of victor web who communicates through the victor Web Server

### 1.3.1 Supporting components

*VideoEdge Recorders*

VideoEdge is a network video recorder (NVR), available with a full range of intuitive clients to manage surveillance in very active environments with both onsite and remote accessibility options. VideoEdge is scalable from a single NVR, to a large multi-site architecture.

*IP Cameras*

An IP camera is a surveillance camera that communicates over the Ethernet using IP addressing. While VideoEdge supports third-party IP cameras, Illustra IP cameras offer enhanced functionality when coupled with a VideoEdge NVR. (Refer to Illustra Security Hardening Guide for more details).

*PoE Camera*

An IP enabled surveillance camera that receives its power from the Ethernet cable – Power over Ethernet (PoE).

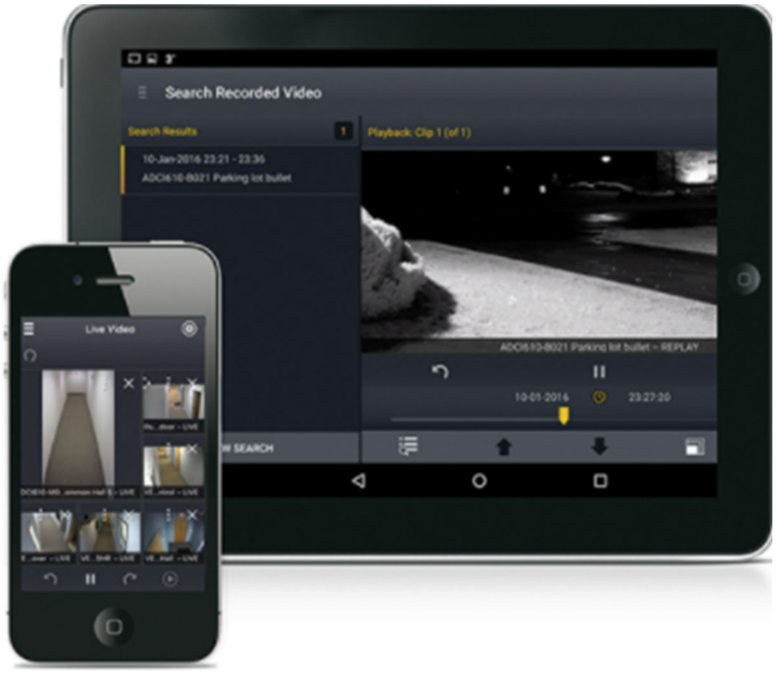
*Isolated Camera Network*

Most cameras today are designed to seamlessly operate on IP networks or via wireless communications. Keeping these cameras secure requires isolation from other devices the normally communicate on the same networks.  Establishing a sub-network or “subnet” you prevent access to the internet and harden your camera network.

### 1.3.2 victor Go Mobile application

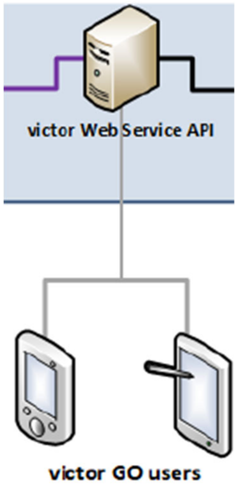
victor Go is a mobile application that you can use to view camera footage from connected network video recorders, and to view system events and alarms. You can also save and push content, such as still images, to other app users instantly to streamline event response while away from the command center.

Features available in the full victor Video Management System are still available at your fingertips, such as SmartSearch, PTZ camera control, and live video retrieval. Save time by simply logging in to the app from an Apple or Android device to manage an incident or monitor a security operation remotely. The 64-bit video surveillance app is designed to provide the right video quality for a mobile device with minimal delay.


Search Recorded Video
Search Results
10-Jan-2016 23:21 - 23:36
ADCi610-B021 Parking lot bullet
Playback: Clip 1 (of 1)
ADCi610-B021 Parking lot bullet - REPLAY
10-01-2016
23:27:20
SEARCH
Live Video

Download victor Go from the iTunes store and the Google Play store. Once installed on your mobile device, you can use victor Go to connect to a victor Application Server through a 3G, 4G or Wi-Fi connection.

**The victor Web Service facilitates communication between victor GO and the victor Application server**



## 1.4.0 Security feature set

This section describes the security features within victor Web vAS

### 1.4.1 User Account Roles

A Role is a set of access rules which is assigned to an operator to govern their authorization and permission levels within victor.   There are five pre-configured roles, ready for assignment to users. Each of these roles, apart from Administrator can be edited to refine them further. Pre-configured roles are as follows (Descending permission level):

- Administrator
- Power User
- Investigator
- Basic User
- Guard
- Viewer

Custom Roles

As well as using pre-configured roles, you can create custom roles. This can be done using the ‘Save As’ feature which allows a current role to be used as a template to build a new role, or you can build a completely new role manually. Each new role created is available for selection when creating or editing operator profiles.

### 1.5.0 Intended environment

The physical access to the device and physical installation of the device can impact the cybersecurity. It is recommended that victor Web be installed in a physically secured location.

#### 1.5.1 Network connectivity

Internet connectivity is only required for the following scenarios:

- Installation of victor
- Remote support tool function
- victor Web Server (See section 2.2.3 Hardening victor Web Server Security Settings)

For all other scenarios, victor does not require Internet access.

You must enable Internet Information Services (IIS) and you must install Application Request Routing (ARR) before you install victor Web or the victor Web Service. If you install victor Web as part of a unified installation, you can install victor Web, the victor Web Service, and the victor Application Server at the same time.

After you install victor Web, you must configure the server-side certificate (SSL) and victor Web configuration files to apply security to your online communication. When a web browser contacts your secured site, the SSL certificate allows the encrypted connection after checks have occurred.

IIS – Internet Information Services

IIS is an extensible web server for Windows that is used in the victor web service. The version of IIS varies based on the Windows operating system that is running on the host device. See the victor Web Installation Guide for additional information (https://www.americandynamics.net/products/GetDocument/57922).

ARR – Application Request Routing

The ARR installer requires an active internet connection to complete the installation. To download an offline ARR installer, click the following URL (https://www.microsoft.com/enus/download/details.aspx?id=47332).

For additional information about ARR 3.0, refer to the Microsoft website.

Web Server Installation

The victor Web installation guide advises installing web servers. Normally, web servers have direct exposure to the internet. Video system installations are sensitive and therefore may be made available only to the trusted networks. It is imperative that users harden those web servers to meet Johnson Controls standards. Hardening is covered in section 2.0 – Deployment.

### 1.6.0 Communication

#### 1.6.1 Hardening the network ports

When you use a protocol, ensure that the corresponding port is open. Validate if any additional open ports are necessary to be open. Otherwise, it is strongly recommended that you close ports that are not mentioned below and unnecessarily open.

For additional information on ports and protocols which are specific to the victor, see tables 1 – 3 over the next several pages, or click the links below to move directly to a page.

The following table lists the port assignments for victor Application Server (vAS).

Table 1: victor Application Server (vAS) port assignments

| Port | Process / Service | Protocol | Direction | Destination System | Description |
|---|---|---|---|---|---|
| **80** | VideoEdge NVR Admin / Alarm Port | TCP | Bidirectional | VideoEdge | VideoEdge NVR Admin / Alarm Port |
| **80** | everRun IIS | TCP | Bidirectional | everRun | everRun IIS port (required to be open) |
| **389** | LDAP | TCP | Outbound | LDAP Server | LDAP which is used to synchronize vAS database with other databases (non-vAS). It allows other databases, such as human resources information, to download information |
| **443** | everRun HTTPS Communications | TCP | Bidirectional | Web | HTTPS Port for SSL connections with vAS Go Stratus (everRun) communication |
| **1433** | SQL Server | UDP and TCP | Bidirectional | SQL Server | Traffic Direction from vAS outbound; Connection Initiate from vAS to SQL server.<br>Communication from vAS to SQL for database writing, reading and modifying. |
| **1434** | SQL Server | UDP | Bidirectional | SQL Server | Traffic Direction from vAS outbound; Connection Initiate from vAS to SQL server.<br>Communication from vAS to SQL for database writing, reading and modifying. |
| **5000** | Intellex Base | TCP | Bidirectional | Intellex | Intellex Base |
| **5001** | Intellex Live | TCP | Bidirectional | Intellex | Intellex Live |
| **5003** | Intellex Alarm | TCP | Bidirectional | Intellex | Intellex Alarm |
| **7144 - 7145** | EMC Replistor | TCP | Transmit | EMC Replistor | For EMC Replistor failover/redundancy |
| **8042 - 8045** | EMC AutoStart | TCP | Transmit | EMC Autostart | For EMC AutoStart failover/redundancy |
| **8085** | Auto Update | TCP | Bidirectional | Client | Auto Update for clients and SAS from MAS |
| **8989** | Update File Server | TCP | Inbound | VideoEdge | Communication from vAS to VideoEdge for Incremental Updates or Camera Firmware updates. |

| | | | | | |
|---|---|---|---|---|---|
| | | | | | **Note**: Ensure that Port 8989 is accessible from the VideoEdge units being upgraded |
| **8990** | Tyco Update Repository | TCP | Inbound | vAS | Tyco Update Repository |
| **8991** | Push upgrade | TCP | Inbound | Connections expected from VideoEdge | VideoEdge software updates |
| **8992** | Tyco Update Client Services | TCP | Outbound | vAS | Tyco Update Client Services |
| **8996** | Crossfire service of web client | TCP | Bidirectional | Client | Location = vAS, Traffic Direction from vAS =inbound, Connection Initiate from victor Client. For clients to access vAS from web. |
| **8997** | Admin / Monitor Client stream | TCP | Bidirectional | Client | location = vAS, Traffic Direction from vAS = inbound, Connection Initiate from victor Client. Client access to administrative or monitor station of vAS |
| **8998** | Crossfire service of HTTP client session | TCP | Bidirectional | Client | location = vAS, Traffic Direction from vAS = inbound, Connection Initiate from victor Client. For HTTP of crossfire for client session |
| **8999** | Crossfire service of TCP client session | TCP | Outbound | Client | location = vAS, Traffic Direction from vAS = inbound, Connection Initiate from victor Client. For crossfire service of TCP client |
| **27000 – 27010** | TycoESS License software Centralized Licensing | TCP | Bidirectional | vAS | location = vAS, traffic direction from vAS = inbound, Connection initiate from vAS. Used for verifying licenses with Software House. Centralized Licensing for VideoEdge |
| **32200 - 38200** | VideoEdge streaming | UDP | Bidirectional | VideoEdge | VideoEdge NVR Streaming Port |

The following table lists the port assignments for victor Client.

Table 2: victor Client port assignments

| Port | Process / Service | Protocol | Direction | Destination System | Description |
|---|---|---|---|---|---|
| **80** | HTTP | TCP | Bidirectional | VideoEdge NVR | VideoEdge NVR Admin / Alarm Port |
| **443** | HTTPS | TCP | Bidirectional | VideoEdge NVR | VideoEdge NVR Admin / Alarm Port encrypted |
| **554** | RTSP | TCP | Bidirectional | VideoEdge NVR | Real-time streaming protocol default port. Creates, controls, and destroys streaming sessions |
| **5000** | Intellex Base | TCP | Bidirectional | Intellex DVR | Intellex Base |
| **5001** | Intellex Live | TCP | Bidirectional | Intellex DVR | Intellex Live |
| **5003** | Intellex Alarm | TCP | Bidirectional | Intellex DVR | Intellex Alarm |
| **6000 – 7999** | RTP / RTCP | UDP | Bidirectional | VideoEdge NVR | Even port numbers = real-time transport protocol, odd port numbers = real-time control protocol, each video stream uses one of each of these port,<br>RTP port is for receiving UDP video packets from the Video Edge,<br>RTCP port sends feedback on the network quality, and keeps the stream alive, Client-side ports,<br>Ports 32200-38200 = server side ports |
| **8999** | Crossfire service of TCP client session | TCP | Bidirectional | vAS | location = vAS, Traffic Direction from vAS = inbound, Connection Initiate from victor Client. For crossfire service of TCP client session. |

The following table lists the port assignments for victor Web.

Table 3: victor Web port assignments

| Port | Process / Service | Protocol | Direction | Destination System | Description |
|---|---|---|---|---|---|
| **80** | HTTP / IIS Proxy | TCP | Bidirectional |  | VideoEdge NVR Admin / Alarm Port |
| **443** | HTTPS / IIS Proxy | TCP | Bidirectional |  | VideoEdge NVR Admin / Alarm Port encrypted |
| **3000** | HTTP victorWeb | TCP | Bidirectional |  | VideoEdge NVR Admin / Alarm Port |
| **3001** | HTTPS victorWeb | TCP | Bidirectional |  | VideoEdge NVR Admin / Alarm Port encrypted |

The following table lists the port assignments for victor GO

Table 4: victor GO port assignments

| Port | Process / Service | Protocol | Direction | Destination System | Description |
|---|---|---|---|---|---|
| **80** | HTTP | TCP | Bidirectional |  | VideoEdge NVR Admin / Alarm Port |
| **443** | HTTPS | TCP | Bidirectional |  | VideoEdge NVR Admin / Alarm Port encrypted |

The following table lists the port assignments for VideoEdge.

Table 5: VideoEdge port assignments

| Port | Process / Service | Protocol | Direction | Destination System | Description |
|---|---|---|---|---|---|
| **22** | SSH | TCP | Bidirectional | Client SSH terminal | SSH |
| **25** | SMTP | TCP | Bidirectional | mail server | SMTP |
| **67** | DHCP | UDP | Bidirectional | DHCP client | Assign DHCP addresses to clients |
| **68** | DHCP | UDP | Bidirectional | DHCP server | obtaining dynamic IP address (DHCP) |
| **80** | HTTP | TCP | Bidirectional | Web/Client | HTTP |
| **123** | NTP | UDP | Bidirectional | NTP (time server) | NTP |
| **161** | SNMP | UDP | Bidirectional | SNMP manager | SNMP |
| **162** | SNMP | UDP | Bidirectional | SNMP manager | SNMP Trap |
| **443** | Secure HTTP | TCP | Bidirectional | Web/Client | HTTPS |
| **554** | RTSP Stream | TCP | Bidirectional | Camera/client | RTSP (video) stream |
| **1900** | UPnP | UDP | Bidirectional | Any | UPnP |
| **1900** | AD discovery | SSDP | Bidirectional | Any | veAutoDiscSSDP - Discovery of devices, close after setup |
| **2980** | AD discovery | UDP | Bidirectional | Any | veAutoDiscScan - Discovery of devices, close after setup |
| **3389** | RDP | TCP | Bidirectional | RCP client | xrdp |
| **3702** | AD discovery | UDP | Bidirectional | Web Server/Any | veAutoDiscovery WSDiscovery - Discovery of devices, close after setup |
| **5353** | AD discovery | UDP | Bidirectional | Any | veAutoDiscMDNS - Discovery of devices, close after setup |
| **6000 – 6199** | RTP/RTCP | UDP | Bidirectional | Camera/client | RTP/RTCP |
| **8848** | AD discovery | UDP | Bidirectional | Any | autoDiscADPort8848 - Discovery of devices, close after setup |
| **8989** | Update File Server | TCP | Outbound | vAS | Communication from vAS to VideoEdge for Incremental Updates or Camera Firmware updates |
| **8991** | Push Upgrade | TCP | Outbound | vAS | VideoEdge software updates |
| **8992** | AD discovery | UDP | Bidirectional | Any | veAutoDiscADScanPort - Discovery of devices, close after |
| **9000 – 9511** | Multicast | UDP | Bidirectional | Camera/client | multicast port range |
| **12345** | AD Discovery | UDP | Bidirectional | Any | autoDiscADPort12345 - Discovery of devices, close after setup |
| **27000 – 27010** | Centralized Licensing | TCP | Bidirectional | vAS or SAS | Centralized Licensing for VideoEdge |
| **32200 – 38199** | victor Client UDP communication | UDP | Bidirectional | victor Client | Default VideoEdge UDP port range (for victor Client connections) |

5: VideoEdge port assignments (Continued)

| Port | Process / Service | Protocol | Direction | Destination System | Description |
|---|---|---|---|---|---|
| **32200 – 38199** | AD Discovery | UDP | Bidirectional | Any | veAutoDiscMDNS - Discovery of devices, close after setup |
| **32200 – 38199** | AD Discovery | UDP | Bidirectional | Any | veAutoDiscScan - Discovery of devices, close after setup |
| **32200 – 38199** | AD Discovery | UDP | Bidirectional | Any | veAutoDiscSSDP - Discovery of devices, close after setup |
| **32200 – 38199** | UPnP | UDP | Bidirectional | Any | nvrupnpn |
| **32200 – 38199** | AD Discovery | UDP | Bidirectional | Any | veAutoDiscSSD - Discovery of devices, close after setup |
| **32200 – 38199** | AD Discovery | UDP | Bidirectional | Any | veAutoDiscWSDi - Discovery of devices, close after setup |
| **55555** | Transmit manager | TCP | Bidirectional | VideoEdge NVR | Remote Transcoding |

The following table lists the port assignments for victor integration software.

Table 6: Integration port assignments

| Port | Process / Service | Protocol | Direction | Destination System | Description |
|---|---|---|---|---|---|
| **80** | Dedicated Micro | TCP | Bidirectional | Dedicated Micro Recorder | Dedicated Micro video recorder |
| **1001** | Elpas | TCP | Bidirectional | Elpas | Elpas real time location |
| **1025 – 65535** | DMP | TCP | Bidirectional | Intrusion Panel | DMP communication |
| **1025** | Sur-Guard | TCP | Bidirectional | Sur-Guard | Sur-Guard communication |
| **2004 – 2005** | KONE Elevator | TCP | Bidirectional | KONE Elevator | KONE Elevator |
| **3001** | Commend | TCP | Bidirectional | Commend Server | Commend Intercom server |
| **3072** | ITV2 | TCP | Bidirectional | DSC PowerSeries | ITV2 – DSC PowerSeries Neo,<br>Command port number is 3072,<br>Alarm port number can be 1-5 digits |
| **4040, 5050, 6060** | Schindler Elevator | TCP | Bidirectional | Schindler Elevator | Schindler Elevator,<br>Port 6060 is for live reporting |
| **5001** | TOA | TCP | Bidirectional | TOA Server | TOA Intercom server |
| **5050** | Mastermind | TCP | Bidirectional | Mastermind System | Mastermind Alarm Management |
| **7800** | Bosch | UDP | Bidirectional | Bosch | Bosch receiver port |
| **7900** | Bosch | UDP | Bidirectional | Bosch | Bosch receiver port |
| **8038 – 8041** | ThyssenKrupp Elevator | UDP | Bidirectional | ThyssenKrupp Elevator | ThyssenKrupp Elevator |
| **8801 – 8802** | Entrapass | TCP | Bidirectional | Entrapass Server | Entrapass Access Control.<br>Use port number 8802 for HTTPS. |
| **8985** | Base Address pf Driver Service | TCP | Bidirectional | vAS | location = Server<br>Base for drivers for VideoEdge, Intellex, etc. used to drive communication |
| **10001-10002** | serial | TCP | Bidirectional | Lantronix | DSC serial through Lantronix and Simplex 4100U serial through Lantronix |
| **10001-10002** | Galaxy | TCP | Bidirectional | Honeywell Galaxy panel | Honeywell Galaxy Panel/Alarm Port,<br>Command port number is fixed port number 10001<br>Alarm port number can be 1-5 digits |
| **22609** | HDVR Admin/Line/Alarm Port | TCP | Bidirectional | HDVR | HDVR Admin/Line/Alarm Port |
| **30000** | CEM | TCP | Bidirectional | CEM CDC server | CEM Access Control |
| **45303, 45307, 45308, 46307, 46308, 47307** | Otis Elevator | UDP | Bidirectional | Otis Elevator | Otis Elevator |
| **47808** | MZX | UDP | Bidirectional | MZX | MZX fire detection integration |
| **47808** | BACNet | TCP | Bidirectional | BACNet controller | BACNet Building Management |

### 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 victor or victor Web system 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 you can build the appropriate level of protection into the network design to protect both the network and endpoints. Keep in mind that some of the system components, while compatible with victor Web, may not support the same level of protection. In those cases, compensating controls may be utilized within the network design to reduce risk.

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

### 1.7.1 Trust boundaries overview

A trust boundary within a system is the boundary in which data is passed between components that do not share an equal level of trust. Products that are not part of the victor or victor Web system or do not provide methods to sufficiently authenticate a component or user may be regarded as having a lower of level of trust. Networks may also have different levels of trust. For example, you may opt for an isolated network with only video cameras and NVRs, which is usually trusted more than a shared use network such as the corporate IT network or a remote network.

When the trust deviation is beyond the risk tolerance, it is best to control the flow of data between trusted and untrusted network using a switch or router with data flow control capabilities, such as a firewall.

### 1.8.0 Patch policy

The policy documented here sets forth the current internal operating guidelines and process, which may change from time to time at the sole discretion of Johnson Controls. Johnson Controls employs commercially reasonable efforts to pursue the operating guidelines and process described herein. However, other mitigating factors may prevent complete adherence to this policy, as determined by Johnson Controls at its discretion. Regardless, Johnson Controls endeavours to address issues that arise with the severity that they warrant.

When CRITICAL security vulnerabilities are discovered within victor Web, Johnson Controls will use commercially reasonable efforts to issue a Critical Service Pack for the current version as soon as is reasonably practicable.

When non-CRITICAL vulnerabilities are discovered within victor Web, Johnson Controls will use commercially reasonable efforts to:

- Apply fixes for HIGH severity vulnerabilities in the next immediate release
- Apply fixes for LOW and MEDIUM vulnerabilities within one of the next two available releases

Note: In line with industry recognized security best practices, backporting of victor Web enhancements and fixes to prior releases is not supported. Updates are only applied to latest version of the released product.

### 1.9.0 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.

You should 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:

1.9.1 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.

1.9.2 Remove or rename default user accounts (as permitted)

By removing or renaming default user accounts, the ability to gain unauthorized access to the system will be reduced as those attempting to do so will need to enter an unpublished username which is much harder to gain knowledge of.

1.9.3 Change default passwords

During installation, all default user accounts that have not been replaced must have their password changed.

1.9.4 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. You can strengthen a password with length and complexity. The length of a password has the biggest impact on making password guessing difficult.

Each User Account password must meet the following criteria (at a minimum):

- 8 Total characters (For additional hardening, create passwords of at least 12-15 characters)
- 1 Special character (such as $, !, &, #, %, ^, etc.)
- 1 Upper case character
- 1 Lower case character
- 1 Number between 0-9
- Cannot be a common dictionary word

1.9.5 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 victor Web vAS begins prior to deployment with careful planning as outlined in section 1 of this guide. It is a good practice to review section 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
- Default security behavior
- Resetting factory defaults
- Considerations for commissioning
- Recommended knowledge level

### 2.2.0 Hardening

While victor Web vAS has several secure-by-default safeguard, you must harden victor Web vAS to meet the security requirements of the target environment.

2.2.1 Hardening checklist

□ Hardening Step 1: Apply Operating System updates

□ Hardening Step 2: Configure Web Server Security Settings

□ Hardening Step 3: Configure IIS Logging

□ Hardening Step 4: User Account hardening

2.2.2 Operating system updates

*Hardening Step 1: Apply Operating System updates*

To reduce attack surfaces on the operating system regularly ensure that the victor Web vAS software is up to date. For further hardening, you may also follow guidance from the Center for Internet Security (CIS) https://www.cisecurity.org/.

victor Unified Client checks for available updates:

- Automatically on client start up - When the client connects to a new victor Application Server
- Daily (automatically) if run for more than 24 hours without a restart

You can also check for updates manually from the About page.

### 2.2.3 Hardening victor Webserver Security Settings

Configure the webserver to ease its available resources (RAM, CPU, network sockets, connection queues, IO performance, number of simultaneous users, etc.). This is important to prevent both malicious DOS attacks, and unintended server outages.

#### *Hardening Step 2: Configure Web Server Security Settings*

IIS Web Server limits should be configured to the **default settings** unless your organization has specific requirements to satisfy. For more information on IIS settings see the victor Administration Guide Appendix C (victor v5.7.1 Administration Guide (americandynamics.net))

Specific fields to set to the **default settings** and monitor are the following:

- Limit the size of **request bodies** to the default
- Limit the number of **request header fields** to the default
- Limit the size of **request header fields** to the default
- Limit the **http request line** to the default (Note: maximum URL length, including with all possible query string parameters and their longest possible values, plus the HTTP method keyword's length, plus spaces --- NOTE: around 2000 is considered reasonable; most browsers set 4096)
- Limit the **XML request body** to the default
- Set the maximum **number of simultaneous connections allowed** to the default. This is to ensure that the server has sufficient resources (RAM and CPU) to cope with the demand from multiple user's browsers making multiple connections (for pages, images, etc.) at any given moment. (Find out overhead of the NodeJS thread/process and add any additional RAM used by loaded resources, database connections, etc. May have to measure this with one user, then two, 5, and 10 for example, using an http benchmarking tool that can ensure the connections are simultaneous) RAM on the server. CPU usage will depend on the server's performance, specific organizations and users' workloads.
- Tune the **Request read timeout** to the default (Select the time that you'd expect the largest request/upload to complete in, on a not-so-fast network). This can be tuned further for your network's performance (decrease for faster networks and clients, increase for slower networks and clients).
- IF HTTP PIPELININING IS SUPPORTED: Tune the HTTP Keep-alive timeout value to favor HTTP pipelining as much as possible, within the capacity and expected load of your server.

**NOTE:** Monitor all the above settings regularly, to anticipate performance issues, detect anomalies, and plan future capacity.

### 2.3.0 Secure IIS Logging

Misconfiguring IIS logging can have the following consequences:

- Many of the fields available in Advanced Logging can provide extensive, real-time data and details not otherwise obtainable. Developers and security professionals cannot identify and remediate application vulnerabilities/attack patterns, if this information is not available to them.
- IIS flushes log information to disk, therefore prior to IIS, administrators do not have access to real-time logging information. Text-based log files can also be difficult and time consuming to process. Therefore, If ETW is not enabled, administrators do not have access to use standard query tools for viewing real-time logging information.
- Refraining from moving IIS logging to a restricted, non-system drive will increase the risk of logs being maliciously altered, removed, or lost in the event of system drive failure(s). Hardening Secure ISS Logging Settings

#### *Hardening Step 3: Configure IIS Logging*

Perform the following best practices with respect to IIS logging:

- Ensure Advanced IIS logging is enabled
- Ensure Default IIS web log location is moved
- Enabling Advanced IIS logging
  IIS Advanced Logging is a module which provides flexibility in logging requests and client data. It provides controls that allow businesses to specify what fields are important, easily add additional fields, and provide policies pertaining to log file rollover and Request Filtering. HTTP request/response headers, server variables, and client-side fields can be easily logged with minor configuration in the IIS management console. It is recommended that Advanced Logging be enabled, and the fields which could be of value to the type of business or application in the event of a security incident, be identified and logged.
- Enabling ETW Logging
- IIS introduces a new logging method. Administrators can now send logging information to Event Tracing for Windows (ETW)
- Moving IIS Web Log Location
  IIS will log relatively detailed information on every request. These logs are usually the first item looked at in a security response and can be the most valuable. Malicious users are aware of this and will often try to remove evidence of their activities. It is therefore recommended that the default location for IIS log files be changed to a restricted, non-system drive.

### 2.3.1 User Account Hardening

*Hardening Step 4: User Account hardening*

*Windows User accounts*

When using victor in a workgroup environment, each victor user must also have identical Windows accounts on both the site manager and client machines. Ensure each account contains both username and password.
Note: blank passwords are not accepted by victor

*Operators*

Operators are users of the client. Assign each operator a role which describes their capabilities and privileges.

Operators are authenticated in one of two ways:

- Windows Authentication - requires an assigned Windows principal (domain/workstation name and username) which relates to a Windows OS account.
- Basic Authentication - victor Site Manager manages users accounts without the need for an assigned Windows principal or Windows OS account.

*Active Directory*

Dual modes of user authentication allows users to log in using Active Directory credentials or via a ‘Basic’ method which does not require a domain controller.

Also, using Microsoft Active Directory, operator profiles can be tied to are portable which allows users to move from one victor client to another as their credentials follow them, regardless of the PC.

Restrict what devices and features an operator can access by assigning roles using victor's included policy management. Permissions can be set system wide for a specific camera.

*Database Accounts*

All database account information is set during installation and encrypted.

# 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.  You may require a higher degree of protection 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 runtime data* | | | ✓ | | | | |
| 2 | *Backup configuration data* | | | | ✓ | | | |
| 3 | *Test backup data* | | | | | | ✓ | |
| 4 | *Lock user accounts of terminated employees* | ✓ | | | | | ✓ | |
| 5 | *Remove inactive user accounts* | | | | | ✓ | | |
| 6 | *Update user account roles and permissions* | | | | | | ✓ | |
| 7 | *Disable unused features, ports, and services* | | | | | | ✓ | |
| 8 | *Check for and prioritize advisories* | | | | ✓ | | | |
| 9 | *Plan and execute advisory recommendations* | | ✓ | | | | | |
| 10 | *Check and prioritize software patches and updates* | | | | ✓ | | | |
| 11 | *Plan and execute software patches and updates* | | ✓ | | | | | |
| 12 | *Review updates to organizational policies* | | | | | | | ✓ |
| 13 | *Review updates to regulations* | | | | | | | ✓ |
| 14 | *Conduct security audits* | | | | | | | ✓ |
| 15 | *Update password policies* | | | | | | | ✓ |
| 16 | *Update as build documentation* | ✓ | | | | | | ✓ |
| 17 | *Update standard operating procedures* | | | | | | | ✓ |
| 18 | *Update logon banners* | | | | | | | ✓ |
| 19 | *Renew licensing agreements* | | | | | | | ✓ |
| 20 | *Renew support contracts* | | | | | | | ✓ |
| 21 | *Check for end-of-life announcements and plan for replacements* | | | | | | ✓ | |
| 22 | *Periodically delete sensitive data in accordance to policies or regulations* | ✓ | | | | | ✓ | |
| 23 | *Monitor for cyber attacks* | ✓ | | ✓ | | | | |

### 3.1.1 Backup runtime data

If you need to restore or replace a configuration of victor Web vAS system for a particular customer, it is important to have a backup of its configuration data to minimize the time required to restore functionality.

### 3.1.2 Backup configuration data

If you need to restore or replace a component it is important to have a backup of its configuration data to minimize the time required to restore its functions. If you need to restore or replace a component it is important to have a backup of its configuration data to minimize the time required to restore its functions. Please not that a manual record of the encryption configuration will help assure that the system can be reconstituted should a self-encrypting drive need to be restored.

### 3.1.3 Test backup data

Test backups to provide assurance that the data backups contain the expected data and integrity. Disable accounts on termination of employment

Disable user accounts of personnel who voluntarily or non-voluntarily are terminated from employment immediately.

### 3.1.4 Lock user accounts of terminated employees

Disable user accounts of personnel who voluntarily or non-voluntarily are terminated from employment immediately.

### 3.1.5 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 you should remove their user account. This is sometimes referred to as a use it or lose it policy. This best practice reduced the amount of active user accounts in the system and therefore lowers the potential attack footprint.

### 3.1.6 Update user accounts roles and permissions

While an employee may still be employed by an organization that owns, manages, or services the system, they may have changed roles or have increased or decrease their need to use the system. When you add a role or a permission to a user's account when that user is granted new authorizations due to an organizational role change, be sure to update roles and permissions no longer required or used in their new role.

### 3.1.7 Disable unused features, ports and services

If you no longer require optional features, ports, and services disable them. This practice lowers the attack surface of victor Web vAS resulting in a higher level of protection.

### 3.1.8 Check for and prioritize advisories

You can find security advisories for victor Web vAS on the Cyber Protection website. Access is provided once you have registered a user account with that site. User account registration is open to JCI customers and authorized representatives. Determine if victor Web vAS is impacted by the conditions outlined in the advisories. Based on how the victor Web vAS system is deployed, configured, and used, the advisory may not be of concern. Referring to as-built documentation of the victor Web vAS system will help with this assessment. A good set of as-built documentation will help you 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 your planning to ensure that any issue impacting your 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.

### 3.1.9 Plan and execute advisory recommendations

If victor Web vAS is impacted by the conditions outlined in the advisories, including those from third party components, 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 victor Web vAS is deployed into. Plans for executing the advisory recommendations must consider the Hosting platform and environment.

### 3.1.10 Check and prioritize patches and updates

While a victor Web vAS 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.

### 3.1.11 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 in order to minimize service disruptions.

### 3.1.12 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

### 3.1.13 Review updates to regulations.

If victor Web vAS 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.

### 3.1.14 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.

### 3.1.15 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.

### 3.1.16 Update as build documentation

Update as-build documentation if the deployment architecture or component configuration changes. Some configuration changes happen without a formal project or plan and if such cases it may be common to negate updating the as-built documentation. Schedule a full update of the as-built documentation on a regular basis to ensure that all changes are documented.

### 3.1.17 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.

### 3.1.18 Update logon banners

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

### 3.1.19 Renew licensing agreements

Assure that your victor Web vAS software license supports the necessary functions.

### 3.1.20 Renew support contracts

Assure that your victor Web vAS software support agreement (SSA) is up to date

### 3.1.21 Check for end-of-life announcements and plan for replacements

Review product announcements to determine if any of the components of victor Web vAS have a planned end-of-life announcement.

### 3.1.22 Periodically delete sensitive data in accordance with policies or regulations

Collect details on policies and regulations that apply

### 3.1.23 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 your responsibility to verify that victor Web vAS continues to operate properly after you have installed any security monitoring tools.