Architectural and Engineering Specification for

Video Management Software

Senstar Symphony™

This document is intended to provide performance specifications and operational requirements for the Senstar Symphony video management system. It is written in a generic format. These specifications may be copied verbatim to form a generic procurement specification.

Part 1 General 4
1.1 System Summary 4
1.2 Quality Assurance 4
1.3 References 4

Part 2 Products 6
2.1 Video Management Software 6
2.2 Manufacturers 6
2.3 Architecture Requirements 6
2.4 Security and Privacy Requirements 7
2.5 Network Requirements 8
2.6 Hardware Requirements 9
2.7 Video Standards 10
2.8 Licensing Requirements 10
2.9 Video Management 11
2.10 System Management Administration 22
2.11 Cloud-Based Management and Administration 22
2.12 System Integration 23

Part 3 Execution 25
3.1 System Installation 25
3.2 System Configuration 25
3.3 User Documentation 25
3.4 Training 25

PART 1 GENERAL

1.1 System Summary

The contractor shall install a scalable, standards-based Video Management Software (VMS) solution. The VMS shall include support for native (built-in) video analytics from the same manufacturer.

The VMS shall be installable on commercial-off-the-shelf (COTS) hardware that runs the Microsoft Windows operating system. The solution must be scalable and have automatic failover capabilities that do not require Microsoft Clustering technology.

The solution shall follow a flexible, per-camera licensing model in which additional cameras can be added to the system on a per-camera license basis, without the need to purchase a group of camera licenses or other type of license.

1.2 Quality Assurance

A. The VMS manufacturer shall perform a vulnerability assessment of its software.

B. The VMS manufacturer shall perform penetration (PEN) testing of its software deployed in a standard configuration.

1.3 References

The following acronyms and abbreviations are used in this document:

- AGC: Automatic gain control
- API: Application Programming Interface
- COTS: Commercial-of-the-shelf
- DHCP: Dynamic Host Configuration Protocol
- DNS: Domain Name System
- EIS: Electronic Image Stabilization
- FPS: Frames per Second
- FTP: File Transfer Protocol
- H.264 (Video Compression Format)
- IP: Internet Protocol
- IR light: Infrared light
- JPEG: Joint Photographic Experts Group (image format)
- LAN: Local Area Network
- LED: Light Emitting Diode
- Lux: A standard unit of illumination measurement
- MPEG: Moving Picture Experts Group
- NTP: Network Time Protocol
- NTSC: National Television System Committee
- ONVIF: Open Network Video Interface Forum
- PAL: Phase Alternating Line

- PoE: Power over Ethernet (IEEE 802.3af/at)
- PTZ: Pan/Tilt/Zoom
- QoS: Quality of Service
- SMTP: Simple Mail Transfer Protocol
- SMPTE: Society of Motion Picture and Television Engineers
- SNMP: Simple Network Management Protocol
- SSL: Secure Sockets Layer
- TCP: Transmission Control Protocol
- TLS: Transport Layer Security
- UPnP: Universal Plug and Play
- UPS: Uninterruptible Power Supply
- VMS: Video Management Software
- WDR: Wide dynamic range

PART 2 PRODUCTS

2.1 Video Management Software

A. The contractor shall supply an IP-based Video Management Software (VMS) solution.

B. The VMS shall include both video management and video analytic capabilities from the same manufacturer.

C. Video management, camera configuration, and video analytics shall be configured from the same user interface.

D. Video management and any alarms or operational data generated by video analytics shall be displayed within same operator interface.

E. The VMS shall be fully integrated with Perimeter Intrusion Detection Systems (PIDS) designed by Senstar Corporation and include the ability to display perimeter and VMS events within the same interface.

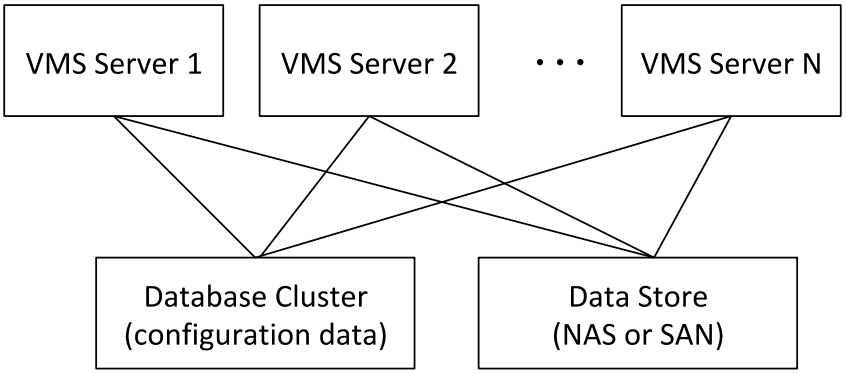
2.2 Manufacturers

A. The Senstar Symphony Video Management System from Senstar Corporation (www.senstar.com) meets the requirements stated in this document.

2.3 Architecture Requirements

A. All VMS software components shall be IP-based and comply with established networking standards.

B. The VMS shall support scalable, enterprise-level deployments that eliminates single points of hardware failure, as shown below.



C. The VMS shall include support for the following top-level components and user interfaces:

1. Server software
2. Web-based configuration interface
3. Microsoft Windows operator client application

4. HTML5-compliant Web-based operator interface with no dependency on plugins
5. Native iOS and Android applications (smartphones and tablets)
6. Cloud-based IT management services
7. Server-based video analytics
8. Camera-based video analytics.

D. Server requirements:

1. The maximum number of supported cameras and video streams per server shall be not be artificially limited by software licensing. The actual camera limit shall be dictated by the performance of the server hardware.
2. The server software shall be capable of running on the following operating systems:
   a. Windows 7 SP1
   b. Windows 10
   c. Windows Server 2008 R2 SP1
   d. Windows Server 2012 and 2012 R2
   e. Windows Server 2016
3. The server software shall be capable of running on virtualization software, including VMWare and virtualization solutions from Microsoft.
4. The server software must support the following storage configurations:
   a. Direct attached storage (DAS)
   b. Network attached storage (NAS)
   c. Storage area networks (SAN)
   d. Edge-based storage (such as network cameras).

E. Data shall support UNC paths and scheduled backup of configuration and data separately.

F. The VMS shall support video analytics in the server running the video management system or embedded in an IP camera or encoder.

G. The VMS shall be extensible and customizable via new component development through a vendor-supplied Software Development Kit (SDK).

H. The VMS shall support r

2.4 Security and Privacy Requirements

A. Data transmission between all core system components shall be fully encrypted to current security standards.

B. Video data transmission shall be securable via the HTTPS protocol and customer SSL security certificates.

C. User access:

1. User security privileges shall be managed directly for a user or through the creation of security groups. Users may be members of more than one security group.
2. Global user groups shall be capable of being fully supported through a cloud-based enterprise management tool.
3. The VMS shall support two-person requirements for specific functions, such as video recording or video export.
4. The VMS shall include controls that limit or block access to video footage based on the time of recording.

D. User Permissions:

1. User privileges shall be customizable through user groups.
2. The VMS shall support different Security Profiles (complete set of all users and associated permissions) that allow administrators to set permissions for a profile under a normal activity. The administrators shall be able to quickly change permissions in case of emergency by selecting new profile groups.
3. Administrators shall have the ability to view active user sessions and to log off users.
4. The VMS shall support supervisor logons that require two users to login together for security requirements.
5. User actions shall be stored by time, location, and/or camera.
6. Access to logging and alerts shall be controlled by user group.
7. The VMS shall have the ability to limit the number of concurrent logons.
8. The VMS shall control user access on a per-camera basis.

E. Audit logging of user actions or server errors shall be stored in plain text or a non-proprietary database.

F. The VMS shall allow privacy masks to be defined per camera on a per user basis. When privacy masks are applied, users with limited permission can view the video but the motion areas are scrambled to protect privacy. Users with the appropriate permission shall view the video with the privacy mask removed.

2.5 Network Requirements

A. The VMS shall be accessible through firewalls with multiple servers on a single IP address masqueraded behind the gateway.

B. The VMS shall support customizable listening ports for client connectivity.

2.6 Hardware Requirements

A. The VMS shall be installable on commercial off-the-shelf hardware such as BCD, Dell, HP, EMC, IBM or equivalent.

B. The VMS manufacturer shall offer pre-built systems, in which the VMS is pre-installed and configured.

C. The VMS manufacturer shall offer a mobile client that runs on iOS and Android devices.

D. The hardware used to run the VMS components shall be:

1. Manufactured in accordance with ISO 14001
2. Compliant with EU directives 2011/65/EU (RoHS) and 2012/19/EU (WEEE)
3. Compliant with EU regulation 1907/2006 (REACH).

E. The hardware devices used to run the VMS components shall carry the following EMC approvals:

1. EN55022 Class B, EN55024, EN61000-6-1, EN61000-6-2
2. FCC Part 15 - Subpart B Class B
3. VCCI Class B
4. C-tick AS/NZS CISPR22 Class B
5. ICES-003 Class B
6. KCC KN22 Class B, KN24

F. The hardware devices used to run the VMS components shall meet the following product safety standards:

1. IEC/EN/UL 60950 -1
2. IEC/EN/UL 60950-22.

G. The hardware devices used to run the VMS components shall meet the following requirements:

1. IEC/EN 60529 IP66/67
2. NEMA 250 Type 4X
3. IEC/EN 62262 IK10+ (50 J)
4. ISO 20653 IP6K9K
5. IEC 60068-2-1
6. IEC 60068-2-2
7. IEC 60068-2-6
8. IEC 60068-2-14
9. IEC 60068-2-27

10. IEC 60068-2-60
11. IEC 60068-2-78.

H. The hardware devices used to run the VMS components shall meet the following railway environment requirements:

1. EN 50121-4
2. IEC 62236-4.

2.7 Video Standards

A. The VMS shall support the following video standards:

1. MJPEG
2. MPEG-4
3. H.264
4. H.265
5. Relevant ONVIF profile as defined by the ONVIF Organization.

2.8 Licensing Requirements

A. The VMS shall follow a flexible, per-camera licensing model in which additional cameras can be added to the system on a per-camera license basis, without the need to purchase a group of camera licenses or other type of license.

B. All camera licenses shall be bound to the server, not the MAC addresses of the cameras. Replacing a camera shall not require that a new camera license to be purchased.

C. Each IP-connected device (camera or other device with an IP address) shall require one license, including multi-sensor cameras and IP encoders.

D. I/O devices shall require only one camera license per device IP address. Individual I/O ports shall not require additional licenses.

E. Support for Perimeter Intrusion Detection Systems (PIDS) from Senstar shall not require additional licensing.

F. The licensing model employed by the VMS shall be as follows:

1. The VMS shall provide licensing options that supports different deployment requirements while maintaining a consistent look and feel.
2. The VMS shall use the following licensing categories:
    a. Standard: Provides basic features for small and mid-sized facilities, including:
        1. View live video
        2. Record video
        3. Interface to I/O devices via dry contacts

4. Microsoft Active Directory support.

b. Professional: Provides the same features as Standard and includes the following additional features:

1. Multi-server integration
2. Access control
3. API/SDK for integration with third-party systems.

c. Enterprise: Provides the same features as Professional and includes the following additional features:

1. Built-in server farm capability for automatic failover, redundancy and load-balancing
2. Video wall capabilities
3. GIS map support.

3. The number of servers, storage devices and clients shall be unlimited, in that the license does not dictate, control, or change depending on their number.
4. Viewing systems do not require license and shall be available on an unlimited basis for each license category.
5. There shall be no cost for mobile devices to connect to the system for viewing.
6. Licenses shall be upgradable to a higher license category (e.g. from Standard to Professional).
7. The camera license shall provide the ability to add analytic capability to a specific camera without requiring all other license to be upgraded.
8. The analytic camera license can be moved from one camera to another without an additional license cost.

2.9 Video Management

A. All viewing clients connected to the system must include support for:

1. Live view
2. PTZ control
3. Recorded video
4. Alarm report
5. I/O status.

B. The VMS shall include the following IP device capabilities:

1. Automatic discovery for cameras on the network.
2. Camera templates to simplify Server set up and administration.
3. Unicast and Multicast IP traffic.

4. Camera resolution and frame rate shall be limited only by the hardware capacity and not the video management software.
5. Support for de-warping of 180 and 360-degree cameras.
6. Analyze all video sources in real time at any bandwidth, frame rate and resolution supported by the camera or IP video encoder devices. Software shall automatically select the most appropriate stream for analysis out of all stream added for the camera.
7. Support for different frame rates for viewing, recording or alarm/analytic video.
8. Support for corridor display (9x16) to maximize view of narrow scenes.
9. Be able to record MJPEG, MPEG-4, H.264, and H.265 video streams from the same camera, as supported by the camera.
10. Software must have the ability to record a different number of days per stream.
11. Support for video, 2-way audio, I/O, PTZ, VMD as well as multiple streams from the following network device manufacturers, when supported by the manufacturer or standard:
    a. Acti
    b. Arecont
    c. Axis
    d. Bosch
    e. Certis
    f. D-Link
    g. Dynacolor
    h. Eneo
    i. Etrovision
    j. Flir
    k. Grundig
    l. HIKVision
    m. IPX
    n. IQinvision
    o. Johnson Controls
    p. JVC
    q. Messoa
    r. Mobotix

s. OnCam-Grand Eye
t. ONVIF Profile S
u. Panasonic
v. Pelco
w. Phoenix Contact
x. RTSP Streaming
y. Samsung
z. Siqura
aa. Sony
bb. Sunell
cc. Toshiba
dd. Vivotek
ee. XTS.

12. The VMS manufacturer shall provide a list of supported video devices.

C. The VMS shall include a Windows client with the following features and capabilities:

1. All operator features available from a single software user interface and in no case requiring multiple software user interfaces.
2. Customizable user interface, including the location of the alarm log, server list, map, camera tree and system log. Authorized users shall be able to save multiple user customization layouts. Layout options include:
    a. Full-screen
    b. Tiled matrix
    c. Floating windows
    d. Dockable windows
    e. Resizing windows.
3. Display live and recorded video:
    a. Up to 25 live video streams from multiple servers per screen
    b. Play back at least four cameras from multiple servers on the same screen at different speeds.
    c. Digital zoom
    d. Digital tracking that follows a zoomed in view of the tracked object when a tracked object appears. If two or more objects are being tracked at the same time, the viewable area shall include the bounded region of all tracked objects.

4. Camera navigation:
    a. Go to PTZ preset
    b. Go to specific camera
    c. Send to clipboard
    d. Send to printer
    e. Send to file
    f. Navigation from maps
    g. View live and archived video streams
    h. Matrix and carousel elements. Different cameras can be configured to be displayed for different amounts time.
5. Multiple monitor support.
6. Camera layout options:
    a. Saved layouts appear in camera tree for easy navigation
    b. Customizable camera tree view spanning one or many physical servers
7. Site map functions:
    a. Support the following image formats for use as site maps: BMP, GIF and JPEG.
    b. Include icons to represent I/O and camera devices, including their current status
    c. Ability to create multiple maps
    d. Ability use hyperlinks to quickly switch between maps
    e. Show the current PTZ viewing angle on the map
    f. Change PTZ viewing angle by clicking on the map
    g. Enable or disable inputs or outputs directly from map.
8. Search options:
    a. Basic search
    b. Time and date
    c. Graphical timeline
    d. Alarm
    e. Smart search (ability to select an area or object in a scene)
    f. Analytic search including:
        1. Direction
        2. Dwell time

3. Area based activity
4. Movement across one or more tripwires in certain directions
5. Tracks the begin or end at a specific location
6. Items left behind or removed
7. License plates
8. Searches can be scheduled to run automatically on a specific interval
9. Deliver search results that:
    A. Include video data with video analytic decorations included (e.g., boxes or contours to identify triggers)
    B. Include a flexible number of seconds pre- and post-event search result
    C. Stitch all qualified video snippets from a camera into a continuous movie (e.g., 20 snippets are stitched together so that you can select play and watch all 20 snippets continuously without interruption)
    D. Provide .JPG images of each qualifying snippet
    E. Each video snippet should be numbered in visible search results
    F. The total number of video snippets results should be visible in the search results

9. Graphical timeline search:
    a. Move to next/previous alarm
    b. Move to next/previous motion
    c. Move to next/previous 10 seconds
    d. Move to next/previous second.
10. Authentication:
    a. Native authentication support
    b. Single sign-on support.
11. Events:
    a. Manually trigger events and outputs
    b. Allow continuous audible alarms until acknowledgement
    c. Audible alerts by motion or event.
12. PTZ support with point-and click controls:
    a. Zoom in/out to marked rectangle

   b. Zoom using mouse.

13. Camera tour support for PTZ devices:
   a. Unlimited camera presets per tour
   b. Go-to preset on event
   c. Automatic pause and resume option
   d. Set multiple patrolling schedules per camera per day
   e. Unlimited number of camera tours.
14. Printing capabilities via the Windows printer subsystem:
   a. Images
   b. Audit logs.
15. Export:
   a. Multiple cameras in the same export package
   b. MPEG
   c. MPEG-4.
16. Public and private bookmarks of events
17. Reporting:
   a. Object counts across a line
   b. Heat map (created by meta-data) with object paths, counts and dwell time
   c. Object count change over time as a graph
   d. Object count tables
   e. Alarm summary reports
   f. Reports can be scheduled to run at certain intervals and deliver results to an email list
   g. Reports shall be exportable to PDF, HTML or Text
   h. Report fundamental data should be exportable to Microsoft Excel.
18. Alarm handling:
   a. Centrally manage alarms from multiple sensors, including video analytics, access control, alarm I/O, and Senstar sensors:
   b. Provide real-time feedback to multiple monitor agents connected to the system when alarms have been viewed by other monitoring agents.
   c. Provide immediate feedback about comments to alarms.
   d. Alarms can be handled using the following methods:

1. FTP
2. Email
3. TCP/IP
4. OPC
5. SNMP.

19. Rules engine:
    a. Shall be capable of starting, stopping or triggering action based on activity such as motion, analytics, access control or intrusion activity.
    b. Actions for events within the rules shall include:
        1. Send a message via alarm, email, etc.
        2. Initiate camera recording
        3. Display camera
        4. Send a PTZ camera to a preset
        5. Trigger an I/O device
        6. Start a script.
    c. Rules can be enabled or disabled through the client interface.
    d. Rules can be turned on or off from a schedule.

D. The VMS shall include a web-based administration interface with the following features and capabilities:
    1. Support for the following HTML5-compliant web browsers (no required browser plugin):
        a. Windows Edge
        b. Google Chrome
        c. Apple Safari
        d. Firefox
    2. Access to all administrative settings
    3. Camera set up including recording and scheduling
    4. Ability to create and administer camera templates
    5. Analytic setup (if done through the server)
    6. Alarm setup and rules programming
    7. Server-based groups and views
    8. Secure user authentication.

E. The VMS shall include a web-based operator interface with the following features and capabilities:
   1. Support for the following HTML5-compliant web browsers (no required browser plugin):
      a. Windows Edge
      b. Google Chrome
      c. Apple Safari
      d. Firefox
   2. Remote view of live or recorded video for up to 16 concurrent cameras
   3. Ability to run reports such as heat map or people counting
   4. Camera navigation with site map
   5. Graphical timeline
   6. Messages
   7. Reports
   8. Secure user authentication.

F. The VMS shall support a thin client video appliance that has the following features and capabilities:
   1. Display live video from the VMS.
   2. Support video playback and export from the VMS.
   3. Decode and display 1080p video on HD monitors using ONVIF or RTSP.
   4. Display live video from any ONVIF-compliant IP camera.
   5. Display live video from any RTSP-compliant IP camera.
   6. Support H.264, MPEG-4 and JPEG compression standards.

G. The VMS shall support a mobile client that has the following features and capabilities:
   1. Included with the VMS at no additional cost
   2. Offers native Android and iOS versions
   3. Displays live and recorded video from the VMS server
   4. Streams JPEGs and H.264 at user-configurable frame/refresh rates
   5. Can transmit video to the VMS for recording by the VMS
   6. Provides a grid view of images from cameras, with the image refresh rate defined by user preference
   7. Provides a searchable list of cameras
   8. Displays video in fast-forward, fast-reverse, and speeds of up to 32X real-time

9. Alarm management capabilities shall include:
    a. Alarm log for alarm review
    b. Alarm event thumbnail view
    c. Historical playback of alarm event
    d. Alarms can be acknowledged (status and comments) from mobile clients
    e. Push notification of alarms (for iOS clients)
    f. User profile defining which alarms are displayed in mobile client on a per user basis
10. Ability to enable or disable digital I/O actions
11. Enable or disable server rules
12. Includes complete online help in supported languages
13. Provides secure SSL authentication and communication connectivity
14. Provides all functionality in both portrait and landscape rotations.

H. The VMS shall include the ability to create extensive rules around analytic activity that include the following:
    1. Trigger action for another camera (such as send PTZ camera to a preset or display another camera.
    2. Trigger action to other integrated systems such as access control or I/O devices.
    3. Send messages to system users text and email.
    4. Video analytic activity shall be able to trigger alarms within the VMS.
    5. Video analytic activity shall be able to trigger video recording.
    6. Server-based video analytics shall have the ability to transfer the analytic license from one camera to another without purchasing another license.
    7. Server-based video analytics shall be independent of camera manufacturer or model.
    8. The VMS shall be ability to record metadata from video analytics at different time lengths than video data.
    9. The Video analytics should run in real-time and should be optimized to allow for the concurrent analysis of up to 32 cameras on a quad core processor at 4CIF resolution.
    10. The following video analytics should be embedded in the VMS and available on a per camera basis:
        a. Object detection
        b. Object removed

c. Object left behind
d. Different analytic rules and masks loaded per location on PTZ cameras
e. Auto-PTZ tracking
f. Auto-PTZ control with a single camera (no human intervention)
g. Use a fixed camera to initiate an auto-PTZ control session
h. Automatically follow an object from a camera that is executing a guard tour
i. Overhead people counting
j. 45-degree people counting
k. Wrong-way detection
l. Anti-tailgating
m. Crowd detection
n. Camera obstruction
o. Camera outage
p. Ability to classify person, vehicle or unknown
q. Anomalous movement detection
r. Zone exclusions
s. Tripwire
t. Tracks that had to begin or end at a specific location
u. Alarm, search and display based on complex contour of an object (not just fixed shapes such as rectangles)
v. Color detection
w. License plate recognition
x. Loitering/dwell time.

11. The VMS shall support edge-based video analytics (installed on a camera or video encoder):
    a. Setup is done through an intuitive browser interface.
    b. Provide seamless integration to the VMS, including support for rules that can interact with devices connected to the VMS.
    c. Include fine tuning parameters to minimize interference from shadows, reflections, fog, and snow.
    d. Supports outdoor object tracking, classification and alarming when used with Axis cameras and encoders equipped with ARTPEC 4+ processors.
12. Video analytics supported by the VMS shall:

a. Accurately detect and track objects while minimizes false alarms.

b. Categorize vehicles and people.

c. Integrate with the VMS rules engine.

d. Support indoor people counting, classification and alarming

e. Tracks bi-directional flow of objects as they pass through a user definable line.

f. Camera should be installed above where objects pass through for best

g. Includes reporting that can be run on an hourly, daily, weekly or annual basis.

h. License Plate Recognition (LPR) video analytics integrated with the VMS shall be able to:

    1. Provide the ability to capture license plate information from an analog or IP video camera (not require a special camera designed for LPR).

    2. Be suitable for vehicle access, traffic control and enforcement applications.

    3. Track vehicle license plate information within the VMS. License plates from different regions and countries shall be recognized and logged.

    4. Provide alarms through the VMS

    5. Support up to 12 FPS for each processor core.

    6. Read plates after analyzing 3 quality video frames, unless traveling at speeds up to 30km/h (18mph), in which 10 FPS may be used.

    7. Require a minimum of pixel size no greater than 32 pixels high for Latin characters and 40 pixels high for non-Latin (Arabic, Chinese) characters.

    8. Function with a camera mounted 5–50 m (16–160 ft) from the spot where the license plate is to be read at a height of 3–9 m (10–30 ft) with an angle of less than 30 degrees.

    9. Function with a camera in line with the vehicle (directly in front or back) or at an angle of less than 15 degrees.

    10. Be configured from within a standard web browser.

i. Facial recognition video analytics integrated with the VMS shall be able to:

    1. Be able to identify people from any analog or IP video camera.

    2. Be able to identify faces with in a scene approximately 20 ft wide.

    3. Provide alarms through the VMS.

    4. Support up to 5 FPS for each processor core.

5. Read faces after 3 video frames.
6. Read faces with a pixel size of 50 Pixels high (face size).
7. Function with camera mounted in line with the face (directly in front) or at an angle of less than 15 degrees elevation.
8. Be configured from within a standard web browser.

2.10 System Management Administration

A. All administrative changes shall be accessible via a standard web browser and not require version compatibility or additional software

B. The VMS shall have the ability to be centrally managed across multiple sites, including performance monitoring, policy settings, software upgrades and cloud-based backups:

   1. Servers shall be capable of being backed up, updated and held to standard policies from the cloud without requiring someone to be on-site.
   2. Client software must be able to be pushed by the server so that manual updates are not required.
   3. Device Packs updates must be deployable from the server and pushed automatically to the clients. Client device packs are needed to support multicast video.
   4. Software updates shall be capable of being automatically managed by the Server without requiring manual user intervention.

C. The VMS shall include the following administration capabilities:

   1. Server farm configuration (master/redundant/failover/overload protection)
   2. Storage
   3. System updates
   4. Database backup and restore.

D. Users shall have the ability to send text messages through the Software which could inform users of upcoming maintenance or act as a collaboration platform where operators can communicate real-time.

2.11 Cloud-Based Management and Administration

A. The VMS shall include the ability to managed from a cloud-based Enterprise Management solution.

B. The Enterprise Management solution shall be hosted by the VMS manufacturer and available on a subscription basis.

C. The Enterprise Management solution shall offer the following functionality:

   1. The monitoring and management of servers, cameras and their associated settings. The solution shall display:

a. Status reporting for offline devices including servers, farms, storage, Thin Clients and cameras.

b. Key performance characteristics including CPU and memory usage.

2. Software upgrades, database backups and policy setting management.

3. User management

4. A management dashboard interface providing access to system status and settings, including VMS servers, farms, cameras and thin clients.

5. All managed servers shall connect to the Enterprise Management system via SSL encryption with minimal bandwidth and firewall configuration.

6. System capabilities:

   a. Software updates to servers and Thin Clients can be scheduled to run automatically without requiring someone to be on site.

   b. Supports database backups for connected servers.

   c. Servers and associated devices are not required to be on the same network to support Enterprise Manager capabilities.

   d. Supports camera templates for updating and maintaining stream parameters within a camera group.

   e. Capable of performing batch level firmware upgrades and password changes to multiple camera manufacturers without requiring someone on site.

   f. Enterprise Manager shall support multiple server groups and settings to maintain policies within each user group.

7. User access:

   a. Access to Enterprise Manager is available through a standard browser (not requiring additional software).

   b. Shall require User Name and Password for login.

   c. Users can be defined and managed centrally allowing for creation, modification and removal of users.

   d. Provides the ability to create user groups to change or view settings in Video Management system, analytics and cameras.

   e. Enables administrators to change login settings on remote servers.

2.12 System Integration

A. The VMS shall support the integration with third-party systems via a vendor-supplied Software Development Kit (SDK).

B. The VMS shall include built-in support for the Senstar Network Manager software.

C. The system shall enable a deployment to be pre-configured off-site, so that the VMS software can become fully functional after installation with minimal on-site configuration.

PART 3 EXECUTION

3.1 System Installation

A. The system shall be installed in accordance with the manufacturer's recommended procedures as defined in the manufacturer's documentation for the system.

3.2 System Configuration

A. The system shall be configured in accordance with the manufacturer's recommended procedures as defined in the documentation for the system.

B. If bundled with a hardware platform, the system may be configured prior to delivery and installation.

C. All device firmware shall be the most-recent provided by the device manufacturer, or of a version specified by the VMS manufacturer.

3.3 User Documentation

A. The manufacturer shall provide user documentation that explains how to install, configure, operate and maintain the software.

B. The installer shall provide the following deployment-specific documentation:

   a. Video surveillance schedule, including all camera names, definition, location, resolution, framerate, recording profile and associated alarms.

   b. Server and storage calculations completed with a video management system design tool. Calculations shall be based on the following:

      1. Type A cameras at 1280X720 resolution, 8 FPS, and 14 days storage

      2. Type B cameras (two video streams):

         A. Stream one: 1920x1080 resolution, 8 FPS, and 30 days storage.

         B. Stream two: 640x360 resolution, 10 FPS (for video analytic processing and no recording)

   c. Schedule listing server, storage, power, and UPS requirements based on server and storage calculations described in section 3.3.B.b.

3.4 Training

A. The manufacturer shall provide training materials that provide instruction in the installation, configuration, and operation of the system.

B. The manufacturer shall offer professional training services to assist the organization in meeting their training requirements.