IDIS Solution Suite

Architectural and Engineering Specifications

Version 2.8.1

(Apr.22.2022)

**Division 28 – Electric Safety and Security**

**Level 1 – 28.20.00 – Electronic Surveillance**

**Level 2 – 28.23.00 – Video Surveillance**

Table of Contents

[1 PART 1 - General 3](#_Toc101529270)

[1.1 Summary 3](#_Toc101529271)

[1.2 Administrative Requirement 3](#_Toc101529272)

[1.3 Submittals 3](#_Toc101529273)

[1.4 Quality Assurance 4](#_Toc101529274)

[1.5 References 4](#_Toc101529275)

[2 PART 2 – System Description 5](#_Toc101529276)

[2.1 Manufacturer 5](#_Toc101529277)

[2.2 General Description 5](#_Toc101529278)

[2.3 System Requirements 6](#_Toc101529279)

[2.4 System Diagram 8](#_Toc101529280)

[3 PART 3 – VMS Features 10](#_Toc101529281)

[3.1 Software Features 10](#_Toc101529282)

[3.2 Product Features 22](#_Toc101529283)

[3.2.1 Administration Service 22](#_Toc101529284)

[3.2.2 Recording Service 22](#_Toc101529285)

[3.2.3 Streaming Service 22](#_Toc101529286)

[3.2.4 Monitoring Service 22](#_Toc101529287)

[3.2.5 Video Analytics Service 22](#_Toc101529288)

[3.2.6 Update Service 23](#_Toc101529289)

[3.2.7 Backup Service 23](#_Toc101529290)

[3.2.8 Recording Redundant Service 23](#_Toc101529291)

[3.2.9 Video Wall Service 24](#_Toc101529292)

[3.2.10 Federation Service 24](#_Toc101529293)

[3.2.11 Failover Service 24](#_Toc101529294)

[3.2.12 Mobile Service 25](#_Toc101529295)

[3.2.13 Web Service 25](#_Toc101529296)

[3.2.14 Person Match Service 25](#_Toc101529297)

[3.2.15 RTP Streaming Service 26](#_Toc101529298)

[4 PART 3 - Execution 26](#_Toc101529299)

[4.1 Preparation 26](#_Toc101529300)

[4.2 Installation 26](#_Toc101529301)

[4.3 System Software 26](#_Toc101529302)

[Appendix. A. User Audit Log Table 28](#_Toc101529303)

[Appendix. C. System log Table 31](#_Toc101529304)

[Version History 42](#_Toc101529305)

# PART 1 - General

## Summary

1. The VMS shall include but not limited to the following applications:
	1. Server Software Applications
		1. IDIS Solution Suite Expert: Standard package
		2. IDIS Solution Suite Add-On: Add-on package
	2. Client Software Applications
		1. IDIS Solution Suite Client
		2. IDIS Solution Suite Video Wall Agent (Client)
		3. IDIS SSM : free mobile VMS client
		4. IDIS Player: the clip-copied image video player
2. Related Requirements:
3. Section 28.23.13 – Video Surveillance Control and Management Systems
4. Section 28.23.16 – Video Surveillance Monitoring and Supervisory Interfaces
5. Section 28.23.19 – Digital Video Recorder and Analog Recording Devices
6. Section 28.23.23 – Video Surveillance Systems Infrastructure
7. Section 28.23.26 – Video Surveillance Remote Positioning Equipment

## Administrative Requirement

1. Coordination
	1. Coordinate with owner regarding camera network configuration and estimated bandwidth utilization prior to connection of cameras to owner’s network.

## Submittals

Submittals described in this section shall be submitted by the Contractor with the original bid.

1. Product Data
	1. Submit manufacturer technical specifications, typical installation drawings, system overview drawings and sample images of items included in this section.
2. Proposal Delta
	1. It is the duty of the contractor to provide a working system. Any omissions or errors or differences between this document and the contractor’s submitted proposal shall be clearly outlined in a separate document labeled “[\*COMPANY NAME] Proposal Deltas”.
3. Qualification Statements
	1. Manufacturer
		1. Submit confirmation and details of manufacturer’s warranty, extended warranty, and replacement policies.
		2. Submit proceeding [\*3 years] financial statements for the equipment manufacturer.
		3. Submit list of available manufacturer provided, fee based professional services available to the contractor or the owner including but not limited to: training, installation, commissioning, remote diagnostics and integration with 3rd party software and hardware systems.
	2. Contractor
		1. Submit confirmation that contractor is licensed to install video surveillance and security equipment as required by the authority having jurisdiction.
		2. Submit history of contractor certification(s) for items in this section.
		3. Submit references with contact information where contractor has installed items in this section.
		4. Submit confirmation that installer [\*Entity who will install this equipment or who will supervise installation of this equipment] has received manufacturer training and is certified by the manufacturer on this equipment and that the training the installer received is current.
		5. Submit proceeding [\*3 years] financial statements for the contractor.

## Quality Assurance

1. Manufacturer
	1. Manufacturer shall have been in business for more than 20 years.
2. Installer
	1. Certification for authorized integrators/electronic technicians shall include at a minimum the installation and service of the equipment provided.

## References

1. Abbreviations and Acronyms
	1. API – Application Programming Interface
	2. DVR – Digital Video Recorder
	3. GUI – Graphic User Interface
	4. NVR – Network Video Recorder
	5. SSM – Solution Suite Mobile
	6. VMS – Video Management System (or Software)

# PART 2 – System Description

## Manufacturer

1. IDIS Co., Ltd.

IDIS Tower, 344 Pangyo-ro, Bundang-gu

Seongnam-si, Gyeonggi-do, 463-400, Korea

Tel: +82 31 723 5400

Fax: +82 31 723 5100

## General Description

1. The VMS specified is a highly scalable and fully integrated network video surveillance solution. The VMS can work together with network cameras, DirectIP NVRs, and DirectCX TVRs while providing superior image quality and extensive coverage. The VMS allows you to manage an unlimited number of devices and to customize your surveillance system cost effectively. So, the VMS is suitable for both large enterprise customers as well as smaller surveillance operations for home security and small business. The VMS provides a general purpose network video recording application that will satisfy a wide range of customer requirements without complicated licensing structures. The VMS is the solution for project-based surveillance rollouts as it optionally integrates and transforms to exact customer requirements.
2. The VMS shall be available as a stand-alone software offering or pre-loaded on turn-key workstations and servers running Microsoft Windows with configurable storage.
3. The VMS shall be available in a module based licensed software solution as follows:
	1. Expert (Standard) Services
		1. Administration Service
		2. Recording Service
		3. Streaming Service
		4. Monitoring Service
		5. Video Analytics Service

+ IDLA Service

* + 1. Update Service
		2. Client application
	1. Add-On Services
		1. Backup Service
		2. Recording Redundant Service
		3. Failover Service
		4. Video Wall Service
		5. Federation Service
		6. Mobile Service
		7. Web Service
		8. Person Match Service
		9. RTP Streaming Service
1. Licensing : USB dongle(Wibu-Key) or Software license.

## System Requirements

1. Server System.

The VMS shall operate on all of the following systems.

Recommended Spec.

OS :

1. Microsoft Windows 7 (Home Premium, Professional, Ultimate)
2. Microsoft Windows 8 (Pro, Enterprise)
3. Microsoft Windows 8.1 (Pro, Enterprise)
4. Microsoft Windows 10 (Home, Pro)
5. Microsoft Windows 11 (Home, Pro)
6. Microsoft Windows Server (2012/2016/2019)

CPU : Intel Core i5-3570 3.30GHz / Intel Xeon E3 or faster (4cores or more)

RAM : 8GB or more

VGA : AMD Radeon HD 2400 or NVIDIA GeForce FX5500 (AMD recommended) (1280x1024, 32bpp or higher)

HDD : 2GB or more free space for each service (for example, 4GB or more free space when installing administration and monitoring services)

LAN : Gigabit Ethernet or faster

1. Client System.

The VMS Client shall operate on all of the following systems.



## System Diagram

1. Single-Server System



1. Multi-Server System



1. Multi-Server Federation and Failover System



# PART 3 – VMS Features

## Software Features

1. The VMS shall permit server and client software applications to be installed and run on both the same computer or on separate computers.
2. The VMS shall support the remote monitoring of live image in multiple clients systems through a streaming service. The number of channels that can be streamed equals the number of channels that can be recorded unless streaming WIBU-Keys have been added.
3. The VMS shall support the stable streaming by using the load balancing function in installation with more than one streaming server.
4. The VMS shall remotely upgrade software and setup multiple systems which provide this feature.
5. The VMS shall display the system log information of devices which use IDIS own protocol.
6. The VMS shall monitor the map image on live monitoring screen.
7. The VMS shall support the centralized system operation, management and event-handling.
8. The VMS shall support the enhanced security using SSL function.
9. The VMS shall support two-way audio communication and audio broadcasting.
10. The VMS shall support the enhanced security by setting up different authorities for each user group.
11. The VMS shall be controlled by IDIS network keyboard.
12. The VMS shall support text-in and alarm function via TCP networking.
13. The VMS shall support receiving digital input triggers and triggering digital outputs through an I/O board.
14. The VMS will provide the mechanism by which individual alarm(s) from a 3rd party system (access control, etc.) can be pre-selected and configured to be monitored, and in turn trigger event driven video operations.
15. The VMS shall support an intuitive GUI.
16. The VMS shall support the following features for network cameras and network video transmitters:
	1. Recording of video and playback of the recorded video
	2. Multiple recording servers for advanced recording performance
	3. Instant Recording/Panic Recording of monitored images
	4. Audio recording
	5. Stable recording using proprietary video database le system
17. The VMS shall support the following features for DVRs:
	1. Playback of video recorded in DVRs
	2. Remote control of panic recording
18. The VMS mobile client shall be free and supported by Android and Apple mobile devices.
19. The VMS shall be available in the following languages:
	1. English
	2. French
	3. German
	4. Italian
	5. Spanish
	6. Croatian
	7. Portuguese (Portugal)
	8. Swedish
	9. Finnish
	10. Russian
	11. Chinese (Simplified)
	12. Chinese (Traditional)
	13. Japanese
	14. Korean
	15. Turkish
	16. Dutch
	17. Czech
	18. Polish
	19. Hungarian
20. The VMS shall support dynamic video stream management architecture which includes:
	1. Support for industry standard compression formats including but not limited to:
		1. MJPEG
		2. MPEG-4
		3. H.264
		4. H.265
	2. The client and server machine shall communicate resolution real estate such that the server machine acts as a video proxy and shall know the maximum monitor resolution supported by the client machine.
	3. Support for reducing the required client bandwidth and processing power of a megapixel video stream by transmitting only the fraction of the video stream that is visible in the video display tile. (e.g. If a user is viewing a 2MP camera in a 352x240 resolution tile then a CIF representation of the 2MP image shall be transmitted).
	4. Dynamic video stream management shall be supported for local users, remote users and mobile devices.
21. The VMS shall support recording and management of video and audio sources including but not limited to:
	1. IDIS IP Cameras and Encoders
	2. Axis Cameras
		1. Axis Encoders are not supported.
	3. IQInvision Cameras
	4. Mobotix Cameras
	5. Panasonic BB Cameras
	6. Panasonic WV (DG) Cameras
	7. Pelco Cameras
	8. Basler Cameras
	9. Sony Cameras
	10. 360 Vision Cameras
	11. ONVIF Cameras
	12. RTSP / RTP Video Streams
22. The VMS shall support recording and monitoring video and audio streams from sources with bandwidth up to 200Mbytes/sec, frame rate up to 30 fps, and video resolution up to 12MP. This specification depends on the performance of server or workstation including HDD performance.
23. The VMS shall support the decompression of H.264 and H.265 video through the quick sync video technology of Intel based client graphics card/graphical processing unit (GPU) instead of using the client processing power.
24. The VMS shall require no proprietary recording hardware, no hardware multiplexer or time-division technology for video and audio recording or monitoring.
25. The VMS shall support the storage capacity with up to 50TB per partition and shall allow for upgrades of recording capacity without additional licensing.

The VMS shall support max 74 partitions per one Recording Service.(Logical Drive Partition 24ea + Physical Drive Partition 50ea)

1. The VMS shall secure video and audio data by securely transmitting all command and control data via TCP/IP using cryptographic keys based on SSL to prevent eavesdropping or tampering.
2. The VMS shall support software level integration via an API. The API integration shall include but not limited to:
	1. Bi-directional alarm event processing for monitoring and acknowledgement
	2. Receiving digital input events
	3. Receiving intrusion zone events
	4. Transmitting live and recorded video
3. The VMS shall support integration with the following systems:
	1. Tyco(Software House)’s CCure 9000
	2. Lenel’s OnGuard
	3. Gallagher Command Centre
	4. Inner range Integriti
	5. DAVANTIS Daview S/LR
4. The VMS client shall provide alarm management operations through the use of the client graphical user interface. Including but not limited to:
	1. Occurrences for “Alarm” and “Reset” conditions for each of the pre-selected access system alarms will be processed and managed from the VMS system’s Live View workspace.
		1. In a section reserved for displaying alarm notifications or from an alarm viewer.
		2. Alarms can also be acknowledged from the camera display tile.
	2. Once an initiated alarm occurrence is acknowledged from the VMS system, it should be automatically acknowledged and processed in the access system alarm monitor queue without further operator intervention.
5. The VMS shall have an easy process for upgrading versions:
	1. Are capable of being upgraded from one version to another without having to uninstall the previous version.
6. The VMS shall run as a service configured to automatically start when the server or workstation is powered on, and automatically recover from failure or attempted tampering.
7. The VMS shall allow users to monitor and administer the system from:
	1. A single client application for monitoring live and recorded video and audio.
	2. A single window for administrating all system connections.
	3. Any client located on the network.
8. The VMS shall provide an automatic discovery solution that will easily find devices and systems by:
	1. Automatically discovering server instances that run on computers connected to the same network as the client.
	2. A search functionality to discover server instances running on computers connected on a different network segment than the client by using IP addresses or hostnames.
	3. Automatically discovering video and audio sources that are connected to the same network as the server.
	4. A search functionality to discover video and audio sources that are connected on a different network segment than the server.
9. The VMS shall allow manually discovered server instances, video and audio sources to be visible to all users of a single client workstation.
	1. Network settings for all server instances will be identical for all users of a single client workstation.
10. The VMS shall provide multiple methods for providing fault tolerant solutions to maintain high availability recording in mission critical installations including:
	1. The ability to maintain a centralized system administration so that the same operation and system configuration settings are shared between all servers in a site. This allows the same user login details and other configurations to be used across a site, and ensure that the settings remain active even if a server fails.
	2. The ability to connect a video or audio source to multiple VMSs to achieve redundant recording.
	3. The ability to create a failover connection for a video or audio source. If the VMS that the video or audio source is connected to goes offline then the failover VMS will take over the connection.
11. The VMS shall detect if the video or audio signal is lost and alert the system administrator.
12. The VMS shall provide the capability to rename all video and audio sources and NVRs.
13. The VMS shall record video and audio streams based on a recording schedule that can be defined individually for each video source. The schedule shall include but not limited to the following parameters:
	1. Recording Mode
		1. Continuous (TimeLapse)
		2. Event
			* Motion Detection
			* TripZone
			* Tampering
			* Face Detection
			* Video Blind
			* Auto Tracking
			* Video Analytics
			* PIR Detection
			* Alarm Input / Output (and Network Alarm Input)
			* Audio Detection
			* POS Transactions (Text-In and Network Text-In)
	2. Time and Date Settings
		1. One day
		2. Daily
		3. Weekly
		4. Monthly
		5. Yearly
14. The VMS shall provide the ability to manually trigger recording.
15. The VMS shall provide a pre-event and post-event recording option.
16. The VMS shall provide a continuous recording option in the absence of events.
17. The VMS shall perform motion detection on each individual video source with adjustable sensitivity, threshold and detection zones.
18. The VMS shall perform analytics event detection on each individual video stream sourced from a device possessing adaptive video analytics capabilities.
	1. The VMS shall allow users to connect individual video sources to analytics appliance channels.
	2. The VMS shall allow users to configure events based on classified object motion detection.
	3. The VMS shall allow configured analytics events to be used as alarm and rule triggers.
19. The VMS shall provide the ability to set a maximum recorded video retention time for each video source.
20. The VMS shall perform dynamic bandwidth management to ensure the total bandwidth does not overload the system.
21. The VMS shall authenticate users before granting access to the system. Access rights for each user can be defined individually for each user, and shall include but not be limited to:
	1. Live monitoring
		1. Use PTZ setup and controls
		2. Use audio in/out controls
		3. Use instant recording
		4. Use image processing
		5. Export live images
		6. Trigger manual recording (panic recording)
		7. Use web browser in live tab
	2. Search and Play
		1. Save AVI or ClipCopy images
		2. Export images
		3. Use image processing
		4. Search the recorded data by motion, object or other events
		5. Play manually recorded data (panic record play)
	3. Device Health Monitoring
	4. Use alarm in/out controls
	5. Search and export log data
	6. Search and export event history
	7. Show device and device group
	8. Create user layout
	9. Show POS transaction (text-in) messages
22. The VMS shall provide the ability to rank access rights based on a user’s position within a corporate hierarchy.
	1. Ranked users may only administer changes to users and groups that are subordinate in rank.
	2. The corporate hierarchy can be used to enforce the authority of a parent site over the user and group settings of one or more child sites.
23. The VMS shall allow the creation of site families.
	1. A child site can be connected to an appropriately licensed parent site.
	2. The parent site will have control over the group and user privileges and information of a child site.
24. The VMS shall support multiple credentials to gain access to the system including, but not limited to:
	1. The ability to import members of Active Directory groups as users in the VMS.
		1. Changes made to members in the Active Directory are automatically synced with the VMS.
		2. Users imported from the Active Directory can be added directly to existing permission groups.
	2. Using Windows credentials to authenticate users.
	3. Accept user credentials entered into the VMS user database.
25. The VMS shall provide the ability to schedule backups of recorded video with associated events to a local folder or mapped network drive.
26. The VMS shall provide the ability to create and schedule alarms and corresponding actions including:
	1. Provide the ability to email users and system administrators when an event or system health error occurs.
	2. Provide the ability to schedule when email notifications are sent.
	3. Provide the ability to include camera images in email notifications.
27. The VMS shall maintain a system event log. Including but not limited to the events shown in APPENDIX.A. System Log Table.
28. The VMS shall have the capability to schedule and execute any of the following actions in response to any of the events listed above:
	1. User Notification Actions
		1. Display on-screen message
		2. Send an email
		3. Play a sound
	2. Monitoring Actions
		1. Start live streaming video
		2. Create Bookmark
		3. Start live streaming on a virtual matrix monitor
		4. Open a map on a virtual matrix monitor
	3. Device Actions
		1. Reboot camera
		2. Trigger digital output
	4. PTZ Actions
		1. Go to Preset
		2. Run a Pattern
	5. Alarm actions
		1. Trigger an alarm
		2. Acknowledge an alarm
29. The VMS shall provide the ability to escalate alarms from one user or group to another if the alarm is unacknowledged for a preset duration.
30. The VMS shall provide a maintenance log and audit trail of all system errors and events.
31. The VMS shall support the operation of a Point of Sale system that include:
	1. The ability to receive transaction information from point-of-sale sources.
	2. Support multiple encoding formats from point-of-sale sources.
	3. The ability to monitor live and recorded transactions from point-of-sale sources with linked video.
	4. The ability to generate events based on point-of-sale transaction exceptions.
32. The VMS shall support the operation of a License Plate Recognition system that include:
	1. The ability to define a region of an image where license plate detection is performed. Detected license plates shall be stored with the video data.
	2. The ability to create a Watch List that is used to create events when specific license plates are detected in the images being analyzed.
33. The VMS shall provide the ability to enable and configure PTZ control on the RS-485 interface of a video source.
34. The VMS shall support PTZ protocols and models. Including but are not limited to the following:
	1. IP Cameras
		1. IDIS IP Cameras and Encoders
		2. Axis Cameras
		3. IQInvision Cameras
		4. Mobotix Cameras
		5. Panasonic BB Cameras
		6. Panasonic WV (DG) Cameras
		7. Pelco Cameras
		8. Basler Cameras
		9. Sony Cameras
		10. 360 Vision Cameras
		11. ONVIF Cameras
		12. RTSP/RTP
	2. The VMS shall support more PTZ models and protocols as shown in [APPENDIX. B. ANALOG PTZ MODEL & PROTOCOL SUPPORTED BY IDIS ENCODERs, DVRs or NVRs] using IDIS Encoder, DVR or NVR additionally.
35. The VMS shall provide the ability to change the network settings for a video and audio source including:
	1. A change in image quality and image rate parameters for a single video source shall not affect the settings of other video sources.
	2. The ability to enable a secondary stream for live viewing.
	3. The ability to change the exposure, iris, IR filter, backlight compensation, gain, sharpening, noise filtering, saturation, focus, and white balance settings for a video source.
	4. The ability to change the image dimensions for a video source.
	5. The ability to rotate the image 90°, 180° or 270° for a video source dependent on camera.
	6. The ability to add privacy zones to a video source to block unwanted areas in the image field of view.
	7. The ability to set a maximum recording duration for manually triggered recording for a video source.
	8. The ability to change the input, output, gain and volume for an audio source.
36. The VMS shall support the use of uni-directional and bi-directional audio.
	1. The VMS shall support full-duplex two-way audio communication.
	2. The VMS shall provide the ability to link any audio source to any video source.
		1. Able to link multiple audio sources to a single video source. But, multiple audio signal output is not supported.
		2. Able to link an audio source to many video sources.
	3. The VMS shall provide the ability to synchronize audio and video on playback regardless of video, audio, network, or storage parameters
37. The VMS shall provide the ability to manage operator access to the VMS and assets, including:
	1. Ability to automatically log in to a VMS.
	2. Ability to override user access to a VMS if there are insufficient licenses.
	3. Ability to automatically log out of a VMS when the application is left idle.
	4. Ability to save and restore the window layout.
	5. Ability to control the system using a PC keyboard, mouse or joystick.
	6. Ability to import and export system settings such as maps, views, web pages, users and groups.
38. The VMS shall support live or recorded video monitoring of 1 to 64 video streams simultaneously on a single monitor with the following standard layouts:
	1. Normal Screen
		1. Full Screen, 2x2, 3x3, 4x4, 5x5, 6x6, 8x8, 1+5, 1+7, 1+11, 1+12, 1+27, 1+32, 2+8, 2+18, 3+4, 4+28, 12+16
		2. Corridor Format: 1x2, 1x3
	2. Wide Screen
		1. 3x2, 4x3, 5x4, 6x5, 7x6, 8x7, 1+2, 1+3, 1+4, 1+5, 1+6, 1+8, 1+10, 2+1, 2+4, 2+12, 4+12, 12+24
		2. Panoramic Format : 1x1, 2x1, 8x1
39. The VMS shall support live or recorded video monitoring in a customizable video display beyond the standard layouts.
40. The VMS shall be able to simultaneously display video streams from maximum 64 client sites.
41. The VMS shall support the ability to bias the displayed video to a lower frame rate or to a lower image resolution if the client network bandwidth or processing power is insufficient for displaying the video at full frame rate and image resolution.
42. The VMS shall support the ability to display image overlays. Including but not limited to the following:
	1. Live
		1. Camera Title, Status Icon, PTZ, Timestamp (Date &Time), Event Alert, Motion Block, Site Name, Face Detection, Text-In messages.
	2. Playback
		1. Camera Title, Recorded Title, Status Icon, ePTZ, Timestamp (Date &Time), Site Name, Face Detection, Text-In messages.
43. The Video Analytics Activity overlay shall provide a color-coded bounding box around moving objects categorized as humans or vehicles.
44. The VMS client software shall:
	1. Maximum four monitors used for monitoring video and audio streams connected to a single workstation.
	2. Support monitoring live and recorded video and audio streams simultaneously on the same monitor.
	3. Support viewing the same live or recorded video stream at different zoom levels and areas of interest.
	4. Support the ability to switch from live to recorded video on demand for an instant replay of recently recorded video.
	5. Support the ability to share the application window display in a joint session with other users for collaborative investigations.
	6. Support the creation various layouts of video streams.
	7. Support the ability to toggle between tiled and full-screen view.
	8. Support the ability to save views.
	9. Support the ability to cycle through views (guard tour) based on a specified interval.
	10. Display all video sources connected to the system.
	11. Support the ability to drag and drop sources from a system tree. Sources include but are not limited to:
		1. A video/audio source for live and recorded display.
		2. A predefined layout view of video/audio sources.
		3. Third party or integrated devices
		4. Web pages
		5. Graphical maps
45. The VMS shall support the ability to configure how the system tree is displayed.
	1. The system tree of video sources, maps, saved views and web pages can be organized into virtual folders that are represented as branches within the Site.
	2. Users can be granted access to individual items or entire folders within the tree.
	3. New items added to a folder automatically inherit the permissions of that folder.
46. Alarm and Digital Output Management:
	1. The VMS shall support monitoring alarms.
	2. The VMS shall support the ability to designate one or more regions/tiles in a window for displaying video directly linked to triggered alarms and rules.
	3. The VMS shall support the ability to acknowledge alarms from the designated video display area.
	4. The VMS shall support the ability to manually trigger digital output:
		1. Through the use of a pre-configured software “button”.
		2. Through the use of a hard-wired dry alarm contact connected to a supported input/output device.
	5. The VMS shall support the ability to assign alarms to users.
	6. The VMS shall support the ability to acknowledge alarms.
	7. The VMS shall support the ability to bookmark alarms.
47. The VMS shall support creating bookmarks for recorded video and audio. Bookmarks can be:
	1. Viewed from multiple sources
	2. Displayed on the timeline during playback
	3. Used as a search criteria for recorded video and audio. Search criteria can include but are not limited to:
		1. Name
		2. Description
		3. Bookmark Creator
48. The VMS shall support the ability to create a map that represents the physical location of cameras and other devices throughout the surveillance system.
	1. Maps shall be created from images stored in standard image formats. Including but not limited to the following:
		1. JPEG
		2. BMP
		3. PNG
		4. GIF
	2. Maps shall have the ability to contain links so as to create a hierarchy of interlinked maps.
	3. Maps shall support the ability to drag and drop a video source from the map into a window for live or recorded video and audio monitoring.
	4. Cameras in a map are highlighted when an alarm linked to the camera is triggered.
49. The VMS shall support physical and digital zooming and panning on live and recorded video streams.
	1. The VMS shall support controlling pan-tilt-zoom, iris, and focus as well as setting presets and patterns.
	2. The VMS shall provide the ability to name pan-tilt-zoom presets.
	3. The VMS shall support the ability to center a PTZ camera’s field of view by clicking anywhere on the video image where the PTZ supports this function.
	4. The VMS shall support the ability to click and drag to define an area for the PTZ camera to optically zoom and center on, where the PTZ supports this function.
	5. The VMS shall support controlling pan-tilt-zoom camera on-screen display and auxiliary controls.
	6. The VMS shall support locking PTZ controls.
	7. The VMS shall support control of a pan-tilt-zoom camera with a network keyboard with joystick.
50. The VMS shall support playback of recorded video and audio.
	1. Forward and reverse playback of recorded video and audio at variable speeds.
	2. Audio and video shall synchronously playback when audio and video sources are linked.
51. The VMS shall support the navigation of recorded video and audio. Including but not limited to the following methods:
	1. Calendar
	2. Timeline
		1. The VMS shall support a timeline that displays all connected video sources and the corresponding motion and recording events.
		2. The VMS shall support a timeline that can display the entire time range down to one second of recorded video and audio.
		3. The VMS shall support a timeline that can synchronize video displayed on multiple tabs to the same point in time.
	3. Events.
52. The VMS shall support searching through recorded video and audio based on various search criteria. Including but not limited to the following parameters:
	1. Bookmarks
	2. Calendar
	3. Timeline (Date & Time)
	4. Event search
		1. Alarm-In
		2. Motion Detection
		3. Video Loss
		4. Video Blind
		5. TripZone
		6. Tampering
		7. Video Analytics
		8. Face Detection
		9. POS transaction (Text-In)
		10. Audio Detection
		11. Device Connection & Disconnection
53. The VMS shall support performing a search through a series of thumbnail images.
	1. Thumbnails can be based on the entire image region or a pre-selected area.
	2. Thumbnails can be stacked to support an automatic secondary search when looking at a large timespan of video.
54. The VMS shall support the ability to take a snapshot of a live or recorded image and export it from the system.
55. The VMS shall support the ability to export recorded video in the following formats including but not limited to:
	1. Video
		1. Self-executable (EXE)
		2. Native (CBF)
		3. AVI
	2. Still Image
		1. JPEG
		2. PNG
		3. BMP
		4. PDF
	3. Print
56. The VMS shall support the ability to export recorded audio in WAV format.
57. The VMS shall support the ability to export a live stream of images in the following formats:
	1. JPEG
	2. PNG
	3. BMP
	4. PDF
58. The VMS shall support the ability to export video in Native format. Native format exported video shall:
	1. Digitally sign recorded video and audio using chained finger print technology so video can be authenticated for evidentiary purposes.
	2. Be able to export video from one or multiple camera streams simultaneously.
	3. Support reviewing of exported video and audio in a secure client.
	4. Support reviewing of backed-up video and audio in a secure client.
	5. Support exporting of video in lower frame-rates than originally recorded.
	6. Include camera properties. Including but not limited to:
		1. Site name
		2. Recorded video time, resolution, frame type and size
		3. POS transactional (Text-In) data
	7. Support additional exporting into Native or open formats.

## Product Features

### Administration Service

1. This service shall manage database information of services, licenses, devices, users and schedules for operating the ISS program.
2. This service shall manage the device up to 1024 per service.
3. This service shall support the live monitoring of video up to 64 users simultaneously.
4. This service shall support the playback of video up to 10 users simultaneously.
5. This service shall support one monitoring service per service.
6. This service shall support the video wall services up to 8 per service.
7. This service shall support the streaming services up to 64 per service for software license, and shall support the streaming services up to 4 per service for USB dongle(Wibukey) license.
8. This service shall support the video analytics services up to 32 per service.

### Recording Service

1. This service shall record video transmitted from the network video device. Recording video continues even if the administration service does not work.
2. This service shall support video recording for network cameras and network video transmitters.
3. This service shall not support video recording for NVR or DVR.
4. This service shall record the video of camera up to 256 per service.

### Streaming Service

1. This service shall transmit the video stream from devices to multiple client systems simultaneously.
2. This service shall stream the video of camera up to 512 per service. (recommended 256 cameras, depend on camera stream bitrate)

### Monitoring Service

1. This service shall notify live events and callback events detected at the device registered in the VMS.

### Video Analytics Service

1. This service shall enable video analytics function. When the settings are configured properly, the video analytics is detected according to the preset rules and the VMS program considers the video analytics as an events. The VMS allows displaying the detection results on the monitoring screen.
2. This service shall manage the device up to 8 cameras per service.
3. IDLA service is one of the Video Analyics services, a function added from IDIS Solution Suite v3.2.0.
	1. IDLA service shall distinguish objects by color and deep learning method, and the distinguished objects are recorded in the Recording service. (Human, Car, Bike)
	2. This shall up to 16ch IP Cameras can be registered in one IDLA service, and up to 64 Video Analytics services (IDLA) can be added to one Admin service.
	3. C. This shall support Intrusion, Loitering, and Line Crossing events, and these event histories are recorded in the Recording service.
	4. This shall search for differentiated objects through Play tab > Meta filtering of IDIS Solution Suite Client.

### Update Service

1. This service shall upgrade all services automatically by running the update service and designating the installation file of the software version to upgrade.

### Backup Service

1. This service shall control backup of recorded video saved in the VMS recording servers, NVRs or DVRs and playback of backed-up video saved in the backup server.
2. The VMS shall perform the backup and playback based on the settings of the administration or federation service. If the backup service is registered on an administration service, the VMS only backs up video saved in the recording servers, NVRs and DVRs which are registered on the administration service. If the backup service is registered on a federation service, the VMS backs up video that is saved in the recording servers, NVRs and DVRs registered on the all administration services that are registered on the federation service.
3. This service shall register maximum of 64 recording service and 512 NVR(DVR) systems per backup service.
4. This service shall register maximum of 1024 channels per backup service depending on the type and number of the license.

### Recording Redundant Service

1. This service shall enhance system stability by recording video redundantly from the recording service. This service has some limitations unlike the recording service or recording failover service.
2. This service shall record video as default profile if the devices do not use the IDIS Solution Suite protocol.
3. This service does not support instant recording.
4. This service shall match the recording service one to one.

### Video Wall Service

1. This service shall allow you to control monitoring on multiple monitors with network keyboards for centralized monitoring in a surveillance center.
2. If this service is registered on an administration service, the VMS shall allow you to control monitoring for devices registered on the administration service.
3. If this service is registered on a federation service, the VMS shall allow you to control monitoring for devices registered on the all administration services that are registered on the federation service.
4. This service shall register maximum of 64 video wall agent systems per video wall service depending on the type and number of the license.
	1. Ask your dealer or distributor about the number of video wall agent system that can be registered using our VMS.

### Federation Service

1. This service shall allow you to monitor live video from devices registered on the administration services and to play back recorded video saved in the recording servers that are registered on the administration services.
2. If a backup service is registered on a federation service, the VMS shall back up video that is saved in the recording servers and DVRs registered on the administration services.
3. If monitoring services are registered on a federation service, the VMS shall allow you to monitor events, which are notified from monitoring services registered on the administration services, in the client system of the federation service.

### Failover Service

1. This service shall enhance system stability using a failover functions:
	1. Administration Failover
	2. Federation Failover
	3. Monitoring Failover
	4. Recording Failover
	5. Streaming Failover
	6. Video Wall Failover
2. This service shall replace the primary service if any problems occur in the service. You can register as many failover services as the number of services.
3. This service shall replace only one of the recording or video wall services when a problem occurs in two or more services. The number of failover services must equal the number of recording or video wall services to replace all services.
4. Mobile Service
5. Web Service
6. Person Match Service
7. RTP Streaming Service

### Mobile Service

1. This shall be a service that provides live streaming and recording by installing the IDIS Mobile Camera app on a mobile phone and transmitting the video captured by the mobile phone to the ISS like an IP camera.
2. Streaming service shall be added to the ISS Admin service.
3. IDIS Mobile Camera app can be installed on Android Mobile Phone through App Store.
4. Each channel follows the third-party license and uses service port 11008.

### Web Service

1. Users can access the ISS using an Internet browser, and Live view is available.
2. Streaming service shall be registered in the same ISS admin service, and registered cameras and NVRs shall be added to the Streaming service.
3. License is not required, service port 8080 is used.
4. Up to 64 users can access one web service at the same time.

### Person Match Service

1. This is one of the Video Analytics services to find similar objects that user selected, during a set period by distinguishing the shape and color of objects.
2. This shall be installed on a separate, independent server, and an NVIDIA GTX 2060 or higher graphics card must be installed.
3. CPU resource heavy operation
4. This shall take recorded image and do Video Analytics, so Recording service or NVR must be added.
5. This function has ‘Recorded Footage’ and ‘Pre-Processed Footage’ Modes.
6. This shall be Intrustion, Loitering, and Line Crossing event support

### RTP Streaming Service

1. This shall be used to access the ISS and receive video streaming from a 3rd party app other than the IDIS Client app
2. Video is transmitted to the client by RTP/RTSP..
3. One RTP streaming service can register 1024ch cameras.

# PART 3 - Execution

## Preparation

1. Prior to installation, the VMS shall be configured and tested in accordance with the manufacturer’s instructions.

## Installation

1. Install system in accordance with manufacturer’s instructions.
2. Perform all work in accordance with acknowledged industry and professional standards.

## System Software

1. Install and test software for the complete and proper operation of systems involved. Assign software license to Owner.
2. The Contractor is responsible for the entire programming and setup of the system such that no additional programming is required. Programming shall include the setup of all available features of the software.
3. Perform a full system back-up at completion of initial programming and deliver the configuration to the Owner.
4. Perform field software changes after the initial programming session to “fine tune” operating parameters and sequence of operations based on any revisions to the Owner’s operating requirements.

# Appendix. A. User Audit Log Table

Based on ver. 2.7.0 over

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
|  | **Type** | **Action** | **Detail action** | **Description** |
| Common | Session | Login | Login Success | User Id, Remote Address |
|  |  |  | Login Fail | User Id, Remote Address, fail reason |
|  |  |  | Logout | User Id, Remote Address |
| Client | Monitoring | PTZ control | Pan Tilt | Device name |
|  |  |  | Zoom | Device name |
|  |  |  | Focus | Device name |
|  |  |  | Iris | Device name |
|  |  |  | Preset Setup | Device name |
|  |  |  | Advanced Menu | Device name |
|  |  |  | Using Network Keyboard | Device name |
|  |  |  | PTZ | Device name |
|  |  | Alarm-Out | on/off | Device name, on/off |
|  |  |  | Beep on/off | Device name, on/off |
|  |  | Color control | Color control | Device name |
|  | Play | Play | Play | Device name, Play begin time |
|  |  | Event Search | Event Search | Device name |
|  |  |  | Textin Search | Device name |
|  |  | Export video | Save clip | Device Name, save period, File name |
|  |  |  | Save avi | Device Name, save period, File name |
|  |  | Bookmark | Add Bookmark | Device Name, Bookmark name, site time |
|  |  |  | Delete Bookmark | Device Name, Bookmark name, site time |
| Service | Setup | Device Setup | Add device | Device name |
|  |  |  | Modify device | Device name |
|  |  |  | Delete device | Device name |
|  |  | DeviceGroup Setup | Add Device Group | Device Group name |
|  |  |  | Modify DeviceGroup | Device Group name |
|  |  |  | Delete DeviceGroup | Device Group name |
|  |  |  | Add User to DeviceGroup | DeviceGroup name, added device name |
|  |  |  | Delete User to DeviceGroup | DeviceGroup name, deleted device name |
|  |  | Layout Setup | Add Layout | Layout name |
|  |  |  | Modify Layout | Layout name |
|  |  |  | Delete Layout | Layout name |
|  |  | Layout Sequece Setup | Add Layout Sequence | Layout Sequence name |
|  |  |  | Modify Layout Sequence | Layout Sequence name |
|  |  |  | Delete Layout Sequence | Layout Sequence name |
|  |  | Camera Sequece Setup | Add Camera Sequence | Camera Sequence name |
|  |  |  | Modify Camera Sequence | Camera Sequence name |
|  |  |  | Delete Camera Sequence | Camera Sequence name |
|  |  | Map setup | Add Map | Map name |
|  |  |  | Modify Map | Map name |
|  |  |  | Delete Map | Map name |
|  |  | Browser setup | Add URL | Browser name |
|  |  |  | Modify URL | Browser name |
|  |  |  | Delete URL | Browser name |
|  |  | UserGroup setup | Add UserGroup | UserGroup name |
|  |  |  | Modify UserGroup | UserGroup name |
|  |  |  | Delete UserGroup | UserGroup name |
|  |  | User setup | Add User | User name |
|  |  |  | Modify User | User name |
|  |  |  | Delete User | User name |
|  |  | User Authority | Add User Authority | UserGroup name, changed permissions |
|  |  |  | Modify User Authority | UserGroup name, changed permissions |
|  |  |  | Delete User Authority | UserGroup name, changed permissions |
|  |  | Remote address accessibility | Add Accessibility | UserGroup name, remote address |
|  |  |  | Delete Accessibility | UserGroup name, remote address |
|  | Recording | Instant Recording | Instant recording on | Device name, Device Address |
|  |  |  | Instant recording off | Device name, Device Address |
|  | Service Setup | Register service | Register Service | Service name, Service Address |
|  |  |  | Unregister Service | Service name, Service Address |
|  | Event Action | Action ack | Request confirmation for ACK | Device name |
|  |  |  | Acknowledgment for ACK | Device name |
|  |  |  | Request forward for ACK | Device name, Forwarded user, Received user |
|  |  |  | Acknowledgment forward for ACK | Device name, Forwarded user, Received user |

# Appendix. C. System log Table

|  |  |
| --- | --- |
| Service Manager |  Install %s |
|  Uninstall %s |
|  Start %s |
|  Shut down %s |
|  Reboot Server |
|  Service Failover |
|  Service has been forced to shut down. |
|  Service forced shutdown failed. |
|  Service forced dump failed. |
|  Service has been forced to shut down by process name. |
| Service Common |  Administration Service Connected |
|  Administration Service Disconnected |
|  Database Error |
|  System Log Database Failed to Open |
|  Debug Log Database Failed to Open |
|  Device Connected |
|  Device Connecting |
|  Device Disconnected |
|  Device Disconnecting |
|  User Logged In |
|  User Logged Out |
|  User Login Failed |
|  Search Client Logged In |
|  Service Started |
|  Service Stopped |
|  Event Log Database Failed to Open |
|  Storage Added |
|  Storage Edited |
|  Storage Deleted |
|  Storage Loaded |
|  Storage Erased |
|  Storage is full. |
|  Storage Formatted |
|  Storage Resized |
|  Storage Overwrite On |
|  Storage Overwrite Off |
|  Timetable Reconstruction Started |
|  Timetable Reconstruction Completed |
|  Timetable Reconstruction Stopped |
|  Timetable Reconstruction Failed |
|  "%s" authentication failed. |
|  %s DEMO period has expired. |
|  User has set time. |
|  User has set timezone. |
|  User has set language |
|  Restart Network |
|  Successfully Upgraded |
|  Storage data partially deleted. |
|  Storage data Auto delete set. |
|  Device Connected(Admin Channel) |
|  Device Connected(Watch Channel) |
|  Device Disconnected(Admin Channel) |
|  Device Disconnected(Watch Channel) |
|  Storage Limit time-lapse set. |
|  Beep On |
|  Beep Off |
|  The storage was automatically deleted. |
|  Storage is not allocated. |
|  Allocated storage has been changed. |
|  Failover started |
|  System successfully recovered by Failover. |
| Admin Service |  Administration Service Started |
|  Administration Service Stopped |
|  Recording Service Registered |
|  Recording Service Unregistered |
|  Recording Service Connected(Login) |
|  Recording Service Disconnected (Logout) |
|  Recording Service Login Failed |
|  Monitoring Service Registered |
|  Monitoring Service Unregistered |
|  Monitoring Service Connected (Login) |
|  Monitoring Service Disconnected (Logout) |
|  Monitoring Service Login Failed |
|  Streaming Service Registered |
|  Streaming Service Unregistered |
|  Streaming Service Connected (Login) |
|  Streaming Service Disconnected (Logout) |
|  Streaming Service Login Failed |
|  Backup Service Registered |
|  Backup Service Unregistered |
|  Backup Service Connected (Login) |
|  Backup Service Disconnected (Logout) |
|  Backup Service Login Failed |
|  Database Error |
|  Database Restored |
|  System time changed. Segment ID of recording is increased. |
|  Maximum service connection limits exceeded. |
|  "%s" authentication failed. |
|  %s DEMO period has expired. |
|  Recording Service Preregistered |
|  Monitoring Service Preregistered |
|  Streaming Service Preregistered |
|  Backup Service Preregistered |
|  Video Analytics Service Preregistered |
|  Federation Service Connected (Login) |
|  Federation Service Disconnected (Logout) |
|  Federation Service Login Failed |
|  Federation Second Service Registered |
|  Federation Second Service Unregistered |
|  Federation Second Service Pre-registered |
|  Not supported product |
|  Administrator Second Service Registered |
|  Administrator Second Service Unregistered |
|  Administrator Second Service Connected (Login) |
|  Administrator Second Service Disconnected (Logout) |
|  Administrator Second Service Login Failed |
|  Administrator Second Service Pre-Registered |
|  Recording Failover Service Registered |
|  Recording Failover Service Unregistered |
|  Recording Failover Service Connected(Login) |
|  Recording Failover Service Disconnected (Logout) |
|  Recording Failover Service Login Failed |
|  Redundant Recording Service Registered |
|  Redundant Recording Service Unregistered |
|  Redundant Recording Service Connected(Login) |
|  Redundant Recording Service Disconnected (Logout) |
|  Redundant Recording Service Login Failed |
|  System setup modified |
|  Firmware Upgrade |
|  Firmware upgraded successfully. |
|  Firmware upgrade failed. |
|  Firmware upgrade canceled. |
|  Monitoring Failover Service Registered |
|  Monitoring Failover Service Unregistered |
|  Monitoring Service Connected (Login) |
|  Monitoring Failover Service Disconnected (Logout) |
|  Monitoring Failover Service Login Failed |
|  Monitoring Failover Service Preregistered |
|  Video Analytics Service Registered |
|  Video Analytics Service Unregistered |
|  Video Analytics Service Connected(Login) |
|  Video Analytics Service Disconnected (Logout) |
|  Video Analytics Service Login Failed |
|  Streaming Relay Service Registered |
|  Streaming Relay Service Unregistered |
|  Streaming Relay Service Connected(Login) |
|  Streaming Relay Service Disconnected (Logout) |
|  Streaming Relay Service Login Failed |
|  Streaming Relay Service Preregistered |
|  Video Wall Service Registered |
|  Video Wall Service Unregistered |
|  Video Wall Service Connected(Login) |
|  Video Wall Service Disconnected (Logout) |
|  Video Wall Service Login Failed |
|  Video Wall Service Preregistered |
|  Video Wall Failover Service Registered |
|  Video Wall Failover Service Unregistered |
|  Video Wall Failover Service Connected(Login) |
|  Video Wall Failover Service Disconnected (Logout) |
|  Video Wall Failover Service Login Failed |
|  Video Wall Failover Service Preregistered |
|  User Audit Log Database Failed to Open |
|  Failover started |
|  System successfully recovered by Failover. |
|  Device Added |
|  Device Edited |
|  Device Deleted |
|  Device Group Added |
|  Device Group Edited |
|  Device Group Deleted |
|  Device Group Member Added |
|  Device Group Member Deleted |
|  Layout Added |
|  Layout Edited |
|  Layout Deleted |
|  Sequence Added |
|  Sequence Edited |
|  Sequence Deleted |
|  Sequence Layout Added |
|  Sequence Layout Edited |
|  Sequence Layout Deleted |
|  Map Added |
|  Map Edited |
|  Map Deleted |
|  User Added |
|  User Edited |
|  User Deleted |
|  User Group Added |
|  User Group Edited |
|  User Group Deleted |
|  User Logged In |
|  User Logged Out |
|  User Login Failed |
|  User Login Failed - Access Denied by IP Address |
|  Time Coverage Preset Added |
|  Time Coverage Preset Edited |
|  Time Coverage Preset Deleted |
|  Condition Preset Added |
|  Condition Preset Edited |
|  Condition Preset Deleted |
|  Action Preset Added |
|  Action Preset Edited |
|  Action Preset Deleted |
|  Schedule Updated |
|  Database Failed |
|  Federation system connected. |
|  Federation system disconnected. |
|  Federation system is registered. |
|  Federation system is unregistered. |
|  Federation process completed. |
|  Federation request denied. |
|  Federation system already registered. |
|  The federation system is different from registered federation system. |
|  Invalid federation system. |
|  Administration failover service has timed out. You should restart Administration Service. |
|  The cached license for AdminFailover Service is invalid. |
|  Device is reassigned to Streaming Service according to Load Balancing Conditions |
|  RTC Sync Performed. |
|  SNTP Sync |
|  Record Storage Error |
| Recording Service |  Recording Service Started |
|  Recording Service Stopped |
|  Administration Service Connected |
|  Administration Service Disconnected |
|  IP Settings Initialized |
|  Service Key Corrupted |
|  Service Key Create Failed |
|  Service Key Write Failed |
|  Service Key Close Failed |
|  Service Key Created |
|  Event Log Writer Initialized |
|  Recording Storage Initialized |
|  Scheduler Initialized |
|  TickSyncManager Initialized |
|  Administration Service Client Started |
|  Administration Service Client Shut Down |
|  Recording Service Server Started |
|  Recording Service Server Shut Down |
|  Recording Client Started |
|  Recording Client Shut Down |
|  Scheduler Shut Down |
|  Scheduler Started |
|  Administartion Service Syncronized |
|  Database Error |
|  Database Restored |
|  System time changed. Segment ID of recording is increased. |
|  Recording Service LicenseKey is different. Service will restart for the changes to take effect. |
|  LicenseKey was not found. |
|  Demo period for recording service has expired. |
|  Recording Service is running in DEMO mode. |
|  Recording Storage Added |
|  Recording Storage Edited |
|  Recording Storage Deleted |
|  Recording Storage Loaded |
|  Recording Storage Cleared |
|  Recording Storage is full. |
|  Recording Storage Formatted |
|  Recording Storage Resized |
|  Recording Storage Overwrite On |
|  Recording Storage Overwrite Off |
|  Recorded Timetable Reconstruction Started |
|  Recorded Timetable Reconstruction Completed |
|  Recorded Timetable Reconstruction Stopped |
|  Recorded Timetable Reconstruction Failed |
|  Disk Bad |
|  Disk Temperature Bad |
|  Disk S.M.A.R.T. Bad |
|  Record Storage Error |
|  Recording Device Added |
|  Recording Device Edited |
|  Recording Device Deleted |
|  Recording Device Connecting |
|  Recording Device Connected |
|  Recording Device Disconnecting |
|  Recording Device Disconnected |
|  Recording Device Record Started |
|  Recording Device Record Stopped |
|  Recording Device Session Deleted |
|  Recording Device Video Lost |
|  Recording Device Video On |
|  Instant Recording Started |
|  Instant Recording Stopped |
|  Failed to write information to database. |
|  User Logged In |
|  User Logged Out |
|  User Login Failed |
|  Search Client Logged In |
|  ClipCopy Started |
|  ClipCopy Ended |
|  ClipCopy Canceled |
|  ClipCopy Failed |
|  ClipCopy User Info |
|  ClipCopy Begin Time |
|  ClipCopy End Time |
|  ClipCopy Duration |
|  ClipCopy Export Time |
|  ClipCopy Camera Title |
|  Schedule Updated |
|  Event Log Database Failed to Open |
|  System Log Database Failed to Open |
|  Debug Log Database Failed to Open |
|  Recording Device Added |
|  Recording Storage Edited |
|  Recording Storage Deleted |
|  Recording Storage Formatted |
|  Recording Performance Profile |
| Streaming Service |  Device has been added according to Load Balancing. |
|  Device has been deleted according to Load Balancing. |
|  Watcher added. |
|  Watcher deleted. |
|  The number of Streaming Channels for this license has been exceeded. |
|  All Streaming Devices will be disconnected |
| Monitoring Service |  Failed to send email. |
|  Failed to connect SMTP server. |
|  Failed to connect using SSL. |
|  No such user. |
|  Failed to authenticate. |
|  Need to authenticate. |
|  Event Scheduler failed to send mail. Check Mail Server settings. |
|  Network Text-In Server Started |
|  Network Text-In Server Stopped |
| Backup Service |  Backup Site Added. |
|  Backup Site Edited. |
|  Backup Site Deleted. |
|  Backup Site Connected. |
|  Backup Site Disconnected. |
|  Backup Start Time was changed. |
|  Summary Backup Setup was changed. |
|  Backup Schedule was modified. |
|  Event Backup setup was changed. |
| Update Service |  Update Service installed. |
|  Update Service uninstalled. |
|  Update Service started. |
|  Update Service stopped. |
|  An error occurred while updating program. |
|  No file |
|  No Administration Information |
|  Update has been canceled by the user. |
|  Update failed. |
|  Update successful. |
|  Starting update. |
|  Update timed out. |
|  File transfer complete |
|  Packages version mismatch |
|  Package file damaged. |
| VideoWall Service |  Video Wall Agent Added. |
|  Video Wall Agent Edited. |
|  Video Wall Agent Deleted. |
|  Video Wall Service User Added. |
|  Video Wall Service User Edited. |
|  Video Wall Service User Deleted. |
|  Video Wall Service User Assigned. |
|  Video Wall Agent Connected. |
|  Video Wall Agent Disconnected. |
|  Video Wall Client Connected. |
|  Video Wall Client Disconnected. |
|  Video Wall Network Keyboard Connected. |
|  Video Wall Network Keyboard Disconnected. |
|  Video Wall Agent Changed. |
| License |  Demo License Expired |
| VideoWall Failover |  Video Wall Failover service has timed out. You should restart Video Wall service. |
|  The cached license for Video Wall Failover Service is invalid. |

# Version History

|  |  |  |  |
| --- | --- | --- | --- |
| **Version** | **Writer** | **Revision Date** | **Remarks** |
| 2.8.1 | Sooho Ahn, Daniel Lee | - | Initial Release |
| 3.6.2 | Roy Lee | 22th Apr.2022 | Updated additional ISS services. |