Powered By

A&E Specification

VMS 6.0.x | Cloud 24.1.x | Mobile 24.1.x

Q4 2024

Table of Contents

1.0 - General

1.1 – Specification Scope

This Architecture and Engineering specification provides a comprehensive guide for solution architects, system integrators, software developers, and application engineers by outlining the requirements and capabilities of an extensible, enterprise-class Video Management System (VMS).

NOTE: Not all product features and the exact method to satisfy every requirement are described.

1.2 – Summary of Requirements

The software product shall be an extensible platform designed to perform the core functions listed below through a graphical user interface or application programming interfaces (APIs):

A. Simultaneously receive and record video data streams from multiple sources.

B. Display live and prerecorded video within a dynamically scalable grid layout.

C. Enable internal and external services to analyze live and recorded video data.

D. Automate actions and notifications based on data analysis and system rules.

E. Process video data to add watermarks and encryption of exporting files.

F. Function as a media player for accessible files created with compatible codecs.

G. Share data across multiple clients (Desktop, Mobile Device, and web browser).

H. Establish a server-hive structure that provides for Nx Server and device failover protection.

I. Implement user management and access controls to system resources and settings.

J. Include APIs and SDKs that enable third parties to expand or create additional functionality.

K. Automatically discover and configure compatible devices found on accessible networks.

L. Installations may be feature-limited when executed without a license or an active subscription.

M. No product features require a license agreement or service fee from third parties.

1.3 – Deliverables

The following deliverables are required for the VMS platform to be complete.

A. Installation packages for supported operating systems shall be free to download.
    1. Local laws and regulations may limit the availability of some installation packages.
    2. A validated email address may be required to download installation packages.

B. User Manuals for the VMS Clients and a public knowledge base.

C. A searchable database of compatible devices.

1.4 – Quality Assurance

System integrators seeking to deploy the VMS into commercial or retail environments shall have five (5) years of experience deploying and supporting similar systems. Integrators may be required to provide the following information before licensing the VMS product or receiving support.

A. A detailed inventory of all hardware and physical devices will comprise the installation.

B. Calculations for system bandwidth and forecasted archive storage capacity.

C. Geo-physical diagrams or maps of device placement and distances between equipment.

D. User management schema (number of users, the types of users, permission groups).

E. System logs and operational data if performance issues or unintended actions are reported.

F. Credentials for support staff to access a Site or System to perform troubleshooting.

G. Technical datasheets and specifications for all third-party equipment and accessories.

H. The certifications and technical training records for installers and users of the VMS system.

I. All data retention policies and requirements that influence system design.

1.5 – Product Support

The VMS Vendor shall record and investigate reported issues while reserving the right to make all resolution and timing decisions at its sole discretion.

A. Public Support

1. The Desktop Client shall have an integrated User Manual with contextual help.
2. The Mobile Client shall have an online User Guide that outlines functions and settings.
3. The technical support shall consist of a free, searchable knowledge base of company-authored articles and engage in a public-community forum.
4. API and SDK packages, including reference documents, are provided without support.

B. Contracted Support

1. Authorized resellers shall have the option to deploy rebranded support services.
2. Direct assistance with, or the creation of, customized API or SDK packages is negotiable.

1.6 – Licensing, Subscriptions, and Updates

A. The Professional Edition shall require a perpetual license (key) to be procured per device to record video. System-wide license keys shall be available for video walls and I/O devices.

B. The Professional Edition permits license keys to be deactivated and reactivated three (3) times before being permanently disabled.

C. The Enterprise Edition shall require a service subscription for each active recording channel.

D. Without licensing, the VMS Software shall demonstrate live streaming or playback of locally stored media for a predefined duration of time, subject to change without notice.

E. The VMS manufacturer shall provide lifetime software upgrades via no-cost releases.

2.0 – VMS Overview

2.1 – VMS Software Components

The specified VMS platform shall consist of four (4) primary software products (Cloud, Nx Server, Desktop Client, and Mobile Client) that share data and resources.

2.1.1 – Cloud Portal

The Cloud Portal shall be an online-only application that provides authorized users access to system resources, video data, and configuration information through an Internet browser.

A. The Cloud Portal shall, as needed, act as a proxy between the Desktop Client, the Nx Server application, and the Mobile client.

B. Cloud Portal users shall each have an account linked to a validated email address protected with a password or other authentication mechanism.

C. The Cloud Portal shall be an optional, free-to-use component for the Professional VMS version.

D. The Cloud Portal shall be a required, free-to-use component of the Enterprise VMS version.

2.1.2 – Nx Server

The Nx Server shall be a cross-platform application that enables authorized users to perform the following activities and consist of these fundamental attributes:

A. No prerequisite software installations are required to install and run the Nx Server application.

B. The Nx Server provides for the active discovery of devices on the network.

C. The Nx Server shall provide media playback and recording of video streams to local storage devices, network-addressable storage, or directly accessible cloud storage services.

D. The Nx Server shall stream video and provide other data to connected and authorized clients.

E. The Nx Server shall establish and maintain secure connections.

F. The Nx Server shall configure Site (system) resources and manage associated metadata.

G. The Nx Server shall include a web browser-based service for performing administrative tasks over a local network without an internet connection.

H. The Nx Server application shall be fully functional when installed in virtual machines or native installations on supported Microsoft Windows and Ubuntu Linux versions.

I. The Nx Server application shall be fully functional when installed on supported versions of the Debian-Linux operating systems for ARM-powered devices.

J. The Nx Server installation package shall be less than 200 MB in size

2.1.3 – Desktop Client

The Desktop Client shall be a cross-platform application that enables authorized users to perform the following activities and have these fundamental attributes:

A. The Desktop Client shall function as a stand-alone media player.

B. The Desktop Client shall be capable of configuring connected devices, managing users, defining rules and actions, and setting operational parameters for a connected Site (system).

C. The Desktop Client shall act as a presentation video wall or remote display.

D. The Desktop Client installation package shall be available for supported versions of Microsoft Windows, macOS, and the Ubuntu operating systems.

E. The Desktop Client shall support two-factor authentication when required by an Nx Server.

F. The Desktop Client Client installation package shall not exceed 200 MB.

G. The Desktop Client shall, at minimum, launch and facilitate configuration on hardware platforms that the operating system vendor supports. Its performance is contingent on the computational hardware and other services running.

H. No prerequisite software is required to install or use the Desktop Client on supported systems.

2.1.3 – Mobile Device Client

The native mobile client shall perform the following activities and have these described attributes:

A. The Mobile Client shall be able to render video and audio data streams via the Nx Server.

B. The Mobile Client shall be able to make limited device configuration changes such as video resolution, PTZ positions, and toggle audio.

C. The Mobile Client shall be able to send audio data to devices for rendering (2-way audio).

D. Support two-factor authentication when required by an Nx Server.

E. The Mobile Client shall run on supported Apple iOS and Google Android operating systems.

F. The Mobile Client installation package should not exceed 100 MB and require no prerequisite software to install and use on supported operating systems.

2.2 – VMS Developer & Integration Tools

The VMS shall have built-in developer tools that are accessible from the WebAdmin interface and shall include, at a minimum:

A. Events Generator

A tool shall be provided to facilitate the development of HTTP Generic Event calls, a method for sending external events to the VMS and triggering actions.

B. The following set of HTTP CRUD REST APIs shall be available:

1. System API
2. Nx Server API
3. Cloud API
4. Video API
5. Audio API
6. Proxy API
7. WebSocket API
8. Authentication & Encryption
9. Breaking Change Log

C. Client (JavaScript API)

This API shall provide a method to interact with web pages open on the embedded browser.

D. Video Source Integration SDK

1. The Video Source SDK shall enable the integration of live or recorded video sources.
2. The Video Source SDK shall provide methods for discovering devices, integrating I/O ports, and incorporating motion detection information.
3. The Video Source SDK shall enable the display, analysis, and recording of media sources.

E. Storage SDK

Enables developers to read and write to local, network, and cloud-hosted storage services.

F. Metadata SDK

Designed to enable third parties to integrate object-driven video analytics and related actions.

2.3 – VMS Architecture

A. The VMS shall have a Server Hive Architecture wherein:

1. All Nx Servers in a Site (system) are equal and peer to each other.
2. Operational databases (device configuration, system settings, user rights) are synchronized in near real-time without requiring a configuration dialog or an administrative interface.
3. The VMS architecture shall provide an automatic Nx Server failover mechanism that will move cameras to another Nx Server and limit the loss of video recording in the event of device failure.
4. The Professional Edition shall allow users to connect to any Nx Server in the Site (system) and perform tasks enabled by their permission group membership.
5. The Enterprise Edition shall provide a hierarchy where systems belonging to an Organization can exist within folders, with each folder having a unique set of permitted users.

B. The Professional Edition shall allow System Administrators to upgrade or deploy a specific VMS version to an entire system via a single button in the Desktop Client.

C. The VMS will use secure technologies for inter-application communication and user credentials.

1. OpenSSL for network connections.
2. Only use TLS v1.2+.
3. Set TLS as the default for external SMTP email routing services.
4. Encryption between the Desktop Client, the Mobile Client, and the Nx Server is optional.
5. Local user credentials shall be protected using a salted MD5 hash,
6. Cloud Credentials shall use a complex multi-level hash.
7. Two-Factor Authentication (2FA) support is available for Cloud user accounts.

D. A Site (system) shall scale to the listed maximums without extra licensing.

1. A Site (system) shall support a maximum of 10 Nx Servers.
2. A Site (system) shall support a maximum of 2,560 video sources in a system.
3. A Site (system) shall support a maximum of 1,000 concurrent users.

3.0 – Nx Server

3.1 – Supported Operating Systems

The Nx Server application shall perform as intended on the following operating systems.

A. Microsoft Windows
   1. Microsoft Windows 10
   2. Microsoft Windows 11
   3. Microsoft Windows Server 2016
   4. Microsoft Windows Server 2019
   5. Microsoft Windows Server 2022

B. Ubuntu Linux
   1. Ubuntu 20.04 LTS
   2. Ubuntu 22.04 LTS

C. macOS (Desktop Client only)
   1. macOS 12
   2. macOS 13
   3. macOS 14

D. ARM-powered Debian Developer Boards
   1. NVIDIA Jetson Devices
   2. Raspberry Pi Devices, starting from Raspberry Pi 4

E. Virtualization and Containerization Platforms
   1. VMWare.
   2. VirtualBox.

3.2 – Nx Server Minimum Hardware

A. The Nx Server will operate on hardware capable of running a compatible operating system.

B. A reference list of minimum and recommended hardware to run Nx Server shall be published:

C. When adhering to the recommended computational platform configurations (see hardware recommendations), each Nx Server shall support recording 256 dual-streaming IP cameras.

https://support.networkoptix.com/hc/en-us/articles/206090177-Nx-Witness-Server-Hardware-Specs

3.3 – Installation & Configuration

A. The Nx Server application shall be a no-cost, publicly available download.

B. A user account may be required to access the free, public download.

C. The Nx Server application does not require prerequisite proprietary or third-party software or database technologies before, during, or after installation.

D. The Nx Server installation process shall not require user input once initiated.

E. After a successful installation, the Nx server setup process shall prompt the installing user to create a new system or merge the newly installed server with an existing Site (system).

F. The Nx Server application shall allow authorized users to set custom network routing configurations for Nx Servers within the Site (system) to optimize traffic and security.

G. The Nx Server application shall provide an events engine that allows authorized users to configure automated actions based on system parameters or HTTP data from external services.

H. The Nx Server application shall be able to send HTTP PUT or GET requests to external devices and third-party systems.

I. The Nx Server application shall support IPv4 and IPv6 addressing.

3.4 – Nx Server Features

3.4.1 – General

A. The Nx Server application shall support sending email notifications via a third-party SMTP service using TLS, SSL, or unsecured connections.

B. The Nx Server application shall support sending email notifications via a built-in proxy service.

C. The Nx Server application shall propagate and refresh shared layouts to authorized users.

3.4.2 – Security

A. The Nx Server application shall include the option to track user actions in an audit trail (log).

B. All Nx Server connections shall use SSL or TLS certificate pinning.

C. By default, Nx Servers and Clients shall support session-based (bearer token) authentication.

3.4.3 – Device Management

A. The Nx Server application shall attempt to automatically discover, stream, and record most ONVIF Profile S-compliant IP devices located on the same network as the Nx Server application.

B. The Nx Server application shall provide a method for searching and connecting to devices when network addresses or unique device identifiers are provided within a search dialog.

C. The Nx Server application shall record and stream video of all possible video resolutions and frame rates to the extent possible with available hardware and computational capacity.

D. The Nx Server application shall provide automatic camera failover without the need for additional licenses or subscription services.

E. The Nx Server application shall be able to provide pass-through high or low-res HLS streams from connected devices.

F. The Nx Server application shall support configuring and responding to events from binary I/O contacts on supported devices.

3.4.4 – User Management

A. The Nx Server application shall support 1,000 concurrent users using TCP.

B. The Nx Server framework shall accommodate an unlimited number of user accounts.

C. The Nx Server application shall support the following LDAP credential management systems.

1. Microsoft Active Directory
2. OpenLDAP
3. JumpCloud

D. The Nx Server application shall enable placing LDAP users into VMS permission groups.

3.4.5 – Data Management

A. The Nx Server shall support the following live camera streams:

1. Video formats: H.264, H.265, and MJPEG.
2. Audio formats: AAC, PCM (Mu-Law, A-law), g711, g726, MP
3. Protocols: TFTP over UDP, RTSP, HTTP

B. The Nx Server shall support the following desktop streams (Microsoft Windows and Linux):

1. Video formats: H.264, MJPEG, WebM.
2. Audio formats: AAC, PCM (Mu-Law, A-law), g711, g726, mp3, and transcoding to WebM
3. Protocols: RTSP, MJPEG, HTTP progressive streaming (WebM), HLS

C. The Nx Server shall support the following streams on ARM devices

1. Video formats: H.265, H.264, MJPEG
2. Audio formats: AAC, PCM (Mu-Law, A-law), g711, g726, MP3
3. Protocols: RTSP, MJPEG, HLS

D. The Nx Server application shall export video in the following formats: AVI MP4 MKV EXE NOV (Network Optix Video).

E. The Nx Server application shall automatically disable any system drive within a server that includes more than one physical drive to prevent the operating system drive from becoming full.

F. The Nx Server application shall store archive indices in the exact location as video archives.

G. The Nx Server application shall allow system administrators to recover archives from accessible, previously used storage mediums using an archive re-index feature.

H. The Nx Server shall allow authorized users to change the size of reserved storage space.

I. The Nx Server application shall have a web administration interface that allows system administrators to view near real-time Server health monitoring metrics.

J. The Nx Server shall use AES 128-bit archive encryption and SHA-256 password encryption.

K. The Nx Server application shall support scheduled and on-demand backup of recorded archives to local, networked, or cloud storage locations.

L. The Nx Server application shall allow concurrent recording of all connected camera streams to two (2) servers in near real-time.

M. The Nx Server shall support ingesting and storing object-driven metadata collected from in-camera, server-based, or cloud-based video analytics solutions.

N. The Nx Server application shall read from and write to physically attached mass storage.

O. The Nx Server application shall read from and write to persistent network-attached storage.

P. The Nx Server application shall read from and write to persistent Cloud storage services.

3.4.6 – Performance

A. The Nx Server application shall allow authorized users to monitor the CPU, RAM, NIC, and physically attached storage usage in near real-time.

B. The Nx Server application shall attempt to generate crash files every time there is an unexpected crash of the Nx Server application.

C. The Nx Server application shall enable CPU-based motion analysis for connected IP cameras.

D. The Nx Server application shall not require a dedicated GPU to function fully.

3.4.7 – WebAdmin Interface

A. The Nx Server application will have a hidden configuration page where authorized users can modify advanced system settings.

B. The Nx Server application shall have a browser-based “WebAdmin” service that provides a graphical user interface where authorized users can perform the following actions:

1. View live video from a single camera at a time in high or low resolutions.

2. View recorded video archives in high or low resolutions using a timeline control.

3. View available camera details (name, ID, IP address).

4. Toggle the display of unique identifiers for Nx Servers and cameras.
5. Change the Site (system) name.
6. View unique camera identifiers, including vendor, model, and preview.
7. Toggle audio functionality for the selected camera.
8. Edit camera authentication credentials.
9. Enable camera motion detection and define regions of interest with adjustable sensitivity.
10. Change the name of the Site.
11. Merge the active Site (system) with another Site (system).
12. View the Cloud connection status or disconnect from the Cloud or an Organization.
13. Change or transfer Site (system) ownership.
14. Toggle the Auto-discovery of cameras and running NX Servers.
15. Toggle the sending of anonymous usage information to developers.
16. Toggle if the systems can automatically optimize camera settings.
17. Toggle the capture of user actions and timestamps into the audit trail (log).
18. Toggle the forcing of Nx Servers to accept only encrypted connections.
19. Toggle the encryption of trafficking between Desktop and Mobile clients.
20. Toggle the session duration control and set the time duration limit.
21. View the email address and permission group for all users.
22. View and change the status (enabled/disabled) of non-Organization users.
23. Remove non-Organization users from the Site (system).
24. Change the Permission Group of users who are not part of an Organization.
25. Add Cloud users who are not part of an Organization to non-administrator groups.
26. Change the Nx Server name or restart the Nx Server.
27. View detailed Nx Server information.
28. Detach Nx Server from a Site (system).
29. Reset the Nx Server to the default configuration.

30. Change analytics database location.
31. Add external storage location to the Nx Server.
32. Change the usage of storage locations.
33. Reindex the primary storage.
34. View alerts using filters for Nx Server, device type, and alert type.
35. View system metadata (ID, version, Nx Servers, channels, users, storage locations).
36. View camera, storage, and network interface details in a table format.
37. View a running line chart of Nx Server (utilization) metrics (CPU RAM. Network, Storage)
38. View Main, HTTP, and system log files.

4.0 – VMS Desktop Client

4.1 – Supported Operating Systems

The VMS Desktop Client shall support the following operating systems.

A. Microsoft Windows

1. Microsoft Windows 11
2. Microsoft Windows 10
3. Microsoft Windows Server 2012
4. Microsoft Windows Server 2012 R2
5. Microsoft Windows Server 2016
6. Microsoft Windows Server 2019
7. Microsoft Windows Server 2022

B. Ubuntu Linux

1. Ubuntu 18.04 LTS
2. Ubuntu 20.04 LTS
3. Ubuntu 22.04 LTS

C. Apple macOS

1. macOS 11
2. macOS 12
3. macOS 13

D. ARM

1. Debian Developer Boards
2. NVIDIA Jetson Devices

4.2 – Minimum Hardware Requirements

A. The VMS Desktop Client shall be fully functional when executed on computational hardware that includes OpenGL2.1 support and is approved to run one of the supported operating systems.

B. The VMS Desktop Client shall not require a discrete graphics processing unit to perform at capacity (64 streams on a 64-bit Operating System) when using sufficiently powerful CPUs with integrated graphics capabilities for the Desktop Client rendering.

   See the Recommended Desktop Client Hardware Specification for more information.

   https://support.networkoptix.com/hc/en-us/articles/115015815928-Nx-Witness-Desktop-Client-Hardware-Specs

4.3 – Installation & Configuration

A. The VMS Desktop Client shall be a no-cost, publicly available download.

B. The VMS Desktop Client shall not require prerequisite proprietary, third-party software or licensed technologies during or after installation.

C. The VMS Desktop Client installation process shall not require user input once initiated.

D. The VMS Desktop Client shall allow authorized users to modify time synchronization settings between utilizing online resources (NTP servers) or a local server providing time data.

E. The VMS Desktop Client shall allow authorized users to connect to Nx Servers running a previous software version by automatically downloading and launching a compatible version.

4.4 – Desktop Client Features

4.4.1 – Graphical Interface

A. The VMS Desktop Client shall consist of five (5) panels that adapt to the permissions of the connected user as described in the following abstract:

   1. The TOP (“Navigation”) panel shall have controls for the Client window, access to the main menu, a cloud-connection menu, a help tool, a Client close button, and a method to display and arrange multiple layouts simultaneously using a standard tab implementation.

   2. The LEFT (“Resources”) panel shall present the Site (system) resources – Nx Servers, Devices, Layouts, Showreels, Webpages, Other Sites (systems), and Local Files.

   3. The RIGHT (“Notifications”) panel shall contain icon-based tabs that toggle the information displayed in the Notification panel or provide access to additional controls for notifications, motion events, bookmarks, system alerts, and detected objects.

4. The BOTTOM (“Timeline”) panel shall provide color-coded bookmarks within a scalable timeline that facilitates navigating, searching, and exporting video archives.
5. The MAIN (“Viewing Grid”) panel shall provide an adaptive drag-and-drop interface to create scenes and layouts containing the resources available to the current user.

B. The VMS Desktop Client user interface shall provide a method for collapsing and expanding the Resources, Timeline, and Notification panels.

C. The VMS Desktop Client shall open the user manual to relevant topics when the contextual help icon is activated atop keyed user interface elements; not linked elements open the user manual.

D. The VMS Desktop Client shall allow authorized users to perform management and configuration tasks on authorized Site (system) devices, users, and resources within a unified user interface.

E. The VMS Desktop Client shall have methods to open the Cloud Portal and the WebAdmin Client.

F. When an authorized user chooses to reset all system warnings, all VMS Desktop Client dialogs that include a ‘do not show again’ option will be reset to their default display mode.

G. The VMS Desktop Client shall overlay camera control icons atop live camera streams according to the device's capabilities and the active user's permission group.

H. The VMS Desktop Client shall support keyboard shortcuts to control various interface options, including PTZ mode, Smart Search mode, and layout controls.

I. The VMS Desktop Client shall provide a method to search resources by unique attributes.

J. The VMS Desktop Client shall allow an authorized user to quickly switch between known Sites (systems) using informational tiles and searchable attributes on the Welcome Screen.

K. The Resources Panel of the VMS Desktop Client shall provide visual indicators to inform the active user which Site (system) is active and connected.

L. The VMS Desktop Client shall automatically recover and reconnect to a Site (systems and Nx Servers) if the connection becomes inaccessible.

M. The VMS Desktop Client shall allow an authorized user to time-synchronize all items displayed on a layout or disable synchronization when viewing live and recorded video simultaneously.

N. The VMS Desktop Client shall have adaptive dialogs that display updated information when the user switches to another resource of the same type, where the user has the same permission.

O. The VMS Desktop Client shall allow users to record their screen in full resolution at up to 30fps.

P. The VMS Desktop Client will allow users to add local files to the Resources panel.

4.4.2 – Viewing Grid, Layouts, and Scenes

A. The VMS Desktop Client shall allow the active user to zoom and scroll using supported Human Interface Devices based on the current cursor location.

B. The VMS Desktop Client (Professional Edition) shall allow authorized users to simultaneously drag and drop multiple system resources from the Resource Panel onto the Viewing Grid.

C. The VMS Desktop Client (Enterprise Edition) shall allow authorized users to drag and drop multiple resources from any accessible Site in the Organization onto the Viewing Grid.

D. The VMS Desktop Client shall display I/O devices as individual items on the viewing grid.

E. The VMS Desktop Client shall allow authorized users to name I/O device inputs and output.

F. The VMS Desktop Client shall allow authorized users to customize the layout of I/O panels on the item in the viewing grid, including indicators for inputs and buttons for outputs.

G. The VMS Desktop Client will allow authorized users to adjust the aspect ratio and streaming quality (high or low resolution) of items displayed on the viewing grid.

H. The VMS Desktop Client (Professional Edition) shall allow administrators to create and share lockable layouts with other Cloud users who can access the system.

I. The VMS Desktop Client (Enterprise Edition) allows authorized users to create and share Cross-Site Layouts with other Organization users belonging to a permission group with access.

J. The VMS Desktop Client shall propagate layout changes to active users accessing the shared Cloud layout (Professional Edition) or the Cross-Site layout (Enterprise Edition).

K. The VMS Desktop Client shall allow authorized users to customize the background image of the viewing grid when using supported image types and sizes.

L. The VMS Desktop Client shall support digital mapping by allowing authorized users to add and customize background images, including opacity and the number of grid points.

M. The VMS Desktop Client shall allow authorized users to modify and refresh a shared layout.

N. The VMS Desktop Client shall have an advanced configurable method for adjusting the number of items allowed on the viewing grid.

O. The VMS Desktop Client shall allow authorized users to add Zoom Windows from active cameras onto the viewing grid.

4.4.3 – Archives and Bookmarks

A. The VMS Desktop Client shall allow authorized users to search archives by date and time.

B. The VMS Desktop Client shall allow authorized users to encrypt exported archives.

C. The VMS Desktop Client shall allow users to export recorded data by selecting a section of the timeline and opening a right-click contextual menu within the chosen area of the timeline.

D. The VMS Desktop Client shall have a rapid review export feature allowing authorized users to compress videos in a time-accelerated fashion using a selectable -acceleration rate.

E. The VMS Desktop Client shall generate multi-video exports into an executable package format that creates a portable version of the VMS media player application, including video files.

F. The VMS Desktop Client will allow fast-forward and fast-reverse viewing of archived video at up to 16 times the recorded speed.

G. The VMS Desktop Client shall support single video export in .avi, .mp4, .mkv, or .nov (Network Optix Video) formats.

H. The VMS Desktop Client shall provide the option to transcode client-side effects (image enhancement, de-warping, timestamps, image overlay, text overlay, and information overlay).

I. The VMS Desktop Client shall present a calendar tool that allows authorized users to advance the archive to a selected bookmark and timestamp (month, day, hour).

J. The VMS Desktop Client shall allow authorized users to manually create bookmarks defined by start and stop times and apply optional metadata tags to optimize search.

K. The VMS Desktop Client shall provide a Storage Analytics feature that allows authorized users to analyze the storage capacity using near real-time and historical (bandwidth) analysis.

L. The VMS Desktop Client shall allow authorized users to backup and restore databases.

4.4.4 – Events and Notifications

A. The VMS Desktop client shall provide an automation framework with conditional rules that initiate specific actions when the rule conditions are satisfied.

   1. Default events are preconfigured actions provided with the VMS Desktop Client installation process to address fundamental operating conditions and routine notification circumstances.

   2. User events are created by modifying default events or combining the provided rules and actions to address unique operational needs and environmental situations.

   3. Site (system) events are notifications directly related to Site operations (storage, connectivity) that users cannot modify, configure, disable, or delete.

B. The VMS Desktop Client shall allow authorized users to create Soft Triggers,

C. Event - Action Framework:

   1. The VMS Desktop Client shall provide a predefined list of '**when** 'event conditions.

   2. The VMS Desktop Client shall provide a predefined list of '**do**' actions for events.

   3. The VMS Desktop Client shall enable the configuration of available attributes for the specific when and do values selected.

   4. The VMS Desktop Client shall be able to create bookmarks using the Rules engine.

   5. The VMS Desktop Client shall allow authorized users to view, search, and export all system events to either an HTML file or a CSV file from within the Event log dialog.

   6. The VMS Desktop Client shall support a defined audio action to play a sound file.

D. User Defined Events must be defined before they are available:

   1. Analytics Event

   2. Analytics Object Detected

   3. HTTP Generic Event

   4. Input Signal on Device

   5. Motion on Camera

   6. Plugin Event

   7. Soft Trigger

E. Site (system) generated events shall exist to provide notification of critical storage and connection issues. The following event rules cannot be modified or deleted by users:

1. Archive Integrity Check Failure
2. Email Address Not Set
3. Email Not Set for Users
4. Email Server Not Configured
5. Error while Sending Email
6. LDAP Sync Issue
7. Licenses Not Configured
8. Local storage is used for analytic and motion data
9. Reindexing Archive Canceled
10. Reindexing Archive Complete
11. Remote Archive Synchronization
12. Storage not Configured
13. System in Safe Mode
14. Time Synchronization Issue

F. The VMS Desktop Client shall provide configurable, '**do**' actions that are taken when the conditions for a defined rule are satisfied:

1. Bookmark
2. Device Output
3. Do Recording
4. Do HTTP Request
5. Execute PTZ Preset
6. Exit Fullscreen
7. Open Layout
8. Panic Recording
9. Play Sound
10. Repeat Sound
11. Send Desktop Notification
12. Send Mobile Notification
13. Send Email
14. Set to Fullscreen
15. Show on Alarm Layout
16. Show Text Overlay
17. Speak
18. Write to Log

4.4.5 – License Keys and Subscription Services

A. The Professional Edition VMS Desktop Client shall provide a method for authorized users to activate, deactivate, and move licenses on Internet-connected Sites (systems).

B. The Professional Edition VMS Desktop Client shall provide a method for authorized users to manually activate licenses on Sites (systems) not connected to the Internet.

4.4.6 – Subscription Services

A. The Enterprise Edition of the VMS Desktop Client shall provide a method for authorized users to apply available services to supported devices.

B. The Enterprise Edition of the VMS Desktop Client shall provide a dialog where authorized users can view the number of available services and the number of services in use.

4.4.6 – Device Settings

A. The VMS Desktop Client shall provide a method for users to access websites or configuration environments embedded within or hosted on a device.

B. The VMS Desktop Client shall allow users to adjust available device configuration settings.

C. The VMS Desktop Client shall attempt to automatically discover Sites (systems), Nx Servers, and devices on properly configured networks.

D. The VMS Desktop Client shall provide authorized users with a comprehensive list of all connected cameras and devices in a single dialog.

E. The VMS Desktop Client shall allow authorized users to replace a camera while preserving the archive from the previous one.

F. The VMS Desktop Client shall allow users to de-warp any fisheye lens using automatic or manual calibration without needing third-party SDKs or services.

G. The VMS Desktop Client shall support two-way audio between authorized users and devices that support 2-way audio communications.

H. The VMS Desktop Client shall have a method to define sequential PTZ presets on each camera, including the time duration when creating a camera tour.

I. The VMS Desktop Client shall support PTZ presets and tours for fisheye cameras when the de-warp mode is enabled.

J. The VMS Desktop client shall allow authorized users to create Hotspots atop one stream that will display another stream when a user interacts with the Hotspot.

4.4.7 – Recording Schedule

A. The VMS Desktop Client shall provide a method for authorized users to define a recording schedule (days of the week and hours of the day).

B. The VMS Desktop Client shall provide a method for authorized users to define motion detection rules as part of the recording schedule on devices that support motion detection.

C. The VMS Desktop Client shall provide notice of available recording licenses (Professional Edition) or available recording services (Enterprise Edition).

D. The VMS Desktop Client shall prevent a recording schedule from being activated when the Site (system) does not contain sufficient recording licenses (Professional Edition) or recording services (Enterprise Edition).

E. The VMS Desktop Client shall allow authorized users to configure minimum and maximum retention durations for recorded data.

F. The VMS Desktop Client shall allow authorized users to configure pre and post-recording times for motion-initiated recording events.

G. The VMS Desktop Client shall provide a method for authorized users to adjust the quality level of camera recording using the preset terms of low, medium, high, and best.

H. The VMS Desktop Client shall allow authorized users to set the bitrate for recorded streams.

I. The VMS Desktop Client will allow batch application of camera recording schedules, quality, and optionally, the archive retention length to multiple cameras in the Site (system).

4.4.8 – Security Features

A. The VMS Desktop Client shall allow authorized users to force HTTPS connections with cameras.

B. The VMS Desktop Client shall allow authorized users to force encryption with Nx Servers.

C. The VMS Desktop Client shall allow authorized users to force encrypted video traffic between the Desktop and Mobile Client.

D. The VMS Desktop Client shall allow authorized users to toggle enforcement of watermarks containing the active username on all video streams.

E. The VMS Desktop Client shall prompt users for two-factor authentication when required.

F. The VMS Desktop Client shall force users to set an initial password for Wisenet cameras.

G. The VMS Desktop Client shall allow authorized users to view, search, and export the audit trail.

H. The VMS Desktop Client shall allow authorized users to view, search, and export system logs.

4.4.9 – Performance Features

A. The Desktop Client shall allow authorized users to enable client-hardware video decoding when the supported graphic processing units are available.

B. The Desktop Client shall utilize adaptive scaling technology to change the resolution of video streams during live and recording playback to optimize CPU and network usage.

C. The Desktop Client shall allow authorized users to analyze the system's storage capacity based on available drives and near real-time or historical bandwidth analysis.

D. The Desktop Client shall display (near) real-time Health Monitoring of connected Nx Servers.

4.4.10 – Analytics

A. The VMS Desktop Client shall allow authorized users to execute an advanced object search by selecting a region of interest within a live camera stream and providing analytical parameters.

B. The VMS Desktop Client shall apply a color mark to the timeline for analytical search matches.

C. The VMS Desktop Client shall conduct an advanced object search covering one full calendar year (365 days) of archived video in less than five (5) seconds on the preferred hardware.

D. The VMS Desktop Client shall allow authorized users to toggle thumbnails in the timeline panel.

E. The VMS Desktop Client shall allow authorized users to browse and export bookmarks.

F. The VMS Desktop Client shall make advanced object search controls and results to be accessible from the Notifications panel.

G. The VMS Desktop Client shall enable and support compatible on-device analytics services.

H. The VMS Desktop Client VMS will allow analytics from supported devices with analytics (Hanwha, Axis, DW, Hikvision, Vivotek, Bosch, Dahua) to function without additional licensing.

4.4.11 – User Management

A. The VMS Desktop Client shall contain a user management framework with predefined and custom groups that simultaneously apply permissions changes to users in the group.

B. The VMS Desktop Client shall allow authorized users to create custom permission groups that can be configured with granular access to Site resources and device controls.

C. The VMS Desktop Client shall allow authorized users to create temporary users who access approved Sites (systems) for a prescribed duration using only a system-generated URL.

D. The VMS Desktop Client shall allow temporary users to join built-in 'viewer' permission groups or custom permission groups created by authorized users.

E. The VMS Desktop Client shall allow administrators to create unlimited custom user groups, each having prescribed access to Site (system) resources and device controls.

F. The VMS Desktop Client shall allow authorized users to enable or disable user accounts.

G. The VMS Desktop Client shall provide a configuration dialog to import LDAP users from Microsoft Active Directory services, OpenLDAP systems, and JumpCloud environments.

H. The VMS Desktop Client shall allow LDAP users in any non-Adminstor Permission Groups.

4.4.12 – Operational Modes

The VMS Desktop Client shall include the following operational modes.

A. The VMS Desktop Client shall function as a media player for the following media formats:

1. Live Streams: H.265 H.264 MJPEG
2. Offline Media: AVI MKV MP4 MOV TS M2TS MPEG MPG FLV WMV 3GP
3. Still Images: JPG PNG GIF BMP TIFF AVI MKV MP4 MOV TS M2TS MPEG MPG 3GGP
4. I/O Devices: Status and Triggers
5. Webpages streaming video as an HTTP element of an HTML page.

B. The VMS Desktop Client shall allow authorized users to create Showreels that combine live video, offline videos, images, websites, I/O devices, and Nx Server health monitoring data.

C. Video Wall mode of the VMS Desktop Client shall:

1. Allow authorized users to control the Client remotely.
2. Render multiple display outputs as a single viewing screen.
3. The VMS Professional Edition requires Video Wall licenses.

5.0 – VMS Mobile Client

5.1 – Supported Operating Systems

The VMS Mobile Client shall be fully functional on devices approved for the vendor to execute one of the following operating systems.

A. Google Android
    1. Android 9
    2. Android 10
    3. Android 11
    4. Android 12
    5. Android 13
    6. Android 14
B. Apple iOS
    1. iOS 16
    2. iOS 17
    3. iPadOS 16
    4. iPadOS 17

5.2 – Installation and Configuration

A. The VMS Mobile Client will be available from the Google Play Store and the Apple iTunes Store without cost or licensing fee;, subject to local laws and regulations.
B. Installing the VMS Mobile Client shall not require user intervention once started.
C. The VMS Mobile Client shall not require device permissions beyond those needed to function.
D. The VMS Mobile Client shall be entirely removed from the device when uninstalled.
E. The VMS Mobile Client shall provide the option to toggle using Site or local time.

5.3 – Features

5.3.1 – Graphical Interface

A. The VMS Mobile Client shall allow authorized users to view live video from one system.

B. The VMS Mobile Client shall allow authorized users to activate existing Soft Triggers.

C. The VMS Mobile Client shall allow authorized users to view available layouts.

D. The VMS Mobile Client shall utilize a proprietary media player to render and display live thumbnails and video.

E. The VMS Mobile Client shall Push Notifications to authorized and active Cloud users.

F. The VMS Mobile Client shall allow authorized users to toggle the viewing of live thumbnails in multi-camera views.

G. The VMS Mobile Client shall allow authorized users to control a camera's PTZ settings using a single touch-to-move mechanism.

H. The VMS Mobile Client shall allow authorized users to navigate through bookmarks.

I. The VMS Mobile Client shall allow authorized users to configure Push Notifications.

J. The VMS Mobile Client shall provide pinch-to-zoom functionality for live video, recorded archives, and the timeline.

K. The VMS Mobile Client shall display a timeline highlighting when archives are present.

L. The VMS Mobile Client shall provide a calendar control that is linked to the timeline.

5.3.2 – Analytics

A. The VMS Mobile client shall allow authorized users to perform Motion Search on the timeline.

B. The VMS Mobile client shall allow authorized users to draw a detection area on the screen.

C. The VMS Mobile client shall allow authorized users to perform Analytical Object Search.

5.3.2 – Device Settings

A. The VMS Mobile Client shall allow users to select from available camera resolutions..

B. The VMS Mobile Client shall allow users to search a Site (system) by resource name.

C. The VMS Mobile Client shall allow users to enable fisheye dewarping.

D. The VMS Mobile Client shall support two-way audio on capable devices.

E. The VMS Mobile Client shall automatically discover available Sites (systems) on the same local area network where the mobile device is connected.

5.3.2 – Security

A. The VMS Mobile Client shall store the credentials for successfully connected Sites and use this information to autocomplete future logins to the same Site (system).

B. The VMS Mobile Client shall provide the option to save connection credentials.

C. The VMS Mobile Client shall allow authorized users to log in to the VMS Cloud from the Mobile Client homepage.

D. The VMS Mobile Client shall support two-factor authentication when required by an Nx Server.

E. The VMS Mobile Client shall provide a toggle (Strict/Recommended) for certificates.

6.0 – VMS Cloud Portal

The VMS Cloud Portal shall exist entirely in the cloud and serve as a proxy for connected Sites (systems) and data exchanged between the Desktop Client, the Mobile Client, and Nx Servers.

6.1 – Supported Browsers

A. The VMS Cloud shall properly function on any W3C-compliant Internet Browser.

6.2 – Installation and Configuration

A. The VMS Cloud portal shall not require installing local software or support services.

B. The VMS Cloud Portal shall provide all configuration controls within the browser interface.

C. The VMS Cloud Portal shall capture and retain all settings within the hosted environment.

D. Before trying other connection methods, the VMS Cloud Portal shall first attempt a direct connection to Nx Servers using NAT Traversal technology.

E. The VMS Cloud Portal shall proxy network traffic between Sites (systems) when routing or internet connectivity issues prevent default communication methods.

F. The VMS Cloud Portal shall allow authorized users to change communication port settings for all Servers in a Site or Organization.

G. The VMS Cloud Portal shall allow authorized users to restart any Nx Server.

H. The VMS Cloud Portal shall allow authorized users to rename any Nx Server.

I. The VMS Cloud Portal shall provide a method to complete a Site (system) merge event.

J. The VMS Cloud Portal shall allow authorized users to transfer Site (system) ownership to another Cloud Portal user.

K. The VMS Cloud Portal shall allow authorized users to transfer a Site (system) to an Organization.

L. The VMS Cloud Portal shall allow authorized users to disconnect a Site (system) from the Cloud Portal.

M. The VMS Cloud Portal shall allow authorized Enterprise users to view the available and in-use services for an Organization.

6.3 – Features

A. The VMS Cloud Portal shall be an optional component of the Professional Edition VMS.

B. The VMS Cloud Portal shall be a required component of the Enterprise Edition VMS.

C. The VMS Cloud Portal shall not require additional licensing or subscription fees.

D. The VMS Portal shall allow users to search for and connect to Sites (systems) by name.

E. The VMS Cloud Portal shall support an unlimited number of user accounts, each having access to an unlimited number of Sites (systems) using a single set of credentials.

F. The VMS Cloud Portal shall allow unlimited systems to connect to the Cloud Portal service without additional licensing.

6.3.1 – Graphical Interface

A. The VMS Cloud Portal interface shall entirely reside within a single browser session without creating additional windows, pop-out boxes, or browser tabs.

B. The VMS Cloud Portal interface shall be responsive to browser size and resolution changes.

C. The VMS Cloud Portal interface shall allow users to select a light theme, a dark theme, or default to the current system theme.

D. The VMS Cloud Portal interface shall provide a persistent heading with links to resources, profile configuration options, and a logout control.

E. The VMS Cloud Portal interface shall have a dynamic banner containing the tabs available to the current user (view, layouts, bookmarks, settings, information, monitoring, and services).

F. The VMS Cloud Portal interface shall present secondary menus, contextual filters, and selection controls within a responsive, left-side panel.

G. The VMS Cloud Portal content display shall scale with changes to the browser zoom setting.

H. The VMS Cloud Portal shall provide a Monitoring Dashboard displaying system resources (CPU, memory, storage, network interface), their status, and associated metrics or running history.

I. The VMS Cloud Portal shall offer a JSON file download containing health information data for the previous 24 hours.

6.3.2 – Viewing

A. The VMS Cloud Portal shall allow authorized users to view the live stream or recorded video archive from one camera at a time.

B. The VMS Cloud Portal shall allow authorized users to adjust the transport format and stream quality and toggle a full-screen view.

C. The Enterprise Edition of the VMS Cloud Portal shall enable authorized users to view Layouts created using the Desktop Client that can display multiple cameras within an Organization.

6.3.3 – Archives and Bookmarks

A. The VMS Cloud Portal shall allow authorized users to search and view bookmarks.

B. The VMS Cloud Portal shall allow authorized users to set data and time parameters and isolate a specific segment of a video archive for viewing or export.

C. The VMS Cloud Portal shall allow authorized users to configure storage locations and related metrics (status, read/write rates, VMS usage percentage, and other available data).

D. The VMS Cloud Portal shall allow authorized users to export portions of a video archive.

6.3.4 – Device Settings

E. The VMS Cloud Portal shall enable authorized users to view and modify camera settings.

6.3.5 – Security

A. The VMS Cloud Portal will utilize secure networking technologies (OpenSSL, HTTPS) and a complex Salted MD5 hash for any stored passwords.

B. The VMS Cloud Portal should allow authorized users to enable and force two-factor / OAUTH2 authentication for all system users.

C. The VMS Cloud Portal should allow system owners to transfer ownership to another user.

6.3.6 – User Management (Professional Edition)

A. The VMS Cloud Portal shall allow authorized users to view the permission groups of Organization users and change the permission groups of non-Organization users.

B. The VMS Cloud Portal shall allow authorized users to add Cloud users to the Site (system) and place the new user into an existing permission group using only the user's email address.

C. The VMS Cloud Portal shall allow authorized users to deactivate or activate users not added at the Organization level.

D. The VMS Cloud Portal shall allow authorized users to remove users who are part of an Organization.

6.3.7 – Organization Dashboard

The VMS Cloud Portal Enterprise Edition shall present Organization Administrators with a dashboard that shall:

A. Display all accessible Organizations.

B. Provide a method to manage folders.

C. Enable browsing of the Organization.

D. Facilitate the management of use at the Organization and Site (system) level.

E. Allow Organization Administrators to change available settings.

7.0 – Abbreviations

Abbreviation or Acronym	Description or Definition
API	Application Programming Interface
AVI	Audio Video Interleave
H.264 / H.265	Advanced Video Coding
HTTP	Hypertext Transport Protocol
IP	Internet Protocol
JPEG / MJPEG	Joint Photographic Experts Group / Motion JPEG
MKV	Matroska video format
MP4	MPEG Layer-4 video format
MPEG	Moving Picture Experts Group
NTP	Network Time Protocol
ONVIF	Open Network Video Interface Forum
PTZ	Pan, Tilt, and Zoom
RAID	Redundant Array of Independent Disks
RTSP	Real-Time Streaming Protocol
SDK	Software Development Kit
SMTP	Simple Mail Transfer Protocol
SSL	Secure Sockets Layer
TCP	Transmission Control Protocol
TLS	Transport Layer Security
VMS	Video Management System