

ACTi

Physical Security End-to-End Solution Provider

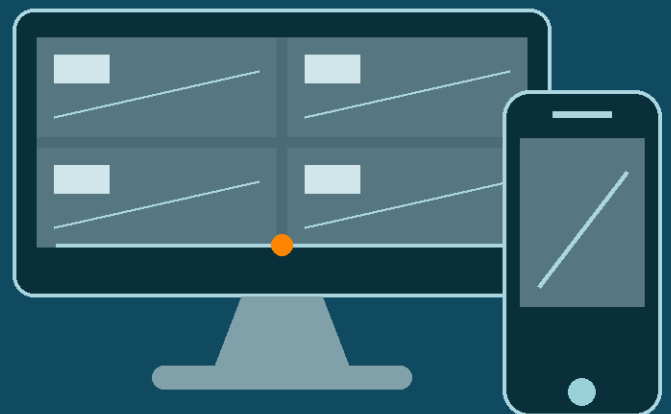
White Paper | VMS Client

VMS CLIENT

A practical guide to workstation, web, and
mobile video management for secure monitoring
and investigation

Prepared by ACTi Corporation

Version 1.1 | July 2026



White Paper | VMS Client

Contents

- 1 Executive Summary
- 2 About ACTi Corporation
- 3 Definition of "VMS Client"
- 4 Core Technical Concepts
- 5 High-Value Applications
- 6 System Architecture
- 7 ACTi Product Portfolio Overview
- 8 Related Keywords and Terminology

Document purpose

This white paper explains how VMS client applications provide secure, role-based access to live video, alarms, recorded evidence, and incident workflows. It is written for system integrators, consultants, security managers, IT administrators, control room teams, and end users planning workstation, browser, or mobile access to a video management system.

1. Executive Summary

A VMS client is the operational interface between authorized users and the video management server. It allows security teams to view cameras, verify alarms, search recordings, synchronize playback, export evidence, control supported devices, and coordinate response from a control room, office computer, browser, or mobile device.

The ACTi VMS Client portfolio includes a Windows-based workstation application, browser-based full and lite clients, and mobile applications for Android and iOS. The official product page states that these client applications are available without separate client charges or usage restrictions, helping project teams assign an appropriate access method to each role. [1]

For system integrators and consultants, the design challenge is not simply choosing a screen. It is matching the client type, workstation resources, network path, display layout, user permissions, cybersecurity controls, and operator procedure to the site's monitoring and investigation requirements.

Core message

Operational principle Use a dedicated workstation for intensive monitoring, a web client for flexible access, and a mobile client for situational awareness—while keeping permissions, evidence, events, and audit records centralized on the VMS server.

Key takeaways

- Client selection should be based on operator role, viewing intensity, location, device capability, and security policy.
- Live view, event handling, search, synchronized playback, export, PTZ, audio, and user management form one evidence workflow.
- The official page highlights up to 225-channel live-view layouts for supported Windows-based NVR deployments and playback speeds from 1/64x to 256x. [1]
- Hardware-accelerated decoding and export can reduce workstation load, but performance still depends on stream count, resolution, codec, display layout, GPU, CPU, memory, and network quality.
- Remote access should use least-privilege permissions, secure network design, encryption, session controls, and complete operation logs.

Procurement principle

Do not specify a VMS client only as “PC software” or “mobile app.” Specify the operator task, concurrent channels, display layout, playback behavior, evidence-export format, response controls, authentication method, and network conditions that must be supported.

2. About ACTi Corporation

ACTi Corporation is the writer and publisher of this document. ACTi is a Taiwan-based international company founded in 2003 and serving customers in more than 100 countries. The company states that it has more than 20 years of security-industry experience and has pioneered video-based security technologies and solutions. [2]

ACTi positions itself as a physical security end-to-end solution provider. Its ecosystem includes cameras, network and hybrid recording, video management, workstation and web applications, mobile access, central management, access control, system health management, backup, and integration with third-party alarm, intercom, access-control, server, sensor, and IoT systems. [2]

This system scope is important for client planning because the client is where operators convert recorded video and event data into decisions. A well-designed client layer supports monitoring, alarm verification, incident investigation, evidence handling, reporting, and controlled access across the complete security workflow.

Why ACTi is relevant to VMS client projects

ACTi strength	Project relevance
End-to-end security scope	Client applications can be planned together with cameras, recording, central management, access control, alarms, system health, and third-party integration.
Multiple access methods	Workstation, full web, lite web, and mobile access let project teams match tools to dedicated operators, supervisors, managers, owners, and remote responders.
Operational workflow	Live monitoring, events, search, playback, export, video analytics, and user management are presented as a connected workflow rather than isolated functions.
Long-term system approach	Centralized permissions, audit logs, evidence protection, and scalable management support projects that may expand across users, displays, sites, and security functions.

3. Definition of “VMS Client”

A VMS client is a software or appliance-based interface used to access a video management server. The server remains responsible for core services such as device management, recording, event processing, user permissions, logs, and evidence storage; the client presents authorized functions to the operator.

ACTi identifies four principal client approaches: a Windows-based workstation application, a browser-based full web client, a browser-based lite web client, and a mobile application for Android and iOS. Web clients require no pre-download, while workstation software is obtained for the relevant VMS platform and mobile software is distributed through the applicable app store. [1]

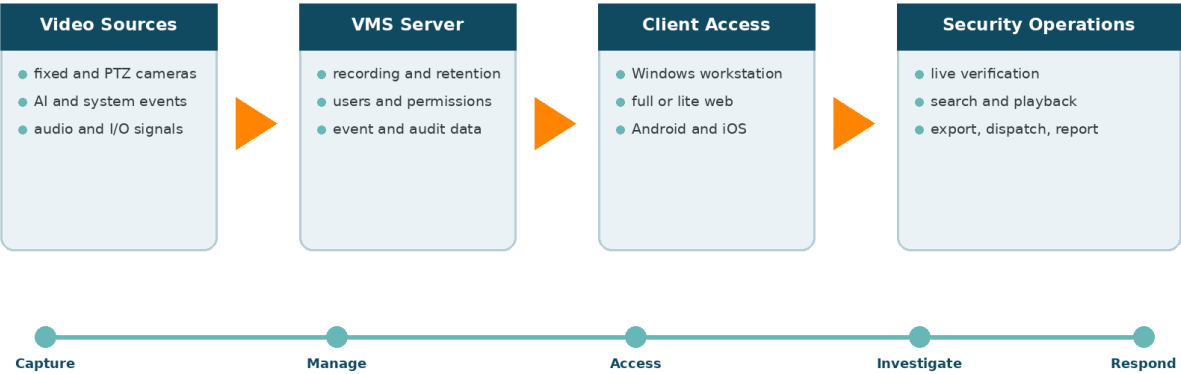
VMS client types and common use

Client type	Best suited to	Design consideration
Windows workstation	Dedicated control-room operators, intensive multi-camera monitoring, investigation, and configuration.	Validate workstation resources, GPU decoding, screen count, display resolution, storage access, and operator ergonomics.
Full web client	Authorized users who need broad VMS access from a compatible browser without maintaining a dedicated workstation installation.	Confirm browser support, feature scope, certificate trust, network latency, and organization security policy.
Lite web client	Users who need streamlined live view or playback access on changing or lower-intensity computers.	Confirm which advanced functions are intentionally simplified and whether the workflow still meets the role's needs.
Mobile client	Guards, supervisors, managers, and responders who need remote live view, PTZ, search, playback, export, notification, or video-push functions.	Prioritize secure connectivity, screen limitations, data usage, battery life, mobile-device management, and incident SOPs.

Visual concept

How a VMS client turns video into operator action

A secure access layer for live monitoring, investigation, evidence export, and response



4. Core Technical Concepts

VMS client performance and usability depend on more than software features. Project teams should combine operational requirements with workstation sizing, stream design, network quality, permissions, evidence integrity, and incident procedures.

Concept	Practical meaning
Live-view layout and decoding	The official page describes flexible grid sizing and up to 225-channel layouts for supported Windows-based NVR use. Large layouts require careful stream selection, hardware-accelerated decoding, suitable CPU/GPU resources, and operator-focused screen design. [1]
Search and playback	Thumbnail search, event-based search, bookmarks, instant playback, embedded playback, and multi-channel synchronized playback help investigators find and reconstruct incidents. Playback speed is listed from 1/64x to 256x. [1]
Event handling	Clients can present analytics, motion, digital-input, tampering, audio, and system-status events, then trigger visual emphasis, PTZ actions, sound, device outputs, commands, notifications, e-mail, or evidence transfer. [1]
Evidence export	The page lists common export formats including AVI, MKV, MOV, and MP4, original-file workflows, an authentic-evidence player, cropping, and hardware-accelerated export. Export policy should define who may export, where files are stored, and how authenticity is preserved. [1]
User and identity management	Unlimited users, Active Directory linkage, customizable group permissions, account lockout, automatic idle logout, dual authentication for playback, password validity controls, operation logging, and recording-file encryption are highlighted. [1]
Device and operator control	PTZ by mouse, joystick, or on-screen controls, two-way audio, digital-output control, maps, dewarping, visual tracking, and embedded work pages can reduce context switching during active incidents. [1]
AI event operations	Client functions can manage people, face, license-plate, and vehicle events generated by compatible AI cameras, allowing operators to use analytics as search and response inputs rather than standalone alerts. [1]

Specification interpretation

A high channel count does not guarantee a usable control room. Effective design balances overview and detail, uses secondary streams where appropriate, reserves full-resolution playback for investigation, limits alarm noise, and gives each role only the functions required for its task.

Procurement warning

Confirm the supported feature set for the selected VMS server, client type, operating system, browser, mobile platform, camera mix, and software version before committing the final design.

5. High-Value Applications

VMS clients create the most value when the access method is matched to a defined security task. Dedicated monitoring, temporary browser access, mobile response, and evidence review are different workflows and should not be forced into one interface.

Application	Operational value	Typical users / locations
Control room monitoring	High-density live views, alarm emphasis, PTZ, audio, maps, visual tracking, and rapid response from a dedicated workstation.	Security officers, dispatchers, command centers, campuses, transport, industry
Incident investigation	Event search, thumbnails, bookmarks, synchronized playback, speed control, evidence export, and auditability.	Investigators, security managers, loss prevention, compliance teams
Supervisor and manager access	Browser access supports review from flexible computers without requiring every user to maintain a dedicated monitoring station.	Supervisors, facility managers, branch managers, owners
Mobile guard response	Remote live view, notification, PTZ, device output, playback, export, or video push can support verification while personnel move through the site.	Guards, patrol teams, field supervisors, emergency responders
Multi-site operations	Central client access can give authorized operators a consistent view of multiple recording servers or sites, subject to the selected management architecture.	Retail chains, schools, healthcare networks, branches, utilities
Remote technical support	Authorized technicians can review system status, camera behavior, configuration, or incident symptoms without immediately traveling to the site.	System integrators, administrators, support engineers

Value by stakeholder

Stakeholder	Main benefit
Security manager	A consistent process for monitoring, alarm verification, investigation, evidence control, and reporting.
Control room operator	Role-focused tools for handling many video channels and events without leaving the operational interface.
IT administrator	Centralized users, directory integration, account controls, encryption, logs, and a clearer remote-access boundary.
System integrator	Multiple client options that can be matched to workstation, browser, mobile, and display requirements.
Consultant / procurement team	Measurable acceptance criteria for channels, screens, search, playback, export, permissions, and client security.
Acceptance test Validate the actual user workflow with representative cameras, simultaneous channels, alarms, playback, exports, user roles, network conditions, and display hardware—not only a feature checklist.	

6. System Architecture

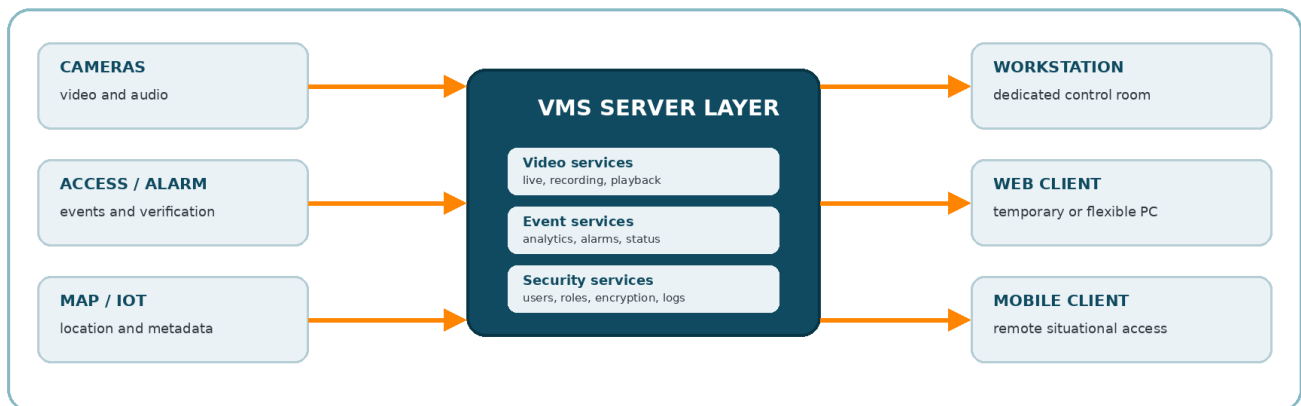
A VMS client should be designed as an access layer, not as an isolated application. Video sources and integrated systems send streams, events, and metadata to the VMS service. The server records evidence and applies permissions. Authorized workstation, web, or mobile clients then present the functions needed by each operator.

The architecture should separate trusted server services from user endpoints, control remote access, minimize exposed services, and preserve consistent time, permissions, logs, and evidence handling across all client types.

Reference system architecture

Reference VMS client architecture

Client choices connect authorized operators to a common VMS service and evidence workflow



Design principle: provide the right client for each role while preserving centralized permissions, auditability, and evidence integrity.

Architecture layers

Layer	Role in VMS client operations
Source and integration layer	Cameras, encoders, audio, access control, alarm inputs, intercom, maps, IoT, analytics, and system-status events.
VMS service layer	Device management, recording, retention, events, user roles, directory integration, encryption, audit logs, search indexes, and export services.
Network and security layer	LAN/WAN/VPN design, routing, certificates, firewall policy, bandwidth, latency, quality of service, remote-access controls, and endpoint security.
Client endpoint layer	Workstation, browser, mobile, video decoder, screens, GPU/CPU, operating system, browser, mobile-device policy, and input devices.
Operations layer	Monitoring SOPs, alarm priorities, dispatch, escalation, investigation, evidence approval, export custody, reporting, maintenance, and training.

7. ACTi Product Portfolio Overview

ACTi presents VMS client access as a portfolio of workstation, web, mobile, and display-oriented options connected to its recording and central-management platforms. The product page emphasizes that clients support remote access to VMS servers from different locations and devices. [1]

Portfolio categories

Category	Where it fits	Representative capabilities to confirm
Windows workstation client	Dedicated PC for full-featured setup, live monitoring, event handling, search, playback, export, analytics, and user administration.	Maximum practical layouts, decoding acceleration, multi-display behavior, joystick support, maps, audio, export performance, and workstation sizing.
Full web client	Browser-based access for users who need broad functionality without a separately installed client application.	Browser and OS support, HTTPS/certificate design, remote bandwidth, permissions, feature parity, and session behavior.
Lite web client	Streamlined browser option for flexible or lower-intensity access.	Live-view and playback scope, simplified controls, browser compatibility, endpoint performance, and role limitations.
Mobile client	Android and iOS access for remote situational awareness and incident response.	Managed channel scale, single-channel live view, PTZ, digital output, search/playback, export, push video, notifications, data use, and mobile security. [1]
Video decoder / display endpoint	Mouse- and keyboard-free local display for selected monitoring scenarios.	Output resolution, display layout, remote control method, supported streams, latency, and operational ownership.
Archive / evidence player	Controlled review of original or authentic evidence exports outside the live VMS interface.	File authenticity, supported export package, player availability, access authorization, audit requirements, and custody procedure.

Portfolio-level capabilities to confirm

- Supported server platform, software version, operating system, browser, mobile OS, and regional availability.
- Concurrent live and playback channels, primary and secondary stream behavior, codec support, fisheye dewarping, PTZ, audio, maps, and event workflows.
- CPU, GPU, memory, display adapter, screen count, display resolution, storage location, and hardware-acceleration compatibility.
- User count, Active Directory integration, role permissions, authentication, idle timeout, password policy, encryption, operation logs, and evidence controls.
- Remote-access method, firewall rules, certificates, bandwidth, latency, mobile-data policy, endpoint hardening, update policy, and incident support procedure.

Project note

Detailed functions and compatibility should be reconfirmed against the latest ACTi product pages, release notes, manuals, mobile-store listings, system requirements, and project quotation documents before formal submission.

8. Related Keywords and Terminology

The following groups collect common terms related to VMS clients, remote video access, control room operations, investigation, evidence management, cybersecurity, and project specification.

Core topic keywords

VMS client, video management client, surveillance client software, security workstation software, video monitoring client, remote VMS access, camera viewing software, control room video software, multi-camera monitoring, video surveillance user interface

Client type keywords

Windows VMS workstation, full web client, lite web client, browser-based VMS, mobile VMS client, Android surveillance app, iOS surveillance app, video decoder client, archive player, evidence player

Live monitoring keywords

multi-channel live view, flexible video grid, hardware-accelerated decoding, fisheye dewarping, PTZ control, joystick camera control, two-way audio, video wall monitoring, GPS camera map, visual tracking

Event and AI keywords

VMS event management, motion alarm response, video analytics event, face event management, people detection event, intrusion event, license plate event, vehicle event, digital input alarm, tampering alert, system status event

Search and playback keywords

thumbnail video search, event-based search, bookmark search, instant playback, synchronized playback, multi-camera investigation, playback speed control, incident reconstruction, recorded video review

Evidence and export keywords

video evidence export, AVI export, MKV export, MOV export, MP4 export, original video file, authentic video evidence, evidence player, video cropping, chain of custody, encrypted recording, audit log

Security and administration keywords

VMS user management, Active Directory VMS, role-based access control, customizable permissions, account lockout, idle logout, dual authentication, password expiry, recording encryption, user operation logging, secure remote video access

Application keywords

control room workstation, security officer live view, mobile guard response, remote supervisor monitoring, incident investigation software, multi-site video management, retail surveillance client, campus security client, critical infrastructure monitoring

Common question phrases

what is a VMS client, workstation client vs web client, how to size a VMS workstation, how many cameras can a VMS client display, how does synchronized playback work, how to export authentic video evidence, how to secure remote VMS access, when to use a mobile VMS client

Source notes

This white paper is based on ACTi public source pages and general video-surveillance system-design practices. Product details should always be reconfirmed against the latest ACTi documentation and regional availability before formal project commitment.

Ref.	Source
[1]	ACTi Corporation, "VMS Client," official product category page, https://www.acti.com/products/vms-client . Accessed July 27, 2026.
[2]	ACTi Corporation, "About ACTi," official corporate page, https://www.acti.com/corporate/about . Accessed July 27, 2026.

Revision note: This document is a marketing and technical-education white paper, not a regulatory certification, cybersecurity standard, or final project design. Validate client compatibility, performance, permissions, network security, and operator workflow in the target environment before deployment.

Prepared by ACTi Corporation

sales@acti.com | www.acti.com