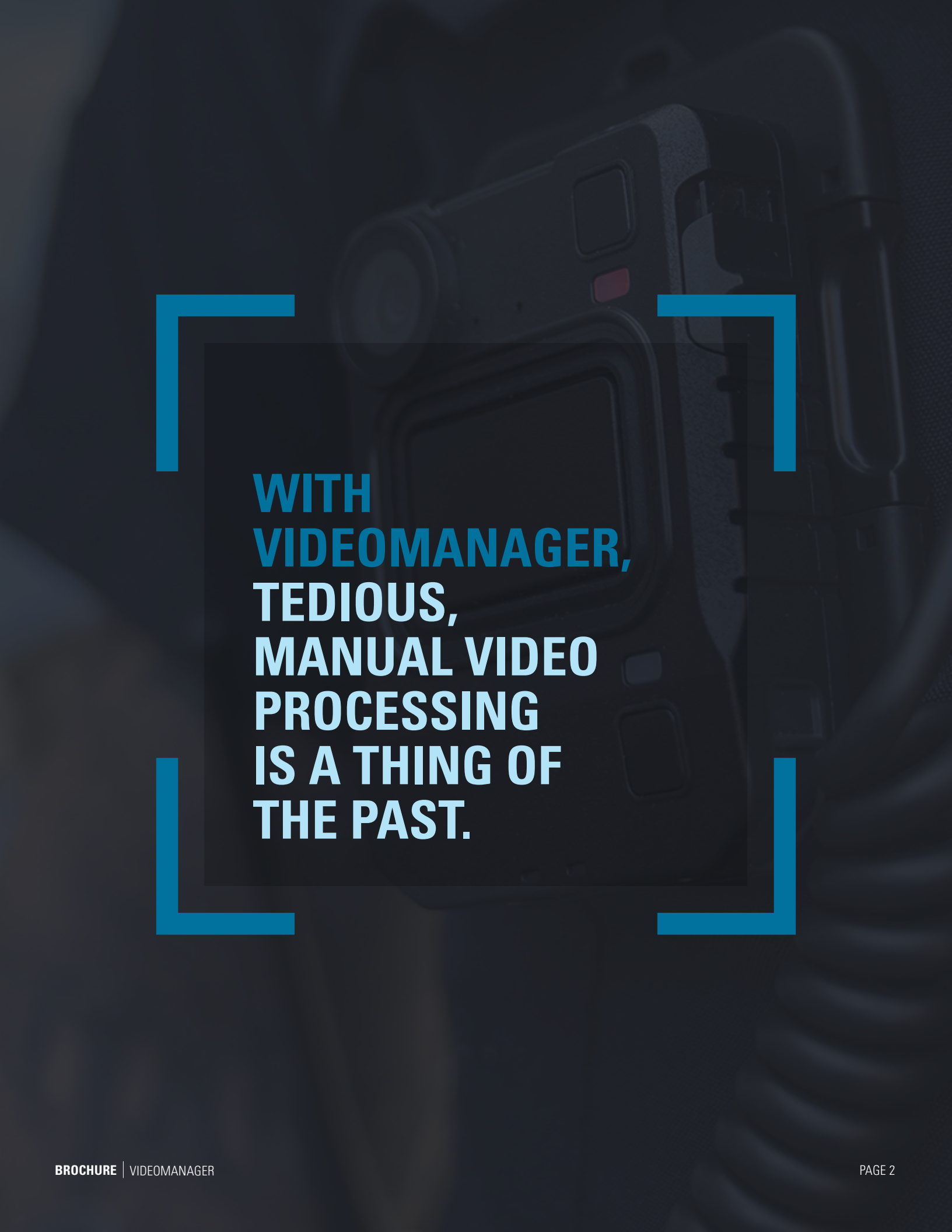




VIDEOMANAGER DEVICE & VIDEO MANAGEMENT MADE EASY



MOTOROLA SOLUTIONS



**WITH
VIDEOMANAGER,
TEDIOUS,
MANUAL VIDEO
PROCESSING
IS A THING OF
THE PAST.**

VideoManager enables the preparation, processing and secure sharing of high-quality video evidence from body-worn cameras and other sources. Now, you can spend less time toggling back and forth between systems, and more time using powerful video evidence to close cases.

INGEST

Your cameras automatically offload their footage to VideoManager automatically as soon as they have been docked.

RETAIN

Create rules to automatically keep media for as long as necessary, as determined by legislative or country guidance, without needing to manually delete redundant files.

PREPARE

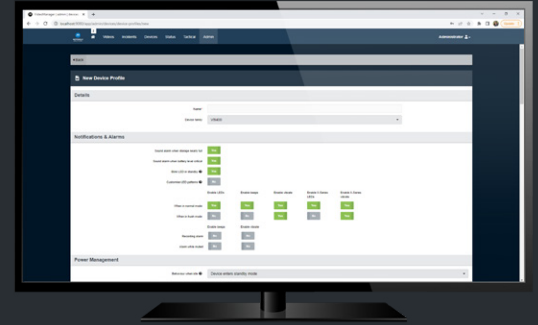
Protect identities and draw attention to key information using redaction and transcription. Preserve the chain of custody via comprehensive audit logging.

SHARE

Get a second opinion with internal and external sharing mechanisms — the review process has never been safer or simpler.



OPTIMIZE CAMERAS FOR EVERY USER



Your Motorola Solutions body-worn cameras aren't just static pieces of equipment - they're an essential part of your operation which need to adapt to your team's needs. And now, you don't need separate systems for device management and video processing; VideoManager does it all, in one user interface. So you're only a page away from configuring a body-camera, streaming to a VMS or securely offloading footage.

Effortlessly administer your cameras with your choice of assignment and footage upload options. No matter your choice, VideoManager will keep cameras up-to-date and ready to use.

DEVICE PROFILES & SETTINGS

Adapt your cameras to your organization, not the other way around. From LED behavior and haptic feedback, to video and audio settings, VideoManager offers multiple customization options.

SYSTEM-SPECIFIC DEVICE KEYS

A lost camera can't compromise your operation. Every one of your cameras is uniquely encrypted to your instance of VideoManager, so your footage can only be viewed by authorized users on your system.

3RD PARTY VMS INTEGRATION

Get the bigger picture by displaying body-worn live streams alongside your fixed video, using VideoManager as an ONVIF-compatible interface for 3rd party VMSs such as Avigilon Control Center (ACC)™.

RAPID DEVICE ASSIGNMENT

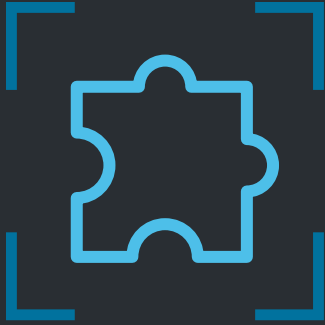
You should always be able to trace body-worn video back to the operator who recorded it - and with multiple ways to assign body-worn cameras, including RFID touch assign, your team can stay accountable while still getting into the field as quickly as possible.

METADATA VIDEO OVERLAYS

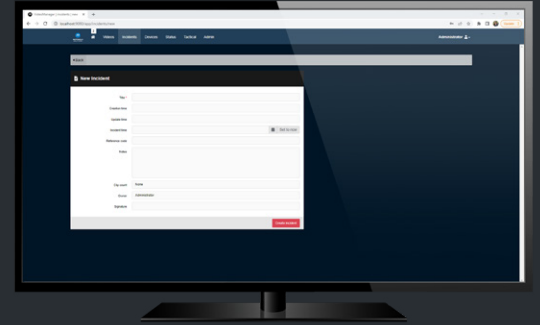
View crucial information about a piece of body-worn video - such as exact GPS location, device serial number, and the name of the operator who recorded it - over the footage itself.

AUTOMATIC FIRMWARE UPGRADES

Avoid time-consuming manual upgrades. Enable automatic upgrades so your firmware is updated alongside your software. To minimize system disruption, you can also restrict upgrades to specific times.



ALIGN YOUR SYSTEM TO YOUR NEEDS



No two teams are alike — but no matter the size, scale or location of your operation, VideoManager is designed to fit seamlessly around your existing architecture. Install on-premises, for complete control over your video, or subscribe to a cloud instance and get access to the latest software as soon as it's available. And once you're up and running, configure VideoManager to match your organization's branding and terminology with our customizable color schemes and easy-to-install language packs.

VideoManager's flexibility, scalability and customization encompasses both initial deployment and everyday use — so there's always a solution which is right for your organization.

CLOUD OR ON-PREMISES DEPLOYMENT

VideoManager's interface can be hosted on a Motorola Solutions cloud instance, for upgrades managed on your behalf. Alternatively, choose an on-premises installation for complete control over your security protocols and highly sensitive data.

ROLE-BASED FEATURE ACCESS

Determine exactly which aspects of VideoManager can be viewed and edited by users, as determined by over 500 permissions — controlling everything from logging in to redacting videos.

UI COLOR SCHEMES & LOGOS

Enhance your brand identity and conform to guidelines by using CSS, HTML or HEX codes to change VideoManager's user interface colors, and importing your logo for display on the log-in and navigational pages.

DISTRIBUTED SITE CONFIGURATION

Ensure lone workers and satellite offices can still get easy access to VideoManager, regardless of local network infrastructure.

STANDARD & CUSTOM LANGUAGE PACKS

Avoid confusing your team with terminology that doesn't align with the rest of your organization. Easily import a custom language pack into VideoManager to ensure your wording is uniform.





FROM CAPTURE TO CLOSURE, ALL IN ONE



Your video is only useful if it can be ingested, accessed, organized and shared as necessary. Redaction isn't just about protecting faces and number plates — it's also about annotating, cropping, and zooming. Body-worn video isn't the only evidence captured during an incident - you also have audio files, still images and documentation that need to be compiled and reviewed together. And when your media is prepared and ready to share, you're only a click away from a second opinion.

From ingest to sharing and deletion, VideoManager covers every step of a video's journey for you in one user interface.

BODY-WORN CAMERA VIDEO IMPORT

VideoManager securely and efficiently ingests the videos stored on your body-worn cameras as soon as they are redocked.

MEDIA-AGNOSTIC IMPORT TOOL

Import your external media however works best for you - whether that's automatically importing at set intervals, dragging and dropping individual files, or leveraging VideoManager's built-in API.

ADVANCED SEARCH PARAMETERS

Being able to find the right piece of media is crucial — but it can be challenging with so much information in one place. In addition to filtering by standard queries like date, ID and owner, VideoManager also offers search parameters based on your custom fields — and with our purpose-built predicate language, your search can be as granular as needed.

INCIDENT CREATION

Collate crucial media into one location to facilitate sharing with both internal and external reviewers, either manually or automatically. Save time by using the bulk edit function to add multiple videos to an incident simultaneously.

CUSTOM TAGGING & CATEGORIZATION

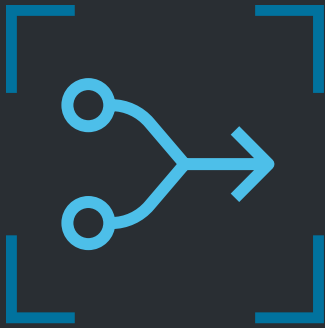
Metadata isn't one size fits all. Whether you need checkboxes, dropdowns, free text or date and time, there's a custom field which meets your purposes. And these fields don't just categorize videos and incidents; you can also use them to gather playback and deletion reasons.

MANUAL REDACTION EDITOR

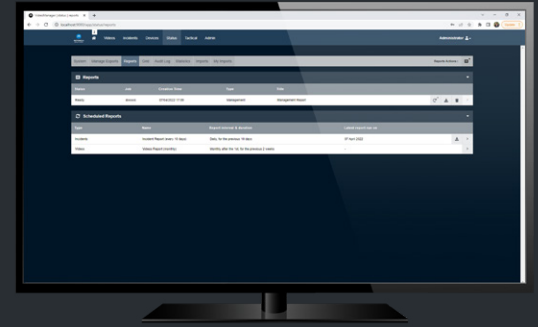
Comply with local laws and regulators by redacting sensitive information including license plates and faces with blurring and pixelation tools. Ensure you never miss a crucial moment with zoom effects, annotations and transcription — all in the same window.

TIME-SENSITIVE SHARING LINKS

Streamline external reviews with VideoManager EX's sharing capabilities; collate important media into one incident, and share it with as many people or organizations as required — no VideoManager EX login needed.



AUTOMATE AWAY THE INEFFICIENCIES



With more videos, devices and users in one place than ever before, we've automated many of the most time-consuming administrative tasks in order to keep your team productive.

Instead of setting up new accounts for each of your employees, simply schedule the user import tool to import them from a CSV file, Excel spreadsheet, or existing database. Once those users are created, you can sync log-in methods across your organization — so your system is still completely secure, but users have one less password to remember. And that automation doesn't stop with users; scheduled custom reports enable you to focus on more important tasks.

USER DATABASE SYNCHRONIZATION

There's no need to re-create your organization's existing users in VideoManager EX one by one; the built-in user import tool can take the information from a CSV file, XML file or Azure AD database to automatically import user accounts at specific times of the day — so joiners and leavers are always accounted for.

SCHEDULED SYSTEM REPORTS

Get regular information on the parameters which matter most to you — whether that's the number of videos you're handling, the number of incidents being created, or how your users are utilising VideoManager EX. In addition to built-in scheduling periods for specific days, weeks and months, you can also import a completely custom schedule based on internal organizational guidance.

SELF-SERVICE PASSWORD RESET

Instead of having to create accounts for new users again and again, let VideoManager EX do the work for you. Grant users access to the system based on their email addresses — so employees, contractors and external reviewers can all view the media and information which is related to their specific roles.

AUTOMATIC CUSTOM FIELD POPULATION

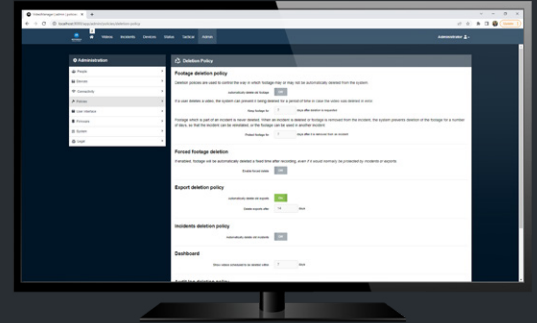
Organise your files the moment they enter your system with import profiles, and avoid uncategorized media getting lost in the process. Automatically populate a piece of media's custom fields based on its origin, or prompt users to do so manually.

ONE-CLICK CONFIGURATION IMPORT & EXPORT

Maintain consistency across your entire organization, no matter how many VideoManager EX installations you have. Export key parameters such as roles, deletion policies and color schemes, and re-import them into another system.



KEEP YOUR DATA SAFE & COMPLIANT



Your confidential data should be just that — confidential. In part, that means restricting access to the system, so only trusted members of your organization can log in. But it also means that, once those users have access, there's a robust trail of accountability. That's where our playback watermarks and audit logs come in; nothing can be watched, edited or deleted without your knowledge. And in addition to built-in AES-256 encryption, we also integrate with OPSWAT™ Anti-Virus technology — so you know that only safe files can enter your organization.

Cutting-edge security protocols keep your information safe at every stage by restricting who can access your system and what they can do on it, while also maintaining the integrity of your media with encryption.

TWO-FACTOR AUTHENTICATION

VideoManager offers over 20 parameters for you to configure password complexity requirements in line with your organisation's policies — but sometimes even that isn't enough. That's where Two-Factor Authentication comes in; users must provide a code sent to an Authenticator app, or click a link in their inbox, before gaining access to the system.

PLAYBACK REASONS & WATERMARKS

It's important that users can review media when needed — but you also need to ensure that they're accessing it appropriately. Customizable playback reason fields require users to provide a rationale for viewing a video, and video watermarks discourage illicit screen recordings by overlaying the username of the person watching it.

DELETION POLICIES

Redundant media shouldn't be kept forever; not only does it take up valuable space on your servers, but local regulations mean it can also pose a legal risk. With VideoManager's comprehensive deletion policies, you can be safe in the knowledge that media and incidents are only kept for as long as they're needed — and not a day more.

AUDIT LOG

Maintaining oversight is crucial, especially when your system is handling large volumes of sensitive data. VideoManager's audit log automatically records every action taken on the system, from the moment a user logs in. And with the ability to filter by a variety of parameters — including over 500 distinct audit log events — you can gain key insights quickly.

MEDIA ENCRYPTION

All media uploaded to VideoManager — whether it comes from body-worn cameras or other external sources — is encrypted at-rest using symmetric AES-256 encryption. Media can also be encrypted when it is exported, requiring recipients to enter a password before they can view it.

