VideoManager EX 16.0 User Guide

This document is intended to serve as a reference to administrators when using basic VideoManager EX features.

Intended purpose

This document is intended to serve as a reference to administrators when using basic VideoManager EX features.

Document ID

ED-012-255-01-NA

Conventions

This document uses the following conventions:

Convention	Description
► For more information...	A cross-reference to a related or more detailed topic.
[ ]	Text enclosed in square brackets indicates optional qualifiers, arguments or data.
<>	Text enclosed in angle brackets indicates mandatory arguments or data.
`Text in code`	Examples of what code could look like in the XML file/user import tool. Examples of what code could look like when using the custom predicate language. Examples of what code could look like in the command line.

Contact address

Motorola Solutions Ltd.
Nova South, 160 Victoria Street
London
SW1E 5LB
United Kingdom

Safety notices

⚠ Caution   *Indicates a hazardous situation which, if not avoided, could result in moderate injury, damage the product, or lead to loss of data.*

💡   *Additional information relating to the current section.*

Contents

1 Welcome to VideoManager EX

Thank you for choosing Motorola Solutions VideoManager EX as your aggregator of evidential-ready media. VideoManager EX is designed as an intuitive browser-based system, requiring minimal training.

If you cannot see aspects of the User Interface (UI) or perform certain actions, it is probably because you do not have sufficient permissions to do so. If this is the case, please contact Motorola Solutions support or speak to your system administrator for further instructions.

2 Home

When the user logs in, the first tab they will see is their 🏠 *Home* tab. This provides a summary of the information and media available to the user on VideoManager EX.
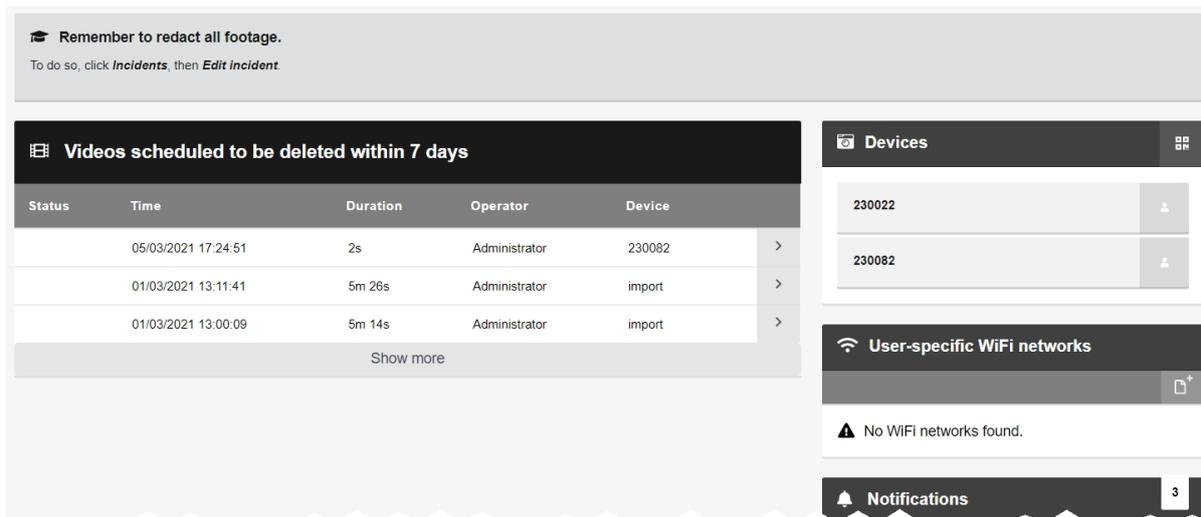
The following information is displayed:

- **Videos scheduled to be deleted within {0} days** - this pane lists all media files owned by the logged-in user which are scheduled to be deleted within a certain time frame, as dictated by the deletion policy.

  This is only visible if the logged-in user is in a role which has the **View media scheduled to be deleted on dashboard** permission enabled.

- ⊞ **Recent media** - this pane gives details about the media files most recently downloaded from a body-worn camera. The user can navigate to a chosen media file for more details and editing functions.

- 📑 **Recently edited incidents** - this pane gives details about the most recently created and edited incidents. Users can navigate to a chosen incident for more details and editing functions.

- 📷 **Devices** - this pane shows which body-worn cameras have been assigned to the current user. Users can also create a QR code configuration for VT-series cameras, by clicking ▦ **Generate device config code**.

- 📶 **User-specific WiFi networks** - this pane shows any user-specific WiFi networks belonging to the user. They can also add a new user-specific WiFi network, by clicking ➕ **Add network**.

- 🔔 *Notifications* - this pane shows a list of event notifications from VideoManager EX. Users can click ✖ *Clear* to dismiss the notifications. Possible notficiations are as follows:

  - ↱ *{0} media shared with you* - media has been shared with the logged-in user or the logged-in user's group.

  If the user clicks 🖼 *View*, VideoManager EX will display the media which has been shared.

  - ✎ *{0} media now owned by you* - a media file's *Owner* field has been changed to the logged-in user or logged-in user's group.

  If the user clicks 🖼 *View*, VideoManager EX will display the media which the user now owns.

  - ↱ *{0} incidents shared with you* - incidents have been shared with the logged-in user or the logged-in user's group.

  If the user clicks 🗃 *View*, VideoManager EX will display the incident which has been shared.

  - ✎ *{0} incidents now owned by you* - incidents' *Owner* fields have been changed to the logged-in user or logged-in user's group.

  If the user clicks 🗃 *View*, VideoManager EX will display the incident which the user now owns.

  - ⬇ *{0} media downloaded* - media files recorded by the logged-in user's body-worn camera have finished downloading to VideoManager EX.

💡 *The number of notifications corresponds to the number of media files which have been downloaded, **not** the number of recordings. For example, if the body-worn camera captured one hour-long recording, but the body-worn camera's device profile was configured to split recordings up into 15-minute chunks, VideoManager EX would display 4 notifications - one for each media file.*

If the user clicks 🖼 *View*, VideoManager EX will display the media which has just been added.

  - ⬆ *You have exports ready for download* - the logged-in user's exports have finished processing and can be downloaded to the PC.

  If the user clicks 📤 *View*, VideoManager EX will display all export jobs. The most recent export jobs will be presented at the top of the list.

  - ⬇ *{0} imports are ready* - the logged-in user's import jobs have finished processing.

  If the user clicks 📥 *View*, VideoManager EX will display the import jobs. The user can then click 🔍 *View assets*, and VideoManager EX will display the imported media file itself.

  - ⚠ - if there are system warnings (e.g. if a licence is expiring within a week), they will be presented here. These notifications cannot be cleared.

If the user clicks 👁 *View*, VideoManager EX will display the warnings.

- 🗹 ***Your licence will expire on this date:*** - when VideoManager EX's licence
  (s) will expire. This notification cannot be cleared.

> 💡 *If VideoManager EX has multiple licences, information for the licence which will*
> *expire **first** is displayed here.*

- 🔒 - the last time the user logged in. This notification cannot be cleared.

- ***System information*** - this dropdown provides information about the version of
  VideoManager EX that the user is utilising. It also gives users the option to export sys-
  tem logs, and lists any licensed features the user has enabled.

- ***Messages*** - this pane displays system messages set by either the user or an admin-
  istrator.

Users can set messages from the ***Messages*** section of the ***User Interface*** pane, in the ***Admin***
tab.

When the number of notifications reaches 99, users will not see any more notifications until they clear some
existing ones.

3 Media

The *Media* tab provides access to all media files available to a user in VideoManager EX and related functions which they can perform on media files.

If users have sufficient permissions, they can:

- Search for media files, filter them by a number of criteria, and perform advanced searches.

>> For more information, see Search Media Files on page 11

- Change the default layout of the *Media* tab on VideoManager EX.

>> For more information, see Change Viewing Options on page 14

- Import media files into VideoManager EX.

>> For more information, see Import Media Files on page 16

- View media files which have been recorded on body-worn cameras or imported into VideoManager EX.

>> For more information, see View Media Files on page 17

- Edit media file properties (e.g. who owns the media file).

>> For more information, see View and Edit Media File Properties on page 20

- Add location information to a video which was recorded without any (e.g. because GPS was disabled, or because the body-worn camera did not have GPS functionality).

>> For more information, see Add Location Information to a Media file on page 22

- Perform actions on a media file, such as adding it to an incident, or rotating it.

>> For more information, see Perform Media File Actions on page 25

- Redact media files
- Bulk edit media files.

>> For more information, see Bulk Edit Media Files on page 28

Media files which have been downloaded from a body-worn camera assigned to the logged-in user are shown under the **My Media** pane. Media files which have been shared with a user by another user are shown under the **Shared Media** pane.

If a user supervises other users, the supervised users' media files are shown under the **Supervised Media** pane.

3.1 Search Media Files

Users can search for individual media files on VideoManager EX. This is useful if there are too many media files on VideoManager EX to scroll through manually.

Media files can be searched by a number of criteria.

1. Navigate to the *Media* tab.

2. Select the 🔍 *Search Media* pane.

Users can now filter media files by the following criteria:

- *Location* - search for media files which were recorded in a specific place. This can be done by clicking *Set Location*. Users can then choose the relevant location on a map, and set a radius to search (minimum radius = 75ft, maximum radius = 6.25 miles).

- *Earliest date* and *Latest date* - search for media files recorded between set earliest and latest dates. Users can also choose a specific time of day (in 24 hour format).

- *Device operator* - search for media files downloaded by a specified user.

- *Owner* - search for media files from a specified owner.

This is normally the same user as the body-worn camera operator, but not always - for instance, if the person who originally recorded the media file has left the organisation and their user has been reassigned to someone else, that user becomes the owner of all their media. From the *Media file Details* page, it is also possible to edit who the owner of the media is.

Click *My media* to search for media files that the logged-in user owns.

- *Device* - search for media files from a specified body-worn camera (or other source, if the user has enabled *Media file Import*). This should be done by serial number.

- *Origin* - this will filter media files by the location to which they were downloaded. This could be a DockController, a mobile phone, or the PC on which VideoManager EX is running.

-ᗧ-   *To find media files which have been downloaded directly to the user's PC, enter*
        local *into the search box.*

- ***Media or Recording ID*** - search for a media file by its unique media file ID.

Alternatively, the user can enter a recording ID. This will return **all** media files which are part of that recording.

There are also filters which can be checked:

- ***Include incident media*** - select whether to include media files which are part of one or more incidents.

- ***Include non-incident media*** - select whether to include media files which are **not** part of one or more incidents.

- ***Only bookmarked media*** - select whether only bookmarked media files are shown.

This will only return media files which had bookmarks added to them in the field by the body-worn camera they were recorded on. It will **not** return media files which had bookmarks added to them in an incident on VideoManager EX.

- ***Include deleted media*** - select whether or not to include recently deleted media files, and media files which are scheduled for deletion due to VideoManager EX's deletion policy.

If users have the ***Undelete*** permission set to ***On***, they can reinstate deleted media files. To do so, check the ***Include deleted media*** box, and click ***Find media***. Next to the media file to be reinstated, click ↻ ***Reinstate media***.

-ᗧ-   *Recently deleted media files will have a red heading.*

- ***Only media that have location data*** - select whether only media files with location data are shown.

This includes both media files with location data recorded alongside them **and** media files whose location data was added in VideoManager EX after recording.

- ***Only media that have been shared*** - select whether only media files that have been shared with other users on the system are shown.

- ***Only media that will be deleted within*** (0) ***days*** - filter media files based on when they are scheduled to be deleted automatically, based on VideoManager EX's deletion policy.

If the deletion policy has not been configured, this filter will not do anything.

> ⚠️ *These conditions have a cumulative effect (e.g. if both **Only bookmarked media**
> **Caution** and **Only media that have location data** are checked, then only media files
> which are both bookmarked **and** have location data will be shown).*

3. Click ***Find media*** to display all media files which match the previously-set criteria.

Users are only able to search for media files if they have the corresponding permissions (***Access***, under the ***Media permissions*** pane).

If the user wants to search for media files using different parameters:

1. Click the ***Filter*** heading. This will re-open the search parameters.

2. Click ✖ ***Clear filter*** to clear the search filters.

Users can now enter the updated criteria.

3. Click ***Find media*** to search for the relevant media files.

Once users have filtered their media files, they can change the way that those media files are presented.

3.1.1 Change Viewing Options

Users can change media file presentation options. This helps users to locate media files faster, and is done from the *Media* tab. Users can only change the preferences for their own session on VideoManager EX.

Users can change how media files are presented either before or after searching for specific media files. To do so:

1. Navigate to the *Media* tab.

2. Select the 🔍 *Search Media* pane.

3. Select the relevant format from the top right-hand *View options* menu. Depending on the user's permissions, the options are as follows:

   - ▦ **Large** - this displays the first frame of each media file, and allows media file playback. Basic information about the media file is displayed, with a list of the media file actions available for this media file.

   - ▦ **Gallery** - this displays each media file in a grid. Each image in the grid is a still frame from one minute of the media file. Click an image to jump to that point in the media file. No other information is displayed, and the only action that can be performed is to delete the media file.

   - ▤ **List** - this displays detailed information about each media file:

     - *Status* - whether the media file has been uploaded from a site, and whether the media file has been bookmarked (by a VB400 in the field).

     - *Time* - when the media file was recorded (date and hours/minutes/seconds).

     - *Duration* - the length of the media file (hours/minutes/seconds).

     - *Operator* - who recorded the media file.

     - *Source* - which body-worn camera recorded the media file, and its serial number.

     If the media file has been imported, the *Source* will be shown as *Import*.

- ⬚ - how many incidents include the media file in question. Clicking this will either open the relevant incident (if the media file only belongs to one) or present the list of incidents (if the media file belongs to more than one).

- Media file actions available for this media file.

>> For more information, see Perform Media File Actions on page 25

Users can change how media files are ordered. This will make it easier to find media files that were either recorded or downloaded more recently. To change how media files are ordered:

1. Navigate to the *Media* tab.

2. Select the 🔍 *Search Media* pane.

3. Click the relevant filter from the top right-hand dropdown menu.

   - **Recording date** - this will present media files from most recently recorded to least recently recorded.

   - **Recording date (least recent)** - this will present media files from least recently recorded to most recently recorded.

   - **Date added** - this will present media files from most recently downloaded to least recently downloaded.

3.2 Import Media Files

Users with the *Media file Import* licence can import a variety of files into VideoManager EX, including still images and PDFs.
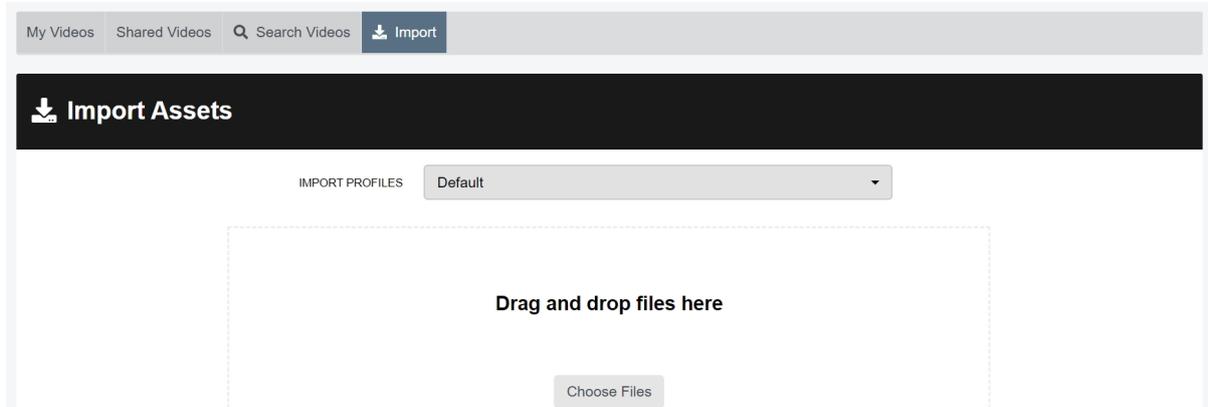
To import a media file:

1. Navigate to the ***Media*** tab.

2. Select the ⬇ ***Import*** pane.

3. Select the relevant import profile from the dropdown.

4. Users can now import a media file by either dragging and dropping the file into VideoManager EX, or by clicking ***Choose Files*** to select a file on their PC.

   Repeat this step for as many media files as necessary.

5. Click ***Start import***.

   Users can view the status of the import from the ***Imports*** pane.

Once a media file has been successfully imported, users can view it from the ***Media*** tab like media files recorded on body-worn cameras.

3.3 View Media Files

Once a media file has been downloaded to VideoManager EX - either from a body-worn camera or from an external source - users can watch it from its *Media file Details* pane. Here, they can also configure the playback controls - this enables the user to change the way they view the media file.
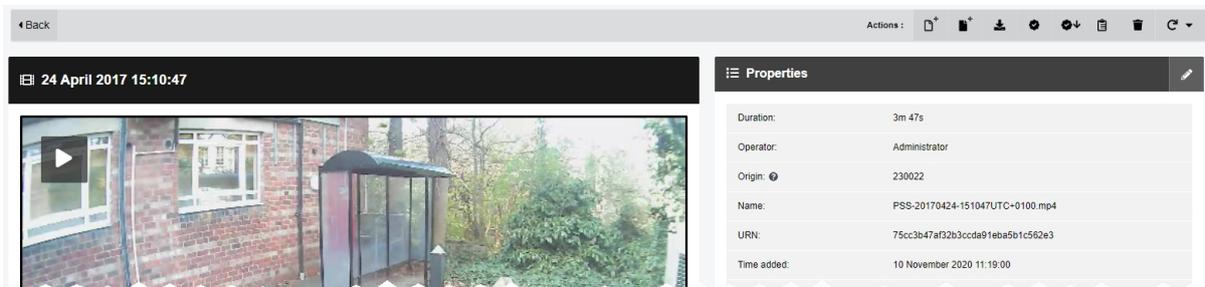
To watch a video on VideoManager EX:

1. Navigate to the *Media* tab.

2. Find the relevant media file, and click ❯ *More Details* next to it.
   Users can find the relevant media file by navigating to the *My Media*, *Shared Media*, or *Supervised Media* panes. They can also search for the relevant media file from the 🔍 *Search Media* pane.

3. Click ▶ *Play media*.
   The media file will start to play.

Once ▶ *Play media* has been clicked, the bottom menu bar will appear. Users can perform the following actions from this bottom menu bar:

- To put the media file in *Theatre* mode (which will fill the entire active window), click 🖥 *Theatre*. Click the button again to revert the media file to its normal size.

- To put the media file in *Fullscreen* mode (which will fill the entire screen), click ⤢ *Fullscreen*. Click the button again to revert the media file to its normal size.

- To skip through the media file, use the following controls:

  - *Cursor handle* - track backwards and forwards through the media file.

  - ▶ *Play* - plays or pauses the media file.

  - ⏮ *Step Backward* - steps backwards through the media file one frame at a time.

  - ⏭ *Step Forward* - steps forwards through the media file one frame at a time.

  - ⏭⏭ *Playback Speed* - plays the media file at different speeds (either **1/4x**, **1/2x**, **Normal**, or **2x**).

- To open the *Playback Controls* menu, click ⚙ *Settings*. From here, users can perform the following actions:

    - ⌨ *Keyboard Shortcuts* - lists certain keyboard shortcuts that users can take.

    - ▦ *Metadata Overlay* - displays or hides the metadata recorded alongside the media file.

    - 🔊 *Audio* - switches audio on or off.

    - 📷 *Take Screenshot* - takes a screenshot of the media file in playback.
    The screenshot will be automatically downloaded to the user's PC.

    - ⚙ *Video Quality* - changes the quality of the media file in playback. This option is only available to users with the correct permissions. It is recommended that the *Highest* setting is only used if there is a good data transfer connection.

If the user has imported a PDF file, the actions they can take are as follows:

- ⊙ *View image* - the PDF will open in a new tab, and can be viewed and downloaded like normal.

- ⬇ *Download file* - the PDF will be downloaded to the PC's default download location.

If the user has imported an audio file, the actions they can take are as follows:

- ▶ *Play media* - the audio file will play. Users can skip, pause, and step through the file like a normal media file.

- ⚙ *Settings* - this is similar to the *Settings* control for media files, but only has options for *Keyboard Shortcuts*, *Metadata Overlay*, and *Audio Quality*.

If the user has imported a still image, the actions they can take are as follows:

- *View image* - the bottom menu bar will open, and users can perform image-specific actions on the media file. These are:

    - 🔍 *Show/Hide zoom panel* - changes whether the zoom panel is visible or not. If it is set to *Visible*, the white slider can be used to zoom in and out on a specific area of the still image. The panel can be moved to focus on different parts of the image.

    - 🖼 *Preparations* - switches between the original still image and the prepared version.

- ⚙ *Settings* - this is similar to the *Settings* control for media files, but only has options for *Keyboard Shortcuts* and *Take Screenshot*.

The *Theatre* and *Fullscreen* controls function as normal.

> >> For more information, see View Media Files on page 17

If the user has imported a file whose file type is different from those mentioned above, they can click 📥 *Download file* to download the file to the PC's default download location.

Once a user has finished watching a media file, they can return to the 🔍 *Search Media* pane by clicking ◀ *Back*.

3.4 View and Edit Media File Properties

Users with sufficient permissions can edit media file properties.
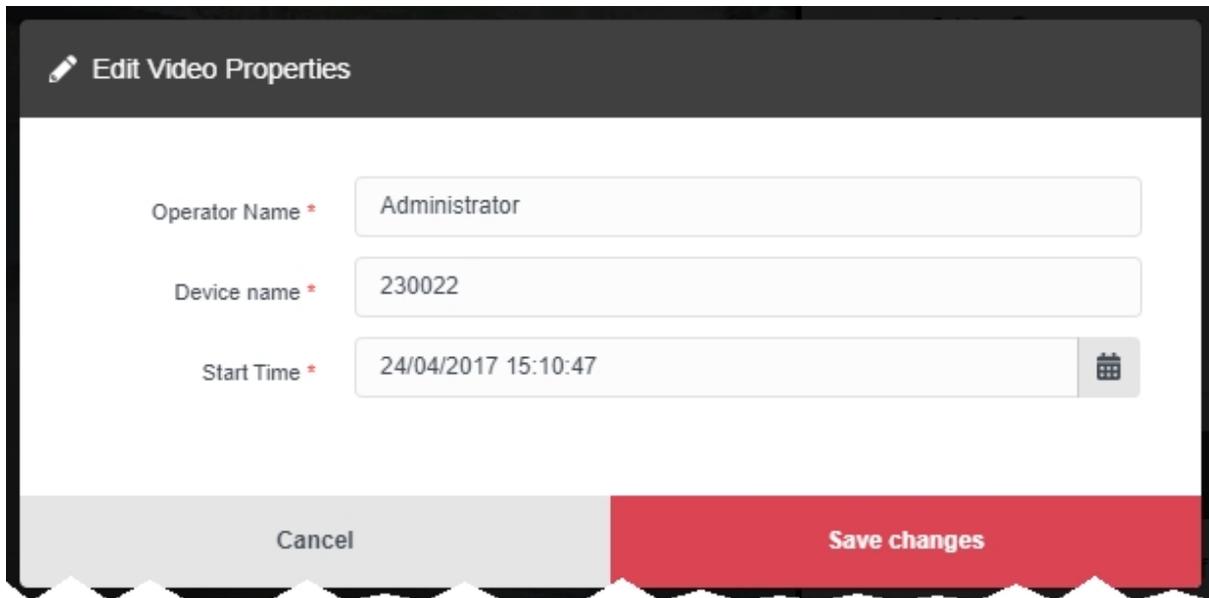
To view the properties of a media file:

1. Navigate to the *Media* tab.

2. Find the relevant media file, and click ❯ *More details* next to it.

   Users can find the relevant media file by navigating to the *My Media*, *Shared Media*, or *Supervised Media* panes. They can also search for the relevant media file from the 🔍 *Search Media* pane.

3. In the ☰ *Properties* pane, the following information will be displayed:

   • *Duration* - the length of the clip.

   • *Operator* - the name of the operator who filmed the media.

   If the media file was imported, this will be the name of the user who imported the media.

   • *Origin* - the body-worn camera on which the media file was filmed.

   • *Name* - the name of the media file on VideoManager EX's file space.

   • *Media file ID* - the unique URN assigned to this media file.

   • *Recording ID* - if the media file is part of a longer recording, this is the unique URN assigned to that recording.

   • *Time Added* - the time and date of when the media file was downloaded to VideoManager EX (either from a body-worn camera, or an external source).

   • *Encoding* - the FPS of the media file.

- ***Scheduled deletion*** - if the deletion policy has been configured, this field shows when the media file will be deleted by VideoManager EX automatically.

This could be based on a number of factors, including how many days have elapsed since the media file was recorded on a body-worn camera or downloaded from a body-worn camera to VideoManager EX.

- ***Signature*** - if file signing has been enabled, VideoManager EX will verify all media files which were recorded on a VB400 against the VB400's certificate.

If the field reads as ***Success***, VideoManager EX has successfully verified that the media file has been recorded on a trusted body-worn camera and has not been tampered with.

If the field reads as ***Untrusted Certificate***, this could be because VideoManager EX does not recognise the certificate of the body-worn camera which recorded the media file.

If the field is not present at all, this could be because the media file was downloaded from a non-VB400 source (e.g. it was imported, or recorded on a VT100) or was downloaded to an older version of VideoManager EX.

Users can edit some of a media file's properties. To do so, click ✎ ***Edit properties***. Users can edit the following properties:

- ***Operator name*** - who recorded the media file.

> 💡 *To change the **owner** of a media file, administrators must instead change the sharing settings for it.*

- ***Device name*** - which body-worn camera recorded the media file.

- 📅 ***Start time*** - when the media file was initially added to VideoManager EX. This either means when the body-worn camera which filmed the media file was redocked, or when the media file was uploaded from the user's PC.

This does **not** change when the media file was actually recorded.

Click ***save changes***.

3.5 Add Location Information to a Media file

Sufficiently privileged users can add location data to VideoManager EX media files which were recorded without it. This is useful if the original media file was recorded on a body-worn camera without GPS, and the user wants to add location data retroactively. Users **cannot** edit location data that was recorded alongside a media file.
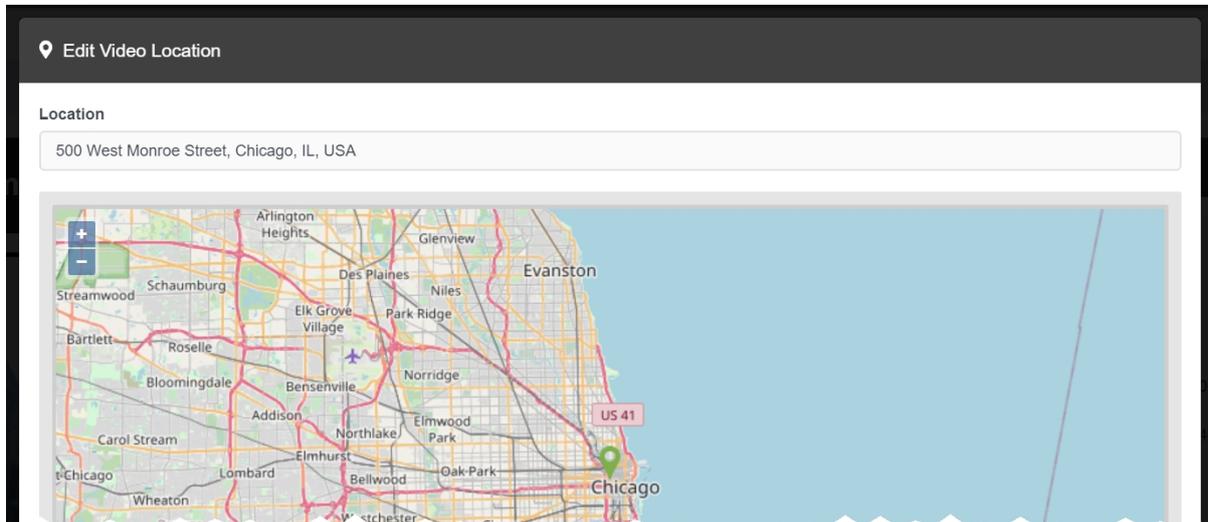
To add location data to a media file, or edit previously existing location data:

1. Navigate to the *Media* tab.

2. Find the relevant media file, and click **>** *More Details* next to it.

    Users can find the relevant media file by navigating to the *My Media*, *Shared Media*, or *Supervised Media* panes. They can also search for the relevant media file from the **🔍** *Search Media* pane.

3. In the **📍** *Location* pane, click **✏** *Edit location*.

4. Click and drag the map to position the marker at the desired location.

    > 💡 *If the user has chosen a lookup provider from the Maps section, in the Admin tab, they can also manually search for a location.*

5. Click *confirm* to save.

3.6 Prepare Media

Users can prepare media to obscure sensitive information.
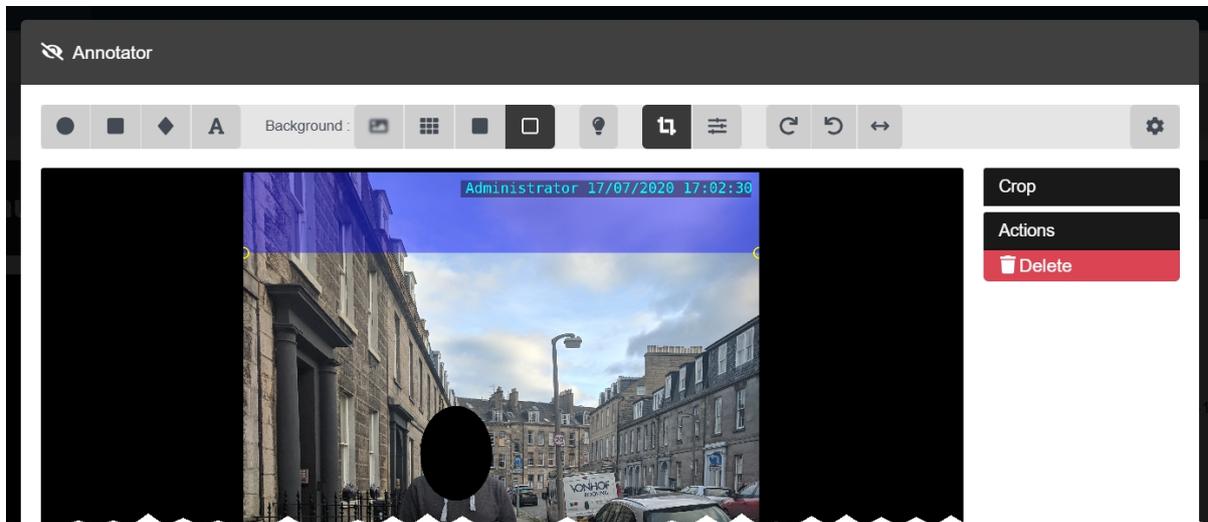
To prepare media:

1. Navigate to the **Media** tab.

2. Find the relevant media file, and click **>** **More Details** next to it.

   Users can find the relevant media file by navigating to the **My Media**, **Shared Media**, or **Supervised Media** panes. They can also search for the relevant media file from the 🔍 **Search Media** pane.

3. Click 👁 **Prepare Media**.

4. The user can now prepare media files in the same way they would redact an incident clip.

   >> For more information, see Redact an Incident Clip on page 37

   If the prepared media file is added to an incident, it will retain the redactions added here - users can add new redactions. However, if the media file is later redacted from this page again, the media file that was added to incidents beforehand will **not** be updated accordingly. The media file must be deleted and re-added to the incident for new changes to appear.

There are some image-exclusive actions that users can take when preparing media. These are:

- ⊡ **Crop the image to size** - draw the square around the subject of the image - anything in the blue section will not be featured in the finished media.

   💡 *The cropped version of the image will not be shown until the user is finished with their preparation and clicks **confirm**.*

- ⇄ *Adjust the image* - if the user clicks this, a set of sliders will appear in the right-hand menu. These sliders control *Contrast*, *Brightness*, *Saturation*, and *Gamma*.

Users can click ✖ *Restore Defaults* to restore the default settings for each slider.

3.7 Perform Media File Actions

VideoManager EX gives users the option to perform actions on their media files from the **More Details** pane. It is possible to perform most of these actions from the **Search Media** page as well.

From the **More Details** pane, sufficiently privileged users can perform a range of actions.

To reach the **＞ More Details** pane:

1. Navigate to the **Media** tab.

2. Find the relevant media file, and click **＞ More Details** next to it.

    Users can find the relevant media file by navigating to the **My Media**, **Shared Media**, or **Supervised Media** panes. They can also search for the relevant media file from the **Q Search Media** pane.

From here, users can perform the following actions:

-   To create an incident including this media file, click **Create new incident**.

This will create an incident containing the media file.

> >> For more information, see Create Incidents Manually and Perform Incident Actions on page 31

-   To add a media file to a previously-created incident, click **Add media to existing incident**. Click **＞ Add to this incident** next to the relevant incident.

-   To verify a media file, which indicates whether it has been tampered with since being uploaded from a user's body-worn camera, click **Verify file integrity**.

If successful, a green icon will appear in the **Verification** section of the **Properties** pane.

-   To download a .zip containing information about the media file's signature, click **Download signature verification report**.

The downloaded .zip contains the following information about the media file:

-   certificate-chain.pem - the PEM-encoded list of certificates included in the signature that was verified by VideoManager EX.

-   signature.jws - the raw signature file retrieved from the body-worn camera.

- signed-payload.txt - the manifest from the report. This is a JSON structure with the body-worn camera DID, filename, file size, and SHA256.

- trust-root.pem - the PEM-encoded trust root from the signature certificate chain.

- signature-info.txt - a report on the signature check. This contains information about the file when it was downloaded (compared against the signature during the initial signature check), information about the signature, information about the file as it is now (compared against the signature when the report was down-loaded), and a description of the certificate chain, including the serial, subject, issuer, and validity period of each certificate.

For more information about setting up Azure authentication with VideoManager EX, please navigate to the Motorola Solutions Learning Experience Portal (registration is free) and search for *VideoManager EX X.509 Footage Signing Explained*.

- To download the media file file to the user's PC, which is the only way to share a media file with workers who are not on VideoManager EX, click 📥 *Download original file*.

The media file will be saved to the PC's default download location.

- To view the media file's audit log, which reflects **all** actions taken on the media file since it has been added to VideoManager EX, click 📋 *View Video Audit Log*, and filter the audit log using the following fields:

  - *Source* - this will return actions performed on the media file by the specified source (e.g. a body-worn camera on VideoManager EX).

  - *Event type* - this will return specific actions performed on the media file.

  If the user starts entering an event, VideoManager EX will suggest various event options (e.g. **FOOTAGE_PLAY**).

  - *User* - this will return actions performed on the media file by the specified user.

  If the user starts entering a username, VideoManager EX will suggest various usernames to match it.

  - *Message* - this will return specific actions performed on the media file, whose details match the keywords entered here.

  For example, the **FOOTAGE_PLAY** event comes with the message *View Media file File*.

  - *Signature* - the user should enter the signature of an incident. This will return actions performed on the media file in relation to this incident.

  For example, when the media file was added to the specified incident.

  - *Location* - this will return actions performed on the media file from a specific DockController or EdgeController.

  - *Client* - this will return actions performed on the media file from a specific IP address.

  - *Server* - this will return actions performed on the media file from a specific server hosting VideoManager EX.

- From the *Date range* dropdown, users can select the date range for these actions.

- To delete the media file, which will remove it from the *Media* tab and VideoManager EX, click 🗑 *Delete Media*.

For a short while a deleted media file can still be "undeleted", depending on how VideoManager EX's deletion policy has been configured, using the *Include deleted media* option when searching from the 🔍 *Search Media* pane.

- To flip the media file, click ↻ *Rotate* and select whether the media file will be flipped to the left, to the right, or horizontally.

Apart from audit logs, it is possible to perform these actions from the *Search Media* page as well.

3.8 Bulk Edit Media Files

Bulk edits allow users to perform actions on multiple media files at once. This is useful if there are too many media files to manually edit.
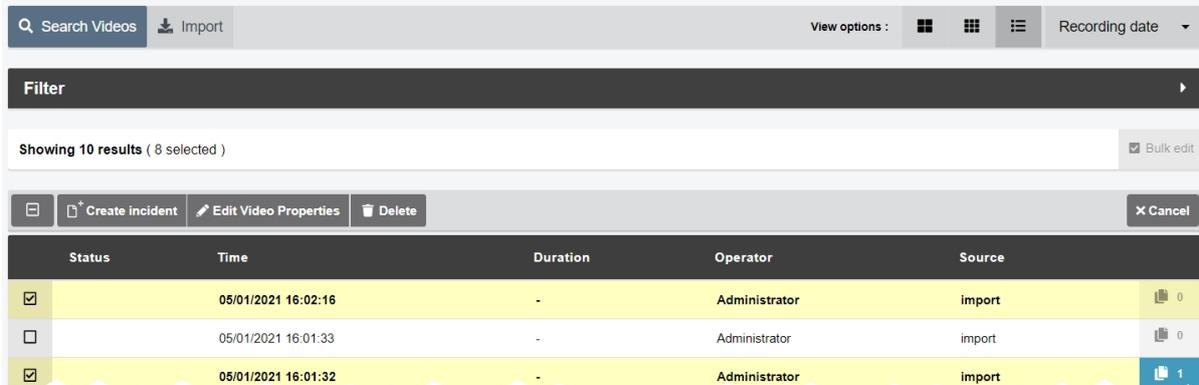
To bulk edit media files:

1. Navigate to the *Media* tab.

2. Select the **Q** *Search Media* pane.

3. Filter the media files as necessary, and click *Find media*.

4. Optionally select ☰ *List* from the *View options* menu.
   This will show more results per page than the *Large* or *Gallery* views.

5. Click ☑ *Bulk edit*.
   The bulk edit user interface appears. The user can now select media files to be bulk edited:

   • To select **indvidiual** media files, click ■ next to their rows.

   • To select **all** media files onscreen, click ■/☑ **Toggle selection of ALL rows.**.
   If there is an overflow of media files, VideoManager EX will also give users the option to select the media files which are not onscreen. To manually de-select individual media files, click on their row.

Once the user has selected media files for bulk editing, the following options are available:

   • ↻ **Rotate** - this presents a dropdown which gives users the ability to rotate multiple media files clockwise, anti-clockwise, 180 degrees, or horizontally.

   • ➕ **Create incident** - this gives users the ability to create an incident with all the selected media files included.

   • ➕ **Add to incident** - this gives users the ability to add multiple media files to an existing incident.

- ✏ **Edit properties** - this gives users the ability to edit the fields for all media files simultaneously.

In addition to the default fields (*Operator name* and *Device name*), users can also edit any user-defined media fields which have been created.

> ⚠ *Caution*   *If fields are bulk edited, any configuration they had previously will be overwritten.*

- ◁ **Edit sharing** - this gives users the ability to share multiple media files with other users simulatenously.

  - In the *Owner* field, administrators can change the owner of the media files.

  This can be a user or an entire group. If the owner of the media files is a group, **all** users in that group will be able to process the media files as if the media files were their own (i.e. adding them to incidents, redacting them).

  - If *Restricted* is set to *Yes*, only users with the *List restricted media* permission will be able to search for the media files. Only users with the *Play restricted media* permission will be able to watch the media files.

  - In the *Shared:* field of the *Sharing* panel, enter the name of the user, with whom these media files will be shared.

  Click ✚ next to this field to add this user to the list - if the user does not click ✚, the other user will not be added.

- 🗑 **Delete** - this gives users the ability to delete all of the selected media files simultaneously. The user will be asked to confirm their choice.

To exit bulk edit mode, click ✖ *Cancel*.

4 Incidents

The *Incidents* tab provides access to all incidents available to VideoManager EX and related functions which users can perform on incidents. Users can:

- Create, edit and delete incidents.

> >> For more information, see Create Incidents Manually and Perform Incident Actions on page 31

- Create, edit and delete incidents with bulk edit.

Users can select multiple media files and include them all in one incident simultaneously.

> >> For more information, see Create Incidents with Bulk Edit on page 34

- Add media files to an incident after it has been created.

> >> For more information, see Add a Media File to an Existing Incident on page 35

- Clip evidential media in an incident.

> >> For more information, see Clip Videos in an Incident on page 36

- Redact media in an incident.

> >> For more information, see Redact an Incident Clip on page 37

- Search previously-created incidents, create saved searches, and perform advanced searches.

> >> For more information, see Search Incidents on page 56

- Bulk edit incidents.

> >> For more information, see Bulk Edit Incidents on page 58

- Create, edit and delete bookmarks for media files in incidents.

These can be used to highlight portions of evidential media.

> >> For more information, see Create, Edit and Delete Bookmarks on page 59

4.1 Create Incidents Manually and Perform Incident Actions

Incidents are the mechanism through which evidence pertaining to a specific event is collated. This evidence could be media files from a body-worn camera, imported media files. Media files in an incident can be edited and redacted to preserve evidential integrity. Incidents can be shared with users either on the VideoManager EX system or outside of it.

There are two ways to create an incident.

The first way to create an incident is from the *Media* tab. Users should follow these steps if there is a specific media file they know they want to include in an incident.

1. Navigate to the *Media* tab.

2. Find the relevant media file, and click ⊞ *Create new incident* next to it.

   Users can find the relevant media file by navigating to the *My Media*, *Shared Media*, or *Supervised Media* panes. They can also search for the relevant media file from the 🔍 *Search Media* pane.

3. If the media file is part of a longer recording because the body-worn camera which recorded it has been configured to split long recordings up into individual media files (through its device profile), the entire recording can be added to this incident as well. To do so, set *Add whole recording to incident?* to *On*.

4. If the operator who recorded this media file also recorded other media files at the same time (e.g. because multiple body-worn cameras were assigned to one operator), those media files can be added to this incident as well. To do so, set *Add other footage from same operator?* to *On*.

5. Click *Create incident*.

The second way to create an incident is from the *Incidents* page. Users should follow these steps if they are not sure of which media files they will include in the incident yet.

1. Navigate to the *Incidents* page.

2. Click ⊞ *Create incident*.

   The *New Incident* page will open, without any media files attached to it. Users can add media files later by navigating to the *Media* tab, finding the relevant media file, and clicking ⊞ *Add to this*

incident next to it.

>> For more information, see Add a Media File to an Existing Incident on page 35

From here, the process for filling in an incident's fields are identical, regardless of how the incident was created:

1. In the *Title* field, enter the name of the incident.

This field is mandatory.

2. Optionally populate the following fields:

   • The *Creation Time* field cannot be edited. It shows when the incident was first created.

   • The *Update Time* field cannot be edited. It shows when the incident was last edited.

   • In the *Incident time* field, enter a time for the incident. This could be when the media files were recorded, or when a specific event took place.

   • In the *Notes* field, enter any notes regarding the incident.

   • The *Clip Count* field cannot be edited. It shows how many media files are in the incident, and is automatically updated when a media file is added or removed.

   • The *Owner* field cannot be edited. It shows the username of whoever is creating the incident.

   • The *Signature* field cannot be edited. It is automatically populated by VideoManager EX upon creation.

3. If necessary, clip the media files which have been added to the incident. This enables users to focus on the relevant sections of media file.

>> For more information, see Clip Videos in an Incident on page 36

4. If necessary, redact the media files which have been added to the incident. This enables users to obscure sections of the media file, in line with privacy regulations.

>> For more information, see Redact an Incident Clip on page 37

5. Click *Create incident*.

Once created, there are multiple actions that can be performed on an incident.

   • Edit an incident.

To do so, click ✏ *Edit incident*, and make the relevant changes. Click *Save incident* to save the incident.

> ☀ *Here, users can add incident attachments from their PC, but they **cannot** add media files from VideoManager EX. This is done from the **Media** tab.*
>
> > >> *For more information, see* Add a Media File to an Existing Incident on page 35

- Duplicate an incident. This will copy the incident's clips (and any redactions applied to them), ***Title***, ***Time***, ***Reference***, and ***Notes***. However, the incident's ***Signature*** and creation time will be different. Furthermore, the ***Owner*** for the duplicated incident will be whoever duplicated the incident, **not** who created the original incident.

To do so, click ⊞ ***Duplicate incident***, and make any necessary changes to the copy of the incident. Click ***Create incident***.

- Delete an incident. This will **not** delete any of the media files within the incident itself.

To do so, click 🗑 ***Delete incident***, and confirm the deletion by clicking ***Delete Incident***.

> ☀ *For a short while, an incident can still be "undeleted", using the **Show recently deleted incidents** option when searching from the* 🔍 ***Search Incidents*** *pane.*

4.2 Create Incidents with Bulk Edit

If a user wishes to add multiple media files to an incident simultaneously, they should use the bulk edit function. This is done from the *Media* tab.

To create an incident with bulk edit:

1. Navigate to the *Media* tab.

2. Select the $\mathbf{Q}$ *Search Media* pane.

3. Filter the media files as necessary, and click *Find media*.

4. Optionally select ☰ **List** from the *View options* menu in the top right-hand corner.

   This will display more media files per page than the **Large** or **Gallery** view, making it easier to select multiple media files simultaneously.

5. Click ☑ *Bulk Edit*.

6. Click ■ next to the relevant media files, or click ☑ **Toggle selection of ALL rows.** to select all media files.

7. Click ➕ **Create incident**.

   All selected media files will be added to the incident as incident clips. Users can rearrange them in the following manners:

   • To arrange the incident clips by recording time (earliest first, latest last), click ↓≡ *Sort by time*.

   • To arrange the incident clips in a custom order, click ❙❙ and drag the incident clip to the desired position.

8. Complete the incident fields as normal, and click *Create incident*.

4.3 Add a Media File to an Existing Incident

Users can add a media file to an already-existing incident. This is useful if the incident was created before the media file was imported or downloaded, but the media file should be added to it anyway.

To add a media file to an already-existing incident:

1. Navigate to the *Media* tab.

2. Find the relevant media file, and click **>** *More Details* next to it.

    Users can find the relevant media file by navigating to the *My Media*, *Shared Media*, or *Supervised Media* panes. They can also search for the relevant media file from the ⊞ *Search Media* pane.

3. The following steps differ, depending on how many media files should be added to the incident:

    *   If the user is adding **one** media file to the incident, click ▤ *Add media to existing incident* next to it.

    *   If the user is adding **multiple** media files to the incident, click ☑ *Bulk edit*. Select the relevant media files by clicking ■ next to their rows, or click ■ **Toggle selection of ALL rows.** to select **all** media files onscreen. Click ⊞ **Add to incident**.

4. Filter the incidents as normal, and click *Find incidents*.

5. Click ⊞ *Add to this incident* next to the relevant incident.

6. If the incident contains multiple incident clips, users can now rearrange them in the following manners:

    *   To arrange the incident clips by recording time (earliest first, latest last), click ↓☰ *Sort by time*.

    *   To arrange the incident clips in a custom order, click ❙❙ and drag the incident clip to the desired position.

7. Click *Save incident*.

4.4 Clip Videos in an Incident

Videos in an incident can be clipped to focus only on the relevant aspects of the evidence. This is useful if, for example, a body-worn camera has recorded many hours of media, of which only a few minutes are relevant. However, the original video is never shortened - only the version of the video in the incident.
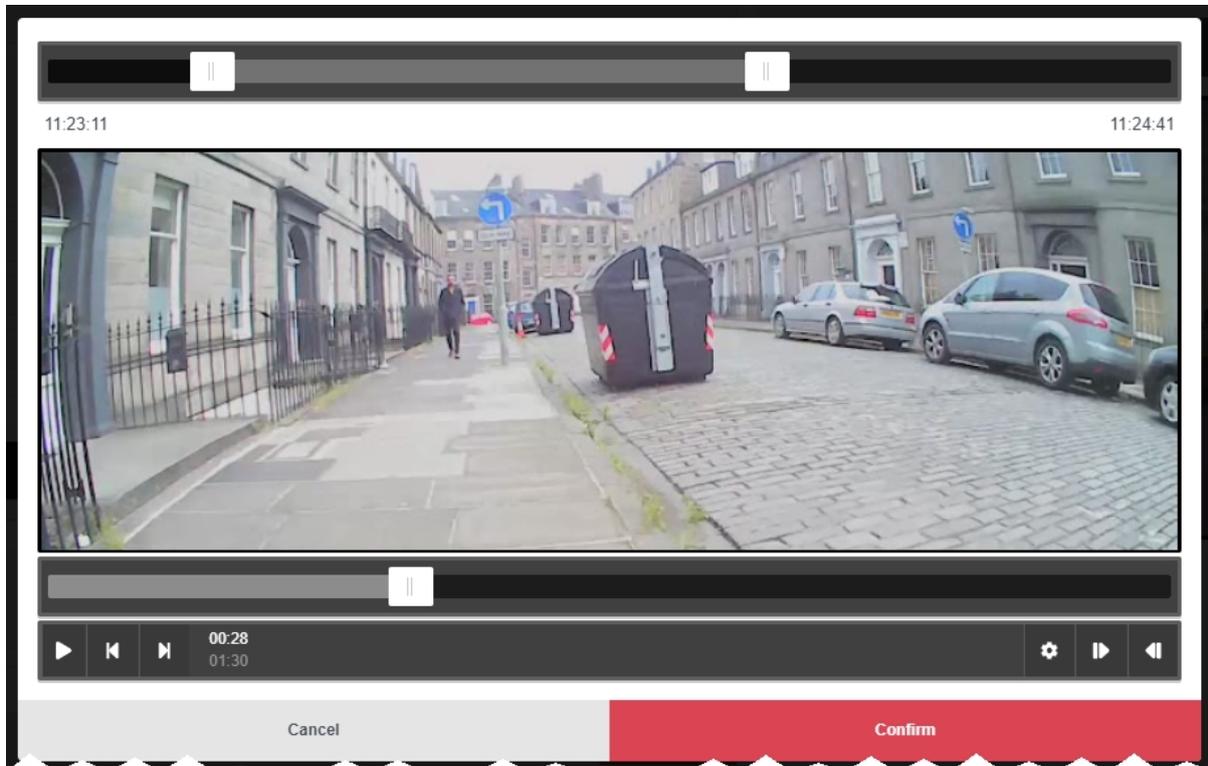
To clip a video:

1. Navigate to the *Incidents* tab.

2. Find the relevant incident, and click ✏ *Edit incident* next to it.

   Users can find the relevant incident by navigating to the *My Incidents*, *Shared Incidents*, or *Supervised Incidents* panes. They can also search for the relevant incident from the 🔍 *Search Incidents* pane.

3. Click ✂ *Edit clip start/end time* next to the relevant media file.

4. To shorten the media file roughly, select the start and end time of the clip by dragging the toggles in the **top** video progress bar.

5. For a more precise clipping, drag the toggle in the **bottom** video progress bar to the relevant point and click *Set Start of Clip* in the bottom right-hand corner. This will shorten the video to the point specified. Do the same for the end of the clip, using *Set End of Clip*.

6. Click *confirm*.

4.5 Redact an Incident Clip

The *Incident Clip Redactor* lets users apply a variety of redactions, text annotations and redaction effects to a media file in an incident. This is useful if data protection laws require certain features of the media file to be obscured (e.g. faces), or if users want to highlight a specific aspect of the media.
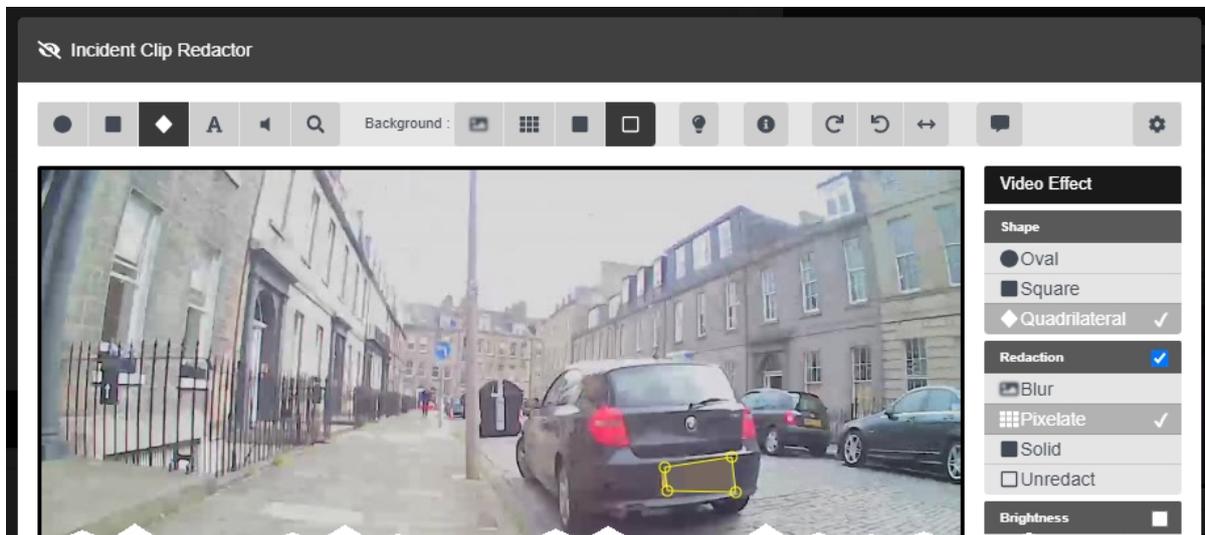
To open the *Incident Clip Redactor*:

1. Navigate to the *Incidents* tab.

2. Find the relevant incident, and click 🖉 *Edit incident* next to it.

   Users can find the relevant incident by navigating to the *My Incidents*, *Shared Incidents*, or *Supervised Incidents* panes. They can also search for the relevant incident from the 🔍 *Search Incidents* pane.

3. In the *Incident clips* section, click 🚫 *Redact parts of this clip*.

There are several types of redaction effect available in VideoManager EX:

- Foreground redactions.

  >> For more information, see Create Foreground Redactions on page 39

- Background redactions.

  >> For more information, see Create Background Redactions on page 41

- Audio redactions.

  >> For more information, see Create Audio Redactions on page 43

- Text redactions.

>> For more information, see Create Text Annotations on page 45

- Brightness redactions.

>> For more information, see Create Brightness Redactions on page 47

- Zoom redactions.

>> For more information, see Create Zoom Redactions on page 49

- Tramscriptions.

>> For more information, see Create a Transcript for an Incident Clip on page 52

- Other redactions, such as flipping and rotating a clip.

>> For more information, see Create Other Redactions on page 51

Users can also access the redaction **Advanced** dropdown.

>> For more information, see Access the Redaction Advanced Dropdown on page 54

Once a redaction has been created, the following actions can be performed on it:

- Edit a redaction.

To do so, click ✏ **Edit incident**. In the **Incident clips** section, click 🔍 **Redact parts of this clip**. Step forwards through the media file to the point that the redaction starts, and select the redaction by clicking it. Make the necessary changes, click **confirm**, then **Save incident**.

- Delete a redaction.

To do so, click ✏ **Edit incident**. In the **Incident clips** section, click 🔍 **Redact parts of this clip**. Step forwards through the media file to the point that the redaction starts, and select the redaction by clicking it. In the right-hand menu bar, click 🗑 **Delete**. Click **confirm**, then **Save incident**.

4.5.1 Create Foreground Redactions

A circle, rectangle, or quadrilateral redaction can blur, pixelate, or solidly cover the focus of a media file. This allows users to redact faces or other sensitive information, in accordance with data protection laws. It is also possible to redact the background and have the area inside the redaction show the original media file.
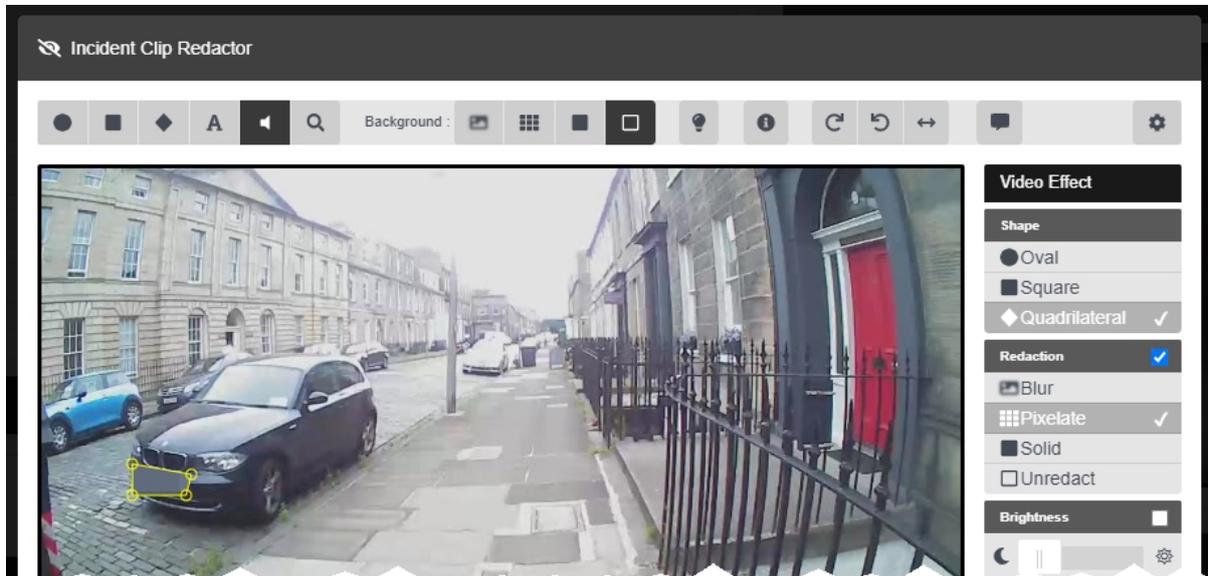
To create a foreground redaction:

1. Navigate to the *Incidents* tab.

2. Find the relevant incident, and click ✏ *Edit incident* next to it.

   Users can find the relevant incident by navigating to the *My Incidents*, *Shared Incidents*, or *Supervised Incidents* panes. They can also search for the relevant incident from the 🔍 *Search Incidents* pane.

3. In the *Incident clips* section, click 🔏 *Redact parts of this clip*.

4. Step forwards through the media file to the point that the redaction should start.

5. Click either ● *Insert oval*, ■ *Insert square*, or ◆ *Insert quadrilateral*.

6. Draw a shape around the area to be redacted. This shape will be saved immediately.

   The user can drag out the corners of the shape to fit the area which must be redacted.

   A right-hand menu will appear.

7. If relevant, users can change the shape of the redaction from the *Shape* pane.

8. If relevant, check the ☑ box in the *Redaction* pane, and select the type of redaction that will fill the highlighted area.

   Users have a choice of 🖼 *Blur*, ⊞ *Pixelate*, and ■ *Solid*.

9. If relevant, check the ☑ box in the *Brightness* pane and adjust the brightness of the redaction using the slider.

10. If the subject of the media file is static, simply skip to the part of the media file where the redaction should end, and click ✖ *End*. Alternatively, if the subject of the media file is moving, the user has two options:

   • **Automatically** track the subject of the media file by pressing and holding 〈 🐾 (to track backwards) or 〉 🐾 (to track forwards). This will follow the subject of the media file frame-by-frame, updating the position of the redaction auto-matically

   ---

   💡   *VideoManager EX can only change the **position** of the redaction, not its **size or shape**. For this reason, the user may still need to manually reposition the redaction.*

   • **Manually** track the subject of the media file by using ◀ *Step Backward* / ▶ *Step Forward* to step through the media file frame-by-frame and repositioning the shape to ensure that it is focused on the subject at all times.

11. When the user reaches the part of the media file where the redaction should end, click ✖ *End*.

12. Repeat this for every new redaction to be added.

13. Click *confirm*.

14. Click *Save incident*.

4.5.2 Create Background Redactions

By redacting a background, the subject of evidential media is made the sole focus. All foreground redactions can be applied to the background of a media file too, leaving an area or areas unaffected by the redaction. This allows users to blur places and surroundings, in accordance with data protection laws.
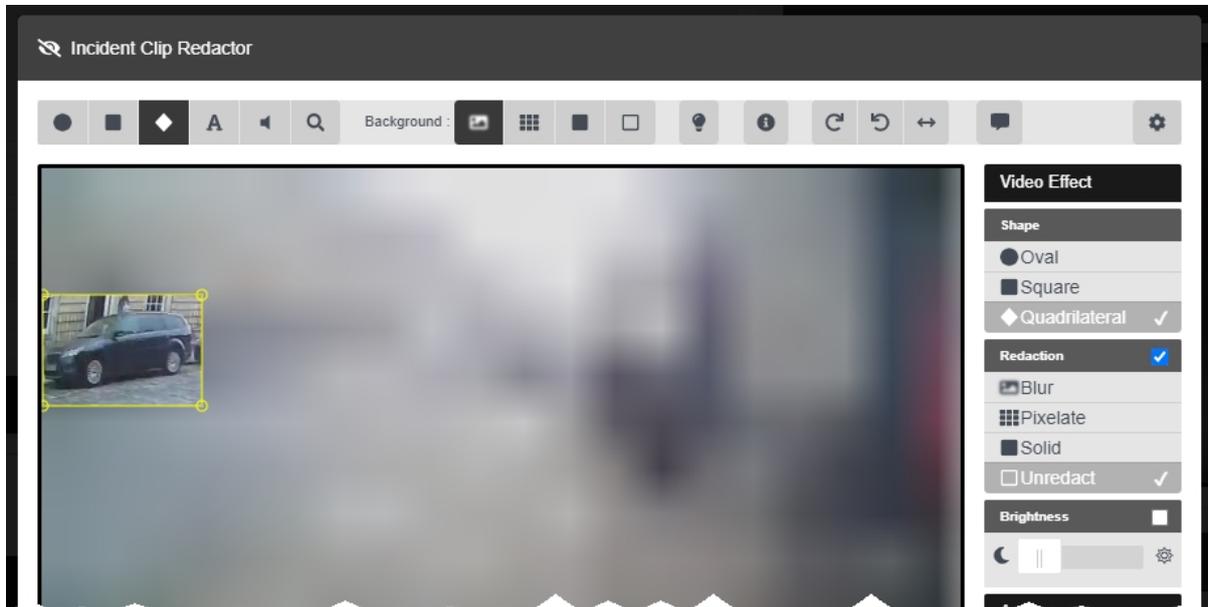
To create a background redaction:

1. Navigate to the *Incidents* tab.

2. Find the relevant incident, and click ✏ *Edit incident* next to it.
    Users can find the relevant incident by navigating to the *My Incidents*, *Shared Incidents*, or *Supervised Incidents* panes. They can also search for the relevant incident from the 🔍 *Search Incidents* pane.

3. In the *Incident clips* section, click 🔍 *Redact parts of this clip*.

4. Step forwards through the media file to the point that the redaction should start.

5. Click either ● *Insert oval*, ■ *Insert square*, or ◆ *Insert quadrilateral*.

6. Draw a shape around the area which will remain **unredacted**. This shape will be saved immediately.
    The user can drag out the corners of the shape to fit the area which must be redacted.
    A right-hand menu will appear.

7. If relevant, users can change the shape of the redaction from the *Shape* pane.

8. For each redaction area, check the ■ box in the *Redaction* pane, and select ■ *Unredact*.

9. In the top menu, select the kind of background redaction required.

Users have a choice of ▨ *Blur*, ⠿ *Pixelate*, and ■ *Solid*.

10. If the subject of the media file is static, simply skip to the part of the media file where the redaction should end, and click ✖ *End*. Alternatively, if the subject of the media file is moving, the user has two options:

- **Automatically** track the subject of the media file by pressing and holding ＜ 🐾 (to track backwards) or ＞ 🐾 (to track forwards). This will follow the subject of the media file frame-by-frame, updating the position of the redaction automatically

---

🔅 *VideoManager EX can only change the **position** of the redaction, not its **size or shape**. For this reason, the user may still need to manually reposition the redaction.*

- **Manually** track the subject of the media file by using ⏮ *Step Backward* / ⏭ *Step Forward* to step through the media file frame-by-frame and repositioning the shape to ensure that it is focused on the subject at all times.

11. When the user reaches the part of the media file where the redaction should end, click ✖ *End*.

12. Click *confirm*.

13. Click *Save incident*.

To delete a background redaction, change the background redaction to *None*.

4.5.3 Create Audio Redactions

Users can mute or beep over audio in media files for a predetermined length of time. This enables users to redact voices and other noises, in accordance with data protection laws. Users can also redact a media file so it plays audio from the body-worn camera's secondary microphone.
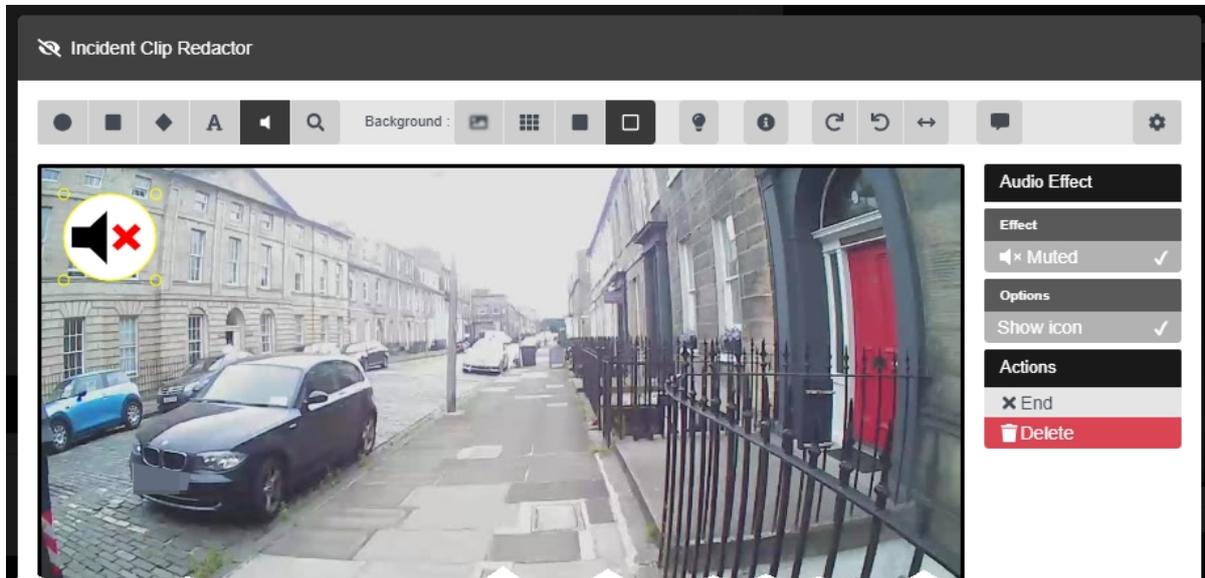
To create an audio redaction:

1. Navigate to the **Incidents** tab.

2. Find the relevant incident, and click ✏ **Edit incident** next to it.

Users can find the relevant incident by navigating to the **My Incidents**, **Shared Incidents**, or **Supervised Incidents** panes. They can also search for the relevant incident from the 🔍 **Search Incidents** pane.

3. In the **Incident clips** section, click 🚫 **Redact parts of this clip**.

4. Step forwards through the media to the point that the redaction should start.

5. From the top toolbar, click 🔊 **Insert audio effect**, and draw it over an area of the media.

If no icon is desired, deselect the **Show Icon** setting from the **Options** pane.

6. In the right-hand menu, select a specific type of audio redaction from the **Effect** section. The options are as follows:

   • **Muted** - no audio will be played for this section of the incident clip.

   • **2nd Channel** - if the media file was recorded on a VB400, only audio recorded by the VB400's second microphone will be played for this section of the incident clip.

   This is useful if the incident clip features a loud noise; using the second microphone may make

other audio in the media file clearer.

- **Beep** - a beep will mask the audio for this section of the incident clip.

7. Step forwards through the media file to the point that the audio redaction is no longer required, and click ✖ *End*.

4.5.4 Create Text Annotations

Text annotations are text boxes which can be moved and resized in the same way as other redactions. This enables users to provide information about a subject or event within the media file itself.
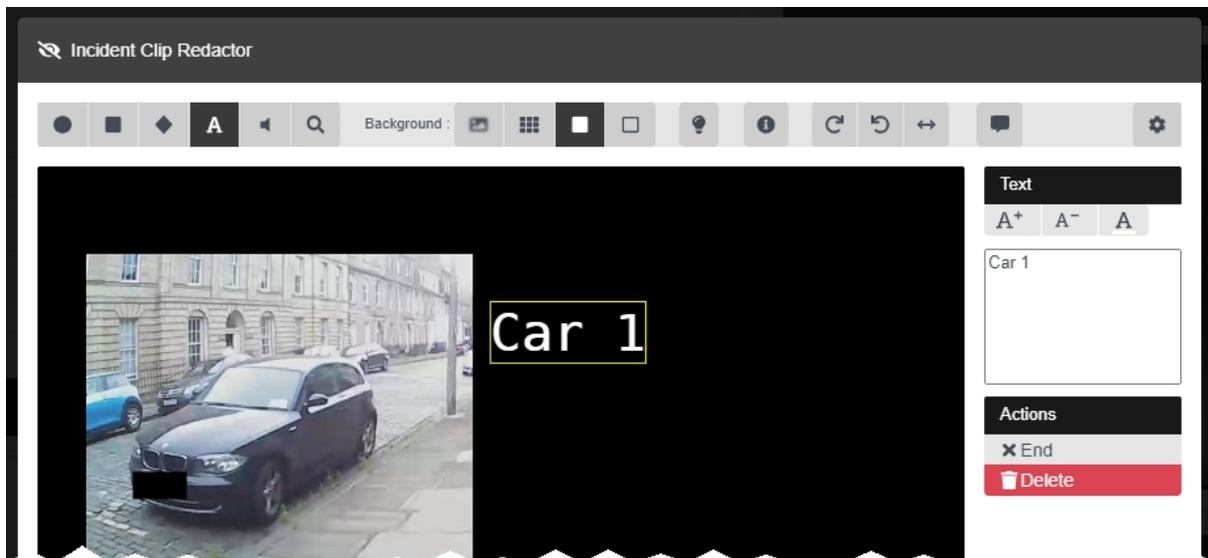
To create a text annotation:

1. Navigate to the **Incidents** tab.

2. Find the relevant incident, and click ✏ **Edit incident** next to it.

Users can find the relevant incident by navigating to the **My Incidents**, **Shared Incidents**, or **Supervised Incidents** panes. They can also search for the relevant incident from the **Q** **Search Incidents** pane.

3. In the **Incident clips** section, click **Redact parts of this clip**.

4. Step forwards through the media file to the point that the redaction should start.

5. Click **A** **Insert text**.

6. Click the area of the media file frame where the text annotation should be displayed.
The **Text** panel is displayed.

7. In the right-hand menu, enter the text to be displayed.

Click **A** ➕ to make the text annotation bigger.

Click **A** ➖ to make the text annotation smaller.

Click **A** to change the colour of a text annotation.

💡 *Users can either choose a colour from the selection presented by VideoManager EX, or enter their own colour using Hex code. By clicking **C**, the Hex code colour will be saved and can be selected again from the row at the top.*

From here, the user has two options:

- If the subject of the media file is moving, step through the media file frame-by-frame and reposition the text manually to ensure that it is focused on the subject at all times, using ◀ *Step Backward* / ▶ *Step Forward*. When the user reaches the part of the media file where the redaction should end, click ✖ *End*.

Users do not need to redraw the annotation, just re-position it.

- If the subject of the media file is static, skip to the part of the media file where the redaction should end, and click ✖ *End*.

8. Click *confirm*.

9. Click *Save incident*.

4.5.5 Create Brightness Redactions

Brightness redactions are used to darken or brighten areas of the media file. This can be used to highlight the relevant parts of a piece of evidential media, and applies to both foreground and background redactions.
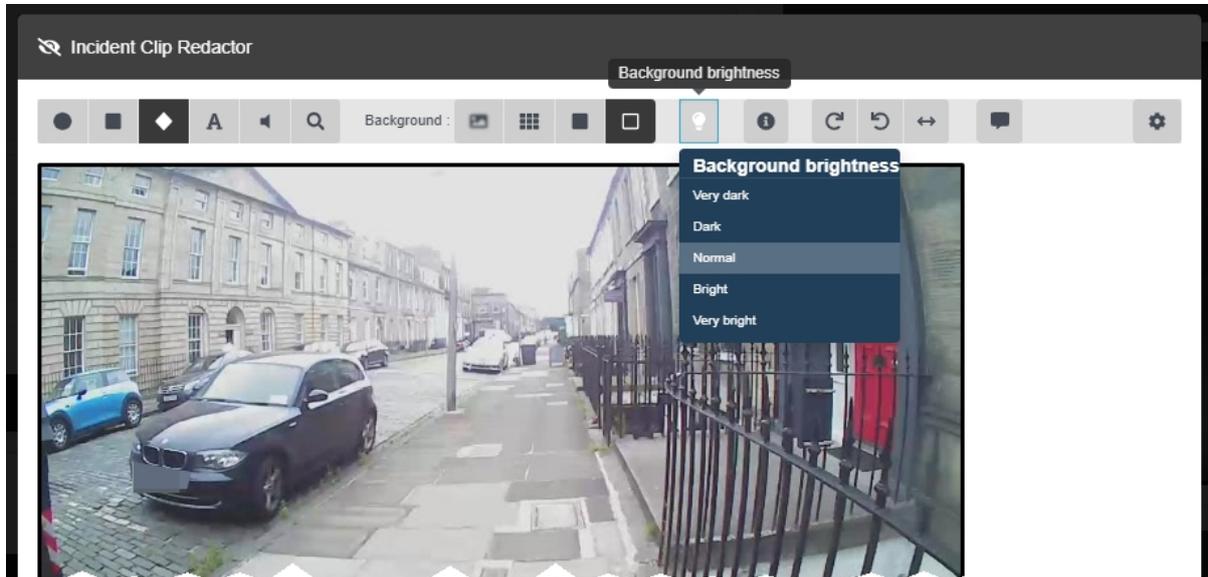
Users can create foreground brightness redactions. These highlight a specific area of the media file, in order to draw attention to it. To do so:

1. Navigate to the *Incidents* tab.

2. Find the relevant incident, and click ✏ *Edit incident* next to it.

   Users can find the relevant incident by navigating to the *My Incidents*, *Shared Incidents*, or *Supervised Incidents* panes. They can also search for the relevant incident from the 🔍 *Search Incidents* pane.

3. In the *Incident clips* section, click �e *Redact parts of this clip*.

4. Step forwards through the media to the point that the redaction should start.

5. Click either ⬤ *Insert oval*, ⬛ *Insert square*, or ◆ *Insert quadrilateral*, and use the cursor to draw the shape around the area that should be brightened or darkened.

6. Check the ☑ box in the *Redaction* pane, and select ⬛ *Unredact*. This will leave the area inside the redaction unredacted.

7. Check the ☑ box in the *Brightness* pane.

8. Use the slider to adjust the required brightness inside the redaction effects area.

   Moving the slider towards the 🌙 will make the area darker. Moving the slider towards the ☀ will make the area lighter.

9. If the subject of the media file is static, simply skip to the part of the media file where the redaction should end, and click ✖ *End*. Alternatively, if the subject of the media file is moving, the user has two options:

   • **Automatically** track the subject of the media file by pressing and holding ❮ 🐾 (to track backwards) or ❯ 🐾 (to track forwards). This will follow the subject of the media file frame-by-frame, updating the position of the redaction auto-matically

   ---

   💡 *VideoManager EX can only change the **position** of the redaction, not its **size or shape**. For this reason, the user may still need to manually reposition the redaction.*

   • **Manually** track the subject of the media file by using ◀| *Step Backward* / |▶ *Step Forward* to step through the media file frame-by-frame and repositioning the shape to ensure that it is focused on the subject at all times.

10. When the user reaches the part of the media file where the redaction should end, click ✖ *End*.

Users can create a background brightness redaction effect. This will affect any areas of the media file which are not covered by foreground redactions. To do so:

1. Select the 💡 *Background brightness* option from the top menu bar.

2. From the dropdown menu, choose the desired brightness level. This will apply to the entire duration of the media file. The options are **Very Dark**, **Dark**, **Normal**, **Bright**, and **Very Bright**.

4.5.6 Create Zoom Redactions

Zoom redaction effects focus on specific aspects of the media file. They can be used to highlight the relevant parts of a piece of evidential media.
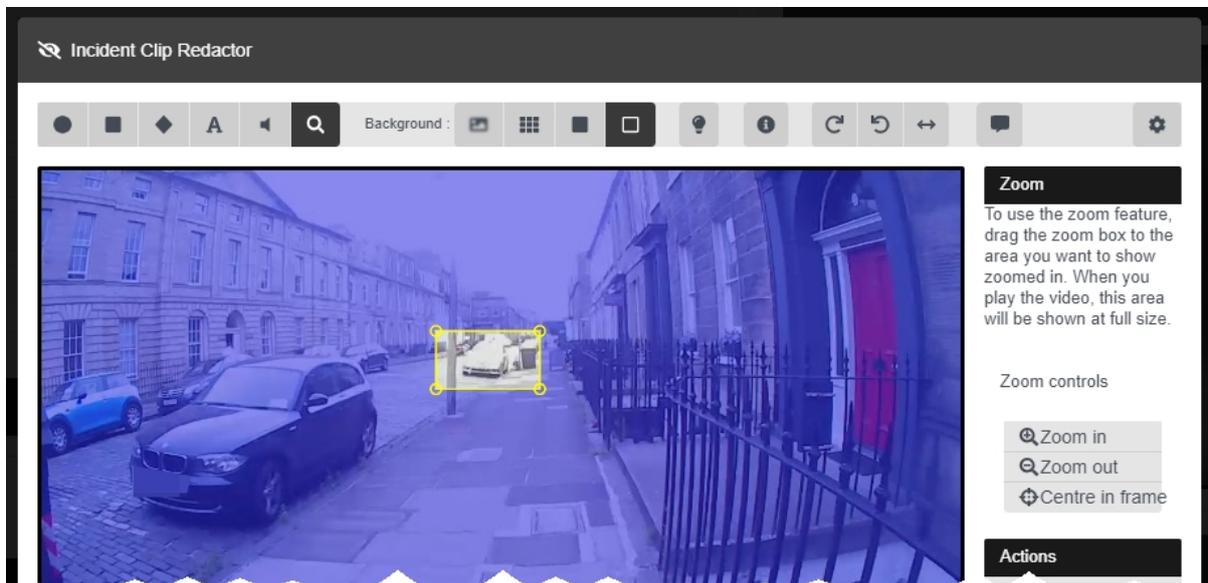
To create a zoom redaction:

1. Navigate to the **Incidents** tab.

2. Find the relevant incident, and click ✏ **Edit incident** next to it.

    Users can find the relevant incident by navigating to the **My Incidents**, **Shared Incidents**, or **Supervised Incidents** panes. They can also search for the relevant incident from the 🔍 **Search Incidents** pane.

3. In the **Incident clips** section, click 🔍 **Redact parts of this clip**.

4. Skip forward through the media file to where the redaction effect should start.

5. Click 🔍 **Zoom in on one area**.

6. Draw the square around the area of the media file which should be zoomed in (or out) on.

7. In the right-hand menu, use ⊕ **Zoom in**, ⊖ **Zoom out**, and ✛ **Centre in frame** to move and scale the redaction over the area which will be affected.

    💡   *The redaction effect will not appear until the media file is played like normal.*

    ---

8. If the subject of the media file is static, simply skip to the part of the media file where the redaction should end, and click ✖ **End**. Alternatively, if the subject of the media file is moving, the user has two options:

- **Automatically** track the subject of the media file by pressing and holding ❮ 🐾 (to track backwards) or ❯ 🐾 (to track forwards). This will follow the subject of the media file frame-by-frame, updating the position of the redaction automatically

---

💡   *VideoManager EX can only change the **position** of the redaction, not its **size or shape**. For this reason, the user may still need to manually reposition the redaction.*


- **Manually** track the subject of the media file by using ⏮ *Step Backward* / ⏭ *Step Forward* to step through the media file frame-by-frame and repositioning the shape to ensure that it is focused on the subject at all times.

9. When the user reaches the part of the media file where the redaction should end, click ✖ *End*.

10. Click *confirm*.

11. Click *Save incident*.

4.5.7 Create Other Redactions

There are some other redaction effects which can be performed on a media file.
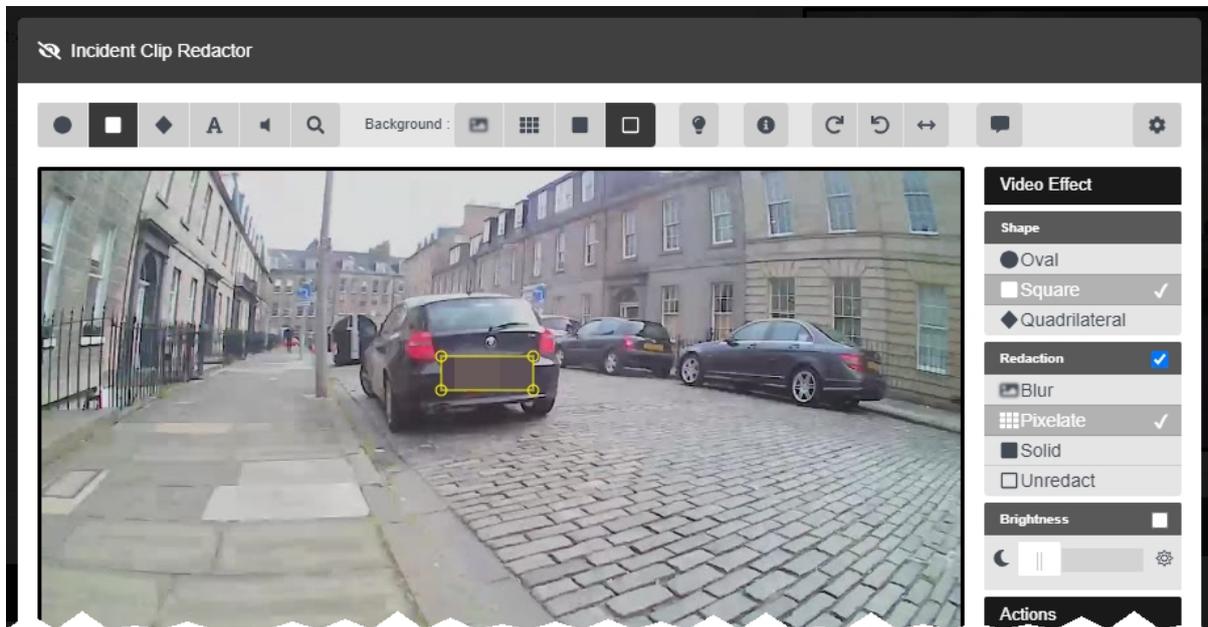
The other redaction effects can be found in the top menu bar. They are as follows:

- **C** *Rotate clockwise* - this rotates the media file by 90 degrees left.

- **⟲** *Rotate anti-clockwise* - this rotates the media file by 90 degrees right.

- **↔** - *Horizontal flip* - this flips the media file horizontally.

- **ⓘ** *Show metadata* - this displays the metadata recorded alongside the media file.
  Clicking this icon multiple times changes the position of the overlay text, then hides it entirely.

4.5.8 Create a Transcript for an Incident Clip

Once an incident clip has been added to an incident, users can create a transcript for it within the incident editor, or import an existing .vtt file. This will display captions over the incident clip.
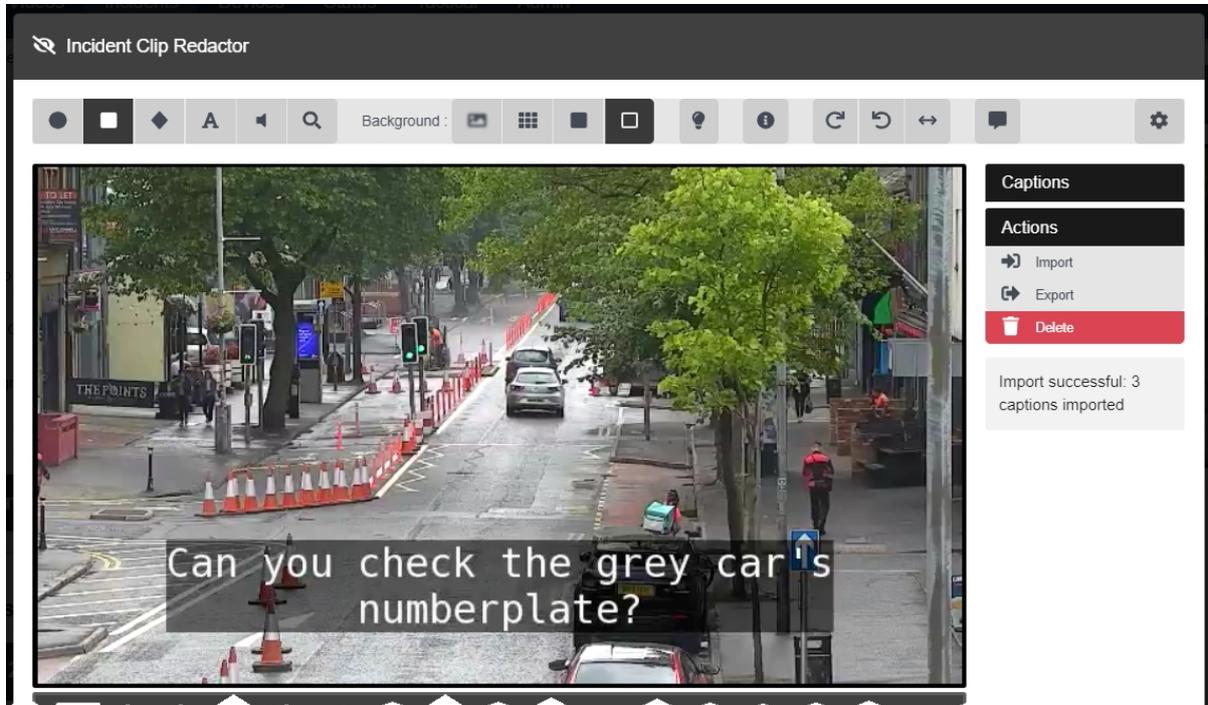
To create a new transcript for an incident clip:

1. Navigate to the *Incidents* tab.

2. Find the relevant incident, and click ✏ *Edit incident* next to it.

   Users can find the relevant incident by navigating to the *My Incidents*, *Shared Incidents*, or *Supervised Incidents* panes. They can also search for the relevant incident from the 🔍 *Search Incidents* pane.

3. In the *Incident clips* section, click 🔏 *Redact parts of this clip*.

4. Click 💬 *Transcription*.

5. In the left-hand *Speaker* window, enter a name or identifier for each individual who is speaking in the incident clip.

6. Use the player in the top left-hand corner to step forward in the incident clip, to the point where the transcription should begin.

7. In the left-hand menu pane, click 💬 *Add caption* next to the speaker who is currently speaking in the incident clip.

8. A new row will appear automatically in the *Transcription* window. Enter the relevant text.

9. Use the ▶ and ◀ buttons to navigate to the point in the incident clip where a new caption is needed.

10. In the left-hand menu pane, click 💬 *Add caption* again next to the speaker who is currently speaking in the incident clip.

11. Repeat as many times as necessary.

12. Once the transcript is complete, click **confirm**. The transcript will be saved.

To import an existing .vtt file into VideoManager EX:

1. Navigate to the *Incidents* tab.

2. Find the relevant incident, and click 🖊 *Edit incident* next to it.

   Users can find the relevant incident by navigating to the *My Incidents*, *Shared Incidents*, or *Supervised Incidents* panes. They can also search for the relevant incident from the 🔍 *Search Incidents* pane.

3. In the *Incident clips* section, click 🖌 *Redact parts of this clip*.

4. Click 💬 *Transcription*.

5. In the *Actions* field, click ➡ *Import*.

6. Select the previously-created .vtt file.

   If successful, the right-hand menu will show the transcript which has been successfully imported.

   To overwrite previously-imported captions with a new set of captions, click ➡ *Import* again and select the desired .vtt file.

To export a transcript from an incident clip, click ➡ *Export*. This will download the .vtt file to the PC running VideoManager EX.

💡   *This .vtt file will **not** be identical to the file which was originally imported - only the captions will be exported, without any styling or comments.*

To delete a set of captions from an incident clip, click 🗑 *Clear*.

4.5.9 Access the Redaction Advanced Dropdown

There are some actions which can be performed on redactions once they have been created. To access these, click *Advanced* in the top right-hand corner.
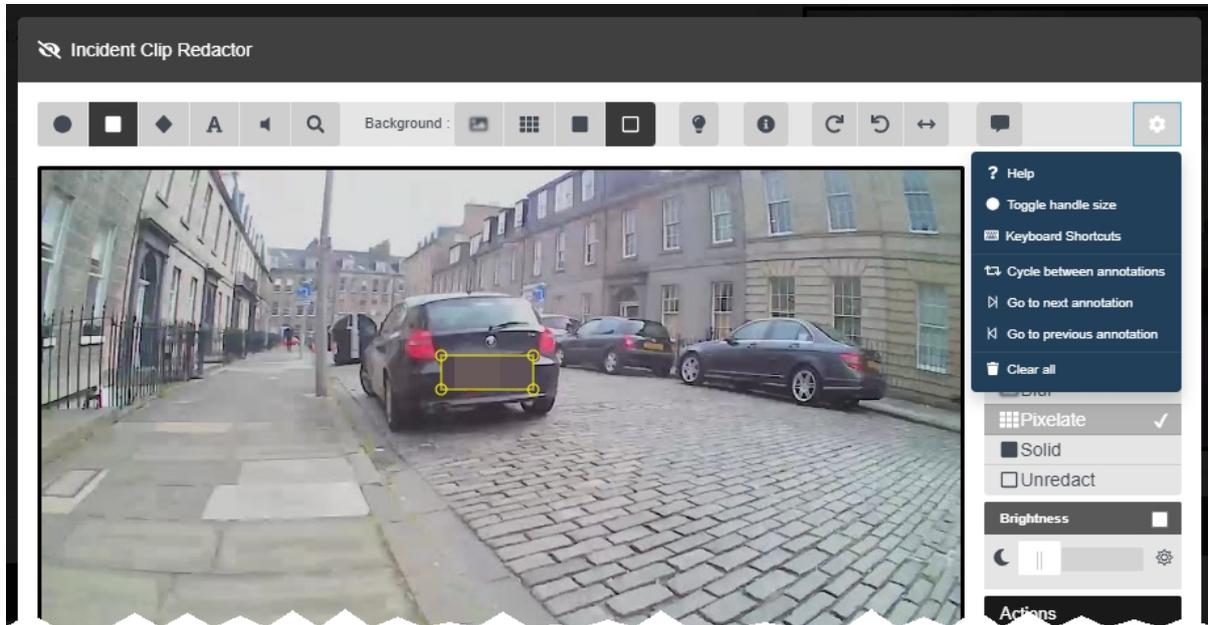
To access the redaction *Advanced* dropdown:

1. Navigate to the *Incidents* tab.

2. Find the relevant incident, and click ✏ *Edit incident* next to it.

    Users can find the relevant incident by navigating to the *My Incidents*, *Shared Incidents*, or *Supervised Incidents* panes. They can also search for the relevant incident from the 🔍 *Search Incidents* pane.

3. In the *Incident clips* section, click 🕲 *Redact parts of this clip*.

Users can now perform the following actions:

*   ❓ *Help* - this presents a brief summary of how to create a redaction effect.

*   ● *Toggle handle size* - if a redaction effect is selected, the handles on the redaction will get bigger. This is useful if the user wants to create a small redaction which needs more precise parameters.

*   ⌨ *Keyboard Shortcuts* - this will give the user information about the possible keyboard shortcuts they can perform to move through the media file more quickly.

*   ↳ *Cycle between annotations* - if a redaction effect is selected, clicking this will cycle through all the redaction effects in the media file, then go back to the beginning and begin again.

*   ▶| *Go to next annotation* - if a redaction effect is selected, clicking this will move to the next redaction effects one by one, then stop at the last one.

- ◀◀ *Go to previous annotation* - if a redaction effect is selected, clicking this will move to the previous redaction effects one by one, then stop at the first one.

- 🗑 *Clear all* - this will delete all redactions in the media file.

4.6 Search Incidents

It is possible to use VideoManager EX's search functions to locate incidents in the *Incidents* tab. This allows users to filter through a large number of incidents quickly.

Incidents can be searched by a number of criteria.

1. Navigate to the *Incidents* tab.

2. Select the 🔍 *Search Incidents* pane.

   Users can now filter incidents by the following criteria:

   - *Title* - search for incidents whose name matches the one entered.

   - *Incident Time* - using the *From:* and *To:* fields, search for incidents whose time matches the dates entered here.

   This refers to the customisable *Incident time* field users can populate when they are creating an incident - **not** the creation time of the incident itself.

   - *Reference Code* - search for incidents whose *Reference Code* field matches the text entered here.

   - *Notes* - search for incidents whose *Notes* field matches the text entered here.

   - 📅 *Earliest date* and *Latest date* - search for incidents whose media files were recorded between set dates.

   - *Device operator* - search for incidents containing media downloaded by a specified user.

   - *Owner* - search for incidents owned by a specified user.

   Click *My incidents* to search only for incidents that the logged-in user owns.

   - *Source* - search for incidents containing media files from a specified body-worn cameras or import sources.

   - *Match text* - search for incidents whose text (including title, reference code, and notes) matches the text entered here.

   There are also filters which can be checked:

- **Show current incidents** - select whether or not to include current (i.e. non-deleted) incidents.

- **Show recently deleted incidents** - select whether or not to include recently deleted incidents.

If users have the **Reinstate** permission set to **On**, they can reinstate deleted incidents. To do so, check the **Show recently deleted incidents** box, and click **Find incidents**. Next to the incident to be reinstated, click $\circlearrowright$ **Reinstate incident**.

      🔅   *Recently deleted incidents will have a red heading.*

- **Only show shared incidents** - select whether or not to include incidents which have been shared with users on VideoManager EX.

- **Only show incidents with external links** - select whether or not to include incidents which have been shared externally, using incident links.

If this filter is checked, users will also be given to option to check **Active external links only**. This will only include incidents whose incident links are active - that is, workers outside VideoManager EX can still access the incident using its link.

3. Click **Find incidents** to display all incidents which match the previously-set criteria.

If the user wants to search for incidents using different parameters:

1. Click the **Filter** heading. This will re-open the search parameters.

2. Click ✖ **Clear filter** to clear the search filters.

Users can now enter the updated criteria.

3. Click **Find incidents** to search for the relevant incidents.

4.7 Bulk Edit Incidents

Bulk edits allow users to perform actions on multiple incidents at once. This is useful if there are too many incidents to manually edit/delete.

To bulk edit incidents:

1. Navigate to the *Incidents* tab.

2. Select the **🔍** *Search Incidents* pane.

3. Filter the incidents as necessary, and click *Find incidents*.

   > >> For more information, see Search Incidents on page 56

4. Click ☑ *Bulk edit*.

   The bulk edit user interface appears. The user can now select incidents to be bulk edited:

   - To select **indvidiual** incidents, click ■ next to their rows.

   - To select **all** incidents onscreen, click ■/☑ **Toggle selection of ALL rows.**.

   If there is an overflow of incidents, VideoManager EX will also give users the option to select the incidents which are not onscreen. To manually de-select individual incidents, click on their row.

Once the user has selected media files for bulk editing, the following options are available:

- 📋 *Create incident collection* - if the user has licensed *Nested Incidents*, this will enable them to create an incident collection containing the selected incidents.

- 🗑 *Delete* - users can delete many incidents simultaneously.

To exit bulk edit mode, click ✖ *Cancel*.

4.8 Create, Edit and Delete Bookmarks

Bookmarks can be used to mark a specific time in a media file. This is useful when a user needs to highlight a specific event or an item of interest - it also enables administrators to skip straight to the necessary parts of a media file for review purposes. Although VB400s can be configured to create a bookmark while in the field, users can also manually create bookmarks after the media file has been uploaded to VideoManager EX and added to an incident.

To add a bookmark to a media file:

1. Ensure that the media file in question is part of an incident.

   >> For more information, see Create Incidents Manually and Perform Incident Actions on page 31

2. Navigate to the **Incidents** tab.

3. Find the relevant incident, and click ✏ **Edit incident** next to it.

   Users can find the relevant incident by navigating to the **My Incidents**, **Shared Incidents**, or **Supervised Incidents** panes. They can also search for the relevant incident from the 🔍 **Search Incidents** pane.

4. If there are multiple clips in the incident, scroll down to the **Incident clips** section and select the relevant clip to which the bookmark will be added.

5. In the media file pane, click ▶ **Play**.

6. Drag the progress bar of the media file to the position where the bookmark will be placed. The media file will be paused automatically.

7. Click 🔖 **Bookmarks**.

> ☼   *If users cannot see the* 🔖 ***Bookmarks*** *option, they are only viewing the incident, not editing it. To change into editing mode, click* ✏ ***Edit incident***.

8. Click ***Add bookmark here***.

    The ***Add a bookmark*** window opens.

    The default name for the bookmark is the date and time position on the media file. Users can overwrite this with their own text.

9. Click ***confirm***. The bookmark will be added to the media file.

10. Repeat this process to add more bookmarks.

11. Click ***Save incident***.

Users can edit a bookmark. This is useful if the bookmark's name should be changed. To edit a bookmark:

1. Navigate to the ***Incidents*** tab.

2. Find the relevant incident, and click ✏ ***Edit incident*** next to it.

    Users can find the relevant incident by navigating to the ***My Incidents***, ***Shared Incidents***, or ***Supervised Incidents*** panes. They can also search for the relevant incident from the 🔍 ***Search Incidents*** pane.

3. Click ▶ ***Play***.

    The playback controls are displayed.

4. Click 🔖 ***Bookmarks***.

5. Next to the bookmark to be edited, select ✏ ***Edit***.

    The ***Edit this bookmark*** window will open.

6. Make the necessary changes.

7. Click ***confirm*** to save the updated bookmark.

Users can delete a bookmark. This may be necessary if the bookmark has become redundant. To delete a bookmark:

1. Navigate to the ***Incidents*** tab.

2. Find the relevant incident, and click ✏ ***Edit incident*** next to it.

    Users can find the relevant incident by navigating to the ***My Incidents***, ***Shared Incidents***, or ***Supervised Incidents*** panes. They can also search for the relevant incident from the 🔍 ***Search Incidents*** pane.

3. Click ▶ ***Play***.

    The playback controls are displayed.

4. Click █ *Bookmarks*.

5. Next to the bookmark to be deleted, select ✖ *Delete*.

The bookmark will be deleted.

To immediately jump to a bookmark in a media file, click █ *Bookmarks* under the relevant media file, and select the bookmark in question. This will skip the media file forward or backward to the bookmark's position.

5 Devices

The *Devices* tab enables the user to administer their body-worn cameras and DockControllers. From here, it is possible to view and configure all body-worn cameras and DockControllers on the network.

If users have sufficient permissions, they can perform the following actions:

- Connect body-worn cameras and DockControllers to VideoManager EX.

For more information about setting up the M500 in-car video system with VideoManager EX, please navigate to the Motorola Solutions Learning Experience Portal (registration is free) and search for *VideoManager EX and the M500 In-Car Video System Explained*.

>> For more information, see Connect Body-Worn Cameras to VideoManager EX on page 63

- Assign a body-worn camera. This will enable users to record media.

>> For more information, see Assign Body-Worn Cameras and Record Media on page 71

- Search for body-worn cameras, and filter them by a number of criteria.

>> For more information, see Search Body-Worn Cameras on page 77

- Edit the properties of a body-worn camera, including its name, custom status, and touch assign settings.

>> For more information, see Edit Body-Worn Camera Properties on page 81

- Perform body-worn camera actions. These actions include upgrading firmware, and factory resetting a body-worn camera.

>> For more information, see Perform Body-Worn Camera Actions on page 83

- Bulk edit body-worn cameras.

>> For more information, see Bulk Edit Body-Worn Cameras on page 86

5.1 Connect Body-Worn Cameras to VideoManager EX

The steps for connecting body-worn cameras to VideoManager EX differ, depending on what equipment has been purchased.

To configure both docks and a DockController:

1. Configure the DockController.

   >> For more information, see Connect a DockController to VideoManager EX on page 64

2. Connect the dock(s) to the DockController. Through this, the body-worn cameras will be connected to VideoManager EX automatically.

   >> For more information, see Connect Docks and Body-Worn Cameras to DockControllers on page 66

Alternatively, to configure a standalone solo dock, connect it directly to the PC running VideoManager EX.

>> For more information, see Connect a Solo Dock to VideoManager EX on page 68

5.1.1 Connect a DockController to VideoManager EX

The DockController must be configured before any body-worn cameras can be connected to VideoManager EX.

To configure a DockController:

1. Plug one end of the DockController's power cable into its power socket, and the other end into mains power.

2. Plug the Ethernet cable into the DockController's Ethernet port.

3. Plug the other end of the Ethernet cable into any available port on the Network Switch.

4. Turn the power on at the mains.
    For more information about DockControllers, please see the DockController Quickstart Guide. This can be downloaded here.

5. On VideoManager EX, navigate to the **Devices** tab.

6. Select the **DockControllers** pane.

7. Click 🔧 **Advanced** in the top right-hand corner.

8. Click ⛴ **Generate DockController Config**.

9. In the **Serial** field, enter the DockController's unique serial number.

This can be found on the bottom of the DockController.

10. In the **Device name** field, enter the name by which this DockController will be known on VideoManager EX.

11. The **Host** field should be pre-populated with VideoManager EX's webserver.

12. If **SSL** is set to **On**, all media passed through this DockController will have an extra layer of encryption.

13. If **Use static IP** is set to **On**, enter an IP address for the DockController.

14. From the **Security** dropdown, select whether the DockController will be protected with **802.1x (WPA2-PEAP-MSCHAPV2)** or not.

15. Click **Generate**.

The file will be saved to the PC's default downloads location.

16. Plug the USB drive into the same PC.

The USB drive must have **FAT32 format**.

17. Drag and drop the DockController configuration file into the root folder of the USB drive.

18. Safely eject the USB drive.

19. Plug the USB drive into one of the two DockController USB ports next to the function button.

> ⚠️ Caution
> *Do **not** plug the USB drive into one of the six DockController USB ports on the front of the device.*

5.1.2 Connect Docks and Body-Worn Cameras to DockControllers

Once the DockController has been configured, dock(s) can be connected. This will enable body-worn cameras to communicate with VideoManager EX.

To connect a 14-slot dock to a DockController:

1. Plug one end of the 14-slot dock's USB cable into its USB port, and the other end into one of the six USB ports on the front side of the DockController.

   The dock's USB indication LED will go green. This indicates that the dock is connected to the DockController.

2. Plug one end of the dock's power cable into its power port, and the other end into mains power.

3. Turn the power on at the mains.

   The dock's power LED will go green. This indicates that the dock is receiving power.

   Repeat these steps for up to six 14-slot docks.

To connect a solo dock to a DockController:

1. Plug one end of the solo dock's USB cable into its USB port, and the other end into one of the six USB ports on the front side of the DockController.

   Repeat these steps for up to four solo docks.

Dock the body-worn cameras into the 14-slot dock(s) or solo dock(s). This will connect the body-worn cameras to VideoManager EX.

To check that the body-worn cameras have been successfully connected to VideoManager EX:

1. On VideoManager EX, navigate to the *Devices* tab.

2. Select the *DockControllers* pane.

3. The DockController should appear in the pane, and its status should read as *Open & Connected*.

4. Click ❯ *View details*.

5. In the *Connected Devices* section, users can see how many body-worn cameras are connected to the DockController in question. The user can also view:

- ***Device*** - the body-worn camera's serial number.

- ***Status*** - the body-worn camera's status (e.g. charging, assigned, etc.).

5.1.3 Connect a Solo Dock to VideoManager EX

If the administrator has not purchased a DockController, it is possible to connect a solo dock directly to the PC running VideoManager EX. To do so:

1. Plug the dock's USB into the PC running VideoManager EX.

2. Insert the body-worn camera into the dock.

3. On VideoManager EX, navigate to the ***Devices*** tab.

4. Click ***Find devices***.

5. The body-worn camera should be visible, and its status should read as ***Unassigned***.

> 💡 *If the body-worn camera is not visible, navigate to the **Admin** tab, select the **Devices** pane, and click the **Device Settings** section. Ensure that **Enable device discovery** has been set to **On**.*

5.1.4 Connect VT-Series Cameras to VideoManager EX Remotely

It is possible to configure a VT-series camera using a QR code. This is important if a user cannot configure their VT-series camera using the VideoManager EX UI. There are two reasons for this: if an administrator does not have physical access to VideoManager EX (e.g. because it is a cloud service), or if the operator does not have access to VideoManager EX but needs to configure their body-worn camera. By creating a QR code, the administrator can either configure the VT-series camera to connect to VideoManager EX via their local WiFi, or share the QR code with the operator who can do it themselves. The VT-series camera can then be assigned like normal.

If the administrator has the VT-series camera and also has access to VideoManager EX themselves:

1. Navigate to the **Devices** tab.

2. Click 🔧 **Advanced** in the top right-hand corner.

3. Choose ⊞ **Generate device config code** from the dropdown.
The **Generate Device Config Code** pane will open.

4. In the **Serial number** field, enter the VT-series camera's serial number.

5. From the **Network name (SSID)** dropdown, the administrator must select the WiFi pro-file which will be used by the VT-series camera to connect to VideoManager EX. The options are as follows:

    • **Enter Network name (SSID) manually** - configure the WiFi network, using the **Network name (SSID)** and **Password** fields, and the **Security type** dropdown.
    This does **not** need to be the same network that VideoManager EX is operating on.

    • Select a previously-created WiFi profile.

6. Click **Generate code**.

7. The VT-series camera can now be connected to VideoManager EX by following the instructions onscreen.
Once the VT-series camera has been connected to VideoManager EX, it can be assigned to operators like normal.

> >> For more information, see Assign Body-Worn Cameras and Record Media on page 71

If the operator has the VT-series camera but does not have access to VideoManager EX:

1. The administrator must navigate to the *Devices* tab.

2. Click 🔧 *Advanced* in the top right-hand corner.

3. Choose ⊞ *Generate device config code* from the dropdown.
The *Generate Device Config Code* pane will open.

4. In the ❶ *Info* pane, click ↗ *Launch the public version of this page*.

5. Copy the URL, and share it with the operator. The operator can access this URL and configure the following settings:

   • In the *Serial number* field, enter the VT-series camera's serial number.

   • From the *Network name (SSID)* dropdown, select the WiFi profile which will be used by the VT-series camera to connect to VideoManager EX. The options are as follows:

      • **Enter Network name (SSID) manually** - configure the WiFi network, using the *Network name (SSID)* and *Password* fields, and the *Security type* dropdown.
   This does **not** need to be the same network that VideoManager EX is operating on.

      • Select a previously-created WiFi profile.

   • Click *Generate code*.

   • The VT-series camera can now be connected to VideoManager EX by following the instructions onscreen.

Once the VT-series camera has been connected to VideoManager EX, it can be assigned to operators like normal.

> >> For more information, see Assign Body-Worn Cameras and Record Media on page 71

5.2 Assign Body-Worn Cameras and Record Media

Before a body-worn camera can be used to record or stream media, it must be assigned to an already-created user. This ensures that all media can be traced back to the user who recorded it. If a body-worn camera is undocked without being first assigned to a user, it **will not** record any media.

The types of body-worn camera assignment are as follows:

- **Single issue** - the body-worn camera will be assigned to the user for one trip into the field, through the VideoManager EX UI. When the body-worn camera is redocked, it will become unassigned and must be reassigned manually.

>> For more information, see Assign Body-Worn Cameras with Single Issue on VideoManager EX on page 72

- **Single issue** and RFID - the user taps their RFID card against an RFID reader. This assigns a body-worn camera to them for one trip into the field. When the body-worn camera is redocked, it will become unassigned and must be reassigned again.

This assignment mode is only possible with a DockController and RFID reader.

>> For more information, see Assign Body-Worn Cameras with Single Issue and RFID on page 73

- **Permanent issue** - the body-worn camera will be assigned to the user through the VideoManager EX UI. When the body-worn camera is redocked, it will stay assigned to the same user, and cannot be assigned to other users.

>> For more information, see Assign Body-Worn Cameras with Permanent Issue on page 74

- **Permanent allocation** - the body-worn camera will be allocated to the user through the VideoManager EX UI. The user must then tap their RFID card against an RFID reader before they can use the body-worn camera in the field. When the body-worn camera is redocked, it will stay allocated to the same user, who must use their RFID time every time they wish to use it.

This assignment mode is only possible with a DockController and RFID reader.

>> For more information, see Assign Body-Worn Cameras with Permanent Allocation on page 75

5.2.1 Assign Body-Worn Cameras with Single Issue on VideoManager EX

If a body-worn camera is assigned with **Single issue** on VideoManager EX, the body-worn camera will be assigned to the user for one trip into the field. Once the user redocks the body-worn camera, it will become unassigned.

To assign a body-worn camera with single issue:

1. Navigate to the *Devices* tab.

2. Select the 🔍 *Search Devices* pane.

3. Filter the body-worn cameras as necessary, and click *Find devices*.

4. Find a suitable body-worn camera, and click 👤⁺ *Assign Device* next to it.

> 💡 *This body-worn camera must be connected to VideoManager EX and unassigned. To unassign a body-worn camera, click* **Return Device***.*

The *Assign Device* dialogue opens. Users must do the following:

5. In the *Operator name* field, enter the name of the user who will be recording with this body-worn camera. This must be a valid username on VideoManager EX.

If the user's name does not appear in the dropdown menu, they do not have the ability to operate body-worn cameras. This is due to their roles. Their roles must be changed before they can use a body-worn camera.

6. From the *Assignment mode* dropdown, select **Single issue**.

7. Select a suitable device profile from the *Device profile* dropdown. This determines how the body-worn camera will behave - which buttons perform which actions, etc.

8. Select a previously-created WiFi profile, if necessary. This determines which WiFi profile the body-worn camera will use, and is only relevant if the body-worn camera will be streaming in the field, uploading media over WiFi, or connecting to VB Companion.

9. Click *Assign Device*.

Wait until the *Status* column changes to *Ready*. At this point, the body-worn camera can be undocked and media files can be recorded like normal.

When the body-worn camera is returned, the media files are automatically downloaded - this will change the body-worn camera's status to *Busy*, then *Downloading*. Once the media files have finished downloading, the body-worn camera's status changes back to *Unassigned*.

5.2.2 Assign Body-Worn Cameras with Single Issue and RFID

Single issue with RFID forces users to tap their RFID cards before they can undock and operate their body-worn cameras. The user does not need access to the VideoManager EX UI in order to use this feature - however, there is some configuration required beforehand.

Users must ensure that they have an RFID reader connected to the DockController associated with their instance of VideoManager EX, and one RFID card for every user which will be operating their body-worn cameras with **Single issue** with RFID.

A user must be associated with one or more RFID cards on VideoManager EX. It is only necessary to do this once. To do so:

1. Tap the relevant RFID card against the reader, and wait until it emits three low beeps.

2. Navigate to the *Admin* tab.

3. Select the 👥 *People* pane.

4. Click the 👤 *Users* section.

5. Next to the user which will be associated with the RFID card in question, click ❯ *Go to user*.

6. In the *Touch Assign ID* field, click ❓ .
   The user will be taken to VideoManager EX's audit log, where the recent RFID scan will be visible.

7. Copy the touch assign ID from the audit log, and paste it into the *Touch Assign ID* field.

8. Click *Save user*.
   From now on, the RFID card will be associated with the relevant user.

> 💡 *If a user should be associated with multiple RFID cards (e.g. if they have a door card and a warrant card), repeat the previous steps for as many cards as necessary (i.e. touching the RFID card to the reader, copying it from the audit log) and separate the touch assign IDs with a comma in the **Touch Assign ID** field (e.g. 543642,873924).*

To assign a body-worn camera with **Single issue** and RFID, the user should tap their RFID card against the RFID reader. The device profile will be chosen depending on what roles the user inhabits, and the WiFi profile will be the default one (if the default WiFi profile has user-specific WiFi networks enabled, the body-worn camera will connect to the user's user-specific WiFi networks).

If a body-worn camera in the pool has been assigned successfully, it will emit a noise and its LEDs will flash - this is the body-worn camera which has been assigned to the user. The user can undock the body-worn camera and record media like normal.

When the body-worn camera is returned, the media files are automatically downloaded - this will change the body-worn camera's status to *Busy*, then *Downloading*. Once the media files have finished downloading, the body-worn camera's status changes back to *Unassigned*.

5.2.3 Assign Body-Worn Cameras with Permanent Issue

If a body-worn camera is assigned with **Permanent issue** on VideoManager EX, the body-worn camera will be assigned to the user indefinitely. Once the user redocks the body-worn camera, it will remain assigned to them. To assign a body-worn camera with permanent issue:

1. Navigate to the *Devices* tab.

2. Select the **Q** *Search Devices* pane.

3. Filter the body-worn cameras as necessary, and click *Find devices*.

4. Find the relevant body-worn camera, and click ⬤⁺ *Assign Device* next to it.

> 💡 *This body-worn camera must be connected to VideoManager EX and unassigned. To unassign a body-worn camera, click **Return Device**.*

The *Assign Device* dialogue opens. Users must do the following:

5. In the *Operator name* field, enter the name of the user who will be recording with this body-worn camera. This must be a valid username on VideoManager EX.

If the user's name does not appear in the dropdown menu, they do not have the ability to operate body-worn cameras. This is due to the roles they inhabit. Their roles must be changed before they can use a body-worn camera.

6. From the *Assignment mode* dropdown, select **Permanent issue**.

7. Select the relevant device profile from the *Device profile* dropdown. This determines how the body-worn camera will behave - which buttons perform which actions, etc.

8. Select a previously-created WiFi profile, if necessary. This determines which WiFi profile the body-worn camera will use, and is only relevant if the body-worn camera will be streaming in the field, uploading media over WiFi, or connecting to VB Companion.

9. Click *Assign Device*.

Wait until the *Status* column changes to *Ready*. At this point, the body-worn camera can be undocked and media files can be recorded like normal.

When the body-worn camera is returned, the media files are automatically downloaded - this will change the body-worn camera's status to *Busy*, then *Downloading*. Once the media files have finished downloading, the body-worn camera's status changes back to *Ready*, and it can be operated again by the same user.

5.2.4 Assign Body-Worn Cameras with Permanent Allocation

Similar to **Permanent issue**, **Permanent allocation** associates a body-worn camera to a user indefinitely. Once the user redocks the body-worn camera, it will remain assigned to them. However, unlike **Permanent issue**, **Permanent allocation** forces users to tap their RFID cards before they can undock and operate their body-worn cameras. There is some configuration required in order to use this feature.

Users must ensure that they have an RFID reader connected to the DockController associated with their instance of VideoManager EX, and one RFID card for every user which will be operating their body-worn cameras with **Permanent allocation**.

A user must be associated with one or more RFID cards on VideoManager EX. It is only necessary to do this once. To do so:

1. Tap the relevant RFID card against the reader, and wait until it emits three low beeps.

2. Navigate to the *Admin* tab.

3. Select the 👥 *People* pane.

4. Click the 👤 *Users* section.

5. Next to the user which will be associated with the RFID card in question, click ❯ *Go to user*.

6. In the *Touch Assign ID* field, click ❓ .

   The user will be taken to VideoManager EX's audit log, where the recent RFID scan will be visible.

7. Copy the touch assign ID from the audit log, and paste it into the *Touch Assign ID* field.

8. Click *Save user*.

   From now on, the RFID card will be associated with the relevant user.

> 💡 *If a user should be associated with multiple RFID cards (e.g. if they have a door card and a warrant card), repeat the previous steps for as many cards as necessary (i.e. touching the RFID card to the reader, copying it from the audit log) and separate the touch assign IDs with a comma in the* ***Touch Assign ID*** *field (e.g. 543642,873924).*

To allocate a body-worn camera with **Permanent allocation**:

1. Navigate to the *Devices* tab.

2. Select the 🔍 *Search Devices* pane.

3. Filter the body-worn cameras as necessary, and click *Find devices*.

4. Find the relevant body-worn camera, and click 👤⁺ *Assign Device* next to it.

> 💡 *This body-worn camera must be connected to VideoManager EX and unassigned. To unassign a body-worn camera, click* ***Return Device****.*

The ***Assign Device*** dialogue opens. Users must do the following:

5. In the ***Operator name*** field, enter the name of the user who will be recording with this body-worn camera and has been associated with an RFID card. This must be a valid username on VideoManager EX.

   If the user's name does not appear in the dropdown menu, they do not have the ability to operate body-worn cameras. This is due to the roles they inhabit. Their roles must be changed before they can use a body-worn camera.

6. From the ***Assignment mode*** dropdown, select **Permanent allocation**.

7. Click ***Assign Device***. The device profile will be chosen depending on what roles the user inhabits, and the WiFi profile will be the default one (if the default WiFi profile has user-specific WiFi networks enabled, the body-worn camera will connect to the user's user-specific WiFi networks).

If the body-worn camera has been allocated successfully, the user can undock the body-worn camera and record media like normal.

When the body-worn camera is returned, the media files are automatically downloading - this will change the body-worn camera's status to ***Busy***, then ***Downloading***. Once the media files have finished downloading, the body-worn camera's status changes back to ***Allocated***.

5.3 Search Body-Worn Cameras

If they have the appropriate permissions, users can utilise VideoManager EX's search functions to locate body-worn cameras in the *Devices* tab. This is necessary if a user needs to discover the status of various body-worn cameras (e.g. whether they are recording, and who is using them), or if a user would like to assign a body-worn camera so media can be recorded.

Body-worn cameras can be searched by a number of criteria.

1. Navigate to the *Devices* tab.

2. Select the 🔍 *Search Devices* pane.

   Users can now filter body-worn cameras by the following criteria:

   - *Device* - this will return the body-worn camera whose serial number **or** body-worn camera ID matches the one specified.

   If users want to search for multiple body-worn cameras, they should separate the values with commas (e.g. *511033,599249*).

   - *Operator* - this will return any body-worn cameras assigned to the operator specified (regardless of whether they are recording, charging, etc.).

   - *Location* - this will return any body-worn cameras who are plugged into the EdgeController, DockController, or site specified.

   - From the *Status* dropdown, users can filter body-worn cameras based on their status. The options are as follows:

     - **All** - this will return all body-worn cameras on the system, regardless of the status they are in.

     - **Docked** - this will return all body-worn cameras which are physically docked to either a PC, a DockController, or an EdgeController associated with the instance of VideoManager EX. If a VT-series camera has a WiFi profile with the *Enable Docking* setting enabled, they will also appear on this list when connected to the WiFi network in question.

     - **Assigned** - this will return all body-worn cameras which have been assigned to a user on the system.

- **Assigned to me** - this will return all body-worn cameras which have been assigned to the user performing the search.

- **Available for assignment** - this will return all body-worn cameras which are ready to be assigned - this means it will return all body-worn cameras which are simultaneously docked, unassigned, and have finished downloading any media.

- **Stream available** - this will return all body-worn cameras which are connected to a WiFi network and streaming successfully to VideoManager EX.

- **Downloading** - this will return all body-worn cameras which are docked and currently downloading recorded media to VideoManager EX.

- **Ready** - this will return all body-worn cameras which are ready to be undocked (all body-worn cameras which are simultaneously docked, assigned to a user, and have finished downloading any media).

- **In use** - this will return all body-worn cameras which are assigned to a user and undocked. Body-worn cameras which are streaming as well as recording will be shown here as well.

- **Busy, Unavailable or Unknown** - this will return all body-worn cameras who are **Busy** (the body-worn camera is preparing to download media to VideoManager EX and therefore cannot be used), **Unavailable** (the instance of VideoManager EX does not have the correct access control key to unlock the body-worn camera), or **Unknown** (the body-worn camera was undocked without being assigned to a user).

- **Error** - this will return all body-worn cameras which are in an error state: this is usually because the body-worn camera cannot download its recorded media (either because VideoManager EX has no more storage space, or because the body-worn camera itself is faulty).

- **Unknown** - this will return all body-worn cameras whose status is **Unknown** (the body-worn camera was undocked without being assigned to a user).

- **Allocated** - this will return all body-worn cameras which are assigned to a specific user but have not been tapped out with an RFID card.

- **Service required** - this will return all body-worn cameras for whom *Service required* has been set to *On*.

- From the *Firmware* dropdown, users can filter body-worn cameras by the firmware they are running. The options are as follows:

  - **Default firmware** - this will return all body-worn cameras running the default firmware, as specified from the *Device Images* section.

  - **Non-default firmware** - this will return all body-worn cameras running firmware other than the default firmware.

- **Other...** - this will give the user the option to enter the name of a specific firmware image. This search is useful if the user wants to find specific body-worn cameras running out-of-date firmware. If the user does not enter anything, **all** body-worn cameras will be returned.

  - If *Touch assign* is set to *Yes*, all body-worn cameras with Touch Assign enabled will be returned. If set to *No*, body-worn cameras with Touch Assign disabled will be returned.

  - If *Auto-upgrade enabled* is set to *Yes*, all body-worn cameras with auto-upgrade enabled will be returned. If set to *No*, body-worn cameras with auto-upgrade disabled will be returned.

If users have forgotten body-worn cameras because they have been lost or are redundant, users will also have the option to include these body-worn cameras in their search by checking ☑ **See forgotten devices**.

  - Click *Find devices* to display all matching body-worn cameras below the search options.

  - Click ✖ *Reset filter* to clear the search filters.

> ˙ᵧ˙   *Some of these search options may not be available depending on how access permissions have been configured.*

Once media files have been filtered, there are some actions that users can take:

- ☷ Change viewing options.

> >> For more information, see Change Viewing Options on page 14

- ❚❚ *Pause*.

This will freeze the list, and no body-worn cameras can be added or removed until it is unpaused.

- ☑ Bulk edit body-worn cameras.

> >> For more information, see Bulk Edit Body-Worn Cameras on page 86

Users may see icons next to their body-worn cameras. Potential combinations are as follows:

- No icon - the body-worn camera is not connected to VideoManager EX.

This could be because it is assigned and in the field (**In use**) or unassigned and in the field (**Unknown**).

- 🔌 - the body-worn camera is charging but has not met the minimum charge criteria for single-issue and RFID.

- 🔌 ✔ - the body-worn camera is charging and has met the minimum charge criteria for single-issue and RFID, but RFID assignment has been disabled for this body-worn camera from the ✎ *Edit device properties* pane.

- ⚡ 🏷 - the body-worn camera is charging, has met the minimum charge criteria for single-issue and RFID, and RFID assignment is enabled for this body-worn camera. It is ready to be assigned with single-issue and RFID.

- 🔋 ✔ - the body-worn camera is fully charged, but RFID assignment has been disabled for this body-worn camera from the ✏ *Edit device properties* pane.

- 🔋 🏷 - the body-worn camera is fully charged and RFID assignment is enabled for this body-worn camera. It is ready to be assigned with single-issue and RFID.

- ▨ - the body-worn camera is not charging.

5.4 Edit Body-Worn Camera Properties

Once a body-worn camera has been connected to VideoManager EX for the first time, users can edit its properties. This can be done while the body-worn camera is docked **or** while it is out in the field.
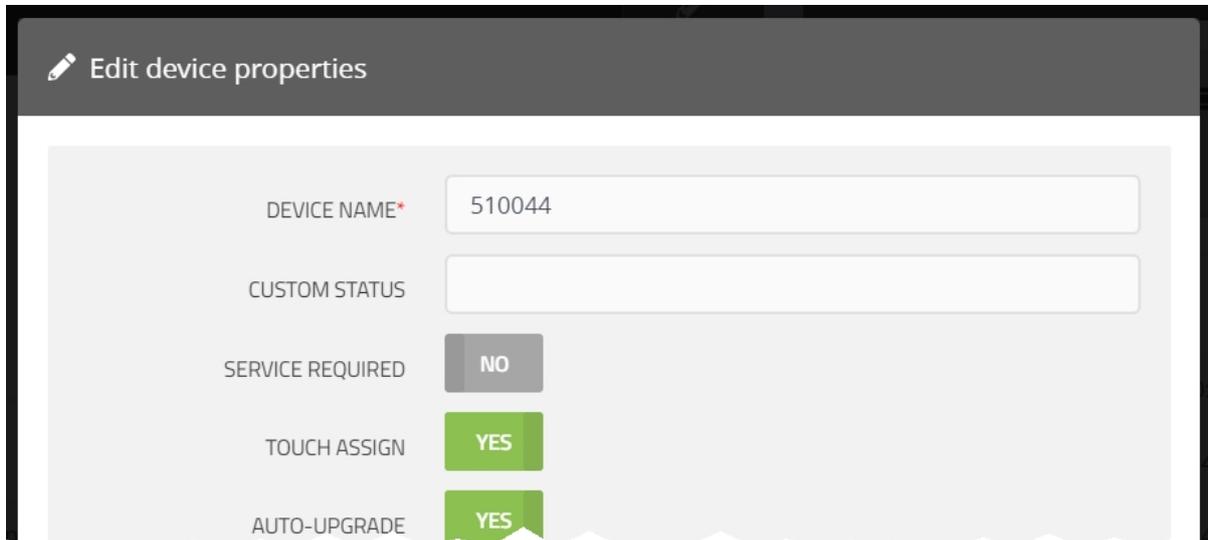
To edit body-worn camera properties:

1. Navigate to the **Devices** tab.

2. Select the 🔍 **Search Devices** pane.

3. Filter the body-worn cameras as necessary, and click **Find devices**.

4. Click **>** **View device info** next to the body-worn camera to be edited.

5. Click ✏ **Edit device properties**.

6. Configure the following settings:

   - In the **Device name** field, users can change the name of the body-worn camera on VideoManager EX. By default, this is the body-worn camera's serial number.

   If this is changed while the body-worn camera is disconnected from VideoManager EX, its name will be overwritten once the body-worn camera is redocked.

   - In the **Custom status** field, users can record notes about the body-worn camera in question - for example, if it has recently been upgraded.

   Users with the **See devices** permission can see custom statuses for assigned body-worn cameras, and users with the **See devices** and **See unassigned devices** permissions can see custom statuses for all body-worn cameras on VideoManager EX.

   - If **Service required** is set to **Yes**, a docked body-worn camera cannot be allocated or assigned to an operator until **Service required** has been set to **No** again.

   An undocked body-worn camera will be unallocated or unassigned as soon as it is redocked.

⚠️
Caution
If the body-worn camera is a VB400, its LEDs will glow yellow as well. This will either happen immediately (if it was already docked) or as soon as it is redocked (if it was out in the field).

- If **Touch assign** is set to **Yes**, the body-worn camera can be assigned or allocated with RFID.

> >> For more information, see Assign Body-Worn Cameras and Record Media on page 71

- If **Auto-upgrade** is set to **Yes**, the body-worn camera's firmware will be automatically upgraded. The firmware to which it is upgraded depends on how the **Firmware Settings** section has been configured.

- If **Use static IP** is set to **Yes**, the user must enter the IP address which the body-worn camera will use.

If set to **Off**, the body-worn camera will have a different IP address every time it starts recording.

7. Click **save changes**.

5.5 Perform Body-Worn Camera Actions

Once a body-worn camera has been connected to VideoManager EX, users can perform actions on it. These actions include upgrading its firmware, factory resetting it, viewing and downloading its audit log, and forgetting it.
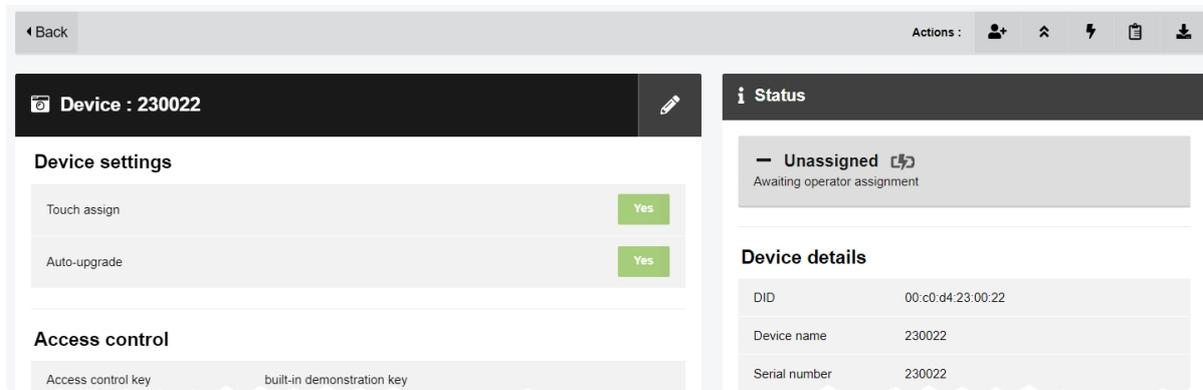
To reach the relevant pane:

1. Navigate to the *Devices* tab.

2. Select the 🔍 *Search Devices* pane.

3. Filter the body-worn cameras as necessary, and click *Find devices*.

4. Find the relevant body-worn camera, and click ❯ *View device info* next to it.

   This will open the body-worn camera's information pane.

To upgrade a body-worn camera's firmware to the latest version:

1. Ensure that the body-worn camera is docked (either with a dock or plugged directly into the PC running VideoManager EX) and charging.

2. Click ⌃ *Upgrade this Device*.

   The *Upgrade this Device* window will open.

   The most recent firmware will appear at the top of the list.

3. To upgrade the device, click *Upgrade Device*.

   ⚠ Caution   *Downgrading firmware (e.g. from V10.0.0 to V9.1.0) is generally not recommended - Motorola Solutions support should be contacted first.*

It may be necessary to factory reset a body-worn camera if it is *Locked* - this will happen if the body-worn camera has recorded media but is redocked to an instance of VideoManager EX which does not have its access control key. While a body-worn camera is locked, it cannot be assigned to a user. To factory reset a body-worn camera:

1. Ensure that the body-worn camera is docked and charging.

2. Click ⚡ *Factory Reset this Device* in the top right-hand corner.

3. To factory reset the body-worn camera, click *Yes, Reset Device*

⚠ Caution   *Factory resetting a body-worn camera means that all media on it which has not already been downloaded to VideoManager EX will be deleted.*

Users can prompt a VB400 to start recording remotely, if the camera is connected to VideoManager EX (either via its WiFi profile, or through VB Companion). To do so, click ● *Start recording*. To stop recording, click ⬛ *Stop recording*.

Users can watch a body-worn camera's live stream, if the camera is streaming to VideoManager EX over its WiFi profile. To do so, click ▶ *View live stream*.

Users can view a body-worn camera's audit log. This will give users insight into how the body-worn camera has been used - who its operator is, when it was last undocked, etc. To do so:

1. Click 📋 *View device audit log* in the top right-hand corner.

2. Filter the audit log using the following fields:

    -   *Event type* - this will return specific actions performed on the body-worn camera.

    If the user starts entering an event, VideoManager EX will suggest various event options (e.g. **DEVICE_DOCKED**).

    -   *User* - this will return actions performed on the body-worn camera by the specified user.

    If the user starts entering a username, VideoManager EX will suggest various usernames to match it.

    -   *Message* - this will return specific actions performed on the body-worn camera, whose details match the keywords entered here.

    For example, the **DEVICE_DOCKED** event comes with the message *Device docked*.

    -   *Signature* - the user should enter the signature of an incident. This will return actions performed on media files recorded by this body-worn camera in the specified incident.

    For example, when a media file recorded by this body-worn camera was added to the specified incident.

    -   *Location* - this will return actions performed on the body-worn camera from a specific DockController or EdgeController.

    -   *Client* - this will return actions performed on the body-worn camera from a specific IP address.

    -   *Server* - this will return actions performed on the body-worn camera from a specific server hosting VideoManager EX.

- From the **Date range** dropdown, users can select the date range for these actions.

3. Click **Filter audit log**.

To download an audit log, click ![download icon] **Download device audit log** in the top right-hand corner.

💡   *The audit log will be downloaded to the PC's default downloads location.*

If a body-worn camera has been undocked from VideoManager EX, it can be forgotten. This will remove it from VideoManager EX's list until it has been redocked. This is useful if a body-worn camera has been lost or taken out of rotation, and the user wants to hide it from any search results for organisational purposes.

1. Click ![camera icon] **Forget Device** in the top right-hand corner.

2. Click **yes** to confirm.

If a body-worn camera has been forgotten, it will not appear on VideoManager EX until it is re-docked.

5.6 Bulk Edit Body-Worn Cameras

Bulk edits can be used to quickly edit all body-worn cameras on an instance of VideoManager EX. This is useful if, for instance, there is a firmware upgrade that applies to many body-worn cameras owned by a user.

To bulk edit body-worn cameras:

1. Navigate to the *Devices* tab.

2. Select the Q *Search Devices* pane.

3. Filter the body-worn cameras as necessary, and click *Find devices*.

   >> For more information, see Search Body-Worn Cameras on page 77

4. Click ✅ *Bulk edit*.

Users should now select the body-worn cameras which will be bulk edited. This can be done in two ways:

   - Select an individual body-worn camera by clicking ⬛ next to it.

   - Select all body-worn cameras by clicking ✅ **Toggle selection of ALL devices.**

Once body-worn cameras have been selected, the following actions are now available:

   - 👤⁺ **Assign** - this will assign all selected body-worn cameras.

   If this is selected, administrators must enter the name of the user to whom these body-worn cameras should be assigned.

   - 👤ˣ **Return** - this will unassign all selected body-worn cameras.

   - ⌃ **Upgrade** - if there is a firmware upgrade available, this will upgrade all selected body-worn cameras.

   - ⚡ **Factory reset** - this will reset all selected body-worn cameras.

   The body-worn camera's access control key and configuration will be reset.

   - 🖉 **Update** - this will update all selected body-worn cameras - users can change the following settings by clicking ✅ next to each one:

- *Change custom status*

- *Change service required*

- *Change touch assign*

- *Change auto-upgrade*

- ⬛ **Forget** - this will delete all selected body-worn cameras from the instance of VideoManager EX.

To exit bulk edit mode, click ✖ *Cancel*.

6 Account Profile

In the *Account Profile* pane, users can edit aspects of their VideoManager EX profile.

To go to the user's account profile:

1. Click the 👤 user icon in the top right-hand corner of the screen.

2. Select **Account Profile** from the dropdown.

From the account profile pane, users can:

- Edit their display name.

In *Display name* field, enter the new display name and click *Save Changes*.

- 🔓 Update their password.

In the *Update password* pane, enter the user's current password, then the new password. Click *Save new password* to save.

- 📶 Create, edit and delete user-specific WiFi networks.

This is necessary if a user wishes to stream media over a personal hotspot.

> >> For more information, see Create User-Specific WiFi Networks on page 93

- 🔓 View two factor authentication settings.

7 Configure Streaming

Body-worn cameras can be configured to send a live stream to VideoManager EX while recording. Administrators can then watch the live stream in real time. To do so:

1. Configure firewalls.

   This step is only necessary if VideoManager EX is configured to use anything other than its default port **or** if VideoManager EX is set up on a public network.

   > >> For more information, see Configure Firewalls on page 90

2. Configure VideoManager EX's public address.

   > >> For more information, see Configure VideoManager EX's Public Address on page 92

3. Create a user-specific WiFi network, if the user will be live streaming over a personal hot-spot.

   > >> For more information, see Create User-Specific WiFi Networks on page 93

4. Create a WiFi profile which can be used for streaming.

   > >> For more information, see Create a WiFi Profile on page 95

5. Assign the body-worn camera to a user, and begin streaming media.

   > >> For more information, see Assign a Body-Worn Camera for Streaming on page 97

6. View the live stream.

   > >> For more information, see View Live Streams on page 99

7.1 Configure Firewalls

Sometimes, body-worn cameras will be unable to stream to VideoManager EX without prior firewall configuration. There are two reasons that firewall configuration might be necessary: the user has either changed VideoManager EX's default port, or has connected it to a public network. The steps below differ, depending on which situation applies to the user's instance of VideoManager EX.

If the user has changed VideoManager EX's default web server port, they must create a new inbound rule. To do so:

1. In the Windows menu, navigate to the **Control Panel** tab.

2. Select the **System and Security** pane.

3. Click the **Windows Defender Firewall** section.

4. In the left-hand menu pane, click 🛡 **Advanced Settings**.

5. Select **Inbound Rules**.

6. In the right-hand menu pane, click **New Rule...**.

7. Set the rule type to **Port**, and click **Next**.

8. In the **Specific Local Ports** section, enter VideoManager EX's port, and click **Next**.
    This can be found on VideoManager EX, in the **Web Server** section of the **System** pane, in the **Admin** tab.

9. Ensure that **Allow the connection** is checked, and click **Next**.

10. Check the relevant profiles for this rule. If in doubt, leave all checked, and click **Next**.

11. Enter a name for the rule and click **Finish**.

> ⚠ *If the user has other firewalls or NAT routers in the network between VideoManager EX*
> Caution *and the WiFi network to which body-worn cameras will connect, they must also be*
> *configured to allow TCP connections between the body-worn camera and the*
> *VideoManager EX server.*

If the user has connected VideoManager EX to a public network:

1. In the Windows menu, navigate to the **Control Panel** tab.

2. Select the **System and Security** pane.

3. Click the **Windows Defender Firewall** section.

4. In the left-hand menu pane, click 🛡 **Advanced Settings**.

5. Select **Inbound Rules**, and scroll down until the *VideoManager EX Web* rule is visible.

6. Double-click on the rule and in the *Advanced* section, ensure that **Public** is checked.

7. Click *OK*.

7.2 Configure VideoManager EX's Public Address

When a body-worn camera connects to VideoManager EX, it does so using VideoManager EX's public address. If the body-worn cameras are connecting to the same IP network as VideoManager EX, users can utilise the same IP address as the VideoManager EX machine.
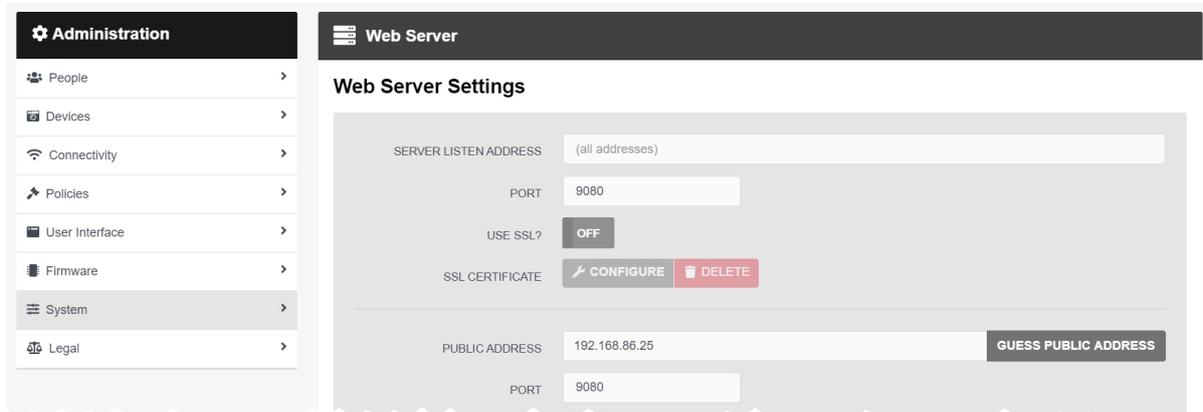

To configure a public address:

1. On VideoManager EX, navigate to the *Admin* tab.

2. Select the ⇌ *System* pane.

3. Click the ▤ *Web Server* section.

4. In the *Public address* field, either enter the public address or click *Guess public address* to guess what this address should be.

5. Click *Save settings*.

VideoManager EX should be configured to use fixed address LAN infrastucture, and operate on a **Private** or **Domain** network, wherever possible.

7.3 Create User-Specific WiFi Networks

It is possible for users to create user-specific WiFi networks which will only appear on their profile and cannot be viewed by other users on the system. These can be added to WiFi profiles later, but they will still be kept private. This is useful if the user has created a mobile phone hotspot for streaming.

The steps for creating a user-specific WiFi network differ, depending on whether the user is creating the network for **another user on VideoManager EX or for themselves**.

If the user is configuring a user-specific WiFi network for another user, the steps are as follows:

1. Navigate to the *Admin* tab.

2. Select the 👥 *People* pane.

3. Click the 👤 *Users* section.

4. Next to the user to be edited, click **>** *Go to user*.

5. In the 📶 *WiFi networks* pane, click ➕ *Add network*.

6. In the *Network name (SSID)* field, enter the name of the WiFi network or hotspot. This cannot be changed later.

7. From the *Security type* dropdown, select which security configuration the user-specific WiFi network will use. The options are **WPA2-PSK**, **WPA-PSK**, **WEP**, or **Open**.

8. In the *Passphrase* field, enter the passphrase of the WiFi network or hotspot.

9. From the *Band* dropdown, select which frequencies the body-worn cameras will attempt to connect to. The options are as follows:

    • **Any** - this option is suitable for all body-worn cameras.

    • **2.4GHz only** - this option is suitable for all body-worn cameras.

    • **5GHz only** - this option is only suitable for VB400s.

10. If *Use static IP* is set to *On*, the user must enter the corresponding static IP details.

11. If *Disconnect on low signal* is set to *On*, body-worn cameras trying to stream over this network will disconnect from it if its signal is weak.

 Users will have the option to define the "weak" signal as a percentage, and the time in seconds that the body-worn camera must be connected to the specified signal level, after which the body-worn camera will disconnect.

12. Click *Add* to save the network.

If the user is creating the user-specific WiFi network for themselves:

1. In the top right-hand corner of VideoManager EX, click the 👤 icon.

2. Select **Account Profile** from the dropdown.

3. In the 📶 *User-specific WiFi networks* pane, click ➕ *Add network*.

4. In the *Network name (SSID)* field, enter the name of the WiFi network or hotspot.
 This cannot be changed later.

5. From the *Security type* dropdown, select which security configuration the user-specific WiFi network will use. The options are **WPA2-PSK**, **WPA-PSK**, **WEP**, or **Open**.

6. In the *Passphrase* field, enter the passphrase of the WiFi network or hotspot.

7. From the *Band* dropdown, select which frequencies the body-worn cameras will attempt to connect to. The options are as follows:

    • **Any** - this option is suitable for all body-worn cameras.

    • **2.4GHz only** - this option is suitable for all body-worn cameras.

    • **5GHz only** - this option is only suitable for VB400s.

8. If *Use static IP* is set to *On*, the user must enter the corresponding static IP details.

9. If *Disconnect on low signal* is set to *On*, body-worn cameras trying to stream over this network will disconnect from it if its signal is weak.

 Users will have the option to define the "weak" signal as a percentage, and the time in seconds that the body-worn camera must be connected to the specified signal level, after which the body-worn camera will disconnect.

10. Click *Add* to save the network.

7.4 Create a WiFi Profile

Administrators must create a WiFi profile which is suitable for live streams. A WiFi profile is a collection of WiFi networks, one of which a body-worn camera must connect to before it can live stream.

To create a WiFi profile:

1. Navigate to the *Admin* tab.

2. Select the 📶 *Connectivity* pane.

3. Click the 📶 *WiFi Profiles* section.

4. Click 🗋 *Create wifi profile* in the top right-hand corner.

5. Enter the following information for the WiFi profile (this will apply to all body-worn cameras which use the profile in question):

   - In the *Name* field, enter a name for the WiFi profile.

   - Ensure that *Default profile* is set to *On*.

   💡 *This ensures that, regardless of how body-worn cameras are assigned, they will always have access to this WiFi profile.*

   - If the administrator has already created user-specific WiFi networks, they can be added to the WiFi profile by setting *User-specific networks* to *On*.

   - To add a new network to the WiFi profile, click 🗋 *Add network*.

   The administrator should enter the WiFi network's information. Unlike user-specific WiFi networks, this WiFi network will be used by all body-worn cameras in this WiFi profile, regardless of the users to which they have been assigned.

   - If VB100s, VB200s, VB300s, or VB400s will be streaming, scroll down to the *VB300/VB400* section set *Enable streaming* to *On*.

- If VT-series cameras will be streaming, scroll down to the ★ *VT50/VT100* section and set *Enable streaming* to *On*.

☀ *VT-series camera streaming settings must be configured for **every network** within a WiFi profile.*

---

6. Click *Save settings*.

7.5 Assign a Body-Worn Camera for Streaming

Users can now operate a body-worn camera and live stream the media back to VideoManager EX. The steps differ, depending on how the body-worn camera will be assigned.

To assign a VB400 to a user through **single issue and RFID**, the user should tap their RFID card against the RFID reader associated with VideoManager EX. In the pool, a VB400's LEDs will light up and it will emit a beep. The user can undock and operate this body-worn camera. For more information, please see the Administrator Guide.

To assign a VB400 to a user through **Single issue**, **Permanent issue**, or **Permanent allocation**:

1. Navigate to the *Devices* tab.

2. Select the 🔍 *Search Devices* pane.

3. Filter the body-worn cameras as necessary, and click *Find devices*.

   -🔆-   *This body-worn camera must be connected to VideoManager EX and unassigned. To unassign a body-worn camera, click **Return Device**.*

   The *Assign Device* dialogue opens.

4. In the *Operator name* field, enter the name of the user who will be recording with this body-worn camera. This must be a valid username on VideoManager EX.

5. Select which *Assignment mode* the body-worn camera will use.

   - **Single issue** - the body-worn camera will be assigned to a user and when it is redocked, it will become unassigned and must be reassigned manually.

   - **Permanent issue** - the body-worn camera will be assigned to the user and when it is redocked, it will stay assigned to the same user.

   - **Permanent allocation** - the body-worn camera will be allocated to a user, who must then tap an RFID card before they can use it in the field. When it is redocked, it will stay allocated to the same user.

If **Permanent allocation** has been chosen, the user will **not** be able to select the relevant device profile and WiFi profile. However, this is not an issue - the default VideoManager EX device profile is suitable for streaming, and the WiFi profile should have already been set as the default.

-🔆-   *If the WiFi profile has not already been set as the default, navigate to the **Admin** tab, select the 🛜 **Connectivity** pane, click the 🛜 **WiFi Profiles** section, click > **Go to profile** next to the newly created WiFi profile, and set **Default profile** to **On**.*

If **Single issue** or **Permanent issue** have been chosen, the user must do the following:

1. From the *Device profile* dropdown, select the default device profile.

2. From the *WiFi profile* dropdown, select the previously-created WiFi profile.

3. Click ***Assign Device***.

Wait until the body-worn camera's status changes to ***Ready***. At this point, the body-worn camera can be undocked and users can start streaming from their body-worn camera.

7.6 View Live Streams

Once a body-worn camera has been assigned to a user and has a WiFi profile that allows streaming, they can begin recording and view the live stream that is created at the same time. Live streams are only broadcasted while the body-worn camera in question is recording.
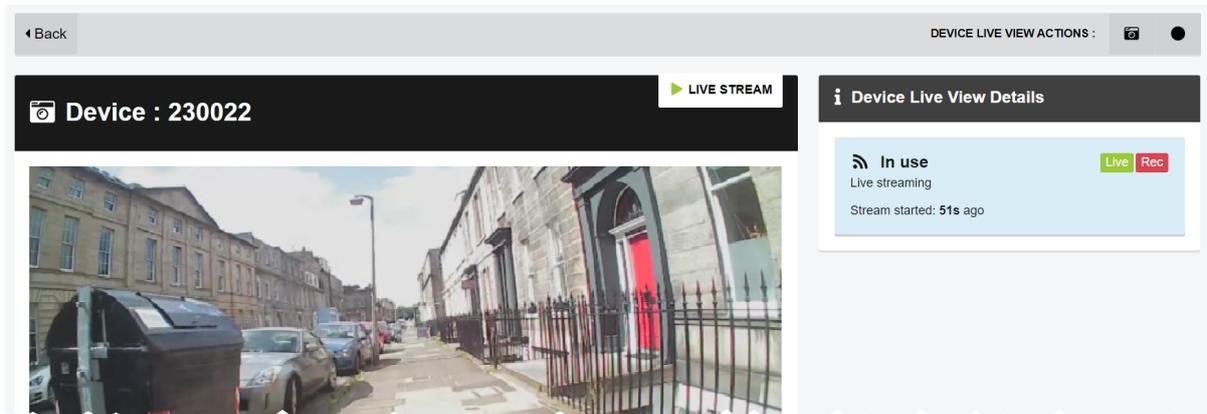
To view a body-worn camera's live stream:

1. Navigate to the *Devices* tab.

2. Next to the streaming body-worn camera, there will be two alerts - one will say *Rec* and one will say *Live*. Click *View live*.

3. This will take the user to a page where they can view the live stream.

    > ⚠️ *Only users with the permission to view body-worn cameras live can see live streams.*
    > Caution *However, even with this permission, they can only see live streams from body-worn cameras they have permission to view (this could be body-worn cameras they own, body-worn cameras they supervise, or all body-worn cameras).*

4. Once a live stream has stopped, the screen will go blue and there will be a message reading *Device not streaming*.

8 Frequently Asked Questions

8.1 Media file FAQs

Q. After recording, how do I download media files from my body-worn camera to VideoManager EX?

A. To download media files from your body-worn camera:

1. Either dock your body-worn camera or plug it in to your PC using a USB cable.

2. Navigate to the *Devices* tab.

3. Locate the body-worn camera you've just plugged in. Click **>** *View device info*.

4. In the *Status* window, you should see the *Downloading* sign.
   The media file should now be available to view under the *Media* tab.

Q. Why are some of the headings on my media files blue?

A. If a media file is part of an incident, its heading will become blue instead of grey. It will also have a star ★ next to its name. You can click the *This video is in {0} incident* button, which will take you to the incident it is part of.

Q. What is the difference between the operator and the owner of a media file?

A. The operator of a media file is the one who physically recorded it on their body-worn camera. The owner has full administrative control over the media file. Normally this will be the same person - however, if the media in question is too sensitive for more junior users to retain control of, it may be necessary to reallocate who the owner is.

Q. I can't see some of the media files on VideoManager EX. Why is this?

A. There are two possible reasons for this - permissions and deletion policies.

- *Permissions* - VideoManager EX gives administrators lots of control over what actions can be performed by other users on the site. It does this through roles - these affect how much privilege a user has on the site. It's possible that when you were creating your admin user after logging in for the first time, you didn't assign it the privileges which will allow you to see the media files filmed by yourself and others on the system. To fix this:

  1. Navigate to the *Admin* tab.

  2. Select the 👥 *People* pane.

  3. Click the 🗐 *Roles* section.

  4. Click *Go to role* button next to your role.

  5. Scroll down to the *Media permissions* window.

6.   Next to the relevant permissions, set each button to **On**.

Remember that these permissions apply to either your media files, media files which have been shared with you, media files which have been recorded by people you supervise, or all media files on the system.

- **Deletion Policies** - you may want to check the configuration of your deletion policy, in case it is configured to delete media almost immediately. To do so:

    1.   Navigate to the **Admin** tab.

    2.   Select the ⚒ **Policies** pane.

    3.   Click the ♻ **Deletion Policy** section.

    4.   Change the number of days that media is kept for after it has been recorded and downloaded.

Q. Why do some of my media files have a cloud symbol instead of a thumbnail?

A. A cloud symbol indicates that a media file is not available on your instance of VideoManager EX because:

- You are on a Central VideoManager and the media file is on the site. You must fetch the media file from the site before you can watch it.

- You are on a site and the media file was fetched from the Central VideoManager.
This means that you can no longer watch the media file on the site.

Q. I've accidentally deleted a media file. Can I undo this action?

A. You can reinstate a deleted media file, as long as your deletion policy has been configured to keep deleted media files for a short period of time after deletion **and** you are in a role which has had the **Undelete** permission set to **On**. To reinstate a media file:

1.   Naviate to the **Media** tab.

2.   Select the 🔍 **Search Media** pane.

3.   Check **Include deleted media**.

4.   The deleted media file will appear with a red heading. Click ↻ **Reinstate media**.

5.   Click **yes**.
The media file will be reinstated and can be watched like normal.

8.2 Device FAQs

Q. Why isn't my VB300 docking?

A. To restart your VB300:

1. Hold the body-worn camera so it is facing you.

2. Simultaneously **press and hold** the two plastic buttons on the top-left and bottom-right corners of the body-worn camera for 5 to 10 seconds.

3. All the lights on the body-worn camera should come on and start flashing.

4. Release the two buttons.

5. Once the lights have stopped flashing, try re-docking the body-worn camera again.

If the procedure above doesn't work, leave the body-worn camera off its charging base until the battery is completely flat (this could take over 24 hours). Once the battery is flat, try re-docking the body-worn camera.

If neither of these procedures work, the body-worn camera must be returned to Motorola Solutions for servicing or repair. To do so:

1. Navigate to motorolasolutions.com/en_xu/support.html, and select **Service Returns** from the dropdown.

2. Fill in the form by entering your company name, email address, telephone number and return address details.
Leave the reseller name **blank**.

3. Select the correct camera model from the dropdown list under "part".

4. Enter the serial number of your faulty body-worn camera.

5. Describe the fault in the *Fault Description* box.
Leave the rest of the fields **blank**.

6. If you are returning more than one body-worn camera, click *Add line for each additional return* and fill out the form as detailed above.

7. Click *Create*.

Q. Why isn't my VB100/VB200 docking?

A. To restart your VB100 or VB200:

1. Turn the body-worn camera upside down.

2. Pull the rubber charging cover upwards gently and rotate it to the side, so you can see the charging/docking port.

3. To the right of the charging/docking port, there is a small plastic switch. Press this switch down for 5 to 10 seconds.

4. Keep looking at the top of the body-worn camera. The green power light will go out. It will then glow orange and red, and the other lights on the top of the body-worn camera will glow green.

This indicates that the body-worn camera is rebooting.

5. Once the lights have stopped flashing, try re-docking the body-worn camera again.

If the procedure above doesn't work, leave the body-worn camera off its charging base until the battery is completely flat (this could take over 24 hours). Once the battery is flat, try re-docking the body-worn camera.

If neither of these procedures work, the body-worn camera must be returned to Motorola Solutions for servicing or repair. To do so:

1. Navigate to motorolasolutions.com/en_xu/support.html, and select **Service Returns** from the dropdown.

2. Fill in the form by entering your company name, email address, telephone number and return address details.

Leave the reseller name **blank**.

3. Select the correct camera model from the dropdown list under "part".

4. Enter the serial number of your faulty body-worn camera.

5. Describe the fault in the *Fault Description* box.

Leave the rest of the fields **blank**.

6. If you are returning more than one body-worn camera, click *Add line for each additional return* and fill out the form as detailed above.

7. Click *Create*.

Q. Why does my body-worn camera appear as "locked" on VideoManager EX?

A. Your body-worn camera will appear as locked if it has been undocked from one instance of VideoManager EX and redocked at a different VideoManager EX which does not have its access control key. This means that all media on the body-worn camera will be inaccessible.

The body-worn camera will be unlocked immediately if you export its access control key from the original VideoManager EX to the VideoManager EX which the body-worn camera is connected to now.

Q. My VB400 is broken. How do I prevent other operators on VideoManager EX from accidentally using it?

A. You can change your VB400's status to *Service Required*. This will remove it from the pool (i.e. it cannot be assigned or allocated), and its LEDs A, B, and C will glow yellow. To do so:

1. Navigate to the *Devices* tab.

2. Select the 🔍 *Search Devices* pane.

3. Filter the body-worn cameras as necessary, and click *Find devices*.

4. Click ❯ **View device info** next to the body-worn camera to be edited.

5. Click ✏ **Edit device properties**.

6. Set **Service required** to **Yes**.

7. Click **save changes**.

The VB400 will be unusable until you set **Service required** to **No**.

Q. Can I return broken body-worn cameras?

A. Yes. Motorola Solutions has a self-service portal that allows you to return your body-worn cameras.

To do so:

1. Navigate to motorolasolutions.com/en_xu/support.html, and select **Service Returns** from the dropdown.

2. Fill in the form by entering your company name, email address, telephone number and return address details.
   Leave the reseller name **blank**.

3. Select the correct camera model from the dropdown list under "part".

4. Enter the serial number of your faulty body-worn camera.

5. Describe the fault in the **Fault Description** box.

6. Leave the rest of the fields **blank**.

7. If you are returning more than one body-worn camera, click **Add line for each additional return** and fill out the form as detailed above.

8. Click **Create**.

Q. What do the icons next to my body-worn cameras mean?

A. You can configure VideoManager EX so it is only possible to assign a body-worn camera with **Single issue** and RFID if its battery has been charged to a certain level. VideoManager EX displays icons next to your body-worn cameras depending on their charging status, and whether they have met this configured level. Potential icon combinations are as follows:

- No icon - the body-worn camera is not connected to VideoManager EX.
  This could be because it is assigned and in the field (**In use**) or unassigned and in the field (**Unknown**).

- 🔋 - the body-worn camera is charging but has not met the minimum charge criteria for single-issue and RFID.

- ⚡✔ - the body-worn camera is charging and has met the minimum charge criteria for single-issue and RFID, but RFID assignment has been disabled for this body-worn camera from the ✏ *Edit device properties* pane.

- ⚡🏷 - the body-worn camera is charging, has met the minimum charge criteria for single-issue and RFID, and RFID assignment is enabled for this body-worn camera. It is ready to be assigned with single-issue and RFID.

- ▭✔ - the body-worn camera is fully charged, but RFID assignment has been disabled for this body-worn camera from the ✏ *Edit device properties* pane.

- ▭🏷 - the body-worn camera is fully charged and RFID assignment is enabled for this body-worn camera. It is ready to be assigned with single-issue and RFID.

- ▭̸ - the body-worn camera is not charging.

9 Glossary

A

Access Control Key

The security mechanism that prevents unauthorised body-worn cameras from connecting to VideoManager EX - in addition, if a body-worn camera is lost or stolen, its recorded footage cannot be recovered unless the person who has possession of the body-worn camera also has its access control key.

Assigned/Unassigned

If a body-worn camera has been assigned, it has been paired with a user and can record footage. An unassigned body-worn camera has not been paired with a user, and cannot record footage until it has been assigned.

Audit Log

The trail of information that records every action on the system. This includes when people logged on, logged off, whether they docked or undocked body-worn cameras, deleted media files, etc. This trail is not deletable.

B

Bandwidth Rule

A configurable rule that determines when footage is uploaded from sites to the Central VideoManager. This is useful if remote workers don't want to put strain on their home WiFi during high-traffic hours.

Bookmark

This draws attention to a specific part of a media file. It can be created by the body-worn camera which is recording the media file in the field, if the operator presses a configured button. Alternatively, users can add bookmarks to a media file in an incident, once the media file has been downloaded to VideoManager EX.

D

Dashboard

VideoManager EX's homepage, to which all users are automatically directed upon logging in. If an administrator has created a message for users, they will see it here.

Device

Motorola Solutions equipment which has been associated with VideoManager EX (e.g. body-worn cameras, DockControllers).

Display Name

The name of a user that will be presented to others on the VideoManager EX system - this is not necessarily the same as a username.

DockController
> A device which converts the media files from body-worn cameras into data that can be sent over a network or the internet - this allows up to 84 body-worn cameras to be used with just one DockController, and enables these body-worn cameras to be installed away from the physical VideoManager EX server.

E

EdgeController
> A small embedded computer with inbuilt storage, which provides remote or home-based workers with a docking location for their body-worn cameras. They are used exclusively as a site, connected to a Central VideoManager.

Export
> Incidents which have been exported from VideoManager EX to the user's PC. A version of the incident will remain on VideoManager EX.

I

Incident
> A collection of evidence - such as footage, notes, and users - which can be exported or shared with people outside of VideoManager EX. In some lines of work, this is known as an exhibit or event.

Incident Clip
> Any media file which has been added to an incident.

L

Licence
> Some features on VideoManager EX are not available unless a licence has been obtained from Motorola Solutions. Such features include assisted redaction, Tactical VideoManager, and ONStream.

M

Media
> Any media files or assets which can be added to an incident for evidential purposes.

Media File
> Any media which has been imported or downloaded to VideoManager EX. This could be a PDF, a still image, a video or an audio file.

Media file ID
> A unique ID that identifies a specific media file. It is used in the audit log to record which media file/asset an entry refers to, and can be used to locate media files/assets.

O

ONStream
> A licensed feature from Motorola Solutions which enables body-worn cameras to send a live stream to VideoManager EX over WiFi.

Operator
By default, this is the user who recorded the media file on a body-worn camera, or imported the asset into VideoManager EX (either manually, or as configured in an automatic import profile).

Owner of a Media file
This is the user who has administrative control over a media file. By default, this is the user who recorded the media file on a body-worn camera, or imported it into VideoManager EX (either manually, or as configured in an automatic import profile). However, this can be changed to a senior user with more permissions.

Owner of an Incident
This is the user who has administrative control over the incident. By default, this is the user who created the incident. However, this can be changed to a senior user with more permissions.

P

Permanent allocation
If a body-worn camera has been assigned to a user with permanent allocation, it will be assigned to the user permanently, even when it is redocked. It does not need to be reassigned every time the user wishes to use it. Unlike permanent issue, the user can only undock the body-worn camera with RFID touch assign.

Permanent issue
If a body-worn camera has been assigned to a user with permanent issue, it will be assigned to the user permanently, even when it is redocked. It does not need to be reassigned every time the user wishes to use it.

Permission
An individual rule which determines the actions users can perform on VideoManager EX.

Post-record
The media file immediately following an event which is captured automatically, once the operator stops recording. This could be between 1 and 120 seconds.

Pre-record
The media file preceding an event which is automatically captured as soon as an operator starts recording. This could be between 1 and 120 seconds.

R

Recording
This is the complete footage recorded by a body-worn camera, from the moment it is prompted to start recording until the moment it is prompted to stop (including any pre- and post-record periods). A recording will be split into multiple media files if it reaches a certain length, as defined in the body-worn camera's device profile.

Recording ID
A unique ID that identifies a specific recording. If a recording has been split up into multiple media files (due to the device profile of the body-worn camera that recorded it), these media files will all have the same recording ID.

Report
> Instead of applying permissions directly to users, they are applied to a role, which is then applied to a user. This means that multiple users can belong to the same role.

Role Assignment Tier
> Every role on VideoManager EX belongs to a role assignment tier. Users can only add other users to roles which are in a tier equal to or lower than the highest assignment tier of their own roles. This includes any roles that they get through their groups.

S

Safety Mode
> While a body-worn camera is in safety mode, all functionality (LEDs, beeps, haptic feedback, recording, Bluetooth connection, etc.) will be disabled. To restore functionality, the operator must either perform the gesture associated with leaving safety mode, or connect the body-worn camera to power.

Saved Search
> VideoManager EX allows incident searches to be saved and re-searched by other users on the system as many times as necessary.

Single issue
> If a body-worn camera has been assigned to a user with single issue, it will only be assigned to the user for one trip. Once the body-worn camera is redocked, it will return to the pool and can be assigned to a different user.

System Administrator
> A role which cannot be edited or deleted. Any users with this role will be able to access any aspect of VideoManager EX.

U

User
> Every individual on an instance of VideoManager EX must have their own user.

User-Specific WiFi Network
> A WiFi network that only appears on the dashboard of the user who configured it - for instance, a mobile phone hotspot for streaming that other users shouldn't be able to access.

V

VB Companion
> Motorola Solutions VB Companion enables users who are still in the field to use their phone to view, and categorise, footage they have recently recorded.

VB200
> A robust body-worn camera designed and sold by Motorola Solutions. It can record for up to 8 hours and has 16GB of recording storage.

VB300
> A robust body-worn camera designed and sold by Motorola Solutions. It can record for up to 8 hours in HD and has 32GB of recording storage. It also has the ability to livestream footage to VideoManager

EX over a WiFi network.

VB400

A robust body-worn camera designed and sold by Motorola Solutions. It can record for up to 8 hours in full HD and has 32GB of recording storage. It also has GPS-tracking, Bluetooth functionality, and can livestream footage to VideoManager EX over a WiFi network.

Video

A section of a recording, the length of which is determined by the body-worn camera's device profile.

VT100

A VT100 is a lightweight, discreet body-worn camera designed and sold by Motorola Solutions. It can record for up to 4 hours, and has the capacity to livestream footage to VideoManager EX if connected to WiFi. It is the first body-worn camera in Motorola Solutions' VT-series camera range to have haptic feedback.

VT50

A lightweight, discreet body-worn camera designed and sold by Motorola Solutions. It can record for up to 2 hours, and has the capacity to livestream footage to VideoManager EX if connected to WiFi.

W

WiFi Profile

A collection of individual WiFi networks that is then applied to a body-worn camera. The body-worn camera in question will stream to VideoManager EX over these networks.

For more information, please visit: www.motorolasolutions.com.

MOTOROLA *SOLUTIONS*