VideoManager 15.0
Admin Guide

This document is intended to serve as a reference guide for system administrators when utilising advanced VideoManager features.

Copyright

Availability is subject to individual country law and regulations. All specifications shown are typical unless otherwise stated and are subject to change without notice. MOTOROLA, MOTO, MOTOROLA SOLUTIONS and the Stylized M Logo are trademarks or registered trademarks of Motorola Trademark Holdings, LLC and are used under license. All other trademarks are the property of their respective owners.

© 2015 - 2021 Motorola Solutions, Inc. All rights reserved.

Intended purpose

This document is intended to serve as a reference guide for system administrators when utilising advanced VideoManager features.

Document ID

ED-012-221-11

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 when using the custom predicate language.

Contact address

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

Safety notices

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

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

Chapters are arranged by the corresponding tabs on VideoManager (***Videos***, ***Incidents***, ***Devices***, ***Status***, ***Tactical*** and ***Admin***). From there, the sub-chapters are arranged by actions you can perform in each tab. The exception for this is the ***Admin*** tab - this is broken down into the panes and sections of the ***Admin*** UI.

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 Initial Configuration

This document assumes that VideoManager installation media has been provided as part of the purchase.

The steps for downloading differ, depending on whether VideoManager is being downloaded for the first time, or being re-downloaded (i.e. to obtain a newer version of the software).

- Download VideoManager for the first time.

>> For more information, see Download VideoManager on page 11

- Re-download VideoManager.

>> For more information, see Re-Download VideoManager on page 13

2.1 Download VideoManager

If this is the first time that the administrator has installed VideoManager on their PC:

1. Ensure that Software Assurance has been obtained from Motorola Solutions.

Please contact edesixsales@motorolasolutions.com to obtain Software Assurance.

2. Double-click the downloaded **VideoManager-setup-15.0.exe** file.
3. Confirm that the installer can make changes to the PC.
4. The VideoManager installer will open. Click ***Next***.
5. The administrator will be given the option to change where VideoManager is installed on their PC - once the destination has been chosen, click ***Install***.

VideoManager will be downloaded.

6. Click ***Finish***.
7. Multiple installers will open. Click through every one by clicking ***Next*** and ***Finish***.
8. Navigate to VideoManager's installation location, and click ***pss.exe***.
9. The web UI will be opened. Click ***Set Up***.
10. Read the licence agreement, and click ***Accept***.
11. Choose where users, groups, and incidents will be stored. The options are as follows:

    - ***Use built-in database server (recommended)*** - if this is selected, all users, groups, incidents, and other VideoManager data will be stored in VideoManager's default database.
    - ***Use external SQL Server database (advanced)*** - if there is an existing SQL Server, the administrator can connect it to VideoManager now.

    If this option is selected, the administrator must enter the following information:

    - ***Server name*** - this must be the name of the administrator's SQL Server.

    To find this information, open the Microsoft SQL Server Management Studio. The log in pane will display the SQL Server name in the ***Server name*** field.

    - ***Port number*** - this must be the SQL Server's port number.

    To find this information, open the SQL Server Configuration Manager, select ***SQL Server Network Configuration***, click ***Protocols for SQLEXPRESS***, and click ***TCP/IP***. Navigate to the ***IP Addresses*** tab, and scroll down to ***IPAll***. The port number is in the ***TCP Port*** field.

    - ***Database name*** - this must be the name of an **empty** database on the SQL Server.

    To create a new database on the SQL Server, open the Microsoft SQL Server Management Studio, click ***New Query***, and paste the following code:

```
USE master;
GO
CREATE DATABASE [pss]
COLLATE Latin1_General_100_CS_AS;
GO
ALTER DATABASE pss SET ALLOW_SNAPSHOT_ISOLATION
ON;
ALTER DATABASE pss SET READ_COMMITTED_SNAPSHOT
ON;
GO
```

Click ▶ ***Execute***. The database will be created automatically.

- ***Connection string*** - this is generated by VideoManager automatically. However, if the SQL Server is using Server Authentication instead of Windows Authentication, click ***Edit connection string*** and delete `integratedSecurity=true;`. Replace it with the following information:

```
username=[USERNAME];password=[PASSWORD]
```

For more information, please contact Technical Support and ask for the technical paper VideoManager and SQL Server Explained [ED-009-032].

12. The administrator will be prompted to create a VideoManager user. Enter a username and password, and re-enter the password to confirm.
13. Click ***confirm*** to save.
14. The administrator will be prompted to configure where their footage is sent initially:
    - If ***Encrypt Footage*** is set to ***On***, all footage will automatically be encrypted when sent between body-worn cameras and VideoManager.
    - In the ***Storage Location*** field, enter the path to which all footage will be sent.

    This can be changed later.

>> For more information, see Create, Edit and Delete File Spaces on page 344

15. Click ***confirm***.
16. The administrator will automatically be logged in to VideoManager and can start using the system.

2.2 Re-Download VideoManager

If VideoManager has previously been installed on the administrator's PC:

1. Ensure that Software Assurance has been obtained from Motorola Solutions.

   Please contact edesixsales@motorolasolutions.com to obtain Software Assurance.

2. Double-click the downloaded **VideoManager-setup-15.0.exe** file.
3. Confirm that the installer can make changes to the PC.
4. The administrator will be asked to uninstall the old version of VideoManager. This will **not** delete the administrator's database, as long as the administrator is upgrading to a newer version. Click ***Yes***, then ***Uninstall***.
5. The VideoManager installer will open. Click ***Next***.
6. The administrator will be given the option to change where VideoManager is installed on their PC - once the destination has been chosen, click ***Install***.

   VideoManager will be re-installed.

7. Click ***Finish***.
8. Multiple installers will open. Click through every one by clicking ***Next*** and ***Finish***.
9. Launch the web UI interface like normal.

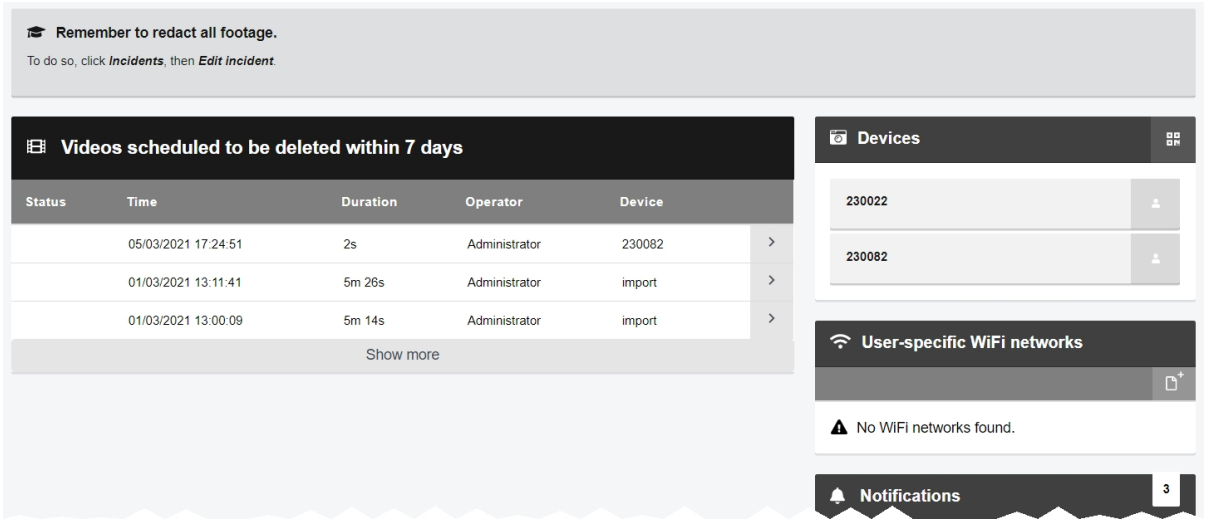
It may take a few moments for VideoManager to load after being updated - the administrator should refresh their browser if VideoManager does not open the first time.

10. Log in as recorderadmin or a previously created administrator.

    If logging in as recorderadmin, the administrator will immediately be asked to set and confirm a new password. If recorderadmin was previously disabled, it has now been deleted.

3 Home

When the user logs in, the first tab they will see is their ***Home*** tab. This provides a summary of the information and footage available to the user on VideoManager.



The following information is displayed:

- ***Videos scheduled to be deleted within {0} days*** - this pane lists all videos 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 videos scheduled to be deleted on dashboard*** permission enabled.

>> For more information, see Configure Deletion Policies on page 240

- ***Recent videos*** - this pane gives details about the videos most recently downloaded from a body-worn camera. The user can navigate to a chosen video 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***.

>> For more information, see Connect VT-Series Cameras to VideoManager Remotely on page 108

- ***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. 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 will display the media which has been shared.

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

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

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

  *The number of notifications corresponds to the number of videos 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 would display 4 notifications - one for each video.*

  If the user clicks ***View***, VideoManager 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 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 will display the import jobs. The user can then click ***View assets***, and VideoManager will display the imported asset 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 will display the warnings.

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

💡 *If VideoManager 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 that the user is utilising. It also gives users the option to export system logs, and lists any licensed features the user has enabled.
- ***Messages*** - this pane displays system messages set by either the user or an administrator.

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

>> For more information, see Create, Edit and Delete Messages on page 317

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

4 Videos

The ***Videos*** tab provides access to all videos available to a user in VideoManager and related functions which they can perform on videos.

If users have sufficient permissions, they can:

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

>> For more information, see Search Videos on page 19

- Change the default layout of the ***Videos*** tab on VideoManager.

>> For more information, see Change Viewing Options on page 22

- Import external videos into VideoManager.

This includes any videos which have **not** been recorded on a Motorola Solutions body-worn camera.

>> For more information, see Import Videos on page 24

- Watch videos which have been recorded on body-worn cameras or imported into VideoManager.

>> For more information, see Watch Videos on page 25

- Edit video properties (e.g. who owns the video, which body-worn camera recorded the video).

>> For more information, see View and Edit Video Properties on page 27

- 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 Video on page 29

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

>> For more information, see Perform Video Actions on page 30

- If *Asset Import* has been licensed, users can import assets into VideoManager.

This includes videos which have **not** been recorded on a Motorola Solutions body-worn camera, and other media including PDFs, JPEGs, and audio files.

>> For more information, see Import Assets on page 33

- View previously-imported assets.

>> For more information, see View Assets on page 35

- Edit asset properties (e.g. who owns the asset, which body-worn camera is associated with the asset).

>> For more information, see View and Edit Asset Properties on page 37

- Perform asset actions (e.g. rotate an asset, view an asset's audit log, etc.).

>> For more information, see Perform Asset Actions on page 39

- Share a video or asset with other users on VideoManager.

>> For more information, see Share Videos and Assets on page 41

- If *Media Preparations* has been licensed, users can redact still images like they would redact videos in an incident.

>> For more information, see Prepare Media on page 43

- Bulk edit videos and any assets which have been imported.

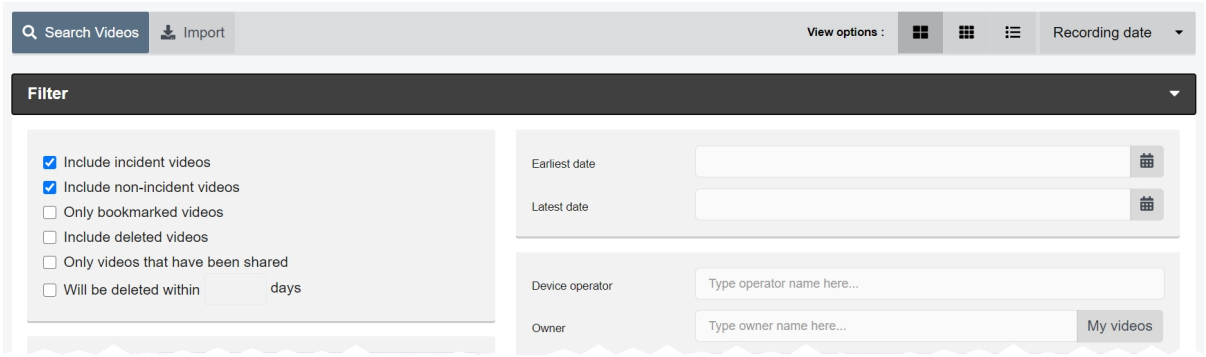
>> For more information, see Bulk Edit Videos and Assets on page 45

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

If a user supervises other users, the supervised users' videos are shown under the ***Supervised Videos*** pane.

4.1 Search Videos

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



Videos can be searched by a number of criteria.

1. Navigate to the ***Videos*** tab.
2. Select the ***Search Videos*** pane.

Users can now filter videos by the following criteria:

- ***Location*** - search for videos 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 videos recorded between set earliest and latest dates. Users can also choose a specific time of day (in 24 hour format).
- ***Device operator*** - search for videos downloaded by a specified user.
- ***Owner*** - search for videos 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 video has left the organisation and their user has been reassigned to someone else, that user becomes the owner of all their footage. From the ***Video Details*** page, it is also possible to edit who the owner of the footage is.

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

- ***Device*** - search for videos from a specified body-worn camera (or other source, if the user has enabled *Asset Import*). This should be done by serial number.
- ***Origin*** - this will filter videos by the location to which they were downloaded. This could be a DockController, a mobile phone, or the PC on which VideoManager is running.

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

- ***Video or Recording ID*** - search for a video by its unique video ID.

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

- ***Match text*** - search for videos whose user-defined media fields match the text entered here.

For example, a drop down field might have two options: *yes* and *no*. If the user enters *yes* into the ***Match text*** field, all videos whose drop down field has been set to *yes* will be returned.

>> For more information, see Create New User-defined Media Fields on page 283

- ***Advanced filter*** - users with knowledge of using sequence conditions can input more advanced search queries here.

>> For more information, see Appendix E: Custom Predicate Language on page 469

There are also filters which can be checked:

- ***Include incident videos*** - select whether to include videos which are part of one or more incidents.
- ***Include non-incident videos*** - select whether to include videos which are **not** part of one or more incidents.
- ***Only bookmarked videos*** - select whether only bookmarked videos are shown.

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

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

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

Recently deleted videos will have a red heading.

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

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

>> For more information, see Add Location Information to a Video on page 29

- ***Only videos that have been shared*** - select whether only videos that have been shared with other users on the system are shown.
- ***Only videos that will be deleted within*** (0) ***days*** - filter videos based on when they are scheduled to be deleted automatically, based on VideoManager's deletion policy.

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

>> For more information, see Configure Deletion Policies on page 240

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

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

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

If the user wants to search for videos 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 videos*** to search for the relevant videos.

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

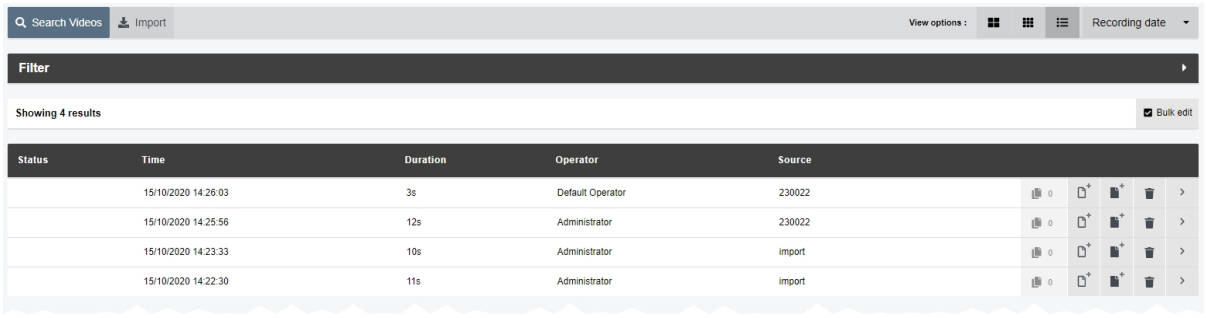
>> For more information, see Change Viewing Options on page 22

4.1.1 Change Viewing Options

Users can change video presentation options. This helps users to locate videos faster, and is done from the ***Videos*** tab. Users can only change the preferences for their own session on VideoManager.

Alternatively, administrators can set the default for **every** user on VideoManager, instead of just changing the default for their session. This is done from the ***Video List*** section of the ***User Interface*** pane, in the ***Admin*** tab.

>> For more information, see Configure the Video List on page 316



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

1. Navigate to the ***Videos*** tab.
2. Select the ***Search Videos*** 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 video, and allows video playback. Basic information about the video is displayed, with a list of the video actions available for this video.
   - **Gallery** - this displays each video in a grid. Each image in the grid is a still frame from one minute of the video. Click an image to jump to that point in the video. No other information is displayed, and the only action that can be performed is to delete the video.
   - **List** - this displays detailed information about each video:
     - ***Status*** - whether the video has been uploaded from a site, and whether the video has been bookmarked (by a VB400 in the field).
     - ***Time*** - when the video was recorded (date and hours/minutes/seconds).
     - ***Duration*** - the length of the video (hours/minutes/seconds).
     - ***Operator*** - who recorded the video.

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

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

- - how many incidents include the video in question. Clicking this will either open the relevant incident (if the video only belongs to one) or present the list of incidents (if the video belongs to more than one).
- Video actions available for this video.

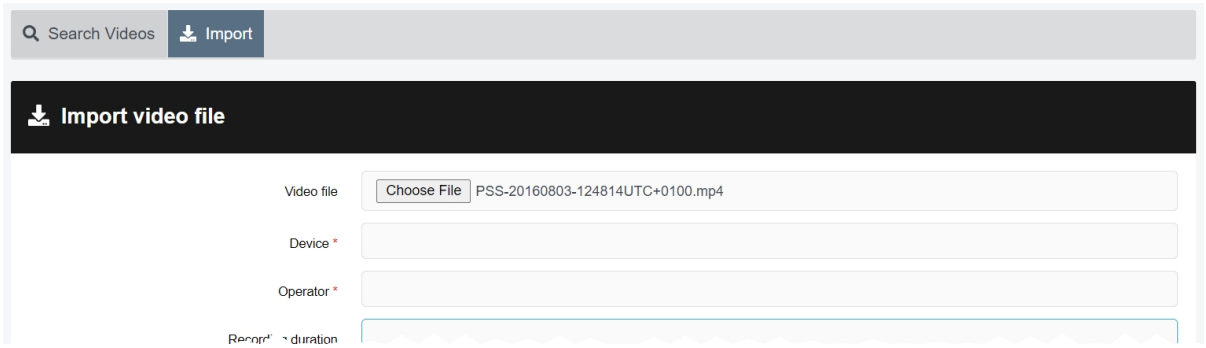
>> For more information, see Perform Video Actions on page 30

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

1. Navigate to the ***Videos*** tab.
2. Select the ***Search Videos*** pane.
3. Click the relevant filter from the top right-hand dropdown menu.
   - **Recording date** - this will present videos from most recently recorded to least recently recorded.
   - **Recording date (least recent)** - this will present videos from least recently recorded to most recently recorded.
   - **Date added** - this will present videos from most recently downloaded to least recently downloaded.

4.2 Import Videos

Users with the *Import* licence can import videos into VideoManager. This may be useful if there are videos from other camera systems that users wish to integrate with VideoManager, or if there are relevant external videos which should be added to an incident.



To import a video:

1. Navigate to the ***Videos*** tab.
2. Select the ***Import*** pane.
3. Click ***Choose File***.

Users should select the relevant video file.

4. In the ***Device*** field, enter the serial number of the body-worn camera which will be associated with this video. This must be a body-worn camera which is associated with VideoManager.

Alternatively, the user can enter the origin of the video instead. This could be another database, or a website name (if relevant).

5. In the ***Operator*** field, enter the name of the operator which will be associated with this video.

Caution *If the user does not enter the name of a previously-created user on VideoManager, the video cannot be imported.*

The ***Recording duration***, ***Recording ended***, and ***Upload name*** fields cannot be edited.

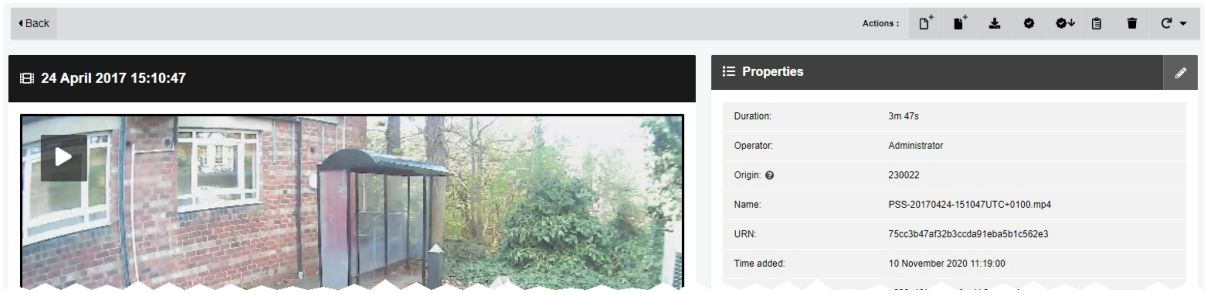
6. Click ***Start import***.

Once they have been successfully imported, these videos can be viewed from the ***Videos*** tab like normal.

>> For more information, see Search Videos on page 19

4.3 Watch Videos

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



There are some optional steps that administrators can complete before users watch videos. They are as follows:

- Configure the playback policy.

This dictates whether users must record a reason for watching a video after a certain time period. It also dictates whether all videos have a watermark overlaid, associated with the user watching it.

>> For more information, see Configure the Playback Policy on page 305

- Configure the default quality of videos which are played back on VideoManager. The default video quality setting is ***Low***.

>> For more information, see Configure Player on page 324

To watch a video on VideoManager:

1. Navigate to the ***Videos*** tab.
2. Find the relevant video, and click > ***More Details*** next to it.

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

3. Click ***Play video***.

The video will start to play.

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

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

- To skip through the video, use the following controls:
  - ***Cursor handle*** - track backwards and forwards through the video.
  - ***Play*** - plays or pauses the video.
  - ***Step Backward*** - steps backwards through the video one frame at a time.
  - ***Step Forward*** - steps forwards through the video one frame at a time.
  - ***Playback Speed*** - plays the video 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 video.

  Administrators can configure the type of metadata recorded alongside videos.

  >> For more information, see Configure Video metadata overlay settings on page 210

  - ***Audio*** - switches audio on or off.
  - ***Take Screenshot*** - takes a screenshot of the video in playback.

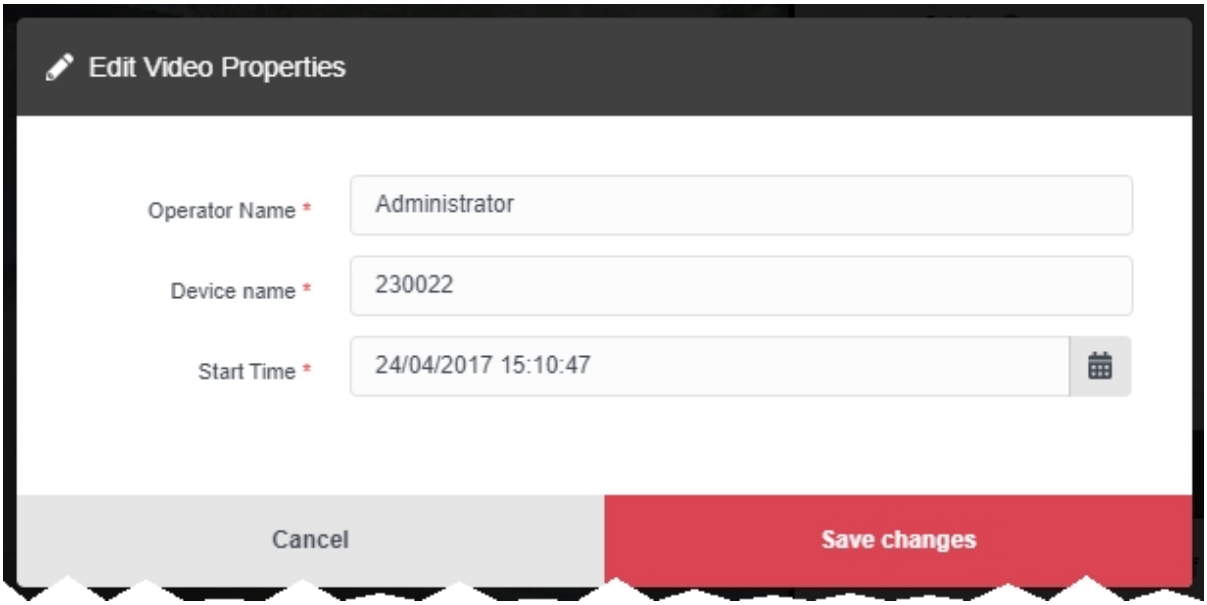
  The screenshot will be automatically downloaded to the user's PC.

  - ***Video Quality*** - changes the quality of the video 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.

Once a user has finished watching a video, they can return to the ***Search Videos*** pane by clicking ***Back***.

4.4 View and Edit Video Properties

Users with sufficient permissions can edit video properties.



To view the properties of a video:

1. Navigate to the ***Videos*** tab.
2. Find the relevant video, and click > ***More details*** next to it.

Users can find the relevant video by navigating to the ***My Videos***, ***Shared Videos***, or ***Supervised Videos*** panes. They can also search for the relevant video from the ***Search Videos*** 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 footage.

   If the video was imported, this will be the name of the user who imported the footage.
   - ***Origin:*** - the body-worn camera on which the video was filmed.
   - ***Name*** - the name of the video on VideoManager's file space.
   - ***Video ID*** - the unique URN assigned to this video.
   - ***Recording ID*** - if the video is part of a longer recording, this is the unique URN assigned to that recording.
   - ***Time added:*** - the time and date of when the video was downloaded to VideoManager (either from a body-worn camera, or an external source).
   - ***Encoding information:*** - the FPS of the video.

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

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

>> For more information, see Configure Deletion Policies on page 240

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

If the field reads as ***Success***, VideoManager has successfully verified that the video 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 does not recognise the certificate of the body-worn camera which recorded the video.

If the field is not present at all, this could be because the video 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.

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

- ***Operator name*** - who recorded the video.

*To change the **owner** of a video, administrators must instead change the sharing settings for it.*

>> For more information, see Share Videos and Assets on page 41

- ***Device name*** - which body-worn camera recorded the video.
- ***Start time*** - when the video was initially added to VideoManager. This either means when the body-worn camera which filmed the video was redocked, or when the video was uploaded from the user's PC.

This does **not** change when the video was actually recorded.

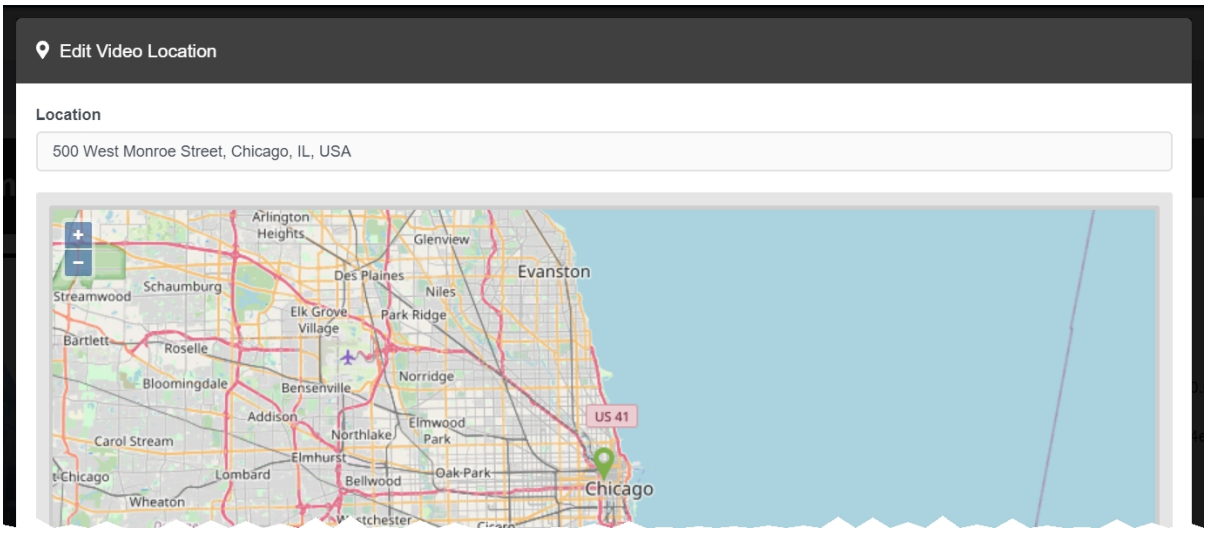
- Any user-defined media fields which have been created.

>> For more information, see Create New User-defined Media Fields on page 283

Click ***save changes***.

4.5 Add Location Information to a Video

Sufficiently privileged users can add location data to VideoManager videos which were recorded without it. This is useful if the original video 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 video.



To add location data to a video, or edit previously existing location data:

1. Ensure that location information has been enabled on VideoManager. This is done from the ***Maps*** section of the ***User Interface*** pane, in the ***Admin*** tab.

>> For more information, see Enable and Configure Maps on page 327

2. Navigate to the ***Videos*** tab.
3. Find the relevant video, and click > ***More Details*** next to it.

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

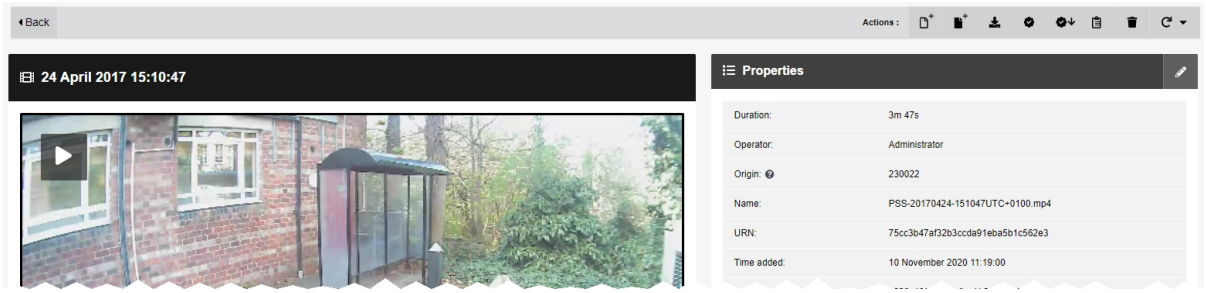
4. In the ***Location*** pane, click ***Edit location***.
5. Click and drag the map to position the marker at the desired location.

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

6. Click ***confirm*** to save.

4.6 Perform Video Actions

VideoManager gives users the option to perform actions on their videos from the ***More Details*** pane. It is possible to perform most of these actions from the ***Search Videos*** 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 ***Videos*** tab.
2. Find the relevant video, and click > ***More Details*** next to it.

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

From here, users can perform the following actions:

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

This will create an incident containing the video.

>> For more information, see Create Incidents Manually and Perform Incident Actions on page 49

- To add a video to a previously-created incident, click ***Add video to existing incident***. Click > ***Add video to this incident*** next to the relevant incident.
- To verify a video, 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 video's signature, click ***Download signature verification report***.

The downloaded .zip contains the following information about the video:

  - certificate-chain.pem - the PEM-encoded list of certificates included in the signature that was verified by VideoManager.
  - 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 downloaded), and a description of the certificate chain, including the serial, subject, issuer, and validity period of each certificate.

For more information, please contact Technical Support and ask for the technical paper *X.509 Signing Explained [ED-009-069]*.

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

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

- To view the video's audit log, which reflects **all** actions taken on the video since it has been added to VideoManager, click ***View Video Audit Log***, and filter the audit log using the following fields:
  - ***Source*** - this will return actions performed on the video by the specified source (e.g. a body-worn camera on VideoManager).
  - ***Event type*** - this will return specific actions performed on the video.

  If the user starts entering an event, VideoManager will suggest various event options (e.g. **FOOTAGE_PLAY**).
  - ***User*** - this will return actions performed on the video by the specified user.

  If the user starts entering a username, VideoManager will suggest various usernames to match it.
  - ***Message*** - this will return specific actions performed on the video, whose details match the keywords entered here.

  For example, the **FOOTAGE_PLAY** event comes with the message ***View Video File***.
  - ***Signature*** - the user should enter the signature of an incident. This will return actions performed on the video in relation to this incident.

  For example, when the video was added to the specified incident.
  - ***Location*** - this will return actions performed on the video from a specific Dock-Controller or EdgeController.
  - ***Client*** - this will return actions performed on the video from a specific IP address.
  - ***Server*** - this will return actions performed on the video from a specific server hosting VideoManager.

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

- To delete the video, which will remove it from the ***Videos*** tab and VideoManager, click ***Delete video***.

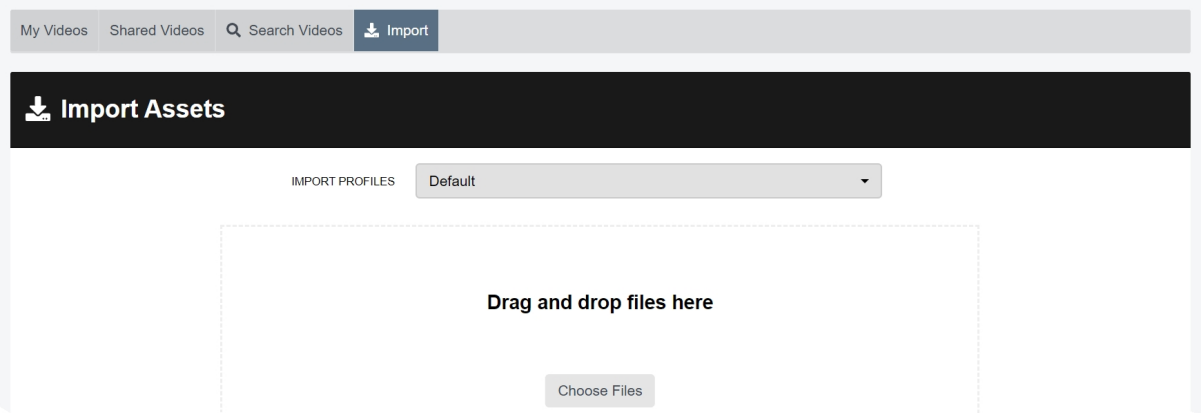
  For a short while a deleted video can still be "undeleted", depending on how VideoManager's deletion policy has been configured, using the ***Include deleted videos*** option when searching from the ***Search Videos*** pane.

- To flip the video, click ***Rotate*** and select whether the video 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 Videos*** page as well.

4.7 Import Assets

Users with the *Asset Import* licence can import a variety of files into VideoManager, including still images and PDFs. These are called assets. This may be necessary if there are external files which should be added to an incident (for example, a scanned PDF of a warrant, or a CCTV still image of a suspect).



Before an administrator imports assets for the first time, there are some optional steps they can complete first:

- Create an import profile. This dictates whether an asset's user-defined media fields will be automatically populated as it is imported.

>> For more information, see Configure Import Profiles on page 300

- Enable and configure VideoManager's antivirus policy. This ensures that all assets are scanned for viruses before they are imported.

>> For more information, see Enable and Configure the Antivirus Policy on page 302

- Configure thumbnail settings.

VideoManager will allocate a thumbnail to assets which are imported without any.

>> For more information, see Configure Thumbnails on page 329

To import an asset:

1. Navigate to the ***Videos*** tab.
2. Select the ***Import*** pane.
3. Select the relevant import profile from the dropdown.
4. Users can now import an asset by either dragging and dropping the file into VideoManager, or by clicking ***Choose Files*** to select a file on their PC.

Repeat this step for as many assets as necessary.

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

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

>> For more information, see View Import Jobs on page 156

Once an asset has been successfully imported, users can view it from the ***Videos*** tab like videos recorded on body-worn cameras.

>> For more information, see Search Videos on page 19

4.8 View Assets

If the user has licensed *Asset Import*, they can view assets in the same way that they would view a video. However, there are also some asset-specfic actions they can take. The actions in question depend on the type of file that has been imported.

To access playback controls:

1. Navigate to the ***Videos*** tab.
2. Find the relevant asset, and click > ***More Details*** next to it.

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

Users can now view imported assets.

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 video*** - the audio file will play. Users can skip, pause, and step through the file like a normal video.
- ***Settings*** - this is similar to the ***Settings*** control for videos, but only has options for ***Keyboard Shortcuts***, ***Metadata Overlay***, and ***Audio Quality***.

>> For more information, see Watch Videos on page 25

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 asset. 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.

>> For more information, see Prepare Media on page 43

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

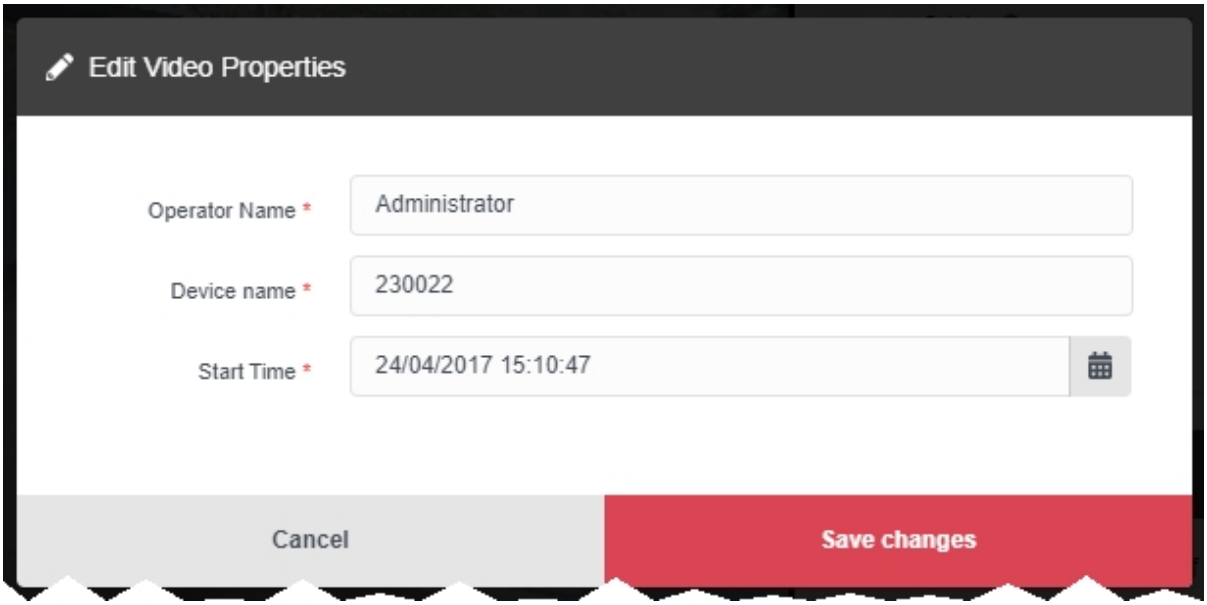
The ***Theatre*** and ***Fullscreen*** controls function as normal.

>> For more information, see Watch Videos on page 25

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.

4.9 View and Edit Asset Properties

Users with sufficient permissions can edit asset properties.



To view the properties of an asset:

1. Navigate to the ***Videos*** tab.
2. Find the relevant asset, and click > ***More details*** next to it.
3. In the ☰ ***Properties*** pane, the following information will be displayed:
   - ***Operator:*** - the name of the operator who created the asset.
   - ***Origin:*** - the body-worn camera which is associated with this asset.
   - ***Video ID:*** - the unique URN assigned to this asset.
   - ***Time added:*** - the time and date of when the asset was uploaded to VideoManager.
   - ***Scheduled deletion:*** - if the deletion policy has been configured, this field shows when the asset will be deleted by VideoManager automatically.

   This could be based on a number of factors, including how many days have elapsed since the assets were downloaded to the PC or uploaded to VideoManager.

>> For more information, see Configure Deletion Policies on page 240

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

- ***Operator name*** - who owns the asset.
- ***Device name*** - which body-worn camera or source is associated with the asset.

This does not need to be a body-worn camera associated with VideoManager - users could enter the name of the website from which the asset was downloaded or retrieved, or the PC from which it was uploaded.

- ***Start time*** - when the asset was imported to VideoManager.
- Any user-defined media fields which have been created.

>> For more information, see Create New User-defined Media Fields on page 283

Click ***save changes***.

4.10 Perform Asset Actions

VideoManager gives users the option to perform actions on their assets from the ***More Details*** pane. It is possible to perform most of these actions from the ***Search Videos*** 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 ***Videos*** tab.
2. Find the relevant asset, and click > ***More Details*** next to it.

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

From here, users can perform the following actions:

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

This will create an incident containing the asset.

>> For more information, see Create Incidents Manually and Perform Incident Actions on page 49

- To add an asset to a previously-created incident, click ***Add video to existing incident***. Click > ***Add video to this incident*** next to the relevant incident.
- To verify an asset, which indicates whether it has been tampered with since being uploaded to VideoManager, click ***Verify file integrity***.

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

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

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

- To view the asset's audit log, which reflects **all** actions taken on the asset since it has been added to VideoManager, click ***View Video Audit Log***, and filter the audit log using the following fields:
  - ***Source*** - this will return actions performed on the asset by the specified source (e.g. a body-worn camera on VideoManager).

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

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

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

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

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

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

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

For example, when the asset was added to the specified incident.

- ***Location*** - this will return actions performed on the asset from a specific Dock-Controller or EdgeController.
- ***Client*** - this will return actions performed on the asset from a specific IP address.
- ***Server*** - this will return actions performed on the asset from a specific server hosting VideoManager.
- From the ***Date range*** dropdown, users can select the date range for these actions.

- To delete the asset, which will remove it from the ***Videos*** tab and VideoManager, click ***Delete video***.

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

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

This is not possible for all assets (e.g. PDFs).

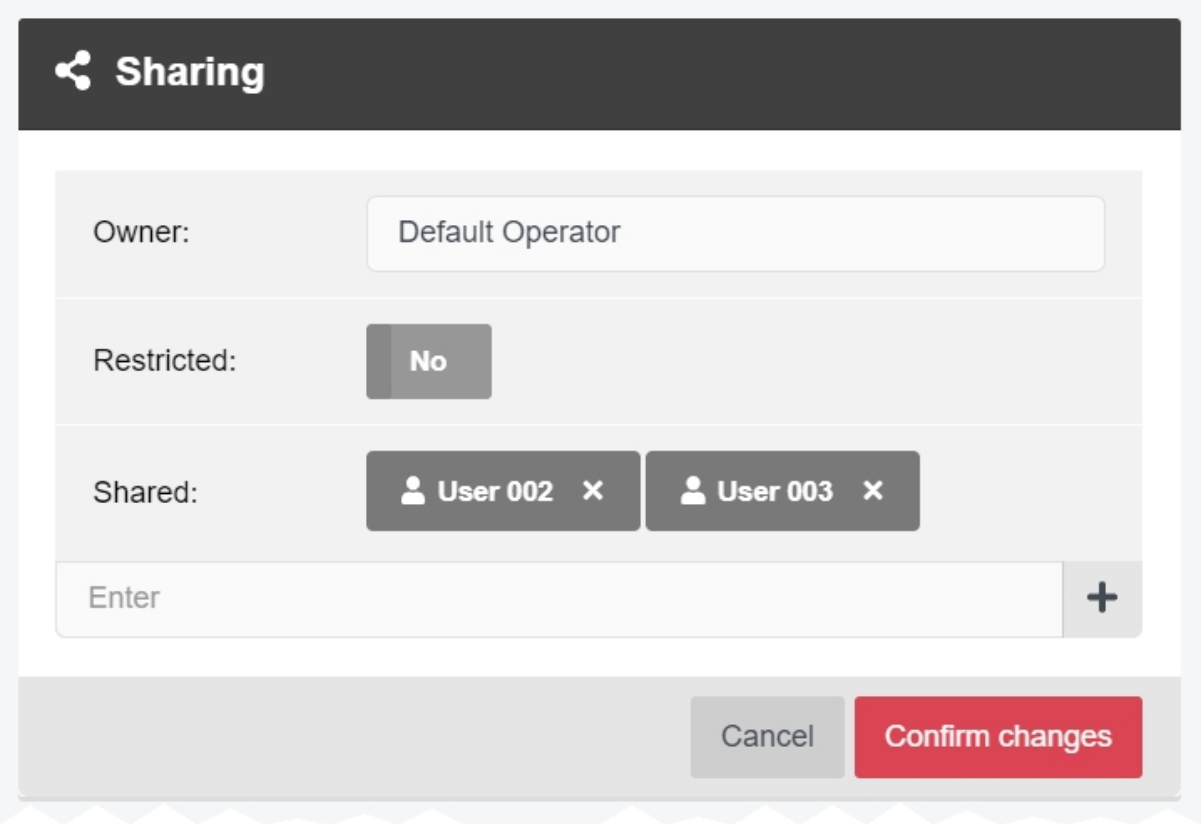
Apart from audit logs, it is possible to perform these actions from the ***Search Videos*** page as well.

4.11 Share Videos and Assets

It may be necessary for users to share their videos/assets with their peers, without having the ability to see all videos/assets on the system (for instance, if they want a second opinion about a procedure or an event). In this case, users can utilise VideoManager's sharing function to give other users access to a video/asset.

It is only possible to share individual videos/assets with other users on VideoManager. To share videos/assets with people who do not have a VideoManager account, users must instead share an entire incident.

>> For more information, see Share Incidents Externally Using a Link on page 91



To share a video/asset on VideoManager:

1. Navigate to the ***Videos*** tab.
2. Find the relevant video/asset, and click > ***More Details*** next to it.
   Users can find the relevant video/asset by navigating to the ***My Videos***, ***Shared Videos***, or ***Supervised Videos*** panes. They can also search for the relevant video/asset from the 🔍 ***Search Videos*** pane.
3. In the ***Sharing*** pane, click ✎ ***Edit sharing settings***.
4. In the ***Owner:*** field, administrators can change the owner of the video/asset.

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

*If administrators want to change the **operator** who recorded the video/imported the asset, they must do so from the **Properties** pane instead.*

5. If ***Restricted:*** is set to ***Yes***, only users with the ***List restricted videos*** permission will be able to search for the video/asset. Only users with the ***Play restricted videos*** permission will be able to watch the video/asset.
6. In the ***Shared:*** field of the ***Sharing*** panel, enter the name of the user, with whom this video/asset will be shared. Click + next to this field to add this user to the list.

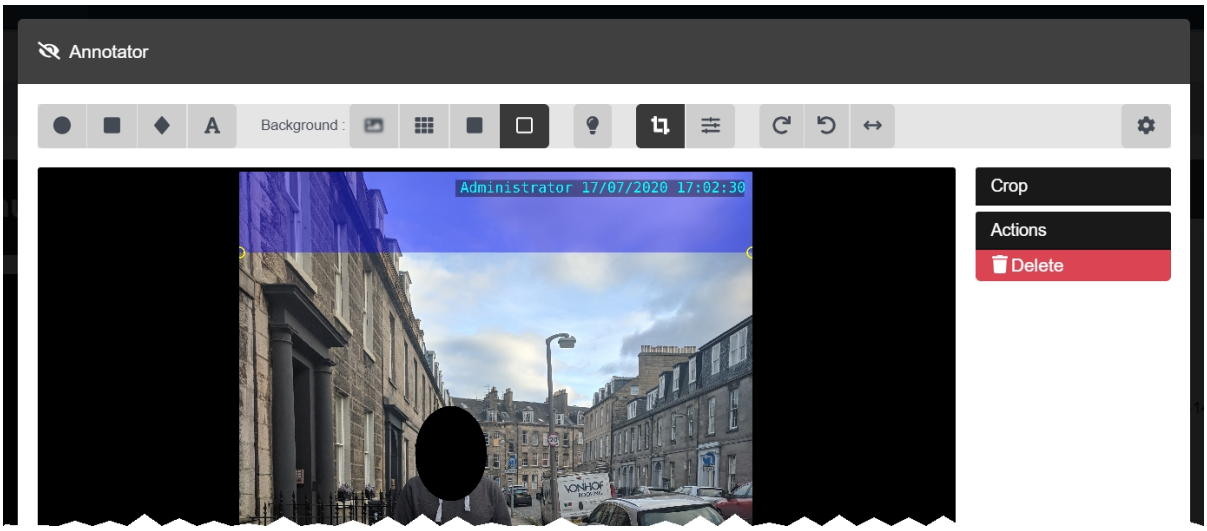
If + is not clicked, the user will not be added.

7. Click ***Confirm Changes***.

Shared videos/assets will appear in the selected user's ***Shared Videos*** list. Depending on the permissions which have been enabled under the ***Shared*** column of the role(s) they are a part of, the user can now access the video/asset like normal.

4.12 Prepare Media

Media Preparations is a licensed feature that gives users the ability to prepare still images in the same manner that they would redact footage in an incident - however, unlike footage, still images **do not** need to be part of an incident in order to be prepared.



To prepare media:

1. Navigate to the ***Videos*** tab.
2. Find the relevant asset, and click > ***More Details*** next to it.
   Users can find the relevant asset by navigating to the ***My Videos***, ***Shared Videos***, or ***Supervised Videos*** panes. They can also search for the relevant asset from the 🔍 ***Search Videos*** pane.
3. Click ***Prepare Media***.
4. The user can now prepare assets in the same way they would redact a video.

>> For more information, see Redact an Incident Clip on page 59

If the prepared asset is added to an incident, it will retain the redactions added here - users can add new redactions in the same manner that they would add redactions to a video. However, if the asset is later redacted from this page again, the asset that was added to incidents beforehand will **not** be updated accordingly. The asset 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**.*

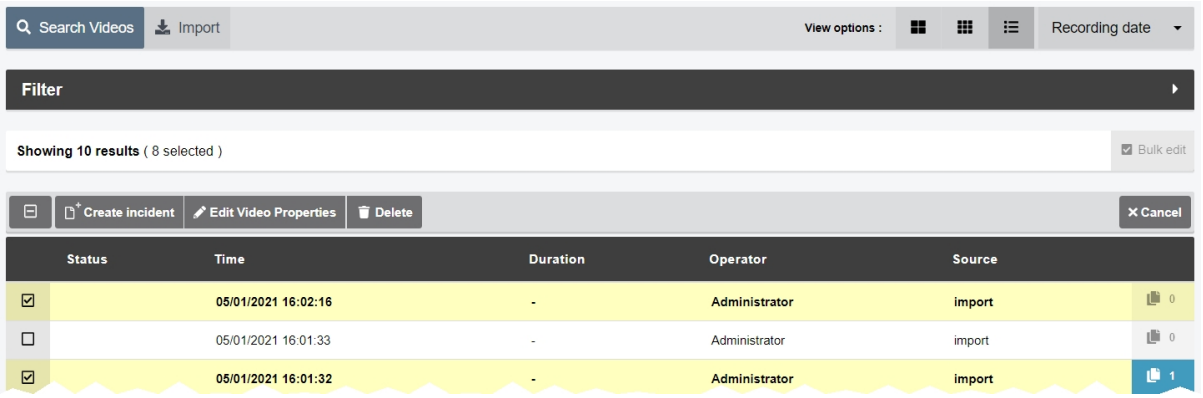
- ***Adjust the image*** - if the user clicks this, a set of sliders will appear in the right-hand menu. These sliders control ***Contrast***, ***Brightness***, ***Saturation***, and ***Gamma***.

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

4.13 Bulk Edit Videos and Assets

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

They are also useful if the user has enabled their VideoManager to act as a Central VideoManager. In this case, every video held in connected sites can be automatically fetched in bulk. This means that they will become editable in the Central VideoManager and unviewable in the original sites.



To bulk edit videos:

1. Navigate to the ***Videos*** tab.
2. Select the 🔍 ***Search Videos*** pane.
3. Filter the videos/assets as necessary, and click ***Find videos***.
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 videos to be bulk edited:
   - To select **indvidiual** videos, click ■ next to their rows.
   - To select **all** videos onscreen, click ■/☑ **Toggle selection of ALL rows.**.

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

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

- ↻ **Rotate** - this presents a dropdown which gives users the ability to rotate multiple videos clockwise, anti-clockwise, 180 degrees, or horizontally.
- 🗎+ **Create incident** - this gives users the ability to create an incident with all the selected videos/assets included.
- ✎ **Edit properties** - this gives users the ability to edit the fields for all videos/assets 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 videos/assets with other users simulatenously.
    - In the ***Owner:*** field, administrators can change the owner of the videos/assets.

  This can be a user or an entire group. If the owner of the videos/assets is a group, **all** users in that group will be able to process the videos/assets as if the videos/assets were their own (i.e. adding them to incidents, redacting them).
    - If ***Restricted:*** is set to ***Yes***, only users with the ***List restricted videos*** permission will be able to search for the videos/assets. Only users with the ***Play restricted videos*** permission will be able to watch the videos/assets.
    - In the ***Shared:*** field of the ***Sharing*** panel, enter the name of the user, with whom these videos/assets 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 videos simultaneously. The user will be asked to confirm their choice.
- **Fetch** - this option is only available if VideoManager is enabled as a Central VideoManager. It gives users the ability to fetch all of the selected videos from their sites simultaneously. This is useful if the user's network is too weak to keep auto-fetch on continuously. Once they have been fetched, the videos are editable like normal in Central VideoManager but are not viewable on the original site.

>> For more information, see Configure Sites on page 374

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

5 Incidents

The ***Incidents*** tab provides access to all incidents available to VideoManager 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 49

- Create, edit and delete incidents automatically.

VideoManager will create incidents from videos which have had their user-defined media fields populated in a specific manner.

>> For more information, see Create Incidents Automatically on page 53

- Create, edit and delete incidents with bulk edit.

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

>> For more information, see Create Incidents with Bulk Edit on page 55

- Add videos to an incident after it has been created.

>> For more information, see Add Videos to an Existing Incident on page 57

- Clip evidential footage in an incident.

>> For more information, see Clip Footage in an Incident on page 58

- Redact footage in an incident.

>> For more information, see Redact an Incident Clip on page 59

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

>> For more information, see Search Incidents on page 78

- Bulk edit incidents.

>> For more information, see Bulk Edit Incidents on page 84

- Create, edit and delete bookmarks for videos in incidents.

These can be used to highlight portions of evidential footage.

>> For more information, see Create, Edit and Delete Bookmarks on page 86

- Share incidents (either internally or externally, using exports).

>> For more information, see Share Incidents on page 89

- View previously-created exports.

>> For more information, see View Exports on page 96

- Commit incidents (if configured as a Central VideoManager or site).

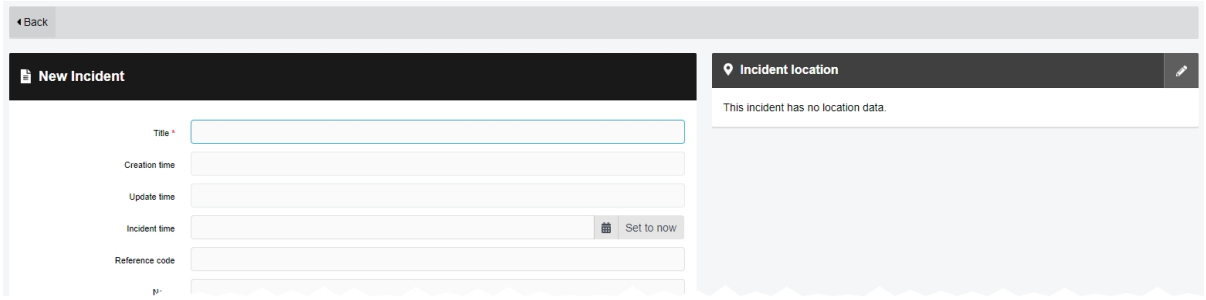
>> For more information, see Commit Incidents on page 98

- If *Nested Incidents* has been licensed, users can edit and delete incident collections.

>> For more information, see Create, Edit and Delete Incident Collections on page 100

5.1 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 videos from a body-worn camera, imported videos, or imported assets. Videos in an incident can be edited and redacted to preserve evidential integrity. Incidents can be shared with users either on the VideoManager system or outside of it.



There are some optional steps that administrators can complete before creating an incident for the first time. They are as follows:

- Create user-defined incident fields.

These fields will be presented automatically when creating and editing incidents, and enable users to categorise incidents in a manner which fits the unique needs of their organisation.

If user-defined incident fields are created **after** incidents have been created, those fields will be added to the ***Edit Incident*** form automatically and can be populated when the user edits an incident.

>> For more information, see Create New User-defined Incident Fields on page 264

- Import videos into VideoManager, either from a body-worn camera or using the *Import* licence.

>> For more information, see Import Videos on page 24

- Import assets (non-video media, such as PDFs) into VideoManager, using the *Asset Import* licence.

>> For more information, see Import Assets on page 33

- Configure whether incident clips are presented as **versions** of the original recording when they are redacted and edited in an incident, or as **unique videos** in their own right.

>> For more information, see Configure Incident Settings on page 330

There are two ways to create an incident.

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

1. Navigate to the ***Videos*** tab.
2. Find the relevant video, and click ***Create new incident*** next to it.

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

3. If the video is part of a longer recording because the body-worn camera which recorded it has been configured to split long recordings up into individual videos (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 video also recorded other videos at the same time (e.g. because multiple body-worn cameras were assigned to one operator), those videos 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 videos 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 videos attached to it. Users can add videos later by navigating to the ***Videos*** tab, finding the relevant video, and clicking ***Add video to this incident*** next to it.

>> For more information, see Add Videos to an Existing Incident on page 57

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 videos 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 videos are in the incident, and is automatically updated when a video 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 upon creation.

3. Populate the user-defined incident fields, if they have been configured.

>> For more information, see Create New User-defined Incident Fields on page 264

4. If necessary, clip the videos which have been added to the incident. This enables users to focus on the relevant sections of video.

>> For more information, see Clip Footage in an Incident on page 58

5. If necessary, redact the videos which have been added to the incident. This enables users to obscure sections of the video, in line with privacy regulations.

>> For more information, see Redact an Incident Clip on page 59

6. 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 videos from VideoManager. This is done from the **Videos** tab.*

>> For more information, see Add Videos to an Existing Incident on page 57

- 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 videos or assets 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.*

- Export an incident. This will create a copy of the incident which can then be shared with workers who are not on VideoManager.

To do so, click ***Export incident***, and click ***Create Export***.

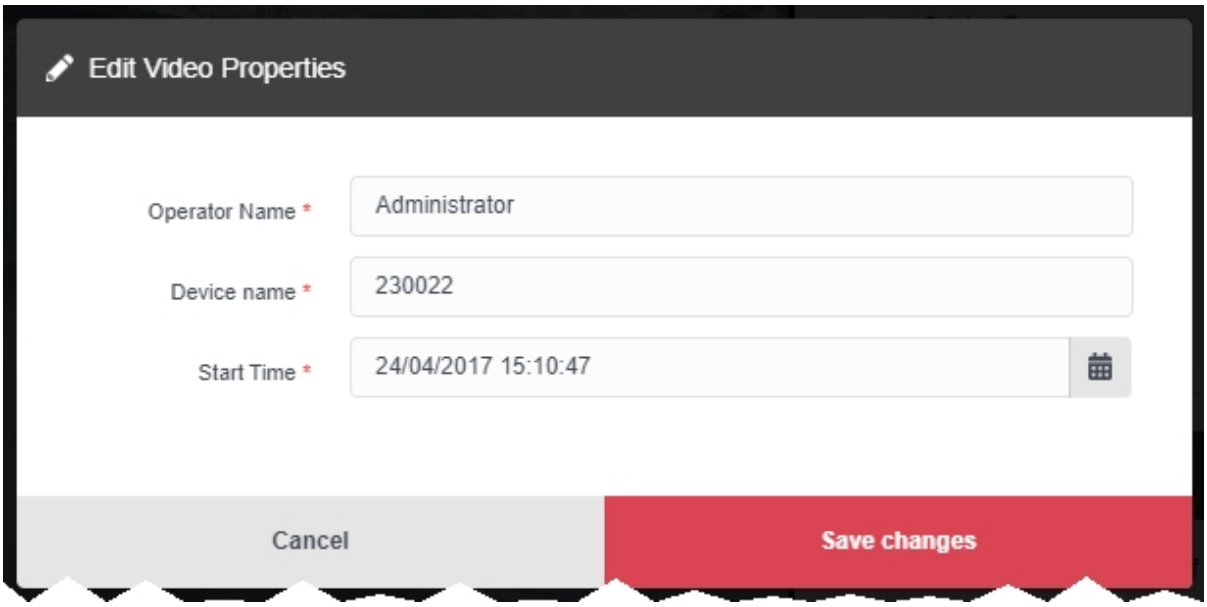
>> For more information, see Share Incidents Externally Using an Export on page 93

- Create an audit log for the incident. This will show a list of all actions which were performed on an incident, and which users performed them.

To do so, click ***View incident audit log***, filter the audit log as necessary, and click ***Filter audit log***.

5.2 Create Incidents Automatically

As well as creating incidents manually from the ***Incidents*** tab, administrators can also configure VideoManager so it will automatically create incidents from videos and assets, depending on the status of the videos/assets's user-defined media fields.



If automatic incident creation should be enabled, an administrator must complete the following steps first:

1. Create user-defined media fields, if they do not exist already.
   The way these fields are populated in an video/asset will determine whether VideoManager automatically creates an incident from the video/asset or not.

   >> For more information, see Create New User-defined Media Fields on page 283

2. Configure automatic incident creation settings.
   These settings determine which user-defined media fields will control automatic incident creation.

   >> For more information, see Enable and Configure Automatic Incident Creation on page 255

Once the configuration has been completed, users can create incidents from videos/assets. To do so:

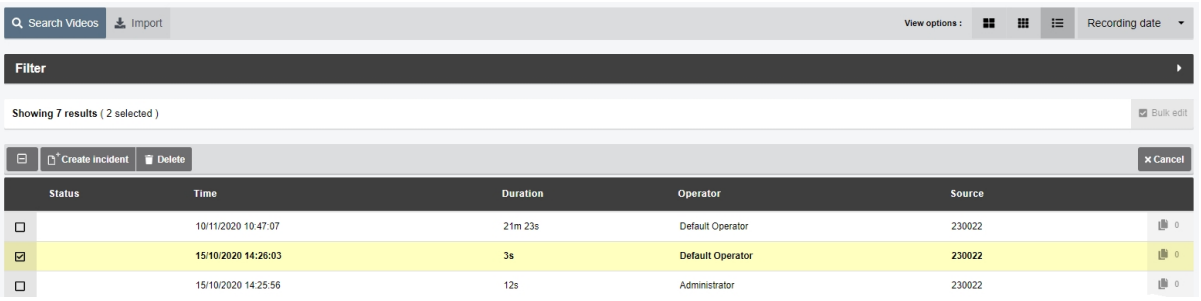
1. Navigate to the ***Videos*** tab.
2. Find the video/asset in question, and click > ***More details*** next to it.
   Users can find the relevant video/asset by navigating to the ***My Videos***, ***Shared Videos***, or ***Supervised Videos*** panes. They can also search for the relevant video/asset from the 🔍 ***Search Videos*** pane.
3. In the ☰ ***Properties*** pane, click ✎ ***Edit properties***.

4. Edit the user-defined media field, as configured from the ***Auto Incident Creation*** section.
5. Click ***save changes***.
6. Click ***confirm***.

To check that the incident has been created correctly, navigate to the ***Incidents*** tab. The incident should appear in the ***Search Incidents*** pane.

5.3 Create Incidents with Bulk Edit

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



There are some optional steps that administrators can complete before creating an incident with bulk edit. They are as follows:

- Create user-defined incident fields.

These fields will be presented automatically when creating and editing incidents, and enable users to categorise incidents in a manner which fits the unique needs of their organisation.

If user-defined incident fields are created **after** incidents have been created, those fields will be added to the ***Edit Incident*** form automatically and can be populated when the user edits an incident.

>> For more information, see Create New User-defined Incident Fields on page 264

- Import videos into VideoManager, either from a body-worn camera or using the *Import* licence.

>> For more information, see Import Videos on page 24

- Import assets (non-video media, like PDFs) into VideoManager, using the *Asset Import* licence.

>> For more information, see Import Assets on page 33

To create an incident with bulk edit:

1. Navigate to the ***Videos*** tab.
2. Select the **Search** ***Search Videos*** pane.
3. Filter the videos as necessary, and click ***Find videos***.
4. Optionally select **List** from the ***View options*** menu in the top right-hand corner.

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

5. Click ☑ ***Bulk Edit***.
6. Click ■ next to the relevant videos, or click ☑ **Toggle selection of ALL rows.** to select all videos.
7. Click **Create incident**.

All selected videos 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***.

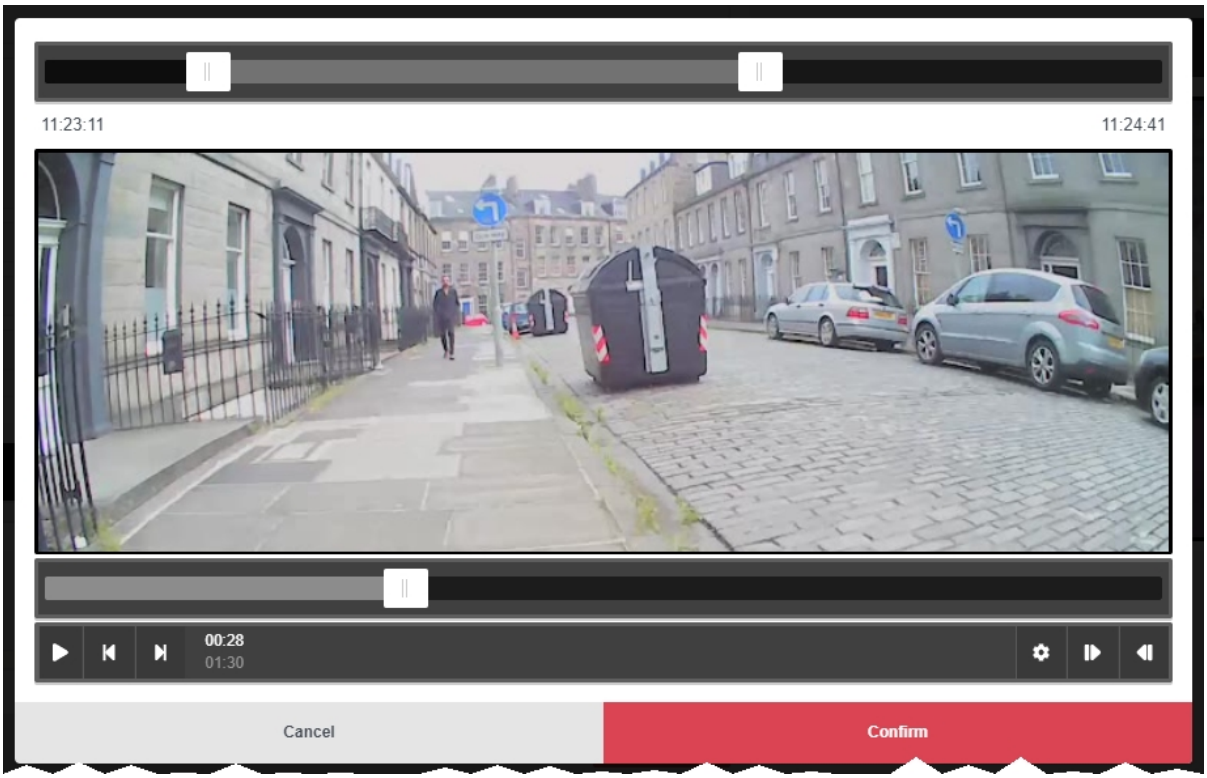
5.4 Add Videos to an Existing Incident

It may be necessary to add more videos to an incident after it has been saved. To do so:

1. Navigate to the ***Videos*** tab.
2. Select the ***Search Videos*** pane.
3. Filter the videos as necessary, and click ***Find videos***.
4. Next to the video which should be added to the incident, click ***Add video to existing incident***.
5. Filter the incidents as necessary, and click ***Find incidents***.
6. Click ***Add video to this incident*** next to the relevant incident.
7. 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.
8. Click ***Save incident***.

5.5 Clip Footage in an Incident

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

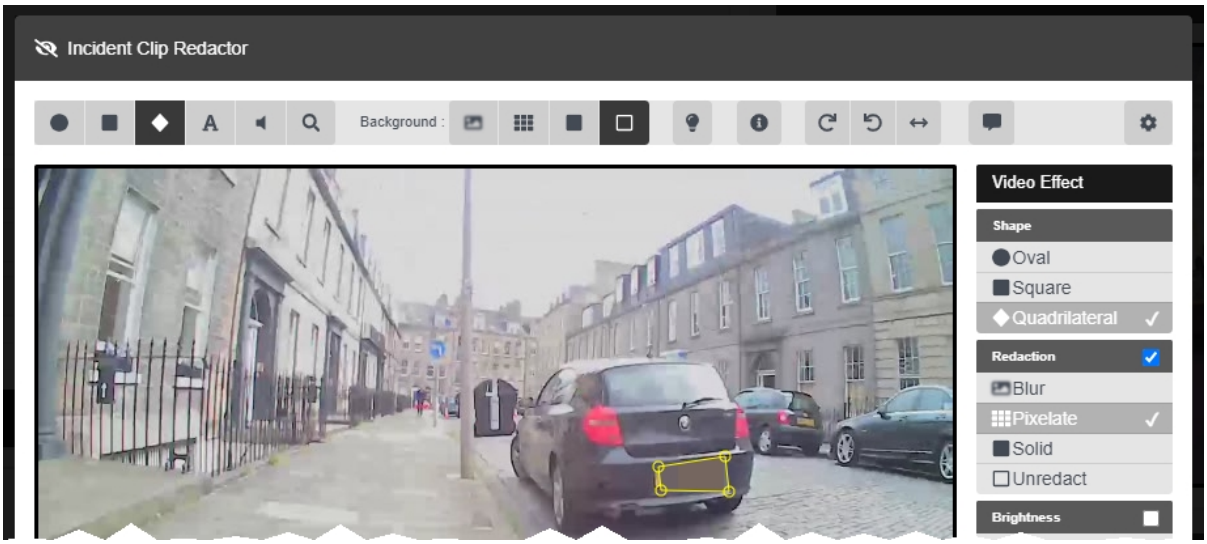


To clip footage:

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 video.
4. To shorten the video 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***.

5.6 Redact an Incident Clip

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



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:

- Foreground redactions.

>> For more information, see Create Foreground Redactions on page 61

- Background redactions.

>> For more information, see Create Background Redactions on page 63

- Audio redactions.

>> For more information, see Create Audio Redactions on page 65

- Text redactions.

>> For more information, see Create Text Annotations on page 67

- Brightness redactions.

>> For more information, see Create Brightness Redactions on page 69

- Zoom redactions.

>> For more information, see Create Zoom Redactions on page 71

- Captions.

>> For more information, see Add Captions to an Incident Clip on page 74

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

>> For more information, see Create Other Redactions on page 73

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

>> For more information, see Access the Redaction Advanced Dropdown on page 76

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

- Edit a redaction.

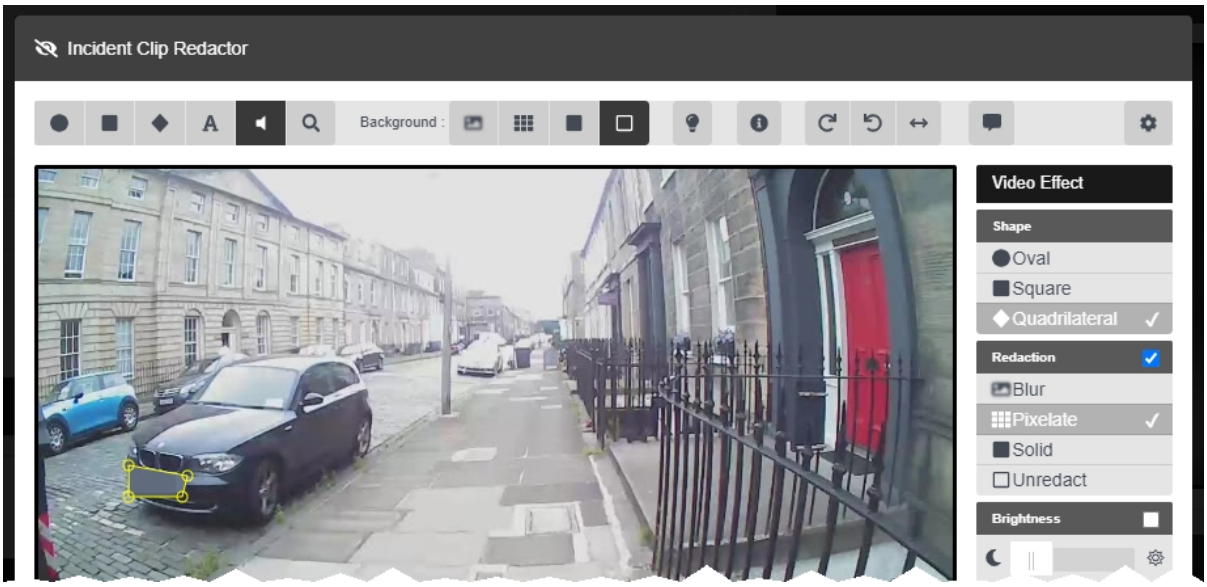
To do so, click ***Edit incident***. In the ***Incident clips*** section, click ***Redact parts of this clip***. Step forwards through the video to the point that the redaction starts, and select the redaction by clicking it. Make the necessary changes, click ***confirm***, then ***Save incident***.

- Delete a redaction.

To do so, click ***Edit incident***. In the ***Incident clips*** section, click ***Redact parts of this clip***. Step forwards through the video 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***.

5.6.1 Create Foreground Redactions

A circle, rectangle, or quadrilateral redaction can blur, pixelate, or solidly cover the focus of a video. 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 video.



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 video 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. From here, the user has two options:

    - If the subject of the video is moving, step through the video frame-by-frame and reposition the shape 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 video where the redaction should end, click ***End***.

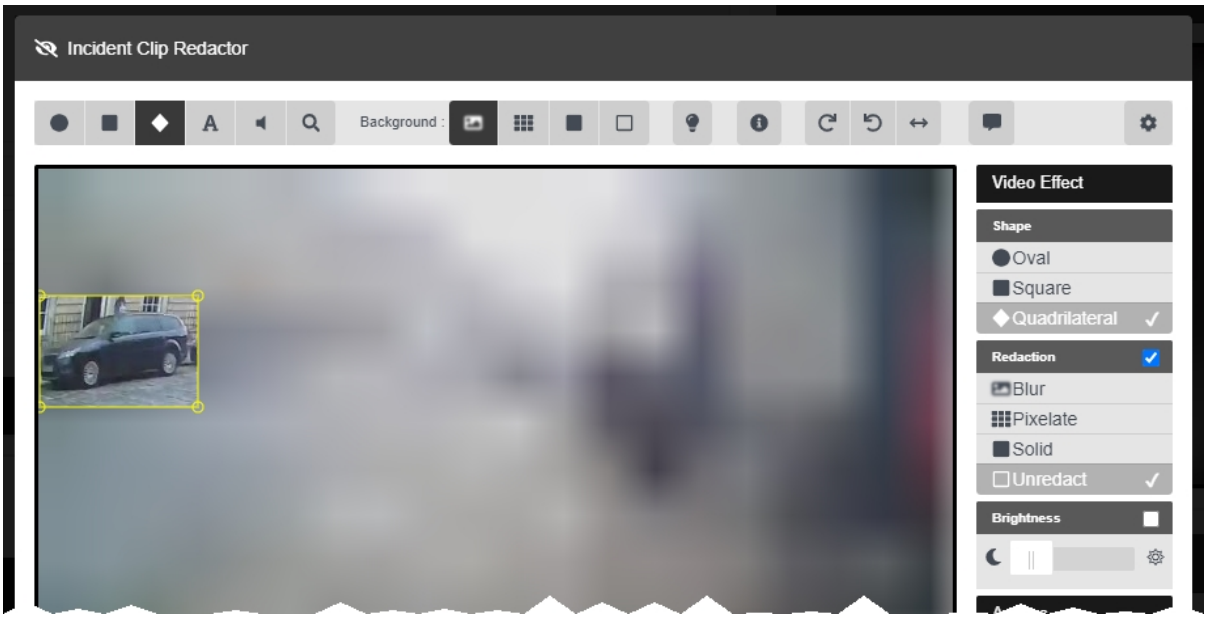
    Users do not need to redraw the annotation, just re-position it.

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

11. Repeat this for every new redaction to be added.
12. Click ***confirm***.
13. Click ***Save incident***.

5.6.2 Create Background Redactions

By redacting a background, the subject of evidential footage is made the sole focus. All foreground redactions can be applied to the background of a video 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 video 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. From here, the user has two options:

    - If the subject of the video is moving, step through the video frame-by-frame and reposition the shape 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 video where the redaction should end, click ***End***.

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

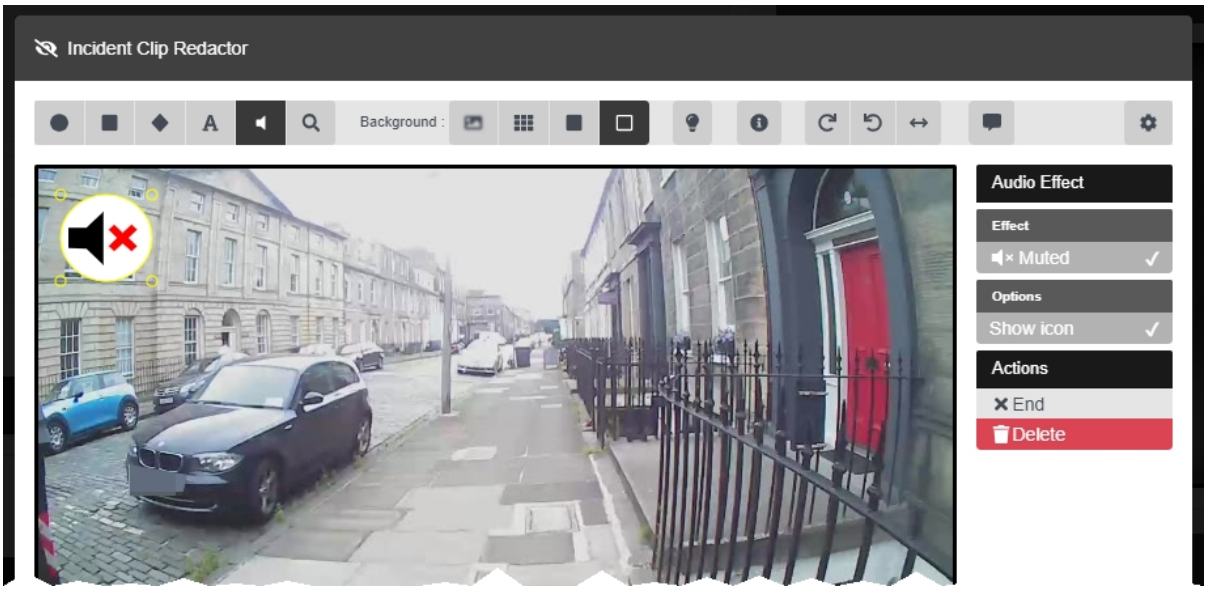
    - If the subject of the video is static, skip to the part of the video where the redaction should end, and click ***End***.

11. Click ***confirm***.
12. Click ***Save incident***.

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

5.6.3 Create Audio Redactions

Users can mute or beep over audio in videos 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 video 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 footage 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 footage.

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 video 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

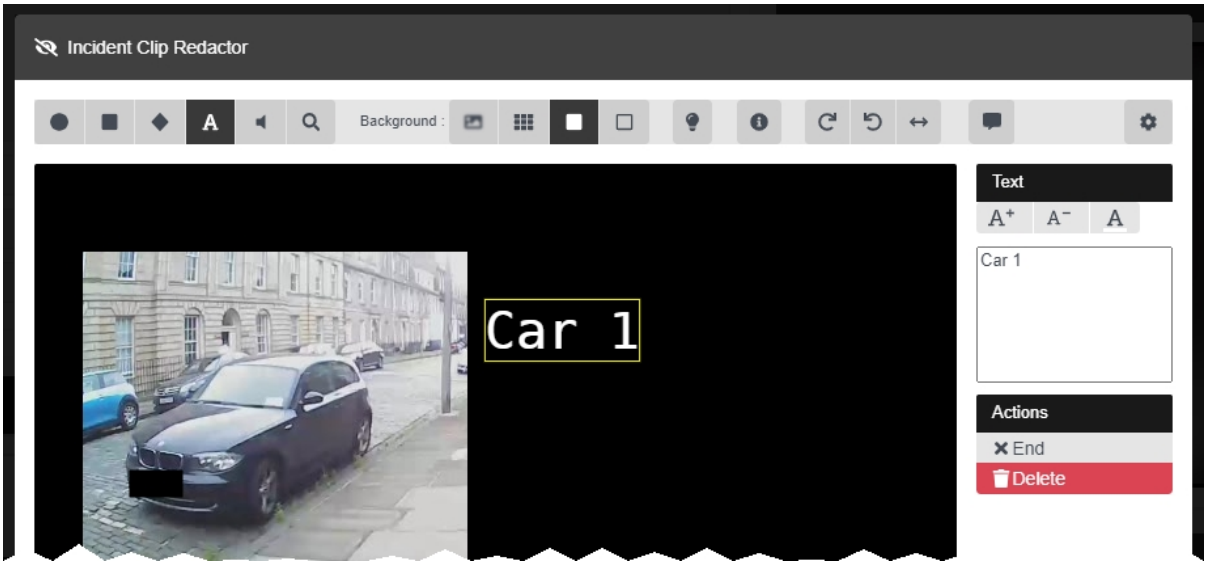
other audio in the video clearer.

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

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

5.6.4 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 video 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 ***Search Incidents*** pane.

3. In the ***Incident clips*** section, click ***Redact parts of this clip***.
4. Step forwards through the video to the point that the redaction should start.
5. Click ***Insert text***.
6. Click the area of the video 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, 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 video is moving, step through the video 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 video where the redaction should end, click ***End***.

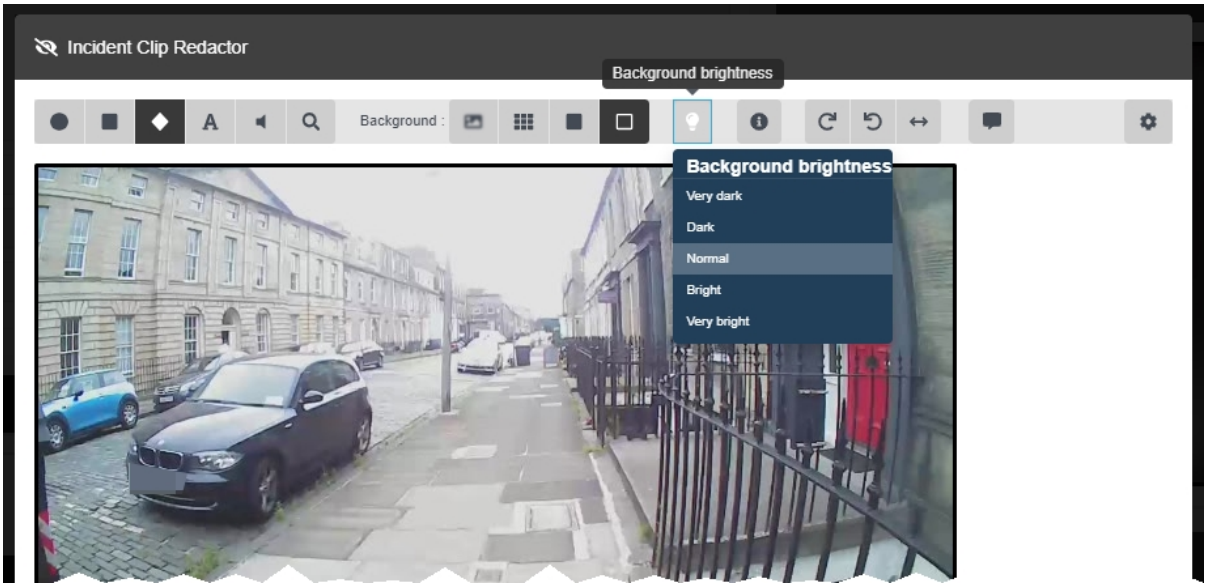
  Users do not need to redraw the annotation, just re-position it.

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

8. Click ***confirm***.
9. Click ***Save incident***.

5.6.5 Create Brightness Redactions

Brightness redactions are used to darken or brighten areas of the video. This can be used to highlight the relevant parts of a piece of evidential footage, and applies to both foreground and background redactions.



Users can create foreground brightness redactions. These highlight a specific area of the video, 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 ***Redact parts of this clip***.
4. Step forwards through the footage 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.

   From here, the user has two options:

- If the subject of the video is moving, step through the video frame-by-frame and reposition the shape 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 video where the redaction should end, click ***End***.

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

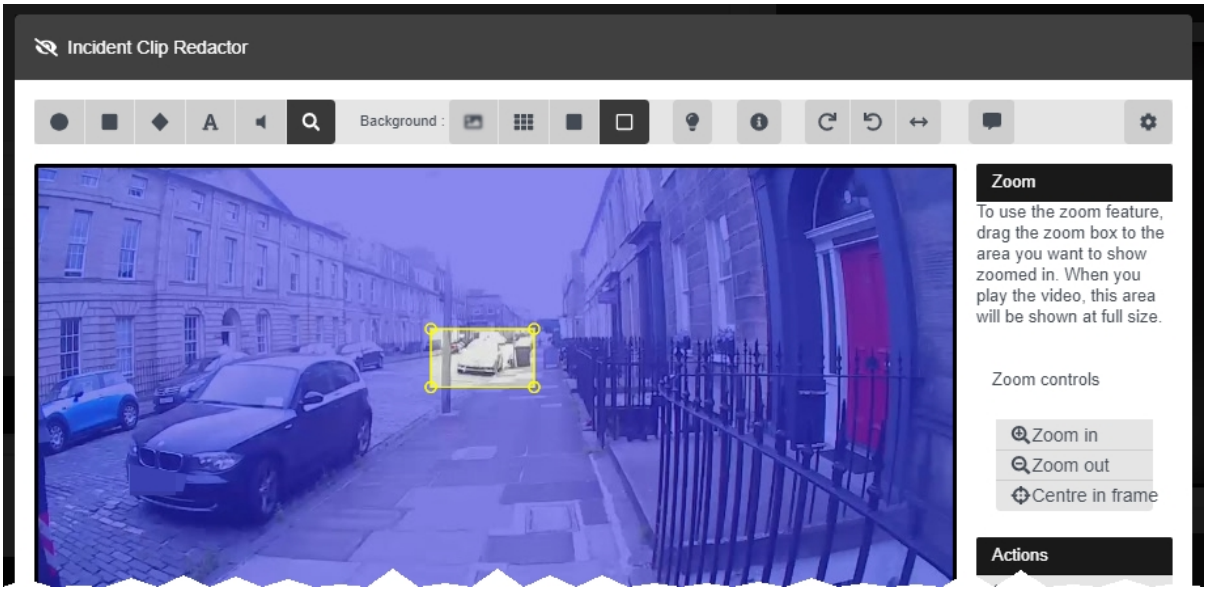
- If the subject of the video is static, skip to the part of the video where the redaction should end, and click ***End***.

Users can create a background brightness redaction effect. This will affect any areas of the video 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 video. The options are **Very Dark**, **Dark**, **Normal**, **Bright**, and **Very Bright**.

5.6.6 Create Zoom Redactions

Zoom redaction effects focus on specific aspects of the video. They can be used to highlight the relevant parts of a piece of evidential footage.



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 video to where the redaction effect should start.
5. Click ***Zoom in on one area***.
6. Draw the square around the area of the video 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 video is played like normal.

From here, the user has two options:

- If the subject of the video is moving, step through the video frame-by-frame and reposition the shape manually to ensure that it is focused on the subject at all time, using ***Step Backward*** / ***Step Forward***. When the user reaches the

part of the video where the redaction should end, click ✕ ***End***.

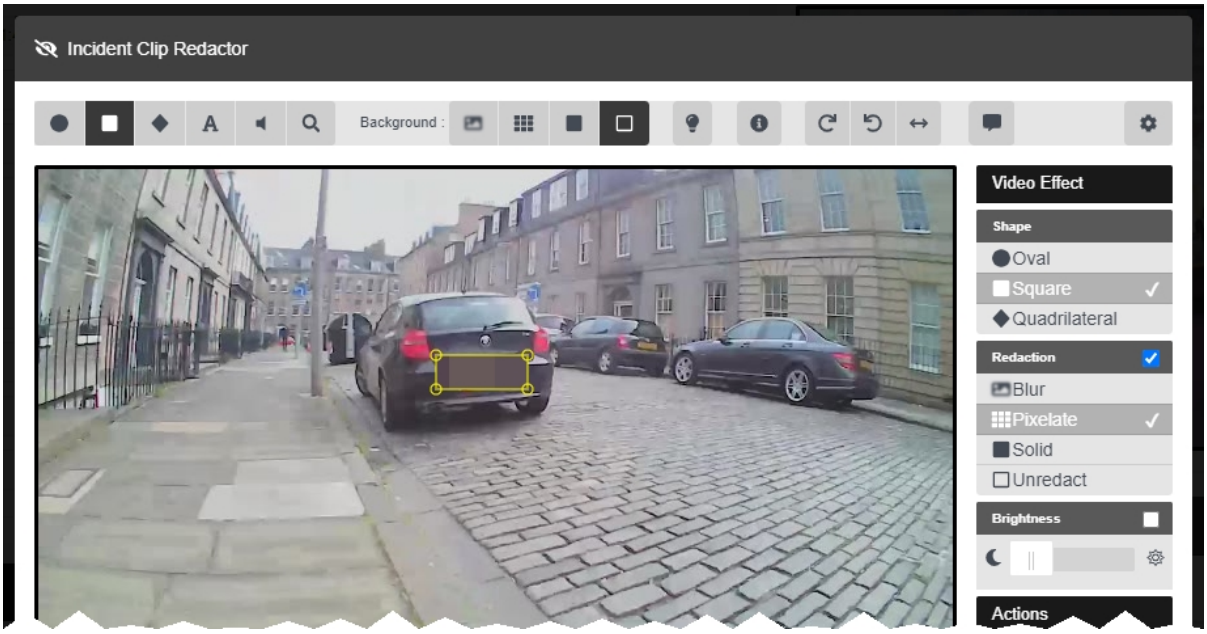
Users do not need to redraw the annotation, just re-position it.

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

8. Click ***confirm***.
9. Click ***Save incident***.

5.6.7 Create Other Redactions

There are some other redaction effects which can be performed on a video.



The other redaction effects can be found in the top menu bar. They are as follows:

- ***Rotate clockwise*** - this rotates the video by 90 degrees left.
- ***Rotate anti-clockwise*** - this rotates the video by 90 degrees right.
- - ***Horizontal flip*** - this flips the video horizontally.
- ***Show metadata*** - this displays the metadata recorded alongside the video.

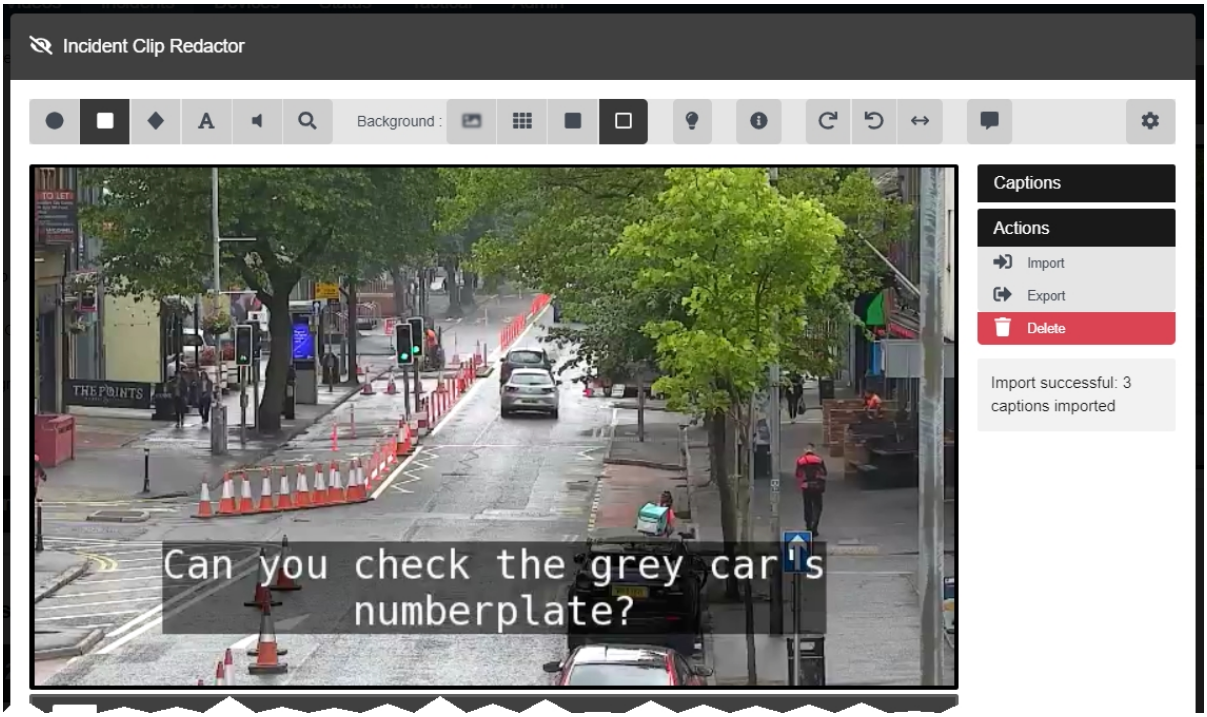
Clicking this icon multiple times changes the position of the overlay text, then hides it entirely.

Administrators can configure the specific metadata information recorded alongside videos.

>> *For more information, see* Configure Video metadata overlay settings on page 210

5.6.8 Add Captions to an Incident Clip

Once a video has been added to an incident, users can import a .vtt file, which will display captions over it.



To import captions 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 ***Captions***.
5. In the ***Actions*** field, click ***Import***.
6. Select the previously-created .vtt file.
   If successful, the right-hand menu will show the number of captions which have been successfully imported.

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

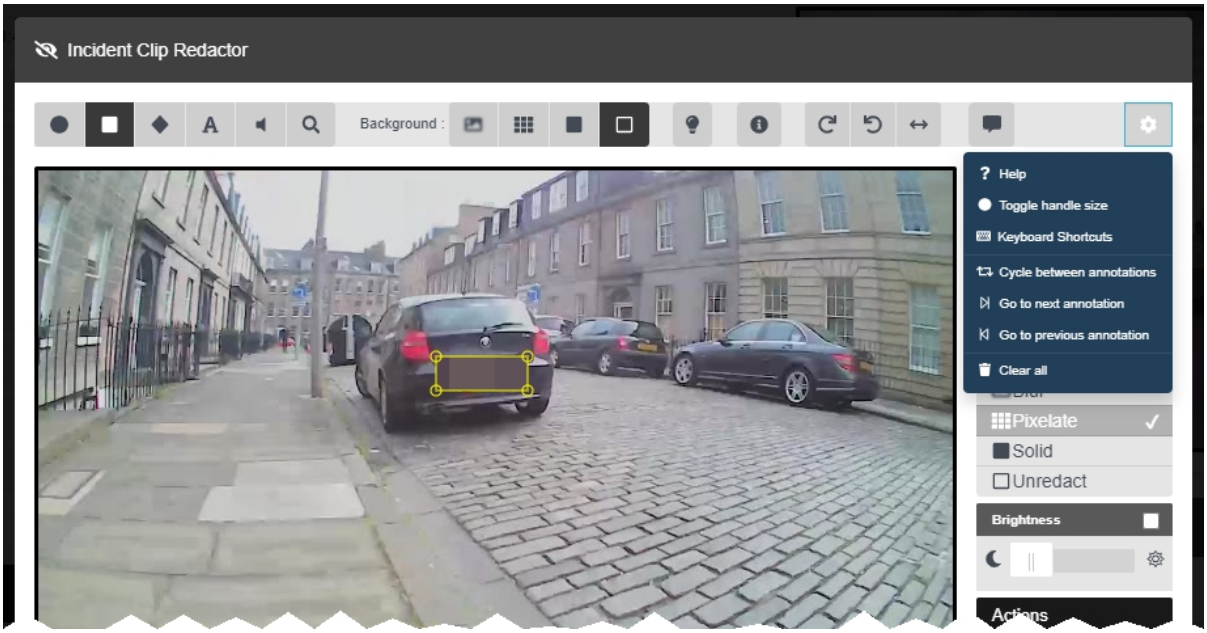
To export a set of captions from an incident clip, click ***Export***. This will download the .vtt file to the PC running VideoManager.

*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 ***Delete***.

5.6.9 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 video more quickly.

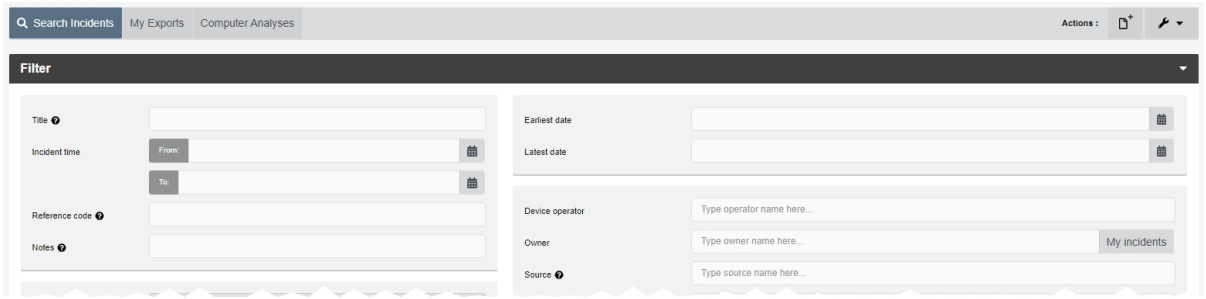
>> For more information, see Appendix D: Keyboard Shortcuts on page 467

- ***Cycle between annotations*** - if a redaction effect is selected, clicking this will cycle through all the redaction effects in the video, 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 video.

5.7 Search Incidents

It is possible to use VideoManager'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:

- **Saved searches**

>> For more information, see Create, Edit and Delete Saved Searches on page 80

- ***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 videos were recorded between set dates.
- ***Device operator*** - search for incidents containing footage 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 videos 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.

This also applies to user-defined incident fields. For example, a drop down field might have two options: *yes* and *no*. If the user enters *yes* into the ***Match text*** field, all incidents whose drop down field has been set to *yes* will be returned.

>> For more information, see Create New User-defined Incident Fields on page 264

- ***Advanced filter*** - users with knowledge of using sequence conditions can input more advanced search queries here.

>> For more information, see Perform Advanced Searches on page 83

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 ***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.
- ***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 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:

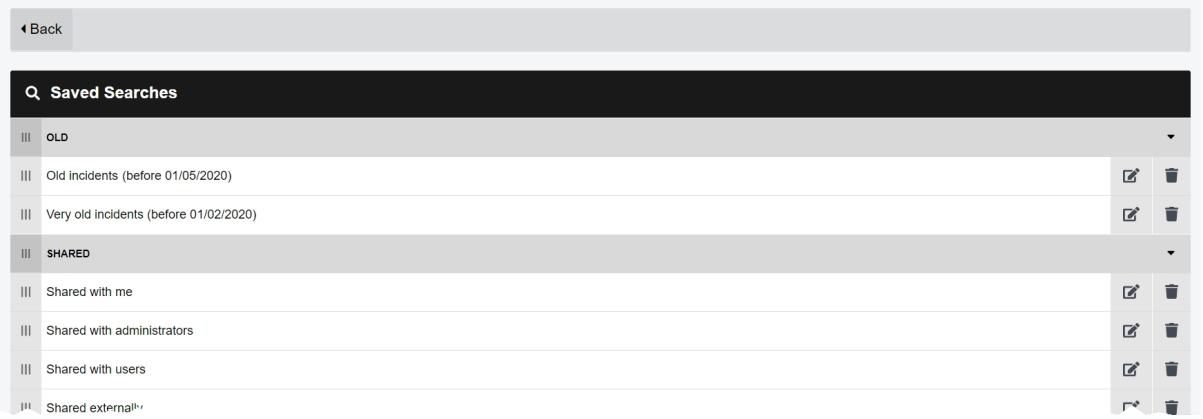
1. Click the ***Filter*** heading. This will re-open the search parameters.
2. Click ***Clear filter*** to clear the search filters.

Users can now enter the updated criteria.

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

5.7.1 Create, Edit and Delete Saved Searches

Sufficiently privileged users can create saved searches for incidents. This allows a query to be saved, searched again, and shared easily. Saved searches are useful if there are certain parameters which users will be searching repeatedly.



Every saved search is potentially shared with every user on the system - for this reason, VideoManager sorts these searches by access group, and only allows users in the corresponding role-assigned access groups to view the saved searches which are relevant to them.

To create a saved search:

1. Navigate to the ***Incidents*** tab.
2. Select the **Search Incidents** pane.
3. Enter the relevant search terms.

>> For more information, see Search Incidents on page 78

4. **Before** searching, click ***Save search***.

The ***Save Incident Search*** window opens.

5. In the ***Search name*** field, enter the name for the saved search.
6. In the **Category** field, enter the name of a previously-existing category **or** enter the name of a new category, which will be created when this saved search is saved.

This makes it easier to sort saved searches in accordance with workflow - e.g. a category dedicated to users who only need to look at incidents that are less than five days old.

7. If the **Permission group** field is left as ***Public***, anyone on VideoManager who has the permission to use saved searches will be able to view this saved search. If changed to an access group, only users whose roles correspond to that access group can view it.

>> For more information, see on page 186

8. Click ***confirm*** to save the search.

Once a saved search has been created, it can be used when searching for incidents. To use a saved search:

1. Navigate to the ***Incidents*** tab.
2. Select the **Search Incidents** pane.
3. From the ***Saved search*** dropdown, select the relevant saved search.

Users can expand saved search categories using + . This will show all saved searches in that category.

Once the user has selected a saved search, it will be searched automatically. If a user wishes to change which saved search they use, or does not want to use a saved search at all, they should click ***Clear filter***.

Users can edit a saved search's properties. This may be necessary if the user wishes to change the saved search's name, or which access groups can see it. To edit a saved search's properties:

1. Navigate to the ***Incidents*** tab.
2. Click ***Search Incidents***.
3. Click ***Advanced*** in the top right-hand corner.
4. Select ***Manage saved searches***.
5. Here, the saved searches are sorted by category, in order of creation.
   Users can only view the saved searches that they have permission to view, as determined by their access groups.
6. Click ***Edit***.
   Users can edit the **Search name**, **Category**, and **Permission group** fields.

Users can edit a saved search's configuration. This may be necessary if the filters applying to the search have changed. To edit a saved search's configuration:

1. Navigate to the ***Incidents*** tab.
2. Click ***Search Incidents***.
3. From the saved search dropdown, select the relevant search from the menu.
   The search will automatically be performed - re-click the ***Filter*** pane to open the saved search pane again.
4. Click ***Edit search***.
5. Make the required changes.
6. Click ***Save search***.
7. The user will be asked whether they want to overwrite the current saved search, or create a new one.

8. Click ***Update existing search***.

The saved search is saved with updated configuration.

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

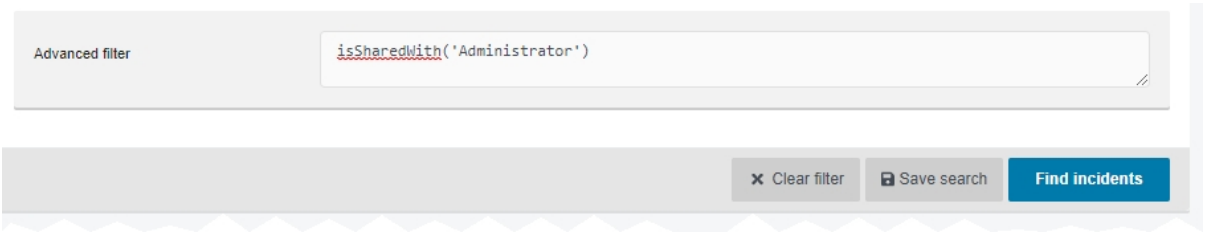
1. Navigate to the ***Incidents*** tab.
2. Click ***Search Incidents***.
3. Click ***Advanced*** in the top right-hand corner.
4. Select ***Manage saved searches***.
5. Next to the relevant saved search, click ***Delete***.
6. Confirm the choice by clicking ***yes***.

A category will be deleted automatically if all the saved searches within it have been deleted.

5.7.2 Perform Advanced Searches

An advanced search allows users to perform complex incident searches which cannot otherwise be expressed with the simple filter controls. The search can be based on user-defined incident fields and built-in fields (e.g. ***Creation Time*** and ***Owner***). This is done from the ***Incidents*** tab, in the ***Advanced Search*** box.

This field will only be viewable if users have the ***Search using advanced filter*** permission enabled.



Advanced searches are complex and should only be performed by administrators.

>> For more information, see Appendix E: Custom Predicate Language on page 469

5.8 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.

It is also useful if the user has enabled their VideoManager to act as a Central VideoManager. In this case, every incident held in connected sites can be automatically fetched in bulk. This means that they will become editable in the Central VideoManager and unviewable in the original sites.

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 78

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 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 videos for bulk editing, the following options are available:

- ***Take control*** - if a user's instance of VideoManager is acting as a Central VideoManager, this action will take control of **all** selected incidents from the connected sites.
- ***Submit*** - if a user's instance of VideoManager is acting as a site, this action will submit **all** selected incidents to the connected Central VideoManager.

>> For more information, see Commit Incidents on page 98

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

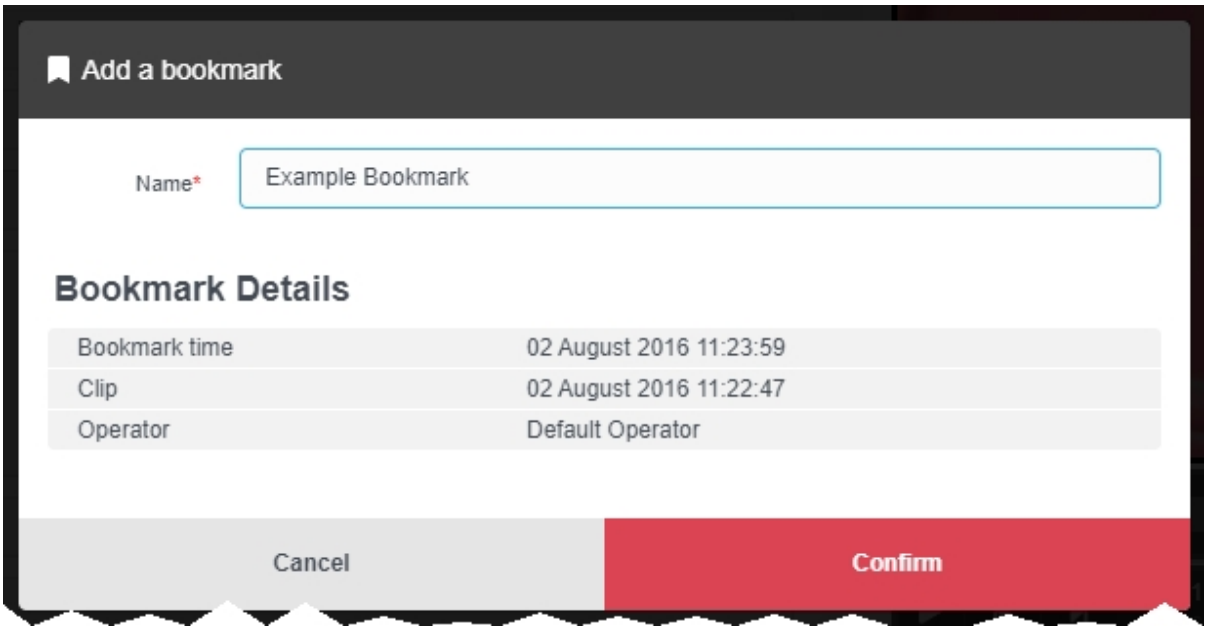
>> For more information, see Create, Edit and Delete Incident Collections on page 100

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

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

5.9 Create, Edit and Delete Bookmarks

Bookmarks can be used to mark a specific time in a video. 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 video for review purposes. Although VB400s can be configured to create a bookmark while in the field, users can also manually create bookmarks after the video has been uploaded to VideoManager and added to an incident.



To add a bookmark to a video:

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

>> For more information, see Create Incidents Manually and Perform Incident Actions on page 49

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 video pane, click ***Play***.
6. Drag the progress bar of the video to the position where the bookmark will be placed. The video 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 video. Users can overwrite this with their own text.

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

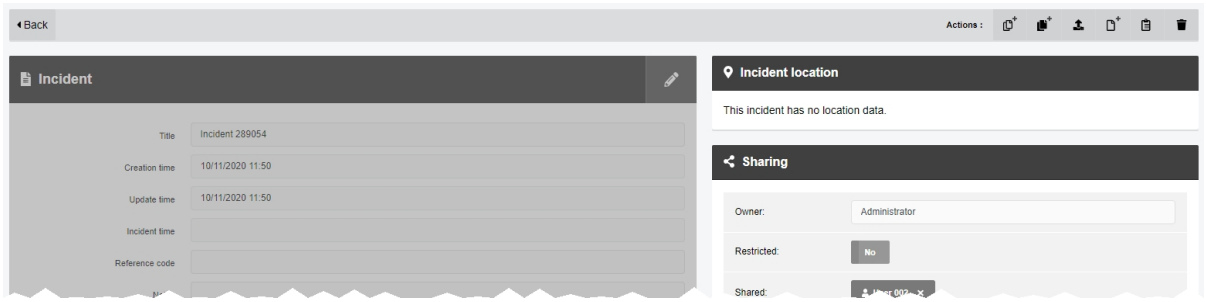
4. Click ***Bookmarks***.
5. Next to the bookmark to be deleted, select ***Delete***.

The bookmark will be deleted.

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

5.10 Share Incidents

There are many ways to share incidents - users can share them internally (with other people on the VideoManager system), or externally (with people who aren't on the VideoManager system) using a link or an export.



All manners of sharing take place in the ***Incidents*** tab.

- Share incidents internally, with other users on VideoManager.

>> For more information, see Share Incidents Internally on page 90

- Share incidents externally using a link.

This method should be used if people outside VideoManager should have **temporary** access to an incident.

>> For more information, see Share Incidents Externally Using a Link on page 91

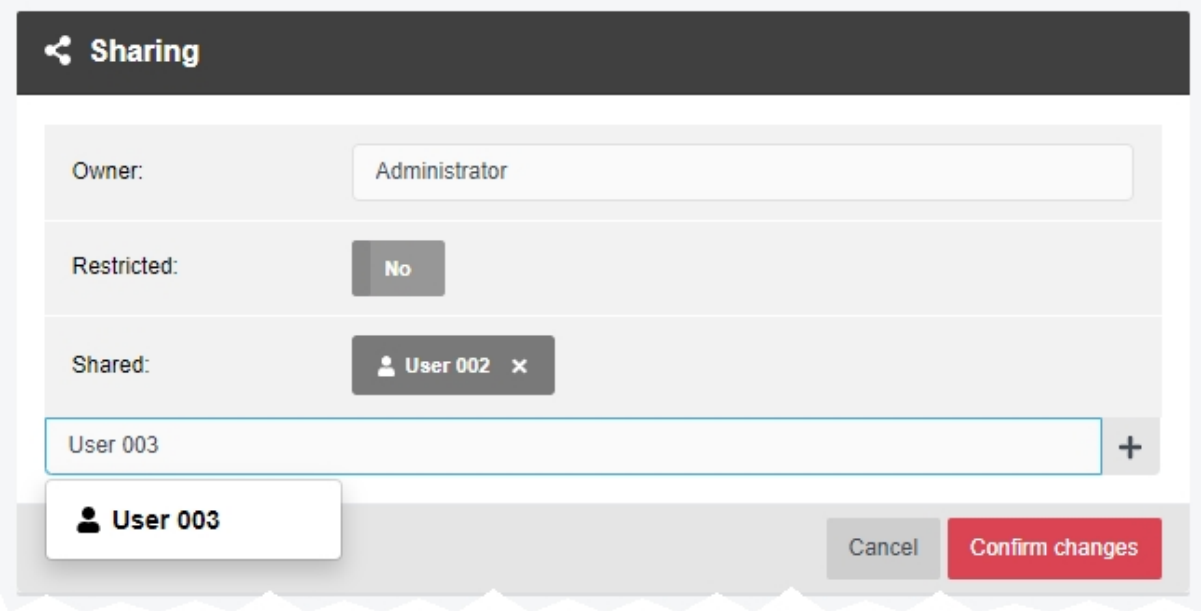
- Share incidents externally using an export.

This method should be used if people outside VideoManager should have **permanent** control over an incident.

>> For more information, see Share Incidents Externally Using an Export on page 93

5.10.1 Share Incidents Internally

It is possible to share incidents with other users on VideoManager. This allows less privileged users to share incidents with each other, without giving them the ability to view all incidents on the system.

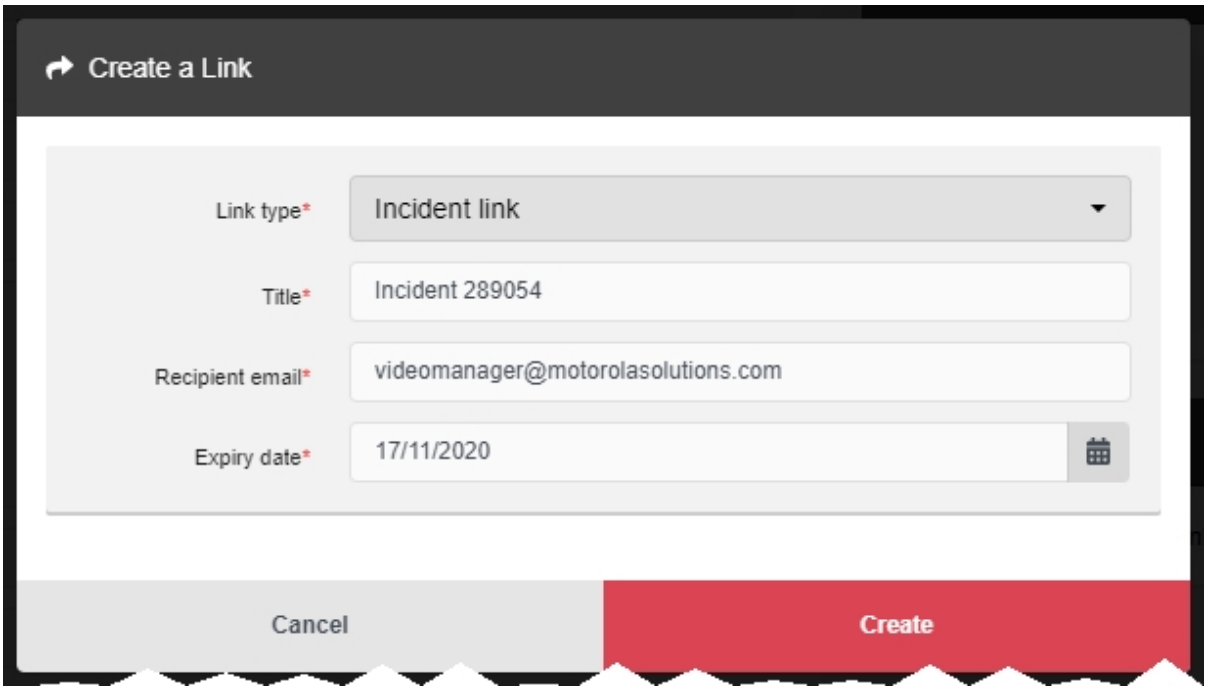


To share an incident internally:

1. Navigate to the ***Incidents*** tab.
2. Find the relevant incident, and click > ***View 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 sharing settings***.
4. Here, administrators can change the owner of the incident.
   This can be a user or an entire group. If the owner of the incident is a group, **all** users in that group will be able to access and edit the incident.
5. If ***Restricted:*** is set to ***Yes***, only users with the ***View any restricted incident*** permission will be able to view the incident when they search for it.
6. In the ***Shared:*** field of the ***Sharing*** panel, enter the name of a user to share the incident with. It is only possible to share incidents with users on VideoManager.
7. Click + to add the user to the list.
8. Click ***Confirm changes***.
   Users can now find the incident using the ***Only show shared incidents*** filter from the ***Incidents*** tab.

5.10.2 Share Incidents Externally Using a Link

Users can share incidents with people who aren't on the VideoManager system, using links. These links allow people outside the system to view an incident without compromising VideoManager's security. There are two types of link: **Incident links** and **Custom links**.



Before administrators create a link, they can optionally configure sharing defaults for incidents from the ***Admin*** tab.

>> For more information, see Configure Sharing Policy on page 304

To share an incident externally using a link:

1. Navigate to the ***Incidents*** tab.
2. Find the relevant incident, and click > ***View 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 + ***Create a link*** in the ***Links*** pane.
4. From the ***Link type*** dropdown, select the type of link to be created. The options are as follows:
   - An **Incident link** can be given to anyone who does not have a VideoManager account. This will expire after a user-selected period, by default a week.

- A **Custom link** is the same as an **Incident link**, but users are given the option to add a description of the incident as well, which is viewable by people who have been given the link. It also expires.

5. In the ***Title*** field, enter the title for the link.
6. If an **Incident link** has been selected, in the ***Recipient email*** field, enter the email address of the recipient.
7. In the ***Expiry date*** field, enter the expiry date for the link.

After this date, the link will expire and the incident will become inaccessible.

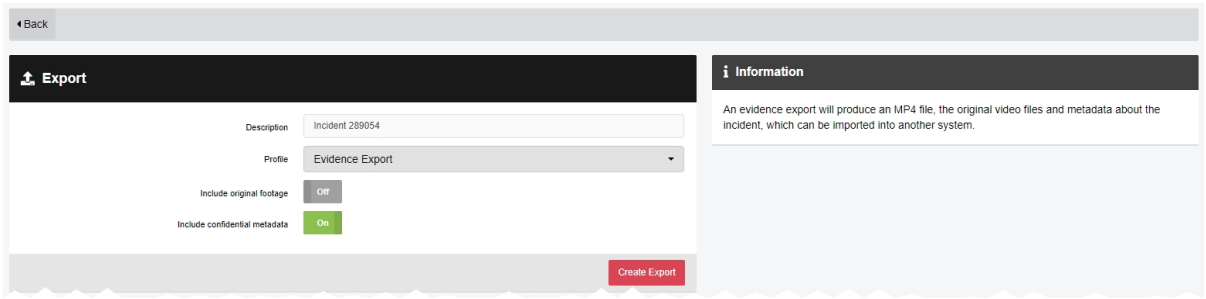
8. Click ***Create***.

Once created, the link can be seen in the ***Links*** panel. Users can perform a variety of actions:

- ***Send in email message*** - if clicked, this will send an email message containing the incident link to the recipient. This is only possible for **Incident links**.
- ***Show link to copy*** - this shows the link to the incident, which can be copied. This is the only way that a **Custom link** can be shared.
- ***Update this link*** - this allows the user to edit the link.
- ***Delete link*** - this deletes the link. This will immediately invalidate the link, and the incident will not be viewable through this link anymore.

5.10.3 Share Incidents Externally Using an Export

After an incident has been created, it may need to be shared with another person for review or as evidence. Unlike incident links, an export is downloaded straight to the worker's PC, and gives the recipient more permanent control over the footage. Users can also send the export to a person outside of VideoManager using an export link.



Users can export incidents in common video formats. The following export profiles are provided by default:

- **MP4** - creates a standard MP4 encoded video. This format of video is useful if users use a file-sharing system or they want other users to be able to see the video across a range of platforms - for example, smart phones or PCs.
- **DVD** - creates an ISO file in PAL or NTSC format and compatible with a range of media types. After burning the ISO file onto a DVD, the user has a secure, offline, copy of the video footage that can not be accessed unless a person has the physical media.
- **Evidence Export** - creates an MP4 of the incident and includes the source footage and all related metadata. This is useful if the original incident needs to be expanded or more information is required about the footage and its origins.

Administrators can also create their own export profiles from the ***Admin*** tab. This dictates what information will be included in a user's exports.

>> For more information, see Configure Incident Exports on page 244

To create an export:

1. Navigate to the ***Incidents*** tab.
2. Find the relevant incident, and click ***Export 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. From the ***Profile*** dropdown, select either **MP4**, **DVD**, or **Evidence Export**.
4. The following step differs, depending on the kind of export profile which has been selected.

If **DVD** has been selected:

- Select the ***Format*** to use for the ISO file.
  - **PAL** - common in Europe and parts of Asia. Delivers a frame rate of 25 fps with 625 lines
  - **NTSC** - common in the U.S. and Canada. Delivers a frame rate of 30 fps with 525 lines.
- Select the ***Output Media*** that the ISO file is going to be burned to.

Choose an output media type that best fits the exported video. For example, use DL (double-layer) discs for large ISO files (4.0 GB or more).

If **Evidence Export** has been selected:

- If ***Include original footage*** is set to ***On***, the full-length videos will be included alongside the incident and incident clips.
- If ***Include confidential metadata*** is set to ***On***, the incident's metadata will be included alongside the incident.

5. If configured in the export profile, users can now manually select which incident clips will be included in the export.

*If the incident only has one incident clip, this clip **must** be selected before the incident can be exported. If multiple incident clips are selected, then the export will include them as a single continuous video with a title and video identification information added to the start of each incident clip.*

6. Click ***Create Export***, then click ***yes*** to confirm.

While the export is being created, users can view the progress of the export from the ***Status*** tab. Once the export has finished processing, users can share it externally in one of two ways: either by **downloading** the export straight to the PC running VideoManager, or by creating an **export link** to share with other workers who do not have access to VideoManager.

To download an export:

1. Navigate to the ***Incidents*** tab.
2. Next to the relevant export, click ***Download Export*** .

   If VideoManager has been configured to encrypt export .zip folders, the user must set a passphrase in the ***Passphrase*** field. Make a note of this passphrase - it must be used later when the user extracts the .zip.
3. The .zip folder will be downloaded to the PC running VideoManager.

   If VideoManager has been configured to encrypt exported .zip folders, the user must download software which can extract encrypted .zips. They will be prompted to enter the previously-set passphrase when they attempt to extract the .zip folder.

To create an export link:

1. Navigate to the ***Incidents*** tab.
2. Select the ***Exports*** pane.
3. Click > ***View Export*** next to the export which will be shared.
4. In the ***Links*** panel, click + ***Create a link***.
5. In the ***Title*** field, enter a title for the export link.
6. In the ***Recipient email*** field, enter the email to which this export link will be sent.

Users can only enter one email address.

7. In the ***Expiry date*** field, select when the export link will expire.

The recipient of the export link must download the export by this time, or the link will stop working. However, once the recpient has downloaded the export, they will have permanent access to it - even once the export link has expired.

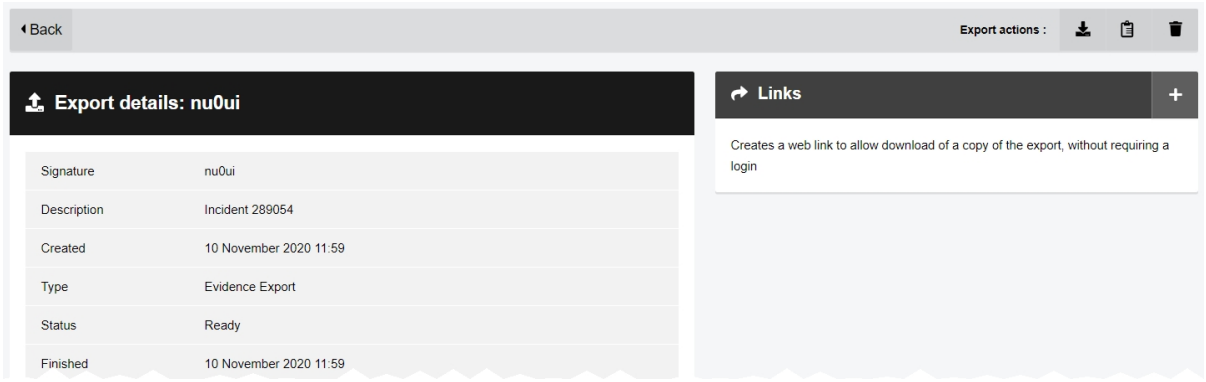
8. Click ***Create***.

The export is ready to be shared.

9. Either click ***Send in email message*** to open a template email message with the link, or click ***Show link to copy*** to display the standalone link which can be manually copied.

5.10.4 View Exports

Once an export has been created, users with the relevant permissions can view it from the ***Incidents*** tab.



To view a previously-created export:

1. Navigate to the ***Incidents*** tab.
2. Select the ***My Exports*** or ***Supervised Exports*** pane, depending on how the user's permissions have been configured.
3. Next to the relevant export, click ➢ ***View Export***.

Users will be able to view the following information about an export:

- ***Signature*** - the unique string of letters generated by VideoManager to identify the export.
- ***Description*** - the title of the export. By default, this is the name of the incident within the export.
- ***Created*** - when VideoManager started to create the export.
- ***Type*** - the type of export. This could be ***MP4***, ***DVD***, or ***Evidence Export***.
- ***Status*** - whether the export is ready to be downloaded, or is still being created.
- ***Finished*** - when VideoManager finished creating the export.

  This field will only be visible if the export has been fully completed.

Here, users can perform the following actions:

- ***Download Export*** - this downloads the export to the user's PC.

Caution *Once an export has been downloaded to a PC, VideoManager has **no control** over it.*

- ***View Export audit log*** - this downloads the export's audit log to the user's PC.
- ***Delete Export*** - this deletes the export from VideoManager.

This will **not** delete the original incident.

Even once an export has been deleted from VideoManager, anyone who has already downloaded it will still have access to the incident within it.

5.11 Commit Incidents

If a user has configured VideoManager to act as a Central VideoManager for various sites, they can move incidents from a site to the Central VideoManager from the ***Incidents*** tab. Although incidents are immediately **viewable** on a Central VideoManager when they are created in a site, they cannot be **edited** unless they are manually moved.

>> For more information, see Configure Sites on page 374

There are two ways to commit an incident.

The first way is submitting it from the site itself:

1. Navigate to the site's ***Incidents*** tab.
2. Find the relevant incident, and click ***Submit*** 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. The incident will immediately be moved to the Central VideoManager.
4. Refresh the site and the incident will be shown as ***Deleted***. It can no longer be edited from this instance of VideoManager.

*Once it has been committed, an incident's audit log in the original site will end immediately, and any changes made to the incident in the Central VideoManager will **not** be replicated in the site.*

The second way to commit an incident is by taking control of it from the Central VideoManager:

1. Navigate to the Central VideoManager's ***Incidents*** tab.
2. Find the relevant incident, and click ***Take control of 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. The incident will immediately be transferred to this instance of VideoManager.
4. Refresh VideoManager and the incident will appear in the ***Incidents*** tab. It can now be edited.

*If using bulk edit, the **Fetch** function is synonymous with taking control of an incident.*

Although submitting and taking control have the same effect on an incident, the actions will look different in an audit log.

Depending on how auto-fetch settings have been configured, videos in the incident may also be transferred to the Central VideoManager as well.

>> For more information, see Configure Metadata/Footage Replication on page 377

Incidents are colour-coded depending on their state.

In the Central VideoManager:

- Incidents which have been automatically made viewable to the Central VideoManager, but haven't been taken control of yet, are coloured **blue**.
- Incidents which have been deleted on the site before they were taken control of are coloured **blue** with **red** text.

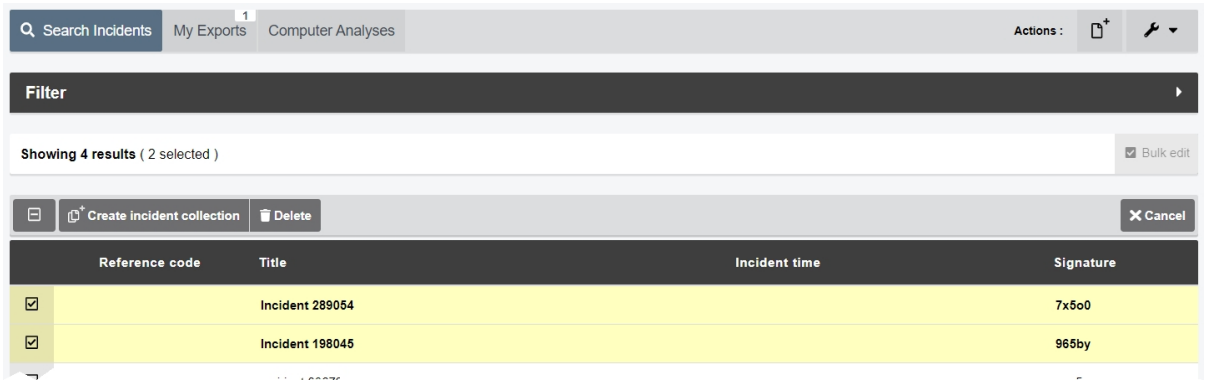
If an incident has been deleted on the site, the Central VideoManager cannot take control of it.

In the site:

- Incidents which have been submitted to the Central VideoManager are coloured **green**.
- Incidents which have been deleted on the site itself are coloured **red**.

5.12 Create, Edit and Delete Incident Collections

Nested Incidents is a licensed feature that allows users to create incident collections. This is useful if multiple members of an organisation have all recorded the same event on different body-worn cameras - an incident collection collates these individual incidents and presents them together for convenience and ease of review.



There are two ways to create an incident collection.

The first way to create an incident collection is useful if the user already knows which incidents they want to include in the incident collection. To do so:

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 78

4. Click ***Bulk edit***.
5. Select the incidents which will be part of the incident collection.
6. Click ***Create incident collection***.

The ***New Incident*** window opens.

7. Create the incident collection like a normal incident.

>> For more information, see Create Incidents Manually and Perform Incident Actions on page 49

8. Click ***Create incident*** to save the changes.

The second way to create an incident collection is useful if the user wants to create a collection around one incident in particular, leaving the option open to add more incidents later. To do so:

1. Navigate to the ***Incidents*** tab.
2. Find the relevant incident, and click ***View 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 ***Create A new incident collection***.

The ***New Incident*** window opens.

4. Create the incident collection like a normal incident.

>> For more information, see Create Incidents Manually and Perform Incident Actions on page 49

5. Click ***Create incident*** to save the changes.

Once an incident collection has been created, other incidents can be added to it. To do so:

1. Navigate to the ***Incidents*** tab.
2. Find the incident which will be added to an incident collection, and click ***View incident*** next to it.
3. Click ***Add To existing incident collection***.
4. The user will be presented with all incidents **and** incident collections.

If the user adds an incident to another incident, the latter will automatically become an incident collection.

It is only possible to have two levels in an incident collection: the incident collection itself, and any incidents it contains. This means that if the user adds an incident collection (C1) to another incident collection (C2), all incidents within C1 will be presented as children of C2, along with C1.

5. Click ***Add To existing incident collection*** next to the relevant incident or incident collection.
6. Click ***Create incident*** to save.

Once created, incident collections can be edited, duplicated, and deleted like normal incidents. It is important to note that an incident collection is like a "snapshot" of multiple incidents - an incident in an incident collection is not automatically updated when it is edited. If a user wants to update an incident, they must re-add it to the incident collection.

6 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.

>> For more information, see Connect Body-Worn Cameras to VideoManager on page 104

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

>> For more information, see Assign Body-Worn Cameras and Record Footage on page 110

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

>> For more information, see Search Body-Worn Cameras on page 122

- Pre-assign a body-worn camera. This is necessary if a remote worker is receiving their body-worn camera at home but cannot access the VideoManager system themselves.

>> For more information, see Pre-Assign a Body-Worn Camera on page 126

- 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 128

- 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 130

- Bulk edit body-worn cameras.

>> For more information, see Bulk Edit Body-Worn Cameras on page 133

- Perform DockController actions. These actions include upgrading firmware, and removing a DockController from VideoManager.

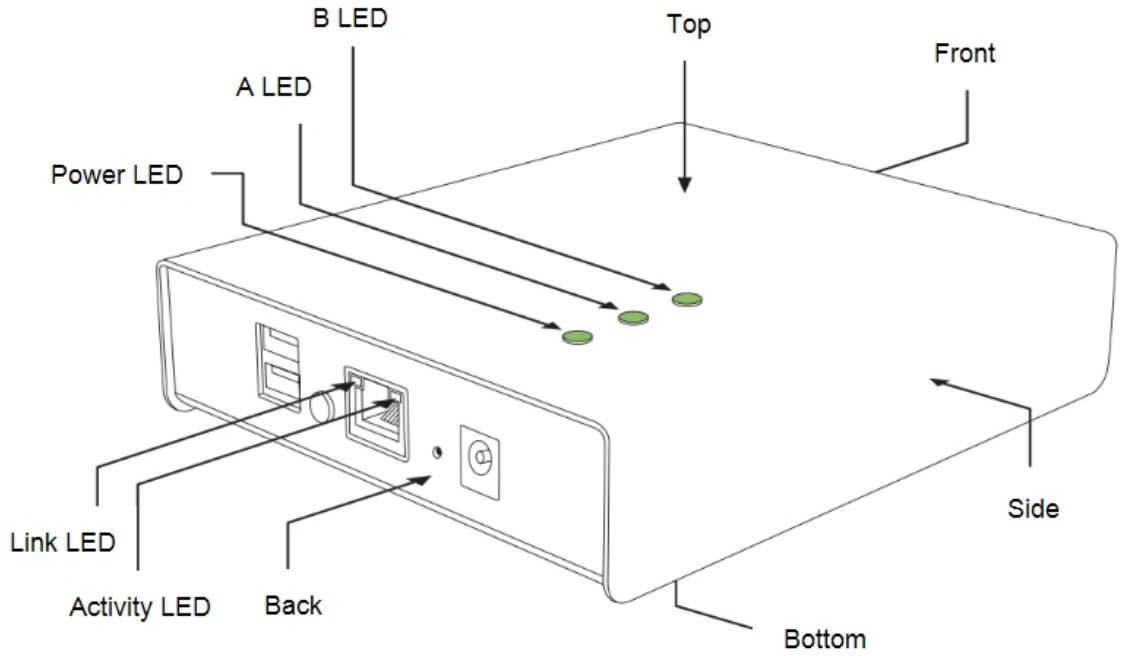
>> For more information, see Perform DockController Actions on page 135

- Bulk edit DockControllers.

>> For more information, see Bulk Edit DockControllers on page 137

6.1 Connect Body-Worn Cameras to VideoManager

DockControllers are the mechanism through which body-worn camera docking stations can be connected to VideoManager. Up to six DOCK7/DOCK14s can be connected to one DC-200.



Administrators must first configure their DockController.

>> For more information, see Configure and Connect a DockController to VideoManager on page 105

Once the DockControllers have been configured, the body-worn cameras should be connected to them. Through this, the body-worn cameras will be connected to VideoManager automatically.

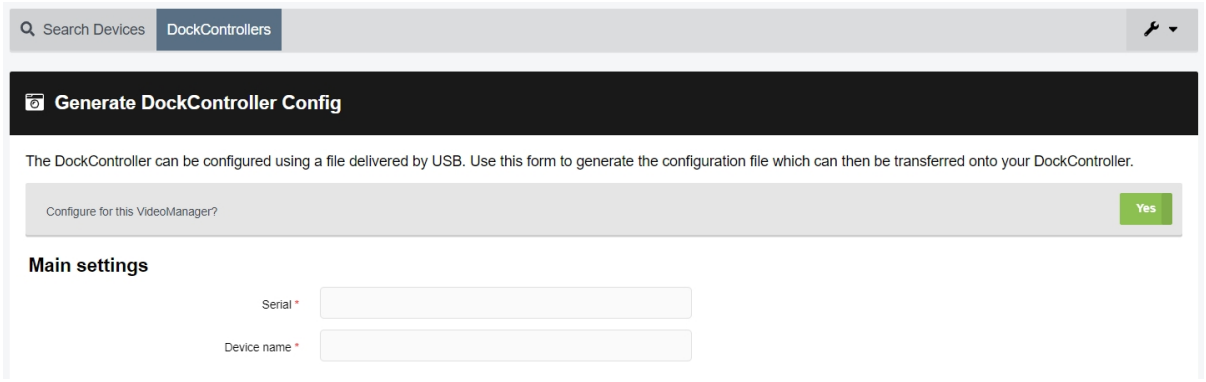
>> For more information, see Connect Docks and Body-Worn Cameras to DockControllers on page 107

Alternatively, if the administrator has a suite of VT-series cameras but does not have physical access to VideoManager, they can connect those body-worn cameras to VideoManager over WiFi, using a QR code.

>> For more information, see Connect VT-Series Cameras to VideoManager Remotely on page 108

6.1.1 Configure and Connect a DockController to VideoManager

An administrator must configure their DockController before any body-worn cameras can be connected to VideoManager.



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.
5. On VideoManager, 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.
11. The ***Host*** field should be pre-populated with VideoManager's webserver.
12. If ***SSL*** is set to ***On***, all footage passed through this DockController will have an extra layer of encryption.
13. If ***Use static IP*** is set to ***On***, the user must enter an IP address for the DockController.
14. From the ***Security*** dropdown, select what kind of whether the DockController will be protected with **802.1x (WPA2-PEAP-MSCHAPV2)** or not.
15. Click ***Generate***.

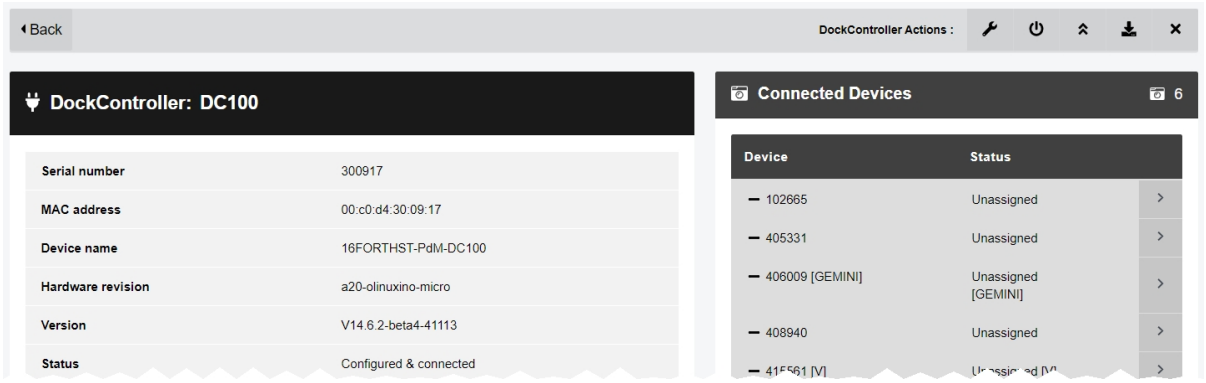
The file will be saved to the PC's default downloads location.

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.

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

6.1.2 Connect Docks and Body-Worn Cameras to DockControllers

Once a user's DockControllers have been configured, a user's docks must be connected to them. This is how body-worn cameras will communicate with VideoManager.



To connect docks to DockControllers:

1. Plug one end of the dock's USB 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 as many docks as necessary.

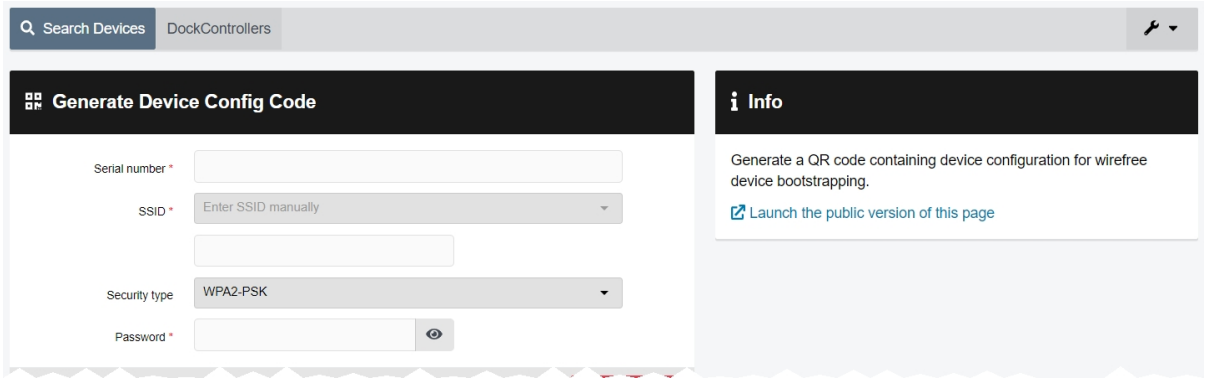
The user can now dock their body-worn cameras into their powered-on dock. This will connect the body-worn cameras to VideoManager.

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

1. On VideoManager, 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.).

6.1.3 Connect VT-Series Cameras to VideoManager Remotely

It is possible to configure a VT-series cameras using a QR code. This is important if a user cannot configure their VT-series cameras using the VideoManager UI. There are two reasons for this: if an administrator does not have physical access to VideoManager (e.g. because it is a cloud service), or if the operator does not have access to VideoManager 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 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 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 profile which will be used by the VT-series camera to connect to VideoManager. 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 is operating on.

   - Select a previously-created WiFi profile.

   >> For more information, see Create WiFi Profiles and Perform WiFi Profile Actions on page 221

6. Click ***Generate code***.
7. The VT-series camera can now be connected to VideoManager by following the instructions onscreen.

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

>> For more information, see Assign Body-Worn Cameras and Record Footage on page 110

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

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 ***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. 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 is operating on.

     - Select a previously-created WiFi profile.

     >> For more information, see Create WiFi Profiles and Perform WiFi Profile Actions on page 221
   - Click ***Generate code***.
   - The VT-series camera can now be connected to VideoManager by following the instructions onscreen.

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

   >> For more information, see Assign Body-Worn Cameras and Record Footage on page 110

6.2 Assign Body-Worn Cameras and Record Footage

Before a body-worn camera can be used to record or stream footage, it must be assigned to an already-created user. This ensures that all footage 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 footage.

There are some optional steps that administrators can complete before assigning a body-worn camera to operators. They are as follows:

- Create a device profile.

This will dictate how the body-worn camera behaves in the field, including how the body-worn camera's LEDs behave when recording, the frame rate and resolution of the video recorded on a body-worn camera, and whether the body-worn camera will pre-record.

>> For more information, see Create, Edit, Reorder and Delete Device Profiles on page 204

- Enable video metadata overlay settings.

If metadata overlay settings have been enabled in the device profiles, administrators can configure the specific information which will be displayed over all videos recorded on body-worn cameras.

>> For more information, see Configure Video metadata overlay settings on page 210

- Configure global device settings.

These dictate how **all** body-worn cameras connected to VideoManager will behave in the field, including the default assignment mode, and how many videos can be downloaded from body-worn cameras simultaneously.

>> For more information, see Configure Device Settings on page 207

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 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 on page 112

- **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.

>> For more information, see Assign Body-Worn Cameras with Single Issue and RFID on page 114

- **Permanent issue** - the body-worn camera will be assigned to the user through the VideoManager 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 116

- **Permanent allocation** - the body-worn camera will be allocated to the user through the VideoManager 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.

>> For more information, see Assign Body-Worn Cameras with Permanent Allocation on page 118

- **Bulk touch assign** - the user taps their RFID card against an RFID reader. This assigns **all** body-worn cameras connected to an instance of VideoManager to that user. Bulk touch assign enables multiple people to start operating body-worn cameras quickly, because users do not need to assign the body-worn cameras first. However, because the footage recorded through bulk touch assign cannot be traced to specific users, it should only be used in an emergency.

>> For more information, see Bulk Touch Assign on page 120

6.2.1 Assign Body-Worn Cameras with Single Issue on VideoManager

If a body-worn camera is assigned with **Single issue** on VideoManager, 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.

Administrators can optionally enable ***Enable shift-long field trips*** from the ***Admin*** tab. This is useful if users will be undocking and redocking their body-worn cameras multiple times in a shift - it ensures that VideoManager will automatically assign the same body-worn camera to them.

>> For more information, see Configure Device Settings on page 207

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***.

>> For more information, see Search Body-Worn Cameras on page 122

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

*This body-worn camera must be connected to VideoManager 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.

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.

>> For more information, see Create, Edit, Copy, Import, Export and Delete Roles on page 182

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.

>> For more information, see Create, Edit, Reorder and Delete Device Profiles on page 204

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 footage over WiFi, or connecting to VB Companion.

>> For more information, see Create WiFi Profiles and Perform WiFi Profile Actions on page 221

9. Click ***Assign Device***.

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

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

6.2.2 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 UI in order to use this feature - however, there is some configuration required beforehand.

Administrators can optionally enable ***Enable shift-long field trips*** from the ***Admin*** tab. This is useful if users will be undocking and redocking their body-worn cameras multiple times in a shift - it ensures that VideoManager will automatically assign the same body-worn camera to them.

>> For more information, see Configure Device Settings on page 207

Users must ensure that they have an RFID reader connected to the DockController associated with their instance of VideoManager, 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. 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'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 footage like normal.

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

6.2.3 Assign Body-Worn Cameras with Permanent Issue

If a body-worn camera is assigned with **Permanent issue** on VideoManager, 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 ***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 122

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

*This body-worn camera must be connected to VideoManager 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.

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.

>> For more information, see Create, Edit, Copy, Import, Export and Delete Roles on page 182

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.

>> For more information, see Create, Edit, Reorder and Delete Device Profiles on page 204

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 footage over WiFi, or connecting to VB Companion.

>> For more information, see Create WiFi Profiles and Perform WiFi Profile Actions on page 221

9. Click ***Assign Device***.

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

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

6.2.4 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, 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. 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'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***.

>> For more information, see Search Body-Worn Cameras on page 122

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

*This body-worn camera must be connected to VideoManager 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.

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.

>> For more information, see Create, Edit, Copy, Import, Export and Delete Roles on page 182

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 footage like normal.

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

6.2.5 Bulk Touch Assign

It is possible to assign **all** docked, unassigned, unallocated body-worn cameras to one user using bulk touch assign. This is intended to be used in situations where it is necessary to deploy a large number of body-worn cameras quickly, and where there is no requirement for the body-worn cameras to be traceable to specific users.

*This permission should only be used in exceptional circumstances and should **not** be assigned to regular users.*

In order to use this feature, users must create a role which is specifically designed for bulk touch assign. To do so:

1. Navigate to the the ***Admin*** tab.
2. Select the ***People*** pane.
3. Click the ***Roles*** section.
4. Click ***Create role***.
5. Scroll down to the ***Device permissions*** pane. The role should be granted the ***Assign device*** and ***Assign all available devices using RFID touch assign*** permissions.
6. Click ***Save role*** to save changes.

A user should be created specifically for bulk touch assign, and this user should be associated with an RFID card. 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 a beep.
2. Navigate to the ***Admin*** tab.
3. Select the ***People*** pane.
4. Click the ***Users*** section.
5. Click ***Create user***.
6. In the ***Touch Assign ID*** field, click .
   The user will be taken to VideoManager'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. In the ***Roles*** panel, set the previously-created role to ***On***.
9. Click ***Save user***.
   From now on, the RFID card will be associated with bulk touch assign and the relevant user.

It is possible to configure which body-worn cameras will be included in bulk touch assign on the basis of their charge levels. This is done from the ***Device Settings*** section of the ***Devices*** pane, in the ***Admin*** tab.

>> For more information, see Configure Device Settings on page 207

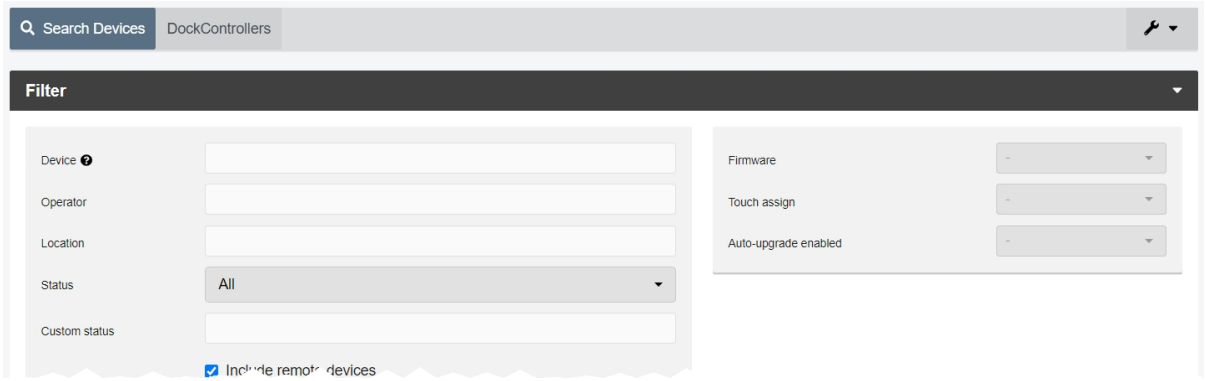
To use bulk touch assign, the user with the previously-created role must touch their RFID card to the reader. By doing so, **all** unassigned body-worn cameras connected to VideoManager will be immediately assigned to that user, and can be used to record footage.

The body-worn cameras remain assigned to that user for 30 seconds. Any body-worn cameras which have not been undocked after 30 seconds will be unassigned again.

When body-worn cameras have been assigned using bulk touch assign, all footage recorded on those body-worn cameras are associated with that single bulk touch assign user. When creating incidents using footage from bulk touch assigned body-worn cameras, VideoManager gives the option to set ***Add other footage from same operator?*** to ***On***. This will add all footage associated with the touch assign user to the incident.

6.3 Search Body-Worn Cameras

If they have the appropriate permissions, users can utilise VideoManager'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 footage 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. 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 footage.
- **Stream available** - this will return all body-worn cameras which are connected to a WiFi network and streaming successfully to VideoManager.
- **Downloading** - this will return all body-worn cameras which are docked and currently downloading recorded footage to VideoManager.
- **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 footage).
- **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 footage to VideoManager and therefore cannot be used), **Unavailable** (the instance of VideoManager 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 footage (either because VideoManager 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***.

>> For more information, see Edit Body-Worn Camera Properties on page 128

- 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.

>> For more information, see Import, Edit and Delete Device Images on page 334

- **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.

>> For more information, see Configure Firmware Settings on page 332

If VideoManager has been configured as a Central VideoManager, users will also have the option to include remote body-worn cameras in their search by checking ☑ **Include remote devices**. This will show the body-worn cameras associated with the Central VideoManager's connected sites as well.

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.

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

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

- ☰ Change viewing options.

>> For more information, see Change Viewing Options on page 22

- ❚❚ ***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 133

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

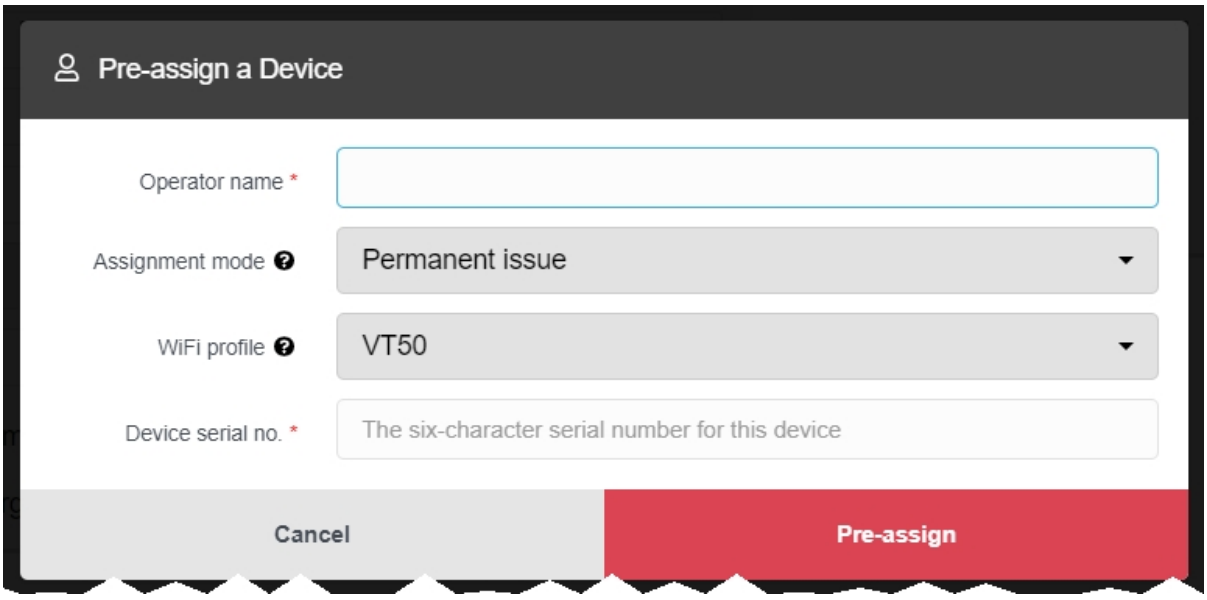
- No icon - the body-worn camera is not connected to VideoManager.

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. Service may be required - check the audit log from the ***Status*** tab.

6.4 Pre-Assign a Body-Worn Camera

It is possible to pre-assign a body-worn camera to a user before it has been docked. Once the pre-assigned body-worn camera has been docked, it will be immediately ready to record. This useful if a remote worker is receiving a brand-new body-worn camera straight to their home, but does not have access to the VideoManager interface. An administrator can assign the body-worn camera to the user without needing to physically dock it to their instance of VideoManager, using pre-assign.



To pre-assign a body-worn camera:

1. Navigate to the relevant site (if the remote worker is using an EdgeController).

>> For more information, see View Sites on page 147

2. Select the ***Devices*** tab.
3. Click ***Advanced*** in the top right-hand corner.
4. Click ***Pre-assign device***.
5. Here, the administrator will be asked to populate the following fields:
    - In the ***Operator name*** field, enter the name of the operator to whom this body-worn camera will be pre-assigned.
    - From the ***Assignment mode*** dropdown, select how the body-worn camera will be pre-assigned to the operator.

>> For more information, see Assign Body-Worn Cameras and Record Footage on page 110

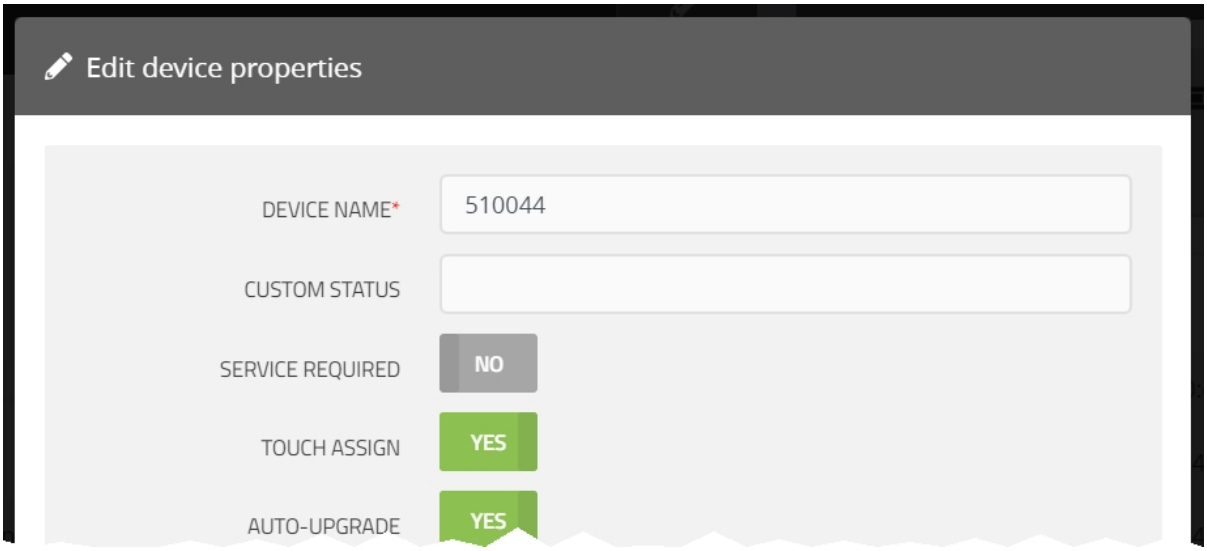
- From the ***WiFi profile*** dropdown, select a previously-created WiFi profile. This dictates which WiFi networks will be utilised by the VT-series camera next time it connects to VideoManager.
- In the ***Device serial no.*** field, enter the serial number of the body-worn camera which is being pre-assigned.

6. Click ***Pre-assign*** to save the changes.

The body-worn camera will be pre-assigned to the operator. As soon as the body-worn camera is connected to VideoManager (e.g. through a DockController), it will be assigned to the previously-determined user.

6.5 Edit Body-Worn Camera Properties

Once a body-worn camera has been connected to VideoManager 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***.

>> For more information, see Search Body-Worn Cameras on page 122

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. By default, this is the body-worn camera's serial number.

   If this is changed while the body-worn camera is disconnected from VideoManager, 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.

   - 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 Footage on page 110

Caution *Depending on how the body-worn camera settings have been configured, it may only be possible to assign a body-worn camera using Touch Assign if its battery is full.*

>> For more information, see Configure Device Settings on page 207

- 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.

>> For more information, see Configure Firmware Settings on page 332

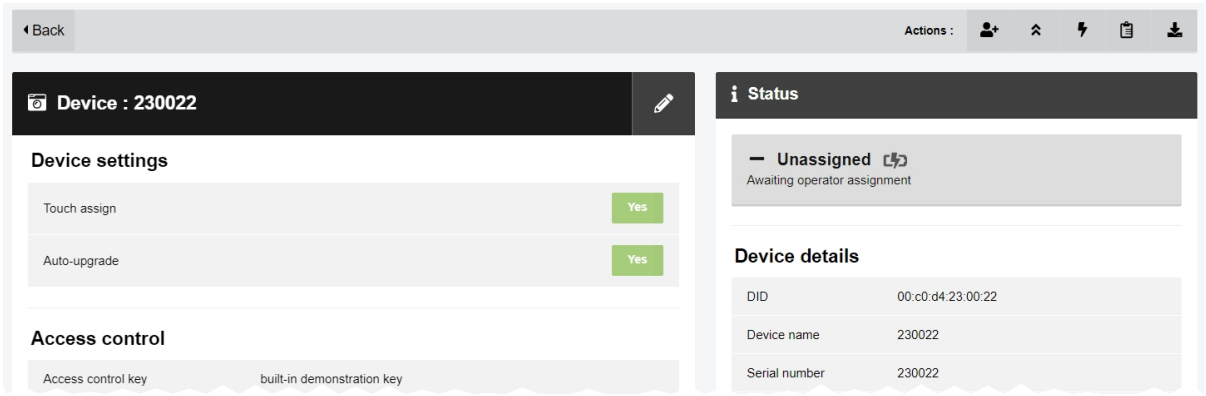
- If ***Use static IP*** is set to ***Yes***, the user must enter the IP address which the body-worn camera will use.

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

7. Click ***save changes***.

6.6 Perform Body-Worn Camera Actions

Once a body-worn camera has been connected to VideoManager, 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***.

>> For more information, see Search Body-Worn Cameras on page 122

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) 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 footage but is redocked to an instance of VideoManager 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 footage on it which has not already been downloaded to VideoManager will be deleted.*

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 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 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 videos recorded by this body-worn camera in the specified incident.

   For example, when a video 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.
   - 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 device audit log*** in the top right-hand corner.

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

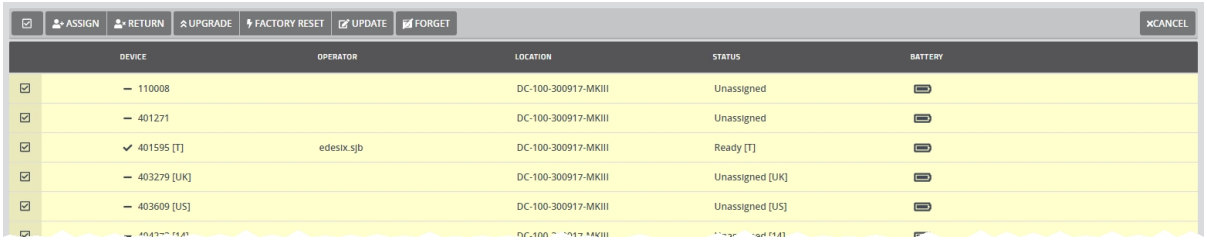
If a body-worn camera has been undocked from VideoManager, it can be forgotten. This will remove it from VideoManager's list until it has been redocked. This is useful if a body-worn camera has been lost or taken out of rotation, and the user wants to hide it from any search results for organisational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

1. Click ***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 until it is re-docked.

6.7 Bulk Edit Body-Worn Cameras

Bulk edits can be used to quickly edit all body-worn cameras on an instance of VideoManager. 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 ***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 122

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.

- **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:

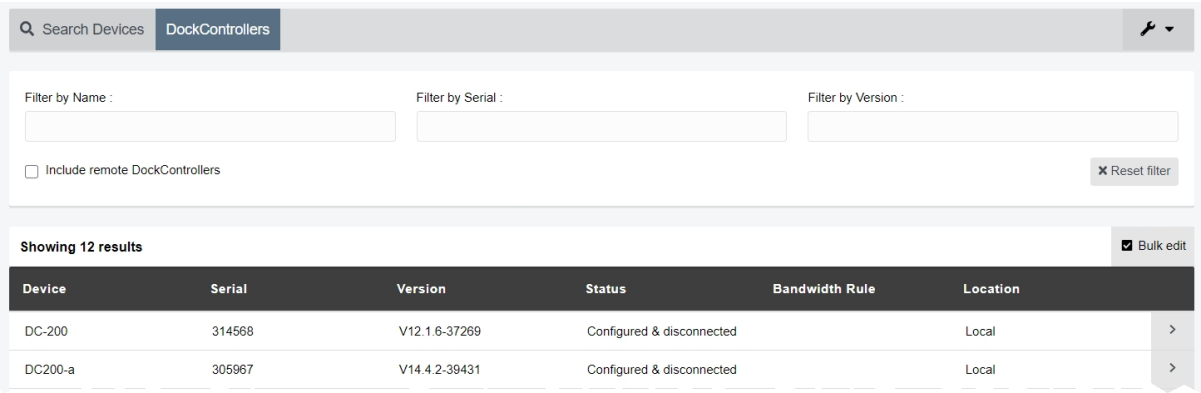
- ***Change custom status***
- ***Change service required***
- ***Change touch assign***
- ***Change auto-upgrade***

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

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

6.8 Perform DockController Actions

Once a DockController has been associated with VideoManager, users can configure it from the ***DockControllers*** pane.



To access any DockControllers associated with the user's instance of VideoManager:

1. Navigate to the ***Devices*** tab
2. Select the ***DockControllers*** pane.
3. Find the relevant DockController, and click > ***View details*** next to it.

Users can filter by **Name**, **Serial**, and **Version**.

If a DockController is offline, the user can view its serial number, mac address, device name, hardware revision, version and status from this pane.

If a DockController is online, the user can view its serial number, mac address, device name, hardware revision, version and status, as well as its ***Bandwidth Rule*** settings, and connected body-worn cameras from this pane. Users can perform the following actions on these DockControllers:

- Change the DockController's name, server settings, and IP settings.

To do so, click ***Configure DockController***.

- Transfer the DockController from one instance of VideoManager to another.

To do so, click ***Configure DockController***, and set ***Configure for this VideoManager?*** to ***Off***. However, for this to be possible, the user must know the API and the API secret for the other instance of VideoManager.

- Restart a DockController.

To do so, click ***Restart DockController*** in the top right-hand corner, and click ***yes***.

- Upgrade a DockController.

To do so, click ***Upgrade DockController*** in the top right-hand corner, select the new DockController image, and click ***Upgrade DockController***.

- Download logs from a DockController.

To do so, click ***Download logs from DockController*** in the top right-hand corner. The log will be downloaded to the user's PC as a ZIP file.

- Delete a DockController from VideoManager.

To do so, click ***Delete DockController*** in the top right-hand corner. Click***yes***.

- Set the bandwidth rules and priority level for a DockController.

To do so, click the ***Bandwidth Rule*** dropdown, and select the relevant bandwidth rule.

>> For more information, see Create, Copy, Edit and Delete Bandwidth Rules on page 226

If ***High Priority DockController*** is set to ***On***, all footage from this DockController will be uploaded as quickly as possible - this means that if the DockController is part of a bandwidth rule that has the ***Shared bandwidth group*** setting enabled, it will halt the downloads of other DockControllers in the group until all of its footage has been uploaded.

- Change whether multiple DockControllers can share the same RFID reader - this means that, if enabled, a user can touch their RFID card to an RFID reader connected to one DockController and receive a body-worn camera from either that DockController or another one.

To do so, set ***Allocate cameras from another touch assign reader*** to ***On***. In the ***Available DockController*** field, enter the name of the other DockController whose RFID reader will be associated with this DockController as well.

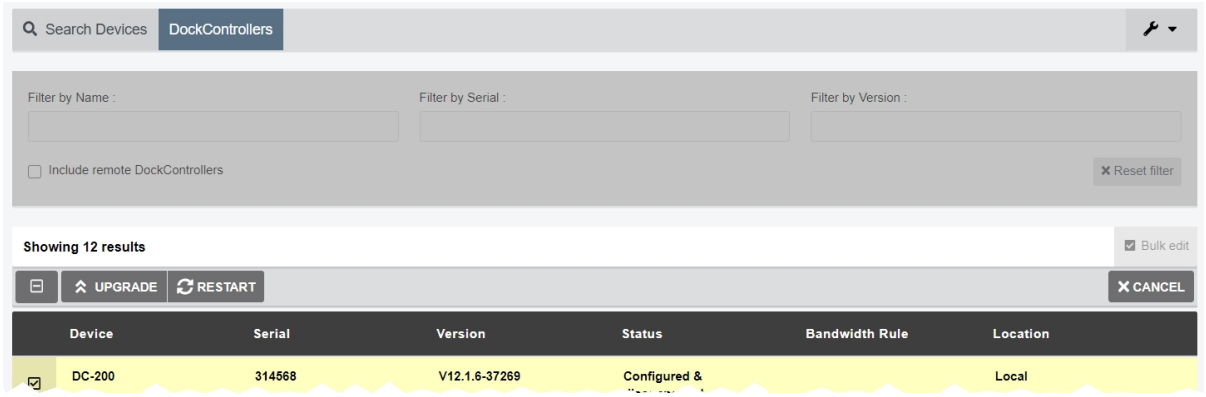
Multiple DockControllers can use the same RFID reader - for example, if DockController A uses DockController B's RFID reader, and DockController C uses DockController A's (which is actually B's).

- Change which touch assign battery settings will be used by this DockController. By default, a DockController will use the system-wide settings configured from the ***Admin*** tab. Alternatively, administrators can configure a DockController to have its own touch assign settings, which are different from the system-wide settings. This is useful if, for example, users will be docking their body-worn cameras at this DockController temporarily, and should be able to touch assign body-worn cameras even if they are not fully charged.

To do so, in the ***Device settings*** pane, set ***Device settings*** to ***Off***. Either set ***Full battery required to touch assign*** to ***On***, or, in the ***Minimum charge time*** field, enter the number of minutes for which body-worn cameras must have been charging before they can be touch assigned.

6.9 Bulk Edit DockControllers

Bulk edits can be used to quickly upgrade and restart DockControllers visible to the system.



To bulk edit DockControllers:

1. Navigate to the ***Devices*** tab.
2. Select the ***DockControllers*** pane.
3. 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 DockController by clicking ■ next to it.
   - Select all DockControllers by clicking ☑ **Toggle selection of ALL devices.**

Once DockControllers have been selected, the following actions are now available:

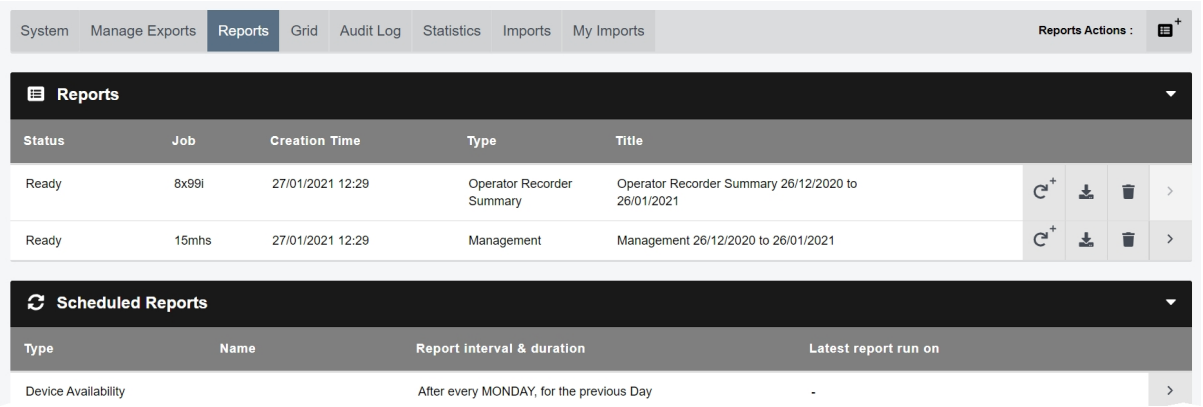
- ⏫ **Upgrade** - if there is a firmware upgrade available, this will upgrade all selected DockControllers.
- 🔄 **RESTART** - this will restart all selected DockControllers.

  This may be necessary if body-worn cameras are having difficulty connecting to VideoManager - restarting a DockController will disconnect, and reconnect, all body-worn cameras connected to it.

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

7 Status

The ***Status*** tab shows reports which have been created in VideoManager, as well as ***Sites*** and ***Site Uploads*** (if the user has configured their instance of VideoManager to act as a Central VideoManager), and ***Audit Log*** and ***Statistics***.



If users have sufficient permissions, they can:

- Check whether there are any system messages from the ***System*** pane.

These messages could include system warnings, such as failed import jobs. Users can click > ***View system warning*** to view more information about the warning.

- Manage exports and perform export actions (retrying and deleting failed exports, viewing completed exports).

>> For more information, see Manage Exports on page 140

- View all scheduled and completed reports from the ***Reports*** pane.

>> For more information, see Create Reports and Perform Report Actions on page 143

- Enable and configure a Central VideoManager and sites (including EdgeControllers). This is part of a multi-step process.

>> For more information, see Configure Sites on page 374

- Review the status of connected sites.

>> For more information, see View Sites on page 147

- Review the uploads occurring at a user's sites from the ***Site Uploads*** pane.

>> For more information, see View Connected Site Uploads on page 149

- Check online grids and their statuses from the ***Grid*** pane.

>> For more information, see View Grids on page 151

- Review the comprehensive list of all actions taken on VideoManager from the ***Audit Log*** pane.

>> For more information, see Filter and Download Audit Logs on page 152

- Watch live statistics based on a user's infrastructure from the ***Statistics*** pane.

>> For more information, see View Statistics on page 154

- If the user has licensed *Asset Import*, they can view the status of imports which have been integrated into VideoManager.

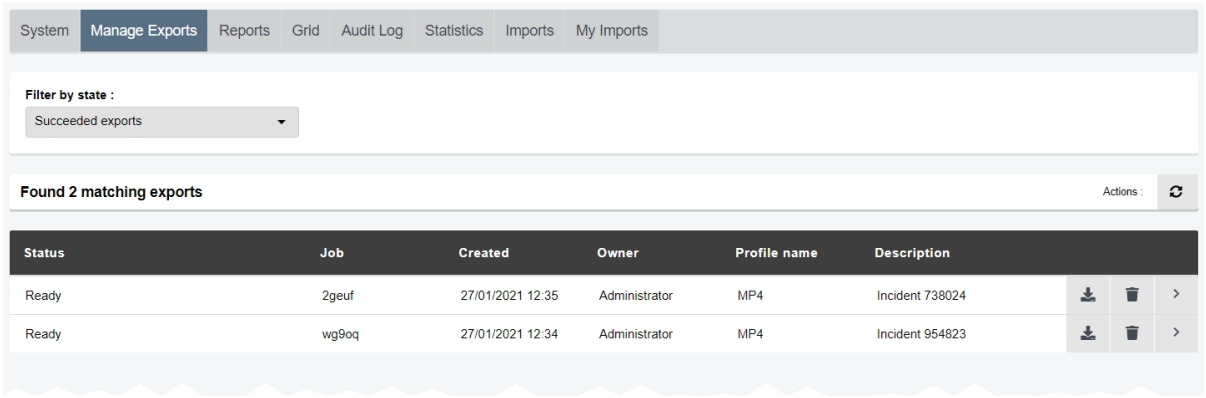
>> For more information, see View Import Jobs on page 156

7.1 Manage Exports

Users can export previously-created incidents. This enables them to share incidents with workers who do not have access to VideoManager. Once a copy of an incident has been exported, it is called an export - however, the original incident will still remain on VideoManager.

>> For more information, see Share Incidents Externally Using an Export on page 93

The ***Manage Exports*** pane enables users with sufficient permissions to view previously created exports. These exports can then be viewed or deleted to free up space on VideoManager.



To view all exports on VideoManager:

1. Navigate to the ***Status*** tab.
2. Select the ***Manage Exports*** pane.
3. From the ***Filter by state*** dropdown, users can select how exports are filtered. The options are as follows:

   - **Failed exports** - this will show all exports which have failed on VideoManager. This might be because the **Exports** file space is full, and therefore no more exports can be sent there.
   - **Pending exports** - this will show all exports which are currently being processed by VideoManager. It will also show in realtime what percentage of the export has been processed by VideoManager.

   Incidents which contain multiple videos will take longer for VideoManager to process than incidents with fewer videos.

   - **Succeeded exports** - this will show all succeeded exports on VideoManager. If an export has succeeded, it is ready to be shared.

The actions a user can perform on exports depends on the status of the export.

- If **Failed exports** has been chosen, users can:
  - ***Delete Export*** - delete a failed export.
  - ***Retry all failed exports*** - retry all failed exports.
  - ***Retry Export*** - retry a single failed export.

> Caution *VideoManager will **not** automatically retry an export, even if more space is made available in the* **Exports** *file space. For this reason, it is necessary to manually retry exports.*

- If **Pending exports** has been chosen, users can:
  - ***Delete Export*** - delete a pending export.

  VideoManager will stop processing the export and it will not be created. This will **not** delete the original incident from which the export was created.

- If **Succeeded exports** has been chosen, users can:
  - ***Delete Export*** - delete an export.

  If the export has an export link associated with it, that link will immediately become invalid. However, if an external party has already used the link to download the export, they will still have access to the export.

  This will **not** delete the original incident from which the export was created.

  - ***Download Export*** - download an export to the PC's default downloads location.

  This is one of two ways to share an export. The other way to share it is using an export link.

>> For more information, see Share Incidents Externally Using an Export on page 93

> Caution *Once an export has been downloaded to a PC, **VideoManager has no control over it**.*

  - ***View Export*** - users can see more information about an export.

  This includes creating a link, viewing the export's audit log, and viewing an export's details, which are as follows:

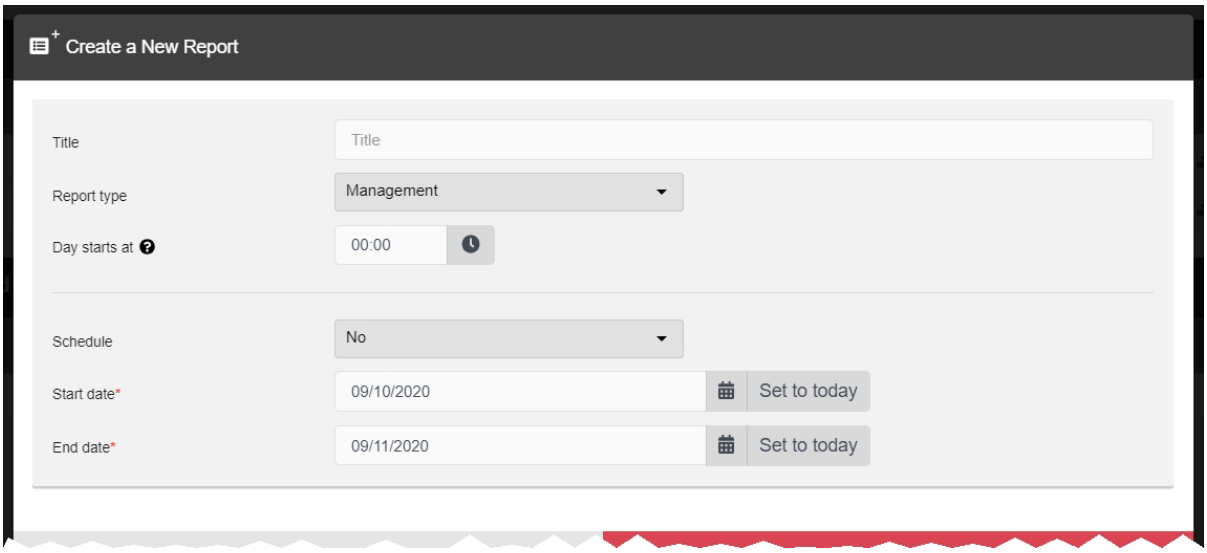
    - ***Signature*** - the export's unique signature, which is automatically generated by VideoManager.
    - ***Description*** - the name of the export. This is not necessarily the same as

the name of the original incident.

- ***Finished*** - when the export finished being processed on VideoManager.

7.2 Create Reports and Perform Report Actions

A report summarises information about how a certain aspect of VideoManager is being used. This is useful if administrators want to check whether the system is being used correctly by other users, or to review body-worn camera usage.



Before administrators create reports, they should configure report settings for VideoManager. These settings dictate when reports will be automatically deleted and run.

>> For more information, see Configure Report Settings on page 259

They can also optionally configure a **Report auto-copy** file space, which will automatically copy every CSV report when it is created, and send it to a specific location.

>> For more information, see Create, Edit and Delete File Spaces on page 344

To create a report:

1. Navigate to the ***Status*** tab.
2. Select the ***Reports*** pane.
3. Click ***Create New Report***.
4. In the ***Title*** field, enter a name for the report.
5. From the ***Report type*** dropdown, select what type of report will be generated.

>> For more information, see Appendix C: Types of Report on page 456

6. Using the ***Day starts at*** field, select at what time the day will begin for this report (for example, an organisation's work day might begin and end at 3am). This option does not apply to **User Export** and **Equipment** reports because they only capture the state of VideoManager at the moment they were run.

This may cause the report to finish the following day (e.g if ***Day starts at*** *is set to 3am, the report will end at 3am the following day).*

7. From the ***Schedule*** dropdown, users can select whether the report will be a one-off, or automatically recurring. The options are as follows:

   - **No** - the report will only be created once. The user must choose the start and end dates that the report will cover.
   - **Minutely** - this is only available if **Equipment** has been selected. From the ***Interval*** dropdown, the user can select how often the report will run.

   VideoManager will run this report from :00 of the hour and continue regularly (e.g. if **Every 30 minutes** *has been selected, the report will always run at :00 and :30 minutes past).*

   - **Hourly** - this is only available if **Equipment** has been selected.
   - **Daily** - the report will be run daily. The user must choose how many previous days the report will cover.
   - **Weekly** - the report will be run weekly. The user must choose on which day of the week the report will run, and how many previous days the report will cover.
   - **Monthly** - the report will be run monthly. The user must choose on which day of the month (e.g. 1st, 2nd, etc.) the report will run, and how many previous days the report will cover.
   - **Custom interval** - the user must choose how often the report will run (days, weeks, or months), and how many previous days the report will cover.
   - If the user has already created a custom report schedule with a JSON file and imported it into VideoManager, they can select it here.

   >> For more information, see Configure Report Settings on page 259

8. If the user has chosen to create a scheduled report, the ***Number of reports retained*** field will appear. In this field, the user can configure how many versions of the report will be kept by VideoManager before the oldest ones are deleted automatically to free up space for new ones.
9. If the user has created a **Report Auto Copy** file space, and has chosen a report which downloads to the their PC as a CSV file, they can choose to set ***Auto Copy File Path*** to ***On***.

>> For more information, see Create, Edit and Delete File Spaces on page 344

Using the ***Add Field*** dropdown, users can choose the name of the subfolder where the report will be sent, within the file space. The options are as follows:

- **{FILE_NAME}**
- **{START_DATE}**
- **{REPORT_TYPE}**

Users can also type in their own folders manually.

10. Click ***Create***.

The status of the report is shown as ***Generating***.

When the report is ready to be reviewed, its status will change to ***Ready***.

11. The steps for viewing a report differ, depending on whether it is non-recurring or recurring:

    - Non-recurring (one-off) reports can be downloaded from the ***Reports*** pane, by clicking ***Download report***.
    - Recurring reports can be viewed and downloaded from the ***Scheduled Reports*** pane, by clicking ***Download latest report***.

    If no reports have been automatically generated yet, the ***Download latest report*** control will not be visible.

Reports cannot be edited like other aspects of VideoManager, such as incidents. Instead, if a user wishes to edit the parameters of a report, it must be **re-run**.

1. Next to the report that will be re-run, click ***Re-run report***.

The ***Re-run an Existing Report*** window will open.

2. Alter the parameters as necessary. All report parameters can be altered, and there is no limit on how many can be changed.
3. Click ***Create***.

The report will be re-run, with the updated parameters.

Once it has been created, users can pause a recurring report. This is useful if a report should be temporarily stopped, but not deleted entirely. To do so:

1. Navigate to the ***Status*** tab.
2. In the ***Scheduled Reports*** pane, next to the report to be paused, click ***View schedule***.
3. Click ***Pause Scheduled Report***.

The report will not run automatically until it is unpaused again, by clicking ***Resume Scheduled Report***.

The steps for deleting a report differ, depending on whether it is non-recurring or recurring.

To delete a non-recurring (one-off) report:

1. Navigate to the ***Status*** tab.
2. In the ***Reports*** pane, next to the report to be deleted, click ***Delete report***.
3. Confirm that the report should be deleted by clicking ***yes***.

To delete a recurring report:

1. Navigate to the ***Status*** tab.
2. In the ***Scheduled Reports*** pane, next to the report to be deleted, click ***View schedule***.
3. Click ***Delete Scheduled Report***.
4. Confirm that the report should be deleted by clicking ***yes***.

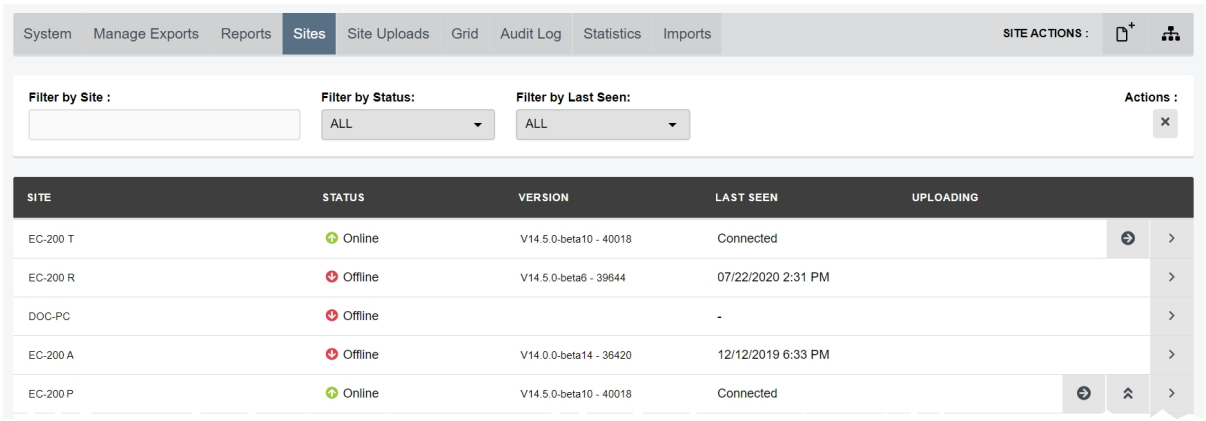
7.3 View Sites

Sites are instances of VideoManager which are connected to a Central VideoManager - this enables administrators on the Central VideoManager to maintain oversight over these other instances of VideoManager, and monitor their activity. Footage and incidents can also be automatically transferred from sites to a Central VideoManager.

Users must configure their sites before they can view them from the ***Sites*** pane. This is part of a multi-step process.

>> For more information, see Configure Sites on page 374

Once a user has configured their sites, they can view the status of these sites from the Central VideoManager. Users can also access their sites' UI from the Central VideoManager.



To view the connected sites:

1. Navigate to the ***Status*** tab.
2. Select the ***Sites*** pane.
3. Users can filter their sites in the following manners:
   - In the ***Filter by site*** field, users can enter the name of the site in question. VideoManager will automatically filter the relevant results as the user types.
   - From the ***Filter by status*** dropdown, users can filter their sites based on whether they are **Online**, **Offline**, or **Disabled**.
   - From the ***Filter by last seen*** dropdown, users can filter their sites based on when they were last seen. The options are **Less than 4 hours ago** or **More than 4 hours ago**.

   The last time a site was "seen" by VideoManager is the last time it was connected to VideoManager.

   - Click ✕ ***Reset filter*** to clear the filters.

4. Once the sites have been filtered, users will be presented with the following columns:

   - ***Site*** - this is the name of the site, which can be configured when initially creating the site itself.
   - ***Status*** - this is the status of the site. A site could be ***Online***, ***Offline***, or ***Disabled***.

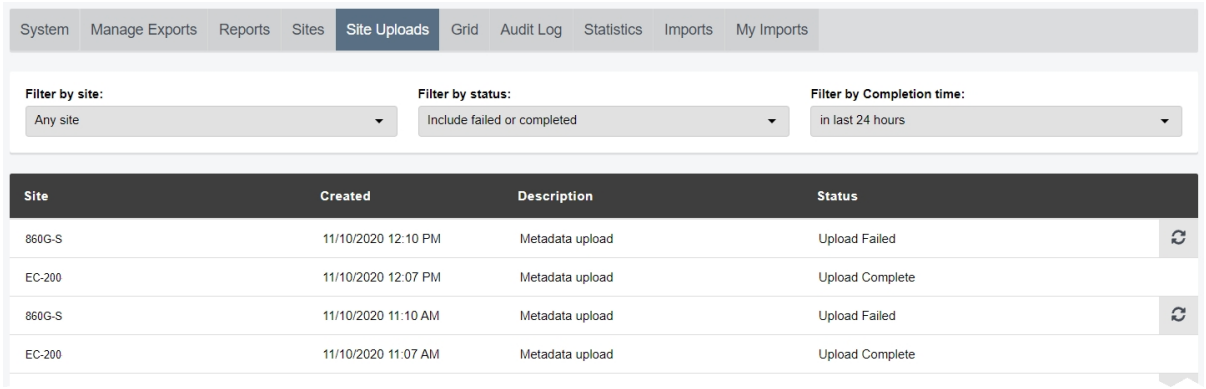
   A site could be ***Offline*** *if the EdgeController hosting the site is turned off, or the network between the site and Central VideoManager is disconnected.*

   - ***Version*** - this is the version of VideoManager running on the site.
   - ***Last seen*** - this is when the site was last connected to VideoManager. If the site is ***Online***, this column will read as ***Connected***.
   - ***Uploading*** - if the site is in the process of uploading footage or incidents to the Central VideoManager, this column will detail the number of jobs running.

   Users can click for more information about the job(s).

7.4 View Connected Site Uploads

Once sites have been configured, the ***Site Uploads*** pane can be used to monitor all uploads from the sites to the Central VideoManager. This enables users to view the progress of site uploads.



To view site uploads:

1. Navigate to the ***Status*** tab.
2. Select the ***Site Uploads*** pane.
3. Users can filter their sites in the following manners:
    - From the ***Site*** dropdown, users can select from which site the uploads will be filtered. Alternatively, it can be left as **Any site** - this will return uploads from all sites.
    - From the ***status*** dropdown, users can filter site uploads by their status. The options are as follows:
        - **Active uploads only** - this will include uploads which are currently in progress, as well as uploads which are queued.
        - **Include failed uploads** - this will include both active uploads and failed uploads (this may be because the footage was deleted from the site before it had a chance to be uploaded).
        - **Include failed or completed** - this will include active uploads, failed uploads, and uploads which have been completed.

    If **Include failed uploads** *or* **Include failed or completed** *has been selected, the results can also be filtered by time frame, using the* ***Filter by Completion Time*** *dropdown.*

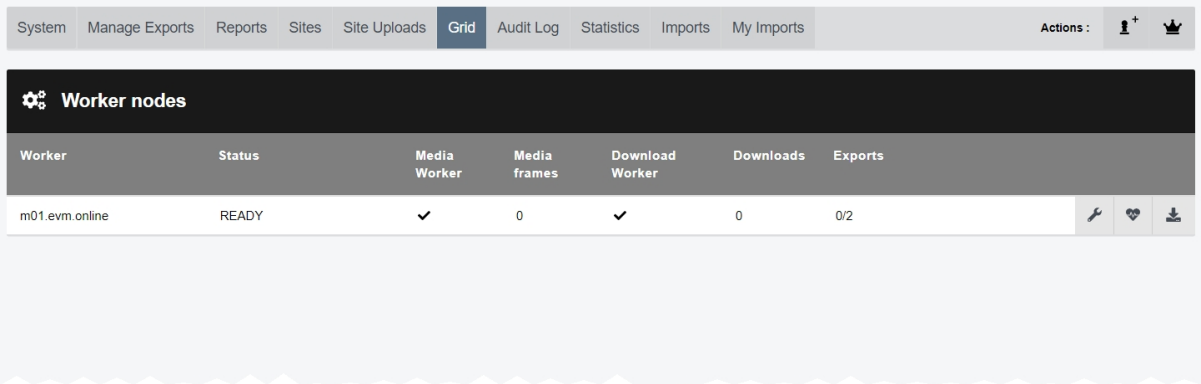
4. Once the site uploads have been filtered, users can view the following columns:
    - ***Site*** - the name of the site from which the upload was sent.
    - ***Created*** - when the upload was sent from the site to the Central VideoManager.

- ***Description*** - the type of upload. This includes ***Metadata upload*** (body-worn camera information and audit logs) and ***Footage*** (the video's URN will be included in the entry).
- ***Status*** - the status of the upload. This could be ***Upload Complete*** or ***Upload Cancelled***.

If a site upload's status is ***Upload Cancelled***, the user can click ***Retry this upload*** to retry the site upload.

7.5 View Grids

If enabled by an administrator, users with the ***View grid status*** permission will be able to access the ***Grid*** pane. Grids are useful if one computer processor is not enough to run VideoManager smoothly, especially if many CPU-intensive actions are being performed regularly (such as exporting videos).



Normal users are unable to add, edit, or delete grids. The main aspects of grids which can be accessed by regular users are worker statuses and logs. To view these:

1. Navigate to the ***Status*** tab.
2. Select the ***Grid*** pane.
3. Click > ***View worker details***.

Here, users can perform two actions:

- To check the status of a grid, click ***Worker settings check***.

This will open a window which displays the status of the grid's URLs.

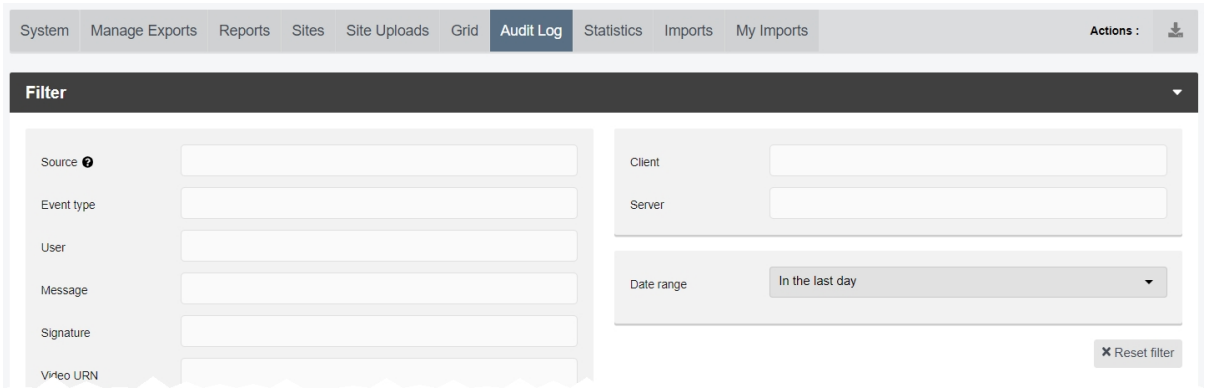
- To download grid logs, click ***Download logs***.

This will download a .zip folder to the PC running VideoManager. The folder contains a .txt file of the grid's logs.

For more information, please contact Technical Support and ask for the technical paper *Grids Explained [ED-009-068]*.

7.6 Filter and Download Audit Logs

An audit log is a record of **all** actions that have been undertaken by the system, and who performed them. This enables administrators to keep tabs on which users, body-worn cameras, and sites are performing which actions. An audit log cannot be edited or deleted - only filtered.



To access the audit log:

1. Navigate to the ***Status*** tab.
2. Select the ***Audit Log*** pane.

It is possible to filter the audit log by a number of criteria, including:

- ***Source*** - view all actions undertaken by the specified body-worn camera (enter the serial number) or import source.
- ***Event type*** - view all instances of the specified action taking place (e.g. creating an incident, or a report). By typing in the relevant action, various matches will appear for users to select.
- ***User*** - view all actions undertaken by a specific user on VideoManager.
- ***Message*** - view all messages whose text matches what is entered here.

A message could be any text entered when searching for an incident or video - for example, by entering text into the ***Title*** field in the ***Search Incidents*** pane.

- ***Signature*** - view all actions performed on an incident with the same signature as the one specified here.
- ***Video URN*** - view all actions performed on a video with the same URN as the one specified here.
- ***Location*** - view all actions performed in a location as the one specified here (e.g. a DockController or EdgeController).
- ***Search by file hash*** - view all actions performed on a video or asset whose digest matches the file hash entered here.

Users can either enter the file hash manually or click ***Read from file*** and select the file from their PC.

- From the ***Date range*** dropdown, users can select a specific time period. All actions undertaken within that time period will be returned. The options are **None**, **In the last day**, **In the last 7 days**, and **In the last 30 days**.

Users can also select **Custom**, where they can choose two dates to filter between.

Once the options have been chosen, users can perform the following actions:

- Click ***Reset filter*** to clear the search filters.
- Click ***Filter audit log*** to view the audit log.

The audit log will be presented to the user immediately. Users can then click ***Download CSV*** to download the audit log to their PC's default download location.

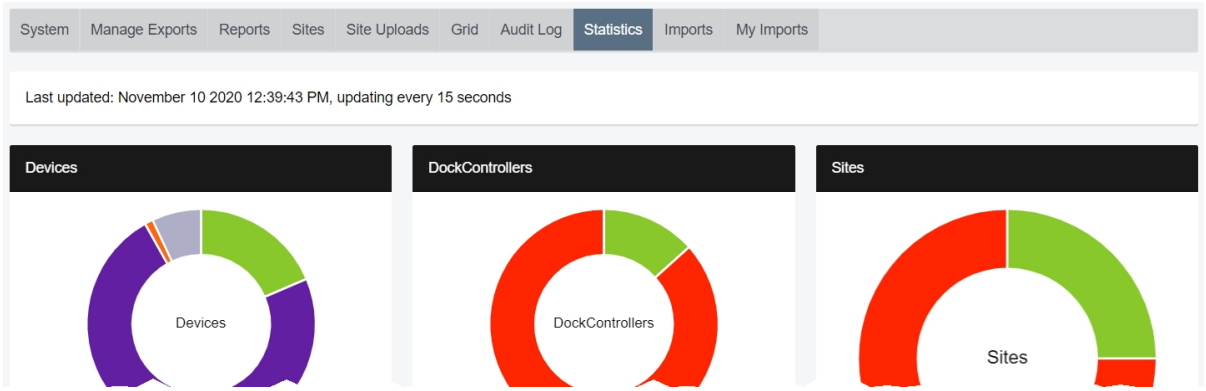
- Click ***Create report*** to create a report based on these filters.

If users choose this option, they must enter a title for the report, and decide whether it will be scheduled or not.

>> For more information, see Create Reports and Perform Report Actions on page 143

7.7 View Statistics

The ***Statistics*** pane is located in the ***Status*** tab. It shows statistics relating to the user's VideoManager infrastructure in real time.



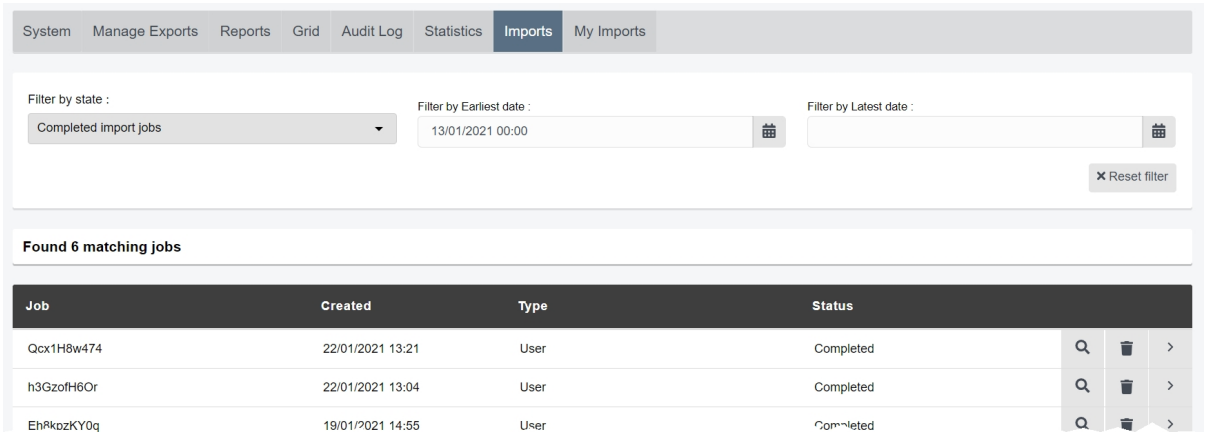
Users can hover their cursor over either the chart or the key beneath it, to break the information down further and view exact percentages. The following statistics are available:

- The ***Devices*** pane shows the number of body-worn cameras visible to VideoManager, and what state they are in.
- The ***DockControllers*** pane shows the number of DockControllers known to VideoManager, and whether they are connected or disconnected.
- The ***Sites*** pane shows the number of EdgeControllers known to VideoManager, and whether they are connected or disconnected.
- The ***Total footage stored*** pane shows the number of megabytes of video stored by VideoManager.
- The ***Footage written today*** pane shows the number of megabytes of video stored by VideoManager that day.
- The ***Footage write rate*** pane shows how much footage has been written to disk by time.
- The ***User activity*** pane shows how many users are logged in by time.
- The ***Video recording counts*** pane shows the number of videos recorded in the past seven days.
- The ***Total videos in system*** pane shows the total number of videos stored in VideoManager.
- The ***Queued downloads*** pane shows the five sites with the highest number of queued downloads and the number of downloads queued at each.
- The ***Total queued downloads*** pane shows a count of the total number of downloads queued by sites and EdgeControllers.

- The ***File spaces*** pane shows how the space allocated to VideoManager has been used. Users can click ***Show file space breakdown*** for more information.

7.8 View Import Jobs

If administrators have licensed *Asset Import* from Motorola Solutions, they can import assets (e.g. PDFs, JPGs, and external videos) into VideoManager. They can also view the status of these import jobs from the ***Imports*** pane (which shows **all** import jobs) or ***My Imports*** pane (which shows the logged-in administrator's import jobs).



To view the status of import jobs into VideoManager:

1. Navigate to the ***Status*** tab.
2. Select the ***Imports*** pane (if administrators will be viewing all import jobs) or the ***My Imports*** pane (if administrators will be viewing only their import jobs).

   Here, administrators can filter imports using the ***Filter by state*** dropdown. The options are as follows:

   - **Failed import jobs** - this will show any import jobs which failed on VideoManager.
   - **In-progress import jobs** - this will show any import jobs which are still in progress.
   - **Completed import jobs** - this will show any import jobs which have been completed.

   Administrators can also use the ***Earliest date*** and ***Latest date*** fields to filter import jobs by date.
3. Once the administrator has filtered the import jobs, they can perform the following actions:

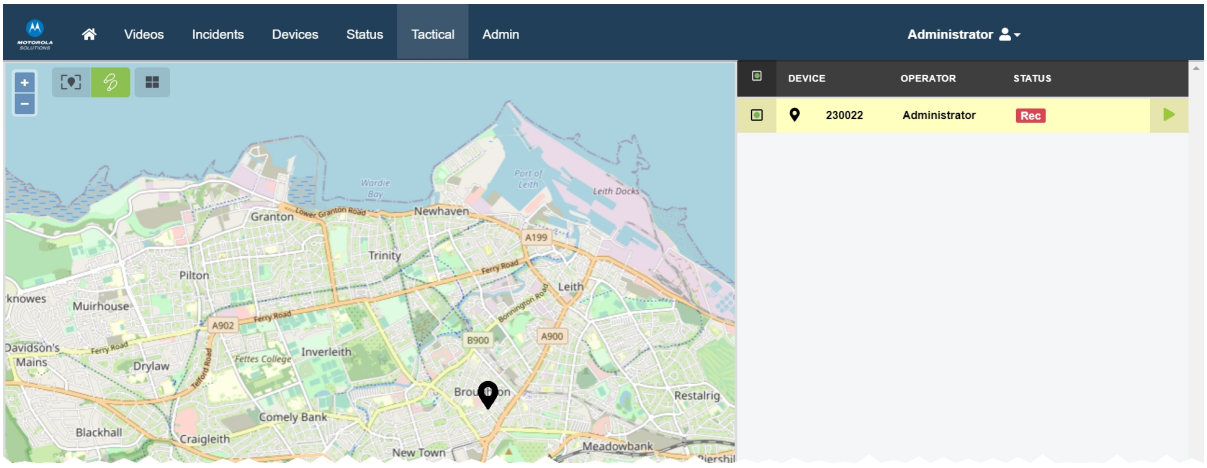
   - > ***View details*** - the administrator can view information about the import job's **Signature** and **Status**, as well as when the job started and finished.
   - 🗑 ***Delete*** - the administrator can delete an import job.

   If the administrator has chosen **Failed import jobs** or **In-progress import jobs** and clicks 🗑 ***Delete***, the asset will not be imported.

If the administrator has chosen **Completed import jobs** and clicks **Delete**, only the import job itself will be deleted. The asset itself will **not** be deleted from VideoManager.

8 Tactical

The ***Tactical*** tab is only visible if users have a *Tactical VideoManager* licence. It gives users the opportunity to see their body-worn cameras' locations represented on a live map.



To configure a body-worn camera to show up on Tactical VideoManager, users must first complete the following steps:

1. Configure a body-worn camera to live stream like normal.

>> For more information, see Configure Streaming on page 364

2. Configure maps.

>> For more information, see Enable and Configure Maps on page 327

3. If the body-worn camera is GPS-enabled, it will automatically appear on the ***Tactical*** tab.

Body-worn cameras will only appear if they are live-streaming. If they are recording but not live-streaming, they will **not** appear on the Tactical VideoManager tab.

There are multiple actions that users can take once the body-worn cameras have appeared. These are as follows:

- View a body-worn camera's live stream. To do so, click its pin on the map, or click its name in the top right-hand corner list.

The live stream will appear in the bottom right-hand corner pane.

- Follow a body-worn camera - in this mode, the map will automatically scale and move to ensure that the followed body-worn cameras are never offscreen. To do so:

1. Follow the relevant body-worn camera, either by clicking its pin on the map, or by clicking its name in the top right-hand corner list.
2. In the leftmost column of the list, check the ■ box.

The map will now "follow" the body-worn camera until the box is unchecked.

- Add videos to, and view, the Tactical VideoManager wall - this gives the user a fullscreen view of selected live streams. To do so:
  1. Focus on the relevant body-worn camera, either by clicking its pin on the map, or by clicking its name in the top right-hand corner list.
  2. Click ***Add to wall*** in the bottom right-hand live stream pane. This will add its live stream to the Tactical VideoManager wall.
  3. Once a few live streams have been added to the wall, users can view the wall by clicking the ⊞ button in the top left-hand corner.
- Perform actions on the Tactical VideoManager wall. The actions are as follows:
  1. Click the ⊞ button in the top left-hand corner.

  This will open the wall in a new tab.
  2. To change the number of live streams shown on the wall simultaneously, click the ⊞ button in the top right-hand corner. This will switch the wall between a 1-screen, 4-screen, and 9-screen view.
  3. To change whether the wall is fullscreen or not, click the ⤢ button in the top right-hand corner.
  4. To remove a live stream from the wall, click ***Clear panel***.

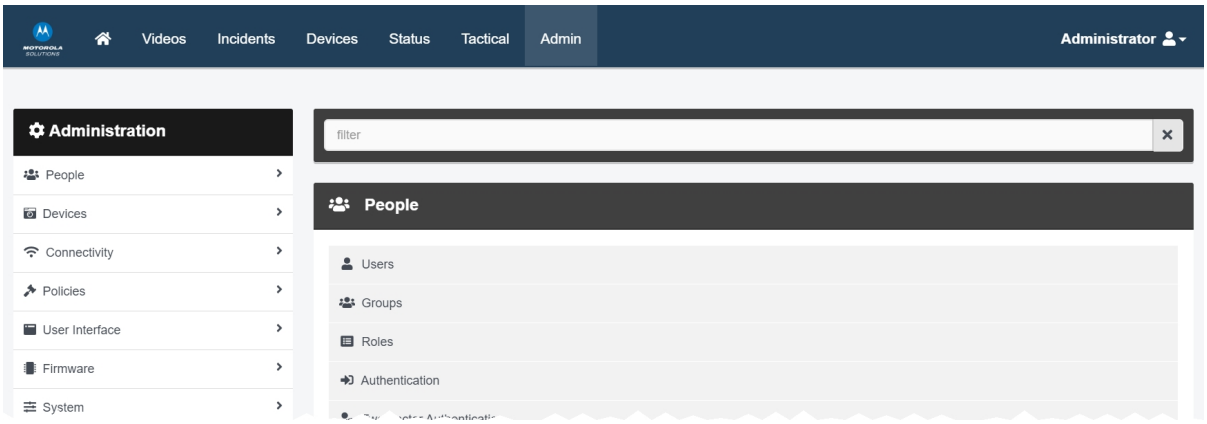
There are multiple actions that users can take to adjust the map itself. These are:

- Zoom in/out. To do so, click the **+/-** buttons in the top left-hand corner.
- Turn the body-worn cameras' trail on. To do so, click the 👣 button in the top left-hand corner. This will show the user a trail behind every body-worn camera, tracking their most recent movements.
- Change whether body-worn camera following is set to ***On*** or ***Off***. To do so, click the 📍 button in the top left-hand corner. This will change whether body-worn camera following is on or off.

If a user follows a body-worn camera, this setting will be turned on **automatically**. However, users may wish to turn this feature off temporarily if they need to view an aspect of the map which is off-screen. Once it is changed back to ***On***, the same body-worn cameras will be followed as before.

9 Admin

The ***Admin*** tab provides access to system administration functions.



This tab is divided into panes, which are divided further into sections. Users can find the relevant section by typing its name into the filter box at the top of the ***Admin*** tab.

The panes, and their sections, are as follows:

- ***People*** (***Users***, ***Groups***, ***Roles***, ***Two Factor Authentication***, ***User Self Service***, and ***User Import Settings***).

>> For more information, see People on page 162

- ***Devices*** (***Device Profiles***, ***Device Settings***, ***Video metadata overlay settings***, ***Access Control Key Management***, and ***Device Certificate Authorities***).

>> For more information, see Devices on page 202

- ***Connectivity*** (***WiFi Profiles***, ***Bandwidth Rules***, ***Metadata/Footage Replication***, ***Configuration Replication***, ***Site Manager***, and ***Email Properties***).

>> For more information, see Connectivity on page 219

- ***Policies*** (***Deletion Policy***, ***Incident Exports***, ***File Exports***, ***Auto Incident Creation***, ***Password Complexity***, ***Reports***, ***User-defined Incident Fields***, ***User-defined Media Fields***, ***CommandCentral Vault Settings***, ***User-defined Playback Reason Fields***, ***Import profiles***, ***Antivirus Policy***, ***Sharing Policy***, ***Playback Policy***, ***VB Companion Settings***, and ***API Key Management***).

>> For more information, see Policies on page 236

- ***User Interface*** (***Login Settings***, ***Video List***, ***Messages***, ***Theme Resources***, ***Player***, ***Language***, ***Maps***, ***Thumbnails***, and ***Incidents***).

>> For more information, see User Interface on page 311

- ***Firmware*** (***Firmware Settings***, ***Device Images***, ***DockController Images***, and ***EdgeController Images***).

>> For more information, see Firmware on page 331

- ***System*** (***Storage***, ***Web Server***, ***Backup Databases***, ***Licences***, ***Advanced Settings***, ***Import/Export System Config***, and ***Server Controls***).

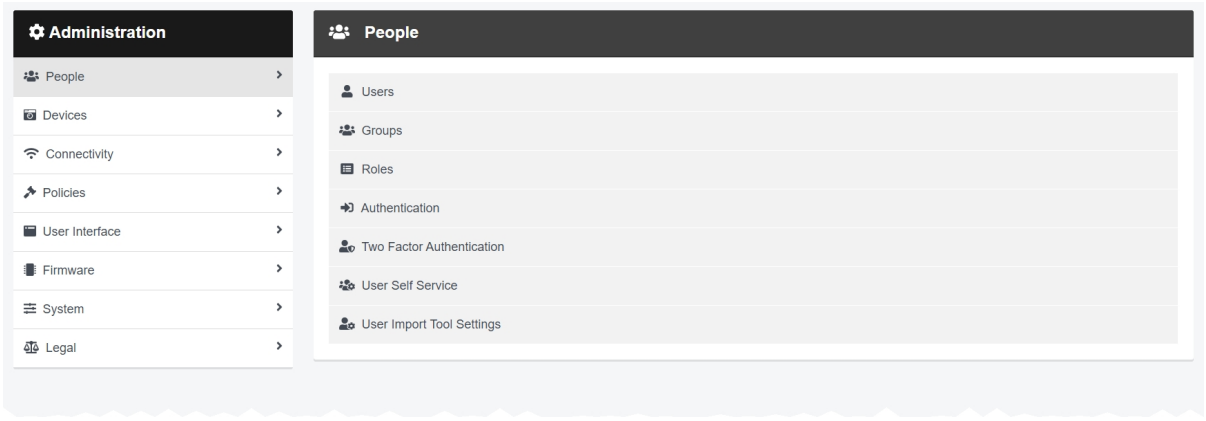
>> For more information, see System on page 340

- ***Legal***.

>> For more information, see View Legal Information on page 359

9.1 People

In the ***People*** pane, administrators can edit aspects of VideoManager related to users and roles.



To access the ***People*** pane:

1. Navigate to the ***Admin*** tab.
2. Select the ***People*** pane.

From here, administrators can access the following sections:

- ***Users*** - administrators can perform the following actions:
  - Create, edit, and delete users.

    >> For more information, see Create, Edit, and Delete Users on page 165

  - Reassign users - this will transfer all videos and incidents from one user to another.

    >> For more information, see Reassign a User on page 170

  - Unlock users - if users cannot access VideoManager because they have entered their password incorrectly too many times, administrators can manually grant them access again.

    >> For more information, see Unlock a User on page 171

  - Export and import users and groups - administrators can download their entire database of users and groups to a CSV file, edit it, then reupload it - this makes it easy to bulk edit users and groups.

    >> For more information, see Export and Import Users and Groups on page 172

- View a user's device affinities - if configured, this will show a list of body-worn cameras which have been assigned to the user with single issue, undocked, and then redocked mid-shift.

>> For more information, see View and Clear Device Affinities for a User on page 174

- ***Groups*** - administrators can perform the following actions:
  - Create, edit, and delete groups.

>> For more information, see Create, Edit and Delete Groups on page 176

  - View the effective permissions for a user or group. This will detail the aspects of VideoManager to which a user or group has access, and how they got their permissions (e.g. from a role, or because they belong to a group).

>> For more information, see View a User or Group's Effective Permissions on page 180

- ***Roles***

Create, edit, and delete roles.

>> For more information, see Create, Edit, Copy, Import, Export and Delete Roles on page 182

- ***Two Factor Authentication*** - administrators can perform the following actions:
  - Enable and configure two factor authentication on VideoManager. This will prompt specific users to enter a code provided by their phone before they can log in to VideoManager, in addition to entering their password as normal.

>> For more information, see Enable and Configure Two Factor Authentication on page 188

  - Enable and configure email login on VideoManager. This will prompt specific users to click a link sent to their email before they can log in to VideoManager, in addition to entering their password as normal.

>> For more information, see Enable and Configure Login by Email on page 192

- ***User Self Service***

Configure user self service. This dictates whether users can reset their own passwords, and whether workers can create their own users on VideoManager.

>> For more information, see Configure User Self Service on page 195

- ***User Import Settings***

Configure the built-in user import tool. This enables administrators to import multiple users/groups simultaneously from a CSV or XLS/XLSX file.

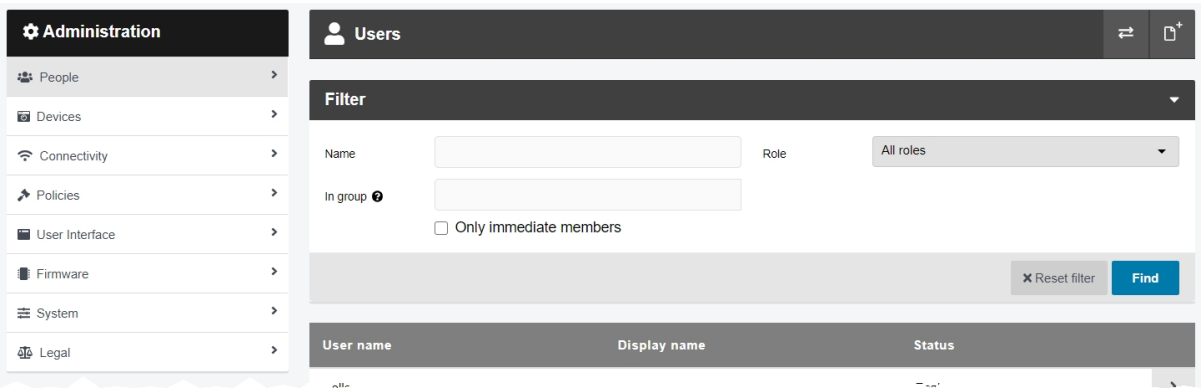
>> For more information, see Configure the Built-in User Import Tool on page 201

9.1.1 Create, Edit, and Delete Users

A user is assigned to every person wishing to access VideoManager. Different users have varying levels of control over the system, depending on how they have been configured. This is done from the ***Users*** section of the ***People*** pane, in the ***Admin*** tab.

As well as creating users manually, it is also possible to configure VideoManager so workers can create their own users.

>> For more information, see Configure User Self Service on page 195



To create a user:

1. Navigate to the ***Admin*** tab.
2. Select the ***People*** pane.
3. Click the ***Users*** section.
4. Click ***Create user***.
5. Enter the following information for the new user:
   - In the ***User name*** field, enter a name for this user. No two users can have the same name on one VideoManager system. This cannot be changed later.
   - In the ***Password*** field, enter a password for the user.

   *Once a value is entered here, the **User must change password** toggle will be automatically set to **On**. This means that the user will be prompted to set their own password the first time they log in.*

   - In the ***Confirm password*** field, enter the same password again to confirm it.
   - In the ***Display name*** field, enter a display name for this user. This can be changed later.
   - In the ***Email notifications*** field, optionally enter an email address for this user.

This may be necessary for multiple reasons:

- Users can receive notifications via email when specific actions are performed on VideoManager. The exact actions which will prompt a notification are determined by the user's roles.
- Users can reset their own password, if the feature has been configured from the ***User Self Service*** section.
- Users may need to click a link sent to their email before they can log in to VideoManager, if the feature has been configured from the ***Two Factor Authentication*** section. Users without email addresses in this field **will not be able to log in**.

- In the ***Touch Assign ID*** field, enter the touch assign ID which will identify a user's RFID card with a body-worn camera. This is only relevant if the user will be assigned a body-worn camera with RFID.

>> For more information, see Assign Body-Worn Cameras and Record Footage on page 110

To find the RFID value of a card, touch the relevant card to the RFID reader. Click ? in the ***Touch Assign ID*** field. This will show a list of failed touch assign scans - the most recent entry will be for that failed scan, which the administrator can copy and paste into the ***Touch Assign ID*** field.

*If a user should be associated with multiple RFID cards (e.g. if they have a door card and a warrant card), repeat the steps above as many times as necessary and separate the touch assign IDs with a comma in the **Touch Assign ID** field (e.g. 543642,873924).*

6. Set additional options for the new user using the following toggles:
   - If ***User must change password*** is set to ***On***, the new user must change their password the first time they log in.

   This makes it possible to assign a predetermined password to a user and then force them to change it for security purposes. Administrators should configure when the password will expire from the ***Password Complexity*** section.

>> For more information, see Configure Password Complexity on page 257

   - If ***Enabled*** is set to ***On***, the user can log in to VideoManager. If set to ***Off***, the user cannot log in.

7. In the ***Roles*** pane, select the roles which the user will inhabit. This determines which aspects of VideoManager the user can see and interact with.

The user's roles can be altered later.

>> For more information, see Create, Edit, Copy, Import, Export and Delete Roles on page 182

8. In the ***Group memberships*** pane, select the groups to which the user will belong. Enter the name of a previously-created group, and click + to add it. This can be changed later.

>> For more information, see Create, Edit and Delete Groups on page 176

9. In the ***Sharing*** pane, select the sharing options required for the user:

   - **Auto share with** - any users or groups entered here will have access to **all** videos, incidents, and exports created by the new user. Click + to add the user or group.

   Users cannot see who their videos are auto-shared with, or if they are auto-shared at all.

   - **For new videos, create shares for** - any users or groups entered here will also be **automatically** entered into the ***Shared:*** field of new videos recorded by the new user. Click + to add the user or group.

   This is useful if certain users or groups should have access to videos recorded by the new user, but should **not** have access to all of their exports or incidents, which **Auto share with** would grant.

   - **For new incidents, create shares for** - any users or groups entered here will also be **automatically** entered into the **Shared:** field of new incidents created by the new user. Click + to add the user or group.

   This is useful if certain users or groups should have access to incidents created by the new user, but should **not** have access to all of their exports or videos, which **Auto share with** would grant.

   - **Supervisor of** - any users or groups entered here will be supervised by the new user. This means that the user can view their videos, incidents, and exports from the ***Supervised Videos***, ***Supervised Incidents***, and ***Supervised Exports*** panes. Click + to add the user or group.

10. If required, add user-specific WiFi networks from the ***WiFi networks*** pane, by clicking ***Add network***. These are networks which only appear on the user's account, and are not viewable by other users on the system.

>> For more information, see Create User-Specific WiFi Networks on page 367

11. Click ***Create user***.

It may be necessary to edit a user if their password should be changed, or if they should be assigned to different roles. To do so:

1. Navigate to the ***Admin*** tab.
2. Select the ***People*** pane.
3. Click the ***Users*** section.
4. Locate the user to be edited. Administrators can filter users in the following ways:
   - A user's name (both username and display name) - enter their username or display name in the ***Name*** field. Click ***Find*** to find the users, or click ✕ to reset the filter.
   - A user's group - enter a group name in the ***In group*** field. Click ***Find*** to find the users, or click ✕ to reset the filter.

   *If the user enters a group name in the **In group** field, they will have the option to change whether **Only immediate members** is set to **On** or not. If set to **On**, only users which are assigned directly to the specified group will be returned (as opposed to if user A is assigned indirectly to group B because A belongs to group C, which is assigned to group B).*

   - A user's role - from the ***Role*** dropdown, select the relevant role. All users who inhabit that role will be returned. Click ***Find*** to find the users, or click ✕ to reset the filter.
5. Next to the user to be edited, click > ***Go to user***.
6. Make the necessary changes, and click ***Save user***.

If a worker leaves an organisation, it may be necessary to delete their user from VideoManager. Deleting a user will **not** delete any of their videos or incidents. To delete a user:

1. Optionally reassign the relevant user to another user on VideoManager. This will transfer all of their incidents, exports, and videos to the other user.

   >> For more information, see Reassign a User on page 170

   If the user is not reassigned, the ***Operator:*** field for their videos will read as *deleted user's name (DELETED)*. If a user is later recreated with the same username, all of the videos, exports, and incidents associated with that username will be automatically associated with that user.

2. Locate the user to be deleted. Administrators can filter users in the following ways:
   - A user's name (both username and display name) - enter their username or display name in the ***Name*** field. Click ***Find*** to find the users, or click ✕ to reset the filter.

- A user's group - enter a group name in the ***In group*** field. Click ***Find*** to find the users, or click ✕ to reset the filter.

*If the user enters a group name in the **In group** field, they will have the option to change whether **Only immediate members** is set to **On** or not. If set to **On**, only users which are assigned directly to the specified group will be returned (as opposed to if user A is assigned indirectly to group B because A belongs to group C, which is assigned to group B).*

- A user's role - from the ***Role*** dropdown, select the relevant role. All users who inhabit that role will be returned. Click ***Find*** to find the users, or click ✕ to reset the filter.

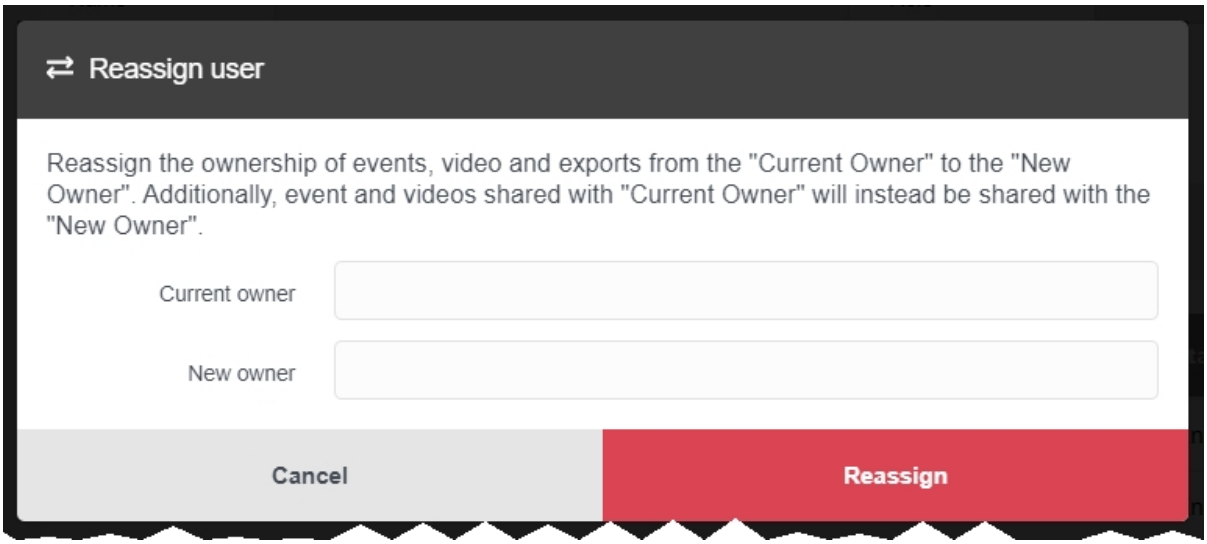
3. Next to the user to be deleted, click > ***Go to user***.
4. Click 🗑 ***Delete user***.

A confirmation window will open.

5. Click ***yes***.

9.1.2 Reassign a User

It is possible to reassign a user. Reassigning a user will transfer all of their videos and incidents to another user. This is advised if a user has left an organisation and they should no longer have access to VideoManager. This is also advised if an organisation plans to re-use usernames on VideoManager: once a user is recreated with the same username as a previously-deleted user, all videos and incidents associated with that username will be reassigned to the user - even if it is not the same worker.



Reassignment can be done before or after a user has been deleted from the system. To do so:

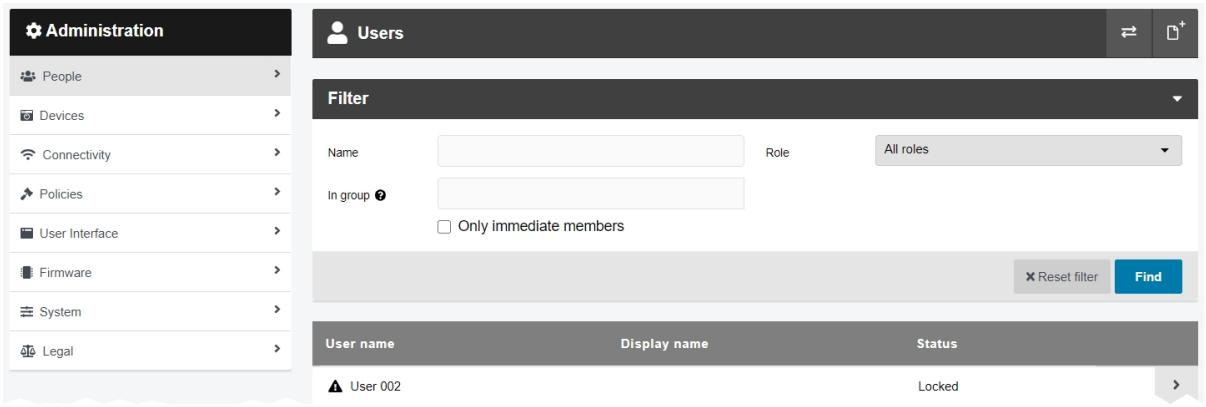
1. Navigate to the ***Admin*** tab.
2. Select the ***People*** pane.
3. Click the ***Users*** section.
4. Click ***Reassign user*** in the top right-hand corner.
5. In the ***Current owner*** field, enter the name of the user whose videos and incidents will be transferred.

   If the user still exists on VideoManager, their name will pop up when typed in. If the user has been deleted, their name will not pop up when typed in, but will still be available for reassignment.

6. In the ***New owner*** field, enter the name of the user who will receive the videos and incidents.
7. Click ***Reassign***.

9.1.3 Unlock a User

Administrators can configure how many login attempts a user can make before their account is locked, and for how long their account is subsequently locked, from the ***Password Complexity*** section of the ***Policies*** pane in the ***Admin*** tab. Once a user's account has been locked, they will be unable to log in to VideoManager until their account is either unlocked by VideoManager automatically, or an administrator unlocks the account manually.



To unlock a user manually:

1. Navigate to the ***Admin*** tab.
2. Select the ***People*** pane.
3. Click the ***Users*** section.
4. Next to the user to be unlocked, click ***Go to user***.

The ***Status*** of a locked user will read as **Locked**, and it will have an icon next to its username.

5. Set ***Unlock now*** to ***Yes***.

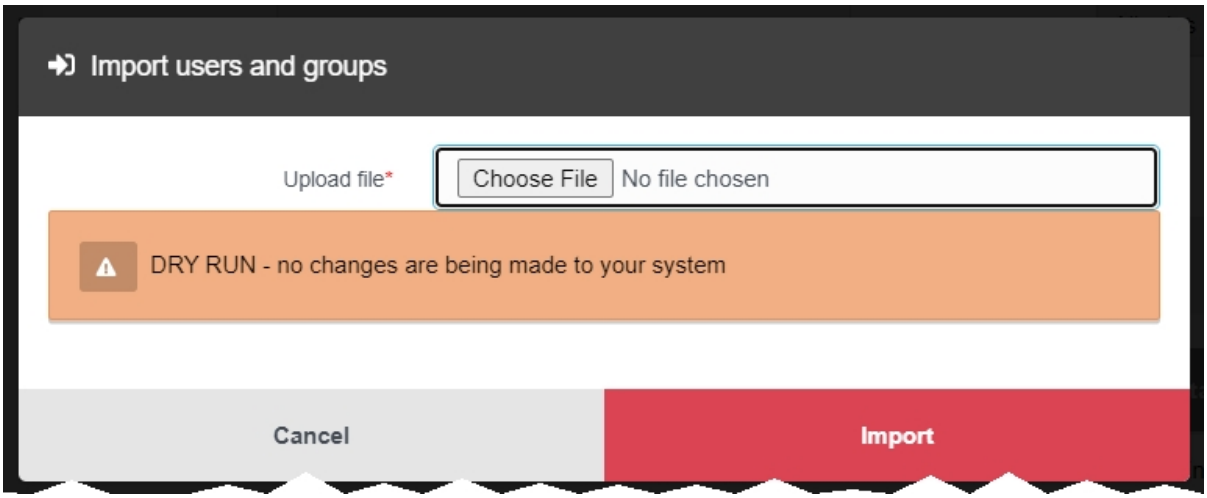
> *If the user made too many incorrect login attempts because they forgot their password, administrators can also reset their password from this pane. Enter the new password in the **Password** and **Confirm password** fields.*

6. Click ***Save user***.

The user will be unlocked and can log in to VideoManager again.

9.1.4 Export and Import Users and Groups

Administrators can download their database of users and groups to a CSV file. This enables them to edit the database in Excel, then reupload the same CSV file to VideoManager. Exporting and importing users and groups is done from the ***Users*** section of the ***People*** pane, in the ***Admin*** tab.



To export the database from VideoManager:

1. Navigate to the ***Admin*** tab.
2. Select the ***People*** pane.
3. Click the ***Users*** section.
4. Click ***Export users and groups***.

This will download a CSV file to the administrator's PC containing information about their users and groups. This includes their roles and relationships (e.g. which users belong to which groups). Administrators can edit this file in Excel.

To import the database back into VideoManager once it has been edited:

1. Navigate to the ***Admin*** tab.
2. Select the ***People*** pane.
3. Click the ***Users*** section.
4. Click ***Import users and groups***.
5. Click ***Choose File*** and select the previously-exported CSV file.

VideoManager will automatically perform a "dry run", allowing the administrator to preview the changes before they come into effect. The following fields will be presented:

- ***Users and groups added:*** - this lists the number of users and groups which are in the CSV file but not on VideoManager.

- ***Users and groups updated:*** - this lists the number of users and groups whose data in the CSV file does not match the data on VideoManager.
- ***Users and groups removed:*** - this lists the number of users and groups which are on VideoManager but not in the CSV file.

6. If the administrator is satisfied with the proposed changes, click ***import***.

The following changes will take place:

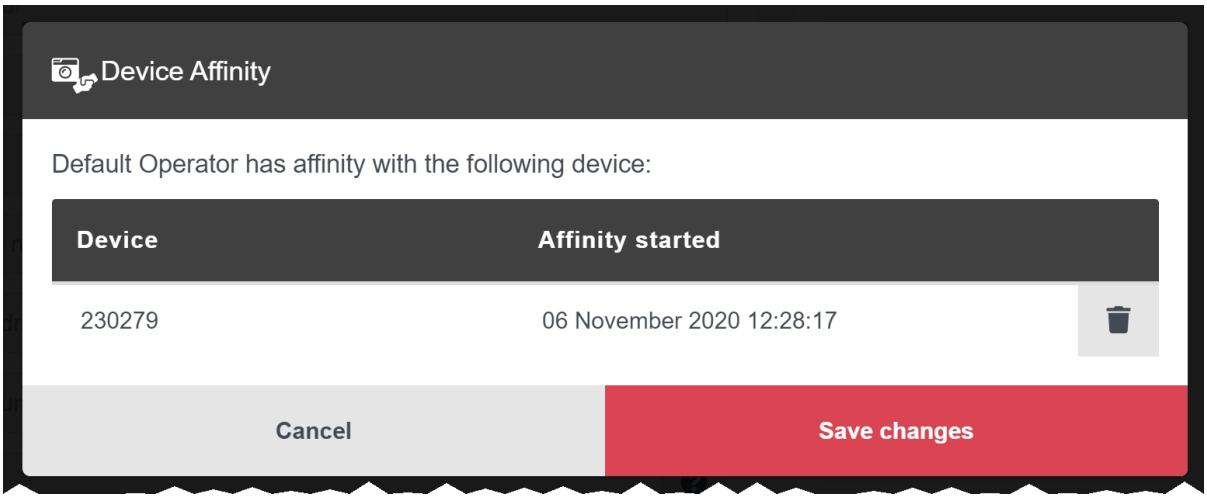
- All users and groups which are in the CSV file but not on VideoManager will be added.
- All users and groups whose data in the CSV file does not match the data on VideoManager will be updated.
- All users and groups which are on VideoManager but not in the CSV file will be deleted.

The administrator can also import the CSV file into a **new** instance of VideoManager. This will copy the database at the time of export, and may be useful if the administrator does not want to configure the built-in user import tool. To do so, follow the same procedure for importing users and groups as outlined above; however, the administrator must also ensure that the roles on the new instance of VideoManager match the roles in the CSV file. If the roles in the CSV file do not match the role names on the new instance of VideoManager, the import job will fail.

To export a role, navigate to the ***Admin*** tab, select the ***People*** pane, and click the ***Roles*** section. Click ***Export role***. On the new instance of VideoManager, navigate to the same place, and click ***Import role***.

9.1.5 View and Clear Device Affinities for a User

If ***Enable shift-long field trips*** has been set to ***On*** from the ***Devices*** section, then all users who have been assigned a body-worn camera with single issue (either with RFID or through VideoManager) will have an affinity with their body-worn camera. This means that if they dock their body-worn camera in the middle of their shift, VideoManager will make a note of the connection and allow them to undock the same body-worn camera later in the shift. Administrators can view these affinities from the ***Edit user*** pane.



To view device affinities for a user:

1. Navigate to the ***Admin*** tab.
2. Select the ***People*** pane.
3. Click the ***Users*** section.
4. Next to the relevant user, click ***Go to user***.
5. Click ***View device affinity***.

The ***Device Affinity*** window will open. This window will show all body-worn cameras which have been associated with the user via single issue (either with RFID or through VideoManager), undocked, and then redocked again.

This window may be empty for one of the following reasons:

- The body-worn camera has not been docked yet.

The affinity is not created until the body-worn camera is docked within the user's shift for the first time.

- The body-worn camera was assigned to the user with permanent issue - this does **not** create an affinity between the user and the body-worn camera, because the same body-worn camera will always be associated with the user anyway.
- Once the body-worn camera was redocked, it charged fully.
- Once the body-worn camera was redocked, it was manually unassigned by an administrator.

- The shift has elapsed (as determined from the ***Devices*** section of the ***Devices*** pane, in the ***Admin*** tab).

6. If the administrator clicks ***Clear***, the affinity will be cleared.

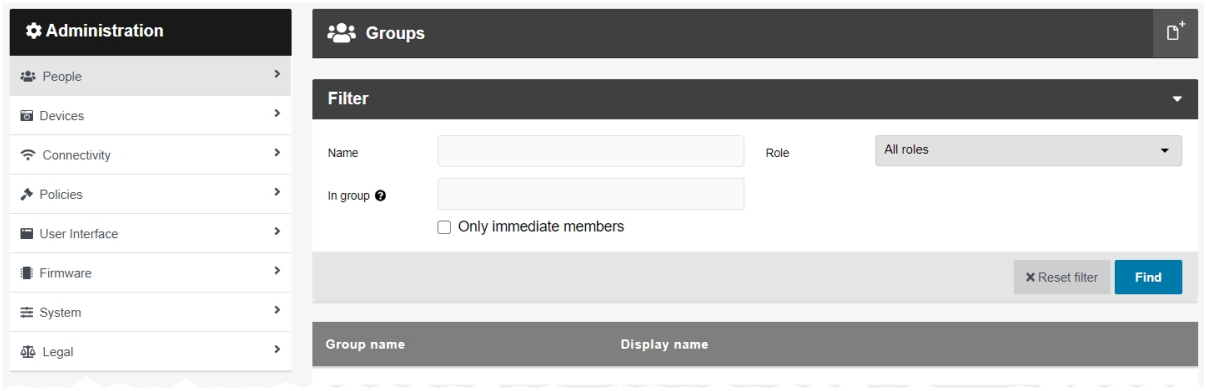
This means that, if the user docks the body-worn camera during their shift, the body-worn camera will return to the pool and must obey the configured battery requirements before it can be used. The user must either swipe their RFID card again, or have another body-worn camera assigned to them on VideoManager, before they can record more footage during their shift.

>> For more information, see Configure Device Settings on page 207

Click ***close*** to return to the ***Edit user*** pane.

9.1.6 Create, Edit and Delete Groups

Administrators can create groups which will associate certain users with each other. This may be necessary if an organisation wishes to share certain videos or incidents with lots of users at once, or if certain users should supervise other users. Groups can be members of groups themselves. This is done from the ***Groups*** section of the ***People*** pane, in the ***Admin*** tab.



To create a group, to which users (or other groups) can be added:

1. Navigate to the ***Admin*** tab.
2. Select the ***People*** pane.
3. Click the ***Groups*** section.
4. Click ***Create group***.
5. In the ***Group name*** field, enter a name for the group.

This cannot be edited later.

6. In the ***Display name*** field, enter a display name for the group.

Caution

*A group cannot have the same name as an existing user or group on the system. However, a group and user **can** have the same display name.*

7. In the ***Roles*** pane, enable the pre-existing roles which will apply to all users in this group.

Caution

*This will **not** add all users which inhabit the role to the group.*

8. In the ***Group memberships*** pane, enter the names of the groups which this group will belong to. Click + to add the user or group.

Administrators can also add individual users to groups. This should be done from the user's page.

>> For more information, see Create, Edit, and Delete Users on page 165

9. In the ***Sharing*** pane, the configurable fields are as follows:

   - **Auto share with** - any users or groups entered here will have access to **all** videos, incidents, and exports created by the group. Click + to add the group.

   Users in a group cannot see who their videos are auto-shared with, or if they are auto-shared at all.

   If group A auto shares with a user, then every user in group A shares their incidents with that user.

   If group A auto shares with group B, then every user in group A auto shares their incidents with every user in group B.

   - **For new videos, create shares for** - any users or groups entered here will also be **automatically** entered into the **Shared:** field of new videos recorded by the users within this group. Click + to add the user or group.

   This is useful if certain users or groups should have access to videos recorded by the users in this group, but should **not** have access to all of their exports or incidents, which **Auto share with** would grant.

   - **For new incidents, create shares for** - any users or groups entered here will also be **automatically** entered into the **Shared:** field of new incidents created by users in the group. Click + to add the user or group.

   This is useful if certain users or groups should have access to incidents created by users in the group, but should **not** have access to all of their exports or videos, which **Auto share with** would grant.

   - **Supervisor of** - this determines which users and groups are supervised by this group.

   If group A supervises a user, then every user in group A supervises that user.

   If group A supervises group B, then every user in group A supervises every user in group B.

   This supervision applies to incidents, exports, and body-worn cameras.

10. In the ***WiFi networks*** pane, optionally create user-specific WiFi networks which will only be available to all users in this group.

    This may be necessary if all users in a group will be live streaming footage with their body-worn cameras, over a specific hotspot.

11. Click ***Create group***.

    After a group has been created, other users and groups can be added to it.

>> For more information, see Create, Edit, and Delete Users on page 165

Administrators can edit an existing group. To do so:

1. Navigate to the ***Admin*** tab.
2. Select the ***People*** pane.
3. Click the ***Groups*** section.
4. Locate the group to be edited. Administrators can filter groups in the following ways:
   - A group's name (both username and display name) - enter their username or display name in the ***Name*** field. Click ***Find*** to find the groups, or click ✕ to reset the filter.
   - Group - enter a group name in the ***In group*** field. Click ***Find*** to find the groups, or click ✕ to reset the filter.

   *If the user enters a group name in the **In group** field, they will have the option to change whether **Only immediate members** is set to **On** or not. If set to **On**, only groups which are assigned directly to the specified group will be returned (as opposed to if group A is assigned indirectly to group B because A belongs to group C, which is assigned to group B).*

   - A group's role - from the ***Role*** dropdown, select the relevant role. All groups which inhabit that role will be returned. Click ***Find*** to find the groups, or click ✕ to reset the filter.
5. Next to the group to be edited, click > ***Go to group***.
6. Make the necessary changes, and click ***Save group***.

If a group becomes redundant, it can be deleted. Deleting a group will **not** delete any of the users within it. Instead, it will immediately affect what those users can see on VideoManager, and to which videos/exports/incidents they have access. To delete a group:

1. Navigate to the ***Admin*** tab.
2. Select the ***People*** pane.
3. Click the ***Groups*** section.
4. Locate the group to be deleted. Administrators can filter groups in the following ways:
   - A group's name (both username and display name) - enter their username or display name in the ***Name*** field. Click ***Find*** to find the groups, or click ✕ to reset the filter.

- Group - enter a group name in the ***In group*** field. Click ***Find*** to find the groups, or click ✕ to reset the filter.

---

*If the user enters a group name in the **In group** field, they will have the option to change whether **Only immediate members** is set to **On** or not. If set to **On**, only groups which are assigned directly to the specified group will be returned (as opposed to if group A is assigned indirectly to group B because A belongs to group C, which is assigned to group B).*

- A group's role - from the ***Role*** dropdown, select the relevant role. All groups which inhabit that role will be returned. Click ***Find*** to find the groups, or click ✕ to reset the filter.

5. Next to the group to be deleted, click > ***Go to group***.
6. Click 🗑 ***Delete Group***.

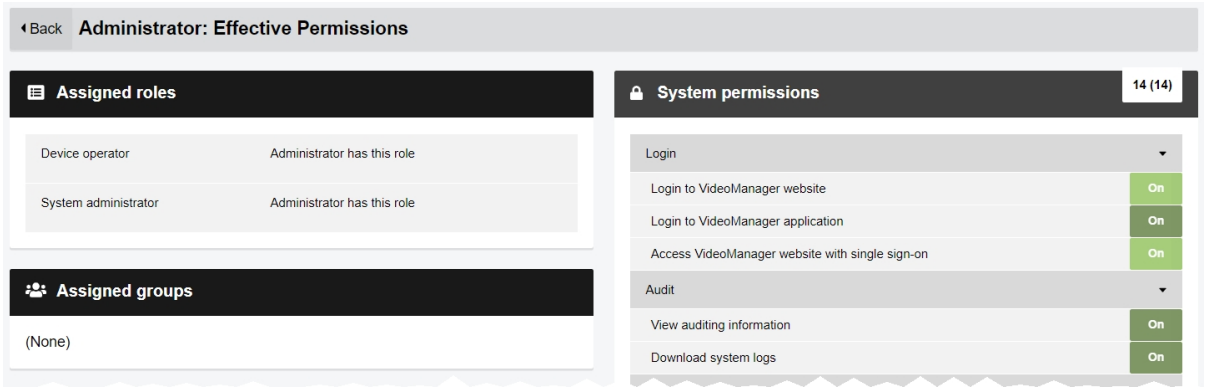
A confirmation window will open.

7. Click ***yes***.

If users belonged to the deleted group, their permissions and abilities will be altered immediately, depending on how the group was configured. This could mean that the users no longer inhabit certain roles, or no longer have access to other users' videos/exports/incidents.

9.1.7 View a User or Group's Effective Permissions

Once a user or group has been created, their effective permissions can be viewed. This will give administrators insight into how the user or group's permissions and roles interact with each other.



To view a previously-created user or group's effective permissions:

1. Navigate to the ***Admin*** tab.
2. Select the ***People*** pane.
3. Click either the ***Users*** or ***Groups*** section.
4. Click ***Go to user*** or ***Go to group*** next to the relevant user or group.
5. Click ***View effective permissions***.

The following information will now be viewable:

- ***Assigned roles*** - for a user, this shows the roles they inhabit, and how they got those roles (i.e. whether the user itself has the role, or whether it belongs to a group which has the role).

For a group, this shows the roles every user in the group will inhabit, and how they got those roles (i.e. whether the group itself has the role, or whether it belongs to another group which has the role).

- ***Assigned groups*** - for a user/group, this shows the groups they belong to, if any.
- ***Assigned WiFi networks*** - for a user/group, this shows which user-specific WiFi networks they have been assigned, if any.

If the user-specific WiFi networks will not be included in the default WiFi profile on VideoManager (because ***User-specific networks*** has been set to ***Off***), a warning will appear alerting the administrator to this fact.

This is relevant because body-worn cameras assigned via single issue (with RFID) and permanent allocation will automatically use the default WiFi profile. If user-specific WiFi networks are not enabled for the default WiFi profile, these body-worn cameras cannot use them to live stream footage.

- ***Device profiles*** - this shows the user/group's device profiles. The user could have these device profiles because:
    1. The user has a role, with which the device profiles are associated.
    2. The user is assigned to a group which has the role, with which the device profiles are associated.

The group could have these device profiles because:

1. The group has a role, with which the device profiles are associated.
2. The group is assigned to another group which has the role, with which the device profiles are associated.

Default device profiles are marked with ★ . The default device profiles will be automatically presented when the user is assigning a body-worn camera.

- ***Permissions*** - for a user/group, this pane on the right-hand side shows their sum total of permissions. The user could have these permissions because:
    1. The user has a role, which contains the permissions.
    2. The user is assigned to a group which has the role, which contains the permissions.

The group could have these permissions because:

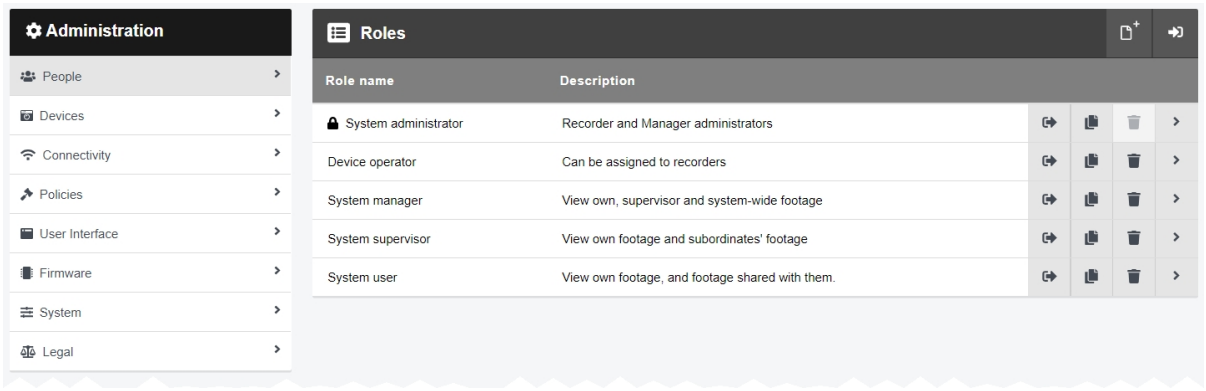
1. The group has a role, which contains the permissions.
2. The group is assigned to another group which has the role, which contains the permissions.

*Users within this group will have these permissions **in addition** to the permissions they would have anyway from the roles they inhabit.*

6. Click ***Back*** to return to the ***Users*** or ***Groups*** section.

9.1.8 Create, Edit, Copy, Import, Export and Delete Roles

A role is a collection of permissions within VideoManager, which can then be assigned to users. Because of this, roles determine what actions users can take on VideoManager, and what aspects of the UI they can see. Each user can have several roles assigned to them. This is done from the ***Roles*** section of the ***People*** pane, in the ***Admin*** tab.



VideoManager provides the following default roles:

- ***System Administrator*** - users assigned to this role can access all aspects of the VideoManager UI (e.g. deleting incidents, creating other users, etc.).
- ***Device Operator*** - users assigned to this role can record videos. They cannot perform any other actions on VideoManager, and cannot log in.
- ***System User*** - users assigned to this role can view their own videos, and videos shared with them. They cannot operate body-worn cameras, or access the ***Admin*** tab.
- ***System Supervisor*** - users assigned to this role can view their own videos and those recorded by users they are supervising. They cannot operate body-worn cameras, or access the ***Admin*** tab.
- ***System Manager*** - users assigned to this role can view all videos on VideoManager. They can also assign body-worn cameras and perform actions on incidents.

Every default role except ***System Administrator*** can be edited manually. However, users may find it necessary to create their own roles, tailored to their workflow. Creating unique roles is a simple process.

To create a role:

1. Navigate to the ***Admin*** tab.
2. Select the ***People*** pane.
3. Click the ***Roles*** section.
4. Click ***Create role***.
5. In the ***Name*** field, enter a name for this role.

6. In the ***Description*** field, enter a description for this role.

7. From the + ***Default device profiles*** dropdown, administrators can select which previously-created device profiles will apply to body-worn cameras which have been assigned to users in this role.

Body-worn cameras assigned with RFID will use this device profile automatically. If body-worn cameras are assigned manually, users can override this device profile if they have the correct permissions.

The administrator should choose a device profile for each body-worn camera family (VB400, VB100 / VB200 / VB300, and VT-series cameras). If they do not, the default device profile will be used.

If a user belongs to multiple roles, but all of the roles' device profiles are set to the system default except one, the one which is **not** the system default will be used.

If a user belongs to multiple roles, but some of the roles' device profiles aren't set to the system default, the device profile which is **highest** in the device profile list (apart from the default profile) will be used.

*This list can be reordered from the **Device Settings** section of the **Devices** pane, in the **Admin** tab. From here, users can also change the system default device profile.*

8. Set additional options for the new role using the following toggles:

   - If ***Add new users to this role?*** is set to ***On***, any new users created on VideoManager from now onwards will automatically inhabit this role.
   - If ***Use alternate password complexity?*** is set to ***Yes***, the users in this role must set a password which conforms to the alternate password rules, instead of the normal password rules.

>> For more information, see Configure Password Complexity on page 257

   - From the ***Role assignment tier*** dropdown, select which tier this role will belong to. By default, roles will belong to tier 1. Users can only add other users to roles which are in **the same tier or lower** as their own roles.

For example, if user A's role is in tier 2, then they can only add other users to roles which are also in tier 2, or lower. This means they cannot add other users - or themselves - to roles which are in tier 1.

*Even users with the **Assign higher privileges** permission will not be able to add other users to roles which are in a higher tier than their own role.*

   - ***Two factor authentication*** - if two factor authentication has already been configured, administrators can configure whether users in this role must scan a QR code with their phone before they can log in to VideoManager.

>> For more information, see Enable and Configure Two Factor Authentication on page 188

- ***Requires privilege elevation?*** - although some aspects of role elevation can be configured from this pane, it is a multi-step process.

>> For more information, see Configure Privilege Escalation on page 390

9. Configure permissions for the role. This will determine what actions users in this role can perform.

>> For more information, see on page 186

10. Click ***Create role*** to save the role.

Roles can also be copied. This will duplicate the entire role except its name. Copying a role is useful if the administrator wants to create many similar roles on their instance of VideoManager. To do so:

1. Navigate to the ***Admin*** tab.
2. Select the ***People*** pane.
3. Click the ***Roles*** section.
4. Next to the role to be copied, click ***Copy role***.

The role will be copied and opened for editing, with the ***Name*** field left blank.

Caution *It is not possible to create two roles with the same name.*

5. Click ***Create role*** to save the changes.

It may be necessary to edit a role if the responsibilities of a user have changed, or if their device profile should be altered. To do so:

1. Navigate to the ***Admin*** tab.
2. Select the ***People*** pane.
3. Click the ***Roles*** section.
4. Next to the role to be edited, click ***Go to role***.

Administrators can edit the properties (***Name***, ***Description***, and ***Default device profiles***) and permissions of a role.

5. Click ***Save role***.

It may be necessary to delete a role if it has become obsolete. To do so:

1. Navigate to the ***Admin*** tab.
2. Select the ***People*** pane.
3. Click the ***Roles*** section.
4. Next to the role to be deleted, click ***Delete role***.

A confirmation window will open. This will alert the administrator if there are users associated with the role.

5. Click ***yes***.

Caution

*If users are associated with the role in question, their ability to use VideoManager may be compromised once it has been deleted. If the deleted role was the user's **only** role, they will be unable to access VideoManager until they have been assigned a new role.*

9.1.8.1 Enable and Disable Permissions

A permission is an individual rule which determines the actions users can perform on VideoManager.

There is a comprehensive list of all permissions in the appendix section.

>> For more information, see Appendix A: Permissions on page 414

A user's permissions are the union of their roles. This means that if a user belongs to two roles, one of which has the permission ***Log in to VideoManager application*** set to ***On*** and one which has it set to ***Off***, that user will still be able to log in. There are no permissions which deny an action - only the absence of permissions denies actions.

The groups of permissions are as follows:

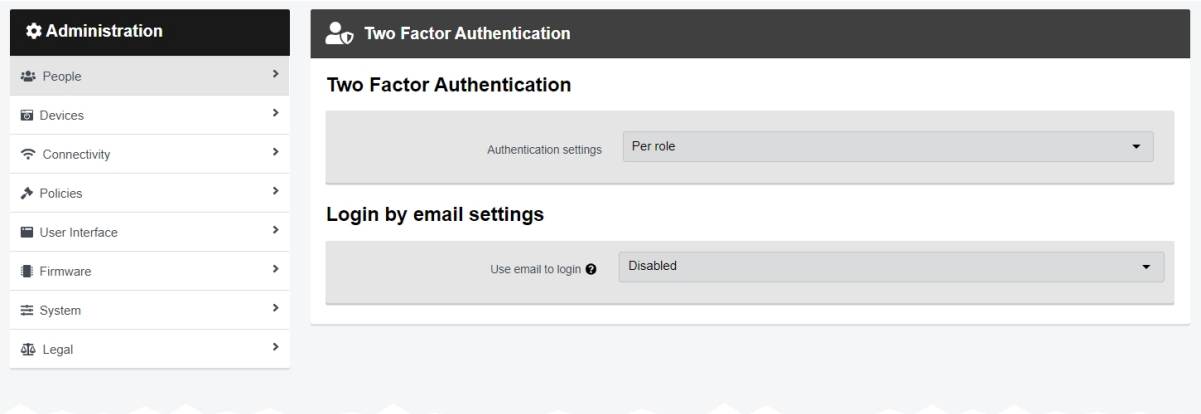
- System permissions - these permissions control users' abilities to log in to VideoManager, as well as their audit and export abilities.
- Video permissions - these permissions control users' abilities regarding videos. The permissions are also sorted by the following criteria:
  - **Owned** - if enabled, users can perform actions on the videos recorded by them.
  - **Shared** - if enabled, users can perform actions on the videos that have been shared with them by other users on the system.
  - **Supervised** - if enabled, users can perform actions on the videos that have been recorded by other users on the system that they supervise.
  - **Any** - if enabled, users can perform actions on any videos on the system, regardless of who recorded them.
- Incident permissions - these permissions control users' abilities regarding incidents. The permissions are also sorted by the following criteria:
  - **Owned** - if enabled, users can perform actions on the incidents created by them.
  - **Shared** - if enabled, users can perform actions on the incidents that have been shared with them by other users on the system.
  - **Supervised** - if enabled, users can perform actions on the incidents that have been created by other users on the system that they supervise.
  - **Any** - if enabled, users can perform actions on any incidents on the system, regardless of who created them.
- Device permissions - these permissions control users' abilities regarding body-worn cameras. The permissions are also sorted by the following criteria:
  - ***User*** - if enabled, users can perform actions on the body-worn cameras assigned to them.

- ***Supervised*** - if enabled, users can perform actions on the body-worn cameras that are assigned to them or other users on the system that they supervise.
- ***Any*** - if enabled, users can perform actions on any body-worn camera on the system.

- User permissions - these permissions control users' abilities regarding other users. The permissions are also sorted by the following criteria:
  - **Supervised** - if enabled, users can perform actions on the users on the system that they supervise.
  - **Any** - if enabled, users can perform actions on any user on the system.
- Notification permissions - these permissions control how notifications work (if they have been licensed).
- Report permissions - these permissions control users' abilities to create reports and view statistics.
- Field permissions - these permissions dictate the access groups to which users belong. This affects which saved searches and user-defined incident fields they can see.
- Advanced permissions - these permissions control users' abilities regarding advanced aspects of VideoManager. The permissions are also sorted by the following criteria:
  - **View** - if enabled, users can view advanced aspects of VideoManager.
  - **Edit** - if enabled, users can edit advanced aspects of VideoManager.

9.1.9 Enable and Configure Two Factor Authentication

By default, users log in to VideoManager with their username and unique password. If an organisation needs an extra layer of security, two factor authentication can be enabled and configured - this prompts users to scan a QR code with their phones, and enter the corresponding code into VideoManager. This is done from the ***Two Factor Authentication*** section of the ***People*** pane, in the ***Admin*** tab.



Before individual users can utilise two factor authentication to log in, it must be enabled on VideoManager. To do so:

1. Navigate to the ***Admin*** tab.
2. Select the ***People*** pane.
3. Click the ***Two Factor Authentication*** section.
4. From the ***Authentication settings*** dropdown, administrators can select how two factor authentication behaves on VideoManager. The options are as follows:
   - **Mandatory** - two factor authentication is mandatory for every user on this instance of VideoManager, regardless of whether it is disabled for individual roles or not.
   - **Per role** - two factor authentication is determined on a role-by-role basis.

   If this setting is selected, the administrator must enable two factor authentication for individual roles.

   >> For more information, see on the next page

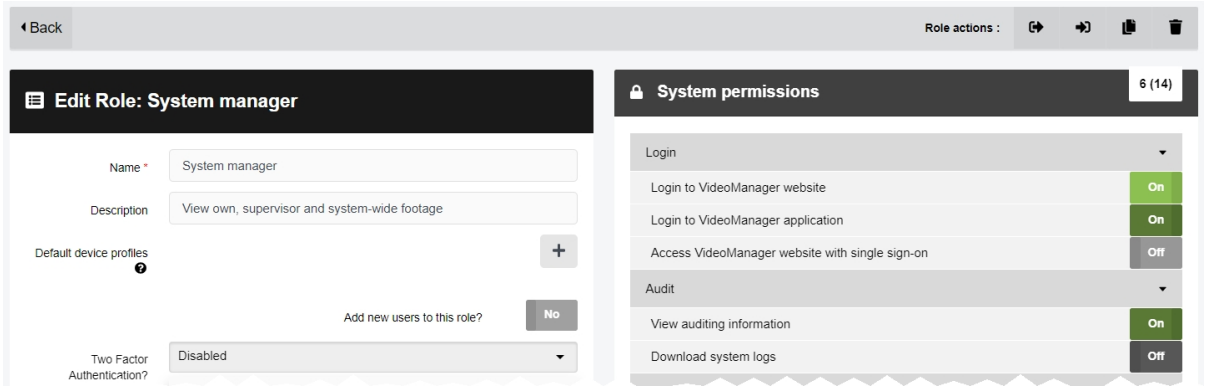
   - **Disabled** - two factor authentication is disabled for this entire instance of VideoManager.
5. Click ***Save settings***.

Every user which is affected by the two factor authentication settings will be prompted to associate their phone with VideoManager the next time they log in.

>> For more information, see on page 190

9.1.9.1 Configure Two Factor Authentication For Roles

If two factor authentication has been set to ***Per role*** from the ***Login Settings*** section, administrators must now manually enable two factor authentication for individual roles. This is done from the ***Roles*** section of the ***People*** pane, in the ***Admin*** tab.



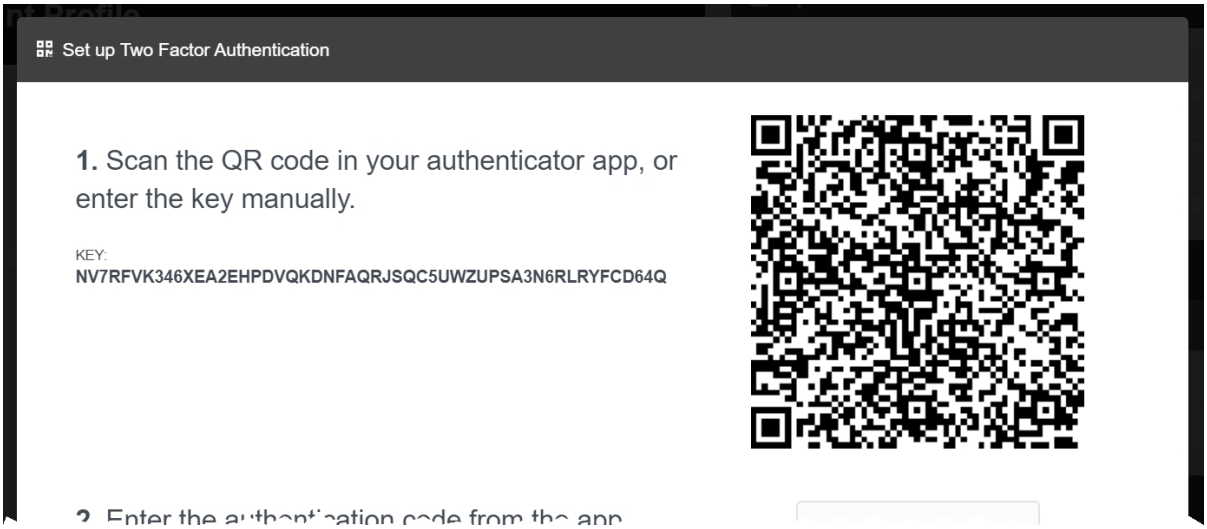
To configure two factor authentication on a per-role basis:

1. Navigate to the ***Admin*** tab.
2. Select the ***People*** pane.
3. Click the ***Roles*** section.
4. Next to the role to be edited, click ***Go to role***.
5. From the ***TOTP two-factor authentication*** dropdown, administrators can configure the two factor authentication settings which will affect all users in this role. The options are as follows:
   - **Mandatory** - two factor authentication is the only function that a user in this role can perform when they first log in, and every login after that will require a 6-digit code to be entered as provided to the user via an app.
   - **Optional** - the user will not be required to go through two factor authentication when initially logging in. However, they can enable it from their ***Account Profile*** page once they are logged in to VideoManager.
   - **Disabled** - two factor authentication is not requested upon first login, and users cannot enable it from their ***Account Profile*** page.

   If a user inhabits two roles with contrasting two factor authentication rules - for example, one is set to **Disabled** *and one is set to* **Mandatory** *- the user will still need to utilise two factor authentication.*
6. Click ***Save role***.

9.1.9.2 Use Two Factor Authentication

Once two factor authentication has been configured, all users affected by it must configure their phones so they work with VideoManager. Users must configure their phones if they belong to a role which has had ***TOTP two-factor authentication*** set to **Mandatory**, or if ***Authentication settings*** has been set to **Mandatory** for the entirety of VideoManager.



To set up two factor authentication:

1. Download an authenticator app onto a phone - Motorola Solutions recommends **Google Authenticator**.
2. Log in to VideoManager as normal.
3. Users will immediately be asked to set up two factor authentication - click ***Set up*** to begin.
4. A QR code will appear on the screen. Using the authenticator app, users can either scan the code directly, or manually type in the key.
5. The authenticator app will provide a 6-digit code. Users should enter this code into the field on VideoManager.
6. Click ***Complete Set Up***.

Now, whenever the user logs in, they will be asked to provide another 6-digit code from the authenticator app on their phone. They do **not** need to re-scan a QR code.

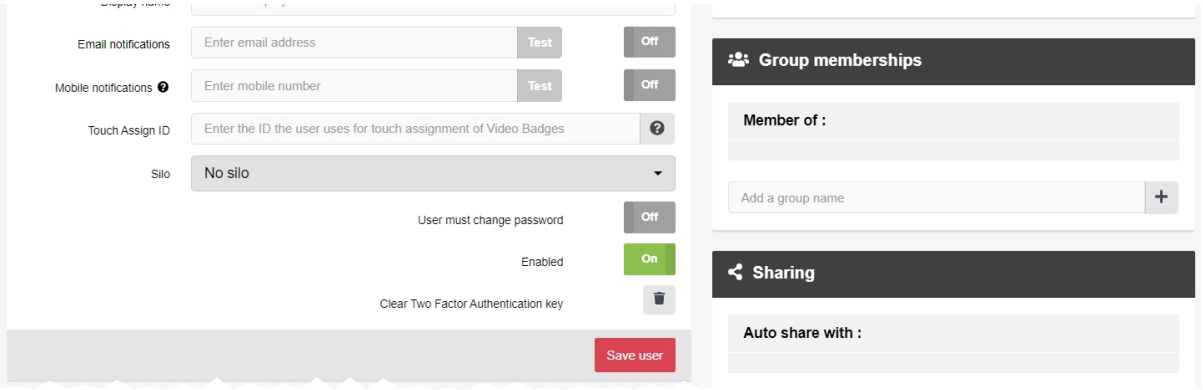
If the user gets a new phone, they must repeat the process of associating it with VideoManager. To do so:

1. Navigate to the ***Account Profile*** tab.
2. In the ***Two Factor Authentication*** pane, click ***Generate new authentication code***.

A new QR code will be created, which users should scan with the phone to be associated with VideoManager.

9.1.9.3 Reset a Two Factor Authentication Key

If a user has lost their phone and therefore cannot use two factor authentication to log in to VideoManager, an administrator must reset their two factor authentication key for them.



To reset a two factor authentication key:

1. Ensure that the administrator is in a role where the ***Clear Two Factor Authentication*** permission has been set to ***On***.

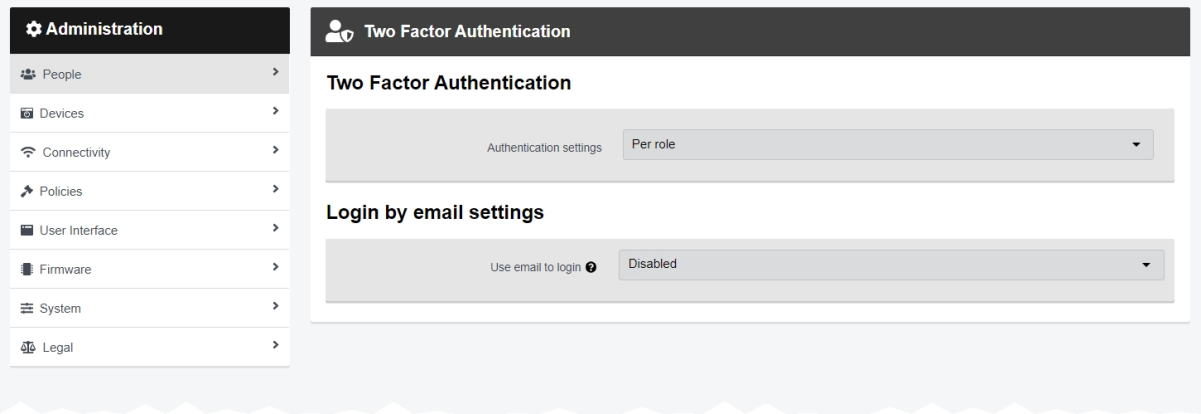
>> For more information, see on page 186

2. Navigate to the ***Admin*** tab.
3. Select the ***People*** pane.
4. Click the ***Users*** section.
5. Next to the user who has lost their phone, click ***Go to user***.
6. Click ***Clear authentication key***.
7. Click ***Save user***.

Next time the user logs in, they will be prompted to scan a new QR code.

9.1.10 Enable and Configure Login by Email

By default, users log in to VideoManager with their unique username and password. If an organisation needs an extra layer of security, administrators can enable and configure email login - users must still enter their password like normal, but they must also click a link sent to their email inbox. They will only have access to VideoManager once they have completed both of these actions. This configuration is done from the ***Two Factor Authentication*** section of the ***People*** pane, in the ***Admin*** tab.



Before individual users can utilise their email to log in, email logins must be enabled on VideoManager. To do so:

1. Ensure email settings have been enabled and configured from the ***Email Properties*** section of the ***Connectivity*** pane, in the ***Admin*** tab.

>> For more information, see Configure Email Properties on page 230

2. Navigate to the ***Admin*** tab.
3. Select the ***People*** pane.
4. Click the ***Two Factor Authentication*** section.
5. From the ***Use email to login*** dropdown, administrators can select which users will be affected by email login. The options are as follows:

   - **Mandatory** - login by email is mandatory for every user on this instance of VideoManager, regardless of whether it is disabled for individual roles or not.

   If this setting is selected, the administrator must ensure that **all** users on VideoManager are associated with an email address, or they will be unable to log in.

   - **Per role** - login by email is determined on a role-by-role basis.

   If this setting is selected, the administrator must enable email login for individual roles.

6. In the ***Email subject template*** and ***Email content template*** fields, the administrator can configure the format of the email that users will receive when they try to log in. Possible variables are as follows:

- `{siteName}` - this corresponds to *Motorola Solutions VideoManager*.
- `${siteUrl}` - this is VideoManager's name (e.g. *194.168.76.230*).
- `${siteHost}` - this is VideoManager's public address (e.g. *http://194.168.76.230:9080/*).
- `${loginUrl}` - this is the link which users must click to log in.

Caution *If `${loginUrl}` is not included in the email, users **will not be able to log in**.*

- `${expirationTime}` - this is the length of time that the link is valid for, as configured in the ***Verification expiry time*** field.

7. In the ***Verification expiry time*** field, the administrator can configure how long a login link is valid for.
8. Click ***Save settings***.

If administrators have selected **Per role** from the dropdown, they must now enable email login for individual roles. If **Mandatory** was selected instead, go straight to the next step. To configure email login on a per-role basis:

1. Navigate to the ***Admin*** tab.
2. Select the ***People*** pane.
3. Click the ***Roles*** section.
4. Next to the role to be edited, click ***Go to role***.
5. Set ***Send a link by email to complete login*** to ***Yes***.
6. Click ***Save role***.
7. Repeat for as many roles as necessary.

The administrator must ensure that all users which are affected by email login (either because they are in a role where email login has been enabled, or because email login has been enabled for all users on VideoManager) have an email address associated with them on VideoManager. To add an email address to a user's profile:

1. Navigate to the ***Admin*** tab.
2. Select the ***People*** pane.
3. Click the ***Users*** section.
4. Locate the user to be edited. Administrators can filter users in the following ways:
   - A user's name (both username and display name) - enter their username or display name in the ***Name*** field. Click ***Find*** to find the users, or click ✕ to reset the filter.

- A user's group - enter a group name in the ***In group*** field. Click ***Find*** to find the users, or click ✕ to reset the filter.

*If the user enters a group name in the **In group** field, they will have the option to change whether **Only immediate members** is set to **On** or not. If set to **On**, only users which are assigned directly to the specified group will be returned (as opposed to if user A is assigned indirectly to group B because A belongs to group C, which is assigned to group B).*

- A user's role - from the ***Role*** dropdown, select the relevant role. All users who inhabit that role will be returned. Click ***Find*** to find the users, or click ✕ to reset the filter.

5. Next to the user to be edited, click > ***Go to user***.
6. In the ***Email notifications*** field, enter the email address which will be sent login links for this user.
7. Click ***Save user***.

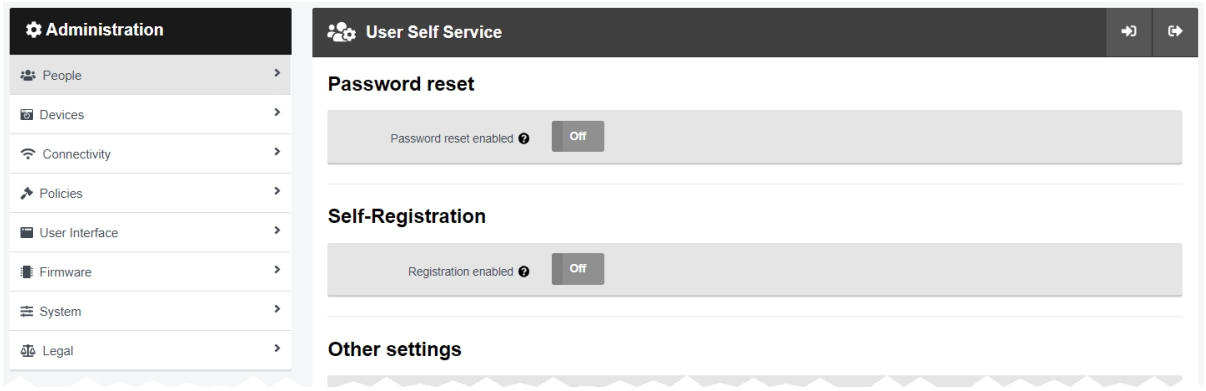
From now on, whenever users try to log in to VideoManager, a link will be sent to their email inbox. They must click this link **in the same browser** which has VideoManager open. The link will only work once; to request a new code, users must re-enter their password on VideoManager and try to log in again.

Administrators can disable login by email once it has been enabled. To do so:

1. Navigate to the ***Admin*** tab.
2. Select the ***People*** pane.
3. Click the ***Two Factor Authentication*** section.
4. From the ***Use email to login*** dropdown, select **Disabled**.
   From now on, users only need to enter their password to log in.
5. Click ***Save settings***.

9.1.11 Configure User Self Service

It is possible to administer users manually from the ***Users*** section - this includes creating new users, and resetting existing users' passwords. However, it is also possible for workers to create their own users and reset their own passwords. This is done from the ***User Self Service*** section of the ***People*** pane, in the ***Admin*** tab.



The actions which administrators can perform from this section are as follows:

- Enable previously-existing users to reset their own passwords.

>> For more information, see on the next page

- Enable workers to create their own user profiles on VideoManager.

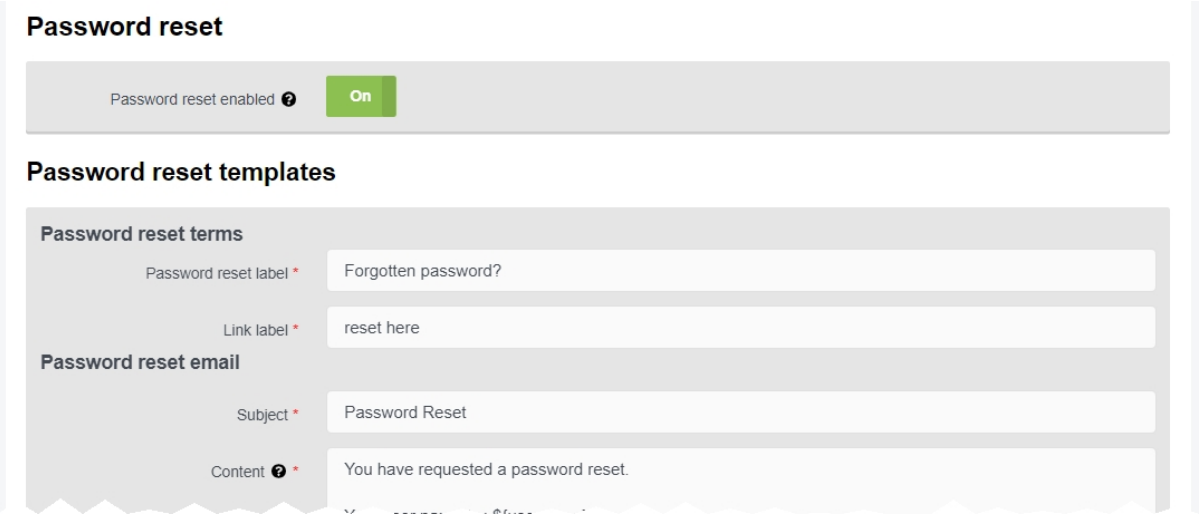
>> For more information, see on page 198

Both password resetting and self-service registration are conducted through links sent via email. From the ***User Self Service*** section, administrators can configure for how many minutes these links are valid. To do so:

1. Navigate to the ***Admin*** tab.
2. Select the ***People*** pane.
3. Click the ***User Self Service*** section.
4. In the ***Verification expiry time (mins)*** field, enter the number of minutes after which a link will expire and must be re-sent.
5. Click ***Save settings***.

9.1.11.1 Enable Users to Reset Their Own Passwords

All users on VideoManager must have a password to log in. If they forget this password, administrators can reset it for them. However, if configured, users can also reset their own passwords via email.



To enable users to reset their own passwords:

1. Ensure that emails have been enabled.

>> For more information, see Configure Email Properties on page 230

2. Navigate to the ***Admin*** tab.
3. Select the ***People*** pane.
4. Click the ***User Self Service*** section.
5. In the ***Password reset*** section, set ***Password reset enabled*** to ***On***.
6. In the ***Password reset templates*** section, configure what users will see from VideoManager's login pane and in the password reset email:
   - In the ***Password reset label*** field, enter the text that users will see on VideoManager's login page if they enter their password incorrectly.

   One example is *Forgotten password?*

   - In the ***Link label*** field, enter the text that users must click in order to send a password reset email. This will be displayed on VideoManager's login page alongside the ***Password reset label*** field.

   Examples include *Reset here* and *Click here*.

   - In the ***Subject*** field, enter the text that will be set as the subject line for the password reset email.
   - In the ***Content*** field, enter the content of the password reset email.

${loginUrl}* and *${completionUrl} can be utilised to direct users to VideoManager's login pane and password reset pane, respectively.

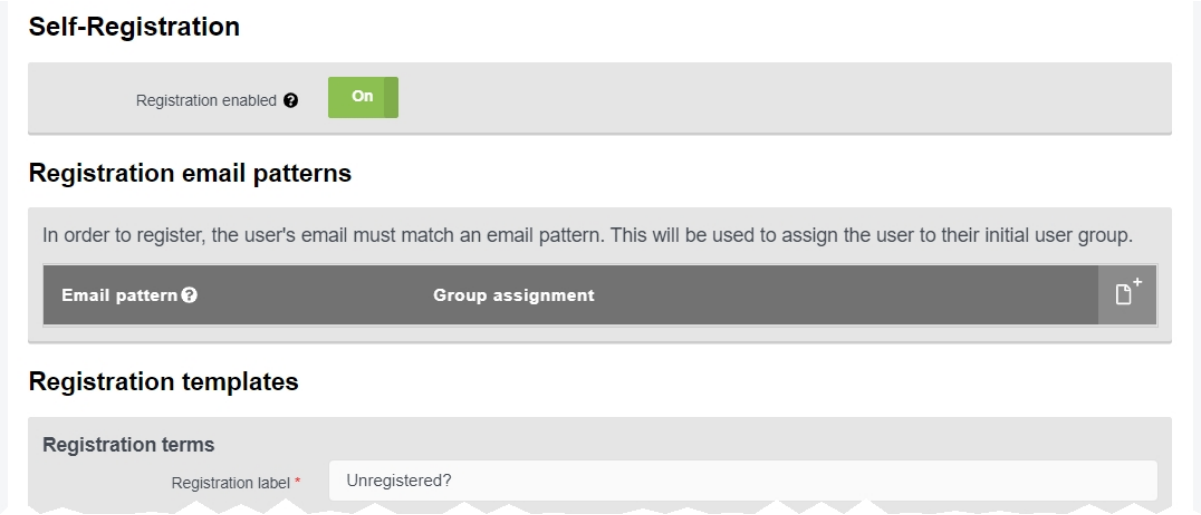
7. Click ***Save settings***.

Users can now reset their passwords if one of two conditions are met:

- If users have been created with self-registration, they can reset their passwords by default because there is an email address associated with their account (their username).
- If users have **not** been created with self-registration (i.e. they have been created manually, or have been imported with the user import tool), an administrator must associate an email address with their account. To do so:
    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 ***Email notifications*** field, enter an email address for the user.
    6. Click ***Save user***.

9.1.11.2 Enable Users to Complete Self-Registration

Every worker who is required to utilise VideoManager must have a unique user profile. Normally, administrators must create these users for them. However, if configured, workers can create their own users.



There are some prerequisites before self-registration can be configured:

1. Ensure that emails have been enabled.

>> For more information, see Configure Email Properties on page 230

2. Ensure that at least one group exists, to which new users can be added.

>> For more information, see Create, Edit and Delete Groups on page 176

To enable and configure self-registration:

1. Navigate to the ***Admin*** tab.
2. Select the ***People*** pane.
3. Click the ***User Self Service*** section.
4. In the ***Self-Registration*** section, set ***Registration enabled*** to ***On***.
5. In the ***Registration email patterns*** section, administrators can configure which email address patterns will be accepted by VideoManager when user creation is requested. Requests from email addresses with patterns not listed here will be ignored. To add an address pattern:
    1. Click ***Add email pattern***.
    2. In the ***Email pattern*** field, enter an email address format.
    3. In the ***Group assignment*** field, enter a previously-existing group, to which all

users with this specific email address format will be added.

4. Click ***create***.

6. In the ***Registration terms*** section, configure what non-registered workers will see from VideoManager's login pane:

   - In the ***Registration label*** field, enter the text that will appear on VideoManager's login pane.

   Examples include *Unregistered?* and *Don't have an account?*.

   - In the ***Link label*** field, enter the text for the link that workers must click in order to send a registration email.

   Examples include *Register here* and *Click here*.

   - In the ***Registration terms*** field, enter the text to which non-registered workers must agree before they can create their new user profile.

   It is possible to customise the text using the following settings (clicking the buttons again will undo the changes):

      - **B** ***Bold*** - any text within the asterisks will appear bold.
      - ***I*** ***Italic*** - any text within the underscores will appear italicised.
      - **H** ***Heading*** - any text on the same line as ### will appear as heading text.
      - ***URL/Link*** - the administrator will be prompted to enter a hyperlink. A link description can be entered in the square brackets.
      - ***Image*** - the administrator can enter a URL for an image. An image description can be entered in the brackets.
      - ***Unordered List*** - any text after the hyphen will appear as part of a bullet point list. ***Unordered List*** must be clicked for each individual list entry.
      - ***Ordered List*** - any text after the hyphen will appear as part of a numbered list. ***Ordered List*** must be clicked for each individual list entry (the numbers will appear in order once the message is previewed).
      - ***Code*** - any text within the single quotation marks will appear as code.
      - ***Quote*** - any text on the same line as > will appear as a quote.

   - By clicking ***Preview***, a previewable version will become visible. To edit the text, click ***Preview*** again.

7. In the ***Welcome email*** section, configure what workers will see when they open VideoManager's welcome email:

- In the ***Subject*** field, enter the text that will be set as the subject line for the welcome email.
- In the ***Content*** field, enter the content of the welcome email.

`${loginUrl}` and `${completionUrl}` can be utilised to direct users to VideoManager's login pane and user profile creation pane, respectively.

`${siteHost}` can be utilised to insert the name of the specific VideoManager instance.

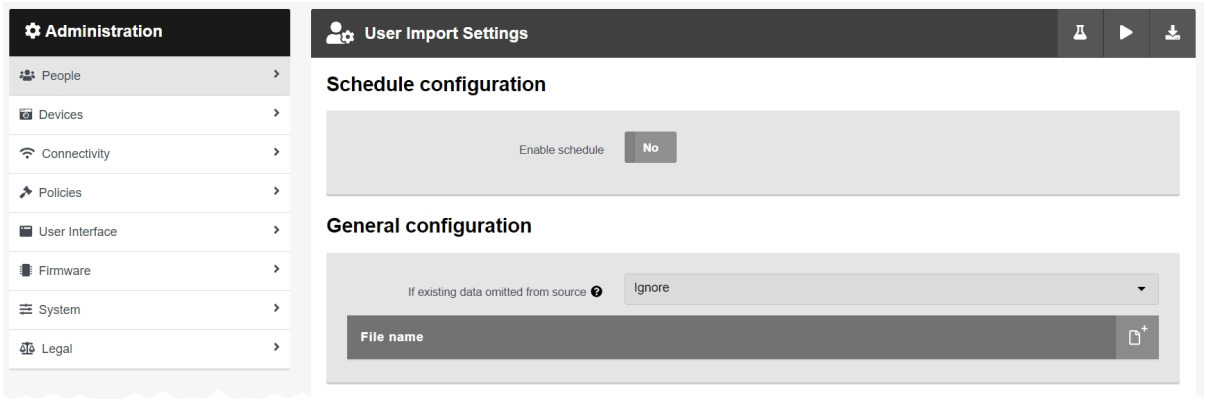
8. In the ***Already registered email*** section, configure what workers will see if an email address they entered for self-registration is already associated with a user on VideoManager:
   - In the ***Subject*** field, enter the text that will be set as the subject line for the email.
   - In the ***Content*** field, enter the content of the email.

   `${loginUrl}` can be utilised to direct users to VideoManager's login pane.

   `${siteHost}` can be utilised to insert the name of the specific VideoManager instance.
9. Click ***Save settings***.

9.1.12 Configure the Built-in User Import Tool

Administrators can import multiple users/groups simultaneously from another instance of VideoManager. This is done from the ***User Import Settings*** section of the ***People*** pane, in the ***Admin*** tab.



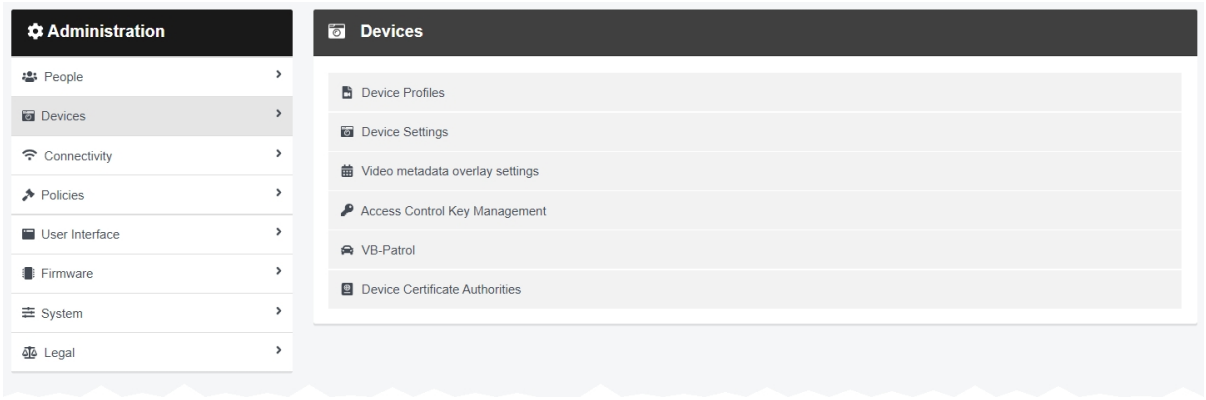
For more information, please see the document *Built-in User Import Tool Guide [ED-012-229]*. This can be found in VideoManager's installation location, in the ***userimporttool*** folder.

Alternatively, administrators can manually export and import their entire user and group database via the ***Users*** section.

>> For more information, see Export and Import Users and Groups on page 172

9.2 Devices

In the ***Devices*** pane, administrators can edit aspects of VideoManager related to body-worn camera configuration.



To access the ***Devices*** pane:

1. Navigate to the ***Admin*** tab.
2. Select the ***Devices*** pane.

From here, administrators can access the following sections:

- ***Device Profiles***

Import, edit, and delete device profiles. These control the way that individual body-worn cameras behave when assigned, depending on the type of body-worn camera they are (i.e. VB400, VB300/VB200/VB100, or VT-series camera).

>> For more information, see Create, Edit, Reorder and Delete Device Profiles on page 204

- ***Device Settings***

Edit global body-worn camera settings. Unlike device profiles, settings configured here apply to **all** body-worn cameras connected to VideoManager, regardless of their type.

>> For more information, see Configure Device Settings on page 207

- ***Video metadata overlay settings***

Edit metadata display settings for all footage on VideoManager. This affects which metadata is recorded alongside videos and subsequently displayed when users watch footage that has been recorded on a body-worn camera.

>> For more information, see Configure Video metadata overlay settings on page 210

- ***Access Control Key Management***

Import, edit, and delete access control keys. Access control keys determine which body-worn cameras can connect to VideoManager - by exporting and importing access control keys, users can access any footage that was still on a body-worn camera when it was moved to a different instance of VideoManager.

>> For more information, see Create, Import, and Export Access Control Keys on page 213

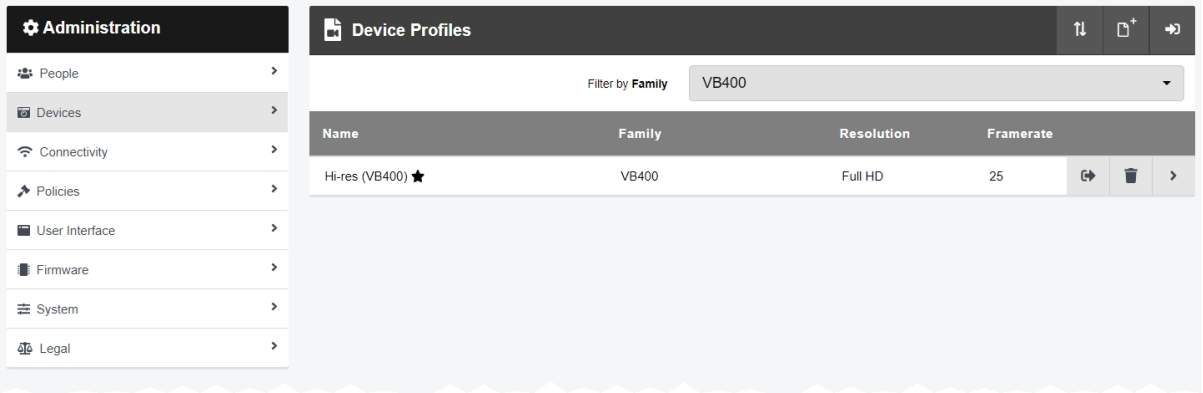
- ***Device Certificate Authorities***

Create, import, export, and delete certificate authorities. These validate videos from VB400s and ensure they have not been tampered with.

>> For more information, see Create, Import, Export, and Delete Device Certificate Authorities on page 216

9.2.1 Create, Edit, Reorder and Delete Device Profiles

Device profiles are used to control the interface between body-worn cameras and VideoManager, as well as the recording behaviour and settings. This is done from the ***Device Profiles*** section of the ***Devices*** pane, in the ***Admin*** tab.



To search for already-created device profiles:

1. Navigate to the ***Admin*** tab.
2. Select the ***Devices*** pane.
3. Click the ***Device Profiles*** section.
4. From the ***Filter by*** dropdown, select one of the following options:
   - **VB400** - this will only show device profiles that are applicable to VB400s.
   - **VB200/300** - this will only show device profiles that are applicable to VB100s/VB200s/VB300s.
   - **VT50/100** - this will only show device profiles that are applicable to VT-series cameras.

   Body-worn camera families which are not present on the administrator's instance of VideoManager will still be presented here as an option in the dropdown.

To create a new device profile:

1. Navigate to the ***Admin*** tab.
2. Select the ***Devices*** pane.
3. Click the ***Device Profiles*** section.
4. Click ***Create profile***.
5. In the ***Name*** field, enter a name for the device profile.

6. From the ***Device family*** dropdown, select to which device family this device profile will apply. The options are as follows:
   - **VB400**
   - **VB200/300**
   - **VT50/100**

Caution *These details cannot be changed later.*

7. Configure the device profile settings.

>> For more information, see Appendix B: Device Profiles on page 443

8. Click ***Save settings*** to save the device profile.

Once a device profile has been created, it can be applied to body-worn cameras. The options are as follows:

- If an operator is obtaining their body-worn camera through **Single Issue** or **Permanent Issue**, they can manually select the device profile when they assign their body-worn camera.

>> For more information, see Assign Body-Worn Cameras and Record Footage on page 110

- If an operator is obtaining their body-worn camera through **Permanent Allocation**, VideoManager will automatically select the system's default device profile, unless the operator is in a role which has a different device profile associated with it.

>> For more information, see Create, Edit, Copy, Import, Export and Delete Roles on page 182

To edit a device profile:

1. Navigate to the ***Admin*** tab.
2. Select the ***Devices*** pane.
3. Click the ***Device Profiles*** section.
4. Find the relevant device profile by selecting a body-worn camera type from the ***Family*** dropdown.
5. Next to the profile to be edited, click ***Go to profile***.
6. Make the relevant changes, and click ***Save settings***.

Administrators can also reorder device profiles. This is necessary if users belong to multiple roles with different assigned device profiles. The device profile which is **highest** in the list here will be the one given to the body-

worn camera. Furthermore, the device profile which is **highest overall** in the list will be the system default. To reorder device profiles:

1. Navigate to the ***Admin*** tab.
2. Select the ***Devices*** pane.
3. Click the ***Device Profiles*** section.
4. Find the relevant device profiles by selecting a body-worn camera type from the ***Family*** dropdown.
5. Click ***Reorder profiles***.
6. Make the necessary changes, and click ***Confirm new order***.

To delete a device profile:

1. Navigate to the ***Admin*** tab.
2. Select the ***Devices*** pane.
3. Click the ***Device Profiles*** section.
4. Next to the device profile to be deleted, click ***Delete profile***.

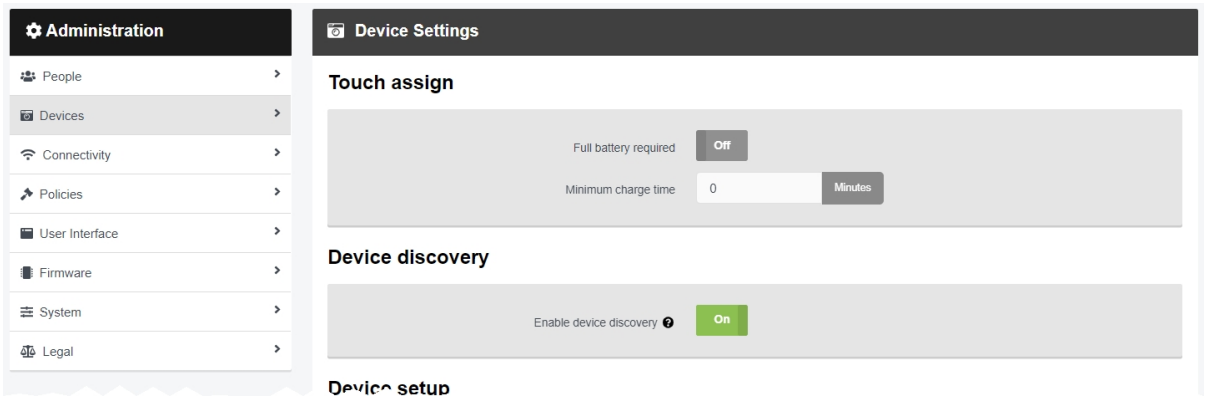
   Any roles which had this device profile as their default will immediately switch back to the VideoManager-wide default.

If an administrator wants to import/export **all** device profiles on VideoManager, they can do so from the ***Import/Export System Config*** section of the ***System*** pane in the ***Admin*** tab.

>> For more information, see Import or Export VideoManager's Configuration on page 356

9.2.2 Configure Device Settings

Administrators can configure settings which apply to all body-worn cameras on VideoManager, regardless of their type. Unlike device profiles, these settings do not need to be applied to body-worn cameras individually - instead, they are automatically applied when a body-worn camera is connected to VideoManager. This is done from the ***Device Settings*** section of the ***Devices*** pane, in the ***Admin*** tab.



To reach the ***Device Settings*** section:

1. Navigate to the ***Admin*** tab.
2. Select the ***Devices*** pane.
3. Click the ***Device Settings*** section.

There are multiple categories of settings which administrators can configure:

In the ***Touch assign*** section, administrators can change whether touch assign is only possible with a full battery.

- If ***Full battery required*** is set to ***On***, only body-worn cameras with a full battery will be eligible for touch assign.

If set to ***Off***, administrators will be given the option to enter a minimum charge time, before which the body-worn camera cannot be assigned by RFID. The exception for this is body-worn cameras which have been permanently allocated to a user - in this case, they can be tapped out by an RFID card even when they have not met the minimum charge time.

In the ***Device discovery*** section, administrators can configure body-worn camera discovery.

- If ***Enable device discovery*** is set to ***On***, VideoManager will discover **all** body-worn cameras which are connected via USB, configured DockControllers, or unconfigured DockControllers.

If set to ***Off***, VideoManager will only discover body-worn cameras which are connected to DockControllers. Any body-worn cameras connected by USB will **not** appear on the ***Devices*** tab.

In the ***Device setup*** section, administrators can configure body-worn camera assignment.

- From the ***Default device assignment mode*** dropdown, select which body-worn camera assignment mode is the default. This saves time when body-worn cameras are being assigned, if one assignment mode is used consistently in an organisation. The

options are as follows:

- **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.

In the **Body-Worn Camera Field Trip***,* **Operator Recorder Summary***, and* **User Summary** *reports, body-worn cameras in this mode will be marked as* ***Unassigned*** *if they have been allocated but not tapped out with an RFID card.*

- If ***Show public QR code bootstrap screen*** is set to ***On***, users have the option to launch a public version of the QR config page when configuring a VT-series camera. This is useful if remote workers do not have access to VideoManager, but still need to assign their body-worn cameras - an administrator can send them the link to the public page, and the remote worker can use it to assign their body-worn cameras from their own office or home.

If set to ***Off***, only users with direct access to VideoManager can assign VT-series cameras via QR code.

>> For more information, see Connect VT-Series Cameras to VideoManager Remotely on page 108

- ***Configure External Application account credentials*** should only be set to ***On*** if directed to do so by Motorola Solutions support.
- In the ***Bluetooth address prefix*** field, administrators can set the range of MAC addresses with which body-worn cameras can pair.

For more information, please contact Technical Support and ask for the technical paper *VideoManager and Tetra Radio Integration Explained [ED-009-062]*.

In the ***Device downloads*** section, administrators can configure how and when body-worn cameras download footage to VideoManager.

- If ***Limit simultaneous downloads to*** is set to ***On***, administrators can set the limit for the number of simultaneous downloads performed by body-worn cameras.

If the download number is set to 10, then only 10 body-worn cameras can download footage to VideoManager simultaneously. Once one body-worn camera finishes downloading, another body-worn camera will take its place.

- If ***Fast download recovery*** is set to ***On***, when a footage download is interrupted and connection is then re-established, it will resume downloading from the same point before connection was broken.

If set to ***Off***, when a footage download is interrupted and connection is then re-established, the download will begin again from the beginning.

In the ***Device properties*** section, administrators can configure their body-worn cameras' battery settings.

- ***Battery life extender*** should only be set to ***On*** if users regularly leave VB300s and VB400s charging in their docks for 24 hours or longer.
- If ***Expect connectivity on charger*** is set to ***On***, VB400s which are charging but cannot connect to VideoManager will restart periodically, in an attempt to connect.

This will improve the reliablility of USB connection to VideoManager, but should be set to ***Off*** if users will be charging their VB400s in the field without connecting to VideoManager (e.g. connected via USB to a PC which does not have VideoManager installed).

In the ***Shift-long field trips*** section, administrators can configure what happens to body-worn cameras which have been assigned to a user, if they are redocked in the middle of a shift:

- If ***Enable shift-long field trips*** is set to ***On***, a body-worn camera assigned to a user will have an affinity with that user once it is redocked in the middle of a shift.

*This does **not** apply to body-worn cameras which have been assigned with permanent issue or permanent allocation, because VideoManager will associate the user to the body-worn camera permanently anyway.*

This means that if an operator redocks their body-worn camera mid-shift and then undocks it later in the shift, VideoManager will automatically assign the same body-worn camera to them, unless one of the following conditions is met:

- The body-worn camera is fully charged.
- The body-worn camera is manually unassigned on VideoManager.
- The shift ends, as determined by the number of hours entered into the ***Maximum shift length*** field.

In the ***Footage signing*** section, administrators can enable footage signing if they have also created or imported a certificate authority from the ***Device Certificate Authorities*** section.

- ***Enable footage signing*** - if set to ***On***, each VB400 will be provided with a certificate which they will use to sign videos. When the videos are downloaded, VideoManager will check that the videos' signatures match the body-worn cameras' certificates, **and** that the body-worn cameras' certificates can be trusted.

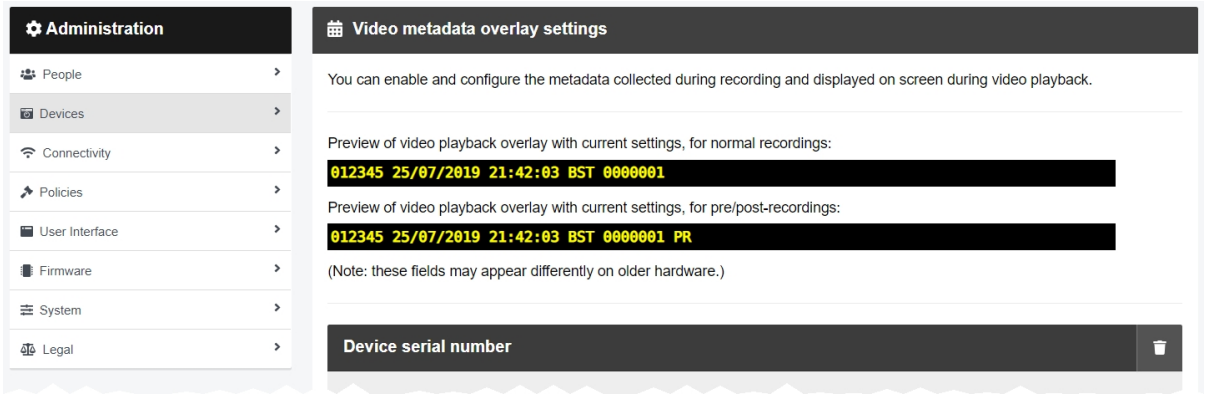
This will only work if a certificate authority has been created or imported into VideoManager. If the administrator has not created or imported a certificate authority, this will do nothing.

>> For more information, see Create, Import, Export, and Delete Device Certificate Authorities on page 216

Click ***Save settings***.

9.2.3 Configure Video metadata overlay settings

VideoManager makes it possible to add metadata to recorded footage. This metadata is stored in the video itself and can be displayed in an overlay during playback and export. These settings will apply to all videos recorded by body-worn cameras whose device profiles have been configured to include metadata. Administrators can edit these settings from the ***Video metadata overlay settings*** section of the ***Devices*** pane, in the ***Admin*** tab.



To configure video metadata overlay settings:

1. Navigate to the ***Admin*** tab.
2. Select the ***Devices*** pane.
3. Click the ***Video metadata overlay settings*** section.
4. To add a metadata element to the video overlay, scroll down to the bottom of the pane, and select an element from the ***Add element*** dropdown.

The order in which an administrator chooses the metadata elements determines the order that those elements will appear in when a video is played (left to right).

The element options are as follows:

- **Device serial number** - the serial number of the body-worn camera on which the footage was recorded.
- **Operator name** - the name of the operator who recorded the footage. Administrators can configure how many characters of the name will be visible over the video, and how many spaces will be added to "pad" the name out to a minimum size.
- **Date and time** - for footage recorded on a VT-series camera or VB400, the administrator can configure the following:
  - ***Timezone*** - **UTC** (Greenwich Mean Time, but without adjustments for daylight savings time) or **Local Time** (taken from VideoManager's server).

- ***Time &date format*** - this sets the format for date and time metadata. The options are as follows:
  - **ISO Standard 8601** - if selected, the time and date will be presented in an internationally standardised manner.
  - **Custom** - if selected, more options will be presented, as detailed below:
    - ***Time display*** - **24-Hour Display** (e.g. 19:00) or **12-Hour Display With AM/PM Markers** (e.g. 12AM).
    - ***Timezone display*** - **None**, **Show Timezone Offset In Hours:Minutes** (e.g. +01:00), or **Show Timezone Name** (e.g. GMT).
    - ***Date format*** - ***DD/MM/YY***, ***MM/DD/YY***, ***YY/MM/DD***, ***DD-MM-YY***, ***MM-DD-YY***, or ***YY-MM-DD***.
    - ***Years format*** - **YY e.g. '19'**, or **YYYY e.g. '2019'**.

- **Frame counter** - for footage recorded on a VB400, VB300, VB200, or VB100, this will show the user which frame is currently being shown in the playback viewer.
- **Recording time** - for footage recorded on a VB400, VB300, VB200, or VB100, this will show the length of the recording. Administrators can configure whether the recording time will start from when the operator pressed record, or when the first frame was actually recorded.

The former option means that any pre-recorded footage will appear as negative time in the metadata overlay (e.g. -00:23:45).

- **Pre/Post-record marker** - for footage recorded on a VB400, VB300, VB200, or VB100, this will indicate which part of the video has been pre-recorded or post-recorded, if any.
- **Text** - administrators can enter text here which will give more information about the body-worn camera, operator, etc.

Unlike other elements, administrators can add as many **Text** elements as necessary.

- **GPS** - for footage recorded on a VB400, this will display the latitude and longitude of the body-worn camera. The administrator can also enable the following settings:
  - ***Include speed*** - if set to ***On***, the speed of the body-worn camera will be displayed in meters per second.
  - ***Include track*** - if set to ***On***, the track of the body-worn camera will be displayed in degrees.
- **Device name** - the name of the body-worn camera, as configured from the ***Edit device properties*** pane.
- **Battery level** - the level of the VB400's battery when it recorded the footage.

5. To delete a metadata element, click ***Delete element***.
   This element will return to the dropdown, and can be reselected for use again.

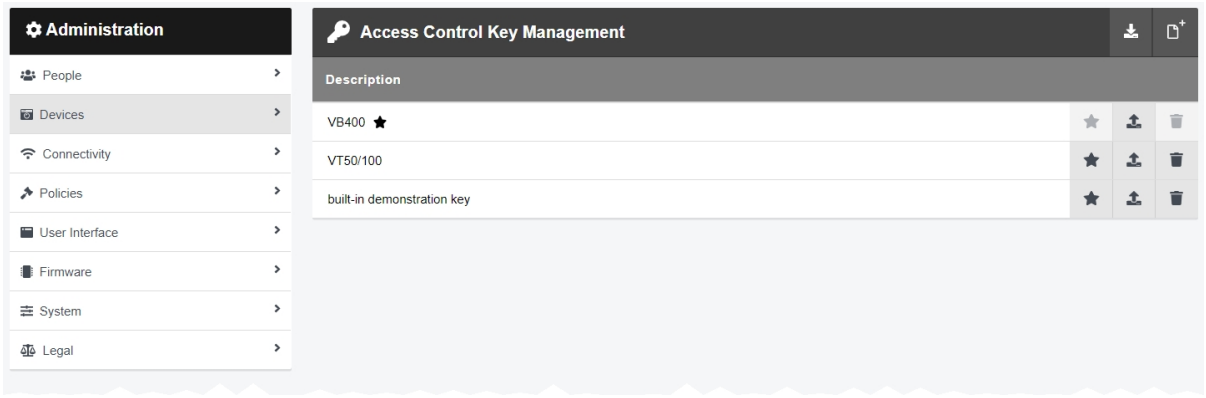
6. Click ***Save settings*** to save the changes.

These changes will affect all body-worn cameras whose device profile has had ***Show video metadata overlay*** set to ***On***. The changes will **not** apply retroactively to videos which have already been recorded.

>> For more information, see Create, Edit, Reorder and Delete Device Profiles on page 204

9.2.4 Create, Import, and Export Access Control Keys

Access control keys are the mechanism that VideoManager uses to encrypt videos. They also prevent body-worn cameras from communicating with unauthorised instances of VideoManager. This is done from the ***Access Control Key Management*** section of the ***Devices*** pane, in the ***Admin*** tab.



To create an access control key:

1. Navigate to the ***Admin*** tab.
2. Select the ***Devices*** pane.
3. Click the ***Access Control Key Management*** section.
4. Click ***Create key***.
5. In the ***Description*** field, enter a name for the access control key.
6. Click ***Create key***.
7. Once an access control key has been created, the administrator can make it the default, by which all new or factory reset body-worn cameras are authenticated, by clicking ***Set as default key***.

It is recommended that all access control keys are exported upon creation to somewhere secure - in event of a system failure, this will ensure that users can still access footage on their body-worn cameras that has not been downloaded already.

If an administrator wishes to move a body-worn camera to another instance of VideoManager, they **must** import the corresponding access control key into that instance of VideoManager as well - otherwise, the body-worn camera will appear as **locked** and the administrator will not be able to access any footage on the body-worn camera which has not already been downloaded to VideoManager. To do so:

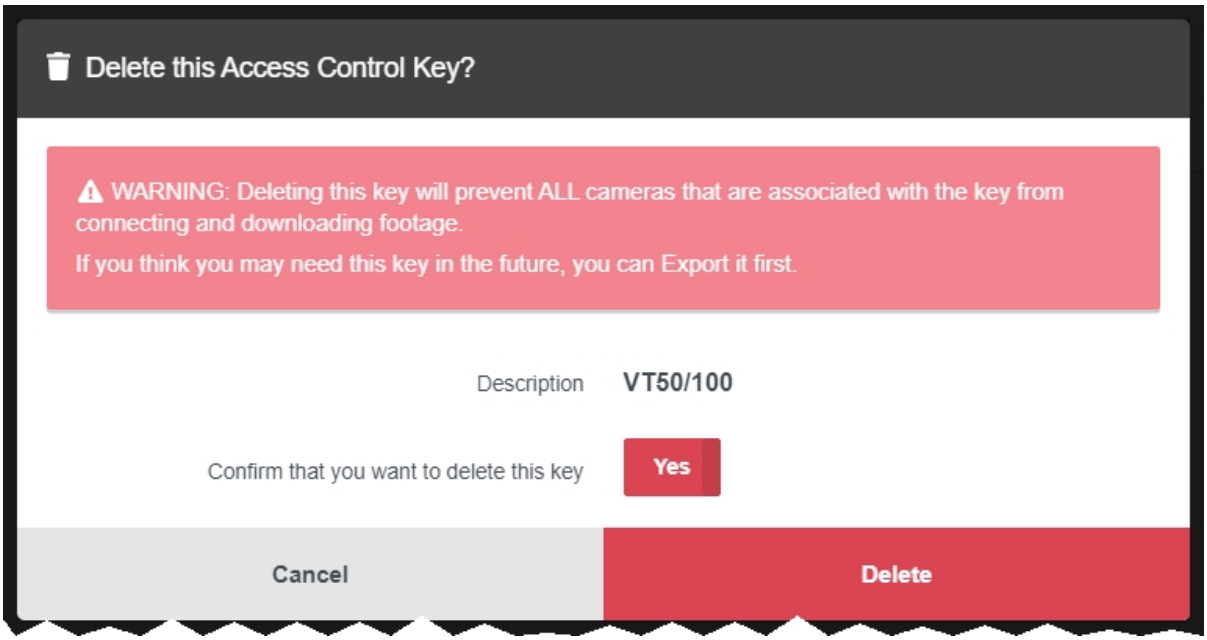
1. In the original VideoManager instance, next to the access control key, click ***Export key***.

The access control key will be downloaded to the administrator's PC.

2. In the new instance of VideoManager, click ***Import key***.
Select the previously downloaded key.

9.2.4.1 Delete Access Control Keys

Administrators can delete an access control key if the body-worn cameras associated with it are no longer connected to the same instance of VideoManager.



To delete an access control key:

1. Navigate to the ***Admin*** tab.
2. Select the ***Devices*** pane.
3. Click the ***Access Control Key Management*** section.
4. Next to the access control key to be deleted, click ***Export key***.

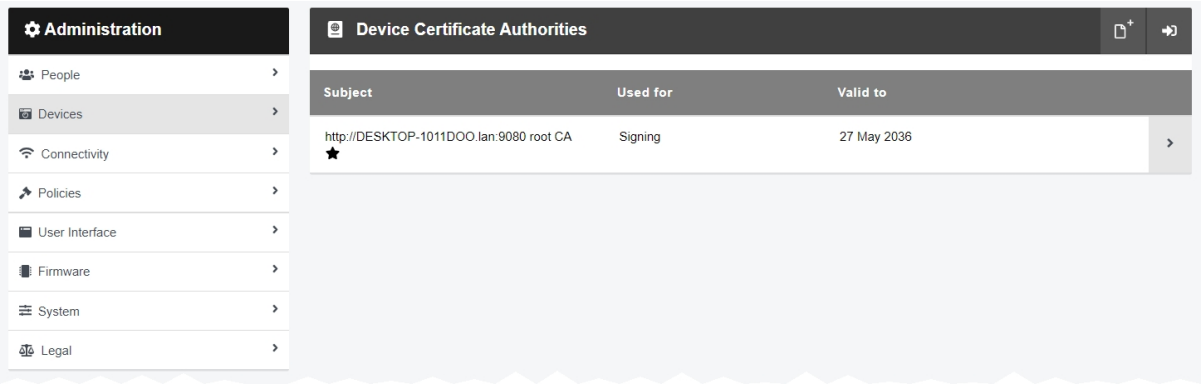
Caution

If an access control key is deleted while body-worn cameras associated with it are still in the field, those body-worn cameras will appear as **Locked** *when redocked and* ***all footage which was not already downloaded to VideoManager will be permanently inaccessible****, unless the administrator has exported the access control key and can import it into VideoManager again.*

5. Click ***Delete key***.
6. Set ***Confirm that you want to delete this key*** to ***On***.
7. Click ***delete***.

9.2.5 Create, Import, Export, and Delete Device Certificate Authorities

VideoManager can verify footage which has been downloaded from body-worn cameras, to check whether the footage has been tampered with and whether it comes from a trusted source (i.e. a genuine Motorola Solutions body-worn camera). In order for this feature to function, administrators must first create or import a certificate authority into VideoManager - this signs the certificates issued to body-worn cameras. The administrator must then enable footage signing. These actions are completed from the ***Device Certificate Authorities*** and ***Device Settings*** sections of the ***Devices*** pane, in the ***Admin*** tab, respectively.



The initial steps differ, depending on whether the administrator is creating or importing a certificate authority.

Caution

If there is an existing certificate authority on VideoManager, the newly-created or imported certificate authority will replace it as the signing certificate authority (i.e. VideoManager will use the new certificate authority to issue certificates to new body-worn cameras from now on). However, body-worn cameras which already have certificates created from the old certificate authority will continue to sign files using their old certificates, and previously-downloaded files contain signatures which refer to the old certificate authority. For this reason, the old certificate authority will be retained so VideoManager can use it to validate the videos from these body-worn cameras. If body-worn cameras should be issued new certificates based on the new certificate authority, the administrator must factory reset them.

If the administrator is creating a new certificate authority on VideoManager:

1. Navigate to the ***Admin*** tab.
2. Select the ***Devices*** pane.
3. Click the ***Device Certificate Authorities*** section.
4. Click ***Create new Certificate Authority***.
5. VideoManager automatically populates the ***Common Name*** field with the public address + *root CA*. Administrators can change this, if desired.
6. In the ***Organisation*** field, optionally enter the name of the administrator's organisation (e.g. Motorola Solutions).
7. In the ***Organisational unit*** field, optionally enter the name of the department that this

certificate authority is for (e.g. Research and Development).

8. Click ***create***.

Alternatively, **if the administrator is importing an existing certificate authority into VideoManager**:

1. Navigate to the ***Admin*** tab.
2. Select the ***Devices*** pane.
3. Click the ***Device Certificate Authorities*** section.
4. Click ***Import Certificate Authority***.
5. Click ***Choose file***.

   Any imported certificate **must** be a certificate authority, **must** be accompanied by a private key, and both the certificate and private key **must** be packaged as a PKCS#12 file. Certificates issued by public certificate authorities are unlikely to be suitable for import - in general, if administrators wish to use their own certificate authority, they must create it themselves.
6. Select the certificate and click ***Open***.
7. Click ***OK***.

Once the certificate authority has been created or imported, the administrator must enable file signing from the ***Device Settings*** of the ***Devices*** pane, in the ***Admin*** tab. The setting is located in the ***Footage signing*** section.

>> For more information, see Configure Device Settings on page 207

From now on, all upgraded VB400s which are docked will be issued with signing certificates. All videos downloaded from these VB400s will be accompanied by a digital signature: VideoManager will check that the downloaded videos match their signatures and that the body-worn cameras' certificate associated with the signature is trusted by VideoManager. Administrators can check whether the videos match this certificate from the ***Videos*** tab.

>> For more information, see View and Edit Video Properties on page 27

If body-worn cameras are being moved from one instance of VideoManager to another, the administrator should also export those body-worn cameras' certificate authority from the original instance and import it into the new instance. This ensures that videos from those body-worn cameras can have their signatures checked against the original certificate. Only the public part of the certificate authority will be exported, so there is no security risk from importing these certificates into a less trusted system. To do so:

1. On the old instance of VideoManager, navigate to the ***Admin*** tab.
2. Select the ***Devices*** pane.
3. Click the ***Device Certificate Authorities*** section.
4. Next to the certificate authority which will be exported, click > ***View Certificate Authority***.

5. Click ***Export Certificate Authority***.

The certificate authority will be downloaded to the administrator's PC.

6. On the new instance of VideoManager, navigate to the ***Admin*** tab.
7. Select the ***Devices*** pane.
8. Click the ***Device Certificate Authorities*** section.
9. Click ***Import Certificate Authority***.
10. Click ***Choose file***.
11. Select the certificate authority and click ***Open***.
12. Click ***OK***.

Finally, if videos from a particular source should no longer be trusted, administrators can delete the corresponding certificate authority from VideoManager. To do so:

1. Navigate to the ***Admin*** tab.
2. Select the ***Devices*** pane.
3. Click the ***Device Certificate Authorities*** section.
4. Next to the certificate authority to be deleted, click ***Delete Certificate Authority***.

If there is no icon next to the certificate authority, this is because the certificate authority is still actively signing certificates: only certificate authorities which are being used for verification can be deleted.

5. Check the checkbox and click ***delete***.

Caution

From now on, videos which would have been signed by the deleted certificate authority will not be trusted by the system when downloaded, and videos which were already downloaded and signed by the deleted certificate will also no longer be trusted. In both cases, the videos' ***Signature*** *field will read as* ***Untrusted Certificate****.*

9.3 Connectivity

In the ***Connectivity*** pane, administrators can edit aspects of VideoManager related to WiFi and sites.

To access the ***Connectivity*** pane:

1. Navigate to the ***Admin*** tab.
2. Select the ***Connectivity*** pane.

From here, administrators can access the following sections:

- ***WiFi Profiles***

Create, edit, and delete WiFi profiles. This is necessary if users want to send live streams from their body-worn cameras to VideoManager.

>> For more information, see Create WiFi Profiles and Perform WiFi Profile Actions on page 221

- ***Bandwidth Rules***

Configure bandwidth rules. This is necessary if administrators have sites uploading footage, and they want to control when the footage is uploaded.

>> For more information, see Create, Copy, Edit and Delete Bandwidth Rules on page 226

- ***Metadata/Footage Replication*** and ***Configuration Replication***

If VideoManager has been configured as a Central VideoManager, these settings will determine which aspects of its configuration (e.g. users and roles) will be automatically shared with its connected sites. This is part of a multi-step process.

>> For more information, see Configure Sites on page 374

- ***Site Manager***

Configure sites. If VideoManager is not already acting as a Central VideoManager, this pane allows administrators to enable their instance of VideoManager to act as a site. This is part of a multi-step process.

>> For more information, see Configure Sites on page 374

- ***Email Properties***

Configure how emails are sent and received in VideoManager.

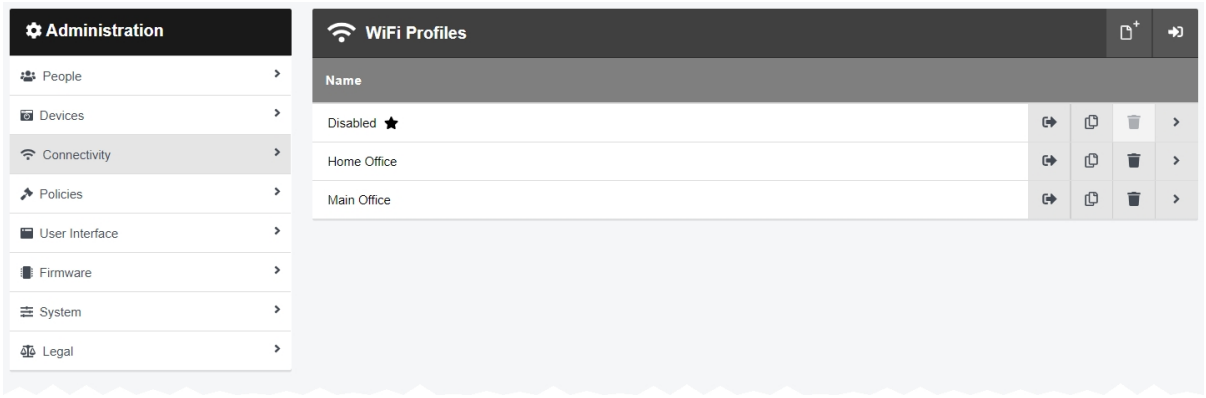
>> For more information, see Configure Email Properties on page 230

- Configure email notifications on VideoManager, including the email template and which actions prompt notifications to be sent to users.

>> For more information, see Configure Email Notifications on page 233

9.3.1 Create WiFi Profiles and Perform WiFi Profile Actions

VideoManager uses WiFi profiles to control the connectivity options available for a body-worn camera. A WiFi profile is a collection of WiFi networks, which a body-worn camera can connect to when attempting to live stream footage. This is done from the ***WiFi Profiles*** section of the ***Connectivity*** pane, in the ***Admin*** tab.



To create a new WiFi profile:

1. Navigate to the ***Admin*** tab.
2. Select the ***Connectivity*** pane.
3. Click the ***WiFi Profiles*** section.
4. Click ***Create wifi profile***.
5. In the ***Name*** field, enter a name for the WiFi profile.
6. If ***Default profile*** is set to ***On***, the WiFi profile will be the default. This means that body-worn cameras assigned with single issue via RFID and Permanent allocation will automatically use this WiFi profile.
7. If ***User-specific networks*** is set to ***On***, a user's user-specific WiFi networks will be added to this WiFi profile. User-specific WiFi networks are networks which only appear on a user's session of VideoManager. This is useful if multiple users have their own individual mobile hotspots which should only be used by body-worn cameras assigned to them.

>> For more information, see Create User-Specific WiFi Networks on page 367

The following settings must be configured if user-specific WiFi networks have been enabled:

- If ***Enable streaming*** is set to ***On***, users with appropriate permissions can live stream footage over VideoManager from VT-series cameras in the field.
- If ***Enable docking*** is set to ***On***, users can assign and unassign VT-series cameras over WiFi, instead of having to manually dock the body-worn cameras first.

8. Click ⊕ ***Add network*** to add WiFi networks to this WiFi profile. Unlike user-specific WiFi networks, these WiFi networks can be used by all body-worn cameras which have this WiFi profile assigned to them, regardless of their operator.

Administrators can now configure the following settings:

- In the ***Network name (SSID)*** field, enter the SSID of the WiFi network.
- From the ***Security type*** dropdown, select the security type of the WiFi network.
- In the ***Passphrase*** field, enter the WiFi network's passphrase.

These credentials can usually be found on the bottom of the WiFi router.

- From the ***Band*** dropdown, select which frequencies the body-worn cameras will attempt to connect to. The options are as follows:
  - **Any** - this option will make VB400s connect to both 2.4GHz and 5GHz frequencies.
  - **2.4GHz only** - this option will make all body-worn cameras connect to 2.4GHz frequencies.
  - **5GHz only** - this option will make VB400s connect to 5GHz frequencies.
- If ***Disconnect on low signal*** is set to ***On***, body-worn cameras will disconnect from the network if it has a low signal. The user can configure for how long the body-worn camera must be connected to the weak signal, after which the body-worn camera will disconnect.
- ***Hidden network*** should only be set to ***On*** if the networks within a WiFi profile are hidden networks. This toggle enables body-worn cameras to connect to hidden networks.

9. VT-series camera settings must be configured for the individual WiFi network. They are as follows:
   - If ***Enable streaming*** is set to ***On***, users with appropriate permissions can live stream footage over VideoManager from VT-series cameras in the field.
   - If ***Enable docking*** is set to ***On***, users can assign and unassign VT-series cameras over WiFi, instead of having to manually dock the body-worn cameras first.
10. If multiple networks should be contained within the WiFi profile, click ⊕ ***Add network*** again and repeat the process until all of the necessary networks have been added.

*Prioritise the networks using **Move up** and **Move down**. The first network shown will be the one which body-worn cameras attempt to connect to first, while the last in the list will only be used if all the others are unavailable.*

11. Once the WiFi networks have been added, administrators must configure settings for VB-series cameras for the entire WiFi profile. They are as follows:

- If ***Enable streaming*** is set to ***On***, body-worn cameras will be able to live stream footage over the WiFi networks in this WiFi profile.
- If ***Download video over WiFi*** is set to ***On***, footage which has been recorded on VB-series cameras can be downloaded to VideoManager over the WiFi networks within this WiFi profile.

If the administrator has configured device profiles so that VB400s can place bookmarks in a video, then only bookmarked videos will be downloaded over the WiFi networks.

If the administrator has **not** configured their device profiles so that VB400s can place bookmarks in a video, then all videos will be downloaded over the WiFi networks when the VB400 is connected to power.

>> For more information, see Create, Edit, Reorder and Delete Device Profiles on page 204 and Appendix B: Device Profiles on page 443

12. Click ***Save profile***.

Once a WiFi profile has been created, it can be applied to body-worn cameras. The options are as follows:

- If an operator is obtaining their body-worn camera through **Single Issue** or **Permanent Issue**, they can manually select the WiFi profile when they assign their body-worn camera.

>> For more information, see Assign Body-Worn Cameras and Record Footage on page 110

- If an operator is obtaining their body-worn camera through **Permanent Allocation**, VideoManager will automatically select the system's default WiFi profile.

Administrators can edit a WiFi profile if certain aspects of its configuration should be changed. To do so:

1. Navigate to the ***Admin*** tab.
2. Select the ***Connectivity*** pane.
3. Click the ***WiFi Profiles*** section.
4. Next to the profile to be edited, click ***Go to profile***.
5. Make the relevant changes, and click ***Save profile***.

Administrators can delete a WiFi profile if it has become redundant. To do so:

1. Navigate to the ***Admin*** tab.
2. Select the ***Connectivity*** pane.
3. Click the ***WiFi Profiles*** section.
4. Next to the profile to be deleted, click ***Delete profile***.

The default WiFi profile **cannot** be deleted. Administrators must first select another WiFi profile which will become the default instead. Next to the WiFi profile which will become the default, click > ***Go to profile***, set ***Default profile*** to ***On***, and click ***Save profile***. The old WiFi profile can now be deleted.

Administrators can duplicate WiFi profiles. This is useful if VideoManager should have multiple similar WiFi profiles. To do so:

1. Navigate to the ***Admin*** tab.
2. Select the ***Connectivity*** pane.
3. Click the ***WiFi Profiles*** section.
4. Next to the profile to be duplicated, click ***Duplicate wifi profile***.

   The ***Create WiFi Profile*** pane opens, with the original WiFi profile's information pre-set.
5. Administrators can edit the WiFi profile like normal. By default, the WiFi profile's ***Name*** will be set to *[name of the duplicated WiFi profile] (copy)*.

   Caution *No two WiFi profiles can share the same name on VideoManager. Administrators cannot save a WiFi profile whose name is identical to a previously-existing WiFi profile.*
6. Once the relevant changes have been made (if any), click ***Save profile***.

Administrators can export WiFi profiles. This is useful if sites should have the same WiFi profiles as their Central VideoManager. To do so:

1. Navigate to the ***Admin*** tab.
2. Select the ***Connectivity*** pane.
3. Click the ***WiFi Profiles*** section.
4. Next to the profile to be exported, click ***Export wifi profile***.

   The WiFi profile will be exported to the PC's default download location, and can be imported to other instances of VideoManager.

Administrators can import previously-created WiFi profiles which have been created on another instance of VideoManager. This is useful if sites should have the same WiFi profiles as their Central VideoManager. To do so:

1. Navigate to the ***Admin*** tab.
2. Select the ***Connectivity*** pane.
3. Click the ***WiFi Profiles*** section.
4. Next to the profile to be imported, click ***Import wifi profile***.
5. Select the relevant file from the user's PC.

6. Click ***import***.

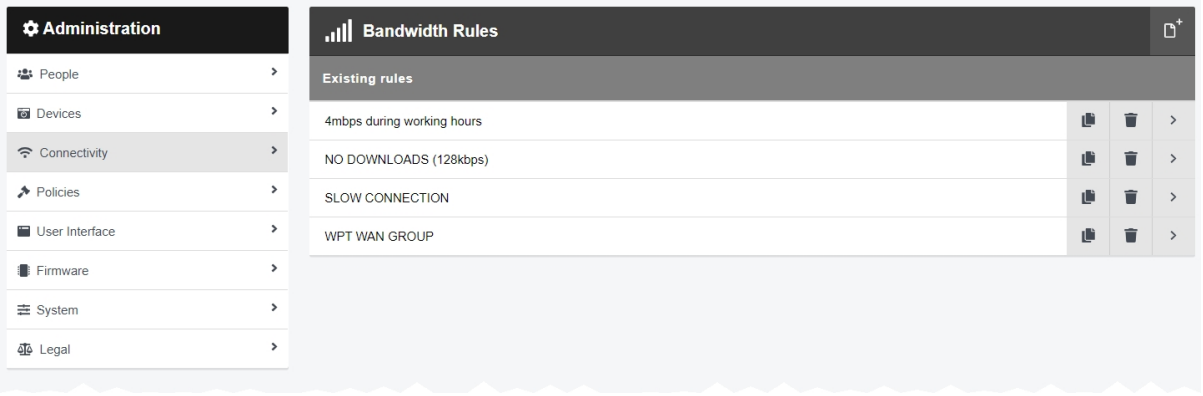
The WiFi profile will now appear on the administrator's instance of VideoManager.

Alternatively, if an administrator wants to import/export **all** of their WiFi profiles simultaneously, they can do so from the ***Import/Export System Config*** section of the ***System*** pane in the ***Admin*** tab.

>> For more information, see Import or Export VideoManager's Configuration on page 356

9.3.2 Create, Copy, Edit and Delete Bandwidth Rules

Administrators may wish to configure bandwidth rules, which affect how much bandwidth is used when downloading data from both sites and DockControllers. This is done from the ***Bandwidth Rules*** section of the ***Connectivity*** pane, in the ***Admin*** tab.



To create a bandwidth rule:

1. On the Central VideoManager (if creating a bandwidth rule for sites), or on VideoManager (if creating a bandwidth rule for DockControllers), navigate to the ***Admin*** tab.
2. Select the ***Connectivity*** pane.
3. Click the ***Bandwidth Rules*** section.
4. Click ***Create bandwidth rule***.
5. In the ***Name*** field, enter a name for the bandwidth rule.
6. If ***Shared bandwidth group*** is set to ***On***, all DockControllers which are added to this rule will be part of the same "group" and will share the same bandwidth limit. This is useful if multiple DockControllers are on the same network connection, and administrators want to stagger the downloads.
7. If ***Slow connection*** is set to ***On***, all DockControllers who are added to this rule will continuously download footage to VideoManager, ignoring the overall download limit. This is useful if the DockControllers in question have a slow network connection.
8. Click ***Add rule*** to create an individual rule. Administrators can configure the following settings:
   - The day(s) of the week when the rule will occur.
   - In the ***from*** field, enter the time of day when this rule will begin.
   - In the ***until*** field, enter the time of day when this rule will finish.
   - In the ***limit to*** field, enter the number of kilobits per second to which uploads will be limited while this rule applies.

Administrators can create multiple rules within one bandwidth rule, by clicking ***Add rule***. This is useful if there are certain "busy" times when footage and other data should not be offloaded, and other "quiet" times when footage and data should be offloaded.

If there are multiple rules within one bandwidth rule, administrators should order them using the controls next to each rule. If there are two overlapping rules (e.g. two rules both applying on Saturday), the rule which is **highest** in the list will take priority.

To delete an individual rule within a bandwidth rule, click ***Delete bandwidth rule***.

9. Click ***Create bandwidth rule***.

Once a bandwidth rule has been created, it must be manually applied in order to take effect. The steps for applying a bandwidth rule differ, depending on whether it is being applied to a DockController or site.

If the administrator is applying a bandwidth rule to a DockController:

1. Navigate to the ***Devices*** tab.
2. Select the ***DockControllers*** pane.
3. Find the relevant DockController, and click ***View details*** next to it.

   Administrators can filter by **Name**, **Serial**, and **Version**.
4. In the ***Bandwidth Rule*** pane, click the dropdown menu.

   Select the relevant rule.
5. If ***High Priority DockController*** is set to ***On***, all footage from this DockController will be downloaded as quickly as possible - this means that if the DockController is part of a bandwidth rule that has the ***Shared bandwidth group*** setting enabled, it will halt the downloads of other DockControllers in the group until all of its footage has been downloaded.
6. Click ***Save Bandwidth Rule***.

If the administrator is applying a bandwidth rule to a site, it can either be applied upon creation or the site can be edited afterwards to include the rule. This is part of a multi-step process.

>> For more information, see Configure Sites on page 374

Administrators can copy a bandwidth rule. This enables administrators to create multiple, similar bandwidth rules. To do so:

1. Navigate to the ***Admin*** tab.
2. Select the ***Connectivity*** pane.
3. Click the ***Bandwidth Rules*** section.
4. Click ***Copy bandwidth rule*** next to the relevant bandwidth rule.

   A new bandwidth rule will be created. Its name will be the original bandwidth rule's name, with _1 (if it is the first copy of the bandwidth rule) at the end.

Unlike groups and users, it is possible to create two bandwidth rules with the same name - however, this is not generally recommended.

5. Make any necessary changes to the copy of the bandwidth rule, and click ***Save bandwidth rule***.

To edit an existing bandwidth rule:

1. Navigate to the ***Admin*** tab.
2. Select the ***Connectivity*** pane.
3. Click the ***Bandwidth Rules*** section.
4. Click ***Go to bandwidth rule***.
5. Make the relevant changes, and click ***Save bandwidth rule***.

The bandwidth rule will automatically update across all DockControllers to which it has been applied.

To delete a bandwidth rule:

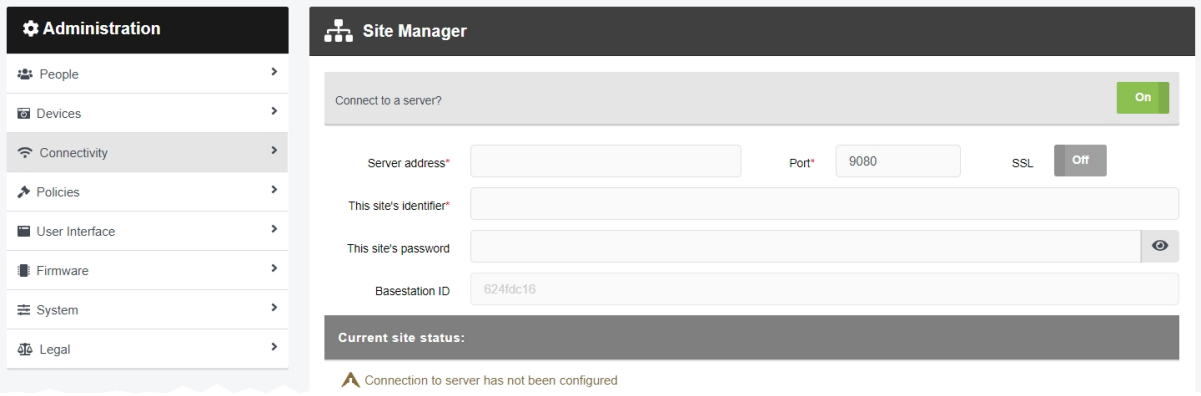
1. Navigate to the ***Admin*** tab.
2. Select the ***Connectivity*** pane.
3. Click the ***Bandwidth Rules*** section.
4. Next to the relevant bandwidth rule, click ***Delete bandwidth rule***.

Caution *If the deleted bandwidth rule was previously applied to a DockController or site, the bandwidth setting for those DockControllers and sites will immediately change to* **No Restriction** *until another bandwidth rule is manually re-applied.*

9.3.3 Configure Site Manager

Administrators can configure whether their instance of VideoManager is acting as a site or not. This is done from the ***Site Manager*** section of the ***Connectivity*** pane, in the ***Admin*** tab.

This section will not be available if VideoManager is already acting as a Central VideoManager.

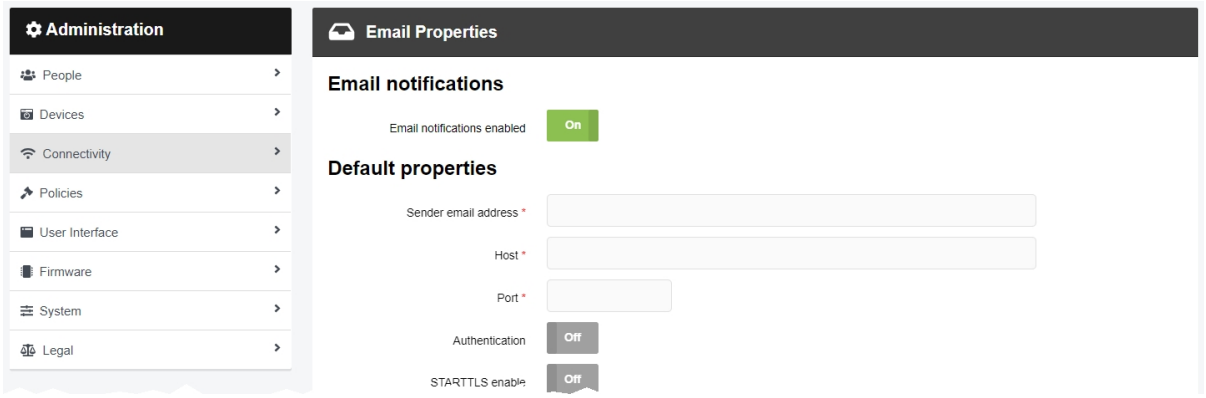


This is part of a multi-step process.

>> For more information, see Configure Sites on page 374

9.3.4 Configure Email Properties

Configuring email properties is necessary to enable additional functionality: users can reset their own passwords, self-register without administrative help, and receive notifications when specific actions are performed on VideoManager. This is done from the ***Email Properties*** section of the ***Connectivity*** pane, in the ***Admin*** tab.



To configure email properties for VideoManager:

1. Ensure that the *Notification* licence has been enabled on VideoManager.

>> For more information, see Import and Delete Licences on page 353

2. Navigate to the ***Admin*** tab.
3. Select the ***Connectivity*** pane.
4. Click the ***Email Properties*** section.
5. Set ***Email notifications enabled*** to ***On***.
6. In the ***Default properties*** section, configure the following settings:

   - In the ***Sender email address*** field, enter the email address from which all VideoManager emails will be sent.

   This includes email notifications, password reset emails, and user profile creation emails.

   - In the ***Host*** field, enter the host from which emails will be sent.

   For Gmail, this is *smtp.gmail.com*.

   - In the ***Port*** field, enter the port from which emails will be sent.

   For Gmail, this is *587*.

   - If ***Authentication*** is set to ***On***, the administrator must enter the ***Username*** and ***Password*** belonging to the email address entered in the ***Sender email address*** field.

The password is not necessarily the same password which is utilised to log in to the email address's account.

For Gmail, administrators must create an app password. To do so:

1. Open the account settings pane for the email address entered in the ***Sender email address*** field.
2. Click the ***Security*** section.
3. Click ***App passwords***.
4. From the ***Select app*** dropdown, select **Other (Custom name)**.
5. Enter *VideoManager*.
6. Click ***Generate***.
7. Copy the password and paste it into the ***Password*** field.

- If ***STARTTLS enable*** is set to ***On***, all emails sent from VideoManager will be protected with Transport Layer Security (TLS).
- If ***Trust server certificates*** is set to ***On***, VideoManager will trust the SMTP server.

If set to ***Off***, VideoManager will check server certificates.

7. In the ***Custom properties*** section, administrators can add specific properties which dictate how VideoManager interacts with the SMTP server. To do so:

- Click ***Add property***.
- In the ***Property*** field, enter the name of the property. This should be the name of a JavaMail SMTP property.

Examples include *mail.smtp.timeout* and *mail.smtp.reportsuccess*.

- In the ***Value*** field, enter the value of the property.

The format of the value (milliseconds, true/false, host name etc.) depends on the property name entered in the ***Property*** field.

8. In the ***Custom templates*** section, administrators can optionally configure the notification email which is sent to users when specific actions are taken on VideoManager:

- If ***First time login*** is set to ***On***, administrators can configure the email that users receive when another user on VideoManager logs in for the first time.
- If ***Device stream start*** is set to ***On***, administrators can configure the email that users receive when a body-worn camera starts streaming. This could be the user's own body-worn camera, or a body-worn camera assigned to someone

they supervise, depending on the way the user's permissions have been configured.

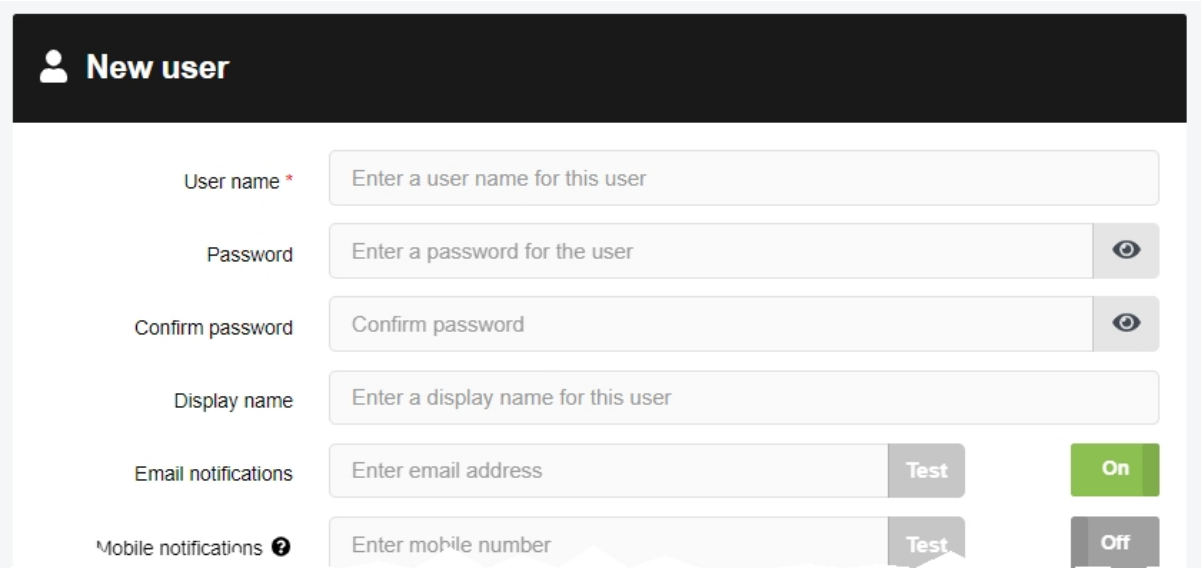
9. In the ***Test Properties*** section, administrators can send a test email. If email notifications have been configured correctly, the email will be sent from VideoManager successfully. In the ***Test recipient*** field, enter the email address to which test emails will be sent, and click ***Test*** to send the test email.

Administrators can also configure how password reset emails and user profile creation emails are sent.

>> For more information, see Configure User Self Service on page 195

9.3.5 Configure Email Notifications

Once administrators have configured email settings on VideoManager, they can enable and configure email notifications. This involves optionally configuring the email template which users will receive for various events, enabling notifications for individual roles, and ensuring that users in those roles have email addresses associated with them. This is done from the ***Connectivity*** and ***People*** panes, in the ***Admin*** tab.



The administrator can first optionally configure the emails that users will receive when specific actions are taken on VideoManager. To do so:

1. Navigate to the ***Admin*** tab.
2. Select the ***Connectivity*** pane.
3. Click the ***Email Properties*** section.
4. Scroll down to the ***Custom templates*** section. The options are as follows:

   - If ***First time login*** is set to ***On***, administrators can configure the email that users receive when another user on VideoManager logs in for the first time.

   If left as ***Off***, the default message is `User has logged in to ${system} for the first time. User ${username}${displayName} has logged in.`

   - If ***Device stream start*** is set to ***On***, administrators can configure the email that users receive when a body-worn camera starts streaming. This could be the user's own body-worn camera, or a body-worn camera assigned to someone they supervise, depending on the way the user's permissions have been configured.

   If left as ***Off***, the default message is `Device started streaming. ${device} started streaming to ${system}.`

   - If ***File storage threshold warning*** is set to ***On***, administrators can configure the email that users receive when one of VideoManager's file spaces is nearly full.

If left as ***Off***, the default message is `A File Space on ${system} has exceeded the threshold: <#list storageWarnings as message> ${message.category} : ${message.level}% </#list> .`

Once the administrator has optionally configured the email templates, they must configure which users will receive notifications on a role-by-role basis. To do so:

1. Navigate to the ***Admin*** tab.
2. Select the ***People*** pane.
3. Click the ***Roles*** section.
4. Next to the role to be edited, click ***Go to role***.
5. Enable the relevant permissions:
   - ***First time login*** - this permission means that users will receive a notification when other users first log into VideoManager.
   - ***Personal device stream start*** - this permission means that users will receive a notification when a body-worn camera assigned to them starts streaming.
   - ***Supervised device stream start*** - this permission means that users will receive a notification when a body-worn camera assigned to users they supervise starts streaming.
   - ***File storage threshold warnings*** - this permission means that users will receive a notification when VideoManager is low on storage space.
6. Click ***Save role***.

The administrator must now ensure that all users in the notification-enabled roles have email addresses associated with them on VideoManager. To do so:

1. Navigate to the ***Admin*** tab.
2. Select the ***People*** pane.
3. Click the ***Users*** section.
4. Locate the user to be edited. Administrators can filter users in the following ways:
   - A user's name (both username and display name) - enter their username or display name in the ***Name*** field. Click ***Find*** to find the users, or click ✕ to reset the filter.
   - A user's group - enter a group name in the ***In group*** field. Click ***Find*** to find the users, or click ✕ to reset the filter.

*If the user enters a group name in the **In group** field, they will have the option to change whether **Only immediate members** is set to **On** or not. If set to **On**, only users which are assigned directly to the specified group will be returned (as opposed to if user A is assigned indirectly to group B because A belongs to group C, which is assigned to group B).*

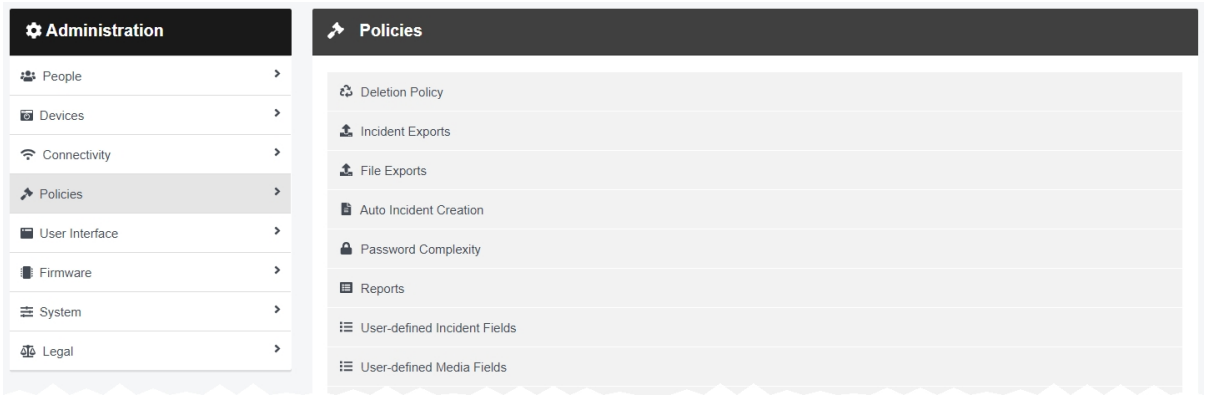
- A user's role - from the ***Role*** dropdown, select the relevant role. All users who inhabit that role will be returned. Click ***Find*** to find the users, or click ✕ to reset the filter.

5. Next to the user to be edited, click > ***Go to user***.
6. In the ***Email notifications*** field, enter an email address for this user.
7. Click ***Save user***.

From now on, all users in the role with notification permissions enabled will receive notifications via email when specific events occur on VideoManager.

9.4 Policies

In the ***Policies*** pane, administrators can edit aspects of VideoManager relating to reoccurring rules and settings.



To access the ***Policies*** pane:

1. Navigate to the ***Admin*** tab.
2. Select the ***Policies*** pane.

From here, administrators can access the following sections:

- ***Deletion Policy***

Configure when old footage and incidents are automatically deleted.

>> For more information, see Configure Deletion Policies on page 240

- ***Incident Exports***

Configure incident export profiles. Incident export profiles determine how a user can export an already-created incident from VideoManager (i.e. **DVD**, **MP4**, or **Evidence Export**).

>> For more information, see Configure Incident Exports on page 244

- ***File Exports***

Configure whether recorded footage will be sent straight from a body-worn camera to a predetermined location on a PC or server, in addition to being stored on VideoManager.

>> For more information, see Configure File Exports on page 253

- ***Auto Incident Creation***

Configure which user-defined media fields trigger automatic incident creation.

>> For more information, see Enable and Configure Automatic Incident Creation on page 255

- ***Password Complexity***

Configure password complexity rules, to which all users on VideoManager must adhere.

>> For more information, see Configure Password Complexity on page 257

- ***Reports***

Configure when old reports are automatically deleted, and at what time of day scheduled reports are run.

>> For more information, see Configure Report Settings on page 259

- ***User-defined Incident Fields*** - administrators can perform the following actions:
  - Edit default user-defined incident fields. These are built into VideoManager and can have various aspects of their configuration changed.

    >> For more information, see Edit Default User-defined Incident Fields on page 261

  - Edit which incident clip properties can be viewed by different users, based on their permission groups.

    >> For more information, see Edit Incident Clip Fields on page 263

  - Create, import and export user-defined incident fields. User-defined incident fields enable users to create incidents with more complex fields than those which VideoManager provides by default.

    >> For more information, see Create New User-defined Incident Fields on page 264

- ***User-defined Media Fields*** - administrators can perform the following actions:
  - Edit default user-defined media fields. These are built into VideoManager and can have various aspects of their configuration changed.

    >> For more information, see Edit Default User-defined Media Fields on page 282

  - Create, import and export user-defined media fields. User-defined media fields enable users to categorise assets and videos, using more complex fields than those which VideoManager provides by default.

    >> For more information, see Create New User-defined Media Fields on page 283

- ***CommandCentral Vault Settings***

View CommandCentral Vault user-defined incident fields.

>> For more information, see Configure CommandCentral Vault Settings on page 297

- ***User-defined Playback Reason Fields***

Create, import and export user-defined playback reason fields. User-defined playback reason fields prompt users to enter a reason as to why they are watching an old video. It is used in tandem with the playback policy configured in the ***Playback Policy*** section of the ***Policies*** pane, in the ***Admin*** tab.

>> For more information, see Create User-defined Playback Reason Fields on page 298

- ***Import profiles***

Configure import profiles. These profiles dictate which user-defined media fields are automatically populated when an asset is imported into VideoManager.

>> For more information, see Configure Import Profiles on page 300

- ***Antivirus Policy***

Configure whether VideoManager scans imported media for viruses.

>> For more information, see Enable and Configure the Antivirus Policy on page 302

- ***Sharing Policy***

Configure which email address will be the default, and which incident clip fields will be visible, when using incident links.

>> For more information, see Configure Sharing Policy on page 304

- ***Playback Policy***

Configure whether users must record their reason for watching a video after a set period of time. It is used in tandem with the user-defined playback reason fields configured in the ***User-defined Playback Reason Fields*** section of the ***Policies*** pane, in the ***Admin*** tab.

>> For more information, see Configure the Playback Policy on page 305

- ***VB Companion Settings***

Configure VB Companion settings, if VB Companion has been licensed from Motorola Solutions.

>> For more information, see Configure VB Companion Settings on page 308

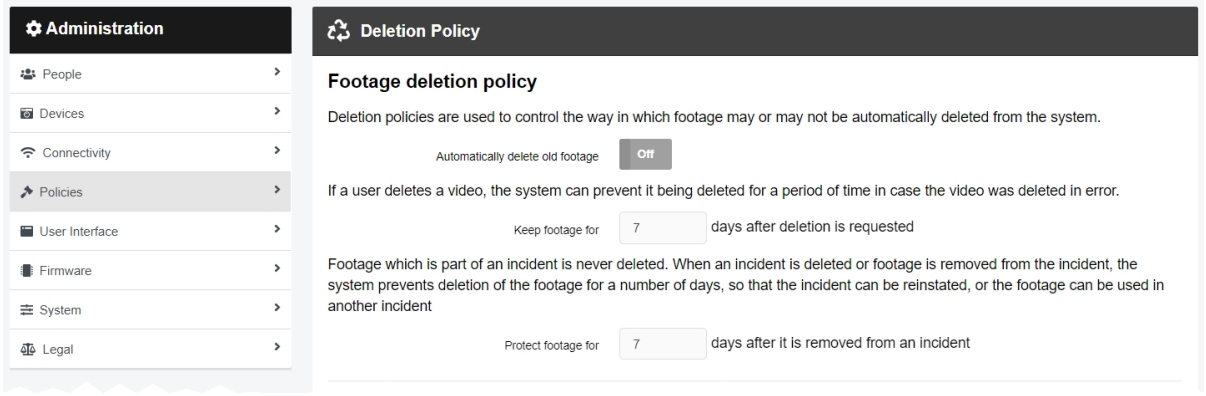
- ***API Key Management***

Create API keys. These keys enable VideoManager to securely communicate with external software.

>> For more information, see Create, View and Delete API Keys on page 309

9.4.1 Configure Deletion Policies

Deletion policies are used to control the way in which videos may or may not be automatically deleted from the system to free storage space. This is done from the ***Deletion Policy*** section of the ***Policies*** pane, in the ***Admin*** tab.



To reach the ***Deletion Policy*** section:

1. Navigate to the ***Admin*** tab.
2. Select the ***Policies*** pane.
3. Click the ***Deletion Policy*** section.

There are multiple categories that administrators can configure:

Footage deletion policy - this section controls the deletion policy regarding footage on VideoManager.

- If ***Automatically delete old footage*** is set to ***On***, old footage on VideoManager will be automatically deleted.

Enter the number of days for which recorded footage should be kept before it is deleted.

Enter the number of days for which downloaded footage should be kept before it is deleted.

This differentiation is useful if footage isn't always downloaded on the same day as it is recorded, and users want more time to review footage or add it to incidents.

- If ***Keep footage until auto file export complete*** is set to ***On***, the deletion policy will be suspended for individual videos until they have been exported. Once a video has been exported, the original video on VideoManager will be subjected to the deletion policy like normal.

*This should **not** be enabled unless users have also enabled automatic incident exports, as determined from the **Incident Exports** section of the **Policies** pane, in the **Admin** tab.*

- If ***Keep all recording footage*** is set to ***On***, an entire recording will be kept if **one** video within it has been added to an incident.

If set to ***Off***, only videos which have been added to incidents will be preserved. The larger recording will be subject to VideoManager's deletion policy like normal.

- A VB400 enables users to bookmark footage in the field, drawing attention to certain portions of footage. From the ***Bookmarked footage policy*** dropdown, select how bookmarked footage will be treated by VideoManager's deletion policy. The options are as follows:
  - **Keep for same period as non-bookmarked footage** - if this option is selected, the deletion policy will treat bookmarked and non-bookmarked footage identically.
  - **No automatic deletion** - if this option is selected, bookmarked footage will be entirely exempt from the deletion policy.
  - **Keep for specified amount of time** - if this option is selected, users will have the option to configure for how long bookmarked footage is kept. The default is 90 days.
- Enter the number of days for which footage is kept after deletion is requested, in case a video has been deleted accidentally.
- Enter the number of days for which footage is protected after it has been removed from an incident. Footage in an incident is never deleted unless:
  - It has been manually removed from the incident.
  - The incident it is a part of has been deleted, in which case the footage will be subject to normal deletion policies.
  - ***Enable forced delete*** is set to ***On***, as described below.

Forced footage deletion - this section controls the deletion policy regarding automatic footage deletion.

- If ***Enable forced delete*** is set to ***On***, footage will be deleted even if it is part of an incident.

Normally, footage will never be deleted while it is part of an incident.

Export deletion policy - this section controls the deletion policy regarding exports on VideoManager.

- If ***Automatically delete old exports*** is set to ***On***, this will automatically delete old exports on VideoManager, even if the export has not already been downloaded to the user's PC.

Enter the number of days for which exports are kept after being created.

*The original incident is **never** deleted - only the export.*

Incidents deletion policy - this section controls the deletion policy regarding incidents on VideoManager. If ***Automatically delete old incidents*** is set to ***On***, the deletion policy will automatically delete old incidents from VideoManager. There is some configuration involved:

1. Create a new user-defined incident field like normal, from the ***User-defined Incident Fields*** section.

>> For more information, see Create New User-defined Incident Fields on page 264

2. From the ***Type*** dropdown, select **Computed Auto-delete**.

There can only be one **Computed auto-delete** *user-defined incident field per instance of VideoManager. If one already exists, this option will not be visible in the dropdown.*

3. In the ***Delete incident if*** field, enter the conditions under which this policy will go into effect, using the Motorola Solutions custom predicate language. The most simple input would be `true`, which would delete all incidents meeting the date specified in the **Auto-deletion date:** field.

>> For more information, see Appendix E: Custom Predicate Language on page 469

4. In the ***Auto-deletion date*** field, enter the relevant time period which determines when an incident will be deleted, using the Motorola Solutions custom predicate language. The most simple input would be something like `dateAdd(6, day, [creation-time])`, which would delete incidents that were 6 days old.

>> For more information, see Appendix E: Custom Predicate Language on page 469

5. Click ***Save settings***.
6. Navigate back to the ***Deletion Policy*** section.
7. Set ***Automatically delete old incidents*** to ***On***.

If there are incidents which will be deleted within the next seven days due to the policy configured in the ***Auto-deletion date*** field, the administrator can preview these incidents by clicking ***{0} incidents will be scheduled for deletion over the next seven days'***.

If there are incidents which will be deleted immediately due to the policy configured in the ***Auto-deletion date*** field, the administrator can preview these incidents by clicking *****1** incident is scheduled for immediate deletion***.

8. Click ***Save settings***.

The administrator must click ***Yes, make these changes.*** and then ***yes*** again to save the changes.

Dashboard - this section controls whether a user's videos which are set to be deleted within a certain time frame are visible on their dashboard:

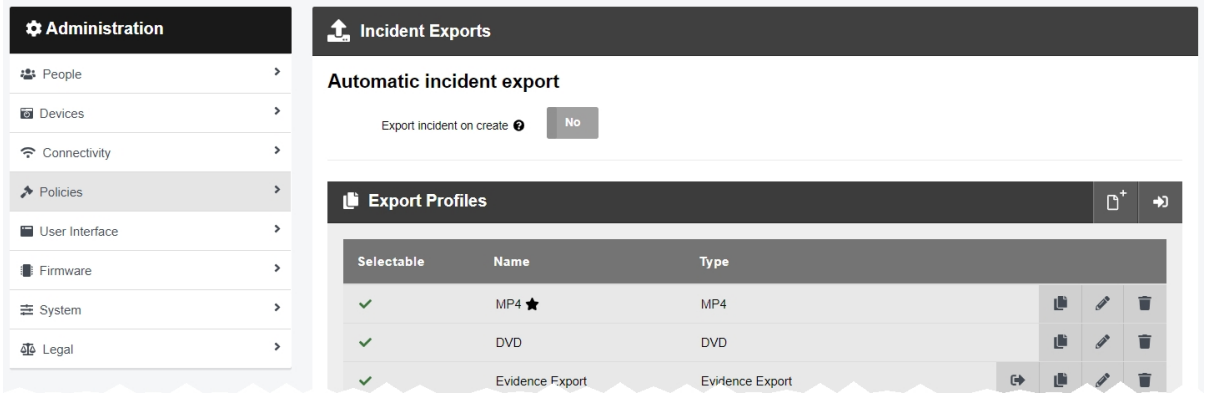
- In the ***Show videos scheduled to be deleted within*** (7) ***days*** field, enter the number of days within which a video will be deleted, before it will show up on a user's dashboard.

This setting only applies to users which have the ***View videos scheduled to be deleted on dashboard*** permission set to ***Yes***.

Optionally click ***Download Change Summary***. This will download a CSV file directly to the administrator's PC which contains information about any changes to which videos and incidents will be deleted as a result of the new policy. Click ***Save settings***.

9.4.2 Configure Incident Exports

Administrators can configure export profiles - these profiles determine the manner in which an incident is exported from VideoManager to the user's PC. This is done from the ***Incident Exports*** section of the ***Policies*** pane, in the ***Admin*** tab.



From the appropriate pane, administrators can perform the following actions:

- Create an export profile.
- Change whether incidents are automatically exported on creation or not.
- Change DVD export defaults.
- Enable accelerated export jobs - if the PC running VideoManager has nVidia hardware, this will increase the rate at which export jobs are processed.

The types of export profile that an administrator can create are as follows:

- DVD

>> For more information, see on page 246

- MP4

>> For more information, see on page 248

- Evidence Export

>> For more information, see on page 250

Administrators can change whether incidents are automatically exported upon creation. This is useful if, due to an organisation's workflow, every incident must be reviewed externally as soon as they have been saved. Administrators may wish to create an export profile first, which all automatically-exported incidents will use. To enable automatic incident exports:

1. Navigate to the ***Admin*** tab.
2. Select the ***Policies*** pane.

3. Click the ***Incident Exports*** section.
4. Set ***Export incident on create*** to ***On***.
5. From the ***Auto-export profile*** dropdown, select the previously-created export profile that automatically exported incidents will inhabit.

> Caution: *Administrators can set rules for export profiles - these will dictate whether the export profile can be applied to the incident in question, based on the status of the incident's user-defined incident fields. However, automatic export will* ***ignore*** *any rules set by the selected export profile.*

6. Click ***Save settings***.

Administrators can change the DVD export defaults. This may be necessary if the an organisation consistently uses a specific type of media. To do so:

1. Navigate to the ***Admin*** tab.
2. Select the ***Policies*** pane.
3. Click the ***Incident Exports*** section.
4. In the ***DVD export defaults*** section, choose the appropriate option from the dropdown.
5. If ***Can override defaults*** is set to ***On***, other users can change the type of DVD media when creating they are creating an export.
6. Click ***Save settings***.

Administrators can optionally enable export acceleration. To do so:

1. Navigate to the ***Admin*** tab.
2. Select the ***Policies*** pane.
3. Click the ***Incident Exports*** section.
4. In the ***Hardware acceleration*** section, set ***Enabled*** to ***Yes***.

If the PC running VideoManager has an nVidia GPU, this will increase the rate at which export jobs are completed. The administrator must click ***Save settings*** and restart VideoManager from the ***Server Controls*** section.

> Caution: *Some nVidia GPUs have limits on the number of simultaneous export jobs they support. If the number of simultaneous export jobs on VideoManager exceeds this limit, the acceleration will not function. To determine what this limit is, navigate to* ***https://developer.nvidia.com/video-encode-and-decode-gpu-support-matrix-new****, open the* ***Encoding*** *table, and look under the* ***Max # of concurrent sessions*** *column.*

If the PC running VideoManager does not have an nVidia GPU, this will do nothing.

9.4.2.1 DVD Export Profile

Export profiles control how exports are handled on VideoManager (e.g. how they are formatted, etc.). To create a DVD export profile:

1. Navigate to the ***Admin*** tab.
2. Select the ***Policies*** pane.
3. Click the ***Incident Exports*** section.
4. In the ***Export Profiles*** section, click ***Create new export profile***.

The ***Create Export Profile*** window will open.

5. In the ***Name*** field, enter a name for the export profile.
6. From the ***Type*** dropdown, select **DVD**.
7. If ***Selectable*** is set to ***Yes***, users can select this export profile when creating an export from the ***Incidents*** tab.

*Users with the **Use any export profile** permission will be able to select any profile, not just those which are enabled. This profile can also still be used if incidents are being exported automatically.*

8. If ***Default*** is set to ***Yes***, this export profile will be the default when creating an export from the ***Incidents*** tab.
9. If ***Select Clips*** is set to ***On***, users can manually select which incident clips will be included in the export when they export the incident.

Caution *Users cannot select individual clips if the incident they are exporting contains a composite clip.*

If set to ***Off***, **all** incident clips within the incident will be included in the export.

10. If ***Encrypt Downloads*** is set to ***On***, the .zip folder containing exports with this profile will be protected with AES 256 encryption. The user must set a passphrase when they download the export to their PC; they must then enter the same passphrase when they extract the .zip folder.

*Windows cannot extract encrypted .zip folders. Instead, install **7-zip** (which can be downloaded for free from www.7-zip.org), and extract the .zip with that instead.*

11. In the ***Ready To Export Rules*** field, administrators can configure the conditions which must be met, before an incident can be exported with this export profile. The conditions are based on how user-defined incident fields have been populated in the incident, and the rules are formatted using Motorola Solutions custom predicate language.

>> For more information, see Create New User-defined Incident Fields on page 264 and Appendix E: Custom Predicate Language on page 469

12. If ***Use Template for Title Page*** is set to ***On***, administrators can customise the export's title page, using markdown.

>> For more information, see Appendix F: Customise Export Title Pages on page 484

13. If ***Title pages***, ***Watermark logo***, and ***Watermark signature*** are set to ***Yes***, these settings will be applied by default.
14. If the toggles in the ***Overridable?*** column are set to ***Yes***, these settings can be changed by the user on a per-export basis, as they are being created in the ***Incidents*** tab.
15. From the ***Format*** dropdown, select the format for the export.

    PAL should be chosen if the exports will be played in Europe, Australia, or Asia. **NTSC** should be chosen if the exports will be played in the United States of America.
16. Click ***create*** to create the export profile.

9.4.2.2 MP4 Export Profile

Export profiles control how exports are handled on VideoManager (e.g. how they are formatted, etc.). To create an MP4 export profile:

1. Navigate to the ***Admin*** tab.
2. Select the ***Policies*** pane.
3. Click the ***Incident Exports*** section.
4. In the ***Export Profiles*** section, click ***Create new export profile***.

The ***Create Export Profile*** window will open.

5. In the ***Name*** field, enter a name for the export profile.
6. From the ***Type*** dropdown, select **MP4**.
7. If ***Selectable*** is set to ***Yes***, users can select this export profile when creating an export from the ***Incidents*** tab.

*Users with the **Use any export profile** permission will be able to select any profile, not just those which are enabled. This profile can also still be used if incidents are being exported automatically.*

8. If ***Default*** is set to ***Yes***, this export profile will be the default when creating an export from the ***Incidents*** tab.
9. If ***Select Clips*** is set to ***On***, users can manually select which incident clips will be included in the export when they export the incident.

Users cannot select individual clips if the incident they are exporting contains a composite clip.

If set to ***Off***, **all** incident clips within the incident will be included in the export.

10. If ***Encrypt Downloads*** is set to ***On***, the .zip folder containing exports with this profile will be protected with AES 256 encryption. The user must set a passphrase when they download the export to their PC; they must then enter the same passphrase when they extract the .zip folder.

*Windows cannot extract encrypted .zip folders. Instead, install **7-zip** (which can be downloaded for free from www.7-zip.org), and extract the .zip with that instead.*

11. In the ***Ready To Export Rules*** field, administrators can configure the conditions which must be met, before an incident can be exported with this export profile. The conditions are based on how user-defined incident fields have been populated in the incident, and the rules are formatted using Motorola Solutions custom predicate language.

>> For more information, see Create New User-defined Incident Fields on page 264 and Appendix E: Custom Predicate Language on page 469

12. If ***Use Template for Title Page*** is set to ***On***, administrators can customise the export's title page, using markdown.

>> For more information, see Appendix F: Customise Export Title Pages on page 484

13. If ***Title pages***, ***Watermark logo***, and ***Watermark signature*** are set to ***Yes***, these settings will be applied by default.
14. If the toggles in the ***Overridable?*** column are set to ***Yes***, these settings can be changed by the user on a per-export basis, as they are being created in the ***Incidents*** tab.
15. Click ***create*** to create the export profile.

9.4.2.3 Evidence Export Profile

Export profiles control how exports are handled on VideoManager (e.g. how they are formatted, etc.). To create an evidence export profile:

1. Navigate to the ***Admin*** tab.
2. Select the ***Policies*** pane.
3. Click the ***Incident Exports*** section.
4. In the ***Export Profiles*** section, click ***Create new export profile***.

The ***Create Export Profile*** window will open.

5. In the ***Name*** field, enter a name for the export profile.
6. From the ***Type*** dropdown, select **Evidence Export**.
7. If ***Selectable*** is set to ***Yes***, users can select this export profile when creating an export from the ***Incidents*** tab.

*Users with the **Use any export profile** permission will be able to select any profile, not just those which are enabled. This profile can also still be used if incidents are being exported automatically.*

8. If ***Default*** is set to ***Yes***, this export profile will be the default when creating an export from the ***Incidents*** tab.
9. If ***Select Clips*** is set to ***On***, users can manually select which incident clips will be included in the export when they export the incident.

Caution *Users cannot select individual clips if the incident they are exporting contains a composite clip.*

If set to ***Off***, **all** incident clips within the incident will be included in the export.

10. If ***Encrypt Downloads*** is set to ***On***, the .zip folder containing exports with this profile will be protected with AES 256 encryption. The user must set a passphrase when they download the export to their PC; they must then enter the same passphrase when they extract the .zip folder.

*Windows cannot extract encrypted .zip folders. Instead, install **7-zip** (which can be downloaded for free from www.7-zip.org), and extract the .zip with that instead.*

11. In the ***Ready To Export Rules*** field, administrators can configure the conditions which must be met, before an incident can be exported with this export profile. The conditions are based on how user-defined incident fields have been populated in the incident, and the rules are formatted using Motorola Solutions custom predicate language.

>> For more information, see Create New User-defined Incident Fields on page 264 and Appendix E: Custom Predicate Language on page 469

12. From the ***Export Location*** dropdown, select where the export will be sent to. The options are as follows: **Default**, **Output directory**, and **Box**.

If **Output directory** has been chosen, the administrator must configure the following settings:

- If ***Overwrite existing files*** is set to ***On***, the export will replace another export which is in the same folder with the same name.
- ***Output directory*** - enter the output directory for the export. This determines where the export will be sent.

If **Box** has been chosen, the administrator must configure VideoManager with their Box's unique information. Contact the network administrator.

Once the basic settings for the export profile have been configured, there are others settings that administrators can configure.

Export Metadata - this section controls what metadata will be exported alongside the incident.

- If ***Add Metadata File*** is set to ***On***, a separate metadata file will be exported alongside the incident file.
- From the ***Metadata File generation level*** dropdown, select which incidents should be exported. This is only relevant if the administrator has licensed *Nested Incidents*. The options are as follows:
  - **For all incident levels** - there will be separate metadata files for the main incident and the nested incidents.
  - **Only the main incident** - there will only be a metadata file for the main incident.
  - **Only nested incidents** - there will only be a metadata file for the nested incidents.
- In the ***Metadata Filename Template*** field, enter the filename template for the metadata file.
- In the ***Metadata Content Template*** field, enter the content template for the metadata file.
- If ***Include Commit File*** is set to ***On***, a file will be created and exported that indicates the export has been completed.

Original Footage - this section controls what original footage will be exported alongside the incident. It is only visible if ***Include original footage*** has been set to ***Yes***.

- If ***Use Template for Filename*** is set to ***On***, the administrator must enter a filename template in the ***Filename Template*** field.
- If ***Add Metadata File*** is set to ***On***, there will be separate metadata files for each original piece of footage. The administrator must enter a metadata filename template and

content template in the ***Metadata Filename Template*** and ***Metadata Content Template*** fields, respectively.

Clip Footage - this section controls what clipped footage will be exported alongside the incident. It is only visible if ***Include clip footage*** has been set to ***Yes***.

- If ***Use Template for Filename*** is set to ***On***, the administrator must enter a filename template in the ***Filename Template*** field.
- If ***Add Metadata File*** is set to ***On***, there will be separate metadata files for each incident clip. The administrator must enter a metadata filename template and content template in the ***Metadata Filename Template*** and ***Metadata Content Template*** fields, respectively.

Administrators can configure other aspects of an evidence bundle. These are controlled through toggles - the toggles in the left-hand column control whether the features will be enabled, and the toggles in the right-hand ***Overridable?*** column control whether users can override the pre-determined configuration when exporting an incident.

- If ***Watermark logo*** is set to ***On***, the export will include the previously-configured watermark over the footage in the incident.

This is configured in the ***Theme Resources*** section.

>> For more information, see Change and Reset Theme Resources on page 320

- If ***Watermark signature*** is set to ***On***, the export's automatically-created signature will be shown over the incident's footage.

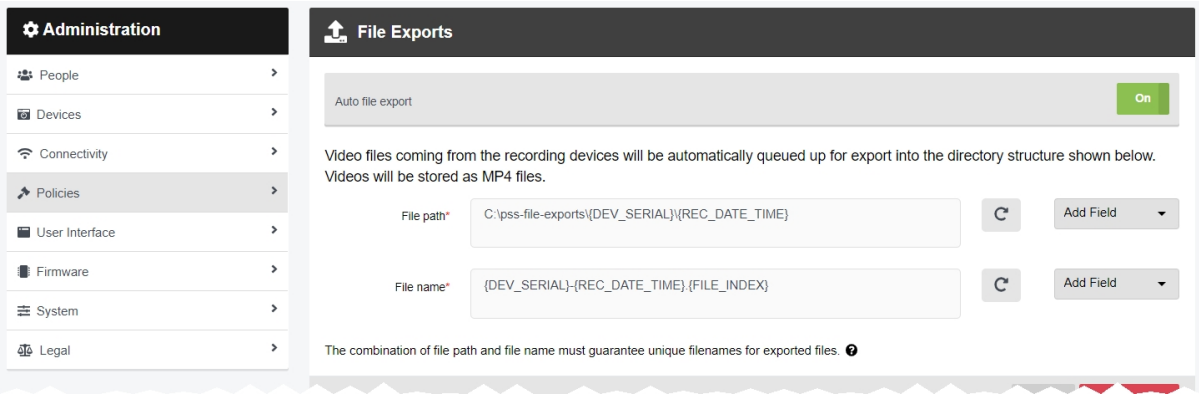
This corresponds with the information shown in the ***Job*** column in the ***My Exports*** pane.

- If ***Include original footage*** is set to ***On***, the export will include the original, full-length footage from which the incident clips were taken.
- If ***Include clip footage*** is set to ***On***, the export will include the incident clips themselves.
- If ***Include confidential metadata*** is set to ***On***, the export will include the incident's fields as a JSON file. This is useful if the user is planning to upload the incident to another instance of VideoManager - this will allow VideoManager to automatically populate the incident fields when the incident is uploaded.
- If ***Single file per incident clip*** is set to ***On***, this will include every redacted incident clip as individual video files instead of one long video file.

Click ***create*** to create the export profile.

9.4.3 Configure File Exports

Administrators can configure VideoManager so that it automatically copies videos to an external location as soon as they have been downloaded from the corresponding body-worn cameras. The videos will still be available on VideoManager like normal. This is done from the ***File Exports*** section of the ***Policies*** pane, in the ***Admin*** tab.



To enable and configure file exports:

1. Navigate to the ***Admin*** tab.
2. Select the ***Policies*** pane.
3. Click the ***File Exports*** section.
4. Set ***Auto file export*** to ***On***.
5. In the ***File path*** field, enter the file path to which videos will automatically be sent.

Administrators can add fields to this path which correlate with the video's properties. To do so, select the relevant fields from the ***Add Field*** dropdown. Separate each field with a slash.

These fields will send the video to sub-folders based on, for instance, the operator who recorded the video, or the body-worn camera's serial number.

If the specified folders do not already exist for this path, they will be created as soon as the videos are automatically exported.

6. If the path should be reset, click ***Reset to Default***.

The path will be reset to *C:\pss-file-exports\{DEV_SERIAL}\{REC_DATE_TIME}*.

7. In the ***File name*** field, enter the name that will be given to individual video files once they have been exported.

Administrators can add fields to this name which correlate with the video's properties, in addition to plaintext. To do so, select the relevant fields from the ***Add Field*** dropdown. Separate each field with a slash.

Caution *VideoManager will not save the **File name** field's configuration unless it generates a unique name for **every** exported video. Click ? for more information about how to guarantee unique names.*

8. If the name should be reset, click ***Reset to Default***.

The name will be reset to *{DEV_SERIAL}-{REC_DATE_TIME}.{FILE_INDEX}*.

9. Click ***Save settings***.

If administrators have licensed and configured CommandCentral Vault, they can configure file exports so the videos go straight there instead. To do so:

1. Ensure that CommandCentral Vault has been configured.

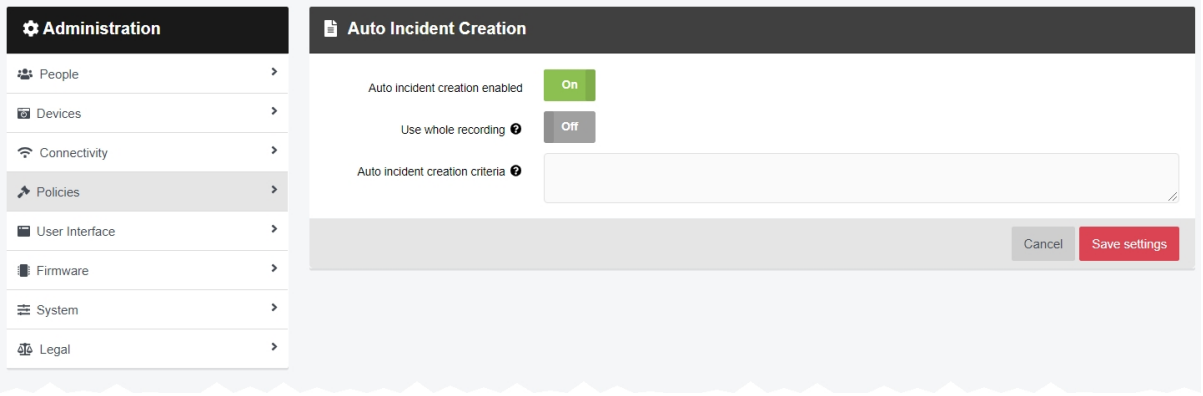
>> For more information, see Configure CommandCentral Vault Settings on page 306

2. Navigate to the ***Admin*** tab.
3. Select the ***Policies*** pane.
4. Click the ***File Exports*** section.
5. Set ***CommandCentral Vault Export*** to ***On***.
6. Administrators can view the CommandCentral Vault fields which map directly on to already-existing user-defined media fields.

Unlike user-defined incident fields, user-defined media fields can only be edited **after** the videos have been downloaded to VideoManager. Because file exports will send videos to CommandCentral Vault immediately, users will not have time to edit the user-defined media fields. For this reason, it is recommended that administrators contact Motorola Solutions Support regarding these user-defined media fields.

9.4.4 Enable and Configure Automatic Incident Creation

Administrators can configure VideoManager so it automatically creates incidents, depending on how a video/asset's user-defined media fields have been populated. This is done from the ***Auto Incident Creation*** section of the ***Policies*** pane, in the ***Admin*** tab.



To enable automatic incident creation:

1. Ensure that the *Media Properties* and *Incidents* licences have been enabled on VideoManager.

For more information, please contact edesixsales@motorolasolutions.com.

>> For more information, see Import and Delete Licences on page 353

2. Create user-defined media fields as necessary.

>> For more information, see Create New User-defined Media Fields on page 283

3. Navigate to the ***Admin*** tab.
4. Select the ***Policies*** pane.
5. Click the ***Auto Incident Creation*** section.
6. Set ***Auto incident creation enabled*** to ***On***.
7. If ***Use whole recording*** is set to ***On***, an entire recording will be added to an automatically-generated incident if **one** video within it meets the requirements for automatic incident creation.

If set to ***Off***, a recording will **not** be added to an incident if one of its videos meets the requirements for automatic incident creation. Instead, VideoManager will only create incidents for the individual videos which meet the requirements.

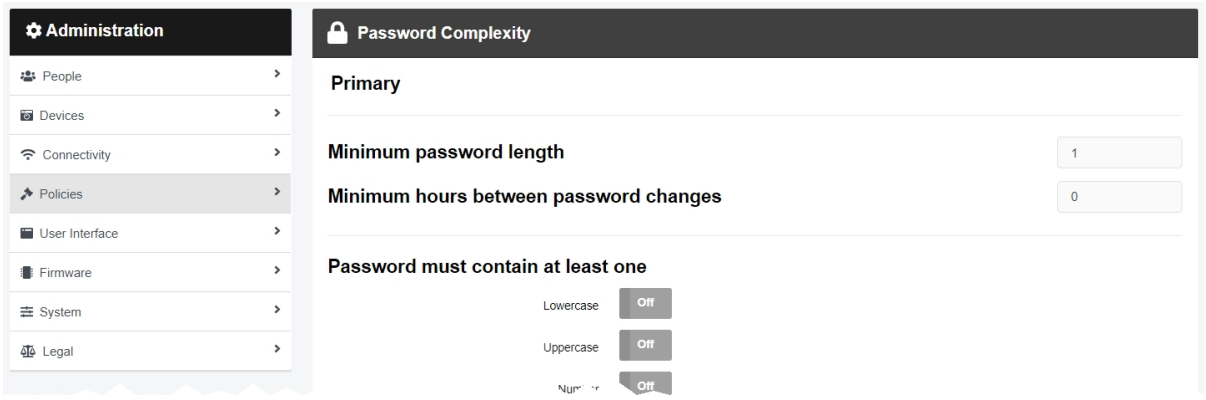
8. In the ***Auto incident creation criteria*** field, use Motorola Solutions custom predicate language to determine which user-defined media fields will prompt VideoManager to create an incident automatically.

>> For more information, see Appendix E: Custom Predicate Language on page 469

9. Click ***Save settings***.

9.4.5 Configure Password Complexity

It is possible to customise the VideoManager password settings to meet existing security regulations, and make VideoManager more secure. This is done from the ***Password Complexity*** section of the ***Policies*** pane, in the ***Admin*** tab.



The ***Password Complexity*** section is divided into ***Primary*** and ***Alternate*** requirements. By default, all passwords must meet the primary requirements. However, if there is a need for administrative passwords to be more secure than user passwords, the alternate requirements can be set more stringently and any role can be set to require passwords to meet them instead.

To configure password complexity:

1. Navigate to the ***Admin*** tab.
2. Select the ***Policies*** pane.
3. Click the ***Password Complexity*** section.
4. In the ***Minimum password length*** field, enter the minimum number of characters which users must meet.
5. In the ***Minimum hours between password changes*** field, enter the minimum number of hours for which a user's password must exist, after which it can be changed by them.

   This only affects a user's ability to change their own password from the ***Update password*** pane of their ***Account Profile*** tab. Administrators can still update passwords from the ***Users*** section, even if doing so violates the rule configured here.

   >> For more information, see Create, Edit, and Delete Users on page 165

6. If ***Lowercase*** is set to ***On***, a password must have at least one lowercase letter.
7. If ***Uppercase*** is set to ***On***, a password must have at least one uppercase letter.
8. If ***Number*** is set to ***On***, a password must have at least one number.
9. If ***Symbol*** is set to ***On***, a password must have at least one symbol.
10. If ***Disallow username in password*** is set to ***On***, a user cannot include their username in their password.

11. If ***Disallow repeated characters*** is set to ***On***, a password cannot have the same character multiple times in a row.

    The administrator must set the maximum number of repeated characters allowed by VideoManager (e.g. if the number is set to 1, then the password *Bubble* would be deemed inadmissible because it has two *b*s in a row).

12. If ***Disallow password reuse*** is set to ***On***, a password cannot match the user's previous passwords.

    The administrator must enter the number of previous passwords which the new password cannot match.

13. If ***Require periodic password changes*** is set to ***On***, the administrator must enter the number of days, after which passwords on VideoManager must be reset.

14. If ***Prevent repeated login attempts*** is set to ***On***, the administrator must enter the number of times someone can try to log in to VideoManager unsuccessfully, after which their account will be locked. The administrator must also enter the number of minutes for which the profile will be locked, before users can try to log in again.

    *Suitably privileged users can unlock other users from the **Users** section of the **People** pane, in the **Admin** tab.*

    >> *For more information, see* Unlock a User on page 171

15. If ***Temporary password expire*** is set to ***On***, a temporary password given to a user (e.g. because they have forgotten their password) will expire after a set number of hours.

    The administrator must enter the number of hours for which the password will be valid.

16. If ***Alternate*** is set to ***On***, the same password restrictions must be configured.

    Any roles which will be utilising the alternate password complexity must have ***Alternate*** set to ***Yes***.

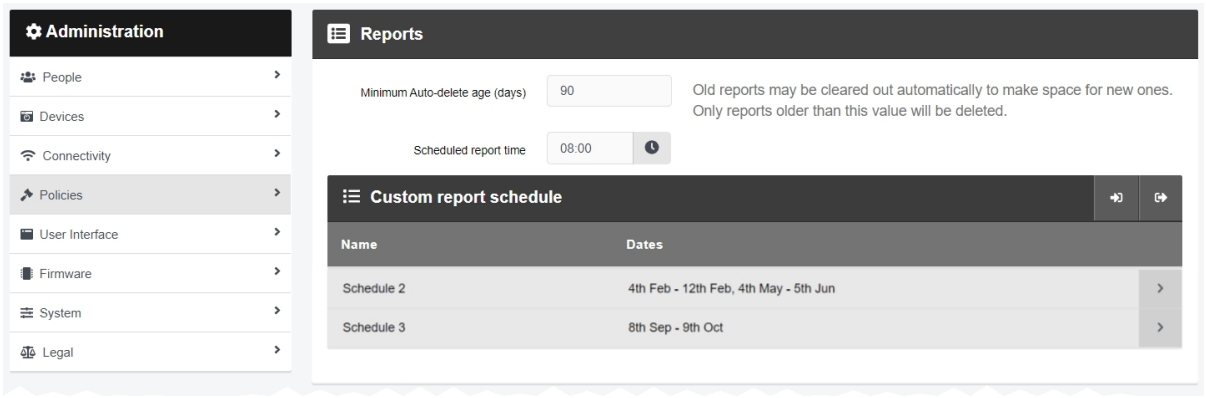
    >> For more information, see Create, Edit, Copy, Import, Export and Delete Roles on page 182

17. Click ***Save settings***.

If the password requirements for a role change, users must change their password upon next login so it meets the new requirements.

9.4.6 Configure Report Settings

VideoManager will automatically delete reports if the reports file space is becoming full. Administrators can configure when their reports will be deleted. They can also configure when scheduled reports will be run, and import a custom report schedule. This is done from the ***Reports*** section of the ***Policies*** pane, in the ***Admin*** tab.



To configure report settings:

1. Navigate to the ***Admin*** tab.
2. Select the ***Policies*** pane.
3. Click the ***Reports*** section.
4. In the ***Minimum Auto-delete age*** field, enter the minimum number of days for which reports must have existed, before they are considered for deletion.
5. In the ***Scheduled report time*** field, select the time of day at which scheduled reports should run.

   This setting will affect **all** scheduled reports on VideoManager, and only dictates when reports are generated, **not** what times they cover.
6. Click ***Save settings***.

Administrators can create a custom report schedule. This dictates what dates a scheduled report will cover, and is selectable by users when creating a scheduled report from the ***Status*** tab. To create and import a custom schedule:

1. Create a JSON file with the desired schedule.

   The administrator can create multiple schedules within one JSON file.

   The format is as follows:

```
[{"name":"NAME OF SCHEDULE",
 "scheduleDates": [{"startDay":DAY OF MONTH,"startMonth":
MONTH,"endDay":DAY OF MONTH,"endMonth":MONTH}]]
```

   The day and month should be entered numerically (e.g. April = 4, May = 5, etc).

In the following example, the JSON would import the schedule `Test`, which covers April 1st until May 20th.

```
[{"name":"Test",
 "scheduleDates": [{"startDay":1,"startMonth":
4,"endDay":20,"endMonth":5}]]
```

In the following example, the JSON would import the schedules `Test` and `Test-2`, which cover April 1st until May 20th and June 1st until July 20th, respectively.

```
[{"name":"Test",
 "scheduleDates": [{"startDay":1,"startMonth":
4,"endDay":20,"endMonth":5}] [{"name":"Test-2",
 "scheduleDates": [{"startDay":1,"startMonth":
6,"endDay":20,"endMonth":7}]]
```

2. Navigate to the ***Admin*** tab.
3. Select the ***Policies*** pane.
4. Click the ***Reports*** section.
5. In the ***Custom report schedule*** pane, click ***Import custom schedule***.
6. Select the relevant JSON file, and click ***import***.

The imported schedule(s) will immediately appear in the ***Custom report schedule*** pane. Users can now select the schedule from the ***Schedule*** dropdown when creating a report.

>> For more information, see Create Reports and Perform Report Actions on page 143

If administrators import a new JSON file to VideoManager, then all schedules with the same name will be overwritten, and all schedules not mentioned in the new JSON file will be deleted.

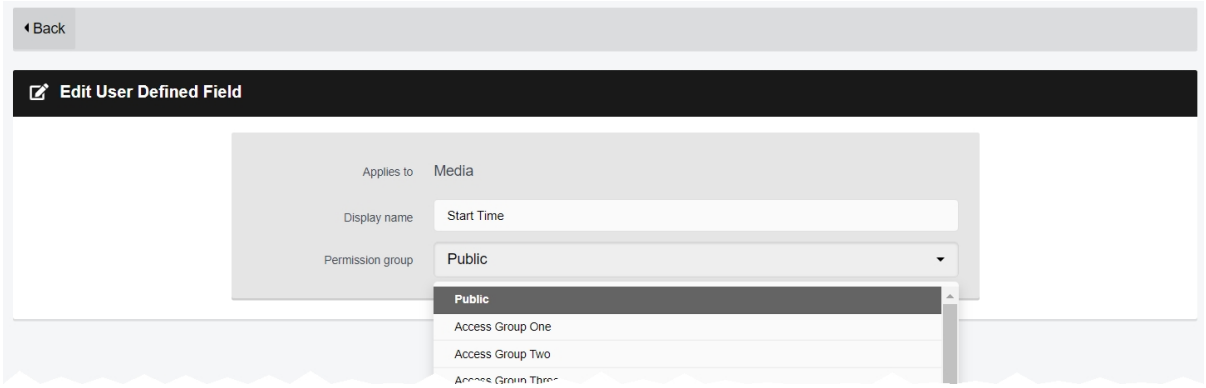
7. Click ***Save settings***.

9.4.7 Edit Default User-defined Incident Fields

Administrators can create user-defined incident fields to meet their organisation's unique needs - however, VideoManager also comes with two types of built-in user-defined incident field, which can be edited as well. The steps for editing default fields differ, depending on the type of field.

Default user-defined incident fields which are **manually populated** by users when creating incidents can have every aspect of their configuration edited (similar to non-default user-defined incident fields). These are the **title**, **incident-time**, **reference-code** and **notes** fields.

Default user-defined incident fields which are **automatically populated** by VideoManager when the incident is saved can only have specific aspects of their configuration edited. These are the **creation-time**, **update-time**, **clip-count**, **owner**, and **signature** fields, and have an icon next to their names.



To edit default user-defined incident fields:

1. Navigate to the ***Admin*** tab.
2. Select the ***Policies*** pane.
3. Click the ***User-defined Incident Fields*** section.
4. Next to the relevant default field, click ***Edit field***.

The following steps differ, depending on the kind of built-in field which will be edited.

If the administrator is editing a user-defined incident field which is **manually populated**:

1. In the ***Identifier*** field, optionally enter an updated identifier for the user-defined incident field.

   This should be all lowercase, and unique.
2. In the ***Display name*** field, optionally enter an updated display name for the user-defined incident field.
3. If ***Mandatory*** is set to ***On***, users will be unable to save an incident unless they populate this field.
4. From the ***Permission group*** dropdown, optionally select to which access group this user-defined incident field will apply. Any users in the selected access group will be able to view this user-defined incident field when creating and editing incidents.

5. From the ***Column width*** dropdown, optionally select how wide this user-defined incident field's column will appear in incident search results.

This is only relevant if the user-defined incident field has been configured to appear in the incident search results pane.

>> For more information, see on page 279

6. Depending on the kind of user-defined incident field which is being edited, administrators can also edit other settings:

   - If the administrator is editing the **title**, **reference-code**, or **notes** field, the administrator can change the configuration in the ***Text*** section.

   >> For more information, see on page 269

   - If the administrator is editing the **incident-time** field, the administrator can change the configuration in the ***Date &Time*** section.

   >> For more information, see on page 272

7. Click ***Save settings***.

If the administrator is editing a user-defined incident field which is **automatically populated** by VideoManager:

1. In the ***Display name*** field, optionally enter an updated display name for the user-defined incident field.
2. From the ***Permission group*** dropdown, optionally select to which access group this user-defined incident field will apply. Any users in the selected access group will be able to view this user-defined incident field when creating and editing incidents.
3. From the ***Column width*** dropdown, optionally select how wide this user-defined incident field's column will appear in incident search results.

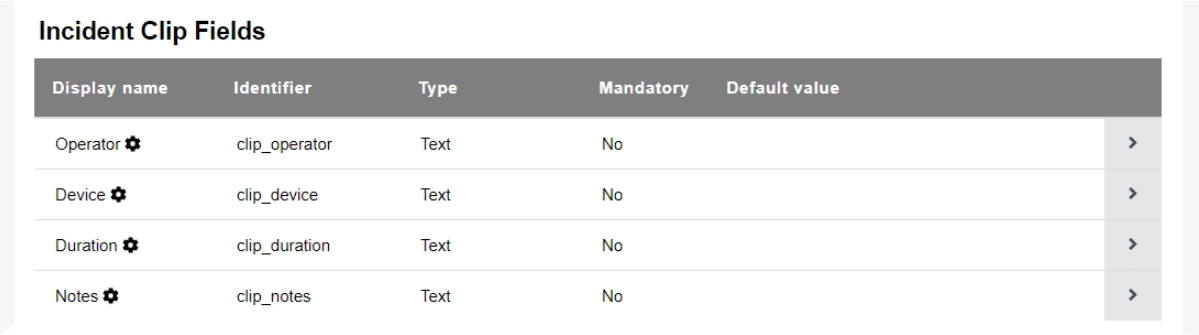
This is only relevant if the user-defined incident field has been configured to appear in the incident search results pane.

>> For more information, see on page 279

4. If ***Show in summary*** is set to ***No***, this user-defined incident field will not be visible when users edit and view incidents.
5. Click ***Save settings***.

9.4.8 Edit Incident Clip Fields

When a video is added to an incident, it becomes an incident clip. Incident clips have **four** properties: ***Operator:***, ***Device:***, ***Duration:***, and ***Notes***. By default, all users on VideoManager can see these four fields. However, administrators may wish to restrict which fields can be seen by users, based on the users' permission groups. This is done from the ***User-defined Incident Fields*** section of the ***Policies*** pane, in the ***Admin*** tab.



To edit incident clip fields:

1. Navigate to the ***Admin*** tab.
2. Select the ***Policies*** pane.
3. Click the ***User-defined Incident Fields*** section.
4. Scroll to the ***Incident Clip Fields*** section and click ***View field*** next to the field which will be edited.

There are four fields - one for each incident clip property.

5. From the ***Permission group*** dropdown, select which users will be able to view this incident clip property.

By default, the dropdown is set to **Public**, meaning that all users on VideoManager and anyone with an incident link can view this property. The administrator can select a specific permission group from the dropdown, so users can only view this property if one of their roles has this permission group enabled.

>> For more information, see Field Permissions on page 438

The administrator cannot edit the incident clip field further. Incident clip fields cannot be deleted, either.

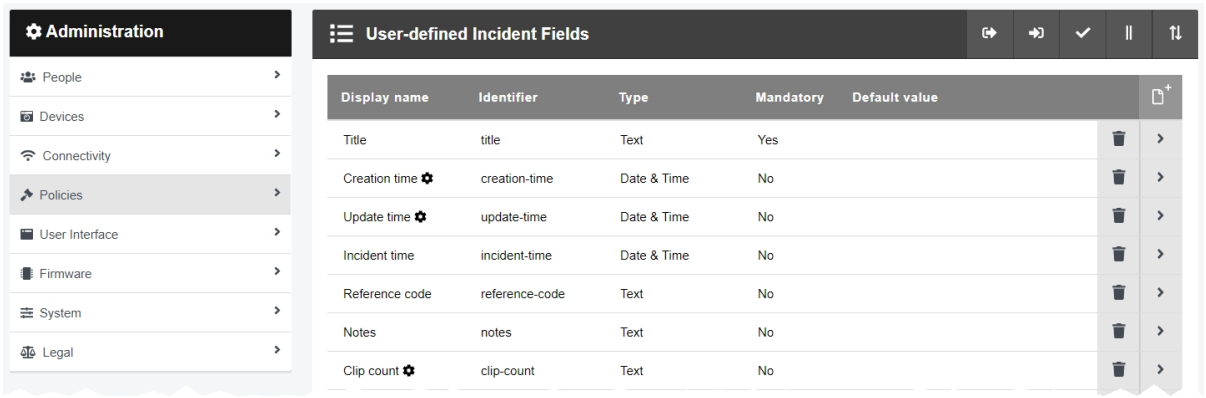
6. Click ***Save settings***.

Once incident clip fields have been configured, administrators can configure which of these fields are visible when viewing an incident link.

>> For more information, see Configure Sharing Policy on page 304

9.4.9 Create New User-defined Incident Fields

VideoManager comes with some built-in incident fields, which enable users to categorise incidents. Administrators can also create their own user-defined incident fields, and edit built-in fields, to reflect the unique needs of their organisation. This is done from the ***User-defined Incident Fields*** section of the ***Policies*** pane, in the ***Admin*** tab.



Before the administrator creates new user-defined incident fields, they can optionally create validators, which define how information entered into user-defined incident fields must be formatted (e.g. as a UK postcode).

>> For more information, see on page 268

To create a user-defined incident field:

1. Navigate to the ***Admin*** tab.
2. Select the ***Policies*** pane.
3. Click the ***User-defined Incident Fields*** section.
   - If the administrator is creating a user-defined incident field which users must populate while **creating** an incident, click ***Create field***.
   - If the administrator is creating a user-defined incident field which users must populate before **deleting** an incident, scroll to the ***Incident Deletion Fields*** section and click ***Create field***.
4. In the ***Identifier*** field, enter an identifier for the user-defined incident field.
   This should be all lowercase, and unique.
5. In the ***Display name*** field, enter a display name for the user-defined incident field.
   This will be what the user-defined incident field is called in the VideoManager UI.
6. If the administrator is creating a field, select the type of user-defined incident field to be created from the ***Type*** dropdown:
   - **Text** - in this user-defined incident field, users can enter text related to the incident.

This is useful if users need to search for a specific phrase or word (e.g. *Assault*, *Arrest*, etc.).

- **Date** - in this user-defined incident field, users can select a date related to the incident.
- **Date &Time** - in this user-defined incident field, users can select a date and time related to the incident.
- **Drop down** - in this user-defined incident field, users can select an option from a dropdown related to the incident.
- **Check box** - in this user-defined incident field, users can either check or uncheck a checkbox related to the incident.
- **URL** - in this user-defined incident field, users can enter a URL related to the incident.
- **Computed** - in this user-defined incident field, users can create URLs from previously-created user-defined incident fields. Administrators can also configure computed fields to appear - and change their appearance - based on how other user-defined incident fields have been populated.
- **Tag List** - in this user-defined incident field, users can select one or more tags related to the incident.

This cannot be changed later.

7. If ***Mandatory*** is set to ***On***, users will be unable to save an incident unless they populate this field.
8. From the ***Permission group*** dropdown, select to which access group this user-defined incident field will apply. Any users in the selected access group will be able to view and edit the user-defined incident field when creating and editing incidents.

If all users should be able to utilise this user-defined incident field when creating and editing incidents, select **Public**.

Computed fields do not need to have the same permission groups as the other user-defined incident fields which determine whether they appear or not. For example, if only some administrators should have the ability to populate the `[review-status]` field with sensitive information, but all users should be able to see the more general `[reviewed-already]` computed field, `[review-status]` could be set to **Access Group One**, while `[review-status]` could be set to **Public**.

9. From the ***Column width*** dropdown, select how wide this user-defined incident field's column will appear in incident search results.

This is only relevant if the user-defined incident field has been configured to appear in the incident search results pane.

>> For more information, see on page 279

The following steps differ, depending on the kind of user-defined incident field to be created:

- **Text**

>> For more information, see on page 269

- **Date**

>> For more information, see on page 271

- **Date &Time**

>> For more information, see on page 272

- **Drop down**

>> For more information, see on page 273

- **Check box**

>> For more information, see on page 274

- **URL**

>> For more information, see on page 275

- **Computed**

>> For more information, see on page 276

- **Tag List**

>> For more information, see on page 277

Once an administrator has created user-defined incident fields, there are actions which can be performed on these user-defined incident fields from the ***User-defined Incident Fields*** pane. They are as follows:

- Export user-defined incident fields from one instance of VideoManager, and import them into another instance.

>> For more information, see on page 278

- Configure how user-defined incident fields are presented when viewing incidents in the ***Search Incidents*** pane.

>> For more information, see on page 279

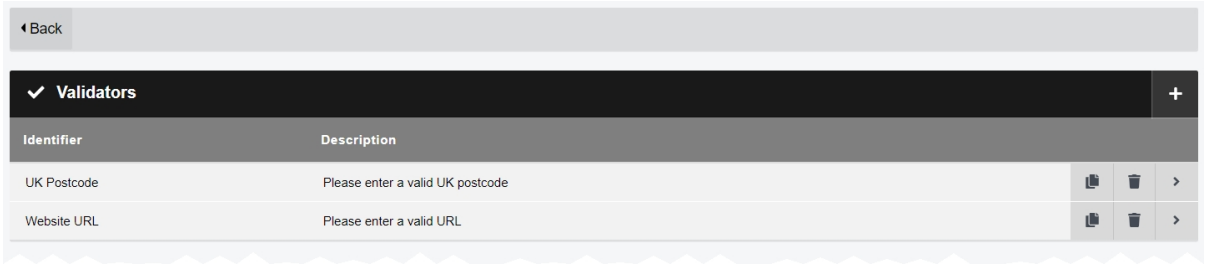
- Reorder user-defined incident fields, which affects how user-defined incident fields are

presented when creating an incident.

>> For more information, see on page 281

9.4.9.1 Create and Apply Validators

Administrators can control the format of information entered into user-defined incident fields. This is done through the creation of validators, which can be configured to accept certain patterns and reject others (e.g. a UK postcode or a URL).



To create a validator:

1. Navigate to the ***Admin*** tab.
2. Select the ***Policies*** pane.
3. Click the ***User-defined Incident Fields*** section.
4. Click ***Edit validators***.
5. Click ***Create validator***.
6. In the ***Identifier*** field, enter a unique name for the validator.
7. In the ***Description*** field, enter the text which users will see when populating a user-defined incident field.

   This should detail the format to which the user-defined incident field will adhere.
8. In the ***Pattern*** field, enter the pattern of the validator itself. This should be done utilising regular expressions.
9. If ***Case insensitive*** is set to ***On***, the validator will ignore the case of the text entered into the user-defined incident field.

   If set to ***Off***, the case of the text entered into the user-defined incident field must match that of the ***Pattern*** field exactly.
10. If the administrator wishes to test the validator, they can enter example text into the ***Test text*** field.

    VideoManager will determine whether the example text would be accepted by the validator or not.
11. Click ***Confirm***.

Once validators have been created, they must be individually applied to user-defined incident fields. This ensures that the user-defined incident fields will obey the patterns detailed in the validators. This must be done **during** user-defined incident field creation - validators cannot be edited after a user-defined incident field has been created.

>> For more information, see Create New User-defined Incident Fields on page 264

9.4.9.2 Create Text Fields

Once the administrator has selected **Text** from the ***Type*** dropdown, the following configuration options will appear in the ***Text*** section:

1. In the ***Number of lines*** field, enter the number of lines (1-50) which will be displayed at once when viewing the text field in an incident. This does not restrict the actual number of lines which can be entered.

For example, if the number of lines is set to 3 and there are 4 lines of text in an incident's text field, a scroll bar will appear on the right-hand side of the pane to show the last line.

2. From the ***Validator*** dropdown, select a previously-created validator or leave as **(None)**.

This will dictate how the text field must be formatted e.g. as a UK postcode.

>> For more information, see on the previous page

3. In the ***Default value*** field, enter a default value. This will be the value if nothing else is entered into the text field.

*If the administrator has selected a validator from the **Validator** dropdown, the default value in the **Default value** field must match this validator.*

4. If ***Include in match text search*** is set to ***On***, incidents can be filtered by the text entered into this text field, using the ***Match Text*** field in the ***Search Incidents*** pane.

5. If ***Show search field*** is set to ***On***, a field will appear in the ***Search Incidents*** pane that enables users to filter incidents **only** by text entered into this text field.

>> For more information, see Search Incidents on page 78

6. In the ***Conditions*** section, administrators can configure whether this user-defined incident field only appears in the ***New Incident*** pane when another drop down field or check box field has been populated in a specific manner. To do so:

   - Ensure there is at least **one** drop down field or check box field on VideoManager already. Conditions can only be used on these fields.
   - Click ***New condition***.
   - From the ***Field*** dropdown, select which previously-created user-defined incident field will dictate the appearance of the current user-defined incident field.
   - From the ***Value*** dropdown, select which of the previously-created user-defined incident field's values will dictate the appearance of the current user-defined incident field.

   This will be presented as a checkbox if a check box field has been chosen, and a dropdown if a drop down field has been chosen.

- Click ***confirm***.

7. Click ***Save settings***.

9.4.9.3 Create Date Fields

Once the administrator has selected **Date** from the ***Type*** dropdown, the following configuration options will appear in the ***Date*** section:

1. In the ***Default value*** field, enter a default value. This will be the value if nothing else is entered into the date field.
2. If ***Search by range*** is set to ***On***, a field will appear in the ***Search Incidents*** pane that enables users to filter incidents **only** by a range of dates entered into this date field.

If set to ***Off***, users can only filter by *one* date at a time.

*This change will not come into effect unless **Show search field** is also set to **On**.*

3. If ***Include in date search*** is set to ***On***, incidents can be filtered by the date entered into this date field, using the ***Earliest date*** and ***Latest date*** fields in the ***Search Incidents*** pane.
4. If ***Show search field*** is set to ***On***, a field will appear in the ***Search Incidents*** pane that enables users to filter incidents **only** by the dates entered into this date field.

>> For more information, see Search Incidents on page 78

5. In the ***Conditions*** section, administrators can configure whether this user-defined incident field only appears in the ***New Incident*** pane when another drop down field or check box field has been populated in a specific manner. To do so:
   - Ensure there is at least **one** drop down field or check box field on VideoManager already. Conditions can only be used on these fields.
   - Click ***New condition***.
   - From the ***Field*** dropdown, select which previously-created user-defined incident field will dictate the appearance of the current user-defined incident field.
   - From the ***Value*** dropdown, select which of the previously-created user-defined incident field's values will dictate the appearance of the current user-defined incident field.

   This will be presented as a checkbox if a check box field has been chosen, and a dropdown if a drop down field has been chosen.
   - Click ***confirm***.
6. Click ***Save settings***.

9.4.9.4 Create Date and Time Fields

Once the administrator has selected **Date &Time** from the ***Type*** dropdown, the following configuration options will appear in the ***Date &Time*** section:

1. In the ***Default value*** field, enter a default value. This will be the value if nothing else is entered into the date and time field.

By clicking ***Set to now***, users can set the default value to the server's current date and time.

2. If ***Include in date search*** is set to ***On***, incidents can be filtered by the date entered into this date and time field, using the ***Earliest date*** and ***Latest date*** fields in the ***Search Incidents*** pane.

3. If ***Show search field*** is set to ***On***, a field will appear in the ***Search Incidents*** pane that enables users to filter incidents **only** by the date and time entered into this date and time field.

>> For more information, see Search Incidents on page 78

4. In the ***Conditions*** section, administrators can configure whether this user-defined incident field only appears in the ***New Incident*** pane when another drop down field or check box field has been populated in a specific manner. To do so:

   - Ensure there is at least **one** drop down field or check box field on VideoManager already. Conditions can only be used on these fields.
   - Click ***New condition***.
   - From the ***Field*** dropdown, select which previously-created user-defined incident field will dictate the appearance of the current user-defined incident field.
   - From the ***Value*** dropdown, select which of the previously-created user-defined incident field's values will dictate the appearance of the current user-defined incident field.

   This will be presented as a checkbox if a check box field has been chosen, and a dropdown if a drop down field has been chosen.

   - Click ***confirm***.

5. Click ***Save settings***.

9.4.9.5 Create Drop Down Fields

Once the administrator has selected **Drop down** from the ***Type*** dropdown, the following configuration options will appear in the ***Drop down*** section:

1. Click + ***New value***. This will add an option to the drop down field, which the user can select when creating an incident. In the ***Value*** field, enter the name of the dropdown option. Click ***confirm***.

   It is possible to create a drop down field with just one value.

2. From the ***Default value*** dropdown, select a default value. This will be the value if nothing else is selected from the drop down field.
3. If ***Include in match text search*** is set to ***On***, incidents can be filtered by the value of the drop down field, using the ***Match Text*** field in the 🔍 ***Search Incidents*** pane.

For example - if the user selects a value from the drop down field called **Assault**, they should enter **Assault** into the ***Match Text*** field.

4. If ***Show search field*** is set to ***On***, a dropdown will appear in the 🔍 ***Search Incidents*** pane that enables users to filter incidents **only** by the value chosen from this drop down field.

>> For more information, see Search Incidents on page 78

5. In the ***Conditions*** section, administrators can configure whether this user-defined incident field only appears in the ***New Incident*** pane when another drop down field or check box field has been populated in a specific manner. To do so:
   - Ensure there is at least **one** drop down field or check box field on VideoManager already. Conditions can only be used on these fields.
   - Click + ***New condition***.
   - From the ***Field*** dropdown, select which previously-created user-defined incident field will dictate the appearance of the current user-defined incident field.
   - From the ***Value*** dropdown, select which of the previously-created user-defined incident field's values will dictate the appearance of the current user-defined incident field.

   This will be presented as a checkbox if a check box field has been chosen, and a dropdown if a drop down field has been chosen.

   - Click ***confirm***.
6. Click ***Save settings***.

9.4.9.6 Create Check Box Fields

Once the administrator has selected **Check box** from the ***Type*** dropdown, the following configuration options will appear in the ***Check box*** section:

1. From the ***Default value*** field, select a default value. This will be the value if the check box field is not edited during the creation of the incident.

This can either be checked or unchecked.

2. If ***Show search field*** is set to ***On***, a checkbox will appear in the ***Search Incidents*** pane that enables users to filter incidents **only** by whether this check box field has been checked or not.

>> For more information, see Search Incidents on page 78

3. In the ***Conditions*** section, administrators can configure whether this user-defined incident field only appears in the ***New Incident*** pane when another drop down field or check box field has been populated in a specific manner. To do so:

   - Ensure there is at least **one** drop down field or check box field on VideoManager already. Conditions can only be used on these fields.
   - Click ***New condition***.
   - From the ***Field*** dropdown, select which previously-created user-defined incident field will dictate the appearance of the current user-defined incident field.
   - From the ***Value*** dropdown, select which of the previously-created user-defined incident field's values will dictate the appearance of the current user-defined incident field.

   This will be presented as a checkbox if a check box field has been chosen, and a dropdown if a drop down field has been chosen.

   - Click ***confirm***.

4. Click ***Save settings***.

9.4.9.7 Create URL Fields

Once the administrator has selected **URL** from the ***Type*** dropdown, the following configuration options will appear in the ***URL*** section:

1. In the ***Default value*** field, enter a default value. This will be the value if nothing else is entered into the URL field.

   This must be in an URL format.

2. If ***Include in match text search*** is set to ***On***, incidents can be filtered by the URL entered into this text field, using the ***Match Text*** field in the ***Search Incidents*** pane.
3. In the ***Conditions*** section, administrators can configure whether this user-defined incident field only appears in the ***New Incident*** pane when another drop down field or check box field has been populated in a specific manner. To do so:
   - Ensure there is at least **one** drop down field or check box field on VideoManager already. Conditions can only be used on these fields.
   - Click ***New condition***.
   - From the ***Field*** dropdown, select which previously-created user-defined incident field will dictate the appearance of the current user-defined incident field.
   - From the ***Value*** dropdown, select which of the previously-created user-defined incident field's values will dictate the appearance of the current user-defined incident field.

   This will be presented as a checkbox if a check box field has been chosen, and a dropdown if a drop down field has been chosen.

   - Click ***confirm***.
4. Click ***Save settings***.

9.4.9.8 Create Computed Fields

Once the administrator has selected **Computed** from the ***Type*** dropdown, the following configuration options will appear in the ***Computed*** section:

1. In the ***Expression*** field, enter the relevant text using Motorola Solutions custom predicate language.

>> For more information, see Appendix E: Custom Predicate Language on page 469

2. If ***As Url*** is set to ***On***, the field will be presented as a URL when creating an incident.

The `encodeURIComponent()` function allows users to encode a string to make it suitable for use in a URL - even if the string contains characters which would normally not be allowed in a URL.

3. In the ***Conditions*** section, administrators can configure whether this user-defined incident field only appears in the ***New Incident*** pane when another drop down field or check box field has been populated in a specific manner. To do so:

   - Ensure there is at least **one** drop down field or check box field on VideoManager already. Conditions can only be used on these fields.
   - Click + ***New condition***.
   - From the ***Field*** dropdown, select which previously-created user-defined incident field will dictate the appearance of the current user-defined incident field.
   - From the ***Value*** dropdown, select which of the previously-created user-defined incident field's values will dictate the appearance of the current user-defined incident field.

   This will be presented as a checkbox if a check box field has been chosen, and a dropdown if a drop down field has been chosen.

   - Click ***confirm***.

4. Click ***Save settings***.

9.4.9.9 Create Tag List Fields

Once the administrator has selected **Tag List** from the ***Type*** dropdown, the following configuration options will appear in the ***Tag List*** section:

1. Click + ***New value***. This will add an option to the tag list field, which the user can select when creating an incident. Click ***confirm***.

   It is possible to create a tag list field with just one value.

2. From the ***Default value*** dropdown, select a default value. This will be the value if nothing else is selected in the tag list field.
3. If ***Show search field*** is set to ***On***, a field will appear in the 🔍 ***Search Incidents*** pane that enables users to filter incidents **only** by the value chosen from this tag list field.

   >> For more information, see Search Incidents on page 78

4. In the ***Conditions*** section, administrators can configure whether this user-defined incident field only appears in the ***New Incident*** pane when another drop down field or check box field has been populated in a specific manner. To do so:
   - Ensure there is at least **one** drop down field or check box field on VideoManager already. Conditions can only be used on these fields.
   - Click + ***New condition***.
   - From the ***Field*** dropdown, select which previously-created user-defined incident field will dictate the appearance of the current user-defined incident field.
   - From the ***Value*** dropdown, select which of the previously-created user-defined incident field's values will dictate the appearance of the current user-defined incident field.

   This will be presented as a checkbox if a check box field has been chosen, and a dropdown if a drop down field has been chosen.

   - Click ***confirm***.
5. Click ***Save settings***.

9.4.9.10 Export and Import User-Defined Incident Fields

If a user has multiple instances of VideoManager, they may wish to transfer a copy of their user-defined incident fields from one instance to another. To do so:

1. In the original instance of VideoManager, navigate to the ***Admin*** tab.
2. Select the ***Policies*** pane.
3. Click the ***User-defined Incident Fields*** section.
4. Click ***Export***.

   The user-defined incident fields will be saved to the PC's default download location.
5. In the new instance of VideoManager (or a site, if ***User-defined Fields*** has been set to ***Off*** in the ***Metadata/Footage Replication*** section), navigate to the ***Admin*** tab.
6. Select the ***Policies*** pane.
7. Click the ***User-defined Incident Fields*** section.
8. Click ***Import***.

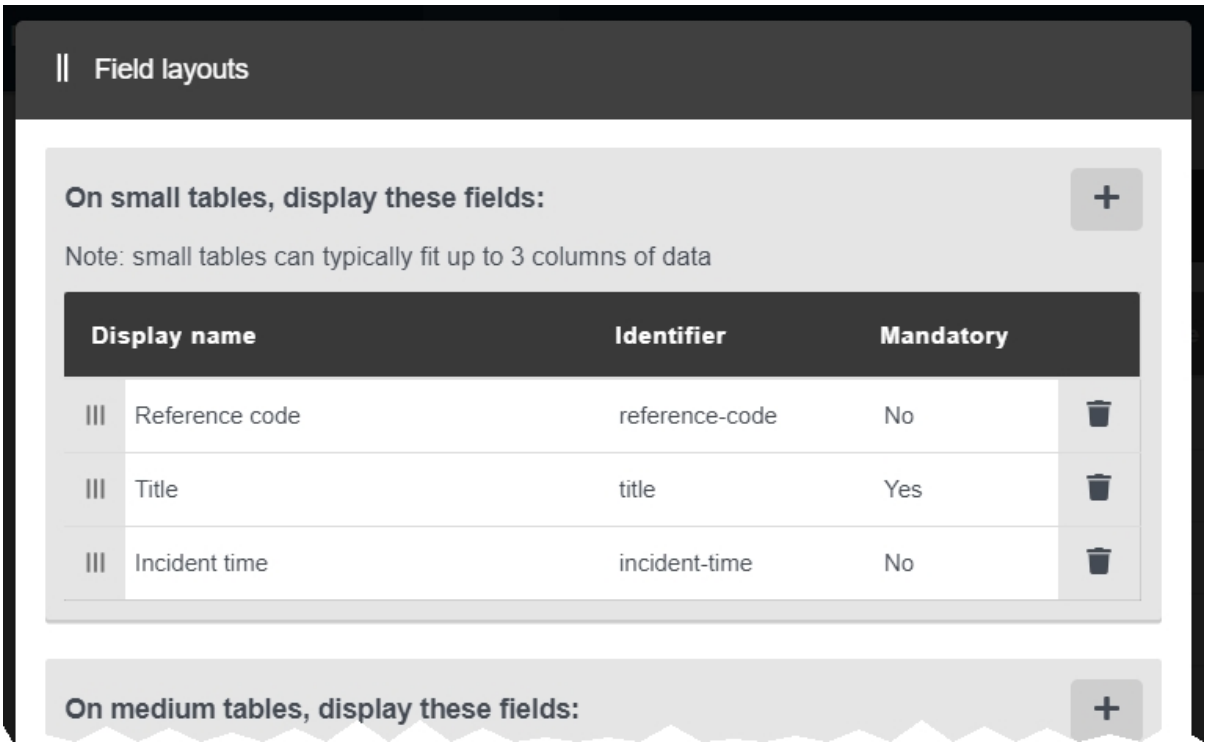
   Select the previously downloaded user-defined incident fields.
9. Click ***Import***.

Alternatively, if an administrator wants to import **all** of their user-defined incident fields simultaneously, they can do so from the ***Import/Export System Config*** section of the ***System*** pane in the ***Admin*** tab.

>> For more information, see Import or Export VideoManager's Configuration on page 356

9.4.9.11 Configure User-Defined Field Layouts

When a user searches for incidents, they are presented with a table showing all relevant incidents in the **Search Incidents** pane. Administrators can configure which user-defined incident fields - if any - are shown in this table.



To configure the user-defined incident field layouts:

1. Navigate to the ***Admin*** tab.
2. Select the ***Policies*** pane.
3. Click the ***User-defined Incident Fields*** section.
4. Click ***Field layouts***.

The administrator is presented with the following sections:

- ***Small tables*** - this shows which user-defined incident fields will be displayed in a small table (e.g. on a mobile phone).
- ***Medium tables*** - this shows which user-defined incident fields will be displayed in a medium table (e.g. on a tablet).
- ***Large tables*** - this shows which user-defined incident fields will be displayed in a large table (e.g. on a computer).

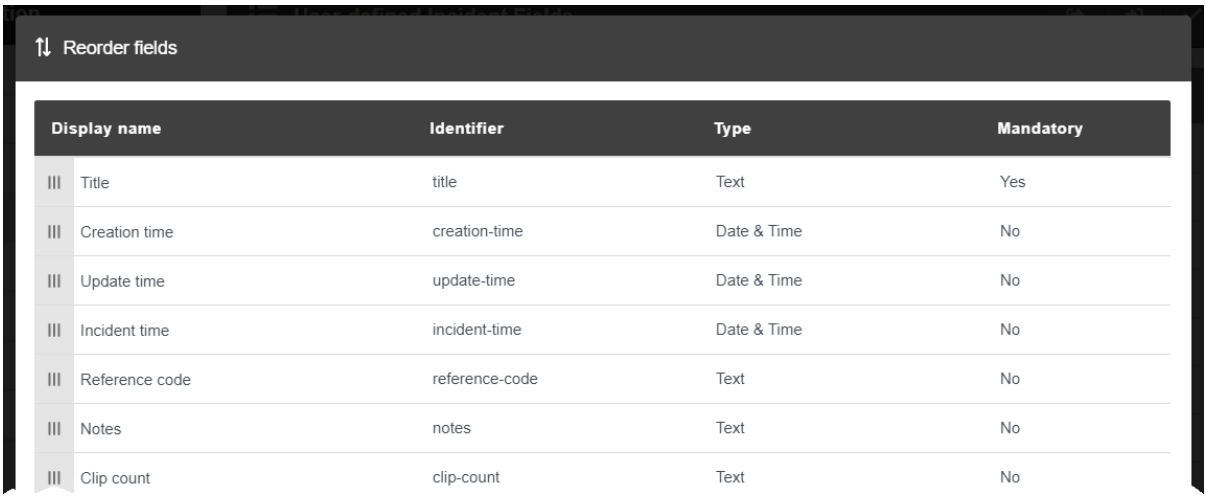
5. In the relevant section, click **+**.
6. From the dropdown, select which user-defined incident field should be added to the table.

The user-defined incident field will be added to the bottom of the list.

7. If necessary, rearrange the user-defined incident fields in the table by grabbing the left-hand side of the relevant user-defined incident field and dragging it to the desired location in the list.
8. Click ***save changes***.

9.4.9.12 Reorder User-Defined Incident Fields

Administrators can reorder user-defined incident fields. This changes the order in which they are presented during incident creation. This is done from the ***User-defined Incident Fields*** section of the ***Policies*** pane, in the ***Admin*** tab.



To reorder user-defined incident fields:

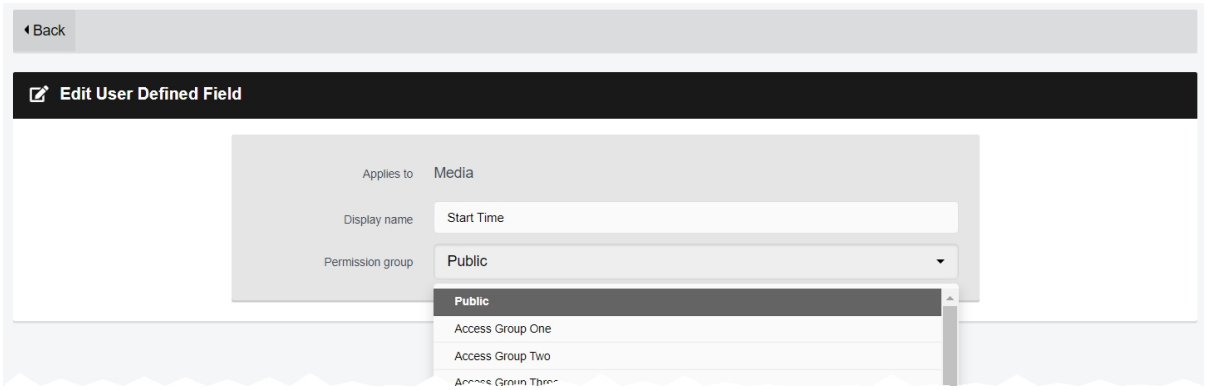
1. Navigate to the ***Admin*** tab.
2. Select the ***Policies*** pane.
3. Click the ***User-defined Incident Fields*** section.
4. Click ***Reorder fields***.
5. Grab the left-hand side of the relevant user-defined incident field and drag it to the desired location in the list.
6. Click ***confirm***.

When users create an incident, the user-defined incident fields to be populated will be presented in the same order which has been configured here.

>> For more information, see Create Incidents Manually and Perform Incident Actions on page 49

9.4.10 Edit Default User-defined Media Fields

VideoManager comes with built-in user-defined media fields. Some of these fields can be edited from the ***Videos*** tab to categorise media on the system, while others are populated by VideoManager automatically. By default, all users on VideoManager can see these fields. However, administrators may wish to restrict which of these built-in fields can be seen by users, based on the users' permission groups. This is done from the ***User-defined Media Fields*** section of the ***Policies*** pane, in the ***Admin*** tab.



To edit VideoManager's default user-defined media fields:

1. Navigate to the ***Admin*** tab.
2. Select the ***Policies*** pane.
3. Click the ***User-defined Media Fields*** section.
4. Default user-defined media fields are marked with an icon. Next to the relevant default field, click ***Edit field***.
5. From the ***Permission group*** dropdown, select which users will be able to view this user-defined media field.

   By default, the dropdown is set to **Public**, meaning that all users on VideoManager can view this field. The administrator can select a specific permission group from the dropdown, so users can only view this field if one of their roles has this permission group enabled.

   The administrator cannot edit the user-defined media field further. Default user-defined media fields cannot be deleted, either.

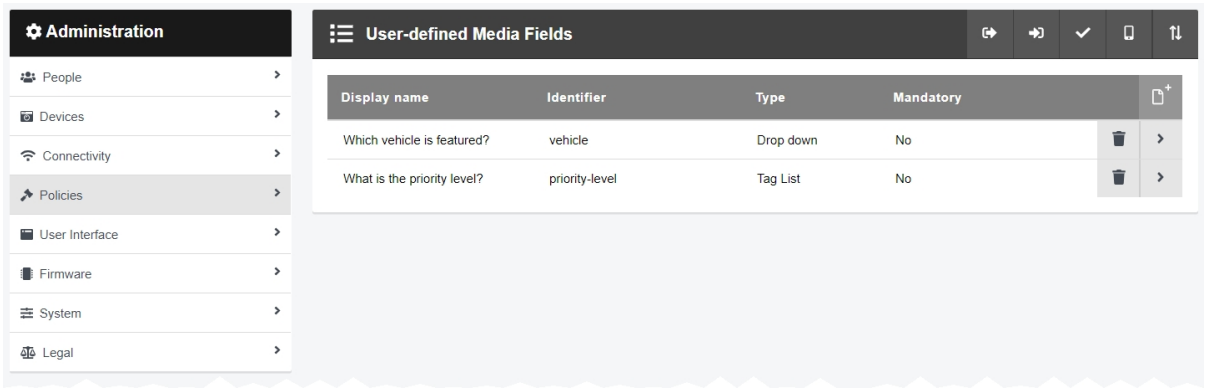
6. Click ***Save settings***.

From now on, only users in a role which has the specified permission group enabled will be able to see and edit this default user-defined media field. Administrators can check a user's permission groups from the ***Field permissions*** pane of the ***Roles*** section.

>> For more information, see Create, Edit, Copy, Import, Export and Delete Roles on page 182

9.4.11 Create New User-defined Media Fields

VideoManager comes with some built-in media fields, which enable users to categorise videos/assets as they are being edited. However, administrators can also create their own user-defined media fields, to reflect the unique needs of their organisation. This is done from the ***User-defined Media Fields*** section of the ***Policies*** pane, in the ***Admin*** tab.



Before the administrator creates user-defined media fields, they can optionally create validators, which define how information entered into user-defined media fields must be formatted (e.g. as a UK postcode).

>> For more information, see on page 286

To create a user-defined media field:

1. Navigate to the ***Admin*** tab.
2. Select the ***Policies*** pane.
3. Click the ***User-defined Media Fields*** section.
4. Click ***Create field***.
5. In the ***Identifier*** field, enter an identifier for the user-defined media field.
   This should be all lowercase, and unique.
6. In the ***Display name*** field, enter a display name for the user-defined media field.
   This will be what the user-defined media field is called in the VideoManager UI.
7. From the ***Type*** dropdown, select the type of user-defined media field to be created.
   - **Text** - in this user-defined media field, users can enter text related to the video/asset.

     This is useful if users need to search for a specific phrase or word (e.g. *Assault*, *Arrest*, etc.).
   - **Date** - in this user-defined media field, users can select a date related to the video/asset.
   - **Date &Time** - in this user-defined media field, users can select a date and time related to the video/asset.

- **Drop down** - in this user-defined media field, users can select an option from a dropdown related to the video/asset.
- **Check box** - in this user-defined media field, users can either check or uncheck a checkbox related to the video/asset.
- **URL** - in this user-defined media field, users can enter a URL related to the video/asset.
- **Computed** - in this user-defined media field, users can create URLs from previously-created user-defined media fields. Administrators can also configure computed fields to appear - and change their appearance - based on how other user-defined media fields have been populated.

Computed fields do not need to have the same permission groups as the other user-defined media fields which determine whether they appear or not. For example, if only some administrators should have the ability to populate the `[review-status]` field with sensitive information, but all users should be able to see the more general `[reviewed-already]` computed field, `[review-status]` could be set to **Access Group One**, while `[review-status]` could be set to **Public**.

- **Tag List** - in this user-defined media field, users can select one or more tags related to the video/asset.

This cannot be changed later.

8. If ***Mandatory*** is set to ***On***, users will be unable to save an video/asset unless they populate this field.
9. From the ***Permission group*** dropdown, select to which access group this user-defined media field will apply. Any users in the selected access group will be able to view and edit the user-defined media field when creating and editing videos/assets.

If all users should be able to utilise this user-defined media field when creating and editing videos/assets, select **Public**.

The following steps differ, depending on the kind of user-defined media field to be created:

- **Text**

>> For more information, see on page 287

- **Date**

>> For more information, see on page 289

- **Date &Time**

>> For more information, see on page 290

- **Drop down**

>> For more information, see on page 291

- **Check box**

>> For more information, see on page 292

- **URL**

>> For more information, see on page 293

- **Computed**

>> For more information, see on page 294

- **Tag List**

>> For more information, see on page 295

Once an administrator has created user-defined media fields, there are actions which can be performed on these user-defined media fields from the ***User-defined Media Fields*** pane. They are as follows:

- Export user-defined media fields from one instance of VideoManager, and import them into another instance.

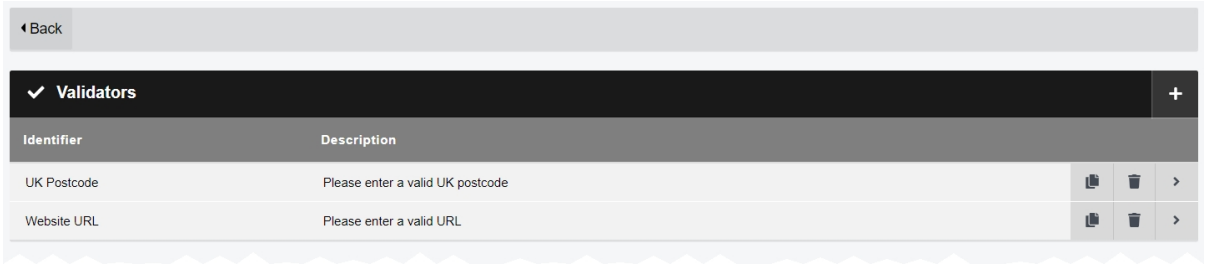
>> For more information, see on page 278

- Reorder user-defined media fields, which affects how user-defined media fields are presented when editing a video/asset.

>> For more information, see on page 281

9.4.11.1 Create and Apply Validators

Administrators can control the format of information entered into user-defined media fields. This is done through the creation of validators, which can be configured to accept certain patterns and reject others (e.g. a UK postcode or a URL).



To create a validator:

1. Navigate to the ***Admin*** tab.
2. Select the ***Policies*** pane.
3. Click the ***User-defined Media Fields*** section.
4. Click ***Edit validators***.
5. Click ***Create validator***.
6. In the ***Identifier*** field, enter a unique name for the validator.
7. In the ***Description*** field, enter the text which users will see when populating a user-defined media field.

   This should detail the format to which the user-defined media field will adhere.
8. In the ***Pattern*** field, enter the pattern of the validator itself. This should be done utilising regular expressions.
9. If ***Case insensitive*** is set to ***On***, the validator will ignore the case of the text entered into the user-defined media field.

   If set to ***Off***, the case of the text entered into the user-defined media field must match that of the ***Pattern*** field exactly.
10. If the administrator wishes to test the validator, they can enter example text into the ***Test text*** field.

    VideoManager will determine whether the example text would be accepted by the validator or not.
11. Click ***Confirm***.

Once validators have been created, they must be individually applied to user-defined media fields. This ensures that the user-defined media fields will obey the patterns detailed in the validators. This must be done **during** user-defined media field creation - validators cannot be edited after a user-defined media field has been created.

>> For more information, see Create New User-defined Media Fields on page 283

9.4.11.2 Create Text Fields

Once the administrator has selected **Text** from the ***Type*** dropdown, the following configuration options will appear in the ***Text*** section:

1. In the ***Number of lines*** field, enter the number of lines (1-50) which will be displayed at once when viewing the text field in a video/asset. This does not restrict the actual number of lines which can be entered.

For example, if the number of lines is set to 3 and there are 4 lines of text in a video's text field, a scroll bar will appear on the right-hand side of the pane to show the last line.

2. From the ***Validator*** dropdown, select a previously-created validator or leave as **(None)**.

This will dictate how the text field must be formatted e.g. as a UK postcode.

>> For more information, see on the previous page

3. In the ***Default value*** field, enter a default value. This will be the value if nothing else is entered into the text field.

*If the user has selected a validator from the **Validator** dropdown, the default value in the **Default value** field must match this validator.*

4. If ***Include in match text search*** is set to ***On***, videos/assets can be filtered by the text entered into this text field, using the ***Match Text*** field in the ***Search Videos*** pane.

5. If ***Show search field*** is set to ***On***, a field will appear in the ***Search Videos*** pane that enables users to filter videos/assets **only** by text entered into this text field.

>> For more information, see Search Videos on page 19

6. If ***Show in Incidents*** is set to ***On***, the way this field has been populated will be viewable in the ***Incident clips*** section of the incident editor once the video/asset has been added to an incident.

7. In the ***Conditions*** section, users can configure whether this user-defined media field only appears in the ***Edit properties*** pane when another drop down field or check box field has been populated in a specific manner. To do so:

   - Ensure there is at least **one** drop down field or check box field on VideoManager already. Conditions can only be used on these fields.
   - Click ***New condition***.
   - From the ***Field*** dropdown, select which drop down field or check box field will dictate the appearance of this user-defined media field.
   - From the ***Value*** dropdown, select which of the drop down field or check box field's values will dictate the appearance of this user-defined media field.

This will be presented as a checkbox if a check box field has been chosen, and a dropdown if a drop down field has been chosen.

- Click ***confirm***.

8. Click ***Save settings***.

9.4.11.3 Create Date Fields

Once the administrator has selected **Date** from the ***Type*** dropdown, the following configuration options will appear in the ***Date*** section:

1. In the ***Default value*** field, enter a default value. This will be the value if nothing else is entered into the date field.
2. If ***Search by range*** is set to ***On***, a field will appear in the ***Search Videos*** pane that enables users to filter videos/assets **only** by a range of dates entered into this date field.

If set to ***Off***, users can only filter by *one* date at a time.

*This change will not come into effect unless **Show search field** is also set to **On**.*

3. If ***Include in date search*** is set to ***On***, videos/assets can be filtered by the date entered into this date field, using the ***Earliest date*** and ***Latest date*** fields in the ***Search Videos*** pane.
4. If ***Show search field*** is set to ***On***, a field will appear in the ***Search Videos*** pane that enables users to filter videos **only** by the dates entered into this date field.

>> For more information, see Search Videos on page 19

5. If ***Show in Incidents*** is set to ***On***, the way this field has been populated will be viewable in the ***Incident clips*** section of the incident editor once the video/asset has been added to an incident.
6. In the ***Conditions*** section, users can configure whether this user-defined media field only appears in the ***Edit properties*** pane when another drop down field or check box field has been populated in a specific manner. To do so:
   - Ensure there is at least **one** drop down field or check box field on VideoManager already. Conditions can only be used on these fields.
   - Click ***New condition***.
   - From the ***Field*** dropdown, select which drop down field or check box field will dictate the appearance of this user-defined media field.
   - From the ***Value*** dropdown, select which of the drop down field or check box field's values will dictate the appearance of this user-defined media field.

   This will be presented as a checkbox if a check box field has been chosen, and a dropdown if a drop down field has been chosen.

   - Click ***confirm***.
7. Click ***Save settings***.

9.4.11.4 Create Date and Time Fields

Once the administrator has selected **Date &Time** from the ***Type*** dropdown, the following configuration options will appear in the ***Date &Time*** section:

1. In the ***Default value*** field, enter a default value. This will be the value if nothing else is entered into the date and time field.

By clicking ***Set to now***, users can set the default value to the server's current date and time.

2. If ***Include in date search*** is set to ***On***, videos/assets can be filtered by the date entered into this date and time field, using the ***Earliest date*** and ***Latest date*** fields in the ***Search Videos*** pane.

3. If ***Show search field*** is set to ***On***, a field will appear in the ***Search Videos*** pane that enables users to filter videos/assets **only** by the date and time entered into this date and time field.

>> For more information, see Search Videos on page 19

4. If ***Show in Incidents*** is set to ***On***, the way this field has been populated will be viewable in the ***Incident clips*** section of the incident editor once the video/asset has been added to an incident.

5. In the ***Conditions*** section, users can configure whether this user-defined media field only appears in the ***Edit properties*** pane when another drop down field or check box field has been populated in a specific manner. To do so:

   - Ensure there is at least **one** drop down field or check box field on VideoManager already. Conditions can only be used on these fields.
   - Click ***New condition***.
   - From the ***Field*** dropdown, select which drop down field or check box field will dictate the appearance of this user-defined media field.
   - From the ***Value*** dropdown, select which of the drop down field or check box field's values will dictate the appearance of this user-defined media field.

   This will be presented as a checkbox if a check box field has been chosen, and a dropdown if a drop down field has been chosen.

   - Click ***confirm***.

6. Click ***Save settings***.

9.4.11.5 Create Drop Down Fields

Once the administrator has selected **Drop down** from the ***Type*** dropdown, the following configuration options will appear in the ***Drop down*** section:

1. Click + ***New value***. This will add an option to the drop down field, which the user can select when editing a video/asset. In the ***Value*** field, enter the name of the dropdown option. Click ***confirm***.

It is possible to create a drop down field with just one value.

2. From the ***Default value*** dropdown, select a default value. This will be the value if nothing else is selected from the drop down field.
3. If ***Include in match text search*** is set to ***On***, videos/assets can be filtered by the value of the drop down field, using the ***Match Text*** field in the 🔍 ***Search Videos*** pane.

For example - if the user selects a value from the drop down field called **Assault**, they should enter **Assault** into the ***Match Text*** field.

4. If ***Show search field*** is set to ***On***, a dropdown will appear in the 🔍 ***Search Videos*** pane that enables users to filter videos/assets **only** by the value chosen from this drop down field.

>> For more information, see Search Videos on page 19

5. If ***Show in Incidents*** is set to ***On***, the way this field has been populated will be viewable in the ***Incident clips*** section of the incident editor once the video/asset has been added to an incident.
6. In the ***Conditions*** section, users can configure whether this user-defined media field only appears in the ***Edit properties*** pane when another drop down field or check box field has been populated in a specific manner. To do so:
   - Ensure there is at least **one** drop down field or check box field on VideoManager already. Conditions can only be used on these fields.
   - Click + ***New condition***.
   - From the ***Field*** dropdown, select which drop down field or check box field will dictate the appearance of this user-defined media field.
   - From the ***Value*** dropdown, select which of the drop down field or check box field's values will dictate the appearance of this user-defined media field.

   This will be presented as a checkbox if a check box field has been chosen, and a dropdown if a drop down field has been chosen.

   - Click ***confirm***.
7. Click ***Save settings***.

9.4.11.6 Create Check Box Fields

Once the administrator has selected **Check box** from the ***Type*** dropdown, the following configuration options will appear in the ***Check box*** section:

1. From the ***Default value*** field, select a default value. This will be the value if the check box field is not edited.

This can either be checked or unchecked.

2. If ***Show search field*** is set to ***On***, a checkbox will appear in the ***Search Videos*** pane that enables users to filter videos/assets **only** by whether this check box field has been checked or not.

>> For more information, see Search Videos on page 19

3. If ***Show in Incidents*** is set to ***On***, the way this field has been populated will be viewable in the ***Incident clips*** section of the incident editor once the video/asset has been added to an incident.

4. In the ***Conditions*** section, users can configure whether this user-defined media field only appears in the ***Edit properties*** pane when another drop down field or check box field has been populated in a specific manner. To do so:

   - Ensure there is at least **one** drop down field or check box field on VideoManager already. Conditions can only be used on these fields.
   - Click ***New condition***.
   - From the ***Field*** dropdown, select which drop down field or check box field will dictate the appearance of this user-defined media field.
   - From the ***Value*** dropdown, select which of the drop down field or check box field's values will dictate the appearance of this user-defined media field.

   This will be presented as a checkbox if a check box field has been chosen, and a dropdown if a drop down field has been chosen.

   - Click ***confirm***.

5. Click ***Save settings***.

9.4.11.7 Create URL Fields

Once the administrator has selected **URL** from the ***Type*** dropdown, the following configuration options will appear in the ***URL*** section:

1. In the ***Default value*** field, enter a default value. This will be the value if nothing else is entered into the URL field.

   This must be in an URL format.

2. If ***Include in match text search*** is set to ***On***, videos/assets can be filtered by the URL entered into this text field, using the ***Match Text*** field in the ***Search Videos*** pane.
3. If ***Show in Incidents*** is set to ***On***, the way this field has been populated will be viewable in the ***Incident clips*** section of the incident editor once the video/asset has been added to an incident.
4. In the ***Conditions*** section, users can configure whether this user-defined media field only appears in the ***Edit properties*** pane when another drop down field or check box field has been populated in a specific manner. To do so:
   - Ensure there is at least **one** drop down field or check box field on VideoManager already. Conditions can only be used on these fields.
   - Click ***New condition***.
   - From the ***Field*** dropdown, select which drop down field or check box field will dictate the appearance of this user-defined media field.
   - From the ***Value*** dropdown, select which of the drop down field or check box field's values will dictate the appearance of this user-defined media field.

   This will be presented as a checkbox if a check box field has been chosen, and a dropdown if a drop down field has been chosen.

   - Click ***confirm***.
5. Click ***Save settings***.

9.4.11.8 Create Computed Fields

Once the administrator has selected **Computed** from the ***Type*** dropdown, the following configuration options will appear in the ***Computed*** section:

1. In the ***Expression*** field, enter the relevant text using Motorola Solutions custom predicate language.

>> For more information, see Appendix E: Custom Predicate Language on page 469

2. If ***As Url*** is set to ***On***, the field will be presented as a URL when editing a video/asset.

The `encodeURIComponent()` function allows users to encode a string to make it suitable for use in a URL - even if the string contains characters which would normally not be allowed in a URL.

3. In the ***Conditions*** section, users can configure whether this user-defined media field only appears in the ***Edit properties*** pane when another drop down field or check box field has been populated in a specific manner. To do so:

   - Ensure there is at least **one** drop down field or check box field on VideoManager already. Conditions can only be used on these fields.
   - Click + ***New condition***.
   - From the ***Field*** dropdown, select which drop down field or check box field will dictate the appearance of this user-defined media field.
   - From the ***Value*** dropdown, select which of the drop down field or check box field's values will dictate the appearance of this user-defined media field.

   This will be presented as a checkbox if a check box field has been chosen, and a dropdown if a drop down field has been chosen.

   - Click ***confirm***.

4. Click ***Save settings***.

9.4.11.9 Create Tag List Fields

Once the administrator has selected **Tag List** from the ***Type*** dropdown, the following configuration options will appear in the ***Tag List*** section:

1. Click + ***New value***. This will add an option to the tag list field, which the user can select when editing a video/asset. Click ***confirm***.

   It is possible to create a tag list field with just one value.

2. From the ***Default value*** dropdown, select a default value. This will be the value if nothing else is selected in the tag list field.
3. If ***Show search field*** is set to ***On***, a field will appear in the 🔍 ***Search Videos*** pane that enables users to filter videos/assets **only** by the value chosen from this tag list field.

   >> For more information, see Search Videos on page 19

4. If ***Show in Incidents*** is set to ***On***, the way this field has been populated will be viewable in the ***Incident clips*** section of the incident editor once the video/asset has been added to an incident.
5. In the ***Conditions*** section, users can configure whether this user-defined media field only appears in the ***Edit properties*** pane when another drop down field or check box field has been populated in a specific manner. To do so:
   - Ensure there is at least **one** drop down field or check box field on VideoManager already. Conditions can only be used on these fields.
   - Click + ***New condition***.
   - From the ***Field*** dropdown, select which drop down field or check box field will dictate the appearance of this user-defined media field.
   - From the ***Value*** dropdown, select which of the drop down field or check box field's values will dictate the appearance of this user-defined media field.

   This will be presented as a checkbox if a check box field has been chosen, and a dropdown if a drop down field has been chosen.

   - Click ***confirm***.
6. Click ***Save settings***.

9.4.11.10 Export and Import User-Defined Media Fields

If administrators have multiple instances of VideoManager, they may wish to transfer a copy of their user-defined media fields from one instance to another. To do so:

1. In the original instance of VideoManager, navigate to the ***Admin*** tab.
2. Select the ***Policies*** pane.
3. Click the ***User-defined Media Fields*** section.
4. Click ***Export***.

   The user-defined media fields will be saved to the PC's default download location.
5. In the new instance of VideoManager (or a site, if ***User-defined Fields*** has been set to ***Off*** in the ***Metadata/Footage Replication*** section), navigate to the ***Admin*** tab.
6. Select the ***Policies*** pane.
7. Click the ***User-defined Media Fields*** section.
8. Click ***Import***.

   Select the previously downloaded user-defined media fields.
9. Click ***Import***.

Alternatively, if an administrator wants to import **all** of their user-defined media fields simultaneously, they can do so from the ***Import/Export System Config*** section of the ***System*** pane in the ***Admin*** tab.

>> For more information, see Import or Export VideoManager's Configuration on page 356

9.4.12 Configure CommandCentral Vault Settings

If VideoManager has been configured so it automatically exports incidents to Motorola Solutions CommandCentral Vault, administrators can also configure whether VideoManager's user-defined incident fields automatically populate CommandCentral Vault's fields when an incident is exported. This is done from the ***CommandCentral Vault Settings*** section of the ***Policies*** pane, in the ***Admin*** tab.

To view already-existing user-defined CommandCentral vault fields:

1. Ensure that VideoManager has been connected to CommandCentral Vault.

>> For more information, see Configure CommandCentral Vault Settings on page 306

2. Navigate to the ***Admin*** tab.
3. Select the ***Policies*** pane.
4. Click the ***CommandCentral Vault Settings*** section.

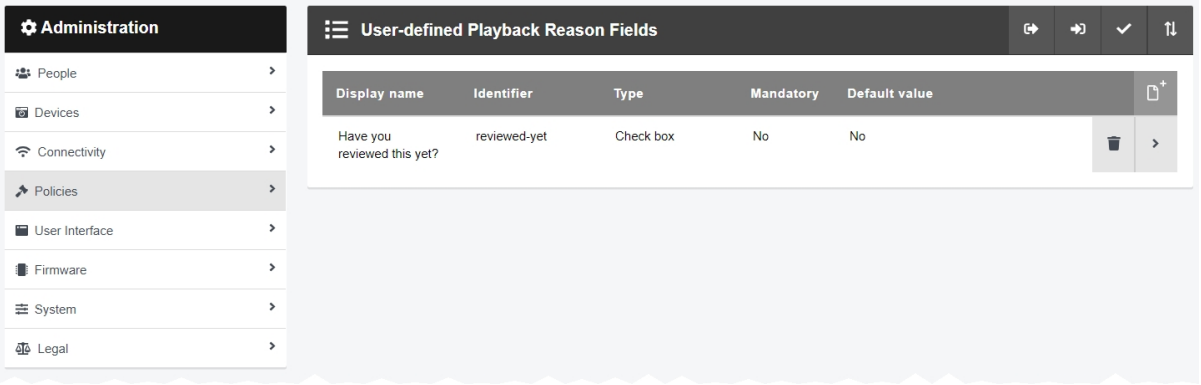
If users wish to sync their user-defined incident fields with the CommandCentral Vault fields, they must create user-defined incident fields on VideoManager which have the **same identifiers** as those in CommandCentral Vault.

>> For more information, see Create New User-defined Incident Fields on page 264

If a user has been successful in creating a user-defined CommandCentral vault field, it will appear in the ***Vault field mappings*** pane of the ***CommandCentral Vault Settings*** section.

9.4.13 Create User-defined Playback Reason Fields

User-defined playback reason fields are used in conjunction with the playback policy. When a user watches a video which is a certain number of days old, VideoManager will prompt them to give a reason as to why they are rewatching it. The user must then enter their answer in the previously-created user-defined playback reason field. Creating this field is done from the ***User-defined Playback Reason Fields*** section of the ***Policies*** pane, in the ***Admin*** tab.



To access the ***User-defined Playback Reason Fields*** pane:

1. Navigate to the ***Admin*** tab.
2. Select the ***Policies*** pane.
3. Click the ***User-defined Playback Reason Fields*** section.

The process for creating user-defined playback reason fields is the same as the process for user-defined incident fields. Administrators can create as many user-defined playback reason fields as necessary.

>> For more information, see Create New User-defined Incident Fields on page 264

Once the user-defined playback reason fields have been created, the playback policy must be configured to prompt users to complete these fields after a certain period of time.

>> For more information, see Configure the Playback Policy on page 305

9.4.13.1 Export and Import User-Defined Playback Reason Fields

If a user has multiple instances of VideoManager, they may wish to transfer a copy of their user-defined playback reason fields from one instance to another. To do so:

1. In the original VideoManager instance, navigate to the ***Admin*** tab.
2. Select the ***Policies*** pane.
3. Click the ***User-defined Playback Reason Fields*** section.
4. Click ***Export***.

   The user-defined playback reason fields will be saved to the PC's default download location.
5. In the new instance of VideoManager (or a site, if ***User-defined Fields*** has been set to ***Off*** in the ***Metadata/Footage Replication*** section), navigate to the ***Admin*** tab.
6. Select the ***Policies*** pane.
7. Click the ***User-defined Playback Reason Fields*** section.
8. Click ***Import***.

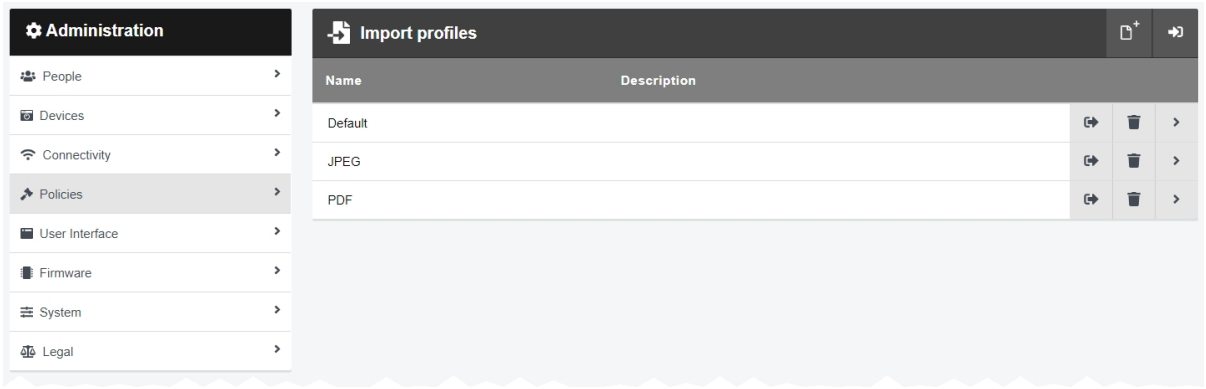
   Select the previously downloaded user-defined playback reason fields.

Alternatively, if an administrator wants to import **all** of their user-defined playback reason fields simultaneously, they can do so from the ***Import/Export System Config*** section of the ***System*** pane in the ***Admin*** tab.

>> For more information, see Import or Export VideoManager's Configuration on page 356

9.4.14 Configure Import Profiles

Import profiles determine how assets can be imported into VideoManager. They can also be used in tandem with user-defined media fields to insert external asset metadata into VideoManager as the assets are imported. This is done from the ***Import profiles*** section of the ***Policies*** pane, in the ***Admin*** tab.



Before administrators configure import profiles, they must create at least one user-defined media field which can be populated by users when they import assets.

>> For more information, see Create New User-defined Media Fields on page 283

To create a new import profile:

1. Navigate to the ***Admin*** tab.
2. Select the ***Policies*** pane.
3. Click the ***Import profiles*** section.
4. Click ***Create new profile***.
5. In the ***Name*** field, enter a name for the import profile.
6. In the ***Description*** field, enter a description for the import profile.

   This will tell other users on VideoManager what this profile controls (for example, which user-defined media fields will be automatically populated).
7. In the ***Profile*** field, enter the profile itself.

   The most simple profile will populate certain user-defined media fields for an asset automatically, when it is imported. This means that the user does not need to do it manually after the asset has been imported. The JSON format is as follows:

```
{"properties": {"name of user-defined media field": "value of user-defined media field"}}
```

   For example, if the administrator had created a user-defined media field called *vehicle-type*, any assets imported with this import profile would have their *vehicle-type* field populated with *car*.

```
{"properties": {"vehicle-type": "car"}}
```

To automatically populate multiple user-defined media fields, enter a comma (,) between the fields, like so:

```
{"properties": {"vehicle-type": "car","category": "arrest"}}
```

Another simple profile will enable users to populate the user-defined media fields for an asset themselves, before the asset is imported. The JSON properties are as follows:

- `promptedFields` - the user importing the asset can optionally populate these user-defined media fields before the asset is imported.
- `promptedMandatory` - the user importing the asset must populate these user-defined media fields before the asset can be imported.

The JSON format is as follows:

```
{"promptedFields": ["name of user-defined media field"]}
```

In the following configuration, users would be prompted to populate the `[import-reason]` user-defined media field when importing their asset.

```
{"promptedFields": ["import-reason"]}
```

In the following configuration, users would have to populate the `[import-reason]` user-defined media field before they could import their asset.

```
{"promptedMandatory": ["import-reason"]}
```

For more complex import profile configurations, Motorola Solutions Support should be contacted.

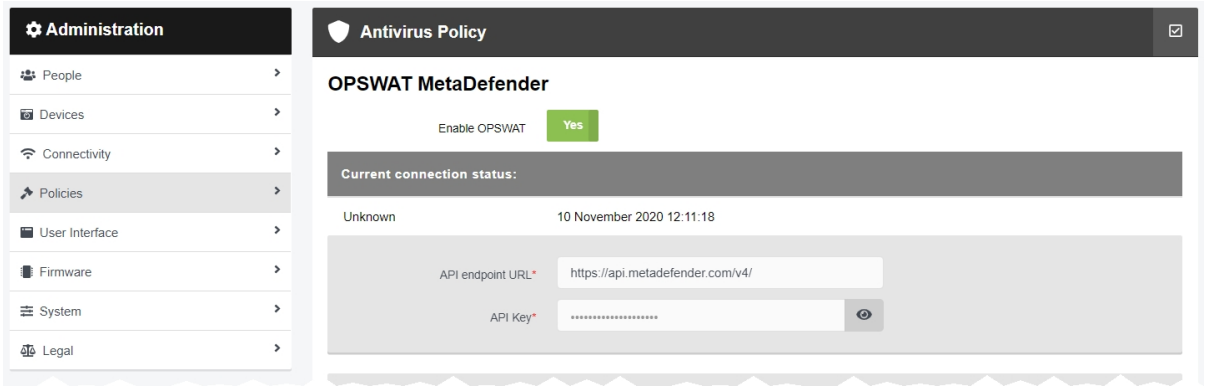
8. Keep ***Automatic import*** set to ***Off*** unless specified by Motorola Solutions Support.

When set to ***Off***, the user must choose the profile from the dropdown when manually importing files from the ***Videos*** tab.

>> For more information, see Import Assets on page 33

9.4.15 Enable and Configure the Antivirus Policy

Users can import assets from external sources into VideoManager. If administrators have an OPSWAT account, they can use it to automatically scan these assets for viruses as they are being imported into VideoManager. To do so, administrators must first configure the antivirus policy, which dictates the type of files to be scanned for viruses. This is done from the ***Antivirus Policy*** section of the ***Policies*** pane, in the ***Admin*** tab.



To configure VideoManager's antivirus policy:

1. Navigate to the ***Admin*** tab.
2. Select the ***Policies*** pane.
3. Click the ***Antivirus Policy*** section.
4. In the ***OPSWAT MetaDefender*** section, set ***Enable OPSWAT*** to ***On***.
5. In the ***API endpoint URL*** field, enter *https://api.metadefender.com/v4/*.

   If the administrator has an on-premise OPSWAT account, this URL will be different. Contact the system administrator for more information.
6. In the ***API Key*** field, enter the API key associated with the administrator's OPSWAT account.

   To find this, log in to the OPSWAT portal and navigate to the ***Dashboard*** tab. The API key is shown in the ***My API Key*** section of the ***MetaDefender Cloud*** pane.
7. Click ***Save settings***.
8. To ensure that the API key is valid, click ***Check OPSWAT connection status***.

   Check the ***Current connection status:*** section:

   - If it reads as ***Connection succeeded***, the API key is valid and working correctly.
   - If it reads as ***Connection failed***, the API key is invalid and should be entered again.
9. In the ***File size limit*** field, enter the size of imported files in megabytes, above which VideoManager will not attempt scan them for viruses.

The file size upper limit depends on the administrator's OPSWAT account. A free account has an upper limit of **140MB**, a commercial account has an upper limit of **256MB**, and an enterprise account does not have a limit.

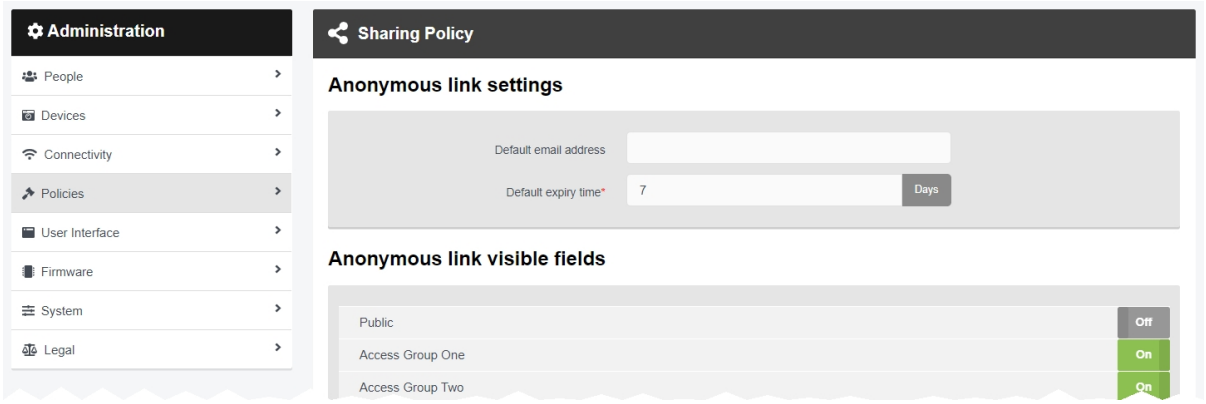
The larger an imported file, the longer OPSWAT will take to scan it for viruses.

10. From the ***Media files*** and ***Non media files*** dropdowns, administrators can determine the default scan policies for media (JPG, JPEG, MP4) and non-media (PDF, XLS/XLSX, CSV) imports, respectively. The options are as follows:
    - **Scan files below the limit, fail files which are too large**
    - **Scan files below the limit, pass files which are too large**
    - **Do not scan any files**
11. Click ***Save settings***.

From now on, depending on the configuration in this section, assets will be scanned for viruses as they are imported into VideoManager. If an asset fails the antivirus scan, it will not be imported.

9.4.16 Configure Sharing Policy

Users can share incidents externally using a link. Administrators can configure which email address these links are sent to, if most or all links will be sent to the same address. Administrators can also set the default expiry time for a link, after which the incident will be inaccessible to anyone who does not have an account on VideoManager, and configure which incident clip fields are visible in a link. This is done from the ***Sharing Policy*** section of the ***Policies*** pane, in the ***Admin*** tab.



To configure VideoManager's sharing policy:

1. Navigate to the ***Admin*** tab.
2. Select the ***Policies*** pane.
3. Click the ***Sharing Policy*** section.
4. In the ***Default email address*** field, enter the email address which will be the default recipient for incident links.

Users can override this email address when creating a link from the ***Incidents*** tab.

5. In the ***Default expiry time*** field, enter the default number of days for which a link will be active, before it expires.

Users can override this expiry time when creating a link from the ***Incidents*** tab.

>> For more information, see Share Incidents Externally Using a Link on page 91

6. In the ***Anonymous link visible fields*** section, administrators can configure which incident clip fields are visible when an incident is shared via an incident link. This depends on which incident clip fields are visible to specific permission groups, as configured in the ***User-defined Incident Fields*** section.

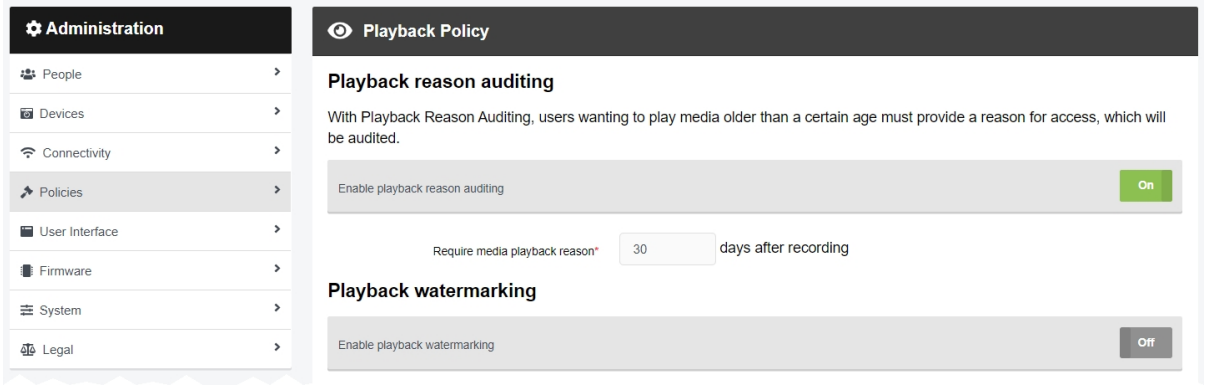
For example, if the ***Operator:*** field has been configured so only users in permission group one can view it, then administrators could enable ***Access Group One*** here. This means that the ***Operator:*** property would be visible in the incident link.

>> For more information, see Edit Incident Clip Fields on page 263

7. Click ***Save settings***.

9.4.17 Configure the Playback Policy

Administrators can control whether, after a certain time, videos cannot be viewed on VideoManager without the user first recording their reason for viewing, and whether all videos on VideoManager have a watermark when played back. This is done from the ***Playback Policy*** section of the ***Policies*** pane, in the ***Admin*** tab.



Before administrators configure the playback policy, they should create a user-defined playback reason field. This enables users to supply their reason for rewatching the video in question. If a user-defined playback reason field is not created once the playback policy has been confiured, then users must still acknowledge that they are rewatching a video after a certain amount of time has elapsed, but VideoManager will not prompt them for a reason.

>> For more information, see Create User-defined Playback Reason Fields on page 298

To configure playback policies on VideoManager:

1. Navigate to the ***Admin*** tab.
2. Select the ***Policies*** pane.
3. Click the ***Playback Policy*** section.
4. If ***Enable playback reason auditing*** is set to ***On***, users must record their reason for watching a video after a set number of days.

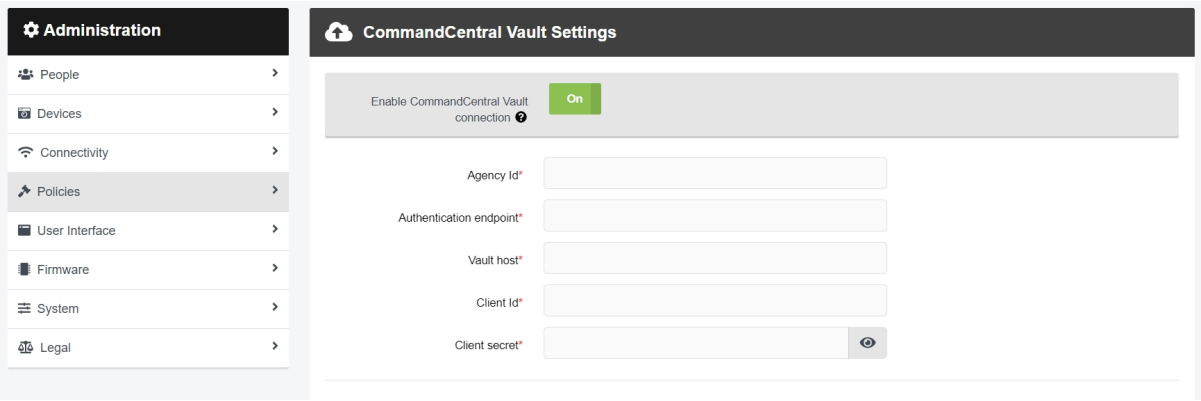
   In the ***Require media playback reason*** section, enter the number of days since the video was recorded, after which a user must give a reason for watching it.
5. If ***Enable playback watermarking*** is set to ***On***, all videos on VideoManager will have a watermark when played back, relating to the user who is watching the video.

   If ***Enable playback signature*** is set to ***On***, every individual playback will have its own unique watermark. This watermark will be shown on the video itself when it is watched, and will appear in the audit log against the user who watched it.

   If ***Enable playback username &datetime*** is set to ***On***, every video will have a watermark displaying the username of the user who is watching it, and the current date and time.
6. Click ***Save settings***.

9.4.18 Configure CommandCentral Vault Settings

VideoManager can be configured to send footage and incidents to Motorola Solutions CommandCentral Vault. This is somewhat similar to a site/Central VideoManager setup, with VideoManager acting as a site and CommandCentral Vault acting as a Central VideoManager. This is done from the ***CommandCentral Vault Settings*** section of the ***Policies*** pane, in the ***Admin*** tab.



To configure the CommandCentral Vault on VideoManager:

1. Navigate to the ***Admin*** tab.
2. Select the ***Policies*** pane.
3. Click the ***CommandCentral Vault Settings*** section.
4. Set ***Enable CommandCentral Vault connection*** to ***On***.

The administrator must enter identifying information provided to them by Motorola Solutions.

5. From the ***User association*** dropdown, select which user will be associated with exports entering CommandCentral Vault. The options are as follows:

   - **None** - if chosen, the media will not have a user associated with it when it is uploaded to CommandCentral Vault.
   - **Specified user** - if chosen, the name of the user who will be associated with the media on CommandCentral Vault must be entered.

   This must be a user on CommandCentral Vault, **not** VideoManager.

   Caution *If the username is entered incorrectly here, the media will not be uploaded.*

   - **Committing user** - if chosen, the media will be associated with the user who is committing it to CommandCentral Vault.

   The user in question must have the **same username** in both CommandCentral Vault and VideoManager.

   - **Device operator** - if chosen, the media will be associated with the user who recorded or imported it.

The user in question must have the **same username** in both CommandCentral Vault and VideoManager. For this reason, if the majority of users who are operating body-worn cameras will not have access to CommandCentral Vault, it is recommended that **Committing user** is chosen instead.

6. If ***Enable vault incident commit*** is set to ***On***, users can export incidents from VideoManager to CommandCentral Vault.

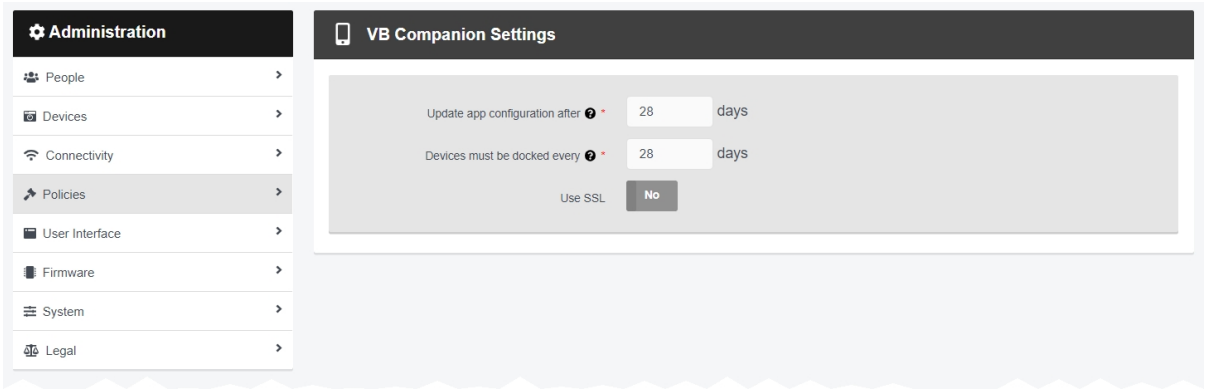
VideoManager's user-defined incident fields can be synced with CommandCentral Vault's fields, so the former automatically populates the latter when an incident is exported. If CommandCentral Vault fields have been configured, they will show up in the ***Vault field mappings*** pane.

>> For more information, see Configure CommandCentral Vault Settings on page 297

7. Click ***Save settings***.

9.4.19 Configure VB Companion Settings

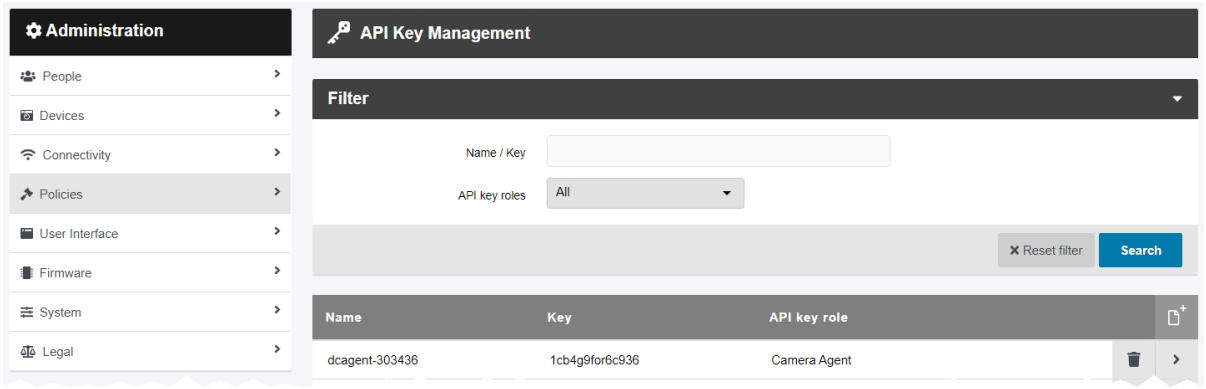
If VB Companion has been licensed from Motorola Solutions, administrators can configure its settings from VideoManager. This is done from the ***VB Companion Settings*** section of the ***Policies*** pane, in the ***Admin*** tab.



This is part of the multi-step process which enables VB Companion to work with VideoManager. Please see the VB Companion guide for more information.

9.4.20 Create, View and Delete API Keys

API keys dictate how VideoManager communicates with external software or body-worn cameras. They can be administered from the ***API Key Management*** section of the ***Policies*** pane, in the ***Admin*** tab.



To create an API key:

1. Navigate to the ***Admin*** tab.
2. Select the ***Policies*** pane.
3. Click the ***API Key Management*** section.
4. Click ***New API key***.
5. In the ***Name*** field, enter a name for the API key.

The name is not required to be unique on VideoManager - however, it is strongly recommended.

6. If ***Generate key*** is set to ***On***, the API key will be automatically generated upon creation. This is necessary if the administrator is creating an entirely new API key.

If set to ***Off***, the administrator can enter the key manually. This is necessary if the administrator is adding a previously-existing API key to VideoManager.

7. If ***Generate secret*** is set to ***On***, the API secret will be automatically generated upon creation. This is necessary if the administrator is creating an entirely new API key.

If set to ***Off***, the administrator can enter the secret manually. This is necessary if the administrator is adding a previously-existing API key to VideoManager.

8. From the ***API key roles*** dropdown, select which role is most appropriate for the API key.

If the administrator will be integrating their own software with VideoManager, the **Use System Role** *option is recommended.*

9. If **Use System Role** has been selected from the previous dropdown, from the ***Roles*** dropdown, select which of VideoManager's roles the API key will inhabit.

10. Double-check that the information entered is correct - API keys **cannot** be edited after creation.
11. Click ***confirm*** to save the API key.

    The API key and API secret will be presented. Make a note of the API secret - **this cannot be viewed again**.

Once API keys have been created, they can be viewed on VideoManager. To do so:

1. Navigate to the ***Admin*** tab.
2. Select the ***Policies*** pane.
3. Click the ***API Key Management*** section.
4. Filter the API keys as necessary, and click ***Search***.

   Administrators can enter the name of the API key in the ***Name / Key*** field, and select the API key's role from the ***API key roles*** dropdown.

   Click ***Reset filter*** to clear the search filters.
5. Next to the API key to be edited, click ***View API key***.

   Here, administrators can view the ***Name***, ***Key***, and ***API key role***.
6. Click ***close***.

If an API key becomes redundant, it can be deleted from VideoManager. To do so:

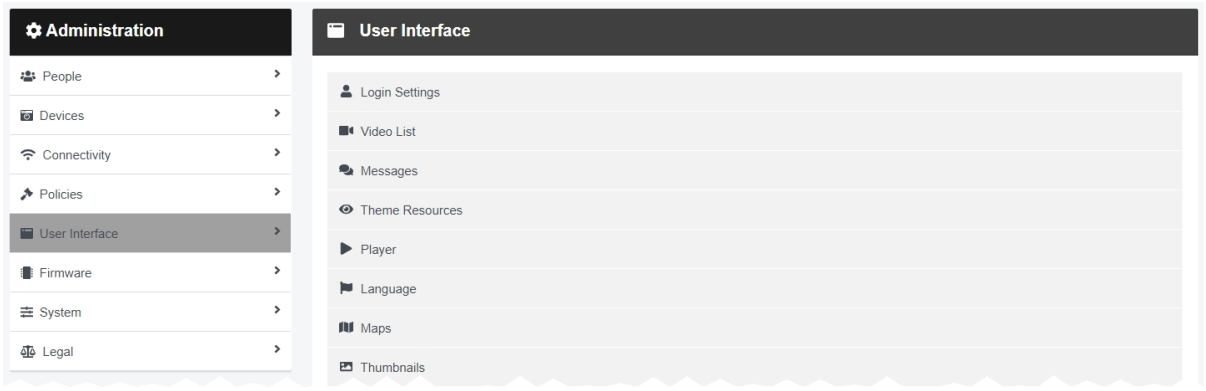
1. Navigate to the ***Admin*** tab.
2. Select the ***Policies*** pane.
3. Click the ***API Key Management*** section.
4. Filter the API keys as necessary, and click ***Search***.

   Administrators can enter the name of the API key in the ***Name / Key*** field, and select the API key's role from the ***API key roles*** dropdown.

   Click ***Reset filter*** to clear the search filters.
5. Next to the API key to be deleted, click ***Delete API key***.

9.5 User Interface

Administrators can edit aspects of VideoManager related to the appearance and layout of the user interface. This is done from the ***User Interface*** pane, in the ***Admin*** tab.



To access the ***User Interface*** pane:

1. Navigate to the ***Admin*** tab.
2. Select the ***User Interface*** pane.

From here, administrators can access the following sections:

- ***Login Settings***

Create, edit, and delete login warnings, and configure user agreements.

>> For more information, see Configure Login Settings on page 313

- ***Video List***

Change how all users will view videos on their homepage.

>> For more information, see Configure the Video List on page 316

- ***Messages***

Create messages which all users will view on their homepage.

>> For more information, see Create, Edit and Delete Messages on page 317

- ***Theme Resources***

Change the logos displayed on VideoManager, and VideoManager's colour scheme.

>> For more information, see Change and Reset Theme Resources on page 320

- ***Player***

Change the default quality at which videos will be played on VideoManager.

>> For more information, see Configure Player on page 324

- ***Language***

Change the default language in which the VideoManager user interface is displayed.

>> For more information, see Configure VideoManager's Language on page 325

- ***Maps***

Change map settings. This is necessary if administrators want to use Tactical VideoManager, view location data for recorded footage, and filter recorded footage by location.

>> For more information, see Enable and Configure Maps on page 327

- ***Thumbnails***

Change the default thumbnail for assets which have been imported without a built-in thumbnail.

>> For more information, see Configure Thumbnails on page 329

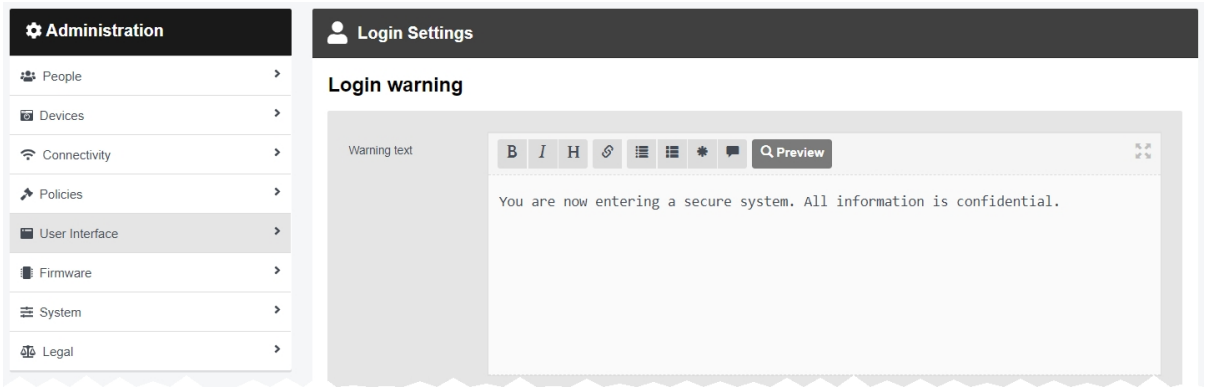
- ***Incidents***

Configure how incident clips are presented in incidents.

>> For more information, see Configure Incident Settings on page 330

9.5.1 Configure Login Settings

VideoManager can be configured to display a login warning and mandatory user agreement which users must agree to before they are permitted to log on. This is done from the ***Login Settings*** section of the ***User Interface*** pane, in the ***Admin*** tab.



To reach the ***Login Settings*** section:

1. Navigate to the ***Admin*** tab.
2. Select the ***User Interface*** pane.
3. Click the ***Login Settings*** section.

There are multiple categories that administrators can configure:

Login warning - this section enables administrators to create a login warning on VideoManager. The login warning will be displayed at the bottom of VideoManager's login pane, and will be visible to all users before they access VideoManager.

1. In the ***Warning text*** field, enter the warning.

   It is possible to customise the text using the following settings (clicking the buttons again will undo the changes):

   - ***Bold*** - any text within the asterisks will appear bold.
   - ***Italic*** - any text within the underscores will appear italicised.
   - ***Heading*** - any text on the same line as ### will appear as heading text.
   - ***URL/Link*** - the administrator will be prompted to enter a hyperlink. A link description can be entered in the square brackets.
   - ***Image*** - the administrator can enter a URL for an image. An image description can be entered in the brackets.
   - ***Unordered List*** - any text after the hyphen will appear as part of a bullet point list. ***Unordered List*** must be clicked for each individual list entry.

- ***Ordered List*** - any text after the hyphen will appear as part of a numbered list. ***Ordered List*** must be clicked for each individual list entry (the numbers will appear in order once the message is previewed).
- ***Code*** - any text within the single quotation marks will appear as code.
- ***Quote*** - any text on the same line as > will appear as a quote.

2. By clicking ***Preview***, a previewable version will become visible. To edit the text, click ***Preview*** again.
3. Click ***Save settings***.

User agreement - this section enables administrators to create a user agreement. All users on VideoManager must agree to this text when logging in for the first time.

1. Set ***Users must accept agreement on login*** to ***On***.
2. In the ***Agreement title*** field, enter a title for the user agreement.
3. In the ***Agreement text*** field, enter the text for the user agreement. This could be legal information, or terms and conditions.

It is possible to customise the text using the following settings (clicking the buttons again will undo the changes):

- ***Bold*** - any text within the asterisks will appear bold.
- ***Italic*** - any text within the underscores will appear italicised.
- ***Heading*** - any text on the same line as ### will appear as heading text.
- ***URL/Link*** - the administrator will be prompted to enter a hyperlink. A link description can be entered in the square brackets.
- ***Image*** - the administrator can enter a URL for an image. An image description can be entered in the brackets.
- ***Unordered List*** - any text after the hyphen will appear as part of a bullet point list. ***Unordered List*** must be clicked for each individual list entry.
- ***Ordered List*** - any text after the hyphen will appear as part of a numbered list. ***Ordered List*** must be clicked for each individual list entry (the numbers will appear in order once the message is previewed).
- ***Code*** - any text within the single quotation marks will appear as code.
- ***Quote*** - any text on the same line as > will appear as a quote.

4. By clicking ***Preview***, a previewable version will become visible. To edit the text, click ***Preview*** again.
5. In the ***Acceptance text*** field, enter an agreement text.

Users must agree to this text before logging in to VideoManager.

*The default text is **I agree to the terms and have read the User Agreement**.*

6. Click ***Save settings***.

Session settings - this section controls how frequently users must log in to VideoManager if the system is inactive.

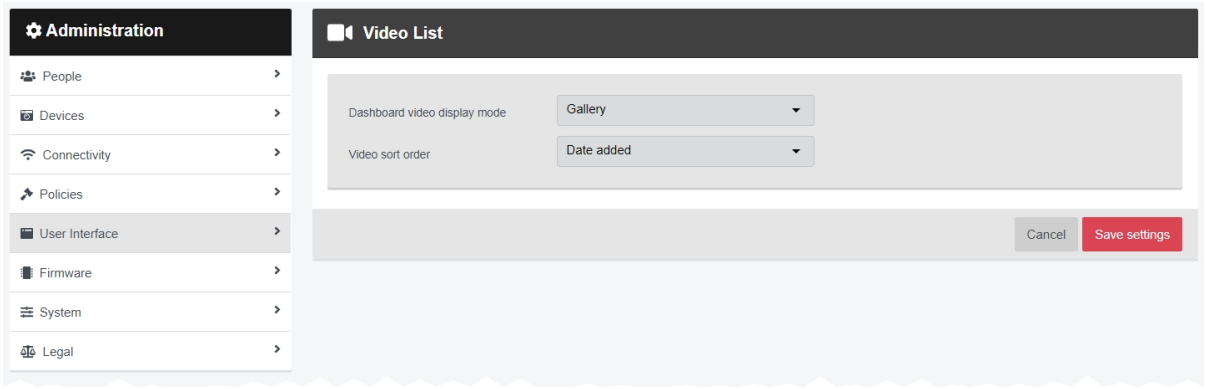
1. In the ***Session timeout*** field, enter the number of minutes for which VideoManager must be inactive, after which the user must log in again.
2. Click ***Save settings***.

Privilege Elevation - this section controls privilege escalation settings. This is part of a multi-step process.

>> For more information, see Configure Privilege Escalation on page 390

9.5.2 Configure the Video List

Administrators can customise how videos are presented by default, for both users' personal dashboards and the ***Videos*** tab. This is done from the ***Video List*** section of the ***User Interface*** pane, in the ***Admin*** tab.



To customise how videos are presented for all users on VideoManager:

1. Navigate to the ***Admin*** tab.
2. Select the ***User Interface*** pane.
3. Click the ***Video List*** section.
4. From the ***Dashboard video display mode*** dropdown, select how videos on users' dashboards are presented. The options are **List** or **Gallery**.
5. From the ***Video sort order*** dropdown, select how videos in the ***Videos*** tab are ordered. The options are **Recording date**, **Recording date (least recent)**, or **Date added**.

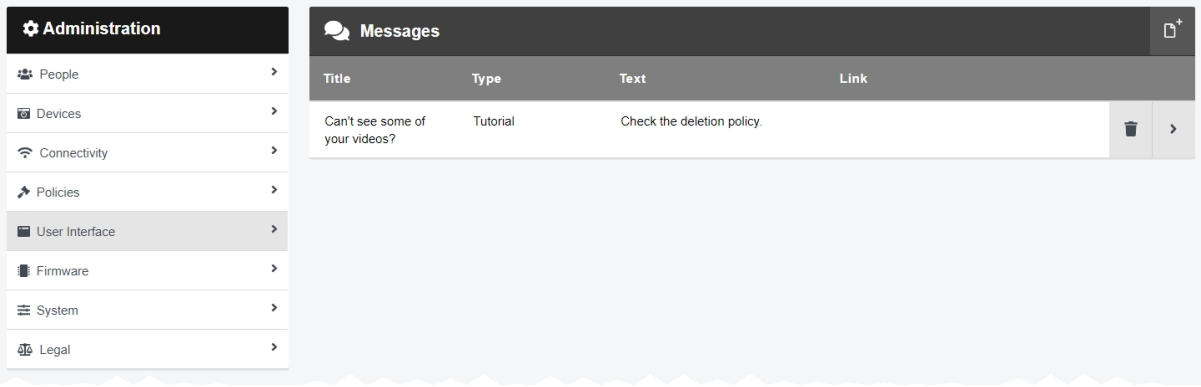
   This sets the default in the ***Videos*** tab for all users. However, users with the correct permissions can override the default for their individual session.

   >> For more information, see Change Viewing Options on page 22

6. Click ***Save settings***.

9.5.3 Create, Edit and Delete Messages

Messages are displayed on the dashboard when a user logs in. From the appropriate pane, administrators can create, edit, and delete messages. This is done from the ***Messages*** section of the ***User Interface*** pane, in the ***Admin*** tab.



To create a message:

1. Navigate to the ***Admin*** tab.
2. Select the ***User Interface*** pane.
3. Click the ***Messages*** section.
4. Click ***Create message***.
5. In the ***Title*** field, enter a title for the message.
   This will appear in **bold** at the top of the message.
6. From the ***Type*** dropdown, select the type of message to be created. The options are as follows:
   - **General** - will appear next to the message.
   - **Warning** - will appear next to the message.
   - **Tutorial** - will appear next to the message.
7. In the ***Text*** field, enter the message itself.
   It is possible to customise the text using the following settings (clicking the buttons again will undo the changes):
   - **B** ***Bold*** - any text within the asterisks will appear bold.
   - ***I*** ***Italic*** - any text within the underscores will appear italicised.
   - **H** ***Heading*** - any text on the same line as ### will appear as heading text.

- ***URL/Link*** - the administrator will be prompted to enter a hyperlink. A link description can be entered in the square brackets.
- ***Image*** - the administrator can enter a URL for an image. An image description can be entered in the brackets.
- ***Unordered List*** - any text after the hyphen will appear as part of a bullet point list. ***Unordered List*** must be clicked for each individual list entry.
- ***Ordered List*** - any text after the hyphen will appear as part of a numbered list. ***Ordered List*** must be clicked for each individual list entry (the numbers will appear in order once the message is previewed).
- ***Code*** - any text within the single quotation marks will appear as code.
- ***Quote*** - any text on the same line as > will appear as a quote.

8. By clicking ***Preview***, a previewable version will become visible. To edit the text, click ***Preview*** again.
9. In the ***Link*** field, administrators can enter the address of another website. This will appear at the bottom of the message, and users can click on it to learn more about the message.
10. If ***User can hide*** is set to ***On***, users can hide the message on their own dashboard by clicking ***Hide***.

This will only hide the message on the user's personal dashboard - other users on VideoManager will still be able to see the message until they hide it themselves.

11. Click ***Create message***.

Administrators can edit a message. This may be necessary if the content or formatting of the message should be changed. To do so:

1. Navigate to the ***Admin*** tab.
2. Select the ***User Interface*** pane.
3. Click the ***Messages*** section.
4. Next to the message to be edited, click ***Go to message***.
5. Make the relevant changes, and click ***Save message***.

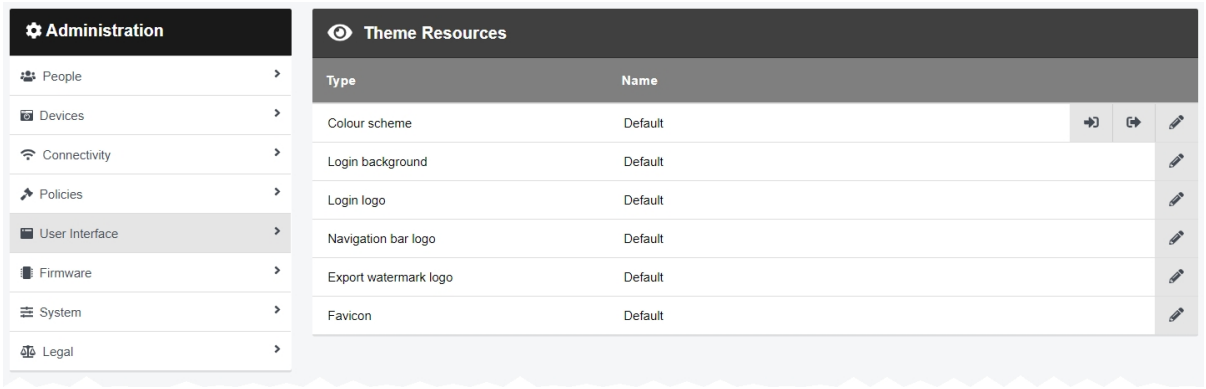
Administrators can delete a message. To do so:

1. Navigate to the ***Admin*** tab.
2. Select the ***User Interface*** pane.

3. Click the ***Messages*** section.
4. Next to the message to be deleted, click ***Delete message***.
A confirmation window will open.
5. Click ***yes***.

9.5.4 Change and Reset Theme Resources

Administrators can specify certain aspects of VideoManager's images, colour scheme, and branding. This is done from the ***Theme Resources*** section of the ***User Interface*** pane, in the ***Admin*** tab.



There are two aspects to configuring theme resources:

- Change VideoManager's logos.

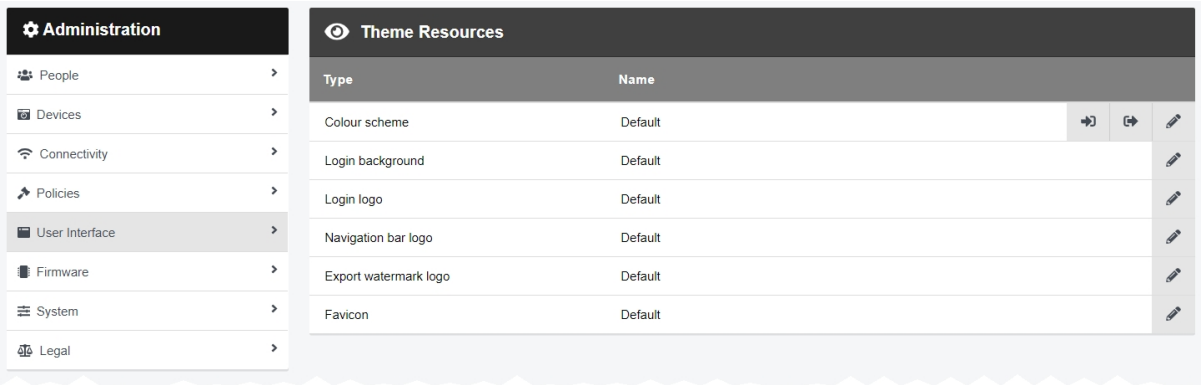
>> For more information, see on the next page

- Change VideoManager's colour scheme.

>> For more information, see on page 322

9.5.4.1 Change VideoManager's Logos

Every instance of the Motorola Solutions logo can be replaced with still or animated images in .jpg, .jpeg, .png or .gif format. This enables users to change VideoManager's logos to match their organisation's branding.



To replace VideoManager's default images:

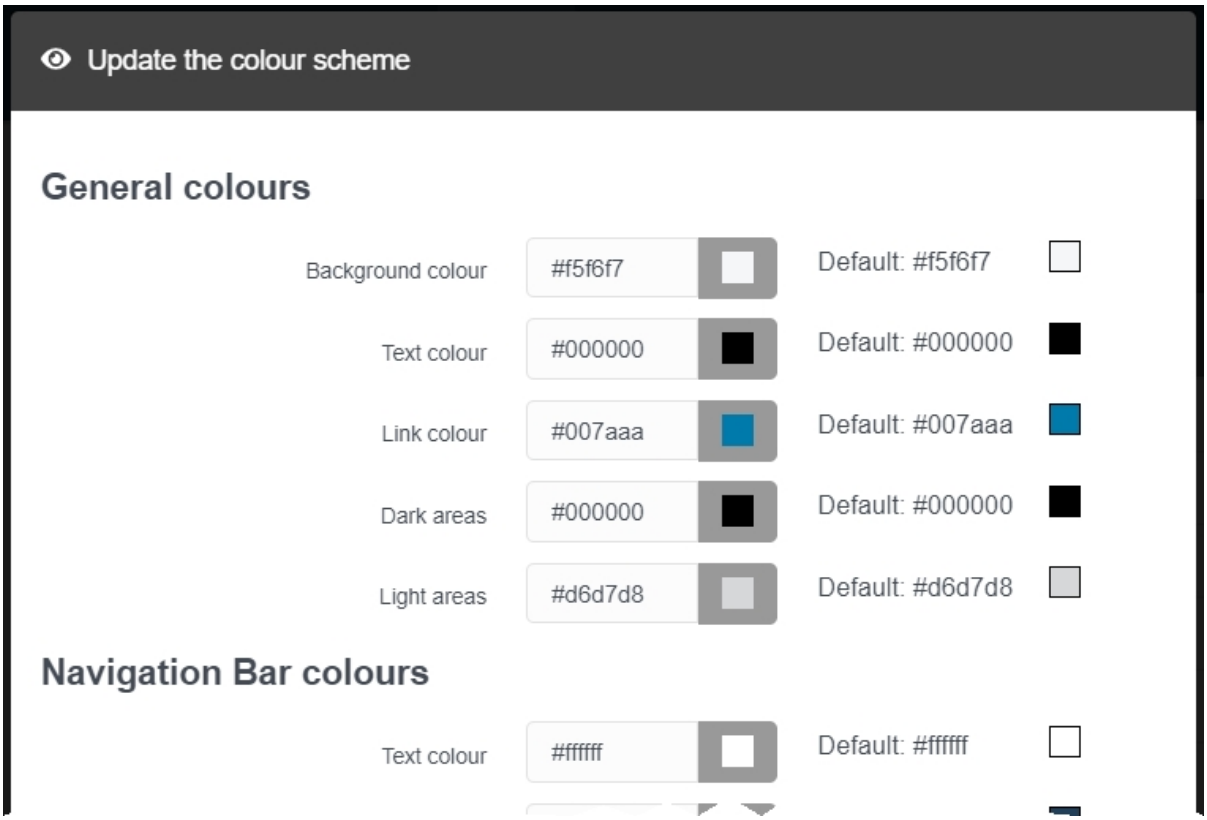
1. Navigate to the ***Admin*** tab.
2. Select the ***User Interface*** pane.
3. Click the ***Theme Resources*** section.
4. The options presented are as follows:
   - ***Login background*** - the image used as the background when users are logging in.
   - ***Login logo*** - the image used in the top left-hand corner of the login box.
   - ***Navigation bar logo*** - the image visible in the top left-hand corner of the navigation bar along the top of the VideoManager user interface.
   - ***Export watermark logo*** - the image used as the watermark for exported incidents. This must be a PNG file with a transparent background.
   - ***Favicon*** - the icon shown in the VideoManager tab. This must be an **ico** file which is 16x16 pixels.
5. Next to the image to be edited, click ***Replace theme resource***.

   The ***Import theme resource*** window will open.
6. Select ***Choose File...***.
7. Select the file to be used, and click ***OK***.

   The new graphics will be updated immediately.
8. To reset the logo, click ***Reset to default*** next to the icon that will be reset.

9.5.4.2 Change VideoManager's Colour Scheme

Administrators can change VideoManager's colour scheme, to match an organisation's corporate branding.



To change VideoManager's colour scheme:

1. Navigate to the ***Admin*** tab.
2. Select the ***User Interface*** pane.
3. Click the ***Theme Resources*** section.
4. Next to the ***Colour scheme*** row, click ***Replace theme resource***.
   Administrators can enter the specific colour name as either a HTML/CSS colour name or a Hex code (e.g. *orangered* and *#ff4500* would produce the same colour in the UI). Alternatively, administrators can click the box on the right-hand side to choose the colour manually.
5. The ***General colours*** options are as follows:
   - ***Background colour*** - this changes VideoManager's background colour.
   - ***Text colour*** - this changes the colour of the text in VideoManager's body, as well as the colour of icons when the cursor is held over them.
   - ***Link colour*** - this changes the colour of UI controls which take the user to a different page (e.g. ***Find incidents***).

- ***Dark areas*** - this changes the colour of pane headings.
- ***Light areas*** - this changes the colour of unselected heading options.

6. The ***Navigation Bar colours*** options are as follows:
   - ***Text colour*** - this changes the colour of unselected text in the main navigation bar.
   - ***Background colour*** - this changes the colour of the background in the main navigation bar.
   - ***Current section text colour*** - this changes the colour of the selected text in the main navigation bar.
   - ***Current section background colour*** - this changes the colour of the selected background in the main navigation bar.
   - ***Background colour (when mouse over)*** - this changes the colour of the background in the main navigation bar when the mouse is hovering over it.
7. The ***Media panel colours*** options are as follows:
   - ***Header background colour (in incidents)*** - this changes the colour of the headings for videos which are included in one or more incidents.
8. To save the colour scheme, click ***OK***.
9. To reset the colour scheme, click ***Reset to defaults***.

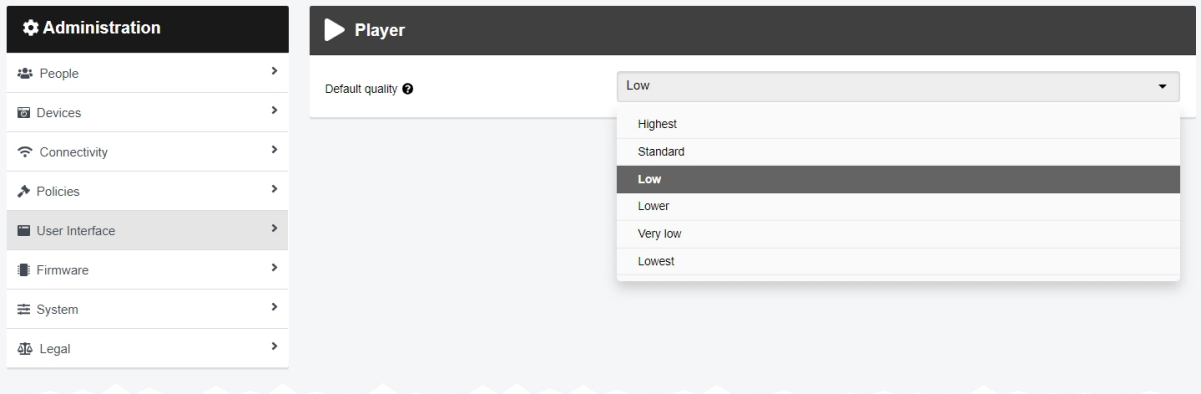
Administrators can transfer a copy of a colour scheme from one instance of VideoManager to another. This is necessary if the instance of VideoManager is acting as a Central VideoManager: colour schemes in a Central VideoManager are **not** automatically updated in its respective sites. To do so:

1. On the original instance of VideoManager, navigate to the ***Admin*** tab.
2. Select the ***User Interface*** pane.
3. Click the ***Theme Resources*** section.
4. Click ***Export*** next to the colour scheme to be exported.

   The colour scheme will be downloaded to the administrator's PC.
5. On the new instance of VideoManager (or a site), navigate to the ***Admin*** tab.
6. Select the ***User Interface*** pane.
7. Click the ***Theme Resources*** section.
8. Click ***Import***.
9. Select the previously-downloaded colour scheme.
10. Click ***import***.

9.5.5 Configure Player

It is possible for administrators to select the default quality at which videos are played in the VideoManager player. This is done from the ***Player*** section of the ***User Interface*** pane, in the ***Admin*** tab.



To change VideoManager's default video playback quality:

1. Navigate to the ***Admin*** tab.
2. Select the ***User Interface*** pane.
3. Click the ***Player*** section.
4. From the ***Default quality*** dropdown, select the default video quality. The options are **Highest**, **Standard**, **Low**, **Lower**, **Very low**, and **Lowest**.
5. Click ***Save settings***.

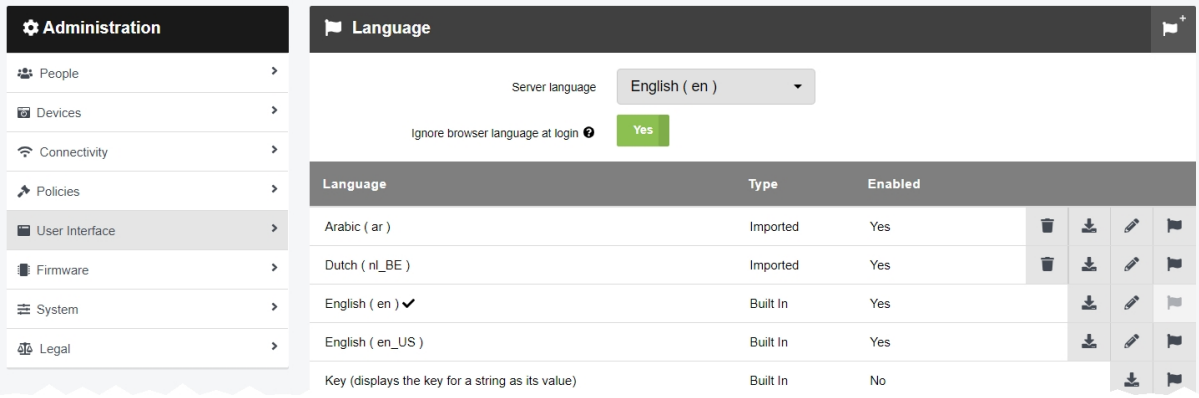
Any changes will come into effect when the administrator logs in again. or when the page is refreshed.

Users who have the ***Control playback quality*** permission enabled can override this default when they watch videos from the ***Videos*** tab. Users without this permission must watch all videos from the ***Videos*** tab in this quality.

>> For more information, see Watch Videos on page 25

9.5.6 Configure VideoManager's Language

VideoManager enables administrators to change the language in which the VideoManager interface is presented to all users. They can also import new language files and disable languages. This is done from the ***Language*** section of the ***User Interface*** pane, in the ***Admin*** tab.



From the appropriate pane, administrators can perform a range of actions regarding VideoManager's language.

Administrators can change VideoManager's server language. This is the default language in which all users will navigate VideoManager.

1. Navigate to the ***Admin*** tab.
2. Select the ***User Interface*** pane.
3. Click the ***Language*** section.
4. In the top pane, select a language from the ***Server language*** dropdown.

This is the language in which all users will navigate VideoManager.

> *The server language cannot be deleted while it is acting as a server language. The **English** and **Key** language files cannot be deleted at all, even if they are not acting as a server language.*

Administrators can change whether the browser language is ignored at login or not. This may be useful if the browser running VideoManager is in one language, but users wish to use it in another. To do so:

1. Navigate to the ***Admin*** tab.
2. Select the ***User Interface*** pane.
3. Click the ***Language*** section.
4. If ***Ignore browser language at login*** is set to ***Yes***, VideoManager will use the previously-set server language and **ignore** the browser language.

If set to ***No***, VideoManager will try to use the browser language.

Administrators can change the current session's language. This is useful if they want to navigate VideoManager in a different language for the duration of their personal session. To do so:

1. Navigate to the ***Admin*** tab.
2. Select the ***User Interface*** pane.
3. Click the ***Language*** section.
4. Next to the relevant language, click ***Select language for current session***.

The language of VideoManager will be changed for the administrator until they log out or their session expires.

*It is also possible for users to select their own language, by clicking in the top right-hand corner and selecting **Language**. This selection will be tied to their user only and permissions to do this must be configured by an administrator. The relevant permission is **Select Language for login session**, under **Advanced permissions**.*

Administrators can import new language files into VideoManager. This will enable them to navigate VideoManager in that language. To do so:

1. Navigate to the ***Admin*** tab.
2. Select the ***User Interface*** pane.
3. Click the ***Language*** section.
4. Click ***Import language file***.

The ***Import language file*** window will open.

5. Browse to the file to be imported and click ***import***.

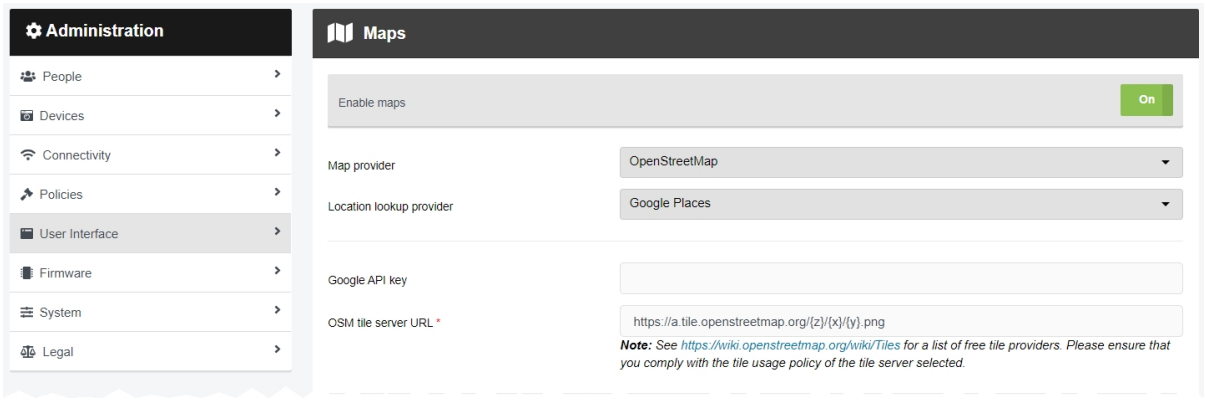
Administrators can disable language files on VideoManager. If a language has been disabled, users cannot select it from their dropdown. However, a disabled language can still be set as VideoManager's server language, or the language for an individual's session, from the ***Admin*** tab. To disable a language file:

1. Navigate to the ***Admin*** tab.
2. Select the ***User Interface*** pane.
3. Click the ***Language*** section.
4. Next to the relevant language file, click ***Enable / disable language***.
5. Set ***Enable language*** to **No**.

9.5.7 Enable and Configure Maps

VideoManager allows administrators to enable or disable maps, select between map and location lookup providers, and set the default location for footage recorded without a GPS track. This is done from the ***Maps*** section of the ***User Interface*** pane, in the ***Admin*** tab.

If the administrator will be using the private ArcGis service, they must first register VideoManager as an app on the service.



To use mapping:

1. Navigate to the ***Admin*** tab.
2. Select the ***User Interface*** pane.
3. Click the ***Maps*** section.
4. Set ***Enable maps*** to **On**.
5. From the ***Map provider*** dropdown, select the maps provider. This will enable administrators to perform actions such as utlising Tactical VideoManager, adding location data to videos, and filtering videos based on this location data. The options are as follows:

   - **Google Places** - if selected, administrators must enter an API key in the ***Google API key*** field.

   An API key can be generated from the Google developers' page.

   - **OpenStreetMap** - if selected, administrators must enter a server URL in the ***OSM tile server URL*** field.
   - **ArcGIS** - if selected, administrators must enter a server URL in the ***ArcGIS tile server URL*** field.

   *If the administrator is using a private ArcGis service, copy the client ID and paste it into the **ArcGIS client ID** field, copy the client secret and paste it into the **ArcGIS client secret** field, and copy the authentication URL and paste it into the **ArcGIS authentication URL** field.*

6. From the ***Location lookup provider*** dropdown, select the location lookup provider. This enables administrators to enter specifc addresses and postcodes when filtering videos based on their location and editing video location data. The options are as follows:

    - **Google Places** - if selected, the administrator can use the same API key entered earlier.
    - **Nominatim** - if selected, the administrator must enter a server URL into the ***Nominatim server URL*** field.

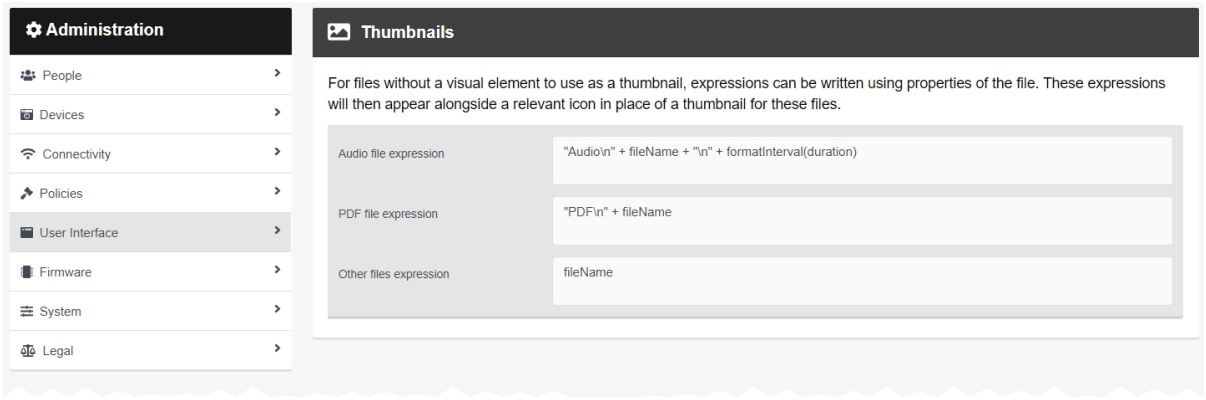
    Nominatim providers may also instruct administrators to enter an API key into the ***Nominatim API key*** field.

    - **ArcGIS** - if selected, the administrator must enter a server URL from their ArcGis account into the ***ArcGIS search server URL*** field.
    - **--** - if selected, no further details must be entered. However, if this is selected, administrators cannot enter specific addresses and postcodes when setting location data for videos. They will only be able to drag and drop a location pin.

7. From the ***Distance units*** dropdown, select the unit of measurement which will be used by VideoManager when presenting maps. The options are **Imperial (ft/mi)** and **Metric (m/km)**.
8. In the ***Default location*** field, administrators can set a default location for videos which do not have GPS data (e.g. because the body-worn camera on which they were recorded is not GPS-enabled). Click ***Set*** to confirm the choice, or ✕ to clear the field.
9. Click ***Save settings***.

9.5.8 Configure Thumbnails

Administrators can utilise markdown to create a phrase which will appear in the place of a thumbnail for assets which were imported without a built-in thumbnail. This is done from the ***Thumbnails*** section of the ***User Interface*** pane, in the ***Admin*** tab.



Administrators can edit the custom thumbnails for imported assets. To do so:

1. Navigate to the ***Admin*** tab.
2. Select the ***User Interface*** pane.
3. Click the ***Thumbnails*** section.
4. Administrators can edit the following fields:
   - ***Audio file expression*** - this dictates the default thumbnail for audio assets.
   - ***PDF file expression*** - this dictates the default thumbnail for PDF assets.
   - ***Other files expression*** - this dictates the default thumbnail for other types of assets.

   There are some thumbnail-specific functions that administrators can input. These are as follows:

   - `\n` - this will create a line break.
   - `+` - this will string multiple values together.
   - `text()` - this will return a string representation of whatever input it is given. This could be a number, or dates.
   - `formatInterval()` - this will rearrange a number of seconds into a more readable format.

   For example, `formatInterval(100)` would return *1m40s*.

   The expression entered will be formatted with markdown.

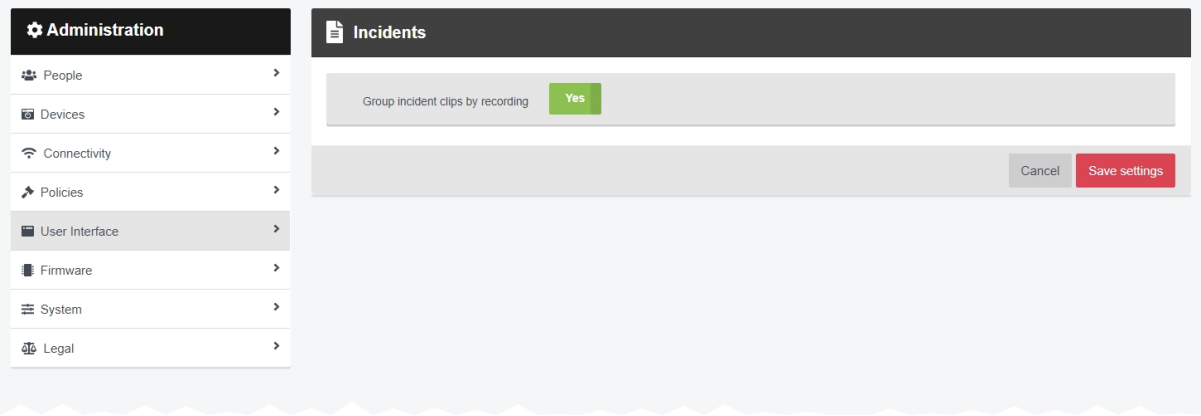
5. Click ***Save settings***.

9.5.9 Configure Incident Settings

If VideoManager was upgraded to 15.0, videos which have been added to an incident (i.e. incident clips) are presented by default as separate clips within that incident, regardless of which recording they came from. However, administrators can also configure VideoManager to present incident clips as children of the original recording they came from. This enables other users on the system to directly compare the original recording to the redacted and shortened incident clips.

If VideoManager was installed with 15.0, incident clips will be presented by default as children of the original recording they came from. However, administrators can also configure VideoManager to present incident clips as separate clips within that incident, regardless of which recording they came from.

Both of these actions can be completed from the ***Incidents*** section of the ***User Interface*** pane, in the ***Admin*** tab.



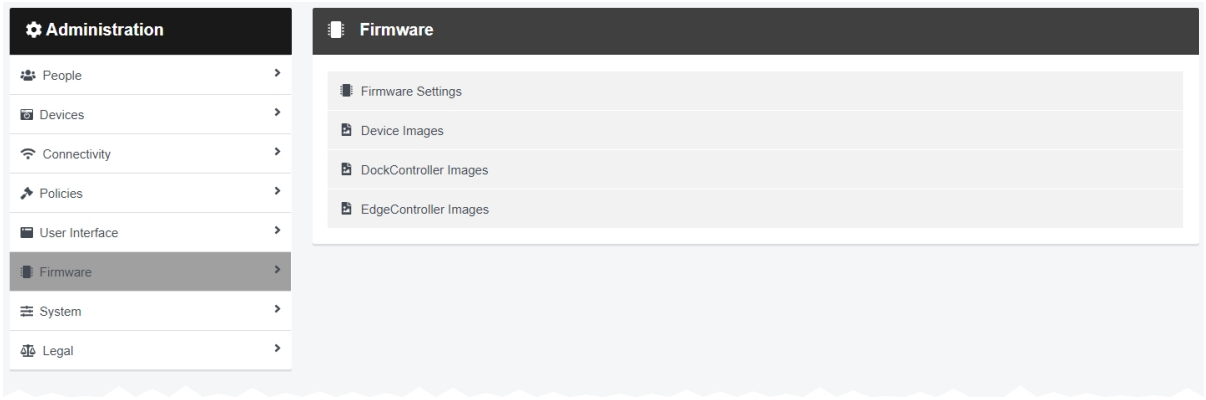
To configure how incident clips are presented in incidents:

1. Navigate to the ***Admin*** tab.
2. Select the ***User Interface*** pane.
3. Click the ***Incidents*** section.
4. Set ***Group incident clips by recording*** to either ***Yes*** to ***No***.
5. Click ***Save settings***.

This change will apply retroactively to all incidents on the system.

9.6 Firmware

In the ***Firmware*** pane, administrators can edit aspects of VideoManager related to body-worn camera firmware.



To access the ***Firmware*** pane:

1. Navigate to the ***Admin*** tab.
2. Select the ***Firmware*** pane.

From here, administrators can access the following sections:

- ***Firmware Settings***

Change global firmware settings, regarding auto-upgrades.

>> For more information, see Configure Firmware Settings on page 332

- ***Device Images***

Import, edit, and delete body-worn camera images.

>> For more information, see Import, Edit and Delete Device Images on page 334

- ***DockController Images***

Import, edit, and delete DockController images.

>> For more information, see Import, Edit and Delete DockController Images on page 336

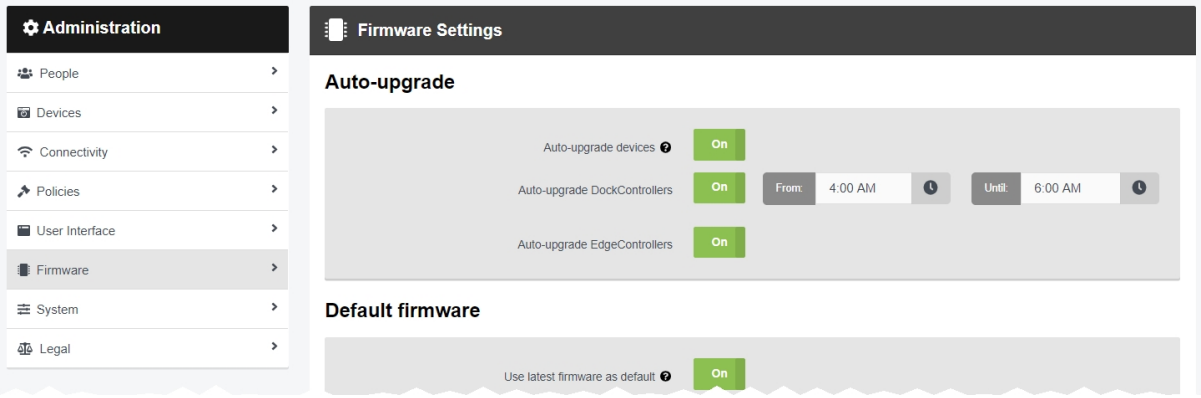
- ***EdgeController Images***

Import, edit, and delete EdgeController images.

>> For more information, see Import, Edit and Delete EdgeController Images on page 338

9.6.1 Configure Firmware Settings

VideoManager can automatically upgrade body-worn cameras when new firmware is released. This eliminates the need for users to manually upgrade their body-worn cameras from the ***Devices*** tab. This is done from the ***Firmware Settings*** section of the ***Firmware*** pane, in the ***Admin*** tab.



To access the ***Firmware Settings*** section:

1. Navigate to the ***Admin*** tab.
2. Select the ***Firmware*** pane.
3. Click the ***Firmware Settings*** section.

There are multiple sections that administrators can configure:

In the ***Auto-upgrade*** section, administrators can configure whether their body-worn cameras, DockControllers and EdgeControllers will be automatically upgraded by VideoManager or not:

- If ***Auto-upgrade*** is set to ***On***, body-worn cameras will automatically be upgraded to whichever firmware has been set as the default.

If set to ***Off***, body-worn cameras must be manually upgraded from the ***Devices*** tab.

- If ***Auto-upgrade DockControllers*** is set to ***On***, all DockControllers connected to VideoManager will automatically be upgraded to whichever firmware has been set as the default.

In the ***From:*** and ***Until:*** fields, administrators can enter the times between which DockControllers will attempt to upgrade. This minimises disruption to the system.

Caution

If a DockController is upgrading, all body-worn cameras connected to it will be inaccessible until it has finished. This means that they cannot be assigned or allocated.

If set to ***Off***, DockControllers must be manually upgraded from the ***DockControllers*** pane.

- If ***Auto-upgrade EdgeControllers*** is set to ***On***, all EdgeControllers connected to VideoManager will automatically be upgraded to whichever firmware has been set as the default.

If set to ***Off***, EdgeControllers must be manually upgraded from the ***Sites*** pane.

In the ***Default firmware*** section, administrators can configure which firmware on VideoManager is set as the default:

- If ***Use latest firmware as default*** is set to ***On***, the default images for body-worn cameras, DockControllers, and EdgeControllers will be automatically set to the **most recent** (e.g. if VideoManager has both 14.3 and 15.0 images, 15.0 will be the default).

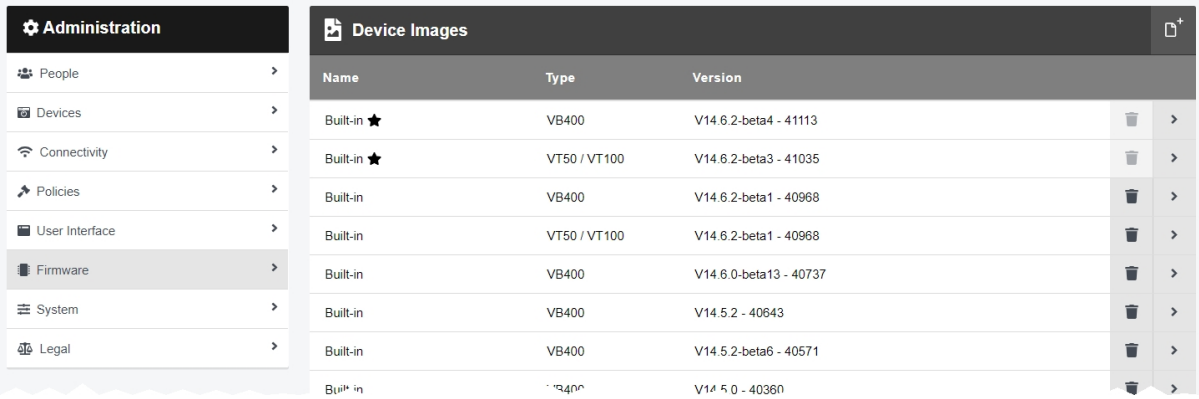
The effect this has depends on how the ***Auto-upgrade*** section has been configured:

- If auto-upgrade has been enabled for devices, then they will be upgraded to the most recent firmware automatically.
- If auto-upgrade has been disabled for devices, then the most recent firmware will be presented as default when a user tries to upgrade them manually from the ***Devices***/***DockControllers***/***Sites*** pane. However, users can also override this default.

Click ***Save settings***.

9.6.2 Import, Edit and Delete Device Images

It is possible to alter device images in case of necessary upgrades. This is done from the ***Device Images*** section of the ***Firmware*** pane, in the ***Admin*** tab.



Once at the relevant section, administrators can choose to either import, edit, or delete the images of their body-worn cameras.

To import a device image:

1. Navigate to the ***Admin*** tab.
2. Select the ***Firmware*** pane.
3. Click the ***Device Images*** section.
4. Click ***Import image***.
5. Choose a file to import as a new image.
6. If ***Default Image*** is set to ***On***, this device image will become the default. When users upgrade a body-worn camera from the ***Devices*** tab, this device image will be presented first. However, users can change which device image will be used.

   This setting is only available if ***Use latest firmware as default*** has been set to ***Off*** in the ***Firmware Settings*** section.

   >> For more information, see Configure Firmware Settings on page 332

7. Click ***OK*** to confirm the choice.

Once a device image has been imported, some of its attributes can be edited. To do so:

1. Navigate to the ***Admin*** tab.
2. Select the ***Firmware*** pane.
3. Click ***Device Images***.
4. Click ***Go to device image*** next to the device image to be edited.

5. In the ***Name*** field, administrators can change the name of the device image.
6. If ***Default Image*** is set to ***On***, this device image will become the default. When users upgrade a body-worn camera from the ***Devices*** tab, this device image will be presented first. However, users can change which device image will be used.

   This setting is only available if ***Use latest firmware as default*** has been set to ***Off*** in the ***Firmware Settings*** section.
7. Click ***More details*** to learn more about the type of image and the hardware which the image can support.
8. Click ***confirm*** to confirm the changes.

To delete a device image:

1. Navigate to the ***Admin*** tab.
2. Select the ***Firmware*** pane.
3. Click ***Device Images***.
4. Next to the device image to be deleted, click ***Delete device image***.

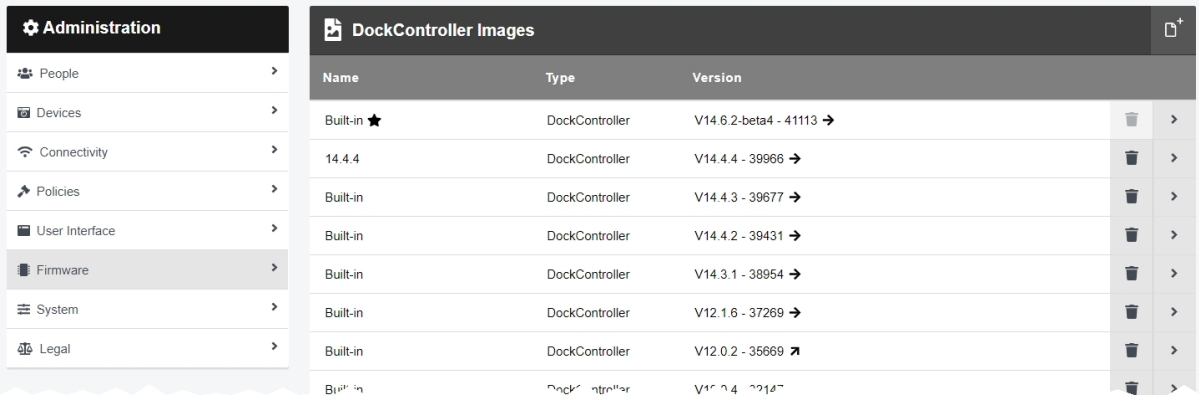
   A default image cannot be deleted.

Body-worn cameras will retain their device images, even if the device image in question has been deleted.

5. Click ***OK*** to confirm deletion.

9.6.3 Import, Edit and Delete DockController Images

It is possible to alter DockController images in case of necessary upgrades. This is done from the ***DockController Images*** section of the ***Firmware*** pane, in the ***Admin*** tab.



Once at the relevant section, administrators can choose to either import, edit, or delete the images of their DockControllers.

To import a DockController image:

1. Navigate to the ***Admin*** tab.
2. Select the ***Firmware*** pane.
3. Click the ***DockController Images*** section.
4. Click ***Import image***.
5. Choose a file to import as a new image.
6. If ***Default Image*** is set to ***On***, this DockController image will become the default. When users upgrade a DockController from the ***DockControllers*** pane, this DockController image will be presented first. However, users can change which DockController image will be used.

   This setting is only available if ***Use latest firmware as default*** has been set to ***Off*** in the ***Firmware Settings*** section.

   >> For more information, see Configure Firmware Settings on page 332

7. Click ***OK*** to confirm the choice.

Once a DockController image has been imported, some of its attributes can be edited. To do so:

1. Navigate to the ***Admin*** tab.
2. Select the ***Firmware*** pane.
3. Click the ***DockController Images*** section.
4. Click ***Go to DockController image*** next to the DockController image to be edited.

5. In the ***Name*** field, users can change the name of the DockController image.
6. If ***Default Image*** is set to ***On***, this DockController image will become the default. When users upgrade a DockController from the ***DockControllers*** pane, this DockController image will be presented first. However, users can change which DockController image will be used.

   This setting is only available if ***Use latest firmware as default*** has been set to ***Off*** in the ***Firmware Settings*** section.
7. Click ***More details*** to learn more about the type of image and the hardware which the image can support.
8. Click ***confirm*** to confirm the changes.

To delete a DockController image:

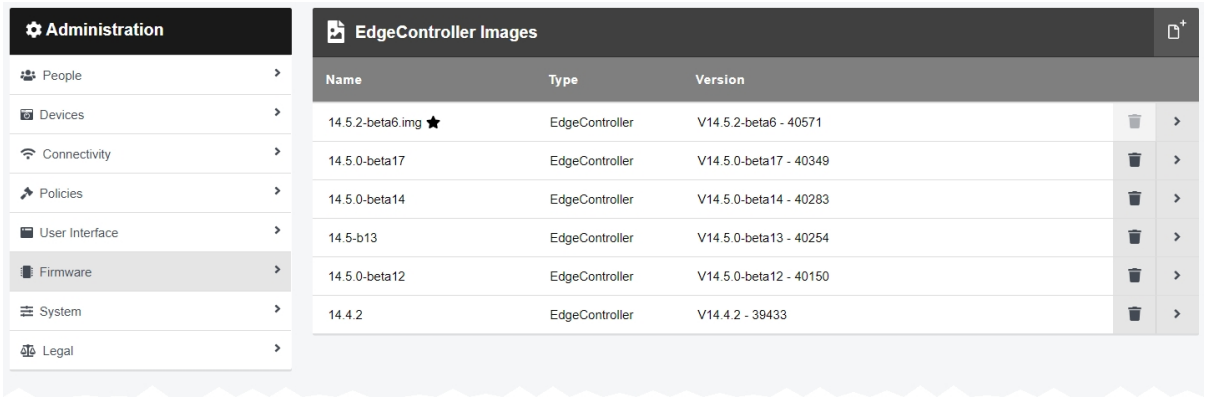
1. Navigate to the ***Admin*** tab.
2. Select the ***Firmware*** pane.
3. Click the ***DockController Images*** section.
4. Next to the DockController image to be deleted, click ***Delete DockController image***.

   A default image cannot be deleted.

   DockControllers will retain their DockController images, even if the DockController image in question has been deleted.
5. Click ***OK*** to confirm deletion.

9.6.4 Import, Edit and Delete EdgeController Images

It is possible to alter EdgeController images in case of necessary upgrades. This is done from the ***EdgeController Images*** section of the ***Firmware*** pane, in the ***Admin*** tab.



Once at the relevant section, administrators can choose to either import, edit, or delete the images of their EdgeControllers.

To import an EdgeController image:

1. Navigate to the ***Admin*** tab.
2. Select the ***Firmware*** pane.
3. Click the ***EdgeController Images*** section.
4. Click ***Import image***.
5. Choose a file to import as a new image.
6. If ***Default Image*** is set to ***On***, this EdgeController image will become the default. When users upgrade an EdgeController from the ***Sites*** pane, this EdgeController image will be presented first. However, users can change which EdgeController image will be used.

   This setting is only available if ***Use latest firmware as default*** has been set to ***Off*** in the ***Firmware Settings*** section.

   >> For more information, see Configure Firmware Settings on page 332

7. Click ***OK*** to confirm the choice.

Once an EdgeController image has been imported, some of its attributes can be edited. To do so:

1. Navigate to the ***Admin*** tab.
2. Select the ***Firmware*** pane.
3. Click the ***EdgeController Images*** section.
4. Click > ***Go to EdgeController image*** next to the EdgeController image to be edited.

5. In the ***Name*** field, users can change the name of the EdgeController image.
6. If ***Default Image*** is set to ***On***, this EdgeController image will become the default. When users upgrade an EdgeController from the ***Sites*** pane, this EdgeController image will be presented first. However, users can change which EdgeController image will be used.

   This setting is only available if ***Use latest firmware as default*** has been set to ***Off*** in the ***Firmware Settings*** section.
7. Click ***More details*** to learn more about the type of image and the hardware which the image can support.
8. Click ***confirm*** to confirm the changes.

To delete an EdgeController image:

1. Navigate to the ***Admin*** tab.
2. Select the ***Firmware*** pane.
3. Click the ***EdgeController Images*** section.
4. Next to the EdgeController image to be deleted, click ***Delete EdgeController image***.

   A default image cannot be deleted.

EdgeControllers will retain their EdgeController images, even if the EdgeController image in question has been deleted.

5. Click ***OK*** to confirm deletion.

9.7 System

In the ***System*** pane, administrators can edit aspects of VideoManager related to storage and server configuration. This pane should not usually be accessed unless the administrator has working knowledge of their PC.

To access the ***System*** pane:

1. Navigate to the ***Admin*** tab.
2. Select the ***System*** pane.

From here, administrators can access the following sections:

- ***Storage*** - administrators can perform the following actions:
  - Configure file containers, if the administrator will be using S3 Object Storage or Azure Blob Storage instead of a filesystem.

    >> For more information, see Create, Edit and Delete File Containers on page 342

  - Configure file spaces and free up space on an instance of VideoManager.

    >> For more information, see Create, Edit and Delete File Spaces on page 344

  - Configure file space warnings, which appear when one of VideoManager's file spaces is almost full.

    >> For more information, see Configure File Space Warnings on page 348

- ***Web Server***

Configure web server settings, and discover the server's listen address and public address.

>> For more information, see Configure the Web Server on page 349

- ***Backup Databases***

Configure how often backups are performed.

>> For more information, see Create Backup Databases on page 351

- ***Licences***

Import or renew licences. Licences determine which actions users can perform on VideoManager - for example, Tactical VideoManager is a licensed feature.

>> For more information, see Import and Delete Licences on page 353

- ***Advanced Settings***

Configure the advanced settings file.

>> For more information, see Configure the Advanced Settings on page 355

- ***Import/Export System Config***

Import or export key aspects of VideoManager's configuration.

>> For more information, see Import or Export VideoManager's Configuration on page 356

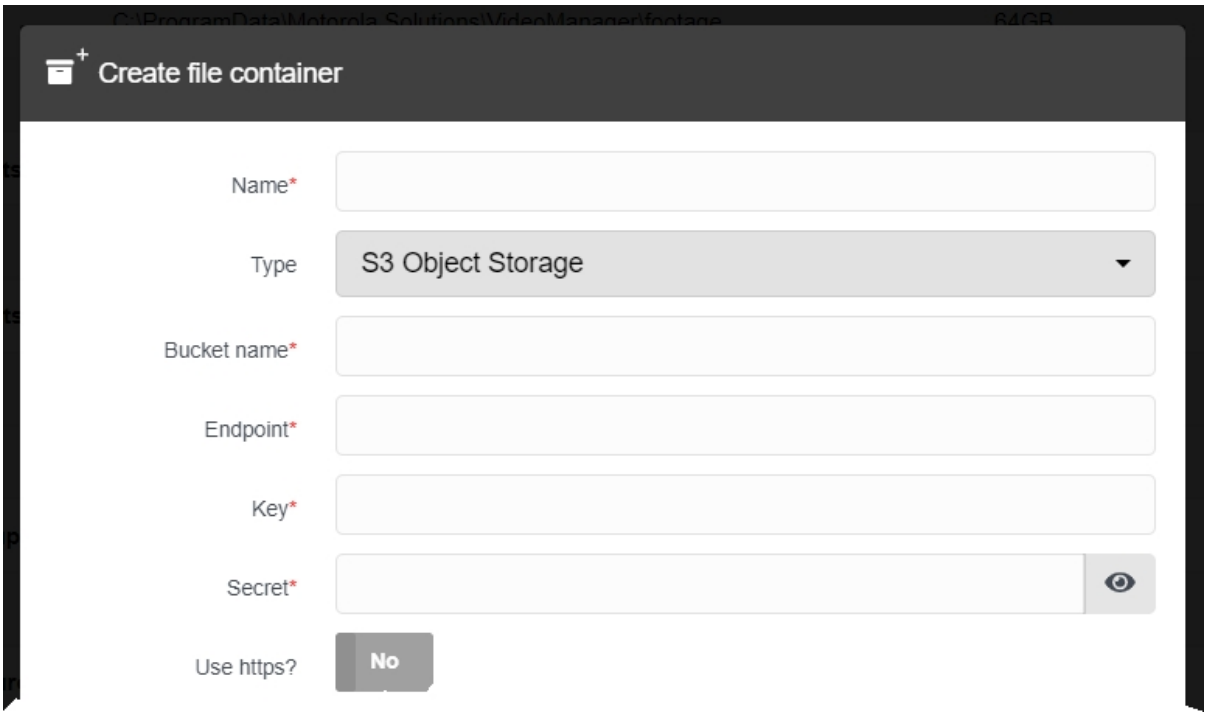
- ***Server Controls***

Restart the server. This will allow certain changes to come into effect - for example, if the administrator has changed VideoManager's ***Server listen address***.

>> For more information, see Restart the Server on page 358

9.7.1 Create, Edit and Delete File Containers

If footage and other data will be stored in object storage instead of a file system, administrators must create file containers on VideoManager which contain information about the object store. This enables file spaces on VideoManager to connect to the cloud. This configuration is completed from the ***Storage*** section of the ***System*** pane, in the ***Admin*** tab.



These steps can be ignored by administrators who haven't bought Amazon S3 Object Storage or Azure Blob Storage, and will be using filesystem storage instead.

To create a file container for use with file spaces:

1. Navigate to the ***Admin*** tab.
2. Select the ***System*** pane.
3. Click the ***Storage*** section.
4. Click ***Create file container***.
5. In the ***Name*** field, enter a name for the file container. This will be how the file container is identified on VideoManager.
6. From the ***Type*** dropdown, select either **S3 Object Storage** or **Azure Blob Storage**.

The following steps differ, depending on the kind of storage purchased by the administrator.

If the administrator is using S3 Object Storage:

1. In the ***Bucket name*** field, enter the bucket name. Motorola Solutions suggests using VideoManager's unique fully qualified domain name.

2. In the ***Endpoint*** field, enter the endpoint of the file container.

To check this information, open the AWS console, navigate to the ***Properties*** tab, and select the ***Bucket overview*** pane. In the ***Region*** section, make a note of the region. Enter it in the ***Endpoint*** field, with the format `s3.region code.amazonaws.com` (where `region code` is replaced with the region).

*The endpoint **must** match the region where the bucket was created.*

3. In the ***Key*** and ***Secret*** fields, enter the IAM user's key and secret, respectively.

The administrator can only get this information immediately after creating an IAM user with S3 access. If the administrator does not have the key and secret for the IAM user, they must create another user and make a note of the key and secret's information which is presented when the user is saved.

If the administrator is using Azure Blob Storage:

1. In the ***Container name*** field, enter the name of the container.

The administrator can either enter the name of a container that already exists in their Azure account, or enter the name for a new container. If a new container name is entered, Azure Blob Storage will automatically create the container - to check whether this has been successful, on Azure, navigate to the ***Storage accounts*** tab, select the ***Storage account*** pane, and click the ***Containers*** section. The new container should be visible.

2. In the ***Endpoint*** field, enter the endpoint of the file container.

To check this information, in the ***Endpoints*** tab, click the ***Blob service*** pane, and copy and paste the value from the ***Blob service field***.

3. In the ***Account*** field, enter the name of the Azure Blob Storage account.

4. In the ***Secret*** field, enter the container's secret.

To check this information, on Azure, navigate to the ***Access Keys*** tab, click ***Show keys***, and copy and paste either of the keys.

Click ***confirm***.

9.7.2 Create, Edit and Delete File Spaces

File spaces determine where information from VideoManager is stored - this could be on the user's PC, a network database, or Amazon S3 Object Storage (if it has been purchased).

To create a file space:

1. Navigate to the ***Admin*** tab.
2. Select the ***System*** pane.
3. Click the ***Storage*** section.
4. Click ***Create file space***. The ***Create file space*** window opens.
5. Enter the path for the new file space.

A network database with a backup system is encouraged if users have this instead. If the user has purchased Amazon S3 Object Storage, they should enter the name of a folder within the bucket, which will then be created.

6. From the ***Category*** dropdown, select a category for the file space.

The categories are as follows:

- **Footage** - this is where all downloaded footage will be stored.
- **Exports** - this is where all incident exports will be stored.
- **Backups** - this is where the VideoManager database information from backups will be stored.

>> For more information, see Create Backup Databases on page 351

- **Reports** - this is where all reports will be stored.
- **Report Auto Copy** - this is where all scheduled reports will be automatically copied to. If this option is selected, no more configuration is necessary from this pane, and the user can click ***confirm***.

7. In the ***Max size*** field, enter the maximum size of the file space. From the dropdown, choose a unit in which the data will be counted - this could be **Bytes**, **Kilobytes**, **Megabytes**, **Gigabytes**, **Terabytes**, or **Petabytes**.

Motorola Solutions recommends that the maximum size is **not** set to the absolute upper limit of the disk/drive.

If every file space of one type is full, system functions will stop working (e.g. if all **Footage** *file spaces are full, body-worn cameras will not be able to download footage to VideoManager when docked, and will instead enter an error state).*

8. From the ***State*** dropdown, select a state for the file space. In most cases, this will be **Online**. However, users can also select:

- **Obsolete** - this is useful if users wish to keep a file space on VideoManager, but do not want footage or other data to be sent there.
- **Offline** - this is useful if the network database or local storage is down for maintenance. However, if the file space is marked as **Offline**, all information that was in the file space will be unavailable until it comes back online again.
- **Evacuate** - this will automatically move all data in the file space to the other file space(s) of the same type. This is useful if an old file space should be deleted, but the data within it should be kept.

If another user on the system is viewing, editing, or exporting the data in a file space which is being evacuated, the evacuation will be forced to wait until the other actions have finished.

9. From the ***Encryption*** dropdown, select an encryption type (if relevant). The options are **NONE**, **AES-128**, **AES-192**, and **AES-256**.

This cannot be changed later. If an encryption mode is chosen, users **must** download the encryption key after creation, and store it offsite. This ensures that the data can be recovered later in case of a disaster. To do so:

- Click > ***Go to file space*** next to the file space whose encryption key should be downloaded.
- Click ***Download Key***.

The key will be downloaded to the PC's default download location. It should be transferred to a secure location offsite.

If unsure, Motorola Solutions recommends that users choose **AES-256***.*

10. If ***Preferred*** is set to ***Yes***, all footage/exports/reports/backups will be sent to this file space until it is full.

If multiple file spaces have ***Preferred*** set to ***Yes***, VideoManager will alternate between those file spaces when storing resources.

If no file spaces have ***Preferred*** set to ***Yes***, VideoManager will alternate between all file spaces when storing resources.

11. Click ***confirm*** to save the changes.

Once file spaces have been created, their paths can be changed. Motorola Solutions recommends creating an entirely new file space with the updated path, and migrating all files in the old file space over to it. To do so:

1. Navigate to the ***Admin*** tab.
2. Select the ***System*** pane.
3. Click the ***Storage*** section.
4. Click ***Create file space***. The ***Create file space*** window opens.

5. Enter the path for the new file space.
6. Configure the rest of the settings as desired, and ensure that ***Preferred*** is set to ***Yes***.
7. Click ***confirm***.
8. Click > ***Go to file space*** next to the old file space whose path must be changed.
9. From the ***Category*** dropdown, select **Evacuate**.

The data in the old file space will be evacuated to the file space with the new path. The old file space can now be deleted, by clicking ***Delete file space***.

Alternatively, administrators can change the path of the original file space itself. Before doing so, they must stop the VideoManager service, and manually move the files to the new location. Then, on VideoManager:

1. Navigate to the ***Admin*** tab.
2. Select the ***System*** pane.
3. Click the ***Storage*** section.
4. Click > ***Go to file space***,
5. Click ***Change***.
6. Make the required edits, and click ***confirm***.

If the user wishes to change the size of the file space because it is becoming full, the steps they must take are as follows:

1. Navigate to the ***Admin*** tab.
2. Select the ***System*** pane.
3. Click the ***Storage*** section.
4. Click > ***Go to file space*** next to the file space whose size should be changed.
5. In the ***Max size*** field, make the relevant changes.
6. Click ***confirm***.

It may become necessary to delete a file space altogether. To do so users must first ensure that **all** data in the file space has been evacuated to another suitable file space. To do so:

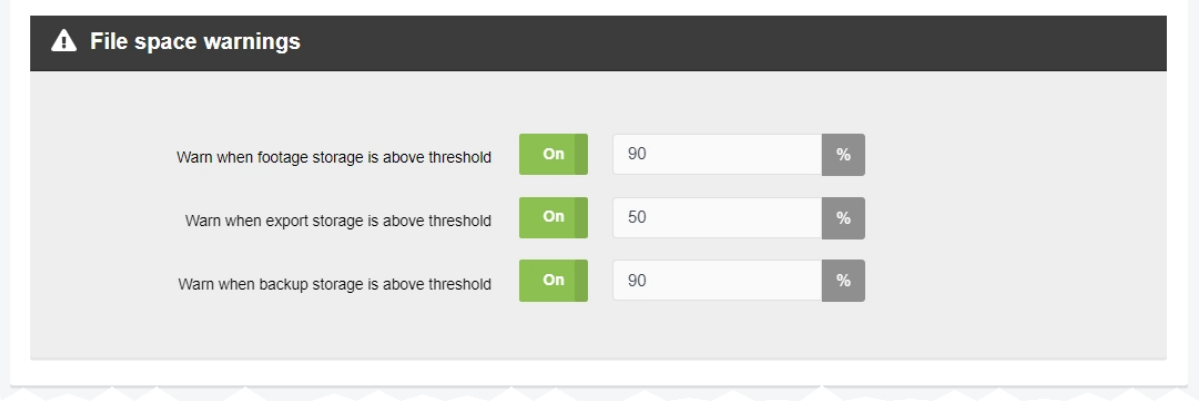
1. Ensure that there is at least one other file space on VideoManager whose ***Category*** matches that of the file space which is being deleted, and whose ***State*** is set to **Online**.
2. Click > ***Go to file space*** next to the file space to be deleted.
3. From the ***Category*** dropdown, select **Evacuate**.
4. Click ***confirm***.

The data in the deleted file space will be evacuated to the other file space(s).

5. Next to the now-empty file space, click **Delete file space**.

9.7.3 Configure File Space Warnings

Administrators can configure file space warnings, which appear when file spaces reach a certain threshold. These are useful because they ensure that administrators can take action before the file spaces are completely full.



To configure file space warnings:

1. Navigate to the ***Admin*** tab.
2. Select the ***System*** pane.
3. Click the ***Storage*** section.
4. In the ***File space warnings*** section, enable the relevant alarms.

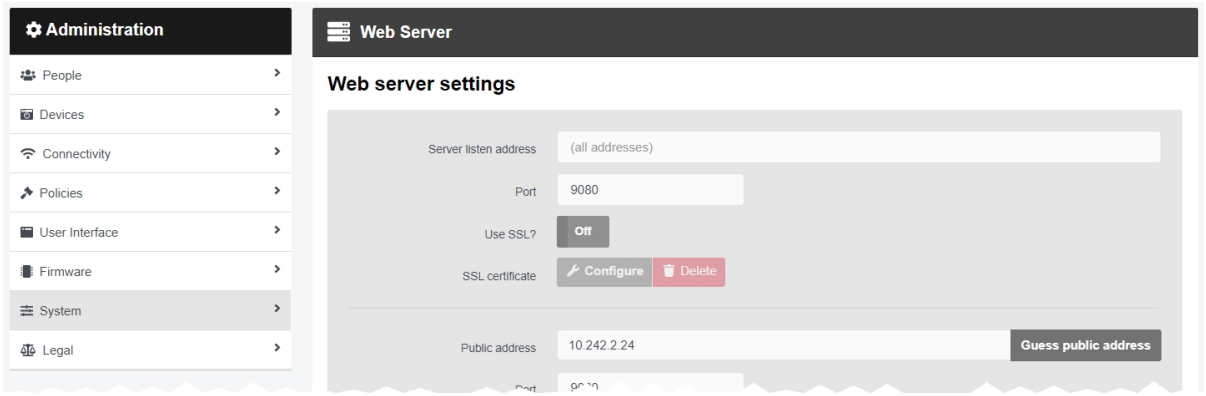
   They are as follows:

   - If ***Warn when footage storage is above threshold*** is set to ***On***, the administrator will be prompted to enter a percentage (between 1 and 100%), above which an alarm will be triggered.
   - If ***Warn when export storage is above threshold*** is set to ***On***, the administrator will be prompted to enter a percentage (between 1 and 100%), above which an alarm will be triggered.
   - If ***Warn when backup storage is above threshold*** is set to ***On***, the administrator will be prompted to enter a percentage (between 1 and 100%), above which an alarm will be triggered.
5. Click ***Save settings***.

From now on, whenever the **Footage**, **Exports** or **Backups** file spaces grow larger than the specified percentage, a system warning will appear in the ***Notifications*** pane on the administrator's homepage, and the ***System*** pane of the ***Status*** tab.

9.7.4 Configure the Web Server

The ***Web Server*** pane is used to control how VideoManager offers the browser-based user interface to users. This is done from the ***Web Server*** section of the ***System*** pane, in the ***Admin*** tab.



To configure the browser-based interface:

1. Navigate to the ***Admin*** tab.
2. Select the ***System*** pane.
3. Click the ***Web Server*** section.
4. Enter the following information:
   - ***Server listen address*** - the address which users should enter to get to VideoManager. This should ordinarily be the local IP address of the server running VideoManager. If the administrator does not know this address, they should click ***Guess public address***
   - ***Port*** - the port which VideoManager will listen on. By default, this is 9080.
   - ***Use SSL?*** - if enabled, connections between the user's browser will be secured with SSL.

   The SSL certificate used to secure the connection can be uploaded by selecting ***Configure***. Click ***Choose File*** and then select the certificate. The correct passphrase must be entered in the ***Passphrase*** box. After it is entered, ***Unlock*** will unlock the certificate. Once unlocked, select ***OK*** to save these details.

   Optionally set ***Enable legacy protocols*** to ***On***. Click for more information.

   Click ***Delete*** to delete the current SSL certificate, if a new certificate should be uploaded.

   - ***Public address*** - this is the address which users can use to access VideoManager if they are not on the same network as the server. ***Guess public address*** will try to guess what this address should be.
   - ***Port*** - the port which VideoManager uses to listen to traffic, including Dock-Controller and body-worn camera information.

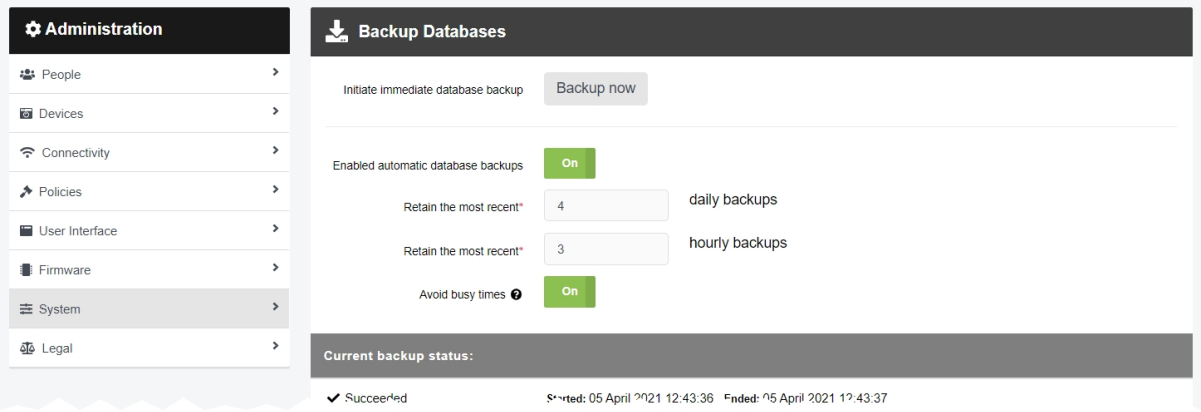
- ***Use SSL?*** - if enabled, then SSL will be used to secure connections to the ***Public address***.

The server's listen address and public address are shown at the bottom of the pane.

5. Click ***Save settings***.

9.7.5 Create Backup Databases

VideoManager offers a backup database service to help prevent the loss of crucial files in the event of an IT failure. A backup contains database metadata, such as the audit log, custom configurations, and descriptions of videos, incidents, and exports. These backups will be used by Motorola Solutions to restore an administrator's instance of VideoManager. Backups are configured from the ***Backup Databases*** section of the ***System*** pane, in the ***Admin*** tab.



The backup function only backs up the system state - it does not back up the contents of the footage, exports or reports filespaces. **Backups should be regularly transferred to a secure location offsite.**

Administrators can initiate an immediate backup. This will capture VideoManager's state at the time when the immediate backup was created. To do so:

1. Navigate to the ***Admin*** tab.
2. Select the ***System*** pane.
3. Click the ***Backup Databases*** section.
4. Click ***Backup now***.

   The backup will be sent to wherever has been configured from the ***Storage*** section.

>> For more information, see Create, Edit and Delete File Spaces on page 344

Administrators can also configure recurring backups, which run automatically every hour. To do so:

1. Navigate to the ***Admin*** tab.
2. Select the ***System*** pane.
3. Click the ***Backup Databases*** section.
4. Set ***Enabled automatic database backups*** to ***On***.

   This will enable the administrator to configure more settings in relation to automatic backups.
5. Enter the number of most recent **daily** and **hourly** backups that will be retained.

A **daily** backup is the last **hourly** backup within a 24-hour window. It is recommended to configure both of these settings

6. If ***Avoid busy times*** is set to ***On***, backups will only occur when there is little or no activity occurring on VideoManager, in order to minimise system load.
7. Click ***Save settings***.

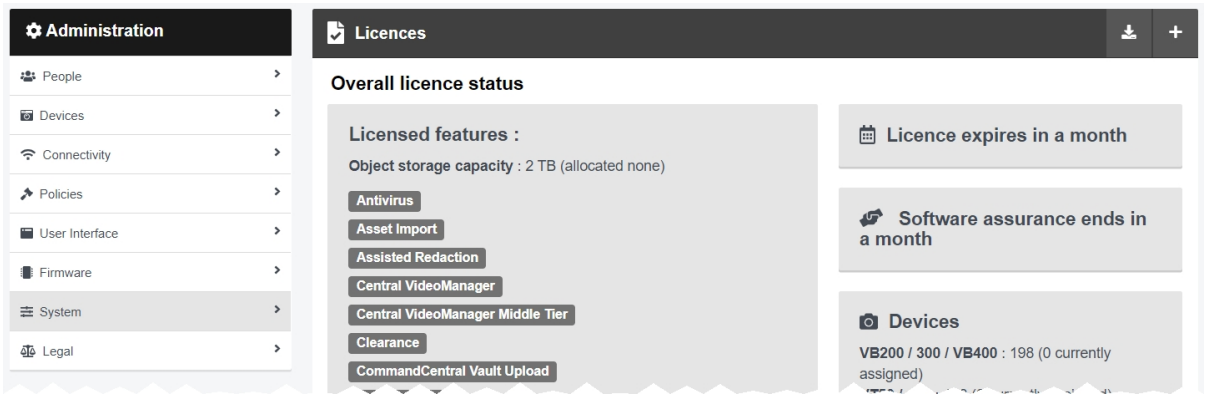
The backup will be sent to wherever has been configured from the ***Storage*** section.

>> For more information, see Create, Edit and Delete File Spaces on page 344

The current backup status will be displayed at the bottom of the pane, as well as the start and end date of the backup.

9.7.6 Import and Delete Licences

The ***Licences*** pane enables administrators to license features of VideoManager which would otherwise be inaccessible. It also allows administrators to view the licences they have already bought, the expiry dates of the licences, and the number of VB-series cameras and VT-series cameras which their licences support. This is done from the ***Import licence*** section of the ***System*** pane, in the ***Admin*** tab.



To import a licence:

1. Navigate to the ***Admin*** tab.
2. Select the ***System*** pane.
3. Click the ***Licences*** section.
4. Click ***Import licence***.
5. Click ***Choose File***.

   Administrators should select the licence provided to them by Motorola Solutions.

   For more information, please contact Motorola Solutions Support.

6. In the ***Activation key*** field, enter the key provided by Motorola Solutions in the licence email.

   *If the key entered here does not match the key set by Motorola Solutions, the licence **will not work**.*

7. Click ***import***.

   If successful, the licence should appear as ***Valid***. All licences are on and enabled by default once imported.

An imported licence will usually have an expiry date. A warning will appear on VideoManager when a licence is **one week** away from expiration. When the licence expires, VideoManager will restart.

It may be necessary to delete a licence once it has expired. To do so:

1. Navigate to the ***Admin*** tab.
2. Select the ***System*** pane.
3. Click the ***Licences*** section.
4. Click ***Delete licence***.

If the licence is still valid, VideoManager will present a list of all the features which will stop working when the licence is deleted.

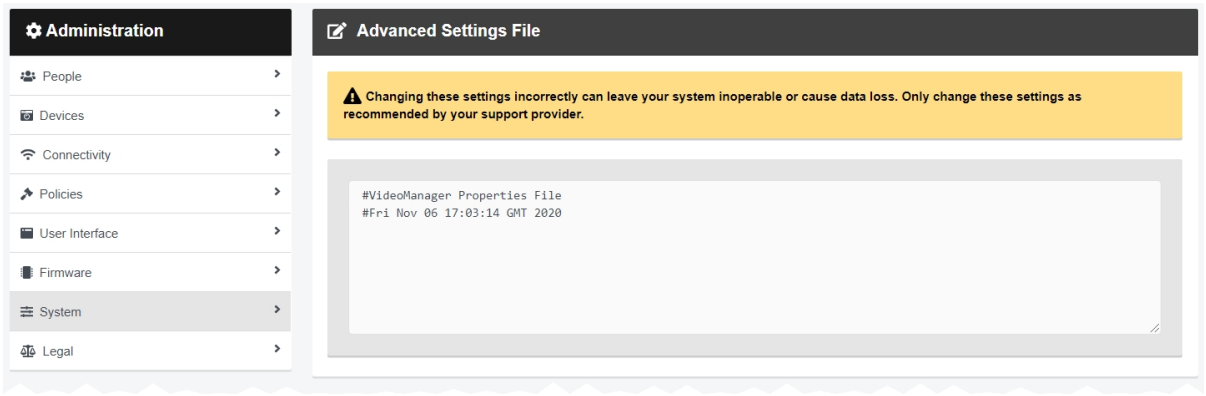
5. Click ***Tick to confirm***.
6. Click ***yes***.

Caution

*If the licence was still valid at the time of deletion, all VideoManager features associated with it will **immediately** stop working.*

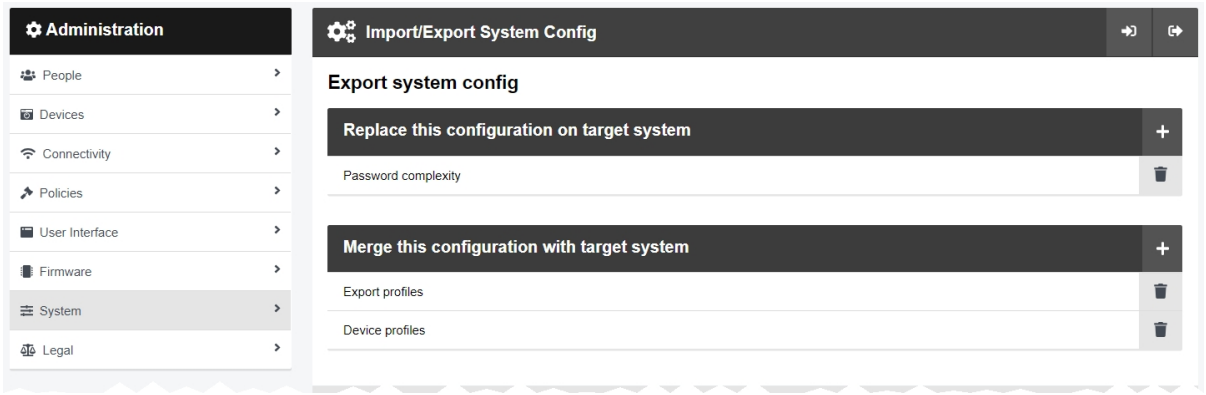
9.7.7 Configure the Advanced Settings

The advanced settings file allows administrators to configure specialised features, for a demonstration or tutorials. This should only be done if the administrator has been given explicit permission from Motorola Solutions Support, and should not be attempted otherwise. All edits to this file are done from the ***Advanced Settings*** section of the ***System*** pane in the ***Admin*** tab.



9.7.8 Import or Export VideoManager's Configuration

It may be necessary for administrators to import or export VideoManager's configuration - for example, if VideoManager has been configured on a test server, and the results should be imported into a live, working version. This is done from the ***Import/Export System Config*** section of the ***System*** pane in the ***Admin*** tab.



To create, and then export, a system configuration:

1. Navigate to the ***Admin*** tab.
2. Select the ***System*** pane.
3. Click the ***Import/Export System Config*** section.
4. From the ***Replace this configuration on target system*** dropdown, administrators can select which policies will be added to the system configuration file.

Caution *Imported policies will **overwrite** previously-existing policies on VideoManager.*

Click + to add a set of information to the exported configuration. The options are as follows:

- **Password complexity** - the password complexity policy will be exported.
- **Deletion policy** - the deletion policy will be exported.

5. From the ***Merge this configuration with target system*** dropdown, administrators can select which roles, fields, and profiles will be added to the system configuration file.

Caution *If any of the imported roles, fields, or profiles from the original VideoManager have the same names as previously-existing roles, fields or profiles on the new instance of VideoManager, the latter will be **overwritten**.*

Click + to add a set of information to the exported configuration. The options are as follows:

- **Roles** - roles will be exported.
- **Shareable device keys** - access control keys will be exported.

- **Import profiles** - import profiles will be exported.
- **Export profiles** - export profiles will be exported.
- **User defined fields** - user-defined incident fields, user-defined media fields, and user-defined playback reason fields will be exported.
- **Device profiles** - device profiles will be exported.
- **WiFi profiles** - WiFi profiles will be exported.

6. Click ***Save settings***.
7. Click ***Export system config***.

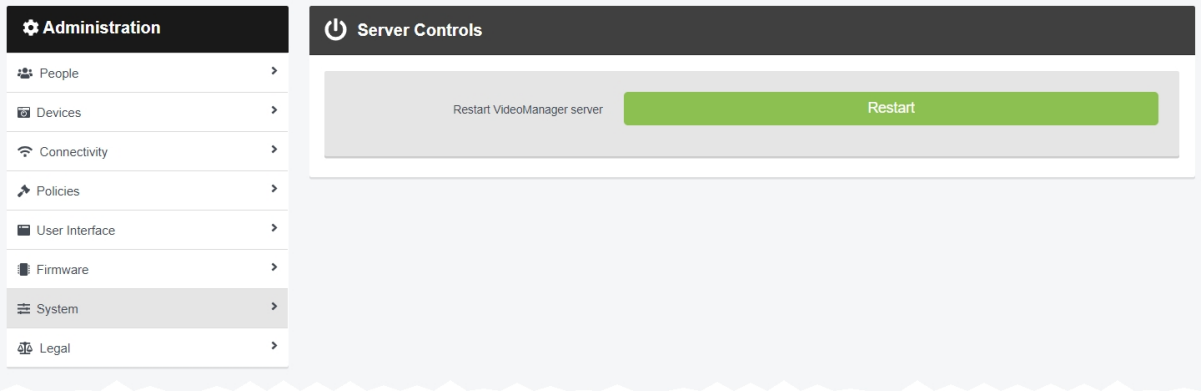
The exported configuration will be downloaded to the PC's default download location.

To import a previously-created system configuration into an instance of VideoManager:

1. Navigate to the ***Admin*** tab.
2. Select the ***System*** pane.
3. Click the ***Import/Export System Config*** section.
4. Click ***Import system config***.
5. Select the previously-downloaded system configuration.
6. Click ***confirm***.

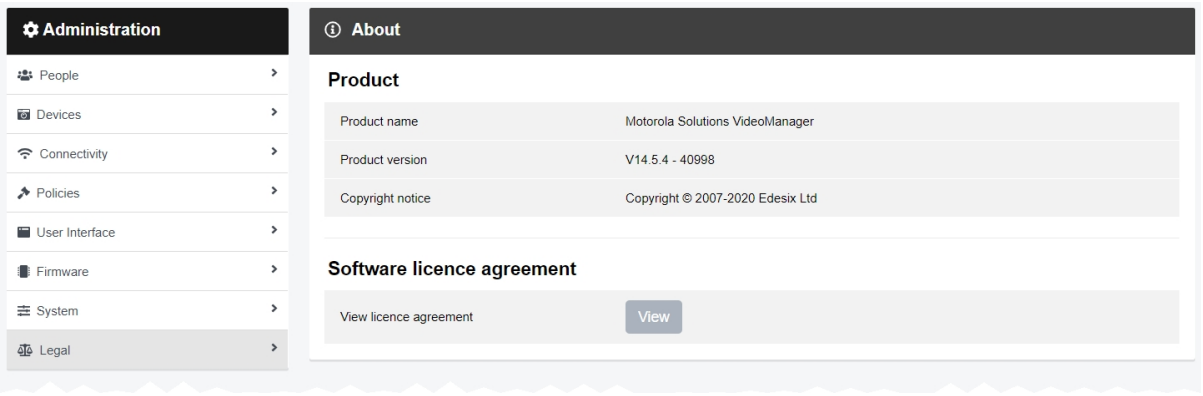
9.7.9 Restart the Server

Under some circumstances, or when advised by Motorola Solutions Support, it may be necessary to restart the VideoManager service. This can be done from the ***Server Controls*** section of the ***System*** pane of the ***Admin*** tab.



9.8 View Legal Information

Administrators may need to view information about VideoManager related to legality and the terms of service. This is done from the ***Legal*** pane in the ***Admin*** tab.



To view VideoManager's legal information:

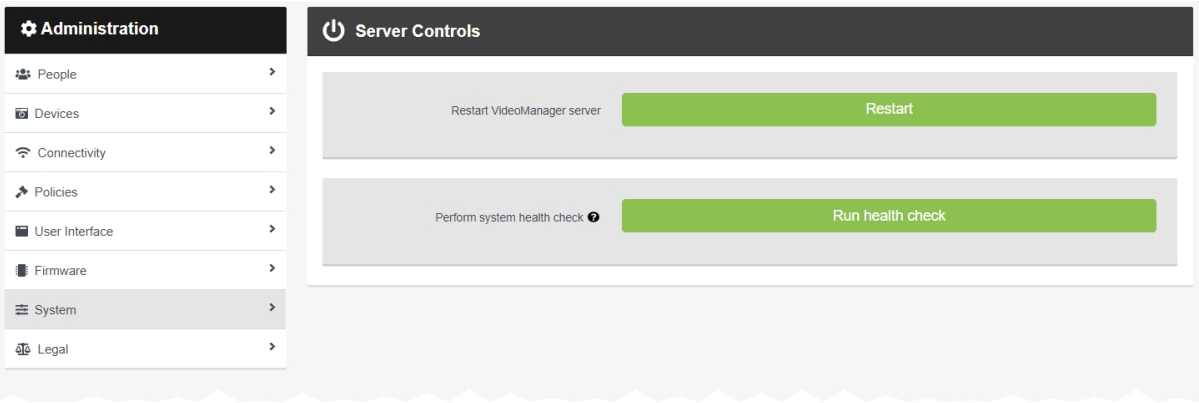
1. Navigate to the ***Admin*** tab.
2. Select the ***Legal*** pane.
3. Click ***About***.

Here, administrators can view the following fields:

- **Product name** - the name of the system.
- **Product version** - the version number of the system.
- **Copyright notice** - who has copyrighted the system, and for how long.
- **View licence agreement** - by clicking ***View***, administrators can check the licence agreement. This will have already been agreed to when initially logging on to the system.

9.9 Create a System Health Check

Normally, the IT department will be able to monitor computers and ensure that they are working properly. However, in some deployment scenarios, it may be helpful to configure an automated check of the health of the computer and warn users that they should contact support if there is something wrong. In this case, the administrator can create a script to check the health of the local computer (e.g. check that the disk RAID array is working correctly) and if not, provide a suitable error message to show to the user.



To create a system health check script:

1. Navigate to VideoManager's *config* folder.

   By default, this will be in the path *C:\ProgramData\Motorola Solutions\VideoManager*.

   > *If ProgramData isn't visible, navigate to the **View** tab at the top of the pane, and tick the **Hidden Items** checkbox.*

2. In the *config* folder, create a file called *health-check.bat*.
3. The script should return an exit code of **1** to indicate that a warning should be shown to users and **2** to indicate that there is an error and that users should be prevented from using VideoManager. If the script outputs a line beginning `Message:` then the message will be shown to users.

   For example, the following batch file script would show the message `This is an error` to users and disable VideoManager:

   ```
   echo Message:This is a warning
    exit /b 1
   ```

   Save the file, and restart VideoManager from the ***Server Controls*** section.

It is possible to configure when the health check is run automatically on VideoManager. To do so:

1. Navigate to the ***Admin*** tab.
2. Select the ***System*** pane.
3. Click the ***Advanced Settings*** section.

4. In the file, enter the following:

```
health.check.period.secs=number of seconds
```

This will set the period between health checks while healthy to the number of seconds specified.

```
health.check.error.period.secs=number of seconds
```

This will set the period between health checks while in an error state to the number of seconds specified.

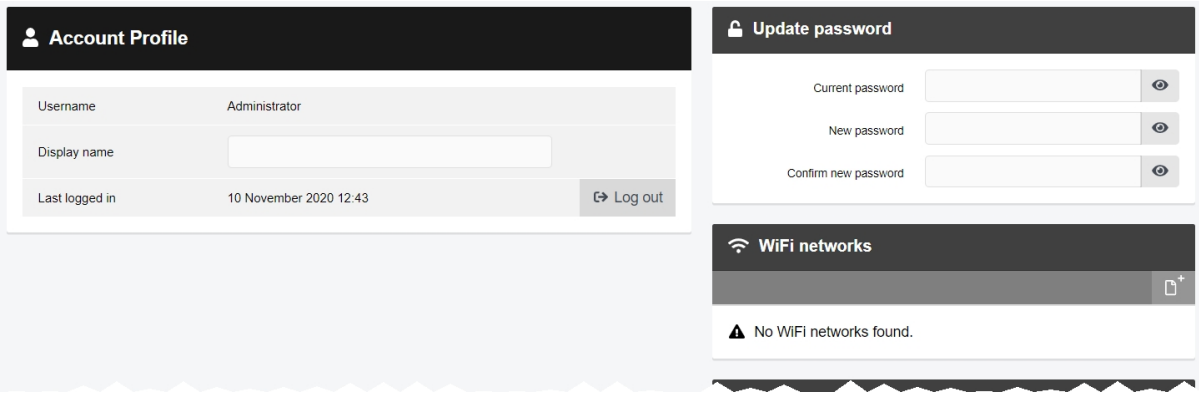
The default time period for a reoccurring healthy system check is an hour. The default time period for a reoccurring error system check is three minutes.

Although the check runs automatically, it is possible to run it manually as well. To do so:

1. Navigate to the ***Admin*** tab.
2. Select the ***System*** pane.
3. Click the ***Web Server*** section.
4. Click ***Run Health Check***.

10 Account Profile

In the ***Account Profile*** pane, users can edit aspects of their VideoManager 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 footage over a personal hotspot.

>> For more information, see Create User-Specific WiFi Networks on page 367

- View two factor authentication settings.

This is covered in the ***Multi-Step Processes*** section.

>> For more information, see Multi-Step Processes on page 363

11 Multi-Step Processes

There are some processes on VideoManager which span multiple sections of the UI - for this reason, they have been compiled here instead.

- Configure streaming.

>> For more information, see Configure Streaming on page 364

- Configure sites.

>> For more information, see Configure Sites on page 374

- Configure privilege escalation.

>> For more information, see Configure Privilege Escalation on page 390

- Use Peer-Assisted Recording (PAR) with VB400s.

>> For more information, see Use Bluetooth with Peer-Assisted Recording (PAR) on page 394

11.1 Configure Streaming

Body-worn cameras can be configured to send a live stream to VideoManager 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 is configured to use anything other than its default port **or** if VideoManager is set up on a public network.

   >> For more information, see Configure Firewalls on page 365

2. Configure VideoManager's public address.

   >> For more information, see Configure VideoManager's Public Address on page 366

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 367

4. Create a WiFi profile which can be used for streaming.

   >> For more information, see Create a WiFi Profile on page 369

5. Assign the body-worn camera to a user, and begin streaming footage.

   >> For more information, see Assign a Body-Worn Camera for Streaming on page 371

6. View the live stream.

   >> For more information, see View Live Streams on page 373

If users have trouble configuring streaming, they should see the FAQs section.

11.1.1 Configure Firewalls

Sometimes, body-worn cameras will be unable to stream to VideoManager without prior firewall configuration. There are two reasons that firewall configuration might be necessary: the user has either changed VideoManager'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.

If the user has changed VideoManager'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's port, and click ***Next***.
   This can be found on VideoManager, 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***.

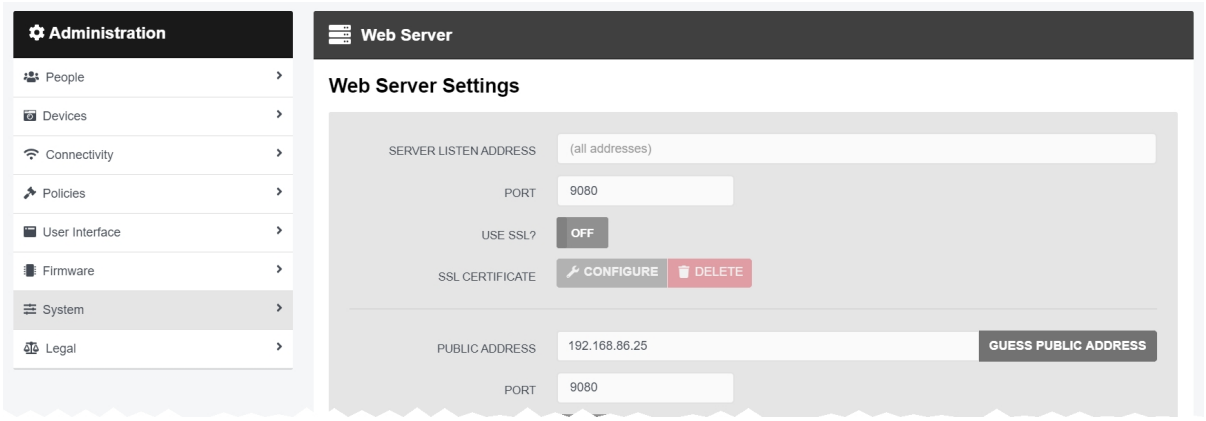
If the user has other firewalls or NAT routers in the network between VideoManager and the WiFi network to which body-worn cameras will connect, they must also be configured to allow TCP connections between the body-worn camera and the VideoManager server.

If the user has connected VideoManager 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 Web* rule is visible.
6. Double-click on the rule and in the ***Advanced*** section, ensure that **Public** is checked.
7. Click ***OK***.

11.1.2 Configure VideoManager's Public Address

When a body-worn camera connects to VideoManager, it does so using VideoManager's public address. If the body-worn cameras are connecting to the same IP network as VideoManager, users can utilise the same IP address as the VideoManager machine.



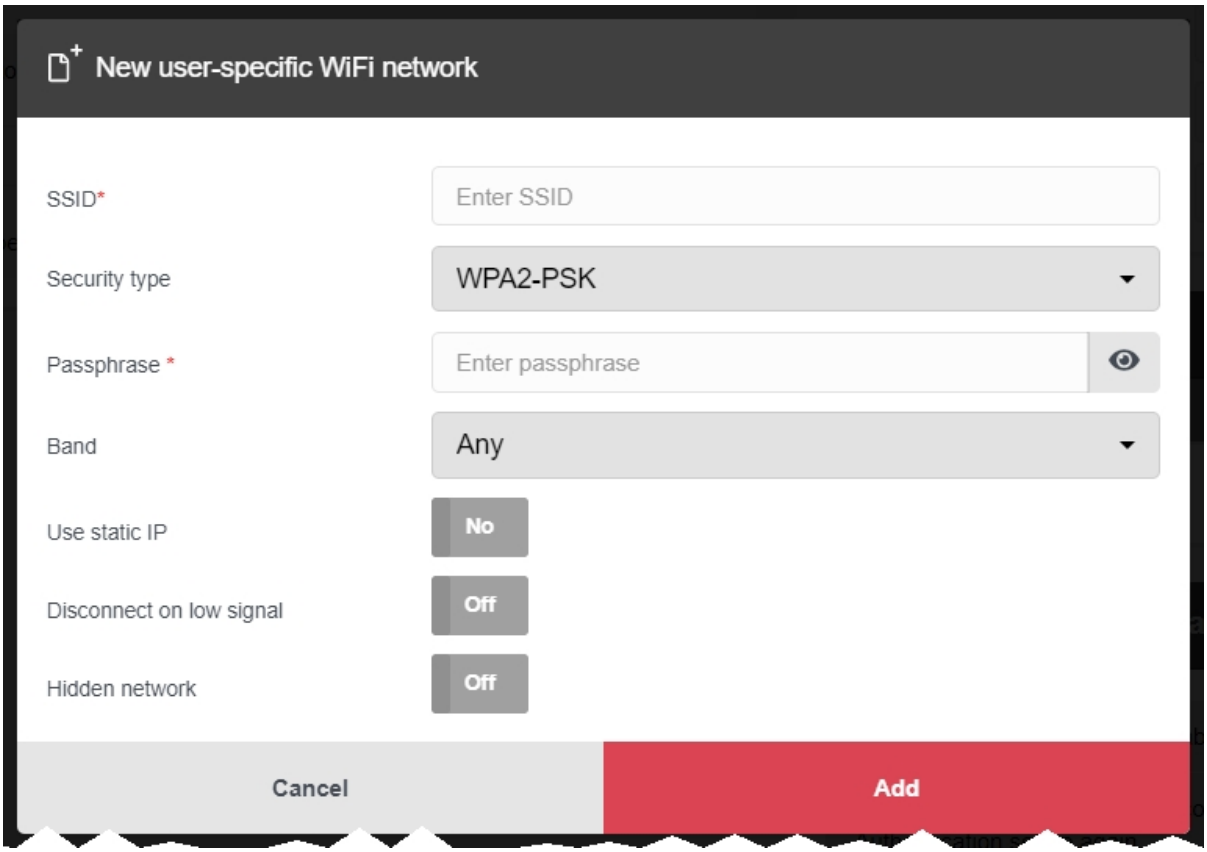
To configure a public address:

1. On VideoManager, 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 should be configured to use fixed address LAN infrastucture, and operate on a **Private** or **Domain** network, wherever possible.

11.1.3 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 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:

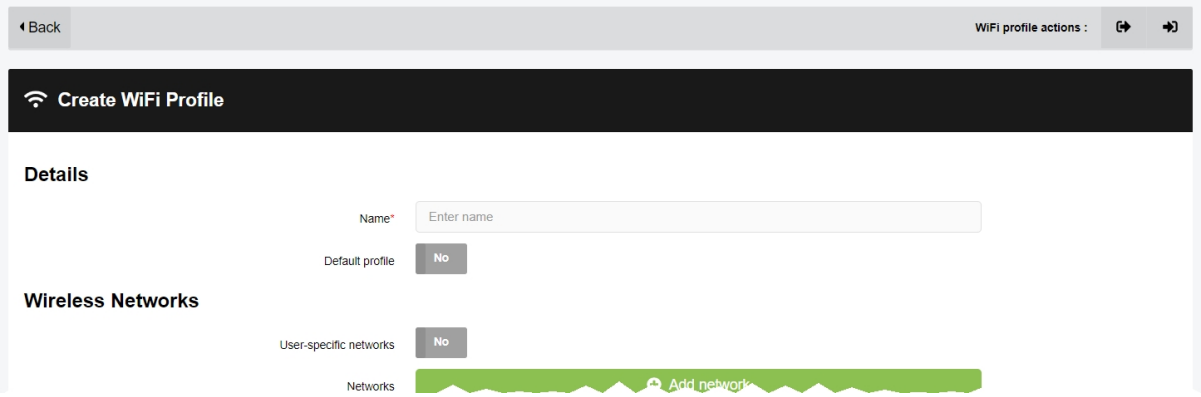
1. In the top right-hand corner of VideoManager, click the icon.
2. Select **Account Profile** from the dropdown.
3. In the ***User-specific WiFi networks*** pane, click ***Add network***.
4. In the ***Network name (SSID)*** field, enter the name of the WiFi network or hotspot.

   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.

11.1.4 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***.
   - 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***.

     >> For more information, see Create User-Specific WiFi Networks on page 367

   - 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.

   >> For more information, see Create WiFi Profiles and Perform WiFi Profile Actions on page 221

   - 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***.

11.1.5 Assign a Body-Worn Camera for Streaming

Users can now operate a body-worn camera and live stream the footage back to VideoManager.

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***.

>> For more information, see Search Body-Worn Cameras on page 122

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

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

The ***Assign Device*** dialogue opens.

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.

>> For more information, see Create, Edit, Copy, Import, Export and Delete Roles on page 182

6. Select which ***Assignment mode*** the body-worn camera will use.

>> For more information, see Assign Body-Worn Cameras and Record Footage on page 110

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 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**.*

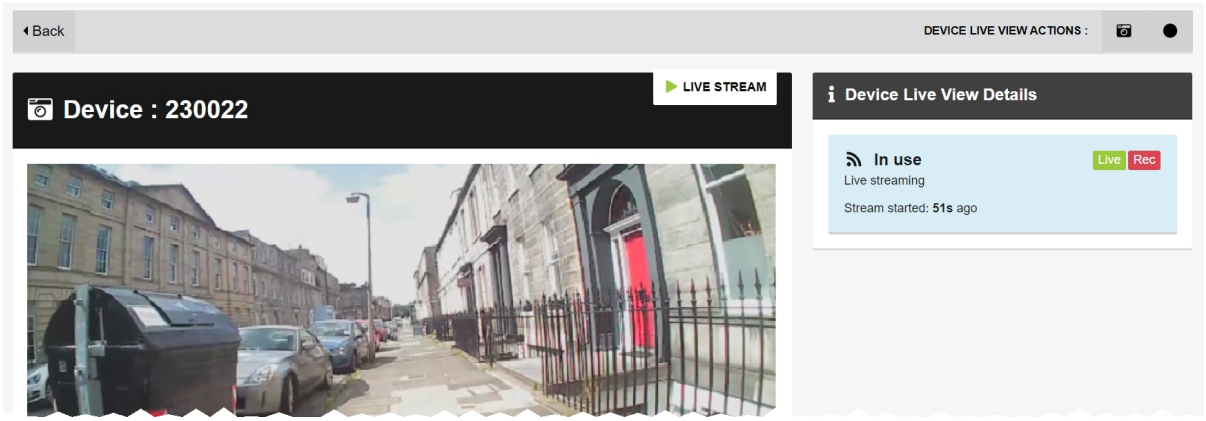
If **Single issue** or **Permanent issue** have been chosen, the user must do the following:

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.

11.1.6 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.

> Caution: *Only users with the permission to view body-worn cameras live can see live streams. 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***.

11.2 Configure Sites

A Central VideoManager acts as a "hub" for other instances of VideoManager to connect to. These other instances of VideoManager act as sites, and can be accessed through the Central VideoManager.

It is highly recommended that these computers are running the same version of VideoManager - there may be problems syncing the configuration otherwise. If the versions of VideoManager are not the same, the computer with the more recent version must act as the Central VideoManager. Check release notes for which versions of VideoManager are compatible.

The steps for configuring a Central VideoManager are as follows:

1. Enable and configure Central VideoManager.

>> For more information, see Enable and Configure a Central VideoManager on page 376

2. Configure how footage on sites is treated (i.e. whether it is automatically uploaded to the Central VideoManager or not).

>> For more information, see Configure Metadata/Footage Replication on page 377

3. Configure how other information on sites is treated (i.e. whether it is automatically replicated from the Central VideoManager to the sites or not).

>> For more information, see Enable Configuration Replication on page 379

Once the Central VideoManager has been configured, sites can be connected to it. The steps for configuring a site differ, depending on the type of site to be used.

If the administrator will be connecting another instance of VideoManager to the Central VideoManager:

1. Create site profiles from the Central VideoManager.

These profiles will map the sites onto the Central VideoManager.

>> For more information, see Create Sites on the Central VideoManager on page 381

2. Enable and configure sites.

>> For more information, see Enable and Configure Sites on page 383

If the administrator will be connecting an EdgeController to the Central VideoManager:

1. Enable and configure sites.

>> For more information, see Configure EdgeControllers on page 384

Once an EdgeController has been configured to act as a site, it can be administered over WiFi.

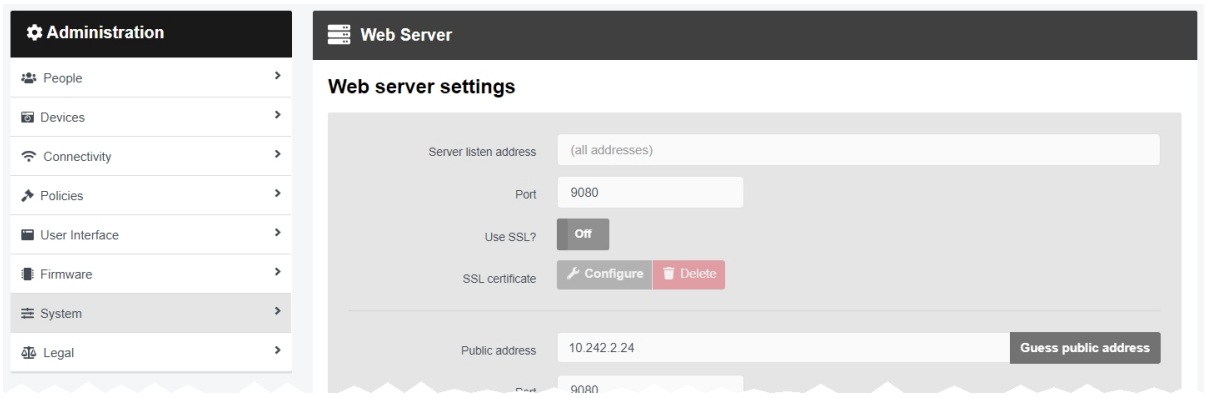
>> For more information, see on page 388

Some configurations require a Three-tier site setup. Motorola Solutions should be contacted first.

>> For more information, see Configure Three-tier Sites on page 389

11.2.1 Enable and Configure a Central VideoManager

A Central VideoManager acts as a "hub", to which other sites can connect.



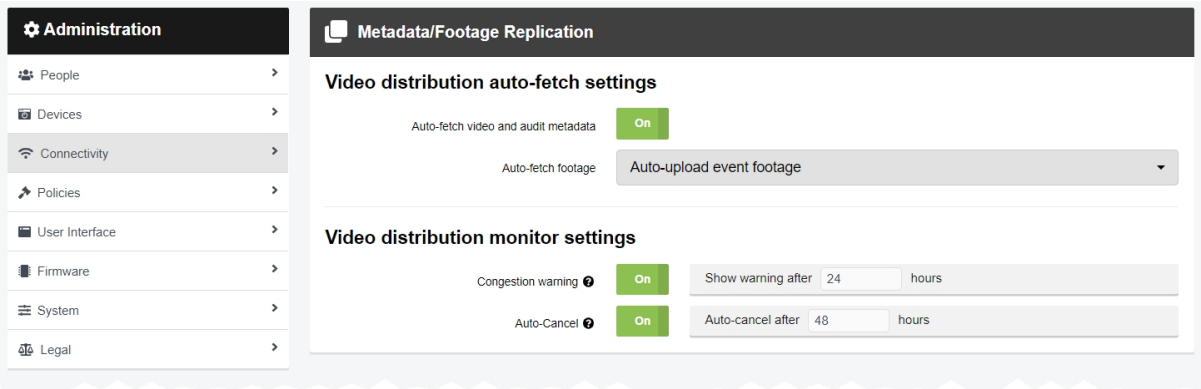
To enable Central VideoManager on a user's instance of VideoManager:

1. Navigate to the ***Admin*** tab.
2. Select the ***System*** pane.
3. Click the ***Web Server*** section.
4. Set ***Central VideoManager mode*** to ***On***.
5. Click ***Save settings***.

The instance of VideoManager is now acting as a Central VideoManager, and sites can be added to it.

11.2.2 Configure Metadata/Footage Replication

It is possible to automatically upload videos from a site to a Central VideoManager, as well as its metadata. In a Central VideoManager, these settings can be controlled from the ***Metadata/Footage Replication*** section of the ***Connectivity*** pane in the ***Admin*** tab. The ***Metadata/Footage Replication*** section is only visible from a Central VideoManager - if VideoManager is configured as a site, it is not visible.



Users might want to automatically share videos with a Central VideoManager because otherwise, every video would have to be manually submitted or committed from the site or Central VideoManager, respectively.

To reach the ***Metadata/Footage Replication*** section:

1. Navigate to the ***Admin*** tab.
2. Select the ***Connectivity*** pane.
3. Click the ***Metadata/Footage Replication*** section.

There are multiple categories that users can configure:

Metadata/Footage Replication - these settings control whether footage will be automatically uploaded from a site to a Central VideoManager.

- If ***Auto-fetch video and audit metadata*** is set to ***On***, all metadata for site footage will be transferred to the Central VideoManager. This metadata will be displayed in the the Central VideoManager.
- From the ***Auto-fetch footage*** dropdown, select how footage is uploaded from a site to a Central VideoManager.The options are as follows:
  - **Don't auto-upload footage** - no footage from a site will be uploaded automatically. This is useful if the user's Central VideoManager does not have a lot of storage.
  - **Auto-upload incident footage** - only footage that is part of an incident will be uploaded automatically (this includes the entire video if the footage has been clipped for the incident), as soon as the incident has been created.
  - **Auto-upload footage from committed incidents** - only footage that is part of an incident when has been **manually** taken control of will be uploaded automatically.

>> For more information, see Commit Incidents on page 98

- **Auto-upload all footage** - all footage on the site will be uploaded automatically, regardless of whether it is in an incident or not. This is only recommended if the user's Central VideoManager has a lot of storage.

>> For more information, see Create Sites on the Central VideoManager on page 381

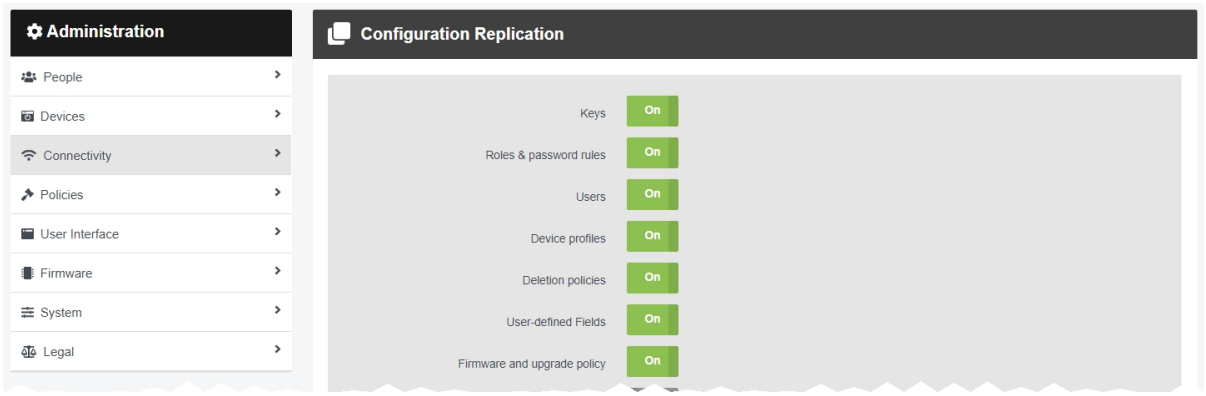
Video distribution monitor settings - these settings control how footage is uploaded from sites to the Central VideoManager.

- If ***Congestion warning*** is set to ***On***, VideoManager will display a warning if a video takes more than a defined amount of time to upload from a site to the Central VideoManager. The actual length of time, after which the warning will be shown, can be configured once it has been set to ***On***.
- If ***Auto-Cancel*** is set to ***On***, VideoManager will automatically cancel an upload if it takes more than a configurable time to upload from a site to the Central VideoManager. The actual length of time, after which the upload will be canceled, can be configured once it has been set to ***On***.

Click ***Save settings***.

11.2.3 Enable Configuration Replication

It is possible to share the configuration of a Central VideoManager with all the sites that connect to it. In a Central VideoManager, these settings can be controlled from the ***Configuration Replication*** section of the ***Connectivity*** pane in the ***Admin*** tab. The ***Configuration Replication*** section is only visible from a Central VideoManager - if VideoManager is configured as a site, it is not visible.



Users might want to share a Central VideoManager's configuration with all of its connected sites because it will allow for the automatic replication of a variety of settings - instead of manually creating roles and password rules, users can configure their Central VideoManager to automatically send this information to the sites. This also means that administrators do not need to manually export individual device profiles and user-defined incident fields. To do so:

1. Navigate to the ***Admin*** tab.
2. Select the ***Connectivity*** pane.
3. Click the ***Configuration Replication*** section.
4. Configure the following settings:

   - If ***Keys*** is set to ***On***, the Central VideoManager will share access control keys with its sites, enabling body-worn cameras assigned at one site to be docked at any other, if necessary.

   This will also replicate VideoManager's filesigning configuration, including certificate authorities: this means that all videos which can be verified by the Central VideoManager can also be verified at the sites.

   *For security reasons, the private key is **not** replicated to sites.*

   - If ***Roles &password rules*** is set to ***On***, the Central VideoManager will share all roles with its sites, enabling users to inhabit the same roles across all devices in an organisation.
   - If ***Users*** is set to ***On***, all users will be shared across sites. This means that if a user can log in to a Central VideoManager, they can also log in to the corresponding site.

It is best practice to share both ***Roles &password rules*** and ***Users***, or neither.

- If ***Device profiles*** is set to ***On***, the Central VideoManager will share device profiles with its sites.
- If ***Deletion policies*** is set to ***On***, the Central VideoManager will share its deletion policy with its sites.
- If ***User-defined Fields*** is set to ***On***, the Central VideoManager will share user-defined incident fields with its sites.
- If ***Firmware and upgrade policy*** is set to ***On***, the Central VideoManager will synchronise the firmware and upgrade policies configured from the Firmware Settings pane.
- If ***Synchronise Clocks*** is set to ***On***, all EdgeControllers which are not connected to the internet will be synchronised with the Central VideoManager clock.

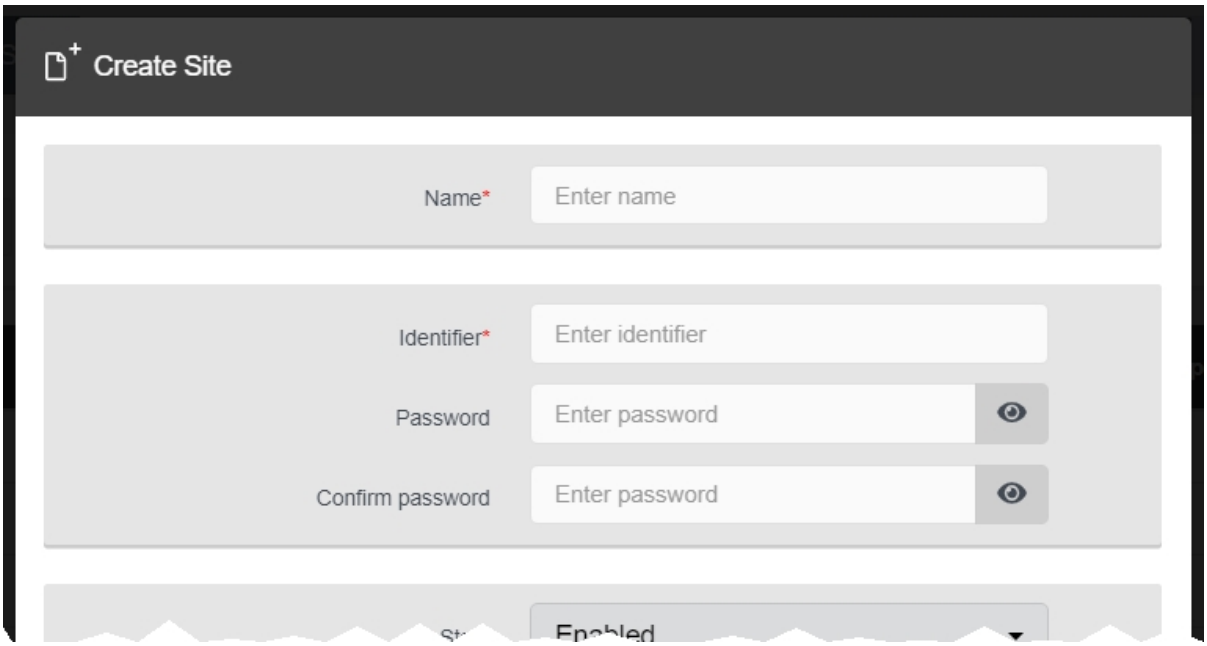
Users with sufficient permissions can still make changes to these settings on their site (e.g. changing the default device profile). However, as soon as the relevant setting is changed in the Central VideoManager, any changes made on the site will be overwritten.

5. Click ***Save settings***.

11.2.4 Create Sites on the Central VideoManager

Administrators should create site profiles **from the Central VideoManager** before connecting any sites. This is only necessary if the sites are instances of VideoManager, **not** EdgeControllers.

Site profiles map the sites themselves onto the Central VideoManager.



To create sites on the Central VideoManager:

1. Navigate to the ***Status*** tab.
2. Select the ***Sites*** pane.

This pane will not be visible unless the administrator has already enabled this instance of VideoManager to act as a Central VideoManager.

>> *For more information, see* Enable and Configure a Central VideoManager on page 376

3. Click ***Create site***.
4. In the ***Name*** field, enter the site's display name.

This will help administrators differentiate between different sites, and can be changed later.

5. In the ***Identifier*** field, enter a unique name for the site. This cannot be changed later.
6. In the ***Password*** field, enter a password for the site.

Make a note of the ***Identifier*** and ***Password*** - these will be needed for authentication when connecting the sites to the Central VideoManager.

7. From the ***State*** dropdown, select the state of the site. The options are as follows:

   - **Enabled** - if a site is enabled, it will function as normal. It can be configured from the Central VideoManager and will automatically upload footage and incidents.
   - **Disabled** - if a site is disabled, it will not transfer footage and incidents to the Central VideoManager. Likewise, any settings which have been configured from the Central VideoManager's ***Metadata/Footage Replication*** and ***Configuration Replication*** panes will not apply until the site's state has been changed to **Enabled**.

   A site whose state has been set to **Disabled** *can still be accessed like a normal instance of VideoManager. However, if the site is not connected to the Central VideoManager* ***within two weeks****, its licences will expire.*

8. From the ***Auto-fetch footage*** dropdown, select what will happen to footage uploaded to this site. Although the default has already been configured from the ***Configuration Replication*** section, it can be overridden for the specific site here. The options are as follows:

   - **Don't auto-upload footage** - footage will not automatically be sent from the site to the Central VideoManager.
   - **Auto-upload incident footage** - footage will only be automatically sent to the Central VideoManager if it is part of an incident.
   - **Auto-upload all footage** - all footage will be automatically sent to the Central VideoManager, regardless of whether it is part of an incident or not.
   - **Default {0}** - this will be the default auto-fetch setting, as configured from the ***Configuration Replication*** section.

   >> For more information, see Enable Configuration Replication on page 379

   - **Auto-upload footage from committed incidents** - footage will only be automatically sent to the Central VideoManager if it is part of an incident which has been committed (i.e. pulled from the site to the Central VideoManager).

9. From the ***Bandwidth rule*** dropdown, select which previously-created bandwidth rule will apply to this site. If no bandwidth rules have been created, the administrator must select **No Restriction**.

   Bandwidth rules dictate when footage is uploaded from sites to the Central VideoManager, and also how much is uploaded at once. A lower bandwidth means that footage and metadata will be transferred more slowly, but will also be less disruptive to other users on the system.

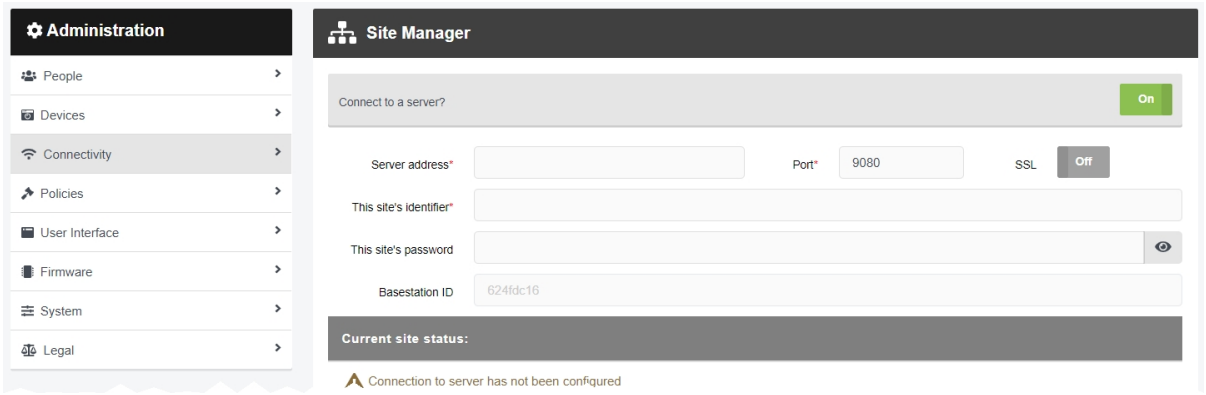
   >> For more information, see Create, Copy, Edit and Delete Bandwidth Rules on page 226

10. Click ***Create site***.

This process should be repeated for every instance of VideoManager which will become a site.

11.2.5 Enable and Configure Sites

Once site profiles have been created from the Central VideoManager, the administrator must convert the relevant instances of VideoManager into sites. This is done from the ***Site Manager*** section of the ***Connectivity*** pane, in the ***Admin*** tab.



To configure an instance of VideoManager to become a site:

1. On the instance of VideoManager which will become a site (**not** the Central VideoManager), navigate to the ***Admin*** tab.
2. Select the ***Connectivity*** pane.
3. Click the ***Site Manager*** section.
4. Set ***Connect to a server?*** to ***On***.
5. Enter the server address and port number of the Central VideoManager.

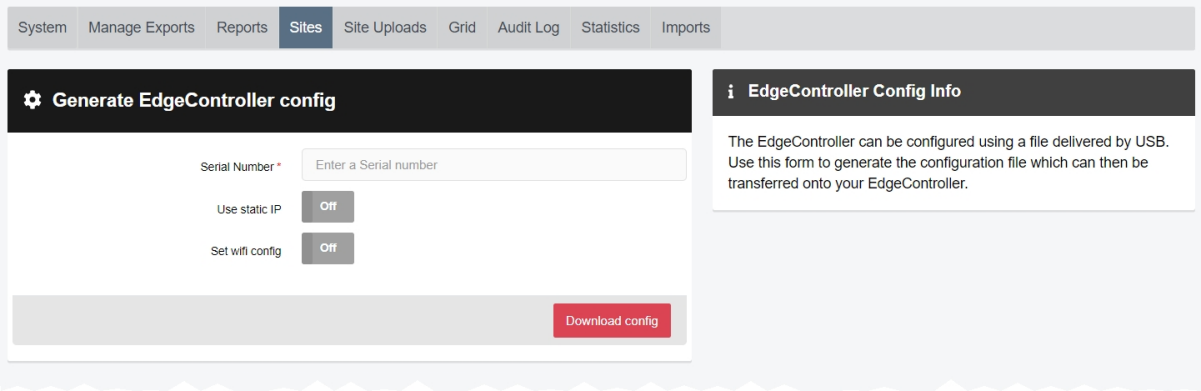
   This is found on the Central VideoManager, from the ***Web Server*** section of the ***System*** pane, in the ***Admin*** tab.
6. Enter the identifier and password of this site, which has already been created from the Central VideoManager.

   >> For more information, see Create Sites on the Central VideoManager on page 381
7. Click ***Save settings***.

If successful, the site should appear in the ***Sites*** tab of the Central VideoManager.

11.2.6 Configure EdgeControllers

Users with sufficient permissions can generate configuration files, which can in turn be used to configure an EdgeController to act as a site. In order to configure an EdgeController, it is necessary to have a USB stick and the EdgeController itself. The configuration file should be generated from the Central VideoManager.



If the EdgeController has not already been connected to mains power, it should be connected now. To do so:

1. Unpackage the EdgeController's power supply.
2. Hold the power supply so that the cable is on the bottom face of the charger and pointing towards the floor.
3. Slide the small plastic cover on the front face of the charging block upwards, and remove it.
4. Select the relevant plug, depending on the region, and slide it downwards into the space where the plastic cover was.
5. Plug the power supply into the mains. Plug the other end into the port on the back of the EdgeController marked **19v**.
6. Plug one end of the RJ45M Ethernet cable into the port on the back of the EdgeController marked **LAN**. Plug the other end into the router.
7. Turn the EdgeController on, using the ⏻ button on the top of the device.

Once the EdgeController has been connected to mains power, its configuration file can be generated on VideoManager and delivered via USB. To do so:

1. On the Central VideoManager, navigate to the ***Status*** tab.
2. Select the ***Sites*** pane.
3. Click ***Generate EdgeController config***.
4. Enter the serial number of the EdgeController in use.

   This is found on the front right-hand corner of the EdgeController.
5. It is recommended that EdgeControllers get their networking by DHCP - if this is not possible, set ***Use static IP*** to ***On***.

This is only necessary if an EdgeController cannot get its networking configuration by DHCP.

6. It is recommended that EdgeControllers are connected to networks over ethernet - if this is not possible, set ***Set WiFi config*** to ***On***.

   This is useful if the user's EdgeController will be connecting to VideoManager via WiFi. Users should enter the WiFi network's SSID and passphrase.

7. Click ***Download config*** to create the file.

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

8. Plug the USB drive into the same PC.

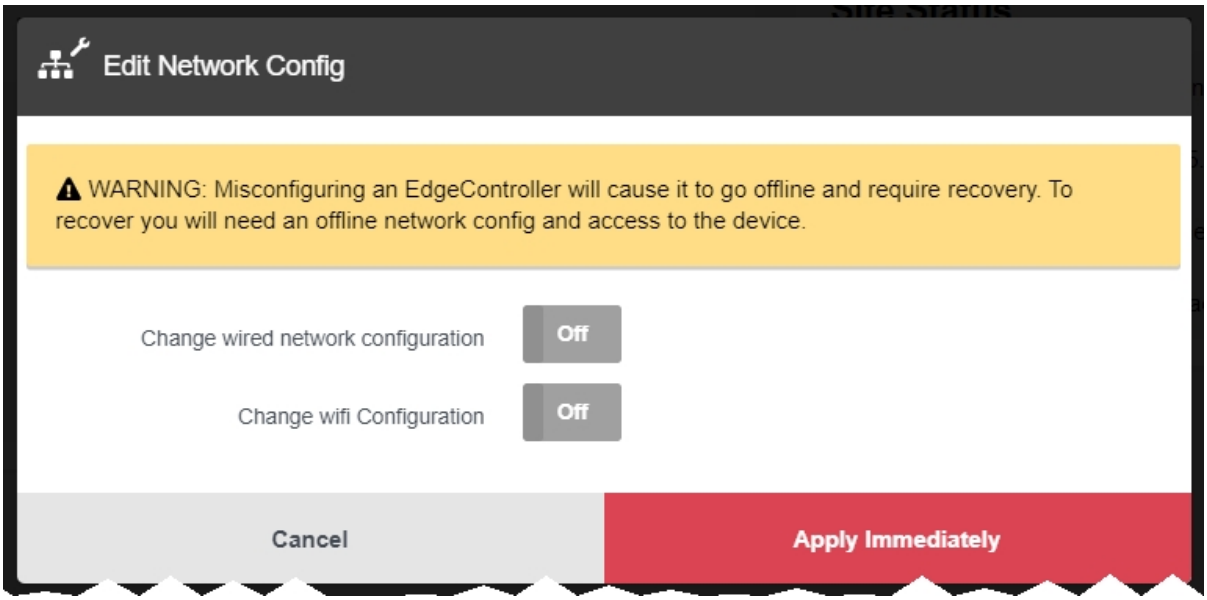
   The USB drive must have **FAT32 format**.

9. Drag and drop the EdgeController configuration file into the root folder of the USB drive.
10. Safely eject the USB drive.
11. Plug the USB drive into one of the EdgeController's USB ports.

If successful, the site should appear in the ***Sites*** tab of the Central VideoManager.

11.2.6.1 Edit an EdgeController's Network Configuration

Occasionally, it may be necessary to update the manner in which an EdgeController connects to a Central VideoManager - for example, if the administrator's WiFi network has changed, or if the EdgeController should be moved from a WiFi network to Ethernet.



To access the relevant EdgeController:

1. On the Central VideoManager, navigate to the ***Status*** tab.
2. Select the ***Sites*** pane.
3. Next to the relevant EdgeController, click ➢ ***View site***.

The following steps differ, depending on the status of the EdgeController.

If the EdgeController is online:

1. Click ***Edit Network Config***.
2. If ***Change wired network configuration*** is set to ***On***, administrators can configure whether the EdgeController will have a static IP address or not.
3. If ***Change WiFi Configuration*** is set to ***On***, the following settings will appear:
   - If ***Set WiFi config*** is set to ***On***, administrators can change the details of the WiFi network to which the EdgeController is connected.

> Caution *If the details entered here are incorrect, and the EdgeController is connected to the Central VideoManager over WiFi (instead of Ethernet), the EdgeController will go offline and must be reconfigured via USB.*

- If ***Clear WiFi configuration*** is set to ***On***, the EdgeController's WiFi configuration will be cleared.

This should only be set to ***On*** if the administrator is transferring their EdgeController from a WiFi network to an Ethernet connection.

4. Click ***Apply Immediately***.

The moment this is clicked, the EdgeController's new configuration will be applied.

If the EdgeController is offline:

1. Click ***Generate Offline Network Config***.
2. If ***Change wired network configuration*** is set to ***On***, administrators can configure whether the EdgeController will have a static IP address or not.
3. If ***Change WiFi Configuration*** is set to ***On***, the following settings will appear:

   - If ***Set WiFi config*** is set to ***On***, administrators can change the details of the WiFi network to which the EdgeController is connected.

   Caution *If the details entered here are incorrect, and the EdgeController is connected to the Central VideoManager over WiFi (instead of Ethernet), the EdgeController will go offline and must be reconfigured via USB.*

   - If ***Clear WiFi configuration*** is set to ***On***, the EdgeController's WiFi configuration will be cleared.

   This should only be set to ***On*** if the user is transferring their EdgeController from a WiFi network to an Ethernet connection.

4. Click ***Download config***.

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

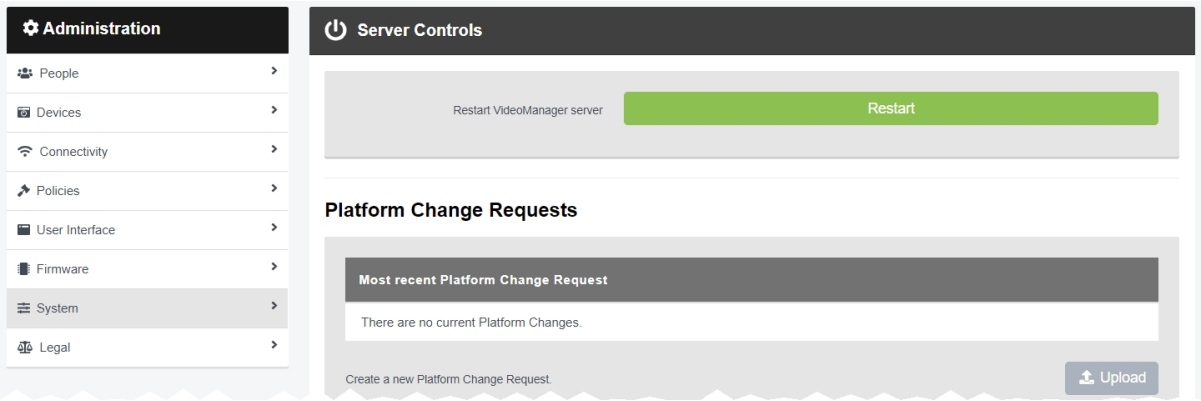
5. Plug the USB drive into the same PC.

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

6. Drag and drop the EdgeController configuration file into the root folder of the USB drive.
7. Safely eject the USB drive.
8. Plug the USB drive into one of the EdgeController's USB ports.

11.2.6.2 Perform EdgeController Platform Change Requests

Occasionally, it may be necessary to upload a configuration file directly from the EdgeController's UI, if instructed to do so by Motorola Solutions.



To upload a configuration file from an EdgeController:

1. On the Central VideoManager, navigate to the ***Status*** tab.
2. Select the ***Sites*** pane.
3. Next to the relevant EdgeController, click ***Open site web interface***.
   This will take the administrator to the EdgeController's UI.
4. On the EdgeController's UI, navigate to the ***Admin*** tab.
5. Select the ***System*** pane.
6. Click the ***Server Controls*** section.
7. In the ***Platform Change Requests*** pane, click ***Upload***.
   This action is only possible if the administrator has the ***Allow platform change requests*** permission enabled.
8. Click ***Choose File***, and select the file provided by Motorola Solutions.
9. Click ***Upload***.

11.2.7 Configure Three-tier Sites

Administrators can create a three-tier site setup. This is structured like a pyramid:

- Central VideoManager at the top.
- An instance of VideoManager acting as both a site **and** a Central VideoManager in the middle.
- Sites at the bottom.

The administrator must have at least three separate instances of VideoManager, a licence on one instance for ***Central VideoManager***, and a licence on another instance for ***Central VideoManager Middle Tier***.

The initial configuration follows the steps as previously detailed in this chapter:

1. Configure the VideoManager Mid-tier like a normal Central VideoManager.

>> For more information, see Enable and Configure a Central VideoManager on page 376

2. Configure the sites and add them to the Central VideoManager Mid-tier.

>> For more information, see Create Sites on the Central VideoManager on page 381 and Enable and Configure Sites on page 383

3. Configure the top tier Central VideoManager like a normal Central VideoManager.

>> For more information, see Enable and Configure a Central VideoManager on page 376

4. Add the VideoManager Mid-tier to the top tier Central VideoManager like a normal site, through the ***Site Manager*** section of the ***Connectivity*** pane.

>> For more information, see Enable and Configure Sites on page 383

*A normal Central VideoManager cannot connect to another Central VideoManager - this is why VideoManager Mid-tier must have a **Central VideoManager Middle Tier** licence.*

The top tier Central VideoManager can take control of incidents from both sites and VideoManager Mid-tier.

11.3 Configure Privilege Escalation

Privilege escalation is the mechanism by which administrators can ensure that there is an extra step of responsibility before important actions (e.g. incident deletion) are taken on VideoManager.

The steps to take when enabling and configuring privilege escalation are as follows:

1. Configure global settings related to privilege escalation.

>> For more information, see Configure Privilege Escalation For VideoManager on page 391

2. Configure privilege escalation on a role-by-role basis.

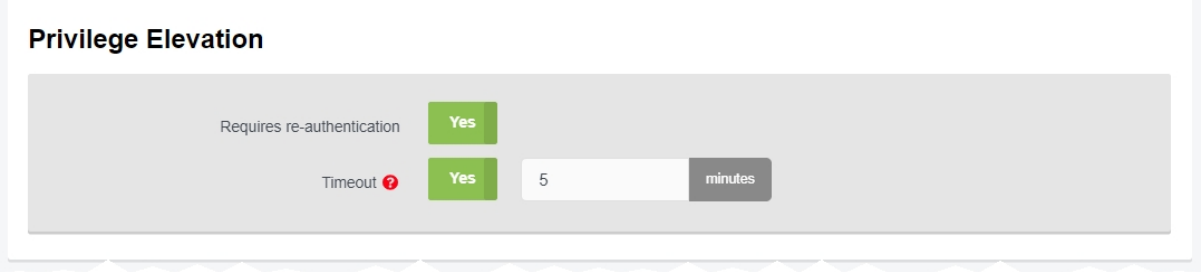
>> For more information, see Configure Privilege Escalation For Roles on page 392

3. Use privilege escalation.

>> For more information, see Use Privilege Escalation on page 393

11.3.1 Configure Privilege Escalation For VideoManager

Although privilege escalation does not need to be **enabled** for the entirety of VideoManager like two factor authentication, it should be **configured** before users have the ability to escalate their privileges.



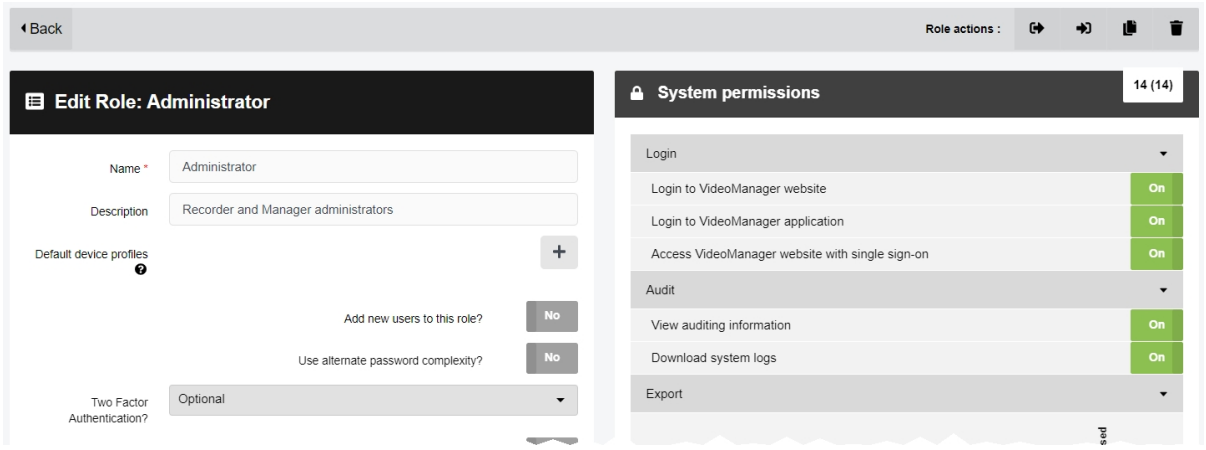
To configure privilege escalation for VideoManager:

1. Navigate to the ***Admin*** tab.
2. Select the ***User Interface*** pane.
3. Click the ***Login Settings*** section.
4. Scroll down to the ***Privilege Elevation*** section.
5. If ***Requires re-authentication*** is set to ***On***, users must re-enter their password before they can escalate their privileges.

   If set to ***Off***, users do not need to re-enter their password when escalating their privileges.
6. If ***Timeout*** is set to ***On***, the user will be automatically returned to their non-escalated role after the specified number of minutes has elapsed. If the escalated role is the user's **only** role, they must re-escalate their privilege before they can perform any actions on VideoManager.
7. Click ***Save settings***.

11.3.2 Configure Privilege Escalation For Roles

Once privilege escalation has been configured for the entirety of VideoManager, it can be configured on a per-role basis.



To enable privilege escalation:

1. Navigate to the ***Admin*** tab.
2. Select the ***People*** pane.
3. Click the ***Roles*** section.
4. Click ***Create role*** or ***Go to role***, if an already-existing role is being edited.
5. Set ***Requires privilege elevation?*** to ***Yes***.

From now on, all users with this role must manually choose to elevate this role before they can perform actions controlled by the permissions in this role.

>> For more information, see Use Privilege Escalation on page 393

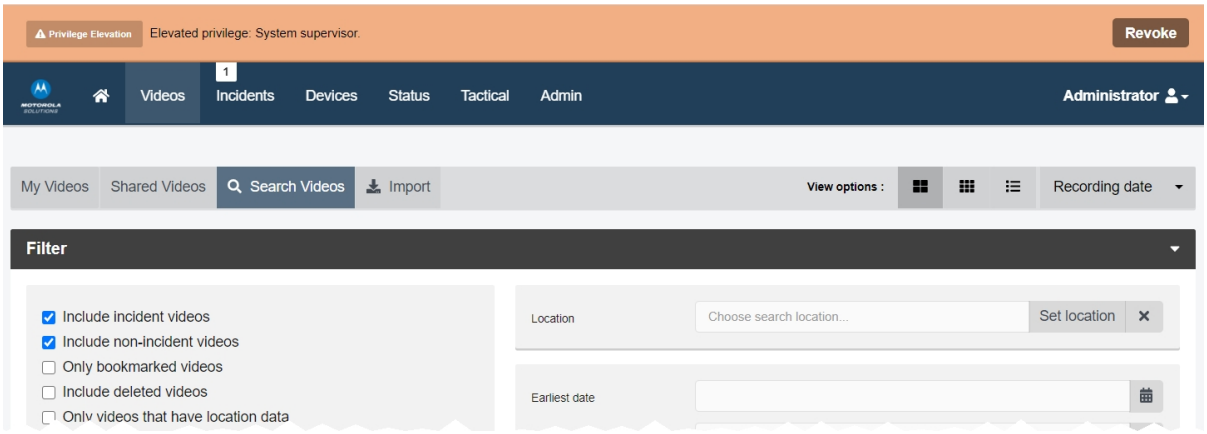
*If there are any users which **only** belong to this role, they will be unable to perform any actions on VideoManager until they have elevated their privileges.*

6. Click ***Save role***.

For any users who inhabit this role, this change will come into effect the next time they log in.

11.3.3 Use Privilege Escalation

Once privilege escalation has been configured, users can escalate their privileges on VideoManager when they wish to perform an action which would usually be unavailable to them.



To escalate privileges:

1. In the top right-hand corner of VideoManager, click the icon.
2. Click ***Elevate Privilege***.

The roles available to the user will appear as a list. The user should choose the relevant role from this list.

> *If **Elevate Privilege** is not available, the user does not inhabit a role which requires privilege escalation.*

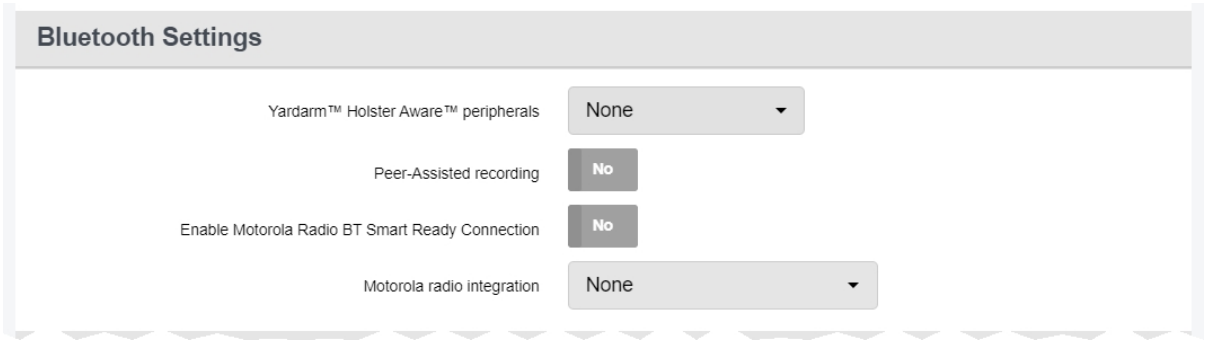
3. If ***Requires re-authentication*** has been set to ***On***, the ***Validate password*** window will open. The user must re-enter their password and click ***Validate***.

The user's privileges will be escalated. An orange banner will appear in VideoManager, which will revoke the user's privileges immediately if clicked.

11.4 Use Bluetooth with Peer-Assisted Recording (PAR)

This mode requires two or more VB400s. When one body-worn camera starts recording, any body-worn cameras in its vicinity will be prompted to start recording too.

This section is intended as a cursory insight into how administrators can configure PAR for immediate use. For more in-depth information about possible configuration options (e.g. how to use PAR with groups), please contact support@edesix.com and ask for the technical paper *Peer-Assisted Recording Explained [ED-009-056]*.



To configure peer-assisted recording with body-worn cameras:

1. Ensure that there are at least two users who have a role with the ***Operate device*** permission enabled.

   Navigate to the ***Admin*** tab, select the ***People*** pane, and click the ***Roles*** section. Click ***Go to role*** next to the relevant role, and set ***Operate device*** to ***On***.

   Navigate to the ***Admin*** tab, select the ***People*** pane, and select the ***Users*** section. Click ***Go to user*** next to the relevant user, and set the relevant role to ***On***.

2. Ensure that there is a device profile on VideoManager which has ***Peer-Assisted recording*** set to ***On***.

   Navigate to the ***Admin*** tab, select the ***Devices*** pane, and click the ***Device Profiles*** section. Click ***Go to profile*** next to the relevant device profile. In the ***Bluetooth Settings*** section, set ***Peer-Assisted recording*** to ***On***.

   If ***Suppress PAR after undocking*** is set to ***On***, the user can enter the number of seconds after assignment, during which a VB400 will **not** prompt other VB400s to start recording.

   If ***Suppress PAR after undocking*** is set to ***Off***, the VB400 will be able to prompt other VB400s to start recording as soon as it has been assigned and undocked.

3. Assign the VB400s to the users. Ensure that the previously-created device profile is chosen.

   Navigate to the ***Devices*** tab. Click ***Assign Device*** next to the relevant VB400. In the ***Operator name*** field, enter the name of the user which will operate the VB400. Select the previously created device profile from the ***Device Profile*** dropdown. Repeat this step for the other VB400.

Whenever one VB400 starts recording in the vicinity of another, the other VB400 will be prompted to start recording as well. However, it is not possible to stop multiple body-worn cameras recording with Bluetooth - users must stop recording individually and manually.

12 Frequently Asked Questions

12.1 Video FAQs

Q. After recording, how do I download videos from my body-worn camera to VideoManager?

A. To download videos 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 video should now be available to view under the ***Videos*** tab.

Q. Why are some of the headings on my videos blue?

A. If a video 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. Can I share videos with people who aren't on VideoManager?

A. If you need to share a video with someone outside of VideoManager, you can share it as part of an incident, using a link via email.

>> For more information, see "Share Incidents Externally Using a Link" on page 91

You can also download the video straight to your PC.

>> For more information, see "Perform Video Actions" on page 30

Q. What is the difference between the operator and the owner of a video?

A. The operator of a video is the one who physically recorded it on their body-worn camera. The owner has full administrative control over the video. Normally this will be the same person - however, if the footage in question is too sensitive for more junior users to retain control of, it may be necessary to reallocate who the owner is.

>> For more information, see "Share Videos and Assets" on page 41

Q. I can't see some of the videos on VideoManager. Why is this?

A. There are two possible reasons for this - permissions and deletion policies.

- ***Permissions*** - VideoManager 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 videos 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 ***Video permissions*** window.
  6. Next to the relevant permissions, set each button to ***On***.

  Remember that these permissions apply to either your videos, videos which have been shared with you, videos which have been recorded by people you supervise, or all videos on the system.

- ***Deletion Policies*** - you may want to check the configuration of your deletion policy, in case it is configured to delete footage 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 footage is kept for after it has been recorded and downloaded.

Q. Why do some of my videos have a cloud symbol instead of a thumbnail?

A. A cloud symbol indicates that a video is not available on your instance of VideoManager because:

- You are on a Central VideoManager and the video is on the site. You must fetch the video from the site before you can watch it.

>> For more information, see "Bulk Edit Videos and Assets" on page 45

- You are on a site and the video was fetched from the Central VideoManager.

This means that you can no longer watch the video on the site.

Q. I've accidentally deleted a video. Can I undo this action?

A. You can reinstate a deleted video, as long as your deletion policy has been configured to keep deleted videos 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 video:

1. Naviate to the ***Videos*** tab.
2. Select the ***Search Videos*** pane.
3. Check ***Include deleted videos***.
4. The deleted video will appear with a red heading. Click ***Reinstate video***.
5. Click ***yes***.

The video will be reinstated and can be watched like normal.

12.2 Incident FAQs

Q. What is the difference between an export link and an incident link?

A. An export link will **download** the footage directly to the recipient's PC - an incident link will only provide the recipient with browser-based access to the footage, which will be disabled after a set period of time.

>> For more information, see "Share Incidents Externally Using a Link" on page 91

Q. Why are my incident headings different colours?

A. If you have enabled your instance of VideoManager to be a Central VideoManager or site, your incidents may be different colours depending on their state.

In the Central VideoManager:

- Incidents which have been automatically made viewable to the Central VideoManager, but haven't been taken control of yet, are coloured **blue**.
- Incidents which have been deleted on the site before they were taken control of are coloured **blue** with **red** text.

If an incident has been deleted on the site, the Central VideoManager cannot take control of it.

In the site:

- Incidents which have been submitted to the Central VideoManager are coloured **green**.
- Incidents which have been deleted on the site itself are coloured **red**.

Q. Why won't VideoManager let me export an incident?

A. You cannot export an incident that does not contain any footage. Once footage has been added to an incident, you will be able to export it. You can still create incident links for incidents without footage.

>> For more information, see "Share Incidents Externally Using a Link" on page 91

Alternatively, you may not be able to export an incident if it does not meet the configured export profile rules.

>> For more information, see "Configure Incident Exports" on page 244

Q. I've accidentally deleted an incident. Can I undo this action?

A. You can reinstate a deleted incident, as long as your deletion policy has been configured to keep deleted incidents for a short period of time after deletion **and** you are in a role which has had the ***Reinstate*** permission set to ***On***. To reinstate an incident:

1. Naviate to the ***Incidents*** tab.
2. Select the ***Search Incidents*** pane.
3. Check ***Show recently deleted incidents***.
4. The deleted incident will appear with a red heading. Click ***Reinstate incident***.
5. Click ***yes***.

The incident will be reinstated and can be edited like normal.

12.3 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. Can I move my body-worn cameras from one VideoManager system to another one?

A. Yes. Before starting this process, ensure that either:

- All footage on the body-worn camera has been downloaded to the instance of VideoManager it was originally associated with - once the body-worn camera has been factory reset, all footage that wasn't downloaded already will be lost.
- You have imported the body-worn camera's access control key from the old instance of VideoManager to the new instance.

>> For more information, see "Create, Import, and Export Access Control Keys" on page 213

Furthermore, if you have enabled file signing, you should export your certificate authority. If your certificate authority is not exported, videos recorded by the moved body-worn cameras cannot be verified on the new instance of VideoManager.

>> For more information, see "Create, Import, Export, and Delete Device Certificate Authorities" on page 216

To move a body-worn camera from one instance of VideoManager to another:

1. Undock your body-worn camera from the PC or DockController associated with the old version of VideoManager.
2. Dock the body-worn camera to the PC or DockController associated with the VideoManager it should be moved to.
3. Navigate to the ***Devices*** tab, and click > ***View device info*** next to the relevant body-worn camera.

If you have not imported the body-worn camera's access control key, it will appear as **locked**. You must click ***Factory Reset this Device*** to associate the body-worn camera with the new instance of VideoManager.

Q. Why does my body-worn camera appear as "locked" on VideoManager?

A. Your body-worn camera will appear as locked if it has been undocked from one instance of VideoManager and redocked at a different VideoManager which does not have its access control key. This means that all footage 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 to the VideoManager which the body-worn camera is connected to now.

Q. My VB400 is broken. How do I prevent other operators on VideoManager 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 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 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.

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. Service may be required - check the audit log from the ***Status*** tab.

12.4 Admin FAQs

Q. Can I change my username once I've created my user?

A. You cannot change your username once you have created and saved your user. You can, however, change your ***Display name*** - this is what other users will see on VideoManager - from the ***Users*** section of the ***People*** pane, in the ***Admin*** tab.

>> For more information, see "Create, Edit, and Delete Users" on page 165

Q. Can I change my password once I've created my user?

A. Yes. You can change your password from the the ***Users*** section of the ***People*** pane, in the ***Admin*** tab. In the ***Password*** section, delete your old password and enter a new one. Re-enter it in the ***Confirm password*** field below. Clicking ***Save user*** will confirm the choice.

Alternatively, if you do not have access to the ***Admin*** tab, click the user icon in the top right-hand corner of the screen, and select **Account Profile** from the dropdown. In the ***Update password*** pane, enter your current password, enter a new password, re-enter it in the ***Confirm new password*** field, and click ***Save new password***.

Q. If I delete a user, what happens to their footage?

A. If you delete a user, none of their footage, exports, or incidents will be deleted from VideoManager.

You can reassign a user's footage, exports and incidents before or after they are deleted. This will transfer their data to another user.

If their data is not reassigned and the username is later reused for a new user, the data will be reassigned to that user automatically - even if the username does not belong to the same worker anymore.

>> For more information, see "Reassign a User" on page 170

Q. I've forgotten my password on VideoManager - how can I reset it?

A. Motorola Solutions cannot change your password for you, unless your server is hosted by us. Another administrator user must reset your password.

To do so:

1. Navigate to the ***Admin*** tab.
2. Select the ***People*** pane.
3. Click the ***Users*** section.
4. Click the ***Go to user*** button next to your user.

Here, the administrator user can change your password for you.

5. Click ***Save user***.

*If you are the **only** administrator on your system, you must contact Motorola Solutions for more information. This can be done by sending an email to support@edesix.com.*

Alternatively, if *Email Notifications* have been licenced, you can have a password reset URL sent to you.

>> For more information, see "Enable Users to Reset Their Own Passwords" on page 196

Q. What are licences?

A. Motorola Solutions sells licences, which can be used to enable functionality in VideoManager that is not otherwise available.

These licences include:

- Composite clips

This allows users to create composite clips in an incident. Composite clips show all videos in an incident simultaneously.

- Object storage

This enables users to create S3 cloud file containers.

- ONStream

Users can connect VideoManager to their VMS if ONStream is enabled.

- Text and Email notifications

Users will be given the opportunity to enter their email addresses and phone numbers. Users can configure when these notifications are sent from the ***Roles*** of the ***Admin*** tab.

Q. Is there a way to set messages that all users on VideoManager will see?

A. Yes. Navigate to the ***Admin*** tab, select the ***User Interface*** pane, and click the ***Messages*** section. You can set a message here that all users will see on their home dashboard.

>> For more information, see "Create, Edit and Delete Messages" on page 317

Q. How can I view VideoManager's legal information?

A. Navigate to the ***Admin*** tab, and click the ***Legal*** pane. By clicking ***About*** and selecting ***View***, VideoManager's licence agreement will be viewable.

Q. Why isn't two factor authentication working when I try to log in?

A. Two factor authentication codes are time-dependent - they expire after a certain period of time, and a new one is re-issued. This means that if your instance of VideoManager has a different time to that of your phone, the code will be out of sync and rendered invalid.

Q. Can I move an EdgeController from one VideoManager system to another one?

A. Due to security risks, you cannot transfer an EdgeController once it has been associated with a specific VideoManager system.

To contact Motorola Solutions for more information and advice, please send an email to support@edesix.com.

12.5 Streaming FAQs

Q. Why isn't my audio working with my live stream?

A. Due to technical limitations, Internet Explorer does not support audio with live streams. You should use another browser, like Google Chrome.

Q. Why isn't my body-worn camera streaming?

A. There are a variety of reasons that your body-worn camera might not be sending a live stream back to VideoManager:

- Ensure you have the correct WiFi profile selected. The WiFi profile must have streaming enabled.
- Try **temporarily** disabling the firewall on the machine running VideoManager. If this fixes the problem, you must turn the firewall back on and configure a firewall rule.

>> For more information, see "Configure Firewalls" on page 365

- Check whether the body-worn camera's device profile enables it to connect to WiFi automatically. It may have been configured so you need to press a button before it connects to WiFi.

>> For more information, see "VB400 Device Profile" on page 444 and "VB100/VB200/VB300 Device Profile" on page 451

- The body-worn camera doesn't have the most recent firmware. To fix this:
  1. Ensure that the body-worn camera is docked.
  2. Navigate to the ***Devices*** tab.
  3. Next to the body-worn camera, click > ***View device info***.
  4. Click ⌃⌃ ***Upgrade this Device***.
  5. Select the newest firmware and click ***Upgrade Device***.

12.6 General FAQs

Q. I can't log in to VideoManager. Why is this?

A. Users may be unable to log in to VideoManager for a variety of reasons -

- Your user has not been enabled. To fix this, an administrator must take the following actions:
  1. Navigate to the ***Admin*** tab.
  2. Select the ***People*** pane.
  3. Click the ***Users*** section.
  4. Click ***Go to user*** next to your user.
  5. Set ***Enabled*** to ***On***.
  6. Save the user.
- You have entered your credentials wrong. VideoManager is case-sensitive - usernames and passwords must be entered exactly as they were configured.
- Your user does not have the correct permissions to log in. To fix this, an administrator must take the following actions:
  1. Navigate to the ***Admin*** tab.
  2. Select the ***People*** pane.
  3. Click the ***Users*** section.
  4. Click ***Go to user*** next to your user.
  5. Check the role(s) they belong to.
  6. Click the ***Roles*** section.
  7. Next to the role to be edited, click ***Go to role***.
  8. In the ***System permissions*** section, check that all of the login permissions are set to ***On***.
  9. Click ***Save role***.

Q. I can’t see some aspects of the VideoManager user interface. Why is this?

A. There are two possible reasons for this - permissions and licensing.

- ***Permissions*** - VideoManager gives administrators lots of control over what actions can be performed by other users on the site. It does this through roles - these affect what aspects of the UI can be viewed and edited by a user. It’s possible that when you were

creating your administrator user after logging in for the first time, you didn't assign it the correct privileges. To fix this:

1. Log out of VideoManager.
2. Log back in as an administrator.
3. Navigate to the ***Admin*** tab.
4. Select the ***People*** pane.
5. Click the ***Users*** section.
6. Click ***Go to user*** next to your user.
7. Set *System Administrator* to ***On***.

You should now be able to see all videos and incidents in VideoManager, along with various other panes.

- ***Licensing*** - some aspects of VideoManager (such as ONStream) are only available to view if they've been licensed by your organisation. For more information, please contact Motorola Solutions Sales.

Q. Can I change the logos that users see on VideoManager?

A. Yes. Navigate to the ***Admin*** tab, select the ***User Interface*** pane, and click the ***Theme Resources*** section. You can download your company's logos here and use them instead.

>> For more information, see "Change and Reset Theme Resources" on page 320

Q. Can I change VideoManager's colour scheme?

A. Yes. Navigate to the ***Admin*** tab, select the ***User Interface*** pane, and click the ***Theme Resources*** section. You can change VideoManager's colour scheme here to match your own corporate branding.

>> For more information, see "Change and Reset Theme Resources" on page 320

Q. Can other users see the passwords of WiFi networks I've added to VideoManager?

A. Other users cannot see the passwords of WiFi networks you've added to VideoManager.

13 Appendices

13.1 Appendix A: Permissions

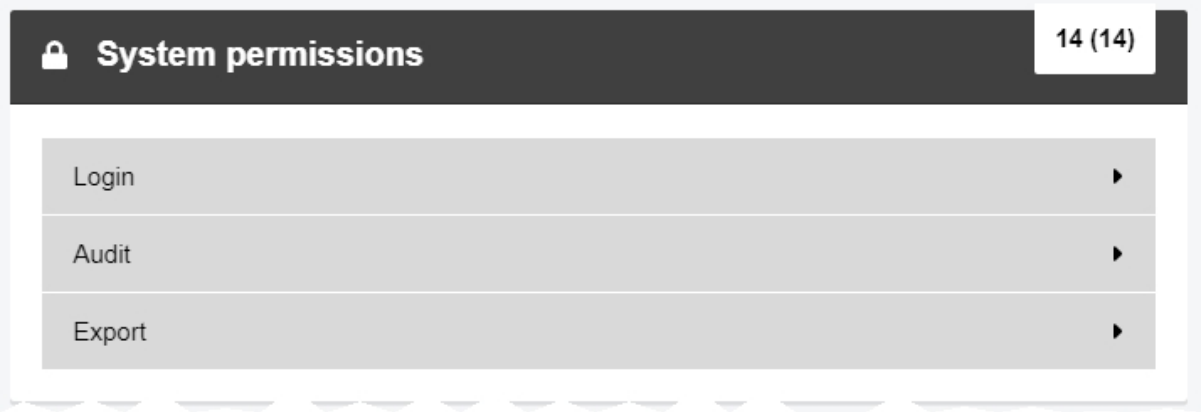
A role is a collection of permissions within VideoManager, which can then be assigned to users. Each user can have several roles assigned to them.

The groups of permissions can be viewed in the ***Roles*** section of the ***People*** pane, in the ***Admin*** tab.

If licences have been purchased from Motorola Solutions, new permissions will be available accordingly.

13.1.1 System Permissions

The ***System permissions*** section offers control over logging into the VideoManager, audit logs, and export abilities.



Login - these permissions affect the manner in which users log into VideoManager.

- ***Login to VideoManager website*** - this permission enables users to log into the VideoManager web interface.
- ***Log in to VideoManager application*** - this permission enables users to log into the desktop VideoManager administrator application. They can use the same credentials as they would use to log into VideoManager normally.
- ***Access VideoManager website with single sign-on*** - this permission enables users to authenticate into VideoManager through their desktop account. If enabled, single sign on will be available to users.

Audit - these permissions control whether users can view audit information and download the system logs.

- ***View auditing information*** - this permission enables users to view VideoManager's audit logs from the ***Status*** tab. An audit log is a list of all actions taken on VideoManager.

This does not apply to individual video audit logs. The ability to view video audit logs is dictated by the ***View audit log*** permission in the ***Video permissions*** section.

>> For more information, see Video Permissions on page 417

- ***Download system logs*** - this permission enables users to download the system logs from the dashboard.

This is useful for troubleshooting - if necessary, the system logs can be sent to Motorola Solutions support, who can diagnose the problem.

Export - these permissions control whether users can view, share, and delete exports, and view the audit log entries for exports. There are toggles accompanying each permission. They determine which exports the permissions apply to: **Owned** (exports created by the user), **Supervised** (exports that have been created by

other users on the system that the user supervises), and **Any** (any exports on the system, regardless of who created them).

- ***View/delete*** - this permission enables users to view and delete finished exports.

If enabled, users will have access to the ***My Exports*** (in accordance with the **Owned** toggle), ***Supervised Exports*** (in accordance with the **Supervised** toggle), and ***Manage Exports*** (in accordance with the **Any** toggle) panes, in the ***Incidents*** tab.

- ***View audit log*** - this permission enables users to view the audit log of all exports. These audit logs only encompass one incident each.

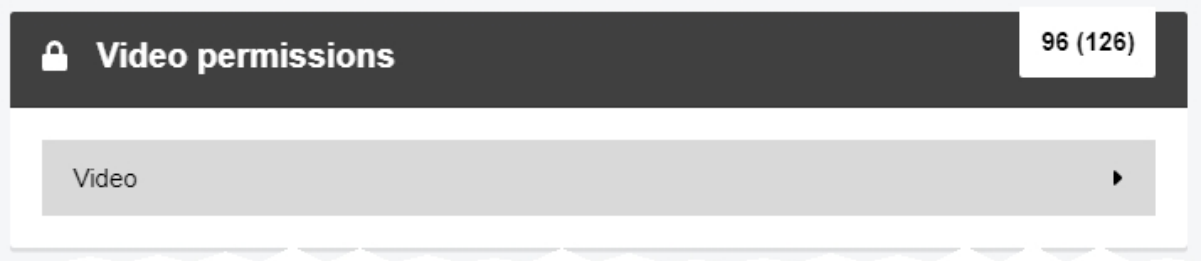
If enabled, users will have access to the ***View Export audit log*** control when viewing their exports.

- ***Externally share*** - this permission enables users to share incidents externally. This means that workers who do not have access to VideoManager can view incidents, either for a predetermined length of time, or permanently.

If enabled, users will have access to the ***Links*** pane when viewing their exports.

13.1.2 Video Permissions

The ***Video permissions*** section offers control over the various operations that can be performed on videos.



Video - there are four toggles accompanying each permission. They determine which videos the permissions apply to: **Owned** (videos created by the user), **Shared** (videos that have been shared with a user by other users on the system), **Supervised** (videos that have been created by other users on the system that the user supervises), and **Any** (any videos on the system, regardless of who created them).

- ***Access*** - this permission controls which videos users can see on the ***Videos*** tab.
- ***List*** - this permission controls whether users are presented with the ***My Videos***, ***Shared Videos***, and ***Supervised Videos*** sections in the ***Videos*** tab.

This also controls whether users can see recently imported assets and downloaded videos on their homepage.

- ***Access deleted*** - this permission enables users to search for deleted videos, by checking the **Include deleted videos** box in the ***Search Videos*** pane.
- ***Play*** - this permission enables users to play previously recorded videos on VideoManager.
- ***Delete*** - this permission enables users to delete videos from VideoManager.

Deleted videos will be retained in line with VideoManager's deletion policy. Even if users have this permission, they **cannot** delete videos which have been added to an incident.

- ***Delete forever*** - this permission enables users to permanently delete footage will immediately remove it from the system, irrespective of VideoManager's deletion policy. This will make it unrecoverable.

To permanently delete a video, the user should also have the ***List***, ***Access***, and ***Access deleted*** permissions enabled. After they have filtered incidents with the **Include deleted videos** box in the ***Search Videos*** pane, deleted footage will appear with a red banner. The user can then click ***Delete video forever*** to permanently delete the footage.

- ***Undelete*** - this permission enables the user to "undelete" previously deleted footage, as long as it has been retained in line with VideoManager's deletion policy.

To undelete a video, the user should also have the ***List***, ***Access***, and ***Access deleted*** permissions enabled. After they have filtered incidents with the **Include deleted videos** box in the ***Search Videos*** pane, deleted footage will appear with a red banner. The user can then click ***Reinstate video*** to permanently undelete the footage.

- ***Add to incident*** - this permission enables users to add videos directly to already-created incidents.

Other permissions are also required in order to use this permission - they are ***Create incident from footage***, ***Use single video as evidence***, ***Use whole recording as evidence***, and ***Add footage to existing incident***.

- ***View audit log*** - this permission enables users to view the audit log of a specific video. Logged actions include adding a video to, and removing a video from, an incident.

This does not apply to the VideoManager audit log. The ability to view the VideoManager audit log is dictated by the ***View auditing information*** permission in the ***Login*** section.

>> For more information, see System Permissions on page 415

- ***Download*** - this permission enables users to download a video from VideoManager straight to their PC.

The only way users can share videos with people who aren't on VideoManager is by downloading a video using the ***Download*** permission and either putting it on a USB stick or emailing it to the relevant people.

*Once a video has been downloaded to a PC, VideoManager has **no control** over it.*

- ***Edit share list*** - this permission enables users to edit the ***Sharing*** pane, which dictates whether the video is shared with other users on VideoManager.
- ***View share list*** - this permission enables users to view the ***Sharing*** pane, which shows whether the video is shared with other users on VideoManager.
- ***Change owner*** - this permission enables users to change the owner of a video, from the ***Sharing*** pane.

This is useful if, for instance, videos of an event were captured on multiple body-worn cameras but one user is creating and administering the incident.

- ***Restrict*** - this permission enables users to restrict a video. This makes it unviewable to other users unless they have the ***List restricted videos*** and ***Play restricted videos*** permissions enabled.
- ***Upload from site*** - this permission enables users to upload videos from a site to a Central VideoManager, if their instance of VideoManager has been configured to act as a site.
- ***Set location*** - this permission enables users to set location data for videos which do not already have location data associated with them.

This is only possible if users have already enabled maps, from the ***Maps*** section.

- ***Edit location*** - this permission enables users to overwrite location data for videos. They can only overwrite data that was set after the video was recorded - they **cannot** overwrite data that was recorded alongside a video.

This is only possible if users have already enabled maps, from the ***Maps*** section.

- ***Edit device*** - this permission enables users to change the recorded name of the body-worn camera that a video was recorded on.

This is done from the ***Edit properties*** pane.

- ***Edit operator*** - this permission enables users to change the recorded name of the user who recorded a video.

This is done from the ***Edit properties*** pane.

- ***Edit timestamps*** - this permission enables users to change the recorded time of a video.

This is done from the ***Edit properties*** pane.

- ***Edit properties*** - this permission enables users to edit the user-defined media fields for a video/asset once it has been downloaded.

This is done from the ***Edit properties*** pane.

- ***View scheduled deletion date*** - this permission enables users to view the deletion date for their video/asset from its ***Properties*** pane, based on VideoManager's deletion policy.
- ***View location*** - this permission enables the user to view location recording information associated with a video they are viewing.
- ***Rotate/Flip*** - this permission enables users to rotate and flip videos in the redaction editor.
- ***Verify*** - this permission enables users to compare a video to VideoManager's database, to ensure it has not been corrupted.
- ***Prepare media*** - this permission enables users to prepare an asset in the same way that they would redact footage in an incident.

Unlike footage, assets can be prepared even if they are not part of an incident.

- ***Import videos*** - this permission enables users to import videos captured on body-worn cameras other than VB-series cameras or VT-series cameras into VideoManager.
- ***Allow large uploads from site*** - this permission enables users on a Central VideoManager to upload more than one hour of footage from a site at a time.

This applies to both multiple videos whose total length is more than one hour, and individual videos whose length is more than one hour.

- ***Bulk-edit videos*** - this permission enables users to bulk edit multiple videos at once. Actions that can be performed on multiple videos simultaneously include **Create incident** and **Delete**.

This is useful because it allows users to perform actions across many videos immediately.

- ***Search by location*** - this permission enables users to filter footage by the location recording data attached to it.

This is only possible if users have already enabled maps, from the ***Maps*** section.

- ***Search using advanced filter*** - this permission enables users to filter videos and assets with the custom predicate language.

>> For more information, see Appendix E: Custom Predicate Language on page 469

- ***Search by scheduled deletion date*** - this permission enables users to filter videos and assets based on when they are set to be deleted by VideoManager's deletion policy.
- ***Control playback quality*** - this permission enables users to change the quality of the videos they watch from the ***Videos*** tab. This will enable them to override the default quality set from the ***Player*** section of the ***User Interface*** pane, in the ***Admin*** tab.
- ***Take screenshot*** - this permission enables users to screenshot a video or asset while it is being viewed.

This screenshot will be downloaded directly to the user's PC.

- ***List restricted videos*** - this permission enables users to view restricted videos in the ***My Videos***, ***Shared Videos***, or ***Supervised Videos*** panes.
- ***Play restricted videos*** - this permission enables users to play videos which have been restricted by other users.
- ***Full control of restricted videos*** - this permission enables a user to treat a restricted video exactly as they would an unrestricted one.
- ***Display audit log of restricted videos*** - this permission enables users to view the audit log entries for restricted videos.
- ***Download restricted videos*** - this permission enables users to download a restricted video, utilising the ***Download original file*** control.

>> For more information, see Perform Video Actions on page 30

- ***Add restricted videos to incidents*** - this permission enables users to add restricted videos to an incident.
- ***Search Videos*** - this permission enables users to search for specific videos from the ***Search Videos*** pane of the ***Videos*** tab.
- ***Search By Shared Videos Only*** - this permission enables users to search for videos that have been shared either by them or with them, from the ***Search Videos*** pane of the ***Videos*** tab.
- ***Create incident from footage*** - this permission enables users to create an incident from a video they are currently viewing.

- ***Create incident with bulk select*** - this permission enables users to create an incident comprising of videos chosen through bulk select.

This is useful if users want to create an incident containing a large number of videos.

- ***Use single video as evidence*** - this permission enables users to add a single video from a longer recording to an incident.

Administrators can configure how a body-worn camera will divide a long recording from its device profile. By default, if a recording is longer than 15 minutes, it will be divided into 15-minute videos upon download.

- ***Use whole recording as evidence*** - this permission enables users to add an entire recording to an incident, instead of just individual videos.
- ***Add footage to existing incident*** - this permission enables users to add videos to already-existing incidents, instead of just new incidents.
- ***Add additional footage from same operator as evidence*** - this permission enables users to add footage from the same operator to an incident, if there is already footage belonging to that operator in the incident.

VideoManager will only offer to add footage from the same operator if the videos' recording times overlap.

- ***View videos scheduled to be deleted on dashboard*** - this permission enables users to view which of their videos are set to be deleted within a certain timeframe, via their personal ***Home*** tab.
- ***View videos in large view mode*** - this permission enables users to view videos from the ***Videos*** tab in large mode if it has been set as the system default.

With this permission, users can also manually select **Large** from the ***View options*** menu. This changes the ***Videos*** tab to large mode if it has not been set as the default.

- ***View videos in gallery view mode*** - this permission enables users to view videos from the ***Videos*** tab in gallery mode if it has been set as the system default.

With this permission, users can also manually select **Gallery** from the ***View options*** menu. This changes the ***Videos*** tab to gallery mode if it has not been set as the default.

- ***View videos in list view mode*** - this permission enables users to view videos from the ***Videos*** tab in list mode if it has been set as the system default.

With this permission, users can also manually select **List** from the ***View options*** menu. This changes the ***Videos*** tab to list mode if it has not been set as the default.

13.1.3 Incident Permissions

The ***Incident permissions*** section offers control over the various operations that can be performed on incidents.

Incident - there are four toggles accompanying each permission. They determine which incidents the permissions apply to: **Owned** (incidents created by the user), **Shared** (incidents that have been shared with a user by other users on the system), **Supervised** (incidents that have been created by other users on the system that the user supervises), and **Any** (any incidents on the system, regardless of who created them).

- ***Access*** - this permission controls which incidents users can see on the ***Incidents*** tab.

*If this permission is set to **Off**, any other incident permissions in the same column will also be set to **Off**. This is because the following permissions all require access to the incident.*

- ***List*** - this permission controls whether users are presented with the ***My Incidents***, ***Shared Incidents***, and ***Supervised Incidents*** sections in the ***Incidents*** tab.

This also controls whether users can see recently edited and created incidents on their homepage.

- ***Access deleted*** - this permission enables users to search for deleted incidents, by checking the **Show recently deleted incidents** box in the ***Search Incidents*** pane.
- ***Play*** - this permission enables users to play previously recorded videos on VideoManager, as long as they are part of an incident.
- ***Duplicate*** - this permission enables users to duplicate incidents - a new incident will be created that contains the same footage, location recording, and title.
- ***Delete*** - this permission enables users to delete incidents from VideoManager.

Deleted incidents will be retained in line with VideoManager's deletion policy.

- ***Reinstate*** - this permission enables the user to "undelete" previously deleted incidents, as long as they have been retained in line with VideoManager's deletion policy.

To reinstate an incident, the user should also have the ***List***, ***Access***, and ***Access deleted*** permissions enabled. After they have filtered incidents with the **Show recently deleted incidents**

box in the ***Search Incidents*** pane, deleted incidents will appear with a red banner. The user can then click ***Reinstate incident*** next to the relevant incident.

- ***Add to incident collection*** - this permission enables users to add an incident to an incident collection, as long as they have the *Nested Incidents* licence as well.

This permission controls **which incidents** users can add to incident collections. This permission must be used in tandem with the ***Create incident collection*** and ***Add incident to existing incident collection*** permissions to actually create incident collections.

- ***Edit*** - this permission enables users to edit the incidents they have access to.

It is only possible to enable this permission if the corresponding ***Access*** permission has been enabled as well.

- ***Export*** - this permission enables users to create exports. Exports, along with incident links, let users share incidents with people who are not already on VideoManager.

Even if a user does not have this permission, automatic exports will still be created if they are enabled.

Caution *Once an incident has been exported, VideoManager has **no control** over it.*

- ***View audit log*** - this permission enables users to view the audit log of incidents they can already access.
- ***Edit share list*** - this permission enables users to edit the ***Sharing*** pane, which dictates whether the incident is shared with other users on VideoManager.
- ***View share list*** - this permission enables users to view the ***Sharing*** pane, which shows whether the incident is shared with other users on VideoManager.
- ***Externally share*** - this permission enables users to create incident links. Incident links, along with exports, let users share incidents with people who are not already on VideoManager.

Incident links only offer access to the incident for a limited time. Once the link expires, people outside VideoManager will not have access to the incident anymore.

- ***Change owner*** - this permission enables users to change the owner of an incident, from the ***Sharing*** pane.

This is useful if the user who created an incident should not own it anymore.

- ***Submit*** - this permission enables users to upload incidents from a site to a Central VideoManager, if their instance of VideoManager has been configured to act as a site.

This is useful if, due to bandwidth limitations, users cannot automatically upload incidents to a Central VideoManager using Metadata/Footage Replication. Instead, users can manually choose to upload incidents from their site.

- ***Take control*** - this permission enables users to upload incidents from a site to a Central VideoManager, if their instance of VideoManager has been configured to act as a Central VideoManager.

This is useful if, due to bandwidth limitations, users cannot automatically upload incidents to a Central VideoManager using Metadata/Footage Replication. Instead, users can manually choose to upload incidents to their Central VideoManager.

- ***Restrict*** - this permission enables users to restrict an incident. If an incident has been restricted, only users with the corresponding ***View any restricted incident*** permission can view it.
- ***Add attachments*** - this permission enables users to add non-video attachments to an incident, such as PDFs or JPGs.
- ***View attachments*** - this permission enables users to view any non-video attachments that have been added to an incident.
- ***Remove attachments*** - this permission enables users to delete any non-video attachments from an incident.
- ***Edit location*** - this permission enables users to edit the location data for a video that belongs to the incident they are editing.

This is only applicable for videos that were recorded without location data. Users cannot overwrite previously recorded location data - they can only edit location data that was added to the video in VideoManager.

- ***View location*** - this permission enables users to view the location data for all videos within the incident they are viewing.

If more than one video with location data has been added to an incident, the location data will be superimposed on top of each other.

- ***Commit incident to CommandCentral Vault*** - this permission enables users to commit incidents from VideoManager to CommandCentral Vault.
- ***Derestrict*** - this permission enables users to derestrict an incident. If an incident has been derestricted, all users with the corresponding ***Access*** permissions can view it.
- ***Search Incidents*** - this permission enables users to search for any incidents from the ***Search Incidents*** pane of the ***Incidents*** tab.
- ***Create incident with no footage*** - this permission enables users to create an incident without any videos in it.
- ***Create incident collection*** - this permission enables users to create incident collections containing incidents.

This permission will not be visible unless the user has the *Nested Incidents* licence.

- ***Add incident to existing incident collection*** - this permission enables users to add incidents to existing incident collections.

This permission will not be visible unless the user has the *Nested Incidents* licence.

- ***View any restricted incident*** - this permission enables users to view restricted incidents.

- ***Create incident custom link*** - this permission enables users to create custom links. Custom links, along with exports, let users share incidents with people who are not already on VideoManager.

Incident links only offer access to the incident for a limited time. Once the link expires, people outside VideoManager will not have access to the incident anymore. Unlike incident links, custom links cannot be emailed. They can only be copied.

- ***Bulk-edit incidents*** - this permission enables users to bulk edit incidents.

Users with this permission can delete a large number of incidents at once, using ***Delete***.

- ***Search by only shared incidents*** - this permission enables users to search for incidents that have been shared either with, or by, them.
- ***Search by only externally linked incidents*** - this permission enables users to search for incidents which have shared with either an incident link or custom link.

>> For more information, see Share Incidents Externally Using a Link on page 91

- ***Search using advanced filter*** - this permission enables users to search for incidents using the advanced search box and VideoManager's custom predicate language.

>> For more information, see Appendix E: Custom Predicate Language on page 469

- ***Can use saved incident search*** - this permission enables users to search for incidents with a saved search.

This is useful if there are a few repeated searches which are regularly performed.

- ***Create saved incident search*** - this permission enables users to create their own saved search.
- ***Edit saved incident search*** - this permission enables users to edit previously created saved searches.
- ***Delete saved incident search*** - this permission enables users to delete saved searches.
- ***Perform Computer Analysis*** - this permission enables users to create computer analyses.

This is an integral part of creating an assisted redaction, in which faces or bodies are redacted automatically.

- ***Use Computer Analysis*** - this permission enables users to utilise a computer anaylses on videos within an incident. Doing so will automatically redact faces or bodies.
- ***Use any export profile*** - this permission enables users to use all export profiles when creating an export, not just export profiles for whom ***Selectable*** has been set to ***On***.

Export profiles can be configured from the ***Incident Exports*** section of the ***Policies*** pane, in the ***Admin*** tab.

Incident clips - once a video has been added to an incident, it becomes an incident clip. The ***Incident clips*** permissions determine what actions users can perform on these incident clips. There are three toggles accompanying each permission. They determine what incident clips the permissions apply to: **New**, **Existing**, and **Duplicate**.

- ***Edit clip times*** - this permission enables users to edit the start/end times of a clip, using ***Edit clip start/end time***.

>> For more information, see Clip Footage in an Incident on page 58

- ***Redact clip*** - this permission enables users to perform redactions on their incident clips.

This is useful if a face or numberplate should be obscured due to GDPR reasons, or if a certain aspect of the footage should be highlighted.

>> For more information, see Redact an Incident Clip on page 59

- ***Edit clip notes*** - this permission enables users to edit the **Notes** section while editing an incident.

Here, users can enter comments about the relevant incident clip.

- ***Edit clip bookmarks*** - this permission enables users to edit an incident clip's bookmarks.

Bookmarks highlight particularly relevant parts of footage - this is useful if an incident clip is too long to be watched in full.

>> For more information, see Create, Edit and Delete Bookmarks on page 86

- ***Delete clip*** - this permission enables users to delete incident clips from an incident.

This will **not** delete the original video.

- ***Can duplicate incident video clip*** - this permission enables users to duplicate an incident clip in an incident, by clicking ***Duplicate clip***. A duplicated incident clip will retain the same redaction effects as the original incident clip.
- ***Can add new clip for recording in incident editor*** - if ***Group incident clips by recording*** has been set to ***Yes*** from the ***Incidents*** section, this permission enables users to add a complete, unredacted recording to an incident. To do so, users must click ***Add new clip for recording***.

13.1.4 Device Permissions

The ***Device permissions*** section offers control over assigning and operating body-worn cameras.

Device - there are toggles accompanying each permission. They determine which body-worn cameras the permissions apply to: **User** (body-worn cameras assigned to the user), **Supervised** (body-worn cameras assigned to users supervised by the user), and **Any** (all body-worn cameras visible to VideoManager).

- ***See devices*** - this permission enables users to see a list of body-worn cameras detected by VideoManager, from the ***Devices*** tab.
- ***View device on dashboard*** - this permission enables users to see body-worn cameras assigned to them on their personal ***Home*** tab.
- ***Operate device*** - this permission enables users to operate body-worn cameras (i.e. have body-worn cameras assigned to them, undock body-worn cameras, and record footage using the body-worn cameras).
- ***See unassigned devices*** - this permission enables users to see body-worn cameras which have not yet been assigned to users, from the ***Devices*** tab.
- ***See devices at sites*** - this permission enables users whose instance of VideoManager is configured as a Central VideoManager to view body-worn cameras which are connected to their sites.

To find these body-worn cameras, navigate to the ***Devices*** tab, select the ***Search Devices*** pane, and check **Include remote devices**. Once the user clicks ***Find devices***, body-worn cameras associated with the Central VideoManager's sites will be returned as well as body-worn cameras directly associated with the Central VideoManager.

- ***See forgotten devices*** - this permission enables users to view body-worn cameras which have been forgotten. Forgotten body-worn cameras are body-worn cameras which used to be connected to VideoManager, but have been manually removed by users because they are redundant.

To find these body-worn cameras, navigate to the ***Devices*** tab, select the ***Search Devices*** pane, and check **Include forgotten devices**. Once the user clicks ***Find devices***, body-worn cameras associated with the Central VideoManager's sites will be returned as well as body-worn cameras directly associated with the Central VideoManager.

- ***Forget devices*** - this permission enables users to "forget" body-worn cameras which were once connected to VideoManager but are now disconnected - either because they are in use, or because they have been replaced/are no longer in circulation.

To forget a body-worn camera, navigate to the ***Devices*** tab, click ***View device info*** next to the relevant body-worn camera, and click ***Forget Device*** in the top right-hand corner. Click ***yes*** to confirm.

- ***Bulk-edit devices*** - this permission enables users to bulk edit body-worn cameras.

Users with this permission can perform a variety of issues on large numbers of body-worn cameras, including ***Upgrade*** and and ***Forget***.

- ***Download device audit logs*** - this permission enables users to download the audit logs of a specific body-worn camera to their PC.

To download a body-worn camera's audit log, navigate to the ***Devices*** tab, click ***View device info*** next to the relevant body-worn camera, and click ***View device audit log*** in the top right-hand corner. Click ***Filter audit log***.

Management - these permissions control body-worn camera settings and factory resetting and updating the firmware of body-worn cameras as well as managing, viewing and deleting DockControllers.

- ***Change device custom status*** - this permission enables users to change a body-worn camera's custom status, from the ***Custom status*** field in the ***Edit device properties*** pane.
- ***Factory reset devices*** - this permission enables users to factory reset docked body-worn cameras.

When a body-worn camera is factory reset, its access control key and any footage that was not already downloaded to VideoManager will be deleted.

- ***Apply device firmware upgrades*** - this permission enables users to upgrade body-worn cameras, if new firmware has become available.
- ***Manage DockControllers*** - this permission enables users to configure, reboot and upgrade connected DockControllers.
- ***View DockControllers*** - this permission enables users to view the list of DockControllers currently visible to VideoManager from the ***Status*** pane, including their statuses (**Online**, **Offline**, and **Disabled**).
- ***Delete DockControllers*** - this permission enables users to remove DockControllers which are no longer connected to VideoManager from the ***DockControllers*** pane of the ***Devices*** tab.
- ***Bulk-edit DockControllers*** - this permission enables users to bulk edit DockControllers from the ***DockControllers*** pane of the ***Devices*** tab.

- ***Associate camera by QR code*** - this permission enables users to assign a VT-series camera with a QR code, instead of needing to dock it first.
- ***Change device name*** - this permission enables users to change a body-worn camera's name, from the ***Device name*** field in the ***Edit device properties*** pane.
- ***Change auto upgrade*** - this permission enables users to change a body-worn camera's auto-upgrade status, using the ***Auto-upgrade*** toggle in the ***Edit device properties*** pane.
- ***Change static IP*** - this permission enables users to change a body-worn camera's static IP settings, using the ***Use static IP*** toggle in the ***Edit device properties*** pane.
- ***Change touch assign*** - this permission enables users to change a body-worn camera's touch assign settings, using the ***Touch assign*** toggle in the ***Edit device properties*** pane.
- ***Set service required*** - this permission enables users to change a body-worn camera's status to ***Service Required***, using the ***Service required*** toggle in the ***Edit device properties*** pane.
- ***Clear service required*** - this permission enables users to change a body-worn camera's status from ***Service Required*** to normal, using the ***Service required*** toggle in the ***Edit device properties*** pane.

VB Companion - these permissions control what actions a user can perform when configuring or using VB Companion.

- ***Setup Companion Services App for myself*** - this permission enables users to configure VB Companion for themselves.
- ***Setup Companion Services App for supervised user*** - this permission enables users to configure VB Companion for users they supervise.
- ***Setup Companion Services App for any user*** - this permission enables users to configure VB Companion for **all** users on VideoManager.
- ***Use VB Companion*** - this permission enables users to utilise VB Companion on their mobile phones.
- ***Use VB Companion view finder*** - this permission enables users to utilise VB Companion's viewfinder function. The viewfinder function enables users to see what their body-worn camera sees and check whether their body-worn camera has been mounted correctly.
- ***Play videos in VB Companion*** - this permission enables users to watch videos in VB Companion.
- ***View/Edit VB Companion metadata*** - this permission enables users to view and edit the metadata of the videos they have recorded in the field.

- ***View system page in VB Companion*** - this permission enables users to access the ***System*** page of VB Companion. The ***System*** page displays the status of the VB400 (i.e. whether it is recording or not) and its serial number.

ONStream - these permissions control what actions a user can perform during a body-worn camera live stream.

- ***Live view via RTSP*** - this permission enables the user to view a body-worn camera's live stream, using a VMS.
- ***Live view*** - this permission enables the user to view a body-worn camera's live stream, using VideoManager.

Assignment - these permissions control the user's ability to assign body-worn cameras, both to themselves and other users on the system.

- ***Return devices*** - this permission enables users to unassign body-worn cameras detected by VideoManager.
- ***Assign device*** - this permission enables users to assign body-worn cameras visible to VideoManager. Body-worn cameras must be assigned to users before they can record footage.

>> For more information, see Assign Body-Worn Cameras and Record Footage on page 110

*This permission must be combined with either **Manually assign a device for single use**, **Manually assign a device for permanent use**, and **Manually allocate a device**.*

- ***Assign device using RFID touch assign*** - this permission enables users to assign body-worn cameras visible to VideoManager using touch assign.
- ***Assign multiple devices using RFID touch assign*** - this permission enables users to assign more than one body-worn camera to a user, using touch assign.

This may be necessary if there is one user to whom all body-worn cameras should be assigned in case of an emergency, so that many operators can undock - and use - body-worn cameras quickly. However, this also means that footage cannot be traced back to one specific operator.

- ***Assign all available devices using RFID touch assign*** - this permission enables users to make all docked body-worn cameras available for recording with touch assign.

>> For more information, see Bulk Touch Assign on page 120

- ***Select device profile when assigning*** - this permission enables users to select the device profile for the body-worn camera they are assigning. If users do not have this permission, VideoManager will use the default device profile as set in the ***Device Profiles*** section of the ***Devices*** pane, in the ***Admin*** tab, or the device profile which has been assigned to the user's role.

- ***Pre-assign device*** - this will allow users to pre-assign a body-worn camera before it has even been docked to VideoManager.

This is useful if a remote worker is being sent a new body-worn camera, but they don't have access to their site's UI. Pre-assign allows the system administrator to assign the body-worn camera from the site's UI so it is ready to use when it arrives at the remote worker's home.

- ***Find and collect allocated device using RFID touch assign*** - this permission enables users to collect a body-worn camera assigned to them using touch assign.
- ***Allocate new device using RFID touch assign*** - this permission enables users without an assigned body-worn camera to permanently assign themselves a body-worn camera from the pool using touch assign.
- ***Manually assign a device for single use*** - this permission enables users to assign a body-worn camera to a user for one trip.

This means that once the body-worn camera has been redocked, it will be unassigned and returned to the pool.

If users wish to enable this permission, they must also enable ***Assign device***.

- ***Manually assign a device for permanent use*** - this permission enables users to assign a body-worn camera to a user permanently, until it is manually unassigned.

This means that once the body-worn camera has been redocked, it will remain assigned to the same user.

If users wish to enable this permission, they must also enable ***Assign device***.

- ***Manually allocate a device*** - this permission enables users to assign a body-worn camera to a user permanently, until it is manually unassigned. The user must undock the body-worn camera using touch assign.

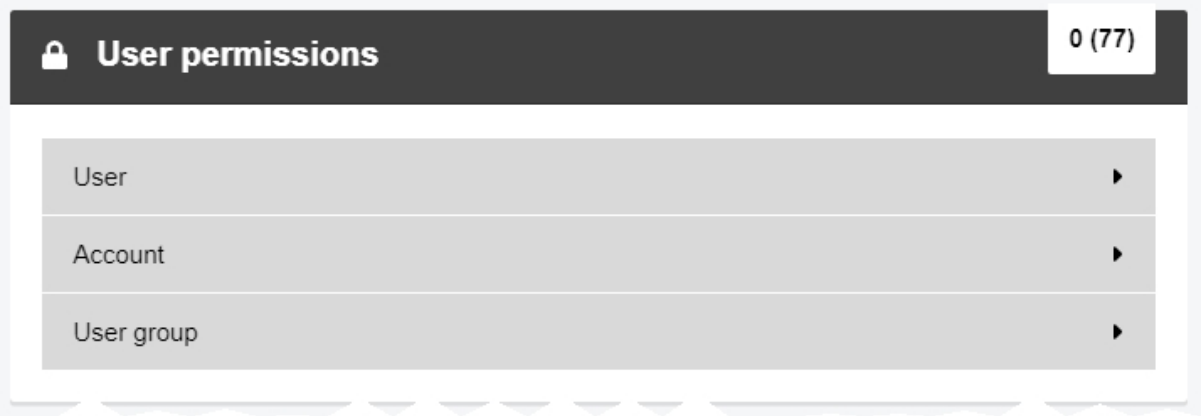
This means that once the body-worn camera has been redocked, it will remain assigned to the same user. If users wish to enable this permission, they must also enable ***Assign device***.

- ***Force unassign*** - this permission enables users to unassign a body worn cameras while it is in the field, from the ***Edit device properties*** pane.

This will not unassign the body-worn camera while the operator is still using it - instead, as soon as the body-worn camera is redocked, it will become unassigned (even if it was originally assigned with permanent issue).

13.1.5 User Permissions

The ***User permissions*** section offers control over what power a user has to change the information of **other** users and groups on the system.



User - these permissions control the user's ability to create, edit and delete other users on VideoManager.

- ***View*** - this permission enables users to view other user's profiles.
- ***Delete*** - this permission enables users to delete other users.
- ***Change touch assign*** - this permission enables users to edit the touch assign value for other users on the system. If this permission is not enabled, a user can still see the ***Touch Assign ID*** field from the ***Edit User*** pane, but cannot change the values within it.
- ***Enable*** - this permission enables users to enable other users. When a user is enabled, they can log in.
- ***Disable*** - this permission enables users to disable other users. When a user is disabled, they cannot log in.
- ***Edit display name*** - this permission enables users to change the display name of other users.
- ***Force password change*** - this permission enables users to force other users to change their password next time they log in to VideoManager, via the ***User must change password*** toggle.
- ***Undo force password change*** - this permission enables users to undo the effects of the previous permission.
- ***Add user-specific WiFi networks*** - this permission enables users to create their own user-specific WiFi networks.
- ***Edit user-specific WiFi networks*** - this permission enables users to edit existing user-specific WiFi networks.
- ***Remove user-specific WiFi networks*** - this permission enables users to remove existing user-specific WiFi networks.

- ***Change password*** - this permission enables users to change the password of other users.
- ***Set password for new user*** - this permission enables a user to set the password for a new user before they log in for the first time.
- ***Edit sharing*** - this permission determines whether or not users can alter the sharing settings of other users, such as whether their footage and incidents are automatically shared with other users on the system.
- ***Edit roles*** - this permission enables users to edit what roles other users inhabit.
- ***Edit groups*** - this permission enables users to edit which users are supervised by groups.
- ***Edit external app config*** - this permission enables users to configure how VB-series cameras interact with the VideoBadge View app.
- ***Create*** - this permission enables users to create other users.
- ***Clear Two Factor Authentication*** - this gives a user the ability to clear the two factor authentication key for another user, from the ***Edit Role*** pane.

This is useful if a user has lost the phone on which their two factor authentication code is configured, because they will be locked out of VideoManager until the key is reset.

- ***Edit user email*** - this permission enables a user to edit the email address of either users they supervise or all users on the system. This permission will only be viewable if email notifications have been licensed from Motorola Solutions.
- ***Edit user mobile*** - this permission enables a user to edit the phone number of either users they supervise or all users on the system. This permission will only be viewable if SMS notifications have been licensed from Motorola Solutions.
- ***Test user email*** - this permission enables a user to send a test email to either users they supervise or all users on the system. This permission will only be viewable if email notifications have been licensed from Motorola Solutions.
- ***Test user mobile*** - this permission enables a user to send a test SMS to either users they supervise or all users on the system. This permission will only be viewable if SMS notifications have been licensed from Motorola Solutions.
- ***View permission report*** - this permission enables users to view a user's effective permissions, utilising the ***View effective permissions*** control.
- ***View Bluetooth pairing*** - this permission enables users to view body-worn cameras which have been paired to a specific user, utilising the ***View device Bluetooth pairings*** control.
- ***Remove Bluetooth pairing*** - this permission enables users to remove Bluetooth Peripherals and other Bluetooth body-worn cameras from users, utilising the ***Remove pairing*** control.
- ***View device affinity*** - this permission enables users to view the device affinities for other users.

- ***Clear user device affinity*** - this permission enables users to clear the device affinities for other users.

>> For more information, see View and Clear Device Affinities for a User on page 174

- ***Reassign user*** - this permission enables users to reassign a user. This will transfer the ownership of **all** incidents, videos, and exports from one user to another. Incidents and videos shared with the first user will now be shared with the second user instead.

This is useful if a user is going to be deleted, and another user should take ownership of their footage and incidents. Users can be reassigned even after they have been deleted.

- ***Assign higher privileges*** - this permission enables users to add themselves and other users to a role which has permissions that the user **does not already have**.

If this permission is set to ***Off***, the user cannot add other users to a role if the role has permissions that the user does not already have.

*Even users with the **Assign higher privileges** permission will not be able to add other users to roles which are in a higher tier than their own role.*

- ***Export users*** - this permission enables users to export VideoManager's entire user database to a CSV file.
- ***Import users*** - this permission enables users to import a user database into VideoManager, via a CSV file.

Account - these permissions control what actions a user can take on themselves, from the ***Account Profile*** pane.

- ***View user-specific WiFi networks*** - this permission enables users to view their own user-specific WiFi networks from the ***Account Profile*** pane.
- ***Edit user-specific WiFi networks*** - this permission enables users to edit their own user-specific WiFi networks from the ***Account Profile*** pane.
- ***Edit own display name*** - this permission enables users to change their own display name from the ***Account Profile*** pane.

User group - these permissions control the user's ability to create, edit and delete groups on VideoManager.

- ***View*** - this permission enables users to view the ***Groups*** section of the ***People*** pane, in the ***Admin*** tab.
- ***Delete*** - this permission enables users to delete groups.
- ***Edit display name*** - this permission enables users to change the display name of a group.

The ***Group name*** cannot be changed once it has been set, but the ***Display name*** can be changed as many times as necessary.

- ***Add user-specific WiFi networks*** - this permission enables users to add a user-specific WiFi network to a group.
- ***Edit user-specific WiFi networks*** - this permission enables users to edit a user-specific WiFi network that has been added to a group.
- ***Remove user-specific WiFi networks*** - this permission enables users to delete a user-specific WiFi network that has been added to a group.

If enabled, users will have access to the ***WiFi networks*** pane in the ***Groups*** section.

- ***Edit sharing*** - this permission enables users to configure which users or groups will have access to the group's videos and incidents.

If enabled, users will have access to the ***Sharing*** pane in the ***Groups*** section.

- ***Edit roles*** - this permission enables users to edit the roles that a group will inherit.

If enabled, users will have access to the ***Roles*** pane in the ***Groups*** section.

- ***Edit groups*** - this permission enables users to edit which groups are supervised by other groups.

If enabled, users will have access to the ***Group memberships*** pane in the ***Groups*** section.

- ***Create*** - this permission enables users to create a new group.
- ***View permission report*** - this permission enables users to view the permissions report for a group, utilising the ***View effective permissions*** control.

13.1.6 Notification Permissions

If notifications have been licensed, the ***Notification*** section controls when users receive notifications. Users can typically receive notifications either through SMS or email - this is configured from the ***Users*** section of the ***People*** pane, in the ***Admin*** tab.

Receive notifications on - these permissions control which actions performed by users on VideoManager will prompt a notification.

- ***First time login*** - this permission means that users will receive a notification when other users first log into VideoManager.
- ***Personal device stream start*** - this permission means that users will receive a notification when a body-worn camera assigned to them starts streaming.
- ***Supervised device stream start*** - this permission means that users will receive a notification when a body-worn camera assigned to users they supervise starts streaming.
- ***File storage threshold warnings*** - this permission means that users will receive a notification when VideoManager is low on storage space.

13.1.7 Report Permissions

These permissions control whether users can view aspects of VideoManager relating to reports and live statistics.

Reports - these permissions control whether users can perform actions on reports.

- ***View reports*** - this permission enables users to view reports from the ***Reports*** pane of the ***Status*** tab.
- ***Create reports*** - this permission enables users to create new reports from the ***Reports*** pane of the ***Status*** tab.

If enabled, users will have access to the ***Create New Report*** control.

If ***Create scheduled reports*** has not been enabled as well, users will not have the ability to make their reports scheduled.

- ***View scheduled reports*** - this permission enables users to view scheduled reports from the ***Reports*** pane of the ***Status*** tab.

If enabled, users will have access to the ***Scheduled Reports*** pane.

- ***Create scheduled reports*** - this permission enables users to create scheduled reports from the ***Reports*** pane of the ***Status*** tab.

If enabled, users will have access to the ***Create New Report*** control.

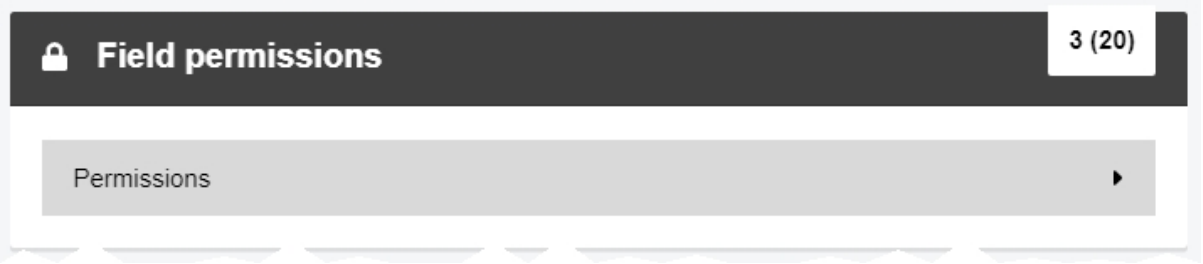
If ***Create reports*** has not been enabled as well, users will not have the ability to make a one-off report. In the ***Schedule*** dropdown, there will not be a **No** option.

Live stats - this permission dictates whether users can view the ***Statistics*** pane in the ***Status*** tab.

- ***View live stats*** - this permission enables users to view statistics related to their instance of VideoManager, from the ***Statistics*** pane.

13.1.8 Field Permissions

The ***Field permissions*** section offers control over which access groups users belong to.



There are twenty permissions - one for each access group. Access groups determine which user-defined incident fields and saved searches users can see.

13.1.9 Advanced Permissions

The ***Advanced permissions*** section offers control over access control keys, viewing sites, and changing manager settings.

Settings - the first half of these permissions control which panes of the ***Admin*** tab users can access. There is a permission for every pane in the ***Admin*** tab. By setting ***View*** to ***On***, users can view the relevant pane. By setting ***Edit*** to ***On***, users can perform actions in the relevant pane. It is not possible to have ***View*** set to ***Off*** and ***Edit*** to ***On***.

The second half of these permissions control advanced actions:

- ***Change manager settings*** - this permission enables users to view the entire ***Admin*** tab in sites which are running instances of VideoManager older than version 10.1.
- ***Export access control keys*** - this permission enables users to export access control keys from an instance of VideoManager.
- ***Delete access control keys*** - this permission enables users to delete access control keys.

If body-worn cameras on VideoManager were using the now-deleted access control key, those body-worn cameras will appear as **Locked** and any footage on them which had not yet been downloaded to VideoManager at time of deletion will be lost forever.

- ***Export file space keys*** - this permission enables users to export keys used for decrypting file spaces.
- ***Select Language for login session*** - this permission enables users to choose in which language their instance of VideoManager will be presented. The language will only apply to their personal session - when they log out, it will be reset to the default specified from the ***Language*** section of the ***User Interface*** pane, in the ***Admin*** tab.

- ***List sites connected to the Manager*** - this permission enables users on a Central VideoManager to see a list of all sites connected to it.

If enabled, users will have access to the ***Sites*** and ***Site Uploads*** panes in the ***Status*** tab.

- ***Visit sites connected to the Manager*** - this permission enables users to access a site's UI through the Central VideoManager.

If enabled, users will have access to the > ***View site*** control in the ***Sites*** pane.

- ***Edit EdgeController network configuration*** - this permission enables users to edit a previously generated EdgeController configuration.
- ***Generate EdgeController network configuration*** - this permission enables users to create an EdgeController configuration.
- ***Export device profile*** - this permission enables users to export a device profile from their instance of VideoManager.

This is useful if device profiles from a Central VideoManager are not automatically replicated to their sites due to bandwidth issues - instead, users can manually export the relevant profiles and, if ***Import device profile*** has also been enabled, import the profiles into their sites.

- ***Import device profile*** - this permission enables users to import a device profile into their instance of VideoManager.

This is useful if device profiles from a Central VideoManager are not automatically replicated to their sites due to bandwidth issues - instead, if ***Export device profile*** has also been enabled, users can manually export the relevant profiles and import the profiles into their site.

- ***Export wifi profile*** - this permission enables users to export a WiFi profile from their instance of VideoManager.

*Doing this will also export the **passwords** associated with the WiFi networks within the WiFi profile.*

- ***Import wifi profile*** - this permission enables users to import a WiFi profile from their instance of VideoManager.
- ***Export self service settings*** - this permission enables users to export a previously-created user self-service configuration, from the ***User Self Service*** section of the ***People*** pane, in the ***Admin*** tab.
- ***Import self service settings*** - this permission enables users to import a previously-created user self-service configuration, from the ***User Self Service*** section of the ***People*** pane, in the ***Admin*** tab.
- ***Restart the server*** - this permission enables users to restart their VideoManager server.

There are many instances where this might be necessary - for instance, if a new licence has been downloaded, if VideoManager's public address has changed, etc.

- ***View system status*** - this permission enables users to view the status of their system from the ***Status*** tab.

If there are any system warnings, they will be viewable here.

- ***Export database*** - this permission enables users to export VideoManager's entire database.
- ***Allow platform change requests*** - this permission enables users to change EdgeController configurations from the EdgeController itself over WiFi, instead of needing to deliver the configuration physically by USB.
- ***View grid status*** - this permission enables users to view the status of their grids, if grids are being used.

If enabled, users will have access to the ***Grid*** pane in the ***Status*** tab.

- ***View UI configuration tab*** - this permission enables users to view the **UI Configuration** tab in the VideoManager administrator application.
- ***View UI login mode tab*** - this permission enables users to view the **UI Login Mode** tab in the VideoManager administrator application.
- ***View about legal page*** - this permission enables users to view the ***Legal*** pane in the ***Admin*** tab.

This pane gives users insight into VideoManager's terms and conditions.

- ***Export import profiles*** - this permission enables users to export their import profile from an instance of VideoManager.
- ***Import import profiles*** - this permission enables users to import their import profile into their instance of VideoManager.
- ***Import system config*** - this permission enables users to import a new system config for VideoManager, from the ***Import/Export System Config*** section of the ***System*** pane in the ***Admin*** tab.
- ***Export system config*** - this permission enables users to export the entire VideoManager system config, from the ***Import/Export System Config*** section of the ***System*** pane in the ***Admin*** tab.

Accessibility - these permissions control printing and copying text from the web interface.

- ***Print from website*** - if enabled, this permission allows users to print pages of VideoManager.

Although the user will still have the ability to use *CTRL + P* like normal if this permission is not enabled, the page will appear as blank.

- ***Copy text from website*** - this permission enables users to copy text from VideoManager.

Although the user will still have the ability to use *CTRL + C* like normal and highlight text if this permission is not enabled, they will not be able to paste the results.

Computer Analysis - these permissions are only viewable if computer analysis has been licensed from Motorola Solutions.

- ***View/delete*** - this permission enables users to view and delete computer analyses from the ***Computer Analysis*** section of the ***System*** pane, in the ***Admin*** tab.

Tactical Video Manager - these permissions are only viewable if Tactical VideoManager has been licensed from Motorola Solutions.

- ***Access tactical mode*** - this permission enables users to view the ***Tactical*** tab.
- ***View Tactical Video Wall*** - this permission enables users to view the Tactical VideoManager wall.
- ***Update Tactical Video Wall*** - this permission enables users to add and remove live streams from the Tactical VideoManager wall.

Asset imports - these permissions are only viewable if asset features have been licensed from Motorola Solutions.

- ***View/delete*** - this permission enables users to view and delete assets.
- ***View audit log*** - this permission enables users to view the audit logs of relevant assets.
- ***Use asset imports*** - this permission enables users to import non-video files (e.g. still images, PDFs), using the ***Advanced Import*** feature.
- ***View/delete automated imports*** - this permission enables users to view and delete automated imports from the ***Videos*** tab.

13.2 Appendix B: Device Profiles

A device profile determines the behaviour of a body-worn camera when it is recording. There is a different device profile for each type of body-worn camera.

- VB400

>> For more information, see VB400 Device Profile on page 444

- VB100 / VB200 / VB300

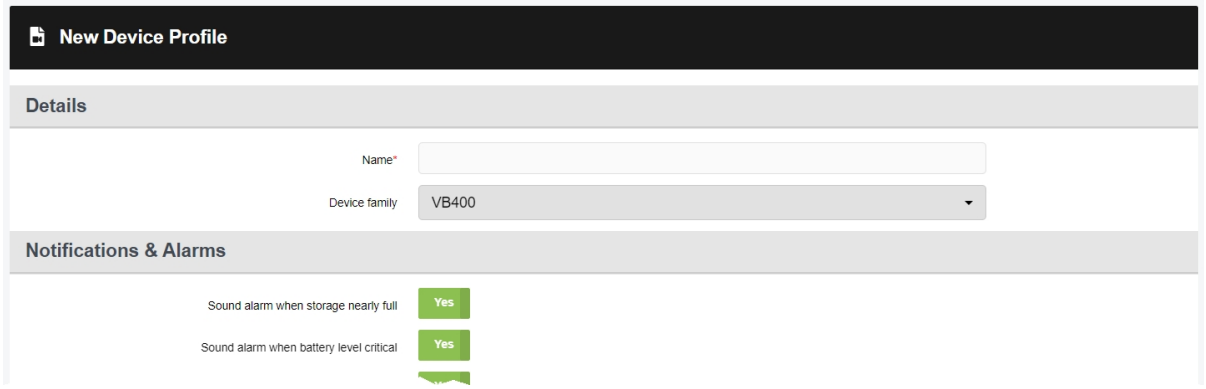
>> For more information, see VB100/VB200/VB300 Device Profile on page 451

- VT-series cameras

>> For more information, see VT-Series Camera Device Profile on page 455

13.2.1 VB400 Device Profile

The device profile section for a VB400 is split into the following sections: ***Details***, ***Notifications &Alarms***, ***Power Management***, ***Recording Behaviour***, ***Video Settings***, ***Bluetooth Settings***, ***VB Companion Settings***, and ***Controls***.



To view the relevant settings:

1. Navigate to the ***Admin*** tab.
2. Select the ***Devices*** pane.
3. Click the ***Device Profiles*** section.
4. Click ***Create profile***.
5. In the ***Name*** field, enter a name for the device profile.
6. From the ***Device family*** dropdown of the ***Details*** pane, select **VB400**.

The following settings are now available:

Notifications &Alarms - this section enables administrators to customise the way that the VB400 alerts its operator to various states and events.

- If ***Sound alarm when storage nearly full*** is set to ***Yes***, the VB400 will beep periodically when its storage space is low.
- If ***Sound alarm when battery level critical*** is set to ***Yes***, the VB400 will beep periodically when its battery level is critically low (less than 10 minutes of recording remaining).
- If ***Customise LED patterns*** is set to ***Yes***, the administrator can customise how a VB400's LEDs will behave when recording and pre-recording, using the ***When recording*** and ***When pre-recording*** dropdowns, respectively. The options for both dropdowns are as follows:
  - **Solid red**
  - **Solid green**

- **Blinking red**
- **Blinking red (top light only)**.

If set to ***No***, the VB400 will use its default LEDs.

- The administrator can customise how a VB400 will behave when in normal mode and hush mode, using the ***When in normal mode*** and ***When in hush mode*** rows, respectively. The options for the rows are as follows:
  - If ***Enable LEDs*** is set to ***On***, LEDs will indicate when a body-worn camera starts and stops recording/pre-recording.
  - If ***Enable beeps*** is set to ***On***, sounds will indicate when a body-worn camera starts and stops recording/pre-recording.
  - If ***Enable vibrate*** is set to ***On***, haptic feedback will indicate when a body-worn camera starts and stops recording/pre-recording.
  - If ***Enable X-Series LEDs*** is set to ***On***, any X-series cameras connected to VB400s in this device profile will have their LEDs enabled to indicate when they are recording.
  - If ***Enable X-Series vibrate*** is set to ***On***, any X-series cameras connected to VB400s in this device profile will have haptic feedback enabled to indicate when they start recording.
- The administrator can customise whether a VB400 will alert the user periodically while it is recording, using the ***Recording alarm*** row. The options for the row are as follows:
  - If ***Enable beeps*** is set to ***On***, the VB400 will beep while recording.
  - If ***Enable vibrate*** is set to ***On***, the VB400 will buzz while recording.

  In the ***seconds*** field, administrators can configure the interval at which the alarm will sound (between 5 and 600 seconds). This will apply to both beeps and haptic feedback, depending on what has been enabled.

*If **Enable beeps** and **Enable vibrate** have not also been set to **On** in the **When in normal mode** or **When in hush mode** rows, none of the configuration in the **Recording alarm** row will take effect.*

Power Management - this section enables administrators to configure advanced battery life management.

- From the ***Behaviour when idle*** dropdown, select how the VB400 will behave when idle (assigned and undocked, but not recording). The options are as follows:
  - **Device enters standby mode** - the body-worn camera will enter standby. The VB400 will leave standby as soon as it is prompted to record again.
  - **Device shuts down** - the body-worn camera will shut down. The VB400 will turn on a few seconds after it is prompted to record.

If **Device shuts down** *is selected, the VB400's battery will last for longer between charges.*

Recording Behaviour - this section controls how a VB400 will act when it is recording.

- If ***Show video metadata overlay*** is set to ***Yes***, metadata will be shown over all videos recorded on body-worn cameras which inhabit this device profile. What precise metadata is shown can be configured from the ***Video metadata overlay settings*** section of the ***Devices*** pane, in the ***Admin*** tab.

>> For more information, see Configure Video metadata overlay settings on page 210

- If ***Overwrite oldest footage when full*** is set to ***Yes***, the body-worn camera will overwrite its oldest footage with newer footage if it has run out of storage space.

If set to ***No***, the body-worn camera will stop recording once it has run out of storage space.

- If ***Allow recording in hush mode*** is set to ***Yes***, the body-worn camera can record footage while in hush mode. The body-worn camera can also enter hush mode while recording.

If set to ***No***, if the body-worn camera is in hush mode and the the operator performs the gesture which prompts their body-worn camera to start recording, the body-worn camera will exit hush mode. If the body-worn camera is recording and the operator performs the gesture which prompts their body-worn camera to enter hush mode, the body-worn camera will stop recording.

Pre-record will still work in hush mode, even if ***Allow recording in hush mode*** *is set to* ***No****.*

- If ***Pre-record*** is set to ***Yes***, pre-recording footage will be enabled.

Once pre-record has been enabled, the following options will become available:

  - In the ***Seconds*** field, enter the number of seconds for which the VB400 will pre-record. The default is 30 seconds, and the upper limit is 120 seconds.
  - From the dropdown, select when pre-record will start. The options are as follows:
    - **Always pre-record when not charging** - pre-record will be enabled as soon as the body-worn camera is undocked.
    - **Manually start/stop pre-record** - the administrator must manually configure an action which, when performed, will start pre-record. This is done from the ***Controls*** pane, covered later in this chapter.
  - Administrators can also set ***Post-record*** to ***On***.

  In the the ***Seconds*** field, enter the number of seconds for which the VB400 will post-record. The default is 30 seconds, and the upper limit is 120 seconds.

- From the ***Record audio*** dropdown, administrators can select whether their body-worn cameras record audio or not. The options are as follows:
    - **Yes** - audio will be recorded during both pre-record and normal recording.
    - **Yes (except during pre-record)** - audio will only be recorded during normal recording.
- If ***Enable GPS*** is set to ***Yes***, GPS location data will be recorded alongside any video.

If set to ***No***, the user can still add location data to the videos after they have been downloaded to VideoManager.

- In the ***Video length*** field, enter the number of minutes for which a VB400 can record, after which the footage will be split into multiple videos.

The administrator can select between 5 and 30 minutes.

- In the ***Suppress recording on undock*** field, enter the number of seconds for which the body-worn camera will be prevented from recording after it has been undocked. This means that in the configured period of time, the body-worn camera will ignore any gestures which would normally prompt it to record.

This also applies to recordings which would be started by Bluetooth Peripherals.

Video Settings - this section controls video resolution and frame rate.

- From the ***Video resolution*** dropdown, administrators can select the video resolution of videos recorded on body-worn cameras which inhabit this device profile. The options are as follows:
    - **Standard** - 1GB/hour, approximates to 360p or lowest resolution available to hardware, whichever is higher.
    - **High** - 2GB/hour, approximates to 720p or highest resolution available to hardware, whichever is lower.
    - **Full HD** - greater than 2GB/hour, approximates to 1080p or highest resolution available to hardware, whichever is lower.
- From the ***Frame rate*** dropdown, administrators can select the frame rate in which body-worn cameras inhabiting this device profile will record. There are two options: **25FPS** or **30FPS**.

Audio Settings - this section controls the VB400's audio options.

- From the ***Audio codec*** dropdown, select the kind of audio which will be recorded by VB400s with this device profile. The options are as follows:
    - **AAC** - this will compress the audio, and results in smaller file sizes.
    - **PCM** - this will record high-quality audio, but results in larger file sizes.

Bluetooth Settings - this section controls whether Bluetooth can be used with a VB400.

- From the ***Yardarm™ Holster Aware™ peripherals*** dropdown, administrators can select how many Bluetooth Peripherals will be associated with body-worn cameras in this device profile. If a VB400 in this device profile cannot find the number of Bluetooth Peripherals specified here when it is out in the field, an alarm will sound.

For more information, please contact Technical Support and ask for the technical paper *Personal Issue Yardarm Holster Aware Sensors Explained [ED-009-038]* or *Pool Issue Yardarm Holster Aware Sensors Explained [ED-009-070]*.

- If ***Peer-Assisted recording*** is set to ***On***, an assigned or allocated VB400 will automatically start recording if another VB400 starts recording in its vicinity.

For more information, please contact Technical Support and ask for the technical paper *Peer-Assisted Recording Explained [ED-009-056]*.

- From the ***Motorola radio integration*** dropdown, administrators can configure which radios will be compatible with body-worn cameras in this device profile.

For more information, please contact Technical Support and ask for the technical paper *VideoManager and Tetra Radio Integration Explained [ED-009-062]*.

VB Companion Settings - this section controls whether VB Companion can be used with a VB400.

- If ***Enable VB Companion*** is set to ***Yes***, the VB400 will be compatible with Motorola Solutions VB Companion.

Controls - this section enables administrators to configure their VB400s' buttons and gestures.

- From the ***Hold timing*** dropdown, select how long an operator must hold a VB400's button for the body-worn camera to register the gesture as a "hold". The options are **Long**, **Normal**, or **Short**.
- From the ***Double click timing*** dropdown, select how quickly an operator must double-click a VB400's button for the body-worn camera to register the gesture as a "double click". The options are **Long**, **Normal**, or **Short**.

Administrators can also map VB400 buttons (e.g. ***Front button***) to gestures (e.g. ***Press***) and the actions which will be performed as a result (e.g. **No action**).

To map a button's gesture onto an action, identify the relevant button and gesture from the ***Control*** column. Using the corresponding ***Action*** dropdowns, select the action which will be performed when the button's gesture is performed. The options are as follows:

- **No action** - the gesture does nothing.
- **Start/stop recording** - the gesture changes recording mode; if the VB400 is already recording, recording will stop when the gesture is performed. If VB400 is not recording when button is pressed, recording starts.
- **Start recording** - the gesture starts recording. If recording is already in progress, the gesture does nothing.
- **Stop recording** - the gesture stops recording. If recording is not in progress, the gesture does nothing.
- **Shutdown** - the VB400 will stop recording and shut down.

- **Show battery status** - the gesture will cause the VB400's LED C to reflect the body-worn camera's battery status. If the LED is *green*, the body-worn camera still has plenty of charge left. If the LED is *yellow*, the body-worn camera's battery is running low and should be recharged as soon as possible. If the LED is *red*, the body-worn camera is about to shut down due to low battery.
- **Record bookmark** - the gesture will place a bookmark in the video. Once the video has been downloaded to VideoManager, users can skip straight to the bookmark while viewing it.

This is the only way that users can place a bookmark directly into a video. Users can place bookmarks into videos on VideoManager, but they must be in an incident first.

>> For more information, see Create, Edit and Delete Bookmarks on page 86

- **Enter hush mode** - the gesture enters hush mode. While in hush mode, the VB400 will obey the settings configured in the ***When in hush mode*** row of the ***Notifications &Alarms*** pane.
- **Exit hush mode** - the gesture exits hush mode. Without hush mode, the VB400 will obey the settings configured in the ***When in normal mode*** row of the ***Notifications &Alarms*** pane.
- **Toggle hush mode** - the gesture changes between hush mode and normal mode.
- **Pair Bluetooth peripheral** - the gesture will prompt the VB400 to pair with a new Bluetooth Peripheral. The Bluetooth Peripheral must be connected to power while this is happening.
- **Bypass peripheral warning** - the gesture will allow users to stop a VB400 from beeping when it cannot find the requisite number of Bluetooth Peripherals, as specified from the ***Yardarm™ Holster Aware™ peripherals*** dropdown.
- **Enter safety mode** - the gesture causes the VB400 to enter safety mode. While in safety mode, the VB400 will be completely inert: start/stop recording gestures will not work, and the body-worn camera will not connect to WiFi networks/Bluetooth, or make noise.
- **Exit safety mode** - the gesture causes the VB400 to exit safety mode. Once the VB400 has exited safety mode, it can record footage, connect to WiFi networks/Bluetooth, and make noise.
- **Toggle safety mode** - if the VB400 is already in safety mode, it will exit safety mode. If the VB400 is **not** in safety mode, it will enter safety mode.

The following dropdown options are only visible if ***Pre-record*** has been set to ***Yes*** in the ***Recording Behaviour*** pane:

- **Start pre-record** - the gesture will start pre-recording. The length of the pre-record depends on the configuration in the ***Recording Behaviour*** pane.
- **Stop pre-record** - the gesture will stop pre-recording, and the pre-recorded footage will be discarded.

- **Toggle pre-record** - if the body-worn camera is already pre-recording, the gesture will stop pre-recording. If the body-worn camera is not pre-recording, the gesture will start pre-recording.

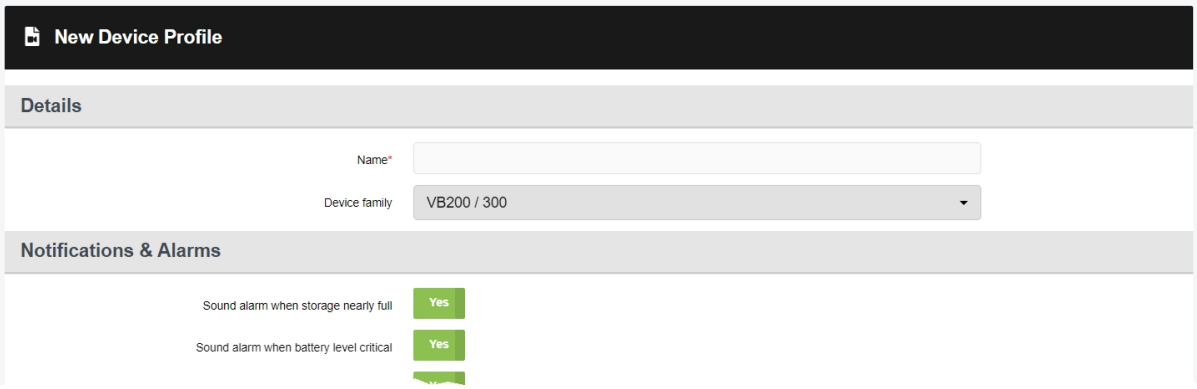
In the ***Controls*** section, there is also an option to make the ***WiFi connection*** either **Automatic** or **Manual**. If set to **Automatic**, the VB400 will search for WiFi upon powering on. If set to **Manual**, the VB400 must be ordered to search for WiFi using a button gesture. For this reason, more options will appear in the dropdown dictating what action the VB400's button will perform:

- **Connect to WiFi** - the gesture will prompt the VB400 to start searching for WiFi. If the VB400 is already connected to WiFi, this button does nothing.
- **Disconnect from WiFi** - the gesture will disconnect the VB400 from WiFi. If the VB400 is not already connected to WiFi, this button does nothing.
- **Toggle WiFi connection** - the gesture will change the state of the WiFi connection - if the WiFi was turned off, it will be turned on, and vice versa.

In the ***X-100/X-200*** section, users can configure how the X-series camera button is mapped onto gestures (***Press***, ***Hold***, and ***Double click***) and the actions which will be performed as a result (e.g. **No action**). To map the gesture's gesture to an action, use the ***Action*** dropdown - the options are the same as in the VB400 section.

13.2.2 VB100/VB200/VB300 Device Profile

The device profile section for a VB100, VB200, and VB300 is split into the following sections: ***Details***, ***Notifications &Alarms***, ***Power Management***, ***Recording Behaviour***, ***Video Settings***, and ***Controls***.



To view the relevant settings:

1. Navigate to the ***Admin*** tab.
2. Select the ***Devices*** pane.
3. Click the ***Device Profiles*** section.
4. Click ***Create profile***.
5. In the ***Name*** field, enter a name for the device profile.
6. From the ***Device family*** dropdown of the ***Details*** pane, select **VB200/300**.

The following settings are now available:

Notifications &Alarms - this section enables administrators to customise the way that the VB-series camera responds when various actions are performed.

- If ***Sound alarm when storage nearly full*** is set to ***Yes***, the VB-series camera will beep periodically when its storage space is low.
- If ***Sound alarm when battery level critical*** is set to ***Yes***, an alarm will sound in addition to the LED warning when battery is critically low (less than 10 minutes of recording remaining).
- If ***Sound alarm when recording starts or stops*** is set to ***Yes***, the VB-series camera will beep when recording starts.
- If ***Sound alarm regularly while recording*** is set to ***Yes***, the VB-series camera will regularly beep while recording video.

Administrators can configure the interval at which the alarm will sound.

- If ***Enable alarms in hush mode*** is set to ***Yes***, any alarms which have been configured in the previous settings will still make a noise when the body-worn camera is in hush mode.

- If ***Blink LED in standby*** is set to ***Yes***, a VB-series camera will blink when it is in standby mode. It will enter standby mode when it has been idle (assigned and undocked, but not recording) for a period of time.
- If ***Show front LEDs when recording VB300*** is set to ***Yes***, the VB-series camera's LEDs will be turned on during recording.
- If ***Show LEDs when recording X-100/X-200*** is set to ***Yes***, the X-100/X-200's LEDs will be turned on during recording.
- If ***Enable X-100/X-200 buzzer*** is set to ***Yes***, X-100s and X-200s will have haptic feedback.

Power Management - this setting enables administrators to configure advanced battery life management.

- If ***Power off when idle*** is set to ***Yes***, administrators can configure for how many hours the VB-series camera must be away from its charger, after which it will power off.

This will preserve battery life - however, the body-worn camera must be manually powered on before it can record. This can be done by pressing any button on the body-worn camera.

Recording Behaviour - this section controls how a VB-series camera will act when it is recording.

- If ***Show video metadata overlay*** is set to ***Yes***, metadata will be shown over all videos recorded on body-worn cameras which inhabit this device profile. What precise metadata is shown can be configured from the ***Video metadata overlay settings*** section of the ***Devices*** pane, in the ***Admin*** tab.

>> For more information, see Configure Video metadata overlay settings on page 210

- If ***Overwrite oldest footage when full*** is set to ***Yes***, the body-worn camera will overwrite its oldest footage with newer footage if it has run out of storage space.

If set to ***No***, the body-worn camera will stop recording once it has run out of storage space.

- If ***Pre-record*** is set to ***Yes***, pre-recording footage will be enabled.

Once pre-record has been enabled, the following options will become available:

  - In the ***Seconds*** field, enter the number of seconds for which the VB300 will pre-record. The default is 30 seconds, and the upper limit is 120 seconds.
  - From the dropdown, select when pre-record will start. The options are as follows:
    - **Always pre-record when not charging** - pre-record will be enabled as soon as the body-worn camera is undocked.
    - **Manually start/stop pre-record** - the administrator must manually configure an action which, when performed, will start pre-record. This is done from the ***Controls*** pane, covered later in this chapter.
- From the ***Record audio*** dropdown, administrators can select whether their body-worn cameras record audio or not. The options are as follows:

- **Yes** - audio will be recorded during both pre-record and normal recording.
- **No** - no audio will be recorded.
- **Yes (except during pre-record)** - audio will only be recorded during normal recording.

This option will only be visible if the administrator has set ***Pre-record*** to ***On***.

- **Require double consent** - the user must go through two steps before audio will be recorded - firstly, they must start recording with their body-worn camera, and then they must perform another gesture (as defined in the ***Controls*** pane) before the audio will be recorded alongside a video.

Video Settings - this section controls video resolution and frame rate.

- From the ***Video resolution*** dropdown, administrators can select the video resolution of videos recorded on body-worn cameras which inhabit this device profile. The options are as follows:
  - **Standard** - 1GB/hour, approximates to 360p or lowest resolution available to hardware, whichever is higher.
  - **High** - 2GB/hour, approximates to 720p or highest resolution available to hardware, whichever is lower.
  - **Full HD** - greater than 2GB/hour, approximates to 1080p or highest resolution available to hardware, whichever is lower.
- From the ***Frame rate*** dropdown, users can select the frame rate in which body-worn cameras inhabiting this device profile will record. There are two options: **25FPS** or **30FPS**.
- If ***Enhanced night vision*** is set to ***Yes***, the body-worn camera's frame rate will be cut in half and its exposure time will be doubled. This produces more well-lit footage but should only be used if the VB-series camera is mounted on a stable surface.

Controls - this section controls which gestures and actions are associated with the buttons of an X-100, X-200, and VB300.

To map a button's gesture onto an action, identify the relevant button and gesture from the ***Control*** column. Using the corresponding ***Action*** dropdowns, select the action which will be performed when the button's gesture is performed. The options are as follows:

- **No action** - the gesture does nothing.
- **Start/stop recording** - the gesture changes recording mode - if the VB300 is already recording, recording will stop when the gesture is performed. If the VB300 is not recording when the gesture is performed, recording starts.
- **Start recording** - the gesture starts recording. If recording is already in progress, the gesture does nothing.
- **Stop recording** - the gesture stops recording. If recording is not in progress, the gesture does nothing.

- **Record bookmark** - the gesture will place a bookmark in the video. Once the video has been downloaded to VideoManager, users can skip straight to the bookmark while viewing it.

>> For more information, see Create, Edit and Delete Bookmarks on page 86

- **Enter hush mode** - the VB300 will enter hush mode, meaning LEDs will turn off and alarms will not sound. If the VB300 is already in hush mode, the gesture does nothing.
- **Exit hush mode** - the VB300 will exit hush mode, meaning LEDs will turn on and alarms will sound as normal. If the VB300 is not in hush mode, the gesture does nothing.
- **Toggle hush mode** - if the VB300 is in hush mode when the gesture is performed, it will exit hush mode. If the VB300 is not in hush mode when the gesture is performed, it will enter hush mode.

The following dropdown options are only visible if ***Pre-record*** has been set to ***Yes*** in the ***Recording Behaviour*** pane:

- **Start pre-record** - the gesture will start pre-recording. The length of the pre-record depends on the configuration in the ***Recording Behaviour*** pane.
- **Stop pre-record** - the gesture will stop pre-recording, and the pre-recorded footage will be discarded.
- **Toggle pre-record** - if the body-worn camera is already pre-recording, the gesture will stop pre-recording. If the body-worn camera is not pre-recording, the gesture will start pre-recording.

In the ***Controls*** section, there is a ***WiFi connection*** dropdown, from which the administrator can select whether WiFi connection is either **Automatic** or **Manual**. If set to **Automatic**, the VB300 will search for WiFi upon powering on. If set to **Manual**, the VB300 must be ordered to search for WiFi using a button gesture. For this reason, more options will appear in the dropdown dictating what action the VB300's button will perform:

- **Connect to WiFi** - the gesture will prompt the VB300 to start searching for WiFi. If the VB300 is already connected to WiFi, this button does nothing.
- **Disconnect from WiFi** - the gesture will disconnect the VB300 from WiFi. If the VB300 is not already connected to WiFi, this button does nothing.
- **Toggle WiFi connection** - the gesture will change the state of the WiFi connection - if the WiFi was turned off, it will be turned on, and vice versa.

In the ***X-100/X-200*** section, administrators can configure how the X-series camera button is mapped onto gestures (***Press***, ***Hold***, and ***Double click***) and the actions which will be performed as a result (e.g. **No action**). To map the button's gesture to an action, use the ***Action*** dropdown - the options are the same as in the VB300 section.

13.2.3 VT-Series Camera Device Profile

The device profile section for a VT-series camera has one section: ***Recording Behaviour***.

To view the relevant settings:

1. Navigate to the ***Admin*** tab.
2. Select the ***Devices*** pane.
3. Click the ***Device Profiles*** section.
4. Click ***Create profile***.
5. Select **VT50/100** from the ***Device family*** dropdown of the ***Details*** pane.
6. If ***Show video metadata overlay*** is set to ***On***, all VT-series cameras in this device profile will record videos with burned-in metadata.

Administrators can configure what information will be included in this metadata from the ***Video metadata overlay settings*** section of the ***Devices*** pane, in the ***Admin*** tab.

>> For more information, see Configure Video metadata overlay settings on page 210

13.3 Appendix C: Types of Report

VideoManager offers many types of report. The following appendix covers every type of report which can be created, and the corresponding columns and values they contain.

Sites

If VideoManager has been configured to act as a Central VideoManager, this will return a list of all sites connected to it, as well as detailing how long the sites have been online/offline (in hours).

- **Site Name** - the name of the site, as configured from the ***Status*** tab.
- **Online** - the number of hours for which the site was online (within the period covered by the report).
- **Offline** - the number of hours for which the site was offline (within the period covered by the report).
- **Bytes** - the number of bytes transferred from this site to the Central VideoManager, including footage and metadata.

Management

This will return a high-level overview of key system parameters, including the total hours of footage recorded, and the total number of incidents and exports created, within the period covered by the report.

- **Recordings (total)** - the total number of recordings captured in the period covered by the report.
- **Recordings (length)** - the total length of recordings captured in the period covered by the report, in minutes.
- **Recordings (MB)** - the total size of recordings captured in the period covered by the report, in MB.
- **Average recording (length)** - the average length of recording captured in the period covered by the report, in minutes.
- **Average recording (MB)** - the average size of recording captured in the period covered by the report, in MB.
- **Media items (total)** - the total number of media. This includes videos recorded on body-worn cameras, imported videos, and imported assets (within the period covered by the report).
- **Media items (length)** - the total length of media recorded or imported in the period covered by the report, in minutes.
- **Media items (MB)** - the total size of media recorded or imported in the period covered by the report, in MB.

- **Media deletions (manual)** - the number of media items which users have manually deleted from VideoManager (within the period covered by the report).
- **Media deletions (policy)** - the number of media items which have been automatically deleted by VideoManager as a result of its deletion policy (within the period covered by the report).
- **Incidents** - the number of incidents created on the system (within the period covered by the report).
- **Exports** - the number of exports created on the system (within the period covered by the report).
- **Active Device Operators** - the number of users which have body-worn cameras assigned to them (within the period covered by the report).
- **Active Devices Video Test Failures** - the number of videos which have been flagged by VideoManager as having dropped frames (within the period covered by the report).
- **Device Key Exports** - the number of times that access control keys have been exported (within the period covered by the report). If the same access control key is exported multiple times, this will count as different events in the report.

User Summary

This will return the metrics for a specified user, including their username, display name, whether they are enabled or not, and the number of days for which they have logged in/not logged in. If no username is entered, the report will present the information for **all** users on the system. If scheduled, this report can be copied to the **Report auto-copy** file space.

- **Username** - the username for the user, as configured in the ***User name*** field.
- **Name** - the display name for the user, as configured in the ***Display name*** field.
- **UserId** - the numeric ID for the user in VideoManager's database.
- **State** - whether the user is enabled (i.e. can log into VideoManager) or disabled (i.e. cannot log into VideoManager).
- **Date Assigned with Recording** - the number of days that the user was assigned a body-worn camera and recorded footage (within the period covered by the report).
- **Date Assigned without Recording** - the number of days that the user was assigned a body-worn camera but did not record footage (within the period covered by the report).
- **Days Not Assigned** - the number of days that the user was not assigned a body-worn camera (within the period covered by the report).
- **Days Logged In** - the number of days that the user logged into VideoManager (within the period covered by the report).
- **Days Not Logged In** - the number of days that the user did not log into VideoManager (within the period covered by the report).

Incidents

This will return a list of all incidents which have been created in the period covered by the report. It will also return the details for these incidents, including their signatures, names, when they were created, and when they were last edited (even if this is not within the period covered by the report). If scheduled, this report can be copied to the **Report auto-copy** file space.

The columns which users will see depend on how user-defined incident fields have been configured. By default, if the administrator has not edited the built-in incident fields (i.e. has not renamed, reordered, or deleted them), the columns will be as follows:

- **ID** - the internal ID for the incident in VideoManager's database.
- **Incident Created** - when the incident was created.
- **Last Edited** - when the incident was last edited.
- **Title** - the incident's title.
- **Incident time** - the incident's time, as configured in the ***Incident time*** field.
- **Reference code** - the incident's reference code, as configured in the ***Reference code*** field.
- **Notes** - the incident's notes, as configured in the ***Notes*** field.
- Any other user-defined incident fields which the administrator has created will appear as separate columns, regardless of whether the fields themselves have been populated in the incidents.

Computed fields will still be shown in the report, even if their conditions have not been met.

- **Other fields** - if a user has populated a now-deleted user-defined incident field for this incident, this column will show the name of the deleted user-defined incident field(s) and the corresponding value(s).
- **Recorded by** - if the incident includes footage, this column will list the operator(s) which recorded the footage.

Videos

This will return a list of all videos which were recorded on body-worn cameras or imported into VideoManager in the period covered by the report. It will also return the details for these videos, including who recorded them, when the recording started and stopped, the videos' duration, and the serial numbers of the body-worn cameras which recorded them. If scheduled, this report can be copied to the **Report auto-copy** file space.

- **URN** - the video's unique ID.
- **Recording identifier** - the video's unique recording ID.

- **Recording index** - if the video is part of a longer recording, this column will show its position in the recording (i.e. the first video will be 0, the second video will be 1, etc.).
- **Username** - the user who recorded or imported the video.
- **Badge ID** - the body-worn camera which recorded the video. If the video was imported, this will read as *import*.
- **Start time** - when the video started.
- **End time** - when the video ended.
- **Duration** - how long the video is.
- **Quality** - the video's resolution and FPS.
- **Data size (MB)** - the size of the video in MB.
- **Bookmarked?** - whether the video was bookmarked in the field.
- **In incident?** - whether the video is in an incident.
- **Deleted?** - whether the video has been deleted from VideoManager
- **SHA-256** - the SHA-256 hash of the video.

User Export

This will return a list of all users on VideoManager at the time the report was created. It will also return the details for these users, including their usernames, display names, RFID IDs, and the roles they inhabit. If scheduled, this report can be copied to the **Report auto-copy** file space.

- **Username** - the username for the user, as configured in the ***User name*** field.
- **Display Name** - the display name for the user, as configured in the ***Display name*** field.
- **Password** - the password of the user.
- **State** - whether the user is enabled (i.e. can log into VideoManager), disabled (i.e. cannot log into VideoManager), or deleted.
- **RFID** - if the user has been associated with an RFID card, this is their Touch Assign ID.
- **BLE MAC Address** - if enabled for the report, this is the user's BLE MAC Address. Users are automatically issued an Address by VideoManager the first time they use Bluetooth (either with VB Companion, peer-assisted recording, or Bluetooth Peripherals).
- **Roles** - the roles which the user inhabits.

Operator Recorder Summary

This will return a summary of operator activity (i.e. how many videos have been recorded in the period covered by the report), broken down by operator and date. It will also return the details for each field trip, including the

serial numbers of the body-worn cameras, and how many videos were recorded. If scheduled, this report can be copied to the **Report auto-copy** file space.

- **Operator Name** - the name of the operator who recorded the footage.
- **Device Number** - the serial number of the body-worn camera which was used by the operator on the specified date.
- **Date** - the date(s) when the operator recorded footage.
- **Number Of Videos** - the number of videos which were recorded by the operator on the specified date.
- **Time of First Video** - the start time of the first recording on the specified date.
- **Time of Last Video** - the start time of the last recording on the specified date.
- **Number of videos < 20 secs** - the number of videos on the specified date which are shorter than 20 seconds.
- **% of videos < 20 secs** - the percentage of videos on the specified date which are shorter than 20 seconds.

Equipment

This will return a list of all equipment associated with this instance of VideoManager (i.e. body-worn cameras, DockControllers, EdgeControllers, Central VideoManager, sites, grid masters and grid workers). It will also return the details for these pieces of equipment, including their type (e.g. VB400), when they were last "seen" by VideoManager, and the software they are running. If scheduled, this report can be copied to the **Report auto-copy** file space.

- **Serial Number** - the serial number of the equipment in question.
- **Type** - the type of equipment (e.g. VB400, DC-200, grid).
- **Identity or custom status** - the information presented here depends on the type of equipment:
  - If the equipment is a body-worn camera, this will be its custom status, as configured from the ***Custom status*** field.
  - If the equipment is not a body-worn camera, this will be its name or serial number.
- **First seen** - when the equipment was first connected to VideoManager.
- **Last seen** - when the equipment was last detected by VideoManager. If the equipment is still connected to VideoManager, this timestamp will be when the report was run.
- **Last location** - the site where the equipment was last detected by VideoManager. If sites have not been configured, or if the equipment was last seen at the Central VideoManager, this will read as *Central*.
- **Last sub-location** - the DockController where the equipment was last detected by VideoManager. If body-worn cameras are directly connected to VideoManager via USB,

this will read as *USB*. If body-worn cameras are connected to VideoManager via WiFi, this will read as *Network: [WiFi Network Name]*.

- **Last software version** - the software version that the equipment was running when it was last seen by VideoManager.
- **Last state** - the last state that the equipment was in when it was last seen by VideoManager.
- **Additional Info** - the information presented here depends on the state of the equipment:
    - If the body-worn camera is assigned, this will read as the operator it is assigned to.
    - If the body-worn camera has been forgotten from VideoManager, this will read as the date when it was forgotten.
    - If equipment was moved from this instance of VideoManager, this will read as *Moved to another location*.
    - If the site was deleted from VideoManager, this will read as the date when it was deleted.

Battery Audit

This report details whether body-worn cameras' batteries have degraded. This could be because the body-worn camera has a faulty battery, has charged down quickly once it has been fully charged and still docked, or has powered down sooner than expected while recording. If scheduled, this report can be copied to the **Report auto-copy** file space.

- **Device Name** - the unique device ID of the body-worn camera which is experiencing battery issues.
- **Event Date** - when VideoManager first registered the battery issue. If the body-worn camera powered down unexpectedly in the field, this will be when it was redocked.
- **Event Type** - the specific kind of battery issue which the body-worn camera is experiencing:
    - *battery status* - the body-worn camera has detected an issue with charging its battery.
    - *high self discharge* or *self discharge* - the body-worn camera's battery charged down quickly while docked after being fully charged. This only applies to VB100, VB200, and VB300 body-worn cameras.
    - *limited battery capacity* - the body-worn camera was fully charged when undocked, but ran out of charge unexpectedly while in the field. This only applies to VB100, VB200, and VB300 body-worn cameras.
- **Summary** - this gives more detail about the battery issue:

- If the body-worn camera's issue is *battery status*, this will provide information about the specific problem with the battery (e.g. whether it is refusing to charge, charging too slowly, or could not be detected).
- If the body-worn camera's issue is *high self discharge* or *self discharge*, this will provide information about how much voltage was discharged from the battery while charging, and when it did so, as measured from when the battery was fully charged (e.g. *3.89V after duration of 6h* means that, 6 hours after the battery was fully charged, the battery voltage dropped to 3.89V).
- If the body-worn camera's issue is *limited battery capacity*, this will provide information about when the body-worn camera shut down unexpectedly, compared to the expected battery life.

Device Availability

This will return a list of body-worn cameras at each location (e.g. a DockController) in five-minute intervals for the duration of the period covered by the report. It will also return the number of body-worn cameras which are busy, charging, or assigned, and the number of body-worn cameras which are available (ready to be assigned) at each location. If scheduled, this report can be copied to the **Report auto-copy** file space.

- **Location** - the DC-200 which is being audited. If body-worn cameras are directly connected to VideoManager via USB, this will read as *USB*. If sites have been configured, this will read as *site name / DockController name (or USB)*.
- **Timestamp** - when VideoManager checked the location. This will be in five-minute intervals.
- **Busy** - the number of body-worn cameras at the location which are upgrading firmware or downloading footage.
- **Charging** - the number of body-worn cameras at the location which are charging.
- **MinimumAvailable** - the minimum number of body-worn cameras available for assignment over the course of the 5-minute interval.
- **Assigned** - the number of body-worn cameras at the location which are assigned to users.

Device Field Trip

This will return a list of trips made by body-worn cameras within the period covered by the report. It will also return the details for these trips, including where the body-worn cameras were initially docked, where they were redocked after recording (e.g. if a body-worn camera was redocked to a different DockController), and the start/end times of the trips. If scheduled, this report can be copied to the **Report auto-copy** file space.

- **Username** - the user who went on the field trip.
- **Start Site** - the site where the body-worn camera was undocked. If sites have not been configured, or if the body-worn camera was undocked at the Central VideoManager, this will read as *Central*.

- **End Site** - the site where the body-worn camera was redocked. If sites have not been configured, or if the body-worn camera was undocked at the Central VideoManager, this will read as *Central*.
- **Start Location** - the DockController where the body-worn camera was undocked. If body-worn cameras are directly connected to VideoManager via USB, this will read as *USB*. If body-worn cameras are connected to VideoManager via WiFi, this will read as *Network: [WiFi Network Name]*.
- **End Location** - the DockController where the body-worn camera was redocked. If body-worn cameras are directly connected to VideoManager via USB, this will read as *USB*. If body-worn cameras are connected to VideoManager via WiFi, this will read as *Network: [WiFi Network Name]*.
- **Badge ID** - the serial number of the body-worn camera which was operated by the user.
- **Start time** - when the body-worn camera was undocked.
- **End time** - when the body-worn camera was redocked. If the body-worn camera is still in the field, this will read as *In Field*.
- **Duration** - the length of the field trip, from the body-worn camera being undocked to redocked.

Operator Activity

This will return a list of every user on VideoManager who has recorded at least one video in the period covered by the report. It will also return the length of the videos (from 30 seconds up to over 40 minutes), whether those videos are in incidents or not, the total number of videos recorded by a user, and the combined length of a user's videos. If scheduled, this report can be copied to the **Report auto-copy** file space.

- **Operator Id** - the name of the operator.
- **Evidential 30 seconds to 5 minutes** - the number of videos recorded by the operator which meet three criteria: they were recorded in the period covered by the report, are between 30 seconds to 4:59 minutes long, and have been added to an incident.
- **Evidential 5 minutes to 15 minutes** - the number of videos recorded by the operator which meet three criteria: they were recorded in the period covered by the report, are between 5 to 14:59 minutes long, and have been added to an incident.
- **Evidential 15 minutes to 30 minutes** - the number of videos recorded by the operator which meet three criteria: they were recorded in the period covered by the report, are between 15 to 29:59 minutes long, and have been added to an incident.
- **Evidential 30 minutes to 40 minutes** - the number of videos recorded by the operator which meet three criteria: they were recorded in the period covered by the report, are between 30 to 39:59 minutes long, and have been added to an incident.
- **Evidential over 40 minutes** - the number of videos recorded by the operator which meet three criteria: they were recorded in the period covered by the report, are more than 40 minutes long, and have been added to an incident.

- **Non-Evidential 30 seconds to 5 minutes** - the number of videos recorded by the operator which meet three criteria: they were recorded in the period covered by the report, are between 30 seconds to 4:59 minutes long, and have not been added to an incident.
- **Non-Evidential 5 minutes to 15 minutes** - the number of videos recorded by the operator which meet three criteria: they were recorded in the period covered by the report, are between 5 to 14:59 minutes long, and have not been added to an incident.
- **Non-Evidential 15 minutes to 30 minutes** - the number of videos recorded by the operator which meet three criteria: they were recorded in the period covered by the report, are between 15 to 29:59 minutes long, and have not been added to an incident.
- **Non-Evidential 30 minutes to 40 minutes** -the number of videos recorded by the operator which meet three criteria: they were recorded in the period covered by the report, are between 30 to 39:59 minutes long, and have not been added to an incident.
- **Non-Evidential over 40 minutes** - the number of videos recorded by the operator which meet three criteria: they were recorded in the period covered by the report, are more than 40 minutes long, and have not been added to an incident.
- **Total number of recordings** - how many recordings have been recorded by the operator (within the period covered by the report).
- **Total number of evidential recordings** - how many of the operator's recordings which were recorded in the period covered by the report have been added to an incident.
- **Total length of recordings** - the total length of the operator's recordings which were recorded in the period covered by the report, in seconds.
- **Count of cameras booked out** - the number of times that a body-worn camera assigned to this user was undocked (within the period covered by the report).

Full User Export

This will create a CSV file with information about all users on the system, including their roles, groups, and (optionally) user-specific WiFi networks. This report can be used with the user import tool to import all users from one VideoManager system into another. If scheduled, this report can be copied to the **Report auto-copy** file space.

The report is divided into different sections, which correspond to different exported information.

The *[USERS]* section provides information about the users exported from VideoManager:

- **Username** - the username for the user, as configured in the ***User name*** field.
- **Display Name** - the display name for the user, as configured in the ***Display name*** field.
- **Enabled** - whether the user is enabled (i.e. can log into VideoManager) or disabled (i.e. cannot log into VideoManager).
- **Email** - the email address associated with the user.
- **Email Notifications** - whether email notifications have been enabled for the user or not.
- **Mobile** - the mobile number associated with the user.

- **Mobile Notifications** - whether mobile notifications have been enabled for the user or not.
- **Touch Assign ID** - if the user has been associated with an RFID card, this is their Touch Assign ID.

The *[GROUPS]* section provides information about the groups exported from VideoManager:

- **Group Name** - the name of the group.
- **Display Name** - the display name of the group.

The *[ROLES]* section provides information about the roles which apply to the exported users/groups:

- **UserOrGroup** - the name of the user/group.
- **Role name** - the name of the role on VideoManager which the user/group inhabits.

The *[RELATIONSHIPS]* section provides information about the relationships between the exported users and groups:

- **UserOrGroup1** - the name of the user/group which has some form of oversight over another user/group.
- **Relationship** - the kind of oversight that **UserOrGroup1** has.

  This could be **Member of**, **Autoshare**, **Videoshare**, **Incidentshare**, or **Supervises**.
- **UserOrGroup2** - the name of the user/group which is subject to oversight from **UserOrGroup1**.

If enabled, the *[WIFIS]* section provides information about the WiFi networks exported from VideoManager and the users they are assigned to:

- **UserOrGroup** - the name of the user/group to whom this WiFi network is assigned.
- **SSID** - the SSID of the WiFi network.
- **Security type** - the security type of the WiFi network. This could be **WPA2-PSK**, **WPA-PSK**, **WEP**, **Open**, or **WPA2-PEAP-MSCHAPV2**.
- **Identity** - this column will be empty unless the user has specified that the WiFi network is **WPA2-PEAP-MSCHAPV2**.
- **PasswordOrKey** - the password of the WiFi network.
- **24Hz only**/**5Hz only** - these columns correspond to the WiFi network's ***Band*** dropdown. These columns are mutually exclusive.
- **Use Static IP**, **IP**, **Network Mask**, **Gateway**, **DNS Server 1**, **DNS Server 2** - this information is only relevant to the network administrator.
- **Signal Threshold** - this corresponds to the ***Disconnect on low signal*** toggle. It will be either *true* or *false*.
- **Signal Percent** - if the **Signal Threshold** column has been populated with *true*, this is the corresponding signal level, below which the WiFi network will be disconnected from the body-worn camera.

- **Signal Threshold Time** - if the **Signal Threshold** column has been populated with *true*, this is the corresponding time in seconds that the signal must be weak for, after which the WiFi network will be disconnected.
- **Hidden Network** - this corresponds with the ***Hidden network*** toggle. It will be either *true* or *false*.

For more information, please see the document *Built-in User Import Tool Guide [ED-012-229]*. This can be found in VideoManager's installation location, in the ***userimporttool*** folder.

13.4 Appendix D: Keyboard Shortcuts

Users can utilise keyboard shortcuts to locate the relevant section in a video.

The following shortcuts can be used when viewing a video that is part of an incident:

- A - ***Cycle between on-screen annotations***
- E - ***Edit selected annotation***
- K - ***Navigate to next annotation***
- J - ***Navigate to previous annotation***

The following shortcuts can be used either when viewing a video that is part of an incident, or when viewing a video like normal from the ***Videos*** pane:

- Space, play/pause - ***Play/pause the video player***
- R - ***Play the video player***
- P - ***Pause the video player***
- Left arrow - ***Step forwards***
- Right arrow - ***Step backwards***
- X - ***Jump forward 5 seconds in the clip***
- Z - ***Jump backward 5 seconds in the clip***
- V - ***Jump forward 60 seconds in the clip***
- C - ***Jump backward 60 seconds in the clip***
- M - ***Mute the video***
- F - ***Toggle fullscreen for player***
- T - ***Toggle theater mode for player***
- D - ***Toggle date time overlay***
- S - ***Download a screenshot of the current frame in the player***
- 0 - ***Jump to start of clip***
- 1 - ***Jump 10% into clip***
- 2 - ***Jump 20% into clip***
- 3 - ***Jump 30% into clip***
- 4 - ***Jump 40% into clip***
- 5 - ***Jump 50% into clip***

- 6 - ***Jump 60% into clip***
- 7 - ***Jump 70% into clip***
- 8 - ***Jump 80% into clip***
- 9 - ***Jump 90% into clip***

13.5 Appendix E: Custom Predicate Language

The Motorola Solutions custom predicate language is used for a variety of advanced features on VideoManager. This appendix will cover the following functions:

- Searching for incidents using an advanced search, from the ***Search Incidents*** pane.
- Searching for media using an advanced search, from the ***Search Videos*** pane.
- Creating incidents automatically, based on how a video/asset's user-defined media fields have been populated.
- Deleting incidents automatically, based on how their user-defined incident fields have been populated.
- Creating rules for an export profile, based on how an incident's user-defined incident fields have been populated.
- Creating computed fields, which appear and change based on how other user-defined incident fields in an incident have been populated.

13.5.1 Custom Predicate Language and Incident and Media Fields

Motorola Solutions custom predicate language is based around incident and media fields, and how they have been populated.

For advanced incident searches, VideoManager can return incidents based on how their built-in and user-defined incident fields have been populated.

For advanced media searches, VideoManager can return assets and videos based on how their built-in and user-defined media fields have been populated.

For automatic incident creation, incidents can be created based on how their built-in and user-defined incident fields have been populated.

For automatic incident deletion, incidents can be deleted based on how their fields have been populated, and how old they are. This is determined by the text entered into the ***Delete incident if*** field, and the date entered into the ***Auto-deletion date*** field.

For export profile rules, exports can be allowed to use export profiles based on how the incident's built-in and user-defined incident fields have been populated. Export profile rules are usually formatted as CASE functions. All examples of export profile rules in this documentation will be formatted as CASE functions.

>> For more information, see CASE Functions on page 478

For computed fields, administrators can determine whether the field appears based on how other built-in and user-defined incident fields have been populated. They can either be formatted as a boolean function (which will present the computed field as a checkbox - checked if true, unchecked if false), or as a CASE function. This documentation will give examples for both.

>> For more information, see CASE Functions on page 478

There are two types of text field: built-in and user-defined incident fields.

Built-in Text Fields

Built-in fields come with VideoManager by default, and can be used to add more information to incidents or assets. For an incident, built-in text fields include `notes` and `owner`.

User-Defined Text Fields

User-defined text fields do not come with VideoManager by default. Instead, sufficiently privileged users must create these fields manually. They enable users to categorise their incidents and media in a more advanced manner which suits the unique needs of their organisation.

13.5.2 Match Text Operators and Values

Users can match text fields to a specific value (e.g. `owner = test`), using the following operators:

- `=` - the text field matches the value (e.g. `title = 'Incident 0001'`).
- `< >` or `!=` - the text field does not match the value (e.g. `title != 'Incident 0001'`).
- `like` - the text field matches the case-sensitive value.
- `ilike` - the text field matches the case-insensitive value.
- `contains()` - this is only for tag list fields. Here, the user must enter the tag list field identifier, and the name of the specific tag(s) - e.g. `contains ([priority-level], 'high priority')`.

As well as matching a text field to a specific value (e.g. `owner = test`), users can also utilise wildcard values that match text fields to letters or characters. The wildcard values are as follows:

- `a%` - the field starts with 'a'.
- `%a` - the field ends with 'a'.
- `%a%` - the field has 'a' in any position.
- `_a%` - the field has 'a' in the second position.
- `a_%_%` - the field starts with'a' and is at least three characters in length.
- `a%o` - the field starts with 'a' and ends with 'o'.

Use the text field's **identifier**, instead of their **display name**. If the identifier is more than one word, either wrap it in square brackets (e.g. `[ready-to-export]`) or use camel case (e.g. `readyToExport`).

Use `and`/`or` functions to link multiple fields together.

The custom predicate language is **case-sensitive** for **identifiers** - for example, if an administrator has created the drop down field `[reason-for-creation]`, VideoManager would not let them save the following entry, because it does not recognise the field.

```
[Reason-For-Creation] = theft
```

The custom predicate language is also **case-sensitive** for **values** - for example, if an administrator has created the drop down field `[reason-for-creation]` with the options `assault` and `theft`, VideoManager would not enforce the following export profile rule because it does not recognise the value.

```
case
 when [reason-for-creation] = 'Theft' then 'You cannot export this
incident.'
 end
```

Advanced Incident Search Example

In the following example, any incident whose owner is `admin` would be returned:

```
owner = admin
```

In the following examples, any incident whose owner is **not** `admin` would be returned:

```
owner != admin
```

```
owner < > admin
```

In the following example, any incident whose title started with `t` would be returned:

```
title like 't%'
```

In the following example, any incident whose title started with `t` or `T` would be returned:

```
title ilike 't%'
```

Advanced Media Search Example

In the following example, any video or asset whose `vehicle` tag list field includes `car` would be returned:

```
contains(vehicle, 'car')
```

In the following example, any video or asset whose `vehicle` tag list field includes `car` and `bus` would be returned:

```
contains(vehicle, 'car, bus')
```

In the following example, any video or asset whose title started with `t` would be returned:

```
title like 't%'
```

In the following example, any video or asset whose title started with `t` or `T` would be returned:

```
title ilike 't%'
```

Auto-Incident Creation Example

In the following example, any media whose `owner` is `admin` would be added to an incident:

```
owner = admin
```

In the following example, any media whose `owner` is `admin` **and** whose `[auto-incident]` user-defined media field has been set to `true` would be added to an incident:

```
owner = admin and [auto-incident] = true
```

In the following example, any media whose title started with `t` would be added to an incident:

```
title like 't%'
```

In the following example, any media whose title started with `t` or `T` would be added to an incident:

```
title ilike 't%'
```

Auto-Incident Deletion Example

In the following example, any incident whose `[ready-to-delete]` user-defined incident field is set to `yes` would be eligible for deletion:

```
[ready-to-delete] = yes
```

In the following example, any incident whose `[reviewed-already]` **and** `[ready-to-delete]` user-defined incident fields are set to `yes` would be elgible for deletion:

```
[reviewed-already] = yes and [ready-to-delete] = yes
```

In the following example, any incident whose title started with `t` would be eligible for deletion:

```
title like 't%'
```

In the following example, any incident whose title does **not** start with `t` would be eligible for deletion:

```
title ilike 't%'
```

Export Profile Example

In the following example, any incidents whose `[ready-to-export]` user-defined incident field is set to `No` could not use the export profile:

```
case
 when [ready-to-export] = 'No' then 'This incident is not ready to
be exported.'
 end
```

In the following example, any incidents whose `[ready-to-export]` user-defined incident field is set to `Yes` could use the export profile, and incidents whose `[ready-to-export]` user-defined incident field is set to anything else could not:

```
case
 when [ready-to-export] = 'Yes' then 'This incident is ready to be
exported.'
 else 'This incident is not ready to be exported.'
 end
```

In the following example, any incidents whose ***Reviewed by*** user-defined incident field is populated with `b%` could use the export profile:

```
case
 when [reviewed-by] = 'b%' then ''
 end
```

Computed Field Example

In the following example, the computed field `[reviewed]` would appear as a checked checkbox in any incidents whose `[reviewer]` user-defined incident field was set to `administrator`:

```
[reviewer] = 'administrator'
```

In the following examples, the computed field `[reviewed]` would appear as a checked checkbox in any incidents whose `[review-notes]` user-defined incident field had been populated:

```
[review-notes] != ''
```

```
[review-notes] < > ''
```

In the following example, the computed field `[reviewed]` would appear with different text, depending on how the `[review-notes]` user-defined incident field had been populated in incidents:

```
 case
  when [review-notes] != '' then 'This incident has been reviewed.'
  when [review-notes] = '' then 'This incident has not been
reviewed.'
  end
```

In the following example, the computed field `[reviewed-by-administrator]` would appear as a checked checkbox in any incidents whose `[reviewer]` user-defined incident field was populated with `admin%`:

```
 [reviewer] = 'admin%'
```

In the following example, the computed field `[reviewed]` would appear with different text, depending on how the `[reviewer]` user-defined incident field had been populated in incidents:

```
 case
  when [reviewer] = 'admin%' then 'This incident has been reviewed
by an administrator.'
  when [reviewer] != 'admin%' then 'This incident has not been
reviewed by an administrator.'
  end
```

13.5.3 Match Date Operators and Values

Users can match values to a built-in date field or user-defined date field, utilising the following operators:

- `=` - the date field matches the value (e.g. `[creation-time] = 2019/12/11`, the ***Creation Time*** field has a value of December 11th, 2019).
- `<` - the date field is less than the value (e.g. `[creation-time] < 2019/12/11`, the ***Creation Time*** field has a value which is earlier than December 11th, 2019).
- `<=` - the date field is equal to, or less than, the value (e.g. `[creation-time] <= 2019/12/11`, the ***Creation Time*** field has a value which is either December 11th, 2019 or earlier).
- `>` - the date field is greater than the value (e.g. `[creation-time] > 2019/12/11`, the ***Creation Time*** field has a value which is later than December 11th, 2019).
- `>=` - the date field is equal to, or greater than, the value (e.g. `[creation-time] >= 2019/12/11`, the ***Creation Time*** field has a value which is either December 11th, 2019 or later).

Instead of matching an incident text field to a specific, fixed value (e.g. `[creation-time] = '2020/04/01'`), users can also utilise wildcard values that match date fields to dates which are relative to today. The wildcard values are as follows:

- `now()` - this is today's date and time.
- `today()` - this is today's date.
- `dateAdd()` - users can add intervals using three formats: number, interval, and dates (e.g. `> dateAdd(-7, day, now())` would set the time to a week before now).

The number can be positive or negative (e.g. `7` or `-7`), and the intervals are `day`, `month`, `year`, `hour`, `minute`, and `second`.

Use the date field's **identifier**, instead of their **display name**. If the identifier is more than one word, either wrap it in square brackets (e.g. `[creation-time]`) or use camel case (e.g. `creationTime`).

Format dates as YYYY/MM/DD, and wrap them in single quotation marks (e.g. `'2007/11/30'`).

Advanced Incident Search Example

In the following example, any incidents which were created before 04/06/2020 will be returned.

```
[creation-time] < '2020-06-04'
```

Advanced Incident Search Example

In the following example, any incidents which were created before today will be returned:

```
[creation-time] < today()
```

In the following example, any incidents which were created within the week before today will be returned:

```
[creation-time] > dateAdd(-7, day, today())
```

Advanced Media Search Example

In the following example, any videos/assets whose `upload-date` user-defined media field has been populated with a date earlier than 04/06/2020 will be returned.

```
[upload-date] < '2020-06-04'
```

In the following example, any videos/assets whose `[upload-date]` user-defined media field has a value before today will be returned:

```
[upload-date] < today()
```

In the following example, any videos/assets whose `[upload-date]` user-defined media field has a value within the week before today will be returned:

```
[upload-date] > dateAdd(-7, day, today())
```

Auto-Incident Creation Example

In the following example, videos/assets whose `upload-date` user-defined media field has been populated with 24/07/2020 will be added to an incident.

```
[upload-date] = '2020-07-24'
```

In the following example, any videos/assets whose `[upload-date]` user-defined media field has a value within the week before today will be added to an incident:

```
[upload-date] > dateAdd(-7, day, today())
```

Auto-Incident Deletion Example

Incident deletion fields match a date **value**, instead of a specific date. This ensures that the field is always valid, no matter when it was created. In the following example, any incident which is one week old **and** meets the deletion requirements will be deleted:

```
dateAdd(7, day, creationTime)
```

Export Profile Example

In the following example, only incidents which were created from 2020 onwards could use the export profile.

```
case
 when [creation-time] < '2020-01-01' then 'Incidents created before
2020 cannot be exported'
 end
```

In the following example, only incidents whose `[created-on]` user-defined incident field was populated with a date at least 7 days before today could use the export profile:

```
case
 when [created-on] > dateAdd(-7, day, now()) then 'You cannot
export incidents until they are one week old'
 end
```

Computed Field Example

In the following example, the computed field `[review-reminder]` would appear with different text, depending on how the `[date-reviewed]` user-defined incident field had been populated in incidents:

```
 case
  when [date-reviewed] > '2020-01-01' then 'This incident been
reviewed recently.'
  when [date-reviewed] < '2020-01-01' then 'This incident has not
been reviewed in some time, and may need to be reviewed again.'
  end
```

In the following example, the computed field `[review-reminder]` would appear with different text, depending on how the `[date-reviewed]` user-defined incident field had been populated in incidents:

```
 case
  when [date-reviewed] < dateAdd(-7,day,now()) then 'This incident
been reviewed in the past week.'
  when [date-reviewed] > dateAdd(-7,day,now()) then 'This incident
has not been reviewed in the past week'
  end
```

13.5.4 CASE Functions

A CASE function evaluates conditions and returns a value when the **first** condition is met. This behaves the same as the SQL case function.

The syntax is as follows:

```
case
when condition1 then value1
when condition2 then value2
else fallbackValue
end
```

Advanced Incident Search Example

In the following example, any incidents which belong to the logged-in user will be returned if their `[priority-level]` field has been set to `high`. Incidents which do not belong to the logged-in user will be returned if their `[priority-level]` field has been set to `medium`.

```
case
when owner = me() then priority = 'high'
when owner != me() then priority = 'medium'
end
```

Advanced Media Search Example

In the following example, any video/assets which belong to the logged-in user will be returned if their `[priority-level]` field has been set to `high`. Videos/assets which do not belong to the logged-in user will be returned if their `[priority-level]` field has been set to `medium`.

```
case
when owner = me() then priority = 'high'
when owner != me() then priority = 'medium'
end
```

Auto-Incident Creation Example

In the following example, any video/asset would be added to an incident if their `title` field started with `t` **and** their `[ready-for-incident]` field was also checked:

```
case
when title = 't%' and [ready-for-incident] = true then true
end
```

Auto-Incident Deletion Example

In the following example, only incidents whose `title` field started with `t` would only be eligible for deletion:

```
case
when title = 't%' then true
end
```

Export Profile Example

CASE functions are the main mechanism for creating export profile rules.

If the conditions are met and there is an error message, the export profile cannot be selected. In the following example, any incidents whose `[title]` field started with `b` could not use the export profile:

```
case
 when title = 'b%' then 'Exports cannot have a title which begins
with b.'
 end
```

Administrators can use the CASE function's `fallbackValue` to determine what happens to incidents whose user-defined incident fields have **not** been populated in the expected manner. In the following example, **only** incidents whose `[title]` field started with "b" could use the export profile.:

```
case
 when title = 'b%' then ''
 else 'You cannot use this export profile.'
 end
```

Computed Field Example

In the following example, the computed field `[send-email-to-reviewer]` would only appear if the `[reviewer-email]` user-defined incident field had been populated in incidents:

```
case
 when [email] != '' then "mailto:" + encodeURIcomponent([reviewer-
email])
 end
```

The administrator would also need to set ***As Url*** to ***On***. This enables them to set the URL text which users will see:

```
case
 when [email] != '' then 'Send an email to this address'
 else 'No email address set'
 end
```

In the following example, the computed field `[search-location]` would only appear if the `[postcode]` user-defined incident field had been populated in incidents:

```
case
 when [postcode] != '' then "https://www.google.com/search?q=" +
[postcode]
 end
```

The administrator would also need to set ***As Url*** to ***On***. This enables them to set the URL text which users will see:

```
case
 when [postcode] != '' then 'Search for this postcode'
 else 'No postcode selected'
 end
```

13.5.5 Other Search Functions

If a user is performing an advanced incident or media search, they can also utilise the following search-specific functions to locate incidents or media:

- `me()` - this refers to the logged-in user performing the search.
- `ownedByMe()` - this will return incidents or assets which are owned by the logged-in user.
- `supervisedByMe()` - this will return incidents or assets which have been created by users supervised by the logged-in user.
- `isShared()` - this will return incidents or assets which have been explicitly shared with other users on the system, through the ***Sharing*** section.

This will not return incidents which have been automatically shared with other users.

- `isSharedWith('user')` - this will return incidents or assets which have been explicitly shared with the specified user, through the ***Sharing*** section.
- `isOwnedBy()` - this will return incidents or assets which are either owned by the specified user, or a group that the specified user belongs to.

The following functions only apply to advanced incident searches:

- `hasExternalLink()` - this will return incidents which have external access links (including expired links).
- `hasActiveExternalLink()` - this will return incidents which have **live** external access links.

The following functions only apply to advanced media searches (i.e. **not** incident searches):

- `operator` - this returns media whose operator matches the user entered here.

By default, this is whoever recorded the video or imported the asset.

- `mediaType` - this returns media with the same media type as the one specified.

Possible media types are `video`, `audio`, `image`, `pdf`, and `other`.

In the following example, only videos will be returned:

```
mediaType = 'video'
```

- `audioCodec` - this returns videos/assets with the same audio codec as the one specified.

Possible audio codecs are `MP2`, `ULAW`, `ACC`, `MP3`, `PCM_S16LE` and `VORBIS`.

In the following example, only videos/assets which have an MP3 audio codec will be returned:

```
audioCodec = 'MP3'
```

- `videoCodec` - this returns assets with the same video codec as the one specified.

These are `H264`, `MPEG4`, `H265`, and `JPEG`.

In the following example, only videos/assets which have an H624 video codec will be returned:

```
videoCodec = 'H624'
```

All audio codec and video codec properties are case-sensitive.

- `width` - this returns videos/assets whose width in pixels matches the one specified (if applicable).

In the following example, only assets which have a width between 320 pixels and 768 pixels will be returned:

```
width >= 320 and width < 768
```

- `height` - this returns videos/assets whose height in pixels matches the one specified (if applicable).

In the following example, only videos/assets which have a height greater than 740 pixels will be returned:

```
height > 740
```

- `startTime` - this returns videos/assets whose start time matches the one specified.

In the following example, only assets whose start time matches today's date will be returned:

```
startTime = today()
```

*If the start time is not applicable, this will return videos/assets which were **added to VideoManager** on the specified date.*

- `duration` - this returns videos/assets whose duration, in seconds, matches the one specified (if applicable).

In the following example, only videos/assets whose duration is longer than 120 seconds will be returned:

```
duration > 120
```

- `deviceId` - this returns videos which were recorded on the device specified.

In the following example, only videos recorded on the device with an ID *00:c0:d0:00:00:00* will be returned:

```
deviceId = '00:c0:d0:00:00:00'
```

*Users can find a body-worn camera's unique ID by navigating to the **Devices** tab, clicking > **View device info**, and looking at the **Device details** pane. The multi-digit string listed by the **DID** entry is the body-worn camera's ID.*

- `deviceName` - this returns videos/assets which were recorded on the body-worn camera specified. This uses the body-worn camera's serial number instead of its ID. If the asset in question was imported, users can specify the name of the source of the file.

In the following example, only videos recorded on the body-worn camera with the serial number *467632* will be returned.

```
deviceName = '467632'
```

In the following example, only assets imported from the source with the name *LAPTOP-458823* will be returned.

```
deviceName = 'LAPTOP-458823'
```

*Users can edit the body-worn camera name for an asset or video from the **More details** pane.*

>> For more information, see View and Edit Asset Properties on page 37 *and* View and Edit Video Properties on page 27

- `urn` - this returns videos/assets whose URN matches the one specified.

In the following example, only videos/assets with the URN *8e31d1f305792c6d7d68705cee864ae4* will be returned:

```
urn = '8e31d1f305792c6d7d68705cee864ae4'
```

- `filename` - this returns assets whose original filename (as it was imported) matches the one specified.

In the following example, only assets with the filename *example.pdf* will be returned:

```
filename = 'example.pdf'
```

- `actualFilename` - this returns assets whose filename in VideoManager's file spaces matches the one specified.

```
actualFilename = 'example_wGzoSjCWxA_2.pdf'
```

This can be found by navigating to VideoManager's footage file space.

- `fileExtension` - this returns assets whose file extension matches the one specified.

In the following example, only assets with the file extension *jpg* will be returned:

```
fileExtension = 'jpg'
```

- `importsignature` - this returns assets whose import signature matches the one entered here.

In the following example, only assets with the import signature *ystKH9cssC* will be returned:

```
importsignature = 'ystKH9cssC'
```

*This can be found by navigating to the **Status** tab.*

13.6 Appendix F: Customise Export Title Pages

Administrators can customise what information is presented on the title page for an incident clip when it is exported. There are multiple models, all of which correspond to an aspect of the export. To customise the title page, ensure that ***Use Template for Title Page*** has been set to ***On***.

Basic Syntax

The syntax to be used with the customisable export title page is as follows:

- `#list` - this is necessary if a field can have multiple values (e.g. an incident can have multiple bookmarks).

Administrators can also use `![]` with the `#list` function, if a field with multiple values can be absent in some exports but present in others (e.g. an incident may not have any bookmarks).

- `#if` - this is necessary if a field can have a null value (e.g. an incident may not necessarily have bookmarks).
- `?string` - this is necessary if a field has a yes/no value.
- `?datetime` - this formats a value as a datetime value (e.g. 20/03/21, 11:02:01).
- By default, VideoManager will present timestamp fields with both a date **and** time value. Alternatively, administrators can specify whether only one value is presented, using the following syntax:
  - `?date` - this presents a date value (e.g. 20/03/21).
  - `?time` - this presents a time value (e.g. 11:02:01).

The information is presented in two columns: by default, the first one is the name of the row, and second one is the row's value.

The models which can be used with this syntax are as follows:

- Incident model - this provides information about incidents in the export.

>> For more information, see Incident Model on page 486

- Incident clip model - this provides information about incident clips in the incident which is being exported.

>> For more information, see Incident Clip Model on page 488

- User-defined incident fields and user-defined media fields model - this provides information about fields in the incident which is being exported.

>> For more information, see User-Defined Incident Fields and User-Defined Media Fields Model on page 489

- Export job model - this provides information about the export job itself.

>> For more information, see Export Job Model on page 495

- Bookmark model - this provides information about the bookmarks in the incident clips **and** incidents which are being exported.

>> For more information, see Bookmark Model on page 496

13.6.1 Incident Model

This model contains information about the incident which is being exported. The fields must be wrapped in curly brackets, and preceded by `incident.`. Potential fields are as follows:

- `${id}` - VideoManager's internal incident ID.
- `${creationTimeStamp}` - when the incident was created.

This field can optionally use `?date` or `?time` syntax.

```
${incident.creationTimeStamp?date}
```

```
${incident.creationTimeStamp?time}
```

- `${editTimeStamp}` - when the incident was last edited.

This field can optionally use `?date` or `?time` syntax.

```
${incident.editTimeStamp?date}
```

```
${incident.editTimeStamp?time}
```

- `${deletionTimeStamp}` - if applicable, when the incident was deleted.

This field can optionally use `?date` or `?time` syntax.

```
${incident.deletionTimeStamp?date}
```

```
${incident.deletionTimeStamp?time}
```

- `${clipCount}` - the number of incident clips in the incident.
- `${signature}` - the incident's signature, which is automatically generated by VideoManager upon creation.
- `${displaySignature}` - the incident's display signature, which may be different from its `${signature}` if it is a child incident in an incident collection.
- `${basestationID}` - the basestation ID of the VideoManager where this incident was created.
- `${owner}` - the owner of the incident. By default, this is the user who created this incident, but administrators can also manually change the owner of an incident.
- `${location}` - the latitude and longitude of the incident, if a location has been set.
- `${isIncidentCollection()}` - whether this incident is an incident collection (i.e. a parent incident containing other incidents).

This field must use `?string` syntax.

```
${incident.isIncidentCollection()?string('yes','no')}
```

- `${isWithinIncidentCollection()}` - whether this incident is part of an incident collection (i.e. a child incident).

This field must use `?string` syntax.

```
${incident.isWithinIncidentCollection()?string('yes','no')}
```

13.6.2 Incident Clip Model

This model corresponds to information about the incident clips which are being exported. The values must be wrapped in curly brackets, and preceded by `clip.`. Potential fields are as follows:

- `${device}` - the device which recorded the incident clip.
- `${startTimeStamp}` - the incident clip start time.

This field can optionally use `?date` or `?time` syntax.

```
${clip.startTimeStamp?date}
```

```
${clip.startTimeStamp?time}
```

- `${endTimeStamp}` - the incident clip end time.

This field can optionally use `?date` or `?time` syntax.

```
${clip.endTimeStamp?date}
```

```
${clip.endTimeStamp?time}
```

- `${notes}` - any notes about the incident clip.
- `${creationTimeStamp}` - when the incident clip was added to the incident.

This field can optionally use `?date` or `?time` syntax.

```
${clip.creationTimeStamp?date}
```

```
${clip.creationTimeStamp?time}
```

- `${editTimeStamp}` - when the incident clip was last edited (e.g. redacted, or clipped further).

This field can optionally use `?date` or `?time` syntax.

```
${clip.editTimeStamp?date}
```

```
${clip.editTimeStamp?time}
```

- `${mediaType}` - whether the incident clip is an MP4, PDF, JPG, etc.

13.6.3 User-Defined Incident Fields and User-Defined Media Fields Model

Using the `customfields` function, administrators can display information about the exported incident's user-defined incident fields, and the exported videos' user-defined media fields. This requires use of the `#list` function, and optionally the `#if` function (if the fields can be left empty).

User-Defined Incident Fields and User-Defined Media Fields Syntax

Firstly, the administrator must decide which user-defined incident fields and user-defined media fields will be included in the template.

To include **all** user-defined incident fields in the template, regardless of whether they have been populated in the incident:

```
<#list incident.customFields?keys as key>
 <#assign field = incident.customFields[key]>
 | EXAMPLE COLUMN NAME : | EXAMPLE COLUMN VALUE |
 </#list>
```

To include **only** user-defined incident fields which have been populated in the template:

```
<#if incident.customFields["custom-field-name"]??>
 <#assign field = incident.customFields["custom-field-name"]>
 | EXAMPLE COLUMN NAME : | EXAMPLE COLUMN VALUE |
 </#if>
```

The syntax is the same for user-defined media fields, but requires use of an additional `#list` function:

```
<#list clip.videoFiles as video>|
 <#list video.customFields?keys as key> <#assign field =
video.customFields[key]>>
 | EXAMPLE COLUMN NAME : | EXAMPLE COLUMN VALUE |
 </#list>
 </#list>
```

```
<#list clip.videoFiles as video>|
 <#if video.customFields["custom-field-name"]??> <#assign field =
video.customFields["custom-field-name"]>
 | EXAMPLE COLUMN NAME : | EXAMPLE COLUMN VALUE |
 </#if>
 </#list>
```

User-Defined Field and User-Defined Media Field Values

Once the administrator has configured the template, they can use the following values to present information about their user-defined incident fields or user-defined media fields:

- `${value}` - the value of the custom field.

```
<#if incident.customFields["custom-field-name"]??> <#assign
field = incident.customFields["custom-field-name"]>
 | ${field.name} : | ${field.value.text} |
 </#if>
```

- `${name}` - the custom field's identifier.

```
<#if incident.customFields["custom-field-name"]??> <#assign
field = incident.customFields["custom-field-name"]>
 | Name : | ${field.name} |
 </#if>
```

- `${displayName}` - the custom field's display name.

```
<#if incident.customFields["custom-field-name"]??> <#assign
field = incident.customFields["custom-field-name"]>
 | Name | ${field.displayName} |
 </#if>
```

- `${isText}` - whether the custom field is a text field or not.

This field must use `?string` syntax.

```
<#if incident.customFields["custom-field-name"]??> <#assign
field = incident.customFields["custom-field-name"]>
 | ${field.name} : | ${field.isText?string('yes','no')} |
 </#if >
```

- `${isDate}` - whether the custom field is a date field or not.

This field must use `?string` syntax.

```
<#if incident.customFields["custom-field-name"]??> <#assign
field = incident.customFields["custom-field-name"]>
 | ${field.name} : | ${field.isDate?string('yes','no')} |
 </#if>
```

- `${isTimestamp}` - whether the custom field is a timestamp or not.

This field must use `?string` syntax.

```
<#if incident.customFields["custom-field-name"]??> <#assign
field = incident.customFields["custom-field-name"]>
 | ${field.name} : | ${field.isTimestamp?string('yes','no')} |
 </#if>
```

- `${isBool}` - Whether the custom field is a check box field or not.

This field must use `?string` syntax.

```
<#if incident.customFields["custom-field-name"]??> <#assign
field = incident.customFields["custom-field-name"]>
 | ${field.name} : | ${field.isBool?string('yes','no')} |
 </#if >
```

- `${mandatory}` - whether the custom field is mandatory (i.e. the user cannot save the incident unless they have populated the field).

This field must use `?string` syntax.

```
<#if incident.customFields["custom-field-name"]??> <#assign
field = incident.customFields["custom-field-name"]>
 | ${field.name} | ${field.mandatory?string('yes','no')} |
 </#if>
```

- `${fieldType}` - the user-defined incident field's type. This could be `USER_DEFINED`, `OWNER`, `CREATION_TIME`, `UPDATE_TIME`, `SIGNATURE`, or `CLIP_COUNT`.

```
<#list incident.customFields?keys as key>
 <#assign field = incident.customFields[key]>
 | ${field.name} : | ${fieldType} |
 </#list>
```

- `${purpose}` - the custom field's purpose. This could be `INCIDENT`, `INCIDENT_DELETE`, `MEDIA`, `CC_VAULT`, or `PLAYBACK_REASON`.

```
<#list incident.customFields?keys as key>
 <#assign field = incident.customFields[key]>
 | ${field.name} : | ${purpose} |
 </#list>
```

- `${derived}` - whether the custom field value is dynamically calculated from other information (e.g. a computed field).

This field must use `?string` syntax.

```
<#if incident.customFields["custom-field-name"]??> <#assign
field = incident.customFields["custom-field-name"]>
 | ${field.name} : | ${field.derived?string('yes','no')} |
 </#if >
```

- `${defaultValue}` - the default value of the custom field, if nothing else is entered.

```
<#list incident.customFields?keys as key>
 <#assign field = incident.customFields[key]>
 | ${field.name} : | ${defaultValue} |
 </#list>
```

- `${deleted}` - whether custom field has been deleted from VideoManager or not.

This field must use `?string` syntax.

```
<#if incident.customFields["custom-field-name"]??> <#assign
field = incident.customFields["custom-field-name"]>
 | Has ${field.name} been deleted? : | ${field.deleted?string
('yes','no')} |
 </#if >
```

- `${permissionGroup}` - The access group that users must belong to in order to view and edit this user-defined incident field. This could be `0` (i.e. public), `ONE`, `TWO`, etc.

```
<#list incident.customFields?keys as key>
 <#assign field = incident.customFields[key]>
 | What is the permission group for ${field.name}? : |
${permission} |
 </#list>
```

13.6.4 Video Model

This model corresponds to information about the videos which are being exported. (i.e. the videos' properties on VideoManager, separate from the incident clips' properties). The values must be wrapped in curly brackets. This requires use of the `#list` function.

Video Syntax

To present information about videos, administrators must use `#list` syntax:

```
<#list clip.videoFiles as video>
 | EXAMPLE COLUMN NAME | EXAMPLE COLUMN VALUE |
</#list >
```

Video Values

- `${device}` - the device used to record the video.

```
<#list clip.videoFiles as video>
 | Device : | ${video.device} |
 </#list >
```

- `${name}` - the name of the file as stored on VideoManager's server.

```
<#list clip.videoFiles as video>
 | Name : | ${video.name} |
 </#list >
```

- `${originalName}` - the original file name. This will be different from the `${name}` if the video is an asset which has been imported from an external source.

```
<#list clip.videoFiles as video>
 | Name : | ${video.originalName} |
 </#list >
```

- `${recordingStartTimeStamp}` - when the recording that this video belongs to was started.

This field can optionally use `?date` or `?time` syntax.

```
<#list clip.videoFiles as video>
 | Time : | ${video.recordingStartTimeStamp} |
 </#list >
```

- `${startTimeStamp}` - the start time of the video. This may be different from `${recordingStartTimeStamp}` if the recording was split into multiple videos.

This field can optionally use `?date` or `?time` syntax.

```
<#list clip.videoFiles as video>
 | Time : | ${video.startTimeStamp} |
 </#list >
```

- `${endTimeStamp}` - the end time of the video. This may be different from `${recordingStartTimeStamp}` if the recording was split into multiple videos.

This field can optionally use `?date` or `?time` syntax.

```
<#list clip.videoFiles as video>
 | Time : | ${video.endTimeStamp} |
 </#list >
```

- `${isPreRecording()}` - whether pre-record was enabled for this video.

This field must use `?string` syntax.

```
<#list clip.videoFiles as video>
 | Was this pre-recorded? : | ${video.isPreRecording()?string
('yes','no')} |
 </#list >
```

- `${duration}` - the duration of the video, in seconds.
- `${operator}` - the operator of the video. By default, this is the user who recorded it.
- `${deletionTimeStamp}` - if applicable, when the video was deleted.

This field can optionally use `?date` or `?time` syntax.

```
<#list clip.videoFiles as video>
 | Time : | ${video.deletionTimeStamp?date} |
 </#list >
```

- `${deletionRequestTimeStamp}` - the requested time of deletion, if the deletion policy has been configured to keep videos after a user has requested them to be deleted.

This field can optionally use `?date` or `?time` syntax.

```
<#list clip.videoFiles as video>
 | Time : | ${video.deletionRequestTimeStamp?time} |
 </#list >
```

- `${recordingIdentifier}` - the recording identifier.
- `${indexInRecording}` - the index (i.e. position) of this video within the recording.

If the recording only consists of this video, the value will be `0`.

- `${downloadTimeStamp}` - when this video was downloaded to VideoManager from a body-worn camera, or imported as external media.

This field can optionally use `?date` or `?time` syntax.

- `${editTimeStamp}` - when the video was last edited.

This field can optionally use `?date` or `?time` syntax.

- `${frameWidth}` - the frame width of this video.
- `${frameHeight}` - the frame height of this video.
- `${videoCodec}` - the video codec of this video.
- `${audioCodec}` - the audio codec of this video.

- `${urn}` - the unique resource identifier of this video.
- `${owner}` - the owner of the video.
- `${restricted}` - whether the video is restricted.

This field must use `?string` syntax.

```
<#list clip.videoFiles as video>
 | Was this pre-recorded? : | ${video.restricted?string
('yes','no')} |
 </#list >
```

- `${size}` - the size in bytes of the video.
- `${customFields}` - the set of user-defined media fields, if any.
- `${location}` - the latitude and longitude of the video, if the body-worn camera which recorded it was GPS-enabled.
- `${exportOriginalFileName}` -
- `${exportConvertedFileName}` -

13.6.5 Export Job Model

This model corresponds to information about the export itself. The values must be wrapped in curly brackets, and preceded by `exportJob.`. Potential fields are as follows:

- `${description}` - the title of the export.

```
${exportJob.description}
```

- `${signature}` - the unique signature of the export, automatically generated by VideoManager upon creation.

```
${exportJob.signature}
```

- `${jobCreationTimeStamp}` - when the export job started.

This field **must** use `?datetime`, `?date` or `?time` syntax.

```
${exportJob.jobCreationTimeStamp?datetime}
```

```
${exportJob.jobCreationTimeStamp?date}
```

```
${exportJob.jobCreationTimeStamp?time}
```

- `${owner}` - who created the export.

```
${exportJob.owner}
```

If the administrator previews a template featuring these fields, the values will all be presented as `example`.

13.6.6 Bookmark Model

This model contains information about bookmarks included in either the incident (which have been manually added on VideoManager) or individual videos within the incident (which were added in the field by the body-worn camera that recorded it).

Bookmark Syntax

Firstly, the administrator must decide which bookmarks will be included in the template.

To present information about an incident's bookmarks, administrators must use `#list` syntax, and optionally `![]` (if not all incidents have bookmarks).

```
<#list incident.bookmarks![] as bookmark >
 | EXAMPLE COLUMN NAME : | EXAMPLE COLUMN VALUE |
</#list>
```

To present information about an individual video's bookmarks, administrators must first use `#list` syntax to list the videos. They must then use `#list` syntax to list the bookmarks, and optionally `![]` (if not all videos have bookmarks).

```
<#list clip.videoFiles as video >
<#list video.bookmarks![] as bookmark >
 | EXAMPLE COLUMN NAME : | EXAMPLE COLUMN VALUE |
</#list>
</#list>
```

Bookmark Values

Once the administrator has configured the template, they can use the following values to present information about their bookmarks:

`name` - the name of the bookmark. The default name of the bookmark depends on whether it was added on VideoManager as part of an incident, or it was added in the field by a body-worn camera:

- If the bookmark was created once the video had been added to an incident, the default bookmark name is the time and date it refers to in the incident.
- If the bookmark was created in the field by the body-worn camera, the default bookmark name is the time it refers to in the video.

- `startTime` - when the bookmark was placed in the video or incident clip.

This field **must** use `?datetime`, `?date` or `?time` syntax.

```
${bookmark.startTime?date}
```

```
${bookmark.startTime?time}
```

```
${bookmark.startTime?datetime}
```

13.7 Appendix G: Profiles Hierarchy

When a body-worn camera is assigned, the device profiles and WiFi profiles it takes are defined by parallel hierarchies.

One hierarchy defines which WiFi profile is chosen for the body-worn camera to use, and which networks within that profile will be used for streaming.

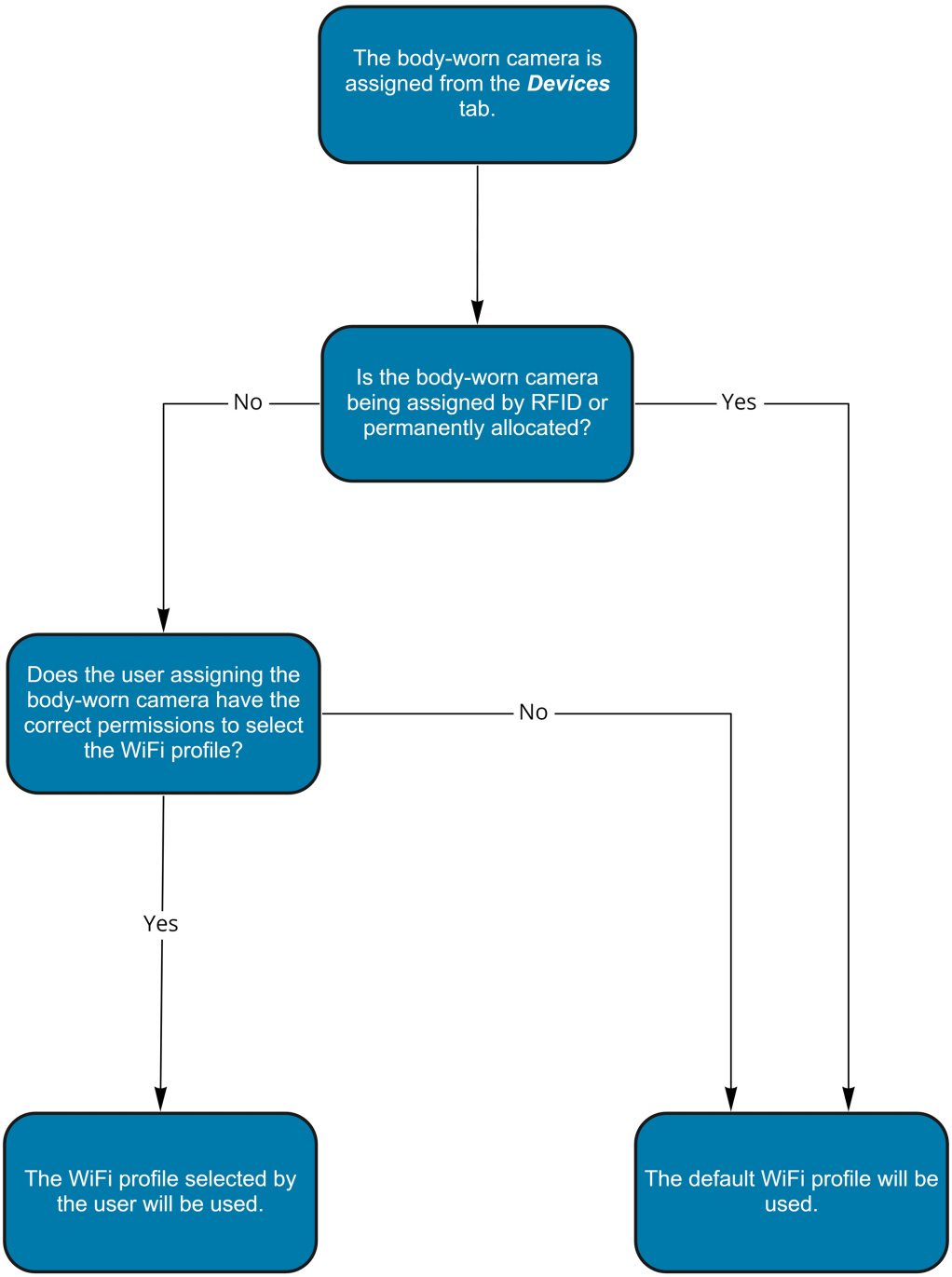
>> For more information, see WiFi Profiles Hierarchy on page 498

One hierarchy defines which device profile is chosen for the body-worn camera to use.

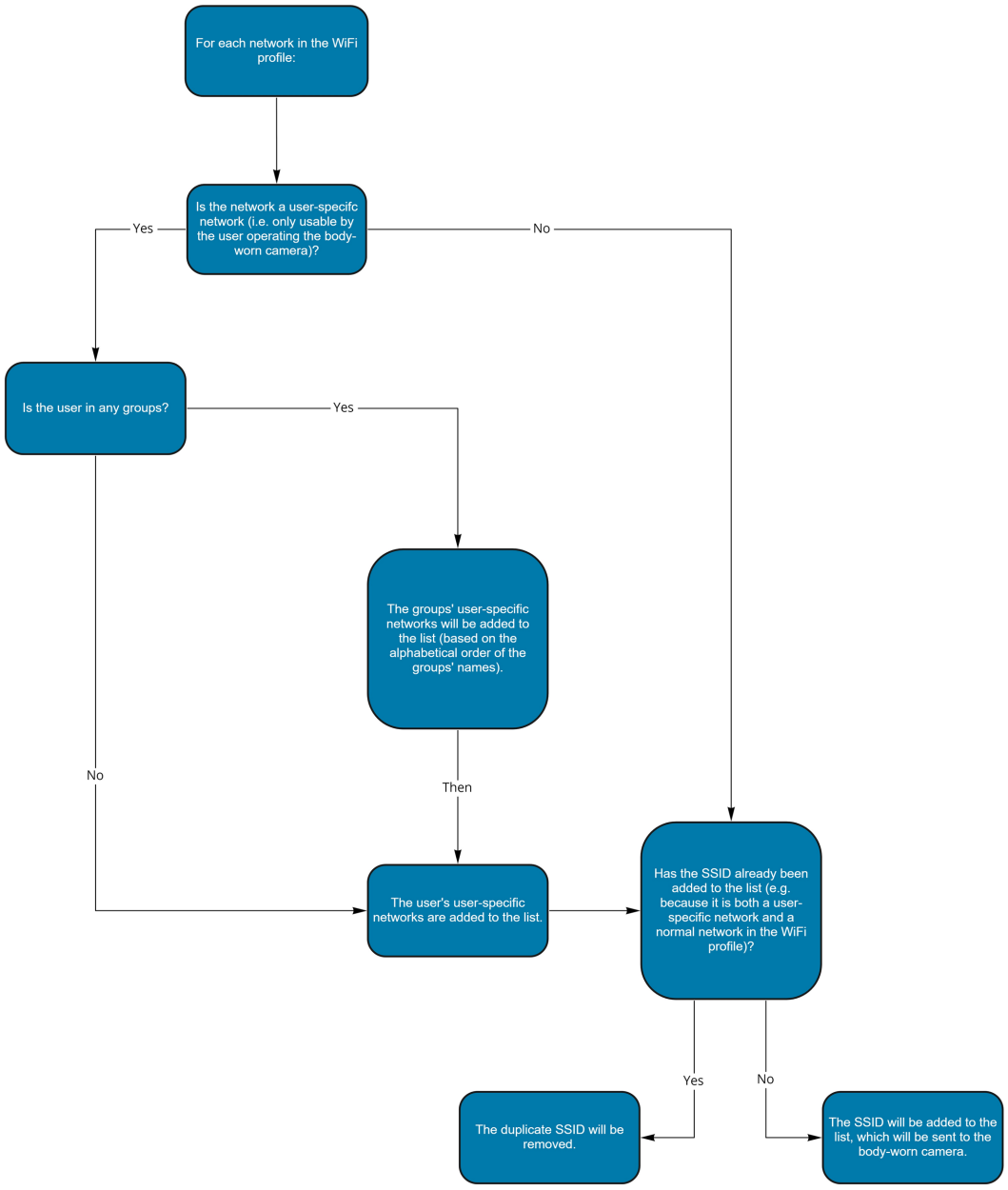
>> For more information, see Device Profiles Hierarchy on page 500

13.7.1 WiFi Profiles Hierarchy

The following flowchart demonstrates how VideoManager determines which WiFi profile will be chosen when a user assigns a VB-series camera or VT-series camera.

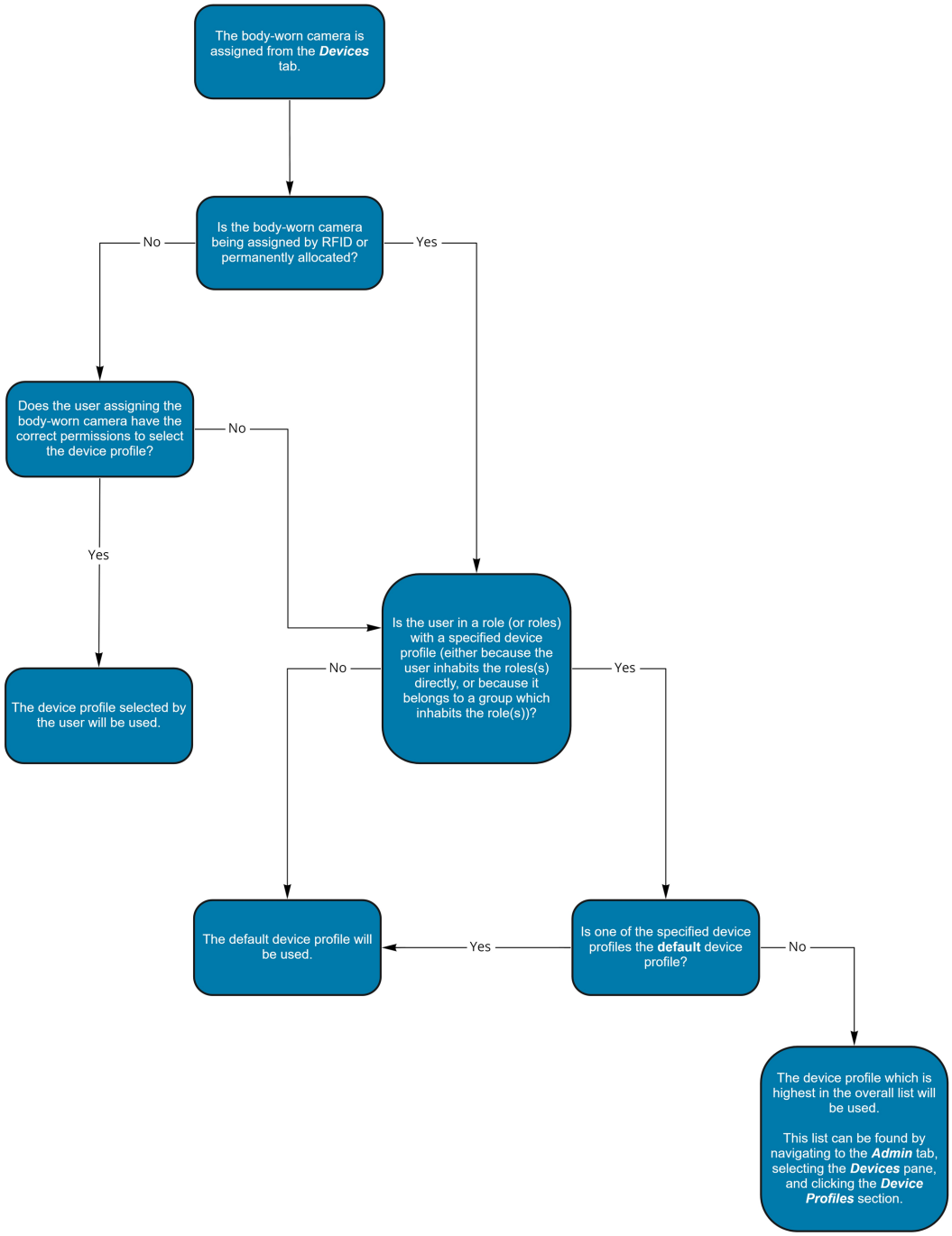


The following flowchart demonstrates how VideoManager determines which individual networks the VB-series camera or VT-series camera will have access to.



13.7.2 Device Profiles Hierarchy

The following flowchart demonstrates how VideoManager determines which device profile will be chosen when a user assigns a body-worn camera.



14 Glossary

A

Access Control Key
The security mechanism that prevents unauthorised body-worn cameras from connecting to VideoManager - 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.

Access Group
Access groups determine which user-defined incident fields, user-defined media fields, and saved searches users can see. There are twenty.

Advanced Settings File
A section in the Admin tab which allows users to modify their VideoManager service in a very precise manner (only with recommendation from Motorola Solutions).

Alternate Password Complexity
A second set of rules that users must adhere to when creating a password, instead of the primary password rules. This is useful if administrators should have more complex passwords than normal users on the system.

Asset
Any non-video import to VideoManager. This could be a PDF, a still image, or an audio file.

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 videos, 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.

Bluetooth Peripheral
A device which sends a notification to body-worn cameras when a change in state is detected (e.g. a gun is unholstered). Administrators can configure body-worn cameras to start recording when they receive this notification. For more information, please contact Technical Support and ask for the technical paper "Personal Issue Yardarm Holster Aware Sensors Explained [ED-009-038]" or "Pool Issue Yardarm Holster Aware Sensors Explained [ED-009-070]".

Bookmark
This draws attention to a specific part of a video. It can be created by the body-worn camera which is recording the video in the field, if the operator presses a configured button. Alternatively, users can add bookmarks to a video in an incident, once the video has been downloaded to VideoManager.

C

Central VideoManager
An instance of VideoManager which acts as a "hub", to which other instances of VideoManager (known as sites) can connect, in order to pass on their footage and metadata.

D

Dashboard
VideoManager'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.

Deletion Policy
A rule which determines whether old footage is deleted from VideoManager automatically, and how long footage is kept for before it can be deleted.

Device
Motorola Solutions equipment which has been associated with VideoManager (e.g. body-worn cameras, DockControllers).

Device Affinity
This is created when a body-worn camera is assigned to a user with single issue (either with RFID or through VideoManager), and the user then redocks the body-worn camera mid-way through their shift. VideoManager will remember the connection, allowing the user to undock the same body-worn camera later in the shift.

Display Name
The name of a user that will be presented to others on the VideoManager system - this is not necessarily the same as a username.

DockController
A device which converts the videos 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 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 to the user's PC. A version of the incident will remain on VideoManager.

I

Incident
A collection of evidence - such as footage, notes, and users - which can be exported or shared with people outside of VideoManager. In some lines of work, this is known as an exhibit or event.

Incident Clip
Any video which has been added to an incident.

L

Licence
Some features on VideoManager are not available unless a licence has been obtained from Motorola Solutions. Such features include assisted redaction, Tactical VideoManager, and ONStream.

M

Media
Any videos or assets which can be added to an incident for evidential purposes.

O

ONStream
A licensed feature from Motorola Solutions which enables body-worn cameras to send a live stream to VideoManager over WiFi.

Operator
By default, this is the user who recorded the video on a body-worn camera, or imported the asset into VideoManager (either manually, or as configured in an automatic import profile).

Owner of a Video/Asset
This is the user who has administrative control over a video/asset. By default, this is the user who recorded the video on a body-worn camera, or imported the asset into VideoManager (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

Peer-Assisted Recording (PAR)
The mechanism which, when one body-worn camera starts recording, will notify other body-worn cameras in the vicinity that a recording has started, via Bluetooth Low Energy (BLE). This allows the receiving body-worn camera to also start recording, if applicable.

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.

Post-record
The video immediately following an event which is captured automatically, once the operator stops recording. This could be between 1 and 120 seconds.

Pre-record
The video 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 videos 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 videos (due to the device profile of the body-worn camera that recorded it), these videos will all have the same recording ID.

Remote Devices
Body-worn cameras which are connected to a site, and can still be configured like normal from the Central VideoManager.

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 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 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.

Site
An instance of VideoManager which connects to another instance of VideoManager (known as a "Central VideoManager"), in order to pass on its footage and metadata.

System Administrator
A role which cannot be edited or deleted. Any users with this role will be able to access any aspect of VideoManager.

T

Two Factor Authentication
Another layer of security on VideoManager - it prompts users to enter a code provided to them by an authenticator app, as well as a password, when logging in.

U

User
Every individual on an instance of VideoManager must have their own user.

User-Defined Field
A manually-created field which helps to filter/categorise incidents in a more advanced manner.

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 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 over a WiFi network.

Video
A section of a recording, the length of which is determined by the body-worn camera's device profile.

Video ID
A unique ID that identifies a specific video/asset. It is used in the audit log to record which video/asset an entry refers to, and can be used to locate videos/assets.

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 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 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 over these networks.

For more information, please visit: www.motorolasolutions.com.

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

Availability is subject to individual country law and regulations. All specifications shown are typical unless otherwise stated and are subject to change without notice. MOTOROLA, MOTO, MOTOROLA SOLUTIONS and the Stylized M Logo are trademarks or registered trademarks of Motorola Trademark Holdings, LLC and are used under license.

© 2015 - 2021 Motorola Solutions, Inc. All rights reserved. (ED-012-221-11)

MOTOROLA SOLUTIONS