MOTOROLA SOLUTIONS

VideoManager Admin Guide

System Release 24.4

NOVEMBER 2024

MN010887A01-AE

Intellectual Property and Regulatory Notices

Copyrights

The Motorola Solutions products described in this document may include copyrighted Motorola Solutions computer programs. Laws in the United States and other countries preserve for Motorola Solutions certain exclusive rights for copyrighted computer programs. Accordingly, any copyrighted Motorola Solutions computer programs contained in the Motorola Solutions products described in this document may not be copied or reproduced in any manner without the express written permission of Motorola Solutions.

No part of this document may be reproduced, transmitted, stored in a retrieval system, or translated into any language or computer language, in any form or by any means, without the prior written permission of Motorola Solutions, Inc.

Trademarks

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.

License Rights

The purchase of Motorola Solutions products shall not be deemed to grant either directly or by implication, estoppel or otherwise, any license under the copyrights, patents or patent applications of Motorola Solutions, except for the normal nonexclusive, royalty-free license to use that arises by operation of law in the sale of a product.

Open Source Content

This product may contain Open Source software used under license. Refer to the product installation media for full Open Source Legal Notices and Attribution content.

European Union (EU) and United Kingdom (UK) Waste of Electrical and Electronic Equipment (WEEE) Directive

The European Union's WEEE directive and the UK's WEEE regulation require that products sold into EU countries and the UK must have the crossed-out wheelie bin label on the product (or the package in some cases). As defined by the WEEE directive, this crossed-out wheelie bin label means that customers and end users in EU and UK countries should not dispose of electronic and electrical equipment or accessories in household waste.

Customers or end users in EU and UK countries should contact their local equipment supplier representative or service center for information about the waste collection system in their country.

Disclaimer

Please note that certain features, facilities, and capabilities described in this document may not be applicable to or licensed for use on a specific system, or may be dependent upon the characteristics of a specific mobile subscriber unit or configuration of certain parameters. Please refer to your Motorola Solutions contact for further information.

Contact Us

The Centralized Managed Support Operations (CMSO) is the primary contact for technical support included in your organization's service agreement with Motorola Solutions. To enable faster response time to customer issues, Motorola Solutions provides support from multiple countries around the world.

Service agreement customers should be sure to call the CMSO in all situations listed under Customer Responsibilities in their agreement, such as:

- To confirm troubleshooting results and analysis before taking action

Your organization received support phone numbers and other contact information appropriate for your geographic region and service agreement. Use that contact information for the most efficient response. However, if needed, you can also find general support contact information on the Motorola Solutions website, by following these steps:

1. Enter motorolasolutions.com in your browser.
2. Ensure that your organization's country or region is displayed on the page. Clicking or tapping the name of the region provides a way to change it.
3. Select "Support" on the motorolasolutions.com page.

Comments

Send questions and comments regarding user documentation to documentation@motorolasolutions.com.

Provide the following information when reporting a documentation error:

- The document title and part number
- The page number or title of the section with the error
- A description of the error

Motorola Solutions offers various courses designed to assist in learning about the system. For information, go to https://learning.motorolasolutions.com to view the current course offerings and technology paths.

Document History

Version	Description	Date
MN010887A01-AA	Initial version of the *VideoManager Admin Guide*.	May 2024
MN010887A01-AB	The following sections were updated: • Network Tab on page 359 • Network Tab on page 363 • Recording Tab on page 355 • General Tab on page 354 • General Tab on page 360 • Device Permissions on page 332 • Configuring Video Metadata Overlay Settings on page 167 • Performing Actions on the Tactical Tab on page 133 • Viewing Sites on page 127 The following sections were added: • V500 Device Profile on page 364 • Configuring ONStream on page 175 • Enabling ONStream on page 175 • Configuring ONStream Settings on page 175 • Creating and Resetting Outputs on page 177 • Creating APNs on page 183 • Importing and Exporting a Streaming Server Configuration on page 186 • Adding Your M500 to VideoManager on page 106 • Moving an M500 to a New Vehicle on page 113 • Creating a Group for Use with the M500 on page 147 • Setting an In-Vehicle Administrator Password on page 173 • Performing Vehicle Network Profile Actions on page 181 • Incident Fields and Rules Configuration for the M500 on page 233 • Media Fields Configuration for the M500 on page 247	July 2024
MN010887A01-AC	The following sections were updated:	July 2024

Version	Description	Date
	• General Tab on page 354 • Device Tab on page 354 • Recording Tab on page 355 • Importing and Deleting Licences on page 286 • Performing Camera Actions on page 115	
MN010887A01-AD	The following section was added: • Assisted Redaction Editor on page 69 with all its subsections The following sections were updated: • Incident Permissions on page 328 • Searching Cameras on page 107 • Other Redactions on page 65 • Changing Viewing Options on page 39	August 2024
MN010887A01-AE	The following sections have been updated: • Configuring Mobile App Settings on page 258 • V500 Device Profile on page 364 • Incident Permissions on page 328 • Creating DVD Export Profiles on page 199 • Creating MP4 Export Profiles on page 200 • Creating Evidence Export Profiles on page 202 • Sharing Incidents Externally Using an Export on page 85 • Types of Reports on page 370 • Other Redactions on page 65 • Media Permissions on page 325 • Configuring the Playback Policy on page 257 • Match Date Operators and Values on page 384 • Other Search Functions on page 388 The following sections have been added: • Configuring Playback Watermarks on page 257 • Accessing the Redaction Settings on page 68	November 2024

Contents

List of Figures

List of Tables

List of Processes

List of Procedures

Chapter 1

Welcome to VideoManager

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

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

Chapters are arranged by the corresponding tabs on VideoManager (**Media**, **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, which 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, you may not have sufficient permissions to do so. If this is the case, contact Motorola Solutions support or speak to your system administrator for further instructions.

Chapter 2

Initial Configuration

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

The procedure for downloading differ, depending on whether VideoManager is being downloaded for the first time, or being re-downloaded, for example, to obtain a newer version of the software.

2.1 Installing VideoManager

Perform the following procedure if this is the first time that VideoManager is being installed on the PC.

Prerequisites: Ensure that you have a valid VideoManager licence, including Software Assurance. The licence you require depends on what features and devices you wish to use with VideoManager.
To obtain licensing, contact edesixsales@motorolasolutions.com.

Procedure:

1. Go to https://www.motorolasolutions.com/en_xu/video-security-access-control/videomanager/downloads.html and click **Download VideoManager**.
2. Double-click the downloaded installation file.
3. Confirm that the installer can make changes to the PC.

   The VideoManager installer opens.
4. In the **VideoManager** installer window, click **Next**.
5. Choose the destination where you want VideoManager to be installed and click **Install**.

   VideoManager is downloaded.
6. Click **Finish**.

   Multiple installers open.
7. Click through every installer by clicking **Next** and **Finish**.
8. Navigate to the installation location of VideoManager and click `pss.exe`.

   The web UI opens.
9. Click **Set Up**.
10. Read the licence agreement and click **Accept**.
11. Choose where you want users, groups, and incidents to be stored by performing one of the following actions:
    - If you want all users, groups, incidents, and other VideoManager data to be stored in the default database of VideoManager, select **Use built-in database server (recommended)**.
    - If there is an existing SQL Server, connect it to VideoManager by selecting **Use external SQL Server database (advanced)** and enter the following information:

Name	Description
Server name	The name of the administrator's SQL Server

Name	Description
	To find this information, open the Microsoft SQL Server Management Studio. The log-in pane displays the SQL Server name in the **Server name** field.
Port number	The port number of the SQL Server To find this information, open the SQL Server Configuration Manager, select **SQL Server Network Configuration**, click **Protocols for SQLEXPRESS**, and then **TCP/IP**. Navigate to the **IP Addresses** tab and scroll down to **IPAll**. The port number is in the **TCP Port** field.

Database name	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_SNAP`
	`SHOT_ISOLATION ON;`
	`ALTER DATABASE pss SET READ_COMMIT`
	`TED_SNAPSHOT ON;`
	`GO`
	To finish, click **Execute**.
	The database is 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**, delete `integratedSecurity=true;` and replace it with the following information: `username=<USERNAME>;password=<PASSWORD>` For more information about setting up an SQL server with VideoManager, you can navigate to the Motorola Solutions Learning Experience Portal (registration is free) and search for *VideoManager and SQL Server Explained*.

You can click **Test connection** to verify the configuration. If successful, a green message box reading `Connection Established` appears. Otherwise, an error appears.

You must click **Confirm configure VideoManager with these settings**.

VideoManager restarts running against external postgres server, and is ready to complete setup.

12. When you are prompted to create a VideoManager administrator user, enter a username and password, and re-enter the password to confirm.

13. To save, click **Confirm**.

    You are prompted to configure where your media will be sent initially.

14. If you want all footage to automatically be encrypted when stored by VideoManager, set **Encrypt Footage** to **On**.
15. In the **Storage Location** field, enter the path to which all media should be sent.

    This can be changed later. For more information, see Performing File Spaces Actions on page 278.
16. Click **Confirm**.

    You are automatically logged on to VideoManager and you can start using the system.

2.2 Re-Installing VideoManager

Perform the following procedure if VideoManager has previously been installed on the PC.

Prerequisites: Ensure that you have a valid VideoManager licence, including Software Assurance. The licence you require depends on what features and devices you wish to use with VideoManager.
To obtain licensing, contact edesixsales@motorolasolutions.com.

Procedure:

1. Go to https://www.motorolasolutions.com/en_xu/video-security-access-control/videomanager/downloads.html and click **Download VideoManager**.
2. Double-click the downloaded installation file.
3. Confirm that the installer can make changes to the PC.

   You are asked to uninstall the outdated version of VideoManager. This action does **not** delete your database, as long as you are upgrading to a newer version.

4. Click **Yes** and then **Uninstall**.

   The VideoManager installer opens.

5. In the **VideoManager** installer window, click **Next**.
6. Choose the destination where you want VideoManager to be installed and click **Install**.

   VideoManager is re-installed.

7. Click **Finish**.

   Multiple installers open.

8. Click through every installer by clicking **Next** and **Finish**.
9. Launch the web UI interface like normal.

   NOTE: It may take a few moments for VideoManager to load after being updated. If VideoManager does not open the first time, you should refresh your browser.

10. Log on as **recorderadmin** or a previously created administrator.

    If logging on as **recorderadmin**, you are immediately asked to set and confirm a new password. If **recorderadmin** was previously disabled, it has now been deleted.

Chapter 3

Home

When you log on, the first tab you see is your **Home** tab. This section provides a summary of the information and media available to you on VideoManager.

The following information is displayed:

Name	Description
Videos scheduled to be deleted within *<0>* days	The pane lists all media files owned by the logged-in user, which are scheduled to be deleted within a certain time frame, as dictated by the deletion policy. The pane is only visible if the logged-in user is in a role, which has the **View media scheduled to be deleted on dashboard** permission enabled. For more information, see Configuring Deletion Policies on page 193.
Recent media	The pane gives details about the media files most recently downloaded from a camera. You can navigate to a chosen media file for more details and editing functions.
Recently edited incidents	The pane gives details about the most recently created and edited incidents. You can navigate to a chosen incident for more details and editing functions.
Devices	The pane shows which cameras have been assigned to the current user. You can create a QR code configuration for VT-series cameras by clicking **Generate device config code**. For more information, see Connecting VT-Series Cameras to VideoManager Remotely on page 97.
User-specific WiFi networks	The pane shows any user-specific WiFi networks belonging to the user. You can also add a new user-specific WiFi network by clicking **Add network**.
Notifications	The pane shows a list of event notifications from VideoManager. You can click **Clear** to dismiss notifications. **NOTE:** When the number of notifications reaches 99, you will not see any more notifications until you clear some existing ones. Possible notifications are as follows:

Name	Description
	• **<0> media shared with you** – Media has been shared with the logged-in user or the logged-in user's group. You can click **View** to see the media, which has been shared. • **<0> media now owned by you** – An **Owner** field of the media file has been changed to the logged-in user or logged-in user's group. You can click **View** to see 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. You can click **View** to see the incident, which has been shared. • **<0> incidents now owned by you** – **Owner** fields of the incidents have been changed to the logged-in user or logged-in user's group. You can click **View** to see the incident, which the user now owns. • **<0> media downloaded** – Media files recorded by the logged-in user's camera have finished downloading to VideoManager. **NOTE:** The number of notifications corresponds to the number of media files, which have been downloaded, not the number of recordings. For example, if the camera captured one hour-long recording, but the camera's device profile was configured to split recordings up into 15-minute chunks, VideoManager would display four notifications – one for each media file. You can click **View** to see 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. You can click **View** to see all export jobs. The most recent export jobs are presented at the top of the list. • **<0> imports are ready** – The logged-in user's import jobs have finished processing.

Name	Description
	You can click **View** to see the import jobs. You can click **View assets** to see the imported media file. • – If there are system warnings, for example, if a licence is expiring within a week, they are presented here. These notifications cannot be cleared. You can click **View** to see the warnings. • **Your licence will expire on this date:** – The date when VideoManager's licence(s) expire. This notification cannot be cleared. **NOTE:** If VideoManager has multiple licences, information for the licence, which will expire first, is displayed here. • – The last time the user logged on. This notification cannot be cleared.
System information	The drop-down list 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 licenced features the user has enabled.
Messages	The pane displays system messages set by either a user or an administrator. You can set messages from the **Messages** section of the **User Interface** pane, in the **Admin** tab. For more information, see Creating, Editing, and Deleting Messages on page 264.

Chapter 4

Media

The **Media** tab provides access to all media files available in VideoManager and related functions, which you can perform on media files.

If you have sufficient permissions, you can perform the following actions:

- Search for media files, filter them by a number of criteria, and perform advanced searches.
  For more information, see Searching Media Files on page 36.
- Change the default layout of the **Media** tab on VideoManager.
  For more information, see Changing Viewing Options on page 39.
- Import media files into VideoManager.
  For more information, see Importing Media Files on page 41.
- View media files, which have been recorded on cameras or imported into VideoManager.
  For more information, see Viewing Media Files on page 42.
- Edit media file properties, such as who owns the media file.
  For more information, see Viewing and Editing Media File Properties on page 44.
- Add location information to a video that was recorded without any if, for example, GPS was disabled, or because the camera did not have GPS functionality.
  For more information, see Adding Location Information to Media Files on page 45.
- Redact media files.
  For more information, see Preparing Media on page 46.
- Perform actions on a media file, such as adding it to an incident, or rotating it.
  For more information, see Performing Media File Actions on page 47.
- Bulk edit media files.
  For more information, see Bulk Editing Media Files on page 49.
- Share a media file with other users on VideoManager.
  For more information, see Sharing Media Files on page 50.

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

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

4.1 Searching Media Files

You can search for individual media files on VideoManager, which can be useful if there are too many media files to scroll through manually.

Media files can be searched by a number of criteria.

Procedure:

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

3. Filter media files by any of the following criteria:

Filter	Description
Media or Recording ID	Searches for a media file by its unique media file ID. Alternatively, you can enter a recording ID. This action returns all media files that are part of that recording.
Location	Searches for media files that were recorded in a specific place. This can be done by clicking **Set Location**. You can either choose the relevant location on a map, and set a radius to search (minimum radius = 75 ft, maximum radius = 6.25 miles), or search the location by latitude and longitude.
Earliest date and **Latest date**	Searches for media files recorded between set earliest and latest dates. You can also choose a specific time of day (in a 24-hour format).
Device operator	Searches for media files downloaded by a specified user.
Owner	Searches for media files from a specified owner. The owner is normally the same user as the camera operator, but not always. For instance, if the person who originally recorded the media file has left the organisation and their user has been reassigned to someone else, that user becomes the owner of all their media. From the **Media file Details** page, it is also possible to edit who the owner of the media is. To search for media files that the logged-in user owns, you can click **My media**.
Source	Searches for media files from a specified name of the import source or the camera.
Origin	Filters media files by the location to which they were downloaded. This could be a DockController, a mobile phone, or the PC on which VideoManager is running. **NOTE:** You can find media files that have been downloaded directly to the user's PC by entering `local` into the search box.
Match text	Searches for media files whose user-defined media fields match the text entered here. For example, a drop-down field can have two options: `yes` and `no`. If you enter `yes` into the **Match text** field, all media files whose drop-down field is set to `yes` are returned.

Filter	Description
	For more information, see Creating User-Defined Media Fields on page 236.
Advanced filter	Users with knowledge of using sequence conditions can input more advanced search queries here. For more information, see Custom Predicate Language on page 380.

4. Select any of the following criteria:

Check Box	Description
Include incident media	If selected, includes media files which are part of one or more incidents.
Include non-incident media	If selected, includes media files which are **not** part of one or more incidents.
Only bookmarked media	If selected, only bookmarked media files are shown. **NOTE:** This filter only returns media files which had bookmarks added to them in the field by the camera they were recorded on. It does not return media files that had bookmarks added to them in an incident on VideoManager.
Include deleted media	If selected, includes recently deleted media files, and media files that are scheduled for deletion due to the deletion policy of VideoManager. If you have the **Undelete** permission set to **On**, you can reinstate deleted media files. You can do so by selecting the **Include deleted media** check box, clicking **Find media**, and then clicking **Reinstate media** next to the media file you want to reinstate. **TIP:** Recently deleted media files have a red heading.
Set whether filter should only return media that have location data	If selected, only media files with location data are shown. This includes both media files with location data recorded alongside them **and** media files whose location data was added in VideoManager after recording. For more information, see Adding Location Information to Media Files on page 45.
Set whether filter should only return media that have been shared	If selected, only media files that have been shared with other users on the system are shown.

Check Box	Description
Only media that will be deleted within *<0>* **days**	If selected, filters media files based on when they are scheduled to be deleted automatically, based on the deletion policy of VideoManager. **NOTE:** If the deletion policy has not been configured, this filter will not do anything. For more information, see Configuring Deletion Policies on page 193.

NOTE: These conditions have a cumulative effect. For example, if both **Only bookmarked media** and **Set whether filter should only return media that have location data** are selected, then only media files that are both bookmarked and have location data are shown.

5. To display all media files, which match the previously set criteria, click **Find media**.

   NOTE: You are only able to search for media files if you have corresponding permissions. You can check your permissions in the **Access** tab, under the **Media permissions** pane.

6. Optional: If you want to search for media files using different parameters, perform the following actions:
   a. Click the **Filter** heading.

      The search parameters re-open.

   b. To clear the search filters, click **Clear filter**.
   c. Enter the updated criteria and click **Find media**.

Postrequisites: Once you have filtered your media files, you can change the way that those media files are presented. For more information, see Changing Viewing Options on page 39.

4.1.1
Changing Viewing Options

You can change media file presentation options, which helps to locate media files faster, from the **Media** tab. You can change how media files are presented either before or after searching for specific media files. You can only change the preferences for your own session on VideoManager.

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

For more information, see Configuring the Media List on page 264.

Procedure:

1. Navigate to the **Media** tab.
2. Select the **Search Media** pane.
3. From the top right-hand **View options** menu, select the relevant format.

   Depending on your permissions, the options are as follows:

Format	Description
Large	Displays the first frame of each media file, and allows media file playback. Basic information about the media file is displayed, with a list of the media file actions available for this media file.
Gallery	Displays each media file in a grid. Usually, each image in the grid is a still frame from one minute of the media file. If the video is greater than 16 minutes, the time gap between each frame increases accordingly and the thumbnail can show up to 16 frames depending on the length of the video. You can jump to that point in the media file by clicking an image. No other information is displayed, and the only action that can be performed is to delete the media file.
List	Displays detailed information about each media file: • **Status** displays whether the media file has been uploaded from a site, and whether the media file has been bookmarked (by a VB400 in the field). • **Time** displays when the media file was recorded (date and hours/minutes/seconds). • **Duration** displays the length of the media file (hours/minutes/seconds). • **Operator** displays who recorded the media file. • **Source** displays which camera recorded the media file, and its serial number. **NOTE:** If the media file has been imported, the **Source** is shown as **Import**. • displays how many incidents include the media file in question. Clicking this either opens the relevant incident (if the media file only belongs to one) or presents the list of incidents (if the media file belongs to more than one). It also displays media file actions available for this media file. For more information, see Performing Media File Actions on page 47.

4. To change how media files are ordered, perform the following actions:
   a. Navigate to the **Media** tab.

b. Select the **Search Media** pane.

c. From the top right-hand drop-down menu, select the relevant filter:

Filter	Description
Recording date	Presents media files from most recently recorded to least recently recorded.
Recording date (least recent)	Presents media files from least recently recorded to most recently recorded.
Date added	Presents media files from most recently downloaded to least recently downloaded.

4.2

Importing Media Files

NOTE: Only users with the *Media file Import* licence can import a variety of files into VideoManager, including still images and PDFs.

Prerequisites: Before importing media files for the first time, an administrator can complete some steps first:

- Create an import profile.
  Creating an import profile dictates whether user-defined media fields of a media file will be automatically populated as it is imported.
  For more information, see Configuring Import Profiles on page 254.
- Enable and configure the antivirus policy of VideoManager.
  Enabling and configuring the antivirus policy of VideoManager ensures that all media files are scanned for viruses before they are imported.
  For more information, see Enabling and Configuring the Antivirus Policy on page 255.
- Configure thumbnail settings.
  VideoManager allocates a thumbnail to media files that are imported without any.
  For more information, see Configuring Thumbnails on page 271.

Procedure:

1. Navigate to the **Media** tab.
2. Select the **Import** pane.
3. From the drop-down list, select the relevant import profile for as many media files as necessary.
   You can import a media file by either dragging and dropping the file into VideoManager or by clicking **Choose Files** to select a file on your PC.
4. Click **Start import**.
   You can view the status of the import from the **Imports** pane. For more information, see Viewing Import Jobs on page 131.
   After a media file is successfully imported, you can view it from the **Media** tab, like media files recorded on cameras.
   For more information, see Searching Media Files on page 36.

4.3
Viewing Media Files

After a media file has been downloaded to VideoManager, either from a camera or from an external source, you can watch it from the **Media file Details** pane from where you can also configure the playback controls, which enables you to change the way you view the media file.

Prerequisites: An administrator can complete some steps first:

- Configure the playback policy.
  Configuring the playback policy dictates whether users must record a reason for watching a media file after a certain time period. It also dictates whether all media files have a watermark overlaid, associated with the user watching it.
  For more information, see Configuring the Playback Policy on page 257.
- Configure the default quality of media files which are played back on VideoManager.
  The default media file quality setting is **Low**.
  For more information, see Configuring Player on page 268.

Procedure:

1. Navigate to the **Media** tab.
2. Next to the relevant media file, click **More Details**.
   TIP: You can find the relevant media file by navigating to the **My Media**, **Shared Media**, or **Supervised Media** panes. You can also search for the relevant media file from the **Search Media** pane.
3. Click **Play media**.
   The bottom menu bar appears where you can perform any of the following actions:
   - Clicking **Theatre** puts the media file in **Theatre** mode, which fills the entire active window. Clicking the button again reverts the media file to its normal size.
   - Clicking **Fullscreen** puts the media file in **Fullscrean** mode, which fills the entire screen. Clicking the button again reverts the media file to its normal size.
   - Using any of the following controls allows you to skip through the media file:
     - **Cursor handle** tracks backward and forward through the media file.
     - **Play** plays or pauses the media file.
     - **Step backward** steps backward through the media file one frame at a time.
     - **Step forward** steps forward through the media file one frame at a time.
     - **Playback speed** plays the media file at different speeds (either 1/4x, 1/2x, Normal, or 2x).
   - Clicking **Settings** opens the **Playback Controls** menu where you can perform any of the following actions:
     - Clicking **Keyboard shortcuts** lists certain keyboard shortcuts that you can take.
     - Clicking **Metadata overlay** displays or hides the metadata recorded alongside the media file.
       Administrators can configure the type of metadata recorded alongside media files. For more information, see Configuring Video Metadata Overlay Settings on page 167.
     - Clicking **Audio** switches audio on or off.

- Clicking **Take screenshot** takes a screenshot of the media file in playback.
  The screenshot is automatically downloaded to your PC.
- Clicking **Video quality** changes the quality of the media file in playback. This option is only available to users with the correct permissions. It is recommended that the **Highest** setting is only used if there is a good data transfer connection.

4. Optional: If you have imported a PDF file, perform any of the following actions:
   - Click **View image**.
     The PDF opens in a new tab, and can be viewed and downloaded like normal.
   - Click **Download file**.
     The PDF is downloaded to the default downloads location of your PC.
5. Optional: If you have imported an audio file, perform any of the following actions:
   - Click **Play media**.
     You can skip, pause, and step through the file like a normal media file.
   - Click **Settings**.
     Clicking **Settings** allows for similar actions to the **Settings** control for media files, but only has options for **Keyboard shortcuts**, **Metadata overlay**, and **Audio quality**.
     For more information, see step 3.
6. Optional: If you have imported a still image, click **View image** and perform any of the following actions:
   - Click **Show/Hide zoom panel**.
     Clicking **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.
   - Click **Preparations**.
     Clicking **Preparations** switches between the original still image and the prepared version.
     For more information, see Preparing Media on page 46.
   - Click **Settings**.
     Clicking **Settings** allows for similar actions to the **Settings** control for media files, but only has options for **Keyboard shortcuts** and **Take screenshot**.
     For more information, see step 3.

   The **Theatre** and **Fullscreen** controls function as normal.
7. Optional: If you have imported a file whose file type is different from those mentioned, to download the file to the default downloads location of your PC, click **Download file**.
8. To return to the **Search Media** pane, click **Back**.

4.4

Viewing and Editing Media File Properties

NOTE: Only users with sufficient permissions can edit media file properties.

Procedure:

1. Navigate to the **Media** tab.
2. Next to the relevant media file, click **More Details**.

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

   The **Properties** pane opens and the following information is displayed:

Name	Description
Duration	The length of the clip
Operator	The name of the operator who filmed the media. If the media file was imported, this would be the name of the user who imported the media.
Origin	The camera on which the media file was filmed.
Name	The name of the media file on the file space of VideoManager
Media file ID	The unique URN assigned to this media file
Recording ID	If the media file is part of a longer recording, this is the unique URN assigned to that recording.
Time added	The time and date of when the media file was downloaded to VideoManager (either from a camera, or an external source)
Encoding	The FPS of the media file
Scheduled deletion	If the deletion policy has been configured, the field shows when the media file will be deleted by VideoManager automatically. The deletion can be based on a number of factors, including how many days have elapsed since the media file was recorded on a camera or downloaded from a camera to VideoManager. For more information, see Configuring Deletion Policies on page 193.
Signature	If file signing is enabled, VideoManager verifies all media files that were recorded on a VB400 against the certificate of VB400. If the field reads as `Success`, VideoManager has successfully verified that the media file has

Name	Description
	been recorded on a trusted camera and has not been tampered with. The field can display `Untrusted Certificate` if VideoManager does not recognise the certificate of the camera that recorded the media file. If the field is not present at all, it could be because the media file was downloaded from a non-VB400 source. For example, it was imported, or recorded on a VT100, or was downloaded to an earlier version of VideoManager.

3. Click **Edit properties** and perform any of the following actions:
   - Edit **Operator name**.
     Operator name is the operator who recorded the media file.

     NOTE: To change the owner of a media file, administrators must instead change the sharing settings for it. For more information, see Sharing Media Files on page 50.
   - Edit **Device name**.
     Device name is the name of the camera that recorded the media file.
   - Edit **Start time**.
     Start time is when the media file was initially added to VideoManager, which either means the time when the camera, which filmed the media file, was redocked, or when the media file was uploaded from the user's PC.

     Editing the property does **not** change when the media file was actually recorded.
   - Edit any user-defined media fields that have been created.
     For more information, see Creating User-Defined Media Fields on page 236.
4. Click **Save changes**.

4.5 Adding Location Information to Media Files

NOTE: Only users with sufficient permissions can add location data to VideoManager media files that were recorded without it.

Adding location information is useful if the original media file was recorded on a camera without GPS, and the user wants to add location data retroactively. Users cannot edit location data that was recorded alongside a media file.

Prerequisites: To add location data to a media file, or edit previously existing location data, ensure that location information is enabled on VideoManager. You can do so from the **Maps** section of the **User Interface** pane, in the **Admin** tab.
For more information, see Enabling and Configuring Maps on page 270.

Procedure:

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

2. Next to the relevant media file, click **More Details**.

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

3. In the **Location** pane, click **Edit location**.
4. To position the marker at the desired location, click and drag the map.

   TIP: If you have chosen a lookup provider from the **Maps** section, in the **Admin** tab, you can also manually search for a location.

5. To save, click **Confirm**.

4.6 Preparing Media

You can prepare the media to obscure sensitive information.

Procedure:

1. Navigate to the **Media** tab.
2. Next to the relevant media file, click **More Details**.

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

3. Click **Prepare media**.

   You can now prepare media files in the same way you would redact an incident clip. For more information, see Manually Redacting Incident Clips on page 58.

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

4. Optional: Perform any of the following actions:

   These are image-exclusive actions.

   - Click **Crop the image to size**.

     Clicking **Crop the image to size** draws the square around the subject of the image. Anything in the blue section will not be featured in the finished media.

     NOTE: The cropped version of the image will not be shown until you click **Confirm**.

   - Click **Adjust the image**.

     Clicking **Adjust the image** opens a set of sliders in the right-hand menu. These sliders control **Contrast**, **Brightness**, **Saturation**, and **Gamma**.

5. Optional: To restore the default settings for each slider, click **Restore Defaults**.

4.7

Performing Media File Actions

VideoManager allows you to perform actions on your media files from the > **More Details** pane. It is possible to perform most of these actions from the **Search Media** page as well.

NOTE: Only users with sufficient permissions can perform a range of actions.

Procedure:

1. Navigate to the **Media** tab.
2. Next to the relevant media file, click > **More Details**.

   TIP: You can find the relevant media file by navigating to the **My Media**, **Shared Media**, or **Supervised Media** panes. You can also search for the relevant media file from the **Search Media** pane.
3. From the > **More Details** pane, perform any of the following actions:

   - To create an incident including the relevant media file, click **Create new incident**.
     For more information, see Creating Incidents Manually and Performing Incident Actions on page 53.
   - To add a media file to a previously created incident, click **Add media to existing incident** and next to the relevant incident, click > **Add to this incident**.
   - To verify a media file, which indicates whether it has been tampered with since being uploaded from a user's camera, click **Verify file integrity**.
     If successful, a green icon appears in the **Verification** section of the **Properties** pane.
   - To download a `.zip` containing information about the signature of the media file, click **Download signature verification report**.
     The downloaded `.zip` contains the following information about the media file:
     - `certificate-chain.pem` is the PEM-encoded list of certificates included in the signature that was verified by VideoManager.
     - `signature.jws` is the raw signature file retrieved from the camera.
     - `signed-payload.txt` is the manifest from the report. This is a JSON structure with the camera DID, filename, file size, and SHA256.
     - `trust-root.pem` is the PEM-encoded trust root from the signature certificate chain.
     - `signature-info.txt` is 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 about X.509 footage signing, you can navigate to the Motorola Solutions Learning Experience Portal (registration is free) and search for *VideoManager X.509 Footage Signing Explained*.
   - To download the media file to your PC, which is the only way to share a media file with workers who are not on VideoManager, click **Download original file**.
     The media file is saved to the default download location of your PC.

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

Name	Description
Source	Returns actions performed on the media file by the specified source, such as a camera on VideoManager.
Event type	Returns specific actions performed on the media file. If you start entering an event, VideoManager will suggest various event options, such as **FOOTAGE_PLAY**.
User	Returns actions performed on the media file by the specified user. If you start entering a username, VideoManager will suggest various usernames to match it.
Message	Returns specific actions performed on the media file, whose details match the keywords entered here. For example, the **FOOTAGE_PLAY** event comes with the message **View Media File**.
Signature	You should enter the signature of an incident, which returns actions performed on the media file in relation to this incident. For example, when the media file was added to the specified incident.
Location	Returns actions performed on the media file from a specific dock or EdgeController.
Client	Returns actions performed on the media file from a specific IP address.
Server	Returns actions performed on the media file from a specific server hosting VideoManager.
Date range drop-down list	You can select the date range for these actions.

- To delete the media file, which removes it from the **Media** tab and VideoManager, click **Delete media**.

  When searching from the **Search media** pane using the **Include deleted media** option, a deleted media file can still be "undeleted" for a short while, depending on how the deletion policy of VideoManager has been configured.

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

4.8

Bulk Editing Media Files

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

Bulk edits are also useful if you have enabled your VideoManager to act as a Central VideoManager. In this case, every media file held in connected sites can be automatically fetched in bulk, which means that they are editable in the Central VideoManager and unviewable in the original sites.

Procedure:

1. Navigate to the **Media** tab.
2. Select the **Search Media** pane.
3. Filter the media files as necessary and click **Find media**.
4. Optional: From the **View options** menu in the top right-hand corner, select **List**.

   The **List** view shows more results per page than the **Large** or **Gallery** views, making it easier to select multiple media files simultaneously.
5. Click **Bulk edit**.

   The bulk edit user interface appears.
6. Perform one of the following actions:
   - To select individual media files, next to their rows, click .
   - To select all media files on-screen, click **Toggle selection of ALL rows**.

   If there is an overflow of media files, VideoManager gives you the option to select the media files that are not on-screen. To manually de-select individual media files, click on their row.
7. After you have selected media files for bulk editing, perform any of the following actions:
   - Click **Rotate**.
     This action presents a drop-down list, which gives users the ability to rotate multiple media files clockwise, anti-clockwise, 180 degrees, or horizontally.
   - Click **Create incident**.
     This action allows you to create an incident with all the selected media files included.
   - Click **Add to incident**.
     This action allows you to add multiple media files to an existing incident.
   - Click **Edit properties**.
     This action allows you to edit the fields for all media files simultaneously.

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

     NOTE: If fields are bulk edited, any configuration they had previously will be overwritten.
   - Click **Edit sharing**.
     This action allows you to share multiple media files with other users simultaneously.
     - In the **Owner** field, administrators can change the owner of the media files. This can be a user or an entire group. If the owner of the media files is a group, all users in that group will be able

to process the media files as if the media files were their own. For example, all users in the group will be able to add the media files to incidents, or redact them.

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

- In the **Shared:** field of the **Sharing** panel, you can enter the name of the user, with whom these media files will be shared, and click + to add the user to the list.

- Click **Delete**.
  This action allows you to delete all of the selected media files simultaneously.
  You will be asked to confirm your choice.

- Click **Fetch**.
  This option is only available if VideoManager is enabled as a Central VideoManager. It allows you to fetch all of the selected media files from their sites simultaneously. This is useful if your network is too weak to keep auto-fetch on continuously. Once the media files have been fetched, they are editable like normal in Central VideoManager but are not viewable on the original site.
  For more information, see Configuring Sites on page 297.

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

4.9 Sharing Media Files

It can be necessary for you to share your media files with your peers, without having the ability to see all media files on the system, for example, if you want a second opinion about a procedure or an event. In this case, you can utilise sharing function of VideoManager to give other users access to a media file.

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

For more information, see Sharing Incidents Externally Using a Link on page 85.

Procedure:

1. Navigate to the **Media** tab.
2. Next to the relevant media file, click **More Details**.

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

3. In the **Sharing** pane, click **Edit sharing settings**.
4. In the **Owner** field, change the owner of the media file.

   NOTE: Only administrators can change the owner of the media file.

   The owner can be a user or an entire group. If the owner of the media file is a group, all users in that group will be able to process the media file as if it were their own. For example, all users in the group will be able to add the media file to incidents, or redact it.

   An administrator can change the operator who recorded the media file/imported the media file from the **Properties** pane.

   NOTE: If **Restricted** is set to **Yes**, only users with the **List restricted media** permission are able to search for the media file. Only users with the **Play restricted media** permission are able to watch the media file.

5. In the **Shared:** field of the **Sharing** panel, enter the name of the user with whom the media file should be shared.
6. To add the user to the list, next to the **Shared:** field, click **+**.
7. Click **Confirm Changes**.

   Shared media files appear in the selected user's **Shared Media** list. Depending on the permissions that have been enabled under the **Shared** column of the role(s) the user is a part of, they can now access the media file like normal.

Chapter 5

Incidents

The **Incidents** tab provides access to all incidents available in VideoManager and related functions, which you can perform on incidents.

If you have sufficient permissions, you can perform the following actions:

- Create incidents manually and perform various actions on them.
  For more information, see Creating Incidents Manually and Performing Incident Actions on page 53.
- Create incidents automatically. VideoManager creates incidents from media files that have had their user-defined media fields populated in a specific manner.
  For more information, see Creating Incidents Automatically on page 56.
- Create incidents with bulk edit. You can select multiple media files and include them all in one incident simultaneously.
  For more information, see Creating Incidents with Bulk Edit on page 56.
- Add media files to an incident after it has been created.
  For more information, see Adding Media Files to Existing Incidents on page 57.
- Clip evidential media in an incident.
  For more information, see Clipping Videos in Incidents on page 58.
- Redact media in an incident.
  For more information, see Manually Redacting Incident Clips on page 58.
- Edit redactions on an incident clip as well as other properties of the clip.
  For more information, see Assisted Redaction Editor on page 69.
- Search previously created incidents, create saved searches, and perform advanced searches.
  For more information, see Searching Incidents on page 77.
- Bulk edit incidents.
  For more information, see Bulk Editing Incidents on page 81.
- Create, edit, and delete bookmarks for media files in incidents. These can be used to highlight portions of evidential media.
  For more information, see Creating, Editing, and Deleting Bookmarks on page 82.
- Share incidents, either internally or externally, using exports.
  For more information, see Sharing Incidents on page 84.
- View previously created exports.
  For more information, see Viewing Exports on page 88.
- Commit incidents, if configured as a Central VideoManager or site.
  For more information, see Committing Incidents on page 89.
- If *Nested Incidents* has been licenced, you can create incident collections.
  For more information, see Creating Incident Collections on page 92.

5.1

Creating Incidents Manually and Performing Incident Actions

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

Prerequisites: Before creating an incident for the first time, an administrator can complete some steps first:

- Create user-defined incident fields.
  These fields are presented automatically when creating and editing incidents, and enable users to categorise incidents in a manner that fits the unique needs of their organisation.
  If user-defined incident fields are created after incidents have been created, those fields are added to the **Edit Incident** form automatically and can be populated when the user edits an incident.
  For more information, see Creating User-Defined Incident Fields on page 219.
- Import media files into VideoManager.
  For more information, see Importing Media Files on page 41.
- Configure whether incident clips are presented as versions of the original recording when they are redacted and edited in an incident, or as unique media files in their own right.
  For more information, see Configuring Incident Settings on page 272.

Procedure:

1. Perform one of the following actions:

   NOTE:
   If there is a specific media file you want to include in an incident, you should create an incident from the **Media** tab.

   However, if you are not sure which media files you want to include in the incident, you should create an incident from the **Incidents** page.

Option	Actions
Creating an incident from the **Media** tab	**a.** Navigate to the **Media** tab. **b.** Next to the relevant media file, click **Create new incident**. **TIP:** You can find the relevant media file by navigating to the **My Media**, **Shared Media**, or **Supervised Media** panes. You can also search for the relevant media file from the **Search Media** pane. **c.** If the media file is part of a longer recording because the camera which recorded it has been configured to split long recordings up into individual media files (through its device profile), the entire recording can be added to this incident as well. To do so, set **Add whole recording to incident?** to **On**. **d.** If the operator who recorded this media file also recorded other media files at the same time (e.g. because multiple cameras were assigned to one operator), those media files can be added to this incident as well. To do so, set **Add other footage from same operator?** to **On**. **e.** Click **Create incident**.
Creating an incident from the **Incidents** page	**a.** Navigate to the **Incidents** page. **b.** Click **Create incident**. The **New Incident** page opens, without any media files attached to it. You can add media files later by navigating to the **Media** tab, finding the relevant media file, and clicking **Add to this incident** next to it. For more information, see Adding Media Files to Existing Incidents on page 57.

2. In the **Title** field, enter the name of the incident.
3. Optional: Populate any of the following fields:

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

NOTE: The following fields cannot be edited:

- The **Creation Time** field shows when the incident was first created.
- The **Update Time** field shows when the incident was last edited.
- The **Clip Count** field shows how many media files are in the incident, and is automatically updated when a media file is added or removed.
- The **Owner** field shows the username of whoever is creating the incident.
- The **Signature** field is automatically populated by VideoManager upon creation.

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

   For more information, see Creating User-Defined Incident Fields on page 219.

5. If necessary, clip the media files which have been added to the incident.

   Clipping media files enables users to focus on the relevant sections of media file. For more information, see Clipping Videos in Incidents on page 58.

6. If necessary, redact the media files which have been added to the incident.

   Redacting media files enables users to obscure sections of the media file, in line with privacy regulations. For more information, see Manually Redacting Incident Clips on page 58.

7. Click **Create incident** and perform any of the following actions:

   - To edit an incident, click **Edit incident**, make the relevant changes, and click **Save incident**.

     NOTE: You can add incident attachments from your PC, but you cannot add media files from VideoManager. This action can be done from the **Media** tab. For more information, see Adding Media Files to Existing Incidents on page 57.

   - To duplicate an incident, click **Duplicate incident**, make any necessary changes to the copy of the incident, and click **Create incident**.

     Duplicating an incident copies 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 delete an incident, click **Delete incident** and confirm the deletion by clicking **Delete Incident**.

     Deleting an incident does not delete any of the media files within the incident.

     When searching from the **Search Incidents** pane using the **Show recently deleted incidents** option, a deleted incident can still be "undeleted" for a short while.

   - To export an incident, click **Export incident**, and then click **Create Export**.

     Exporting an incident creates a copy of the incident which can then be shared with workers who are not on VideoManager.

     For more information, see Sharing Incidents Externally Using an Export on page 85.

   - To create an audit log, click **View incident audit log**, filter the audit log as necessary, and click **Filter audit log**.

     Creating an audit log for the incident shows a list of all actions which were performed on an incident, and which users performed them.

5.2
Creating Incidents Automatically

NOTE: Only administrators can configure VideoManager to automatically create incidents from media files, depending on the status of the user-defined media fields of the media files.

Prerequisites: 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 a media file will determine whether VideoManager automatically creates an incident from the media file or not. For more information, see Creating User-Defined Media Fields on page 236.
2. Configure automatic incident creation settings.
   These settings determine which user-defined media fields will control automatic incident creation. For more information, see Enabling and Configuring Automatic Incident Creation on page 214.

After the configuration is completed, users can create incidents from media files.

Procedure:

1. Navigate to the **Media** tab.
2. Next to the relevant media file, click **More Details**.

   TIP: You can find the relevant media file by navigating to the **My Media**, **Shared Media**, or **Supervised Media** panes. You can also search for the relevant media file from the **Search Media** 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**.

   If the incident has been created correctly, it should appear in the **Search Incidents** pane.

5.3
Creating Incidents with Bulk Edit

If you want to add multiple media files to an incident simultaneously, you should use the bulk edit function.

Prerequisites: Before creating an incident with bulk edit, an administrator can complete some steps first:

- 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 that fits the unique needs of their organisation.

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

  For more information, see Creating User-Defined Incident Fields on page 219.
- Import media files into VideoManager using the *Media file Import* licence.
  For more information, see Importing Media Files on page 41.

Procedure:

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

2. Select the **Search Media** pane.
3. Filter the media files as necessary and click **Find media**.
4. Optional: From the **View options** menu in the top right-hand corner, select **List**.

   The **List** view shows more results per page than the **Large** or **Gallery** views, making it easier to select multiple media files simultaneously.
5. Click **Bulk edit**.
6. Perform one of the following actions:
   - To select individual media files, next to their rows, click .
   - To select all media files on-screen, click **Toggle selection of ALL rows**.
7. Click **Create incident**.

   All selected media files are added to the incident as incident clips. You can rearrange them in the following manners:
   - You can arrange the incident clips by recording time (earliest first, latest last) by clicking **Sort by time**.
   - You can arrange the incident clips in a custom order by clicking and dragging the incident clip to the desired position.
8. Complete the incident fields as normal and click **Create incident**.

5.4 Adding Media Files to Existing Incidents

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

Procedure:

1. Navigate to the **Media** tab.
2. Next to the relevant media file, click **More Details**.

   TIP: You can find the relevant media file by navigating to the **My Media**, **Shared Media**, or **Supervised Media** panes. You can also search for the relevant media file from the **Search Media** pane.
3. Perform one of the following actions:
   - If you want to add one media file to the incident, next to the incident, click **Add media to existing incident**.
   - If you want to add multiple media files to the incident, click **Bulk edit** and perform one of the following actions:
     - To select individual media files, next to their rows, click and click **Add to incident**.
     - To select all media files on-screen, click **Toggle selection of ALL rows** and click **Add to incident**.
4. Filter the incidents as normal and click **Find incidents**.

5. Next to the relevant incident, click **Add to this incident**.

   If the incident contains multiple incident clips, you can rearrange them in the following manners:

   - You can arrange the incident clips by recording time (earliest first, latest last) by clicking **Sort by time**.
   - You can arrange the incident clips in a custom order by clicking and dragging the incident clip to the desired position.

6. Click **Save incident**.

5.5 Clipping Videos in Incidents

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

Procedure:

1. Navigate to the **Incidents** tab.
2. Next to the relevant incident, click **Edit incident**.

   TIP: You can find the relevant incident by navigating to the **My Incidents**, **Shared Incidents**, or **Supervised Incidents** panes. You can also search for the relevant incident from the **Search Incidents** pane.

3. Next to the relevant media file, click **Edit clip start/end time**.
4. Perform one of the following actions:
   - To shorten the media file roughly, select the start and end time of the clip by dragging the toggles in the top video progress bar.
   - 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 action shortens the video to the point specified. You can do the same for the end of the clip by clicking **Set end of clip**.
5. Click **Confirm**.

5.6 Manually Redacting Incident Clips

The **Incident Clip Redactor** allows you to apply a variety of redactions, text annotations, and redaction effects to a media file in an incident. This is useful if data protection laws require certain features of the media file to be obscured, such as faces, or if you want to highlight a specific aspect of the media.

Procedure:

1. Navigate to the **Incidents** tab.
2. Next to the relevant incident, click **Edit incident**.

   TIP: You can find the relevant incident by navigating to the **My Incidents**, **Shared Incidents**, or **Supervised Incidents** panes. You 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 Creating Foreground Redactions on page 59.
   - Background redactions
     For more information, see Creating Background Redactions on page 60.
   - Audio redactions
     For more information, see Creating Audio Redactions on page 63.
   - Text redactions
     For more information, see Creating Text Annotations on page 62.
   - Brightness redactions
     For more information, see Creating Brightness Redactions on page 63.
   - Zoom redactions
     For more information, see Creating Zoom Redactions on page 64.
   - Other redactions, such as flipping and rotating a clip
     For more information, see Other Redactions on page 65.
   - Transcriptions
     For more information, see Creating and Importing Transcripts for Incident Clips on page 66.
   - You can also access the redaction Advanced drop-down list
     For more information, see Accessing the Redaction Advanced Drop-Down List on page 67.

Postrequisites: After creating a redaction, you can perform any of the following actions on it:

- To edit a redaction, click **Edit incident**. In the **Incident clips** section, click **Redact parts of this clip**. Step forward through the media file to the point that the redaction starts and select the redaction by clicking it. After making necessary changes, save the incident by clicking **Confirm**, and then **Save incident**.
- To delete a redaction, click **Edit incident**. In the **Incident clips** section, click **Redact parts of this clip**. Step forward through the media file to the point that the redaction starts and select the redaction by clicking it. Delete the redaction by clicking **Delete** in the right-hand menu bar. Save the incident by clicking **Confirm**, and then **Save incident**.

5.6.1
Creating Foreground Redactions

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

Procedure:

1. Navigate to the **Incidents** tab.
2. Next to the relevant incident, click **Edit incident**.

   TIP: You can find the relevant incident by navigating to the **My Incidents**, **Shared Incidents**, or **Supervised Incidents** panes. You 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 forward through the media file to the point where the redaction should start.
5. Click one of the following:
   - **Insert oval**
   - **Insert square**
   - **Insert quadrilateral**
6. Draw a shape around the area that you want to redact.

   The shape is saved immediately. You can change the shape of the redaction from the **Shape** pane. You can drag out the corners of the shape to fit the area that must be redacted.

   A right-hand menu appears.

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

   You have a choice of **Blur**, **Pixelate**, and **Solid**.
8. If relevant, in the **Brightness** pane, select the check box and adjust the brightness of the redaction by using the slider.
9. Perform one of the following actions:
   - If the subject of the media file is static, skip to the part of the media file where the redaction should end.
   - If the subject of the media file is moving, perform one of the following actions:
     - Automatically track the subject of the media file by pressing and holding to track backward, or to track forward.
       This action follows the subject of the media file frame-by-frame, updating the position of the redaction automatically.

       NOTE: VideoManager can only change the position of the redaction, not its size, or shape, so you may still need to manually reposition the redaction.
     - Manually track the subject of the media file by using **Step backward** / **Step forward** to step through the media file frame-by-frame and reposition the shape to ensure that it is focused on the subject at all times.
10. When you reach the part of the media file where the redaction should end, click **End**.
11. Repeat step 4 through step 10 for every new redaction to be added.
12. Click **Confirm**.
13. Click **Save incident**.

5.6.2 Creating Background Redactions

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

Procedure:

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

2. Next to the relevant incident, click **Edit incident**.

   TIP: You can find the relevant incident by navigating to the **My Incidents**, **Shared Incidents**, or **Supervised Incidents** panes. You 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 forward through the media file to the point that the redaction should start.
5. Click one of the following:
   - **Insert oval**
   - **Insert square**
   - **Insert quadrilateral**
6. Draw a shape around the area that should remain unredacted.

   The shape is saved immediately. You can change the shape of the redaction from the **Shape** pane. You can drag out the corners of the shape to fit the area that must be redacted.

   A right-hand menu appears.

7. For each redaction area, select the check box in the **Redaction** pane and select **Unredact**.
8. In the top menu, select the type of background redaction.

   You have a choice of **Blur**, **Pixelate**, and **Solid**.
9. Perform one of the following actions:
   - If the subject of the media file is static, skip to the part of the media file where the redaction should end.
   - If the subject of the media file is moving, perform one of the following actions:
     - Automatically track the subject of the media file by pressing and holding to track backward, or to track forward.

       This action follows the subject of the media file frame-by-frame, updating the position of the redaction automatically.

       NOTE: VideoManager can only change the position of the redaction, not its size, or shape, so you may still need to manually reposition the redaction.

     - Manually track the subject of the media file by using **Step backward** / **Step forward** to step through the media file frame-by-frame and reposition the shape to ensure that it is focused on the subject at all times.
10. When you reach the part of the media file where the redaction should end, click **End**.
11. Click **Confirm**.
12. Click **Save incident**.
13. Optional: To delete a background redaction, change the background redaction to **None**.

5.6.3

Creating Text Annotations

Text annotations are text boxes, which can be moved and resized in the same way as other redactions, and can provide information about a subject or event within the media file.

Procedure:

1. Navigate to the **Incidents** tab.
2. Next to the relevant incident, click **Edit incident**.

   TIP: You can find the relevant incident by navigating to the **My Incidents**, **Shared Incidents**, or **Supervised Incidents** panes. You 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 forward through the media file to the point that the redaction should start.
5. Click **Insert text**.
6. Click the area of the media file frame where the text annotation should be displayed.

   The **Text** panel is displayed.
7. In the right-hand menu, enter the text to be displayed.

   You can click **A+** to make the text annotation bigger.

   You can click **A—** to make the text annotation smaller.

   You can click **A** to change the colour of the text annotation.

   NOTE: You can either choose a colour from the selection presented by VideoManager, or enter your own colour using the Hex code. By clicking **C**, the Hex code colour is saved and can be selected again from the row at the top.
8. Perform one of the following actions:
   - If the subject of the media file is static, skip to the part of the media file where the redaction should end.
   - If the subject of the media file is moving, manually track the subject of the media file by using **Step backward** / **Step forward** to step through the media file frame-by-frame and reposition the text to ensure that it is focused on the subject at all times.

     You do not need to redraw the annotation, just re-position it.
9. When you reach the part of the media file where the redaction should end, click **End**.
10. Click **Confirm**.
11. Click **Save incident**.

5.6.4

Creating Audio Redactions

You can mute or beep over audio in media files for a predetermined length of time, which allows you to redact voices and other noises, in accordance with data protection laws. You can also redact a media file so it plays audio from the secondary microphone of the camera.

Procedure:

1. Navigate to the **Incidents** tab.
2. Next to the relevant incident, click **Edit incident**.

   TIP: You can find the relevant incident by navigating to the **My Incidents**, **Shared Incidents**, or **Supervised Incidents** panes. You 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 forward through the media file to the point where the redaction should start.
5. From the top toolbar, click **Insert audio effect** and draw it over an area of the media.

   If you do not want an icon to appear, you can deselect the **Show Icon** setting from the **Options** pane.
6. In the right-hand menu, from the **Effect** section, select a specific type of audio redaction.

   The options are as follows:

   - **Muted** – No audio is played for this section of the incident clip.
   - **2nd Channel** – If the media file was recorded on a VB400, only audio recorded by the second microphone of VB400 is played for this section of the incident clip.

     This audio redaction is useful if the incident clip features a loud noise. Using the second microphone may make other audio in the media file clearer.
   - **Beep** masks the audio for this section of the incident clip.
7. When you reach the part of the media file where the redaction should end, click **End**.

5.6.5

Creating Brightness Redactions

Brightness redactions are used to darken or brighten areas of the media file, highlight relevant parts of a piece of evidential media, and applies to both foreground and background redactions.

Procedure:

1. Navigate to the **Incidents** tab.
2. Next to the relevant incident, click **Edit incident**.

   TIP: You can find the relevant incident by navigating to the **My Incidents**, **Shared Incidents**, or **Supervised Incidents** panes. You 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 forward through the media file to the point that the redaction should start.
5. Click one of the following:

   - **Insert oval**

- **Insert square**
- **Insert quadrilateral**

6. Using the cursor, draw a shape around the area that should be brightened or darkened.
7. In the **Redaction** pane, select the check box and click **Unredact**.
   The action leaves the area inside the redaction unredacted.
8. In the **Brightness** pane, select the check box.
9. Use the slider to adjust the required brightness inside the redaction effects area.
   Moving the slider toward makes the area darker, while moving the slider toward makes the area lighter.
10. Perform one of the following actions:
    - If the subject of the media file is static, skip to the part of the media file where the redaction should end.
    - If the subject of the media file is moving, perform one of the following actions:
      - Automatically track the subject of the media file by pressing and holding to track backward, or to track forward.
        This action follows the subject of the media file frame-by-frame, updating the position of the redaction automatically.

        NOTE: VideoManager can only change the position of the redaction, not its size, or shape, so you may still need to manually reposition the redaction.
      - Manually track the subject of the media file by using **Step backward** / **Step forward** to step through the media file frame-by-frame and reposition the shape to ensure that it is focused on the subject at all times.
11. When you reach the part of the media file where the redaction should end, click **End**.

Postrequisites: You can create a background brightness redaction effect, which affects any areas of the media file that are not covered by foreground redactions.

1. From the top menu bar, select the **Background brightness** option.
2. From the drop-down menu, choose the desired brightness level.
   This action applies to the entire duration of the media file. The options are as follows: **Very Dark**, **Dark**, **Normal**, **Bright**, and **Very Bright**.

5.6.6 Creating Zoom Redactions

Zoom redaction effects focus on specific aspects of the media file and can be used to highlight the relevant parts of a piece of evidential media.

Procedure:

1. Navigate to the **Incidents** tab.
2. Next to the relevant incident, click **Edit incident**.

   TIP: You can find the relevant incident by navigating to the **My Incidents**, **Shared Incidents**, or **Supervised Incidents** panes. You 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 forward through the media file to the point that the redaction should start.
5. Click **Zoom in on one area**.
6. Draw the square around the area of the media file that should be zoomed in (or out) on.
7. To move and scale the redaction over the area that should be affected, in the right-hand menu, use **Zoom in**, **Zoom out**, or **Centre in frame** .

   NOTE: The redaction effect is not visible until the media file is played like normal.
8. Perform one of the following actions:
   - If the subject of the media file is static, skip to the part of the media file where the redaction should end.
   - If the subject of the media file is moving, perform one of the following actions:
     - Automatically track the subject of the media file by pressing and holding to track backward, or to track forward.
       This action follows the subject of the media file frame-by-frame, updating the position of the redaction automatically.

       NOTE: VideoManager can only change the position of the redaction, not its size, or shape, so you may still need to manually reposition the redaction.
     - Manually track the subject of the media file by using **Step backward** / **Step forward** to step through the media file frame-by-frame and reposition the shape to ensure that it is focused on the subject at all times.
9. When you reach the part of the media file where the redaction should end, click **End**.
10. Click **Confirm**.
11. Click **Save incident**.

5.6.7
Other Redactions

There are some other redaction effects that can be performed on a media file. Those redaction effects can be found in the top menu bar.

Name	Description
Show metadata	Displays the metadata recorded alongside the media file. From the **Metadata position** drop-down list, you can select the position of the overlay text or hide it completely. You can choose which metadata to redact by selecting any of the available check boxes: • **Device serial #** • **Operator** • **Date & time**

Name	Description
	• **Frame counter** • **Recording time** • **Pre-record flag** • **GPS** • **Device name** • **Battery level**
Rotate clockwise	Rotates the media file by 90 degrees left.
Rotate anti-clockwise	Rotates the media file by 90 degrees right.
Horizontal flip	Flips the media file horizontally.
Hide captions	Hides the transcription. Clicking this icon again displays the transcription.

NOTE: Administrators can configure the specific metadata information recorded alongside media files. For more information, see Configuring Video Metadata Overlay Settings on page 167.

5.6.8

Creating and Importing Transcripts for Incident Clips

After an incident clip is added to an incident, you can create a transcript for it within the incident editor, or import an existing `.vtt` file. Creating a transcript displays captions over the incident clip.

Administrators can optionally add previously created user-defined incident fields to the transcript editor, to provide more context during transcript creation and editing. For more information, see Creating User-Defined Incident Fields on page 219.

Administrators can also configure export profiles so that transcripts are exported as a PDF alongside the incident itself. For more information, see Creating Evidence Export Profiles on page 202.

Creating New Transcripts for Incident Clips

Procedure:

1. Navigate to the **Incidents** tab.
2. Next to the relevant incident, click **Edit incident**.

   TIP: You can find the relevant incident by navigating to the **My Incidents**, **Shared Incidents**, or **Supervised Incidents** panes. You can also search for the relevant incident from the **Search Incidents** pane.
3. Click **Transcription**.
4. In the left-hand **Speaker** window, enter a name or identifier for each individual who is speaking in the incident clip.
5. Use the player in the top left-hand corner to step forward in the incident clip, to the point where the transcription should begin.

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

   A new row appears automatically in the **Transcription** window.

7. Enter the relevant text.
8. To navigate to the point in the incident clip where a new caption is needed, use the and buttons.
9. Repeat step 6 through step 7 as many times as necessary.
10. When you are finished, to save the transcript, click **Confirm**.

Importing Existing .vtt Files into VideoManager

Procedure:

1. Navigate to the **Incidents** tab.
2. Next to the relevant incident, click **Edit incident**.

   TIP: You can find the relevant incident by navigating to the **My Incidents**, **Shared Incidents**, or **Supervised Incidents** panes. You can also search for the relevant incident from the **Search Incidents** pane.

3. In the **Incident clips** section, click **Redact parts of this clip**.
4. Click **Transcription**.
5. In the **Actions** field, click **Import**.
6. Select the previously created `.vtt` file.

   If successful, the right-hand menu shows the transcript that has been successfully imported.

   You can overwrite previously imported captions with a new set of captions by clicking **Import** again and selecting the desired `.vtt` file.

Postrequisites: You can perform any of the following actions:

- To export a transcript from an incident clip, click **Export**.
  This action downloads the `.vtt` file to the PC running VideoManager.

  NOTE: This `.vtt` file will not be identical to the file that was originally imported. Only the captions will be exported, without any styling or comments.

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

5.6.9

Accessing the Redaction Advanced Drop-Down List

Procedure:

1. Navigate to the **Incidents** tab.
2. Next to the relevant incident, click **Edit incident**.

   TIP: You can find the relevant incident by navigating to the **My Incidents**, **Shared Incidents**, or **Supervised Incidents** panes. You 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. In the upper right-hand corner, click .

   The drop-down list opens.

Name	Description
Help	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 get bigger, which is useful if you want to create a small redaction that needs more precise parameters.
Keyboard Shortcuts	Gives information about the possible keyboard shortcuts you can perform to move through the media file more quickly. For more information, see Keyboard Shortcuts on page 379.
Cycle between annotations	If a redaction effect is selected, clicking this cycles through all the redaction effects in the media file, then goes back to the beginning and begins again.
Go to next annotation	If a redaction effect is selected, clicking this moves to the next redaction effects one by one, then stops at the last one.
Go to previous annotation	If a redaction effect is selected, clicking this moves to the previous redaction effects one by one, then stops at the first one.
Clear all	Deletes all redactions in the media file.

5.6.10

Accessing the Redaction Settings

Procedure:

1. Navigate to the **Incidents** tab.
2. Next to the relevant incident, click **Edit incident**.

   TIP: You can find the relevant incident by navigating to the **My Incidents**, **Shared Incidents**, or **Supervised Incidents** panes. You 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. In the lower right-hand corner of the video, click .

   The drop-down list opens.

Name	Description
Keyboard shortcuts	Lists certain keyboard shortcuts that you can take.
Audio	Switches audio on or off.
Playback watermark	Toggles the playback watermark to enable easier redaction. **NOTE:** Toggling the playback watermark is audited with the relevant username and signature. The signature can be associated with the relevant footage play audit message.
Video quality	Changes the quality of the video. 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.

5.7
Assisted Redaction Editor

IMPORTANT: You must be assigned to the **Assisted redaction** role to access the Redaction editor. For more information, see Incident Permissions on page 328.

The VideoManager Redaction editor for assisted redaction projects allows editing redactions on an incident clip. Assisted redaction projects are processed using an Artificial Intelligence (AI) redaction tool. This tool automatically masks common objects for redaction, such as faces, people, licence plates, vehicles, and screens in the video. You can use the Redaction editor to ensure the privacy of personal information, security of sensitive details, and provide relevant information for legal proceedings in video evidence.

To access the Redaction editor, perform the following actions:

1. Navigate to the **Incidents** tab.
2. Select the **Assisted Redaction** pane.
3. Filter redactions by any of the following criteria:

Filter	Description
Redaction reference	Searches for redactions whose **Redaction reference** field matches the text entered here.
Title	Searches for redactions whose name matches the one entered.
Owner	Searches for redactions owned by a specified user.
Status drop-down list	From the **Status** drop-down list, you can select the current status of the redaction.

To clear the search filters, click **Clear filter**.

4. To search for the relevant redactions, click **Filter redactions**.
5. Next to the relevant redaction, click **Redact clip**.
   The Redaction editor opens in the new window, showing the video from the redaction project.

   The redaction assistant feature automatically detects and numbers objects for differentiation.

   The redaction assistant feature automatically masks faces (heads), people, licence plates, vehicles, documents, and technology screens for redaction during the redaction project analysis.

The Redaction editor includes the following elements:

Table 1: Redaction Editor Description for Assisted Redaction Projects

Item	Description
Select (Select and modify)	Allows moving, resizing, and deleting masks in the video. For more information, see Editing Masks for Redaction on page 73. **NOTE:** When selecting a mask, the **Manual** menu opens. The **Track object** option on the menu only applies to tracking objects that were manually masked. The additional menu options available by clicking **More** only apply to tracked and automatically masked objects.
Add (Create mask)	Allows manually masking objects for redaction in the video. For more information, see Masking Objects Manually for Redaction on page 72.
Undo/Redo	The **Undo** button reverts your changes, and the **Redo** button restores the changes that you previously undid.
Size drop-down list	Clicking the size opens the following options for adjusting the video zoom level: • **Size**: Click and drag the control to adjust the zoom level. • **Zoom in**: Click **Zoom in** or press CTRL + to increase the video size until reaching your desired zoom level. • **Zoom out**: Click **Zoom out** or press CTRL - to decrease the video size until reaching your desired zoom level. • **Zoom 100%**: Click to adjust the video zoom level by 100% **NOTE:** The default zoom level is 100%.
Redaction Effect	Click **Solid color** to change the mask effect. **NOTE:** The default **Redaction Effect** setting is **Solid color**. • **Solid color**: Changes the masks to a solid block of color and provides a set of preset colors to choose from. • **Blur**: Changes the masks to the blur effect and provides options to change their intensity level (**Low**, **Med**, or **High**). • **Pixelate**: Changes the masks to the pixel effect and provides options to change their intensity level (**Low**, **Med**, or **High**).
Chapters	Opens the list of available chapters that you can navigate to. The Redaction editor automatically segments the video into chapters. Each chapter is labeled with the video timestamp and a brief description of its con-

Item	Description
	tent. You can navigate to specific parts of the video by selecting the desired chapter from the list.
Transcript	Opens the available transcription for the video.
Render	Opens the **Render Clip** dialog box when finished with the video for redaction. The **Render Clip** dialog box allows you to name and render a segment of the video for redaction. For more information, see Rendering a Video for Redaction on page 74.
More	Displays the name of the redaction project associated with the video.
Saved	Displays the saving status of the video. **NOTE:** The Redaction editor automatically saves your changes.
Comments	Allows viewing, solving, and reopening comments that were added to the video. For more information, see Performing Redaction Comments Actions on page 74.
Help	Displays keyboard shortcuts for masking objects in the video.
<User name>	Allows logging out.
Timeline bar	Shows the playback progress of the video. You can drag the handle to navigate to different video frames. You can also hover over the timeline bar to find a specific chapter, which shows the chapter timestamp and description.
Previous frame	Allows moving back through the video, one frame at a time.
Play / **Pause**	Allows stopping or playing the video.
Next frame	Allows moving forward through the video, one frame at a time.
Playback speed	Allows changing how fast or slow you want to move through the video.
Time elapsed/Duration	Displays how much the video has been played and how long the video is.
Redact Audio	Opens the **Click to add audio effect** field for selecting segments of audio for redaction. For more information, see Selecting Audio for Redaction on page 73. **TIP:** Click and drag the **Zoom control** to adjust the zoom level of the **Click to add audio effect** field.
Volume control	Allows adjusting the volume of the video audio by clicking and dragging the control.
Display Settings	Allows managing the display of automatically and manually masked objects and comments in the video. For more information, see Managing the Redaction Display Settings on page 76.
Preview toggle	Displays a preview of the redacted video. Clicking the toggle again turns off the preview.

5.7.1

Completing a Redaction (Recommended Workflow)

NOTE: This section covers a basic workflow for users and does not cover all possible situations.

Process:

1. Ensure that you are assigned to the **Assisted redaction** role.
   For more information, see Performing Roles Actions on page 149.
2. Start a redaction.
   For more information, see Manually Redacting Incident Clips on page 58.
3. Open a redaction project.
   For more information, see Assisted Redaction Editor on page 69.
4. Manually mask objects in the video for redaction.
   For more information, see Masking Objects Manually for Redaction on page 72.
5. Select portions of the video audio for redaction.
   For more information, see Selecting Audio for Redaction on page 73.
6. Render the video for redaction.
   For more information, see Rendering a Video for Redaction on page 74.

5.7.2

Masking Objects Manually for Redaction

The **Create mask** option allows you to manually draw masks over objects for redaction when pausing the video.

Procedure:

1. Pause on the video frame that you want to edit.
2. Click + **Add (Create mask)** or press and hold SHIFT.
3. Click and drag your cursor over the desired object.
   An outline of the mask appears to show its size and shape.
4. Release your cursor when you are finished.

Result: The object is masked and the **Manual** menu opens with the following options for the masked object:

- Clicking **Track object** allows setting how long to mask the object in the video.
  For more information, see Tracking an Object for Redaction on page 73.
- Clicking 🗑 deletes the current frame.
- Clicking ⋮ **More** allows for the following actions:
  - Clicking **Go to Mask Start** jumps you to the frame where the masked object first appears.
  - Clicking **Go to Mask End** jumps you to the frame where the masked object last appears.
  - Clicking **Delete entire mask** deletes the mask from every frame in which it appears.

5.7.2.1
Tracking an Object for Redaction

The **Track object** option allows you to manually set the duration for masking an object in a video for redaction.

Procedure:

1. Perform Masking Objects Manually for Redaction on page 72.
2. In the **Manual** menu, click **Track object**.

   The Redaction editor enters Tracking Mode, providing instructions for how to track the object.
3. Click and hold the icon inside the mask to start the video.
4. Move your cursor to follow the object while the video plays.
5. Release your cursor when finished, and click **Done**.

Result: The Redaction editor exits Tracking Mode, and the object is now masked, numbered for object differentiation, and tracked.

5.7.2.2
Editing Masks for Redaction

The **Select and modify** option allows you to select a mask in the video so you can:

- Move it to mask a different object for redaction.
- Resize it to better mask the object for redaction.
- Delete it if you no longer need to mask the object for redaction.

Procedure:

1. Click **Select (Select and modify)**.
2. Select the desired mask in the video.

   The mask is highlighted and outlined with squares, and the **Manual** menu opens.
3. Perform any of the following actions:
   - To move the mask, drag and release the mask over the desired object.
   - To resize the mask, select one of the squares and drag it until you reach the desired size.
   - To delete the mask from the current frame, click .
   - To delete the mask from every frame in which it appears, select **More** → **Delete entire mask**.

5.7.3
Selecting Audio for Redaction

The **Redact Audio** option allows you to select segments of video audio for redaction.

Procedure:

1. Click **Redact Audio**.

   The **Click to add audio affect** field opens, showing the audio waveforms.

2. Click a region within the **Click to add audio affect** field.

   Your selected audio segment is highlighted for redaction, and the **Redact Audio** dialog box opens.

3. From the **Type** drop-down list, select whether the video should be **Mute** or play a **Beep** sound.

   NOTE: The default audio **Type** setting is **Mute**.

4. Optional: If you want to adjust the selected range, perform one of the following actions:
   - Enter values in the **Start** and **End** fields.
   - Drag and release either end of the audio segment.
5. Optional: If you want to select a different audio segment, perform one of the following actions:
   - Click and drag the audio segment to another region within the field.
   - To delete the audio segment, click .
6. When finished, click **Done**.
7. To check the redacted audio file, switch the **Preview** toggle to the right.
8. To close the **Click to add audio affect** field, click **Redact Audio** .

5.7.4
Rendering a Video for Redaction

The **Render** button allows you to process your video for redaction and transfer a copy to VideoManager.

Procedure:

1. Click **Render**.

   The **Render clip** dialog box opens, showing a preview of the redacted video.

2. Enter a **Clip name** for the redacted copy.
3. Optional: If you want to render a portion of the video for redaction, perform one of the following actions:
   - Enter values in the **Start time** and **End time** fields.
   - Drag and release either end of the horizontal control.
4. Click **Render clip**.

   You can find the rendered clip by filtering redactions in the **Assisted Redaction** pane in the **Incidents** tab. If successful, the clip displays status `Rendered`.

5.7.5
Performing Redaction Comments Actions

Adding Redaction Comments

You can add comments to any video frame that VideoManager users can view anytime when editing the video for redaction.

Procedure:

1. Pause on the desired video frame.
2. Right-click the desired area on the video frame.

3. Click **Add comment**.

   A comment field opens.

4. Enter your comment within the field.
5. When finished, press ENTER or click the arrow.

Result: Your comment is automatically saved and added to the video. Your VideoManager initials represent the comment on the frame. A number also appears on the icon to indicate a new comment has been added.

Viewing Redaction Comments

Procedure:

Perform one of the following actions:

Option	Actions
Viewing a Comment from a Video Frame	a. Find the comment represented by the initials of a VideoManager user name. b. Hover over the user name initials. The comment opens, showing the name of the user who added the comment and when it was added.
Viewing All Comments from the Comments List	a. Click **Comments**. The **Comments** list opens, showing both unresolved and resolved comments with the names of VideoManager users who added them.

Resolving Redaction Comments

Procedure:

Perform one of the following actions:

Option	Actions
Resolving a Comment from a Video Frame	a. Find the comment represented by the initials of a VideoManager user name. b. Hover over the user name initials. The comment opens, showing the name of the user who added the comment and when it was added. c. Click **Resolve** within the comment. The comment is resolved and removed from the video frame to which it was added. You can view resolved comments by clicking **Comments**.

Option	Actions
Resolving a Comment from the Comments List	a. Click **Comments**. The **Comments** list opens, showing both unresolved and resolved comments with the names of VideoManager users who added them. b. Click **Resolve** within the desired comment. The comment is resolved, showing the `Resolved` status.

Reopening a Resolved Comment from the Comments List

Procedure:

1. Click **Comments**.

   The **Comments** list opens, showing both unresolved and resolved comments with the names of VideoManager users who added them.

2. Find the desired resolved comment.
3. Click **Re-open** within the resolved comment.

Result: The `Resolved` status is replaced with the **Resolve** icon, and the comment reappears on the video frame to which it was added.

5.7.6
Managing the Redaction Display Settings

By default, all masks and comments in a video are visible. However, the **Display Settings** allow you to hide them.

Procedure:

1. Click .

   The **Display Settings** menu opens.

2. Perform any of the following actions:
   - To hide all automatic masks, click the **Automatically redacted** toggle.
     Clicking the **Automatically redacted** toggle again redisplays all the automatic masks.
   - To hide automatic masks individually, clear the check boxes for automatic masks for **People**, **Heads**, **Vehicles**, **Screens**, or **Documents**.
     Selecting the check boxes redisplays the automatic masks.
   - To hide all manual masks, click the **Manually redacted** toggle to switch it to the left.
     Clicking the **Manually redacted** toggle again redisplays all manual masks.
   - To hide all comments, click the **Comments** toggle to switch it to the left.
     Clicking the **Comments** toggle again redisplays all comments.

5.8
Searching Incidents

It is possible to use search functions in VideoManager to locate incidents in the **Incidents** tab, which allows you to filter through a large number of incidents quickly.

Procedure:

1. Navigate to the **Incidents** tab.
2. Select the **Search Incidents** pane.
3. Filter incidents by any of the following criteria:

Filter	Description
Saved searches	For more information, see Performing Saved Searches Actions on page 79.
Title	Searches for incidents whose name matches the one entered.
Incident Time	By using the **From:** and **To:** fields, you can search for incidents whose time matches the dates entered here. This refers to the customisable **Incident time** field you can populate when you are creating an incident, **not** the creation time of the incident itself.
Reference Code	Searches for incidents whose **Reference Code** field matches the text entered here.
Notes	Searches for incidents whose **Notes** field matches the text entered here.
Earliest date and **Latest date**	Searches for incidents whose media files were recorded between set dates.
Device operator	Searches for incidents containing media downloaded by a specified user.
Owner	Searches for incidents owned by a specified user. If you want to search only for incidents that you own, you can click **My incidents**.
Source	Searches for incidents containing media files from a specified cameras or import sources.
Match text	Searches 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 you enter `yes` into the **Match text** field, all incidents whose drop-down field has been set to `yes` are returned.

Filter	Description
	For more information, see Creating User-Defined Incident Fields on page 219.
Advanced filter	Users with knowledge of using sequence conditions can input more advanced search queries here. For more information, see Advanced Searches on page 81.

4. Select any of the following criteria:

Check Box	Description
Show current incidents	Selecting this filter includes current, that is non-deleted, incidents.
Show recently deleted incidents	Selecting this filter includes recently deleted incidents. If you have the **Reinstate** permission set to **On**, you can reinstate deleted incidents. You can do it by selecting the **Show recently deleted incidents** check box, and clicking **Find incidents**. Next to the incident to be reinstated, you can click **Reinstate incident**. **TIP:** Recently deleted incidents have a red heading.
Only show shared incidents	Selecting this filter includes incidents that have been shared with users on VideoManager.
Only show incidents with external links	Selecting this filter includes incidents that have been shared externally, using incident links. If this filter is selected, you also have the option to select the **Active external links only** check box. This filter only includes incidents whose incident links are active. That is, workers outside VideoManager can still access the incident using its link.

5. To display all incidents that match the previously set criteria, click **Find incidents**.
6. Optional: If you want to search for incidents using different parameters, perform the following actions:
   a. Click the **Filter** heading.
      The search parameters re-open.
   b. To clear the search filters, click **Clear filter**.
      You can now enter the updated criteria.
   c. To search for the relevant incidents, click **Find incidents**.

5.8.1

Performing Saved Searches Actions

Users with sufficient privileges can create saved searches for incidents. This action 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.

Creating Saved Searches

Procedure:

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

   For more information, see Searching Incidents on page 77.
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 action makes it easier to sort saved searches in accordance with workflow, for example, a category dedicated to users who only need to look at incidents that are less than five days old.

   NOTE: If the **Permission group** field is left as **Public**, anyone on VideoManager who has the permission to use saved searches is 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 Enable and Disable Permissions on page 152.
7. To save the search, click **Confirm**.

Using Saved Searches

Procedure:

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

   You can expand saved search categories using + to show all saved searches in that category.

   When you have selected a saved search, it will be searched automatically. If you want to change which saved search you use, or do not want to use a saved search at all, you should click **Clear filter**.

Editing Properties of Saved Searches

Editing properties of a saved search can be necessary if you want to change the name, or which access groups can see the saved search.

Procedure:

1. Navigate to the **Incidents** tab.
2. Select the **Search Incidents** pane.
3. In the top right-hand corner, click **Advanced**.
4. Select **Manage saved searches**.

   The saved searches are sorted by category, in order of creation. You can only view the saved searches that you have permission to view, as determined by your access groups.
5. Click **Edit**.

   You can edit the **Search name**, **Category**, and **Permission group** fields.

Editing Configuration of Saved Searches

Editing configuration of a saved search can be necessary if the filters applying to the search have changed.

Procedure:

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

   The search is performed automatically. Re-clicking the **Filter** pane opens the saved search pane again.
4. Click **Edit search**.
5. Make the required changes.
6. Click **Save search**.

   You are asked if you want to overwrite the current saved search, or create a new one.
7. Click **Update existing search**.

Deleting Saved Searches

Deleting a saved search can be necessary if the saved search has become redundant.

Procedure:

1. Navigate to the **Incidents** tab.
2. Select the **Search Incidents** pane.
3. In the top right-hand corner, click **Advanced**.
4. Select **Manage saved searches**.
5. Next to the relevant saved search, click **Delete**.

6. Confirm by clicking **Yes**.

   NOTE: A category is deleted automatically if all the saved searches within it have been deleted.

5.8.2 Advanced Searches

NOTE: Advanced searches are complex and should only be performed by administrators. For more information, see Custom Predicate Language on page 380.

An advanced search allows you to perform complex incident searches that cannot otherwise be expressed with the simple filter controls. The search can be based on user-defined incident fields and built-in fields such as **Creation Time** and **Owner**. This search can be done from the **Incidents** tab in the **Advanced Search** box.

NOTE: This field is only viewable if you have the **Search using advanced filter** permission enabled.

5.9 Bulk Editing Incidents

Bulk edits allow you to perform actions on multiple incidents at once, which is useful if there are too many incidents to manually edit or delete.

It is also useful if you have enabled your VideoManager to act as a Central VideoManager. In this case, every incident held in connected sites can be automatically fetched in bulk, which means that incidents become editable in the Central VideoManager and unviewable in the original sites.

Procedure:

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 Searching Incidents on page 77.
4. Click **Bulk edit**.

   The bulk edit user interface appears.
5. Perform one of the following actions:

   - To select individual incidents, next to their rows, click .
   - To select all incidents on-screen, click **Toggle selection of ALL rows**.

   If there is an overflow of incidents, VideoManager also gives you the option to select the incidents that are not on-screen. To manually de-select individual incidents, click on their row.
6. After you have selected incidents for bulk editing, perform any of the following actions:

   - Click **Take control**.
     If your instance of VideoManager is acting as a Central VideoManager, this action takes control of all selected incidents from the connected sites.
   - Click **Submit**.
     If your instance of VideoManager is acting as a site, this action submits all selected incidents to the connected Central VideoManager.

     For more information, see Committing Incidents on page 89.

- Click **Create incident collection**.
  If you have licenced *Nested Incidents*, this action enables you to create an incident collection containing the selected incidents.
  For more information, see Creating Incident Collections on page 92.
- Click **Delete**.
  This action deletes many incidents simultaneously.

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

5.10
Creating, Editing, and Deleting Bookmarks

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

Adding Bookmarks to Media Files

Procedure:

1. Ensure that the media file is part of an incident.
   For more information, see Creating Incidents Manually and Performing Incident Actions on page 53.
2. Navigate to the **Incidents** tab.
3. Next to the relevant incident, click **Edit incident**.
   TIP: You can find the relevant incident by navigating to the **My Incidents**, **Shared Incidents**, or **Supervised Incidents** panes. You 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 you want to add the bookmark.
5. In the media file pane, click **Play**.
6. Drag the progress bar of the media file to the position where you want to place the bookmark.
   NOTE: The media file is automatically paused.
7. Click **Bookmarks**.
   NOTE: If you cannot see the **Bookmarks** option, you are only viewing the incident, not editing it. To change into editing mode, you must click **Edit incident**.
8. Click **Add bookmark here**.
   The **Add a bookmark** window opens.
   The default name for the bookmark is the date and time position on the media file. You can overwrite the default name with your own text.

9. Click **Confirm**.

   The bookmark is added to the media file.

10. When you have added all bookmarks, click **Save incident**.

    TIP: You can immediately jump to a bookmark in a media file by clicking **Bookmarks** under the relevant media file and selecting the relevant bookmark. This action skips the media file forward or backward to the position of the relevant bookmark.

Editing Bookmarks

Editing bookmarks can be useful if, for example, you want to change the name of the bookmark.

Procedure:

1. Navigate to the **Incidents** tab.
2. Next to the relevant incident, click **Edit incident**.

   TIP: You can find the relevant incident by navigating to the **My Incidents**, **Shared Incidents**, or **Supervised Incidents** panes. You 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**.

   TIP: You can immediately jump to a bookmark in a media file by clicking **Bookmarks** under the relevant media file and selecting the relevant bookmark. This action skips the media file forward or backward to the position of the relevant bookmark.

   The **Edit this bookmark** window opens.

6. Make the necessary changes.
7. To save the updated bookmark, click **Confirm**.

Deleting Bookmarks

Deleting bookmarks can be necessary if the bookmark has become redundant.

Procedure:

1. Navigate to the **Incidents** tab.
2. Next to the relevant incident, click **Edit incident**.

   TIP: You can find the relevant incident by navigating to the **My Incidents**, **Shared Incidents**, or **Supervised Incidents** panes. You 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**.

   TIP: You can immediately jump to a bookmark in a media file by clicking **Bookmarks** under the relevant media file and selecting the relevant bookmark. This action skips the media file forward or backward to the position of the relevant bookmark.

5.11 Sharing Incidents

You can share incidents internally with other people on the VideoManager system, or externally with people who are not on the VideoManager system by using a link or an export.

Procedure:

- To share incidents internally with other users on VideoManager, see Sharing Incidents Internally on page 84.
- To share incidents externally by using a link, see Sharing Incidents Externally Using a Link on page 85.

  This method should be used if people outside VideoManager should have temporary access to an incident.
- To share incidents externally by using an export, see Sharing Incidents Externally Using an Export on page 85.

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

5.11.1 Sharing Incidents Internally

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

Procedure:

1. Navigate to the **Incidents** tab.
2. Next to the relevant incident, click **View incident**.

   TIP: You can find the relevant incident by navigating to the **My Incidents**, **Shared Incidents**, or **Supervised Incidents** panes. You can also search for the relevant incident from the **Search Incidents** pane.
3. Click **Edit sharing settings**.

   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.

   NOTE: If **Restricted** is set to **Yes**, only users with the **View any restricted incident** permission are able to view the incident when they search for it.
4. In the **Shared:** field of the **Sharing** panel, enter the name of a user to share the incident with.
5. To add the user to the list, click **+**.
6. Click **Confirm changes**.

   Added users can now find the incident using the **Only show shared incidents** filter from the **Incidents** tab.

5.11.2

Sharing Incidents Externally Using a Link

It is possible to share incidents with people who are not on the VideoManager system using links. These links allow people outside the system to view an incident without compromising the security of VideoManager. There are two types of links: **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 Configuring Incident Sharing on page 256.

Procedure:

1. Navigate to the **Incidents** tab.
2. Next to the relevant incident, click **View incident**.

   TIP: You can find the relevant incident by navigating to the **My Incidents**, **Shared Incidents**, or **Supervised Incidents** panes. You can also search for the relevant incident from the **Search Incidents** pane.
3. In the **Links** pane, click **Create a link**.
4. From the **Link type** drop-down list, select the type of link to be created.
   - An **Incident** link can be given to anyone who does not have a VideoManager account. The link expires after a user-selected period, by default a week.
   - A **Custom** link is the same as an **Incident** link, but in addition, it allows to add a description of the incident, which is viewable by people who have been given the link. The link 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 expires and the incident becomes inaccessible.
8. Optional: In the **Password (optional)** field, set the password that recipients must enter before they can view the incident.
9. Click **Create**.

   The link can be seen in the **Links** panel and you can perform a variety of actions:
   - Clicking **Send in email message** sends an email message containing the incident link to the recipient. This is only possible for **Incident** links.
   - Clicking **Show link to copy** shows the link to the incident, which can be copied. This is the only way that a **Custom link** can be shared.
   - Clicking **Update this link** allows you to edit the link.
   - Clicking **Delete link** deletes the link. This action immediately invalidates the link, and the incident cannot be viewable through this link anymore.

5.11.3

Sharing 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 media. Users can also send the export to a person outside of VideoManager using an export link.

You can export incidents in common media file formats. The following export profiles are provided by default:

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

Administrators can also create their own export profiles from the **Admin** tab, which dictates what information is included in a user's exports. For more information, see Configuring Incident Sharing on page 256.

Procedure:

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

   TIP: You can find the relevant incident by navigating to the **My Incidents**, **Shared Incidents**, or **Supervised Incidents** panes. You can also search for the relevant incident from the **Search Incidents** pane.
3. From the **Profile** drop-down list, select one of the following options:

Option	Actions
Selecting **MP4**	go to step 5.
Selecting **DVD**	**a.** Select one of the following formats to use for the ISO file: • **PAL** is common in Europe and parts of Asia and delivers a frame rate of 25 fps with 625 lines. • **NTSC** is common in the U.S. and Canada, and delivers a frame rate of 30 fps with 525 lines. **b.** Select the **Output Media** that you want to burn the ISO file to. **NOTE:** You should choose an output media type that best fits the exported media file. For example, for large ISO files (4.0 GB or more), you should use DL (double-layer) discs.

Option	Actions
Selecting **Evidence Export**	• To include the full-length media files alongside the incident and incident clips, set **Include original footage** to **On**. • To include the metadata of an incident alongside the incident, set **Include confidential metadata** to **On**.

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

NOTE: 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, the export includes them as a single continuous media file with a title and media file identification information added to the start of each incident clip.

4. If you want this incident to be prioritised when exporting, set **High priority export** to **On**.

   NOTE: Ensure that the **Enable export priority** toggle is enabled for your export profile. For more information, see Configuring Incident Exports on page 197.

5. Click **Create Export**.
6. To confirm, click **Yes**.

   While the export is being created, you can view the progress of the export from the **Status** tab.

   Once the export has finished processing, you 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.

7. Share the link by using one of the following options:

Option	Actions
Downloading an export	a. Navigate to the **Incidents** tab. b. Next to the relevant export, click **Download Export**. If VideoManager has been configured to encrypt exported `.zip` folders, you must set a passphrase in the **Passphrase** field. Make a note of this passphrase because it must be used later when you extract the `.zip`. The `.zip` folder is downloaded to the PC running VideoManager. If VideoManager has been configured to encrypt exported `.zip` folders, you must download software that can extract encrypted `.zip` folders. When you attempt to extract the `.zip` folder, you are prompted to enter the previously set passphrase.

Option	Actions
Creating an export link	a. Navigate to the **Incidents** tab. b. Select the **Exports** pane. c. Next to the export that you want to share, click > **View Export**. d. In the **Links** pane, click + **Create a link**. e. In the **Title** field, enter a title for the export link. f. In the **Recipient email** field, enter the email to which you want to send this export link. You can enter only one email address. g. 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 recipient has downloaded the export, they will have permanent access to it, even after the export link expires. h. Click **Create**. i. Perform one of the following actions: • To open a template email message with the link, click **Send in email message**. • To display the standalone link, which can be manually copied, click **Show link to copy**.

5.12
Viewing Exports

After an export is created, users with relevant permissions can view it from the **Incidents** tab.

Procedure:

1. Navigate to the **Incidents** tab.
2. Depending on how your permissions have been configured, select either the **My Exports** or **Supervised Exports** pane.
3. Next to the relevant export, click > **View Export**.

   You are able to view the following information about an export:

   - **Signature** is the unique string of letters generated by VideoManager to identify the export.
   - **Description** is the title of the export. By default, this is the name of the incident within the export.
   - **Created** is when VideoManager started to create the export.
   - **Type** is the type of export. This could be **MP4**, **DVD**, or **Evidence Export**.

- **Status** is whether the export is ready to be downloaded, or is still being created.
- **Finished** is when VideoManager finished creating the export.

  NOTE: This field is only visible if the export has been fully completed.

4. Optional: Perform any of the following actions:
   - To download the export to your PC, click **Download Export**.

     NOTE: After an export has been downloaded to a PC, VideoManager has no control over it.

   - To download the audit log of the export to your PC, click **View Export audit log**.
   - To delete the export from VideoManager, click **Delete Export**.

     NOTE: Deleting an export does not delete the original incident. Even if an export has been deleted from VideoManager, anyone who has already downloaded it will still have access to the incident within it.

5.13 Committing Incidents

If you have configured VideoManager to act as a Central VideoManager for various sites, you 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 Configuring Sites on page 297.

There are two ways to commit an incident: either by submitting it from the site, or by taking control of it from the Central VideoManager.

Procedure:

Commit an incident by using one of the following options:

Option	Actions
Submitting an incident from the site	**a.** Navigate to the **Incidents** tab of the site. **b.** Next to the relevant incident, click **Submit**. **TIP:** You can find the relevant incident by navigating to the **My Incidents**, **Shared Incidents**, or **Supervised Incidents** panes. You can also search for the relevant incident from the **Search Incidents** pane. The incident is immediately moved to the Central VideoManager. **c.** Refresh the site. The incident should be shown as **Deleted** and can no longer be edited from this instance of VideoManager. **NOTE:** Once an incident has been committed, the audit log of the incident in the original site ends immediately, and any changes made to the incident in the Central VideoManager will not be replicated in the site.
Taking control of an incident from the Central VideoManager	**a.** Navigate to the **Incidents** tab in the Central VideoManager. **b.** Next to the relevant incident, click **Take control of incident**. **TIP:** You can find the relevant incident by navigating to the **My Incidents**, **Shared Incidents**, or **Supervised Incidents** panes. You can also search for the relevant incident from the **Search Incidents** pane. The incident is immediately transferred to this instance of VideoManager. **c.** Refresh VideoManager. The incident should appear in the **Incidents** tab and can now be edited. **NOTE:** 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 look different in an audit log.

Depending on how auto-fetch settings have been configured, media files in the incident may also be transferred to the Central VideoManager as well. For more information, see Configuring Metadata/ Footage Replication on page 298.

Incidents are colour-coded depending on their state.

In the Central VideoManager:

- Incidents that have been automatically made viewable to the Central VideoManager, but have not been taken control of yet, are coloured blue.
- Incidents that 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 that have been submitted to the Central VideoManager are coloured green.
- Incidents that have been deleted on the site are coloured red.

5.14

Creating Incident Collections

Nested Incidents is a licenced feature that allows you to create incident collections, which is useful if multiple members of an organisation have all recorded the same event on different cameras. An incident collection collates these individual incidents and presents them together for convenience and ease of review.

Procedure:

1. Create an incident collection by performing one of the following actions:

If...	Then...
If you already know which incidents you want to include in the incident collection,	perform the following actions: **a.** Navigate to the **Incidents** tab. **b.** Select the **Search Incidents** pane. **c.** Filter the incidents as necessary and click **Find incidents**. For more information, see Searching Incidents on page 77. **d.** Click **Bulk edit**. **e.** Select the incidents that will be part of the incident collection. **f.** Click **Create incident collection**. The **New Incident** window opens. **g.** Create the incident collection like a normal incident. For more information, see Creating Incidents Manually and Performing Incident Actions on page 53. **h.** To save the changes, click **Create incident**.

If...	Then...
If you want to create a collection around one incident in particular, leaving the option open to add more incidents later,	perform the following actions: **a.** Navigate to the **Incidents** tab. **b.** Next to the relevant incident, click > **View incident**. **TIP:** You can find the relevant incident by navigating to the **My Incidents**, **Shared Incidents**, or **Supervised Incidents** panes. You can also search for the relevant incident from the **Search Incidents** pane. **c.** Click **Create A new incident collection**. The **New Incident** window opens. **d.** Create the incident collection like a normal incident. For more information, see Creating Incidents Manually and Performing Incident Actions on page 53. **e.** To save the changes, click **Create incident**.

2. Optional: After an incident collection has been created, add other incidents to it by performing the following actions:
   a. Navigate to the **Incidents** tab.
   b. Find the incident that you want to add to an incident collection and click > **View incident** next to it.
   c. Click **Add To existing incident collection**.
      You are presented with all incidents and incident collections.
      If you add an incident to another incident, the latter incident automatically becomes an incident collection.
      It is only possible to have two levels in an incident collection: the incident collection itself, and any incidents it contains, which means that if you add an incident collection (C1) to another incident collection (C2), all incidents within C1 are presented as children of C2, along with C1.
   d. Next to the relevant incident or incident collection, click > **Add To existing incident collection**.
   e. To save the changes, click **Create incident**.

Postrequisites: Once created, incident collections can be edited, deleted, and duplicated like normal incidents. An incident collection is like a "snapshot" of multiple incidents, which means that an incident in an incident collection is not automatically updated when it is edited. If you want to update an incident, you must re-add it to the incident collection.

Chapter 6

Devices

The **Devices** tab allows you to administer your devices, such as cameras, docks, and vehicles. From here, it is possible to view and configure all devices on the network.

If you have sufficient permissions, you can perform the following actions:

- Connect cameras and docks to VideoManager.
  For more information, see Connecting Cameras to VideoManager on page 95.

  For more information about setting up the M500 in-car video system with VideoManager, you can navigate to the Motorola Solutions Learning Experience Portal (registration is free) and search for *M500 In-Car Video System and VideoManager Explained*.
- Assign a camera. This action enables you to record media.
  For more information, see Devices Assignment and Media Recording on page 100.
- Add a new instance of M500 to VideoManager.
  For more information, see Adding Your M500 to VideoManager on page 106.
- Search for cameras, and filter them by a number of criteria.
  For more information, see Searching Cameras on page 107.
- Search for docks, such as DockControllers or Smart Docks, and filter them by a number of criteria.
  For more information, see Searching Docks on page 111.
- Search for vehicles and filter them by a number of criteria.
  For more information, see Searching Vehicles on page 112.
- Clear the serial number of the M500 if you need to move your M500 to a new vehicle.
  For more information, see Moving an M500 to a New Vehicle on page 113.
- Pre-assign a camera. This action is necessary if a remote worker is receiving their camera at home but cannot access the VideoManager system themselves.
  For more information, see Pre-Assigning Cameras on page 113.
- Edit the properties of a camera, including its name, custom status, and touch assign settings.
  For more information, see Editing Camera Properties on page 114.
- Perform camera actions, which include upgrading firmware, and factory resetting a camera.
  For more information, see Performing Camera Actions on page 115.
- Bulk edit cameras.
  For more information, see Bulk Editing Cameras on page 118.
- Perform dock actions, which include upgrading firmware, and removing a dock from VideoManager.
  For more information, see Performing Dock Actions on page 119.
- Bulk edit docks.
  For more information, see Bulk Editing Docks on page 120.

6.1
Connecting Cameras to VideoManager

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

Process:

Perform one of the following actions:

Option	Actions
Configuring both docks and a DockController	a. Configure the DockController. For more information, see Connecting DockControllers to VideoManager on page 95. b. Connect the dock(s) to the DockController. Performing this action connects the cameras to VideoManager automatically. For more information, see Connecting Docks and Cameras to DockControllers on page 96.
Configuring a standalone solo dock and connecting it directly to the PC running VideoManager	a. Perform Connecting Solo Docks to VideoManager on page 97.

6.1.1
Connecting DockControllers to VideoManager

The DockController must be configured before any cameras can be connected to VideoManager.

Procedure:

1. Plug one end of the power cable of the DockController into its power socket, and the other end into mains power.
2. Plug the Ethernet cable into the Ethernet port on the DockController.
3. Plug the other end of the Ethernet cable into any available port on the Network Switch.
4. Turn the power on at the mains.

   For more information about DockControllers, see the *DockController Quickstart Guide* which you can download at https://www.motorolasolutions.com/en_us/video-security-access-control/videomanager-ex/downloads.html.
5. On VideoManager, navigate to the **Devices** tab.
6. Select the **Search Docks** pane.
7. In the top right-hand corner, click **Advanced**.
8. Click **Generate dock config**.
9. In the **Serial** field, enter the unique serial number of the DockController.

   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.

The **Host** field should be pre-populated with the webserver of VideoManager.

11. If you want all media that pass through this DockController to have an extra layer of encryption, set **SSL** to **On**.
12. If **Use static IP** is set to **On**, enter an IP address for the DockController.
13. From the **Security** drop-down list, select whether the DockController will be protected with **802.1x (WPA2-PEAP-MSCHAPV2)** or not.
14. Click **Generate**.

    The file is saved to the default downloads location of your PC.

15. Plug the USB drive into the same PC.

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

16. Drag and drop the DockController configuration file into the root folder of the USB drive.
17. Safely eject the USB drive.
18. Plug the USB drive into one of the two DockController USB ports next to the function button.

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

6.1.2
Connecting Docks and Cameras to DockControllers

After the DockController has been configured, dock(s) can be connected. This action enables cameras to communicate with VideoManager.

Procedure:

1. Connect the dock(s) using one of the following options:

Option	Actions
Connecting a 14-slot dock to a DockController	**a.** Plug one end of the 14-slot dock's USB cable into its USB port, and the other end into one of the six USB ports on the front side of the DockController. The USB indication LED on the dock should go green, which indicates that the dock is connected to the DockController. **b.** Plug one end of the dock's power cable into its power port, and the other end into mains power. **c.** Turn the power on at the mains. The power LED on the dock should go green, which indicates that the dock is receiving power. You can repeat this procedure for up to six 14-slot docks.

Option	Actions
Connecting a solo dock to a DockController	a. Plug one end of the solo dock's USB cable into its USB port, and the other end into one of the six USB ports on the front side of the DockController. You can repeat this procedure for up to four solo docks.

2. Dock the cameras into the 14-slot dock(s) or solo dock(s).

   This action connects the cameras to VideoManager.

3. To check that the cameras have been successfully connected to VideoManager, perform the following actions:

   a. On VideoManager, navigate to the **Devices** tab.

   b. Select the **Docks** pane.

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

   c. Click > **View details**.

      In the **Connected Devices** section, you can see how many cameras are connected to the relevant DockController. You can also view the following:

      - **Device** is the serial number of the camera.
      - **Status** shows the status, such as charging, assigned, and more, of the camera.

6.1.3
Connecting Solo Docks to VideoManager

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

NOTE: The use of a solo dock is not supported. A single wired device can be used directly to test the system, but a DockController is required.

Procedure:

1. Plug the USB of the dock into the PC running VideoManager.
2. Insert the camera into the dock.
3. On VideoManager, navigate to the **Devices** tab.
4. Click **Find devices**.

   The camera should be visible, and its status should read as `Unassigned`.

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

6.1.4
Connecting VT-Series Cameras to VideoManager Remotely

There are two reasons as to why you may not be able to configure your VT-series camera using the VideoManager UI: if an administrator does not have physical access to VideoManager (for example, because it is a cloud service), or if the operator does not have access to VideoManager.

It is possible to configure a VT-series camera using a QR code. By creating a QR code, an 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.

NOTE: Some of these steps can be performed only by administrators.

Procedure:

Perform one of the following actions:

If...	Then...
If the administrator has the VT-series camera and access to VideoManager,	as the administrator, perform the following actions: **a.** Navigate to the **Devices** tab. **b.** In the top right-hand corner, click **Advanced**. **c.** From the drop-down list, select **Generate device config code**. The **Generate Device Config Code** pane opens. **d.** In the **Serial number** field, enter the serial number of the VT-series camera. **e.** From the **Network name (SSID)** drop-down list, select the network profile to 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** drop-down list. **Network name (SSID)** does not need to be the same network that VideoManager is operating on. • Select a previously created network profile. For more information, see Performing Network Profile Actions on page 178. **f.** Click **Generate code**. **g.** To connect the VT-series camera to VideoManager, follow the on-screen instructions.

If...	Then...
If the operator has the VT-series camera but does not have access to VideoManager,	as the administrator, perform the following actions: **a.** Navigate to the **Devices** tab. **b.** In the top right-hand corner, click **Advanced**. **c.** From the drop-down list, select **Generate device config code**. The **Generate Device Config Code** pane opens. **d.** In the **Info** pane, click **Launch the public version of this page**. **e.** Copy the URL and share it with the operator. As the operator, access the URL and configure the following settings: **a.** In the **Serial number** field, enter the serial number of the VT-series camera. **b.** From the **Network name (SSID)** drop-down list, select the network profile to 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** drop-down list. **Network name (SSID)** does not need to be the same network that VideoManager is operating on. • Select a previously created network profile. For more information, see Performing Network Profile Actions on page 178. **c.** Click **Generate code**. **d.** To connect the VT-series camera to VideoManager, follow the on-screen instructions.

Postrequisites: After the VT-series camera is connected to VideoManager, it can be assigned to operators like normal. For more information, see Devices Assignment and Media Recording on page 100.

6.2
Devices Assignment and Media Recording

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

There are some optional steps that administrators can complete before assigning a camera to operators. The steps are as follows:

- Creating a device profile
  This action dictates how the camera behaves in the field, including how LEDs on the camera behave when recording, the frame rate and resolution of the media file recorded on a camera, and whether the camera will pre-record.
  For more information, see Performing Device Profiles Actions on page 163.
- Enabling media file 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 media files recorded on cameras.
  For more information, see Configuring Video Metadata Overlay Settings on page 167.
- Configuring global device settings
  The global device settings dictate how all cameras connected to VideoManager behave in the field, including the default assignment mode, and how many media files can be downloaded from cameras simultaneously.
  For more information, see Configuring Device Settings on page 165.

The types of camera assignment are as follows:

- **Single issue** – The camera is assigned to the user for one trip into the field, through the VideoManager UI. When the camera is redocked, it becomes unassigned and must be reassigned manually.
  For more information, see Assigning Cameras with Single Issue on page 101.
- **Single issue** and RFID – The user taps their RFID card against an RFID reader. This assigns a camera to them for one trip into the field. When the camera is redocked, it becomes unassigned and must be reassigned again.
  This assignment mode is only possible with a dock and RFID reader.
  For more information, see Assigning Cameras with Single Issue and RFID on page 102.
- **Permanent issue** – The camera is assigned to the user through the VideoManager UI. When the camera is redocked, it stays assigned to the same user, and cannot be assigned to other users.
  For more information, see Assigning Cameras with Permanent Issue on page 103.
- **Permanent allocation** – The camera is 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 camera in the field. When the camera is redocked, it stays allocated to the same user, who must use their RFID time every time they wish to use it.
  This assignment mode is only possible with a dock and RFID reader.
  For more information, see Assigning Cameras with Permanent Allocation on page 103.
- **Bulk touch assign** – The user taps their RFID card against an RFID reader. This action assigns all cameras connected to an instance of VideoManager to that user. Bulk touch assign enables multiple people to start operating cameras quickly, because users do not need to assign the cameras first. However, because the media 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 Assigning on page 105.

6.2.1

Assigning Cameras with Single Issue

If a camera is assigned with **Single issue**, the camera is assigned to the user for one trip into the field. Once the user redocks the camera, it becomes unassigned.

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

For more information, see Configuring Device Settings on page 165.

Procedure:

1. Navigate to the **Devices** tab.
2. Select the **Search Devices** pane.
3. Filter the cameras as necessary and click **Find devices**.

   For more information, see Searching Cameras on page 107.
4. Next to the relevant camera, click **Assign Device**.

   NOTE: The camera you choose must be connected to VideoManager and unassigned. You can unassign a camera by clicking **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 camera.

   This must be a valid username on VideoManager.

   If the user's name does not appear in the drop-down menu, they do not have the ability to operate cameras and their roles must be changed before they can use a camera.

   For more information, see Performing Roles Actions on page 149.
6. From the **Assignment mode** drop-down list, select **Single issue**.
7. From the **Device profile** drop-down list, select a relevant device profile.

   The device profile determines how the camera behaves. For example, which buttons perform which actions, and more.

   For more information, see Performing Device Profiles Actions on page 163.
8. If necessary, select a previously created network profile.

   This action determines which network profile the camera will use, and is only relevant if the camera will be streaming in the field, uploading media over WiFi, or connecting to the Mobile App.

   For more information, see Performing Network Profile Actions on page 178.
9. Click **Assign Device**.

   After the **Status** column changes to `Ready`, the camera can be undocked and media files can be recorded like normal.

   When the camera is returned, the media files are automatically downloaded and the status of the camera changes first to `Busy`, and then to `Downloading`. Once the media files have finished downloading, the status changes back to `Unassigned`.

6.2.2

Assigning Cameras with Single Issue and RFID

Single issue with RFID forces users to tap their RFID cards before they can undock and operate their 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, which is useful if users will be undocking and redocking their cameras multiple times in a shift. This ensures that VideoManager will automatically assign the same camera to them.

For more information, see Configuring Device Settings on page 165.

Prerequisites: Ensure that you have an RFID reader connected to the dock associated with your instance of VideoManager, and one RFID card for every user that will be operating their cameras with **Single issue** and RFID.

You must be associated with one or more RFID cards on VideoManager. It is only necessary to do this once.

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 to be associated with the RFID card, click **Go to user**.
6. In the **Touch Assign ID** field, click .
   You are directed to an audit log of VideoManager where the recent RFID scan is visible.
7. Copy the touch assign ID from the audit log and paste it into the **Touch Assign ID** field.
8. Click **Save user**.

The RFID card is now associated with the relevant user.

NOTE: If a user should be associated with multiple RFID cards (for example, if they have a door card and a warrant card), you can repeat the procedure for as many cards as necessary, but you must separate the touch assign IDs with a comma in the **Touch Assign ID** field (for example, *<543642, 873924>*).

Procedure:

To assign a camera with **Single issue** and RFID, tap your RFID card against the RFID reader.

The device profile is chosen depending on what roles the user inhabits, and the network profile is the default one.

NOTE: If the default network profile has user-specific WiFi networks enabled, the camera connects to the user's user-specific WiFi networks

If a camera in the pool has been assigned to the user successfully, it emits a noise and its LEDs flash. The user can undock the camera and record media like normal.

When the camera is returned, the media files are automatically downloaded and the status of the camera changes first to `Busy`, and then to `Downloading`. Once the media files have finished downloading, the status changes back to `Unassigned`.

6.2.3

Assigning Cameras with Permanent Issue

If a camera is assigned with **Permanent issue**, the camera is assigned to the user indefinitely. Once the user redocks the camera, it remains assigned to them.

Procedure:

1. Navigate to the **Devices** tab.
2. Select the **Search Devices** pane.
3. Filter the cameras as necessary and click **Find devices**.

   For more information, see Searching Cameras on page 107.
4. Next to the relevant camera, click **Assign Device**.

   NOTE: The camera you choose must be connected to VideoManager and unassigned. You can unassign a camera by clicking **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 camera.

   This must be a valid username on VideoManager.
   If the user's name does not appear in the drop-down menu, they do not have the ability to operate cameras and their roles must be changed before they can use a camera.

   For more information, see Performing Roles Actions on page 149.
6. From the **Assignment mode** drop-down list, select **Permanent issue**.
7. From the **Device profile** drop-down list, select a relevant device profile.

   The device profile determines how the camera behaves. For example, which buttons perform which actions, and more.
   For more information, see Performing Device Profiles Actions on page 163.
8. If necessary, select a previously created network profile.

   This action determines which network profile the camera will use, and is only relevant if the camera will be streaming in the field, uploading media over WiFi, or connecting to the Mobile App.
   For more information, see Performing Network Profile Actions on page 178.
9. Click **Assign Device**.

   After the **Status** column changes to `Ready`, the camera can be undocked and media files can be recorded like normal.
   When the camera is returned, the media files are automatically downloaded and the status of the camera changes first to `Busy`, and then to `Downloading`. Once the media files have finished downloading, the status changes back to `Ready`, and the camera can be operated again by the same user.

6.2.4

Assigning Cameras with Permanent Allocation

Similar to **Permanent issue**, **Permanent allocation** associates a camera with a user indefinitely. Once the user redocks the camera, it remains assigned to them. However, unlike **Permanent issue**, **Permanent allocation**

forces users to tap their RFID cards before they can undock and operate their cameras, and configuration is required in order to use this feature.

Prerequisites: Ensure that you have an RFID reader connected to the dock associated with your instance of VideoManager, and one RFID card for every user that will be operating their cameras with **Permanent allocation**.

You must be associated with one or more RFID cards on VideoManager. It is only necessary to do this once.

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 to be associated with the RFID card, click **Go to user**.
6. In the **Touch Assign ID** field, click .
   You are directed to an audit log of VideoManager where the recent RFID scan is visible.
7. Copy the touch assign ID from the audit log and paste it into the **Touch Assign ID** field.
8. Click **Save user**.

The RFID card is now associated with the relevant user.

NOTE: If a user should be associated with multiple RFID cards (for example, if they have a door card and a warrant card), you can repeat the procedure for as many cards as necessary, but you must separate the touch assign IDs with a comma in the **Touch Assign ID** field (for example, *<543642, 873924>*).

Procedure:

1. Navigate to the **Devices** tab.
2. Select the **Search Devices** pane.
3. Filter the cameras as necessary and click **Find devices**.

   For more information, see Searching Cameras on page 107.
4. Next to the relevant camera, click **Assign Device**.

   NOTE: The camera you choose must be connected to VideoManager and unassigned. You can unassign a camera by clicking **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 camera.

   This must be a valid username on VideoManager.
   If the user's name does not appear in the drop-down menu, they do not have the ability to operate cameras and their roles must be changed before they can use a camera.

   For more information, see Performing Roles Actions on page 149.
6. From the **Assignment mode** drop-down list, select **Permanent allocation**.
7. Click **Assign Device**.

The device profile is chosen depending on what roles the user inhabits, and the network profile is the default one.

NOTE: If the default network profile has user-specific WiFi networks enabled, the camera connects to the user's user-specific WiFi networks.

If the camera has been allocated successfully, you can undock the camera and record media like normal.

When the camera is returned, the media files are automatically downloaded and the status of the camera changes first to `Busy`, and then to `Downloading`. Once the media files have finished downloading, the status changes back to `Allocated`.

6.2.5
Bulk Touch Assigning

It is possible to assign all docked, unassigned, unallocated cameras to one user using bulk touch assign.

Bulk touch assign is intended to be used in situations where it is necessary to deploy a large number of cameras quickly, and where there is no requirement for the cameras to be traceable to specific users.

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

Procedure:

1. Create a role that is specifically designed for bulk touch assign by performing the following actions:
   a. Navigate to the **Admin** tab.
   b. Select the **People** pane.
   c. Click the **Roles** section.
   d. Click **Create role**.
      When you 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.
   e. Click **Save role**.
2. Associate the user with an RFID card by performing the following actions:
   NOTE: It is only necessary to do this once.
   a. Tap the relevant RFID card against the reader, and wait until it emits a beep.
   b. Navigate to the **Admin** tab.
   c. Select the **People** pane.
   d. Click the **Users** section.
   e. Click **Create user**.
   f. In the **Touch Assign ID** field, click .
      You are directed to an audit log of VideoManager where the recent RFID scan is visible.
   g. Copy the touch assign ID from the audit log and paste it into the **Touch Assign ID** field.
   h. In the **Roles** panel, set the previously created role to **On**.

i. Click **Save user**.

The RFID card is now associated with bulk touch assign and the relevant user.

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

For more information, see Configuring Device Settings on page 165.

3. To use bulk touch assign, touch your RFID card to the reader.

All unassigned cameras connected to VideoManager are immediately assigned and can be used to record media.

NOTE: The cameras remain assigned for 30 seconds. Any cameras that have not been undocked after 30 seconds will be unassigned again.

When cameras have been assigned using bulk touch assign, all media recorded on those cameras are associated with that single bulk touch assign user. When creating incidents using media from bulk touch assigned cameras, VideoManager gives the option to set **Add other footage from same operator?** to **On**. Setting this option to **On** adds all media associated with the touch assign user to the incident.

6.3 Adding Your M500 to VideoManager

Procedure:

1. Navigate to the **Devices** tab.
2. Select the **Search Vehicles** pane.
3. In the top right-hand corner, click **Advanced**, and select **Configure new M500**.
4. In the **Vehicle name** field, enter the name of the vehicle.

   This field is normally the number plate of the vehicle.
5. In the **Operator name** field, enter the name of the previously created group.
6. Optional: In the **Default Owner**, enter the name of the user who should be the default owner.
7. From the **Device profile** drop-down list, select the previously created M500 device profile.
8. From the **Vehicle network profile** drop-down list, select the previously created M500 network profile.
9. Click **Create M500**.

   The M500 appears in the **Search Vehicles** tab. However, the DVR must still be configured before it can be used.
10. Configure the DVR by performing the following actions:
    a. Click **Assign Device**.
    b. Enter the same information as in the previous steps, and click **Assign Device**.
    c. Click **View device info**.
    d. Click **Download configuration**.
    e. Drag and drop the downloaded configuration file to a FAT32-formatted USB stick, in the following folder: `\Configurations\`.

f. Plug the USB stick into the M500.

If your M500 is new, it shows you all of the individual XML config files on the memory stick. Choose the correct config file that is appropriate to the M500 you are configuring and press **Load**. The M500 will then reboot and adopt the device profile.

If your M500 has been configured already, you can be prompted for an administrative password to load the new config.

6.4 Searching Cameras

Users with appropriate permissions can utilise search functions on VideoManager to locate cameras in the **Devices** tab, which can be necessary if you need to discover the status of various cameras (for example, whether they are recording, and who is using them), or if you want to assign a camera so that media can be recorded.

Procedure:

1. Navigate to the **Devices** tab.
2. Select the **Search Devices** pane.
3. Filter cameras by any of the following criteria:

Filter	Description
Device	Returns the cameras whose serial number or camera ID matches the one specified. If you want to search for multiple cameras, you should separate the values with commas (for example, *<511033, 599249>*).
Operator	Returns any cameras assigned to the operator specified, regardless of whether they are recording, charging, or more.
Location	Returns any cameras that are plugged into the EdgeController, dock, or site specified.
Status drop-down list	The options are as follows: • **All** returns all cameras on the system, regardless of the status they are in. • **Docked** returns all cameras that are physically docked to either a PC, a dock, or an EdgeController associated with the instance of VideoManager. If a VT-series camera has a WiFi pro-file with the **Enable Docking** setting enabled, they will also appear on this list when connected to the relevant WiFi network. • **Assigned** returns all cameras that have been assigned to a user on the system.

Filter	Description
	• **Assigned to me** returns all cameras that have been assigned to the user performing the search. • **Available for assignment** returns all cameras that are ready to be assigned which means all cameras which are simultaneously docked, unassigned, and have finished downloading any media. • **Stream available** returns all cameras that are connected to a WiFi network and streaming successfully to VideoManager. • **Offloading** returns all cameras that are docked and currently offloading recorded media to VideoManager. • **eSIM provisioning** returns all cameras that are in some state relating to eSIM provisioning. • **Ready** returns all cameras that are ready to be undocked (all cameras which are simultaneously docked, assigned to a user, and have finished downloading any media). • **In use** returns all cameras that are assigned to a user and undocked, as well as cameras that are streaming and recording. • **Busy, Unavailable or Unknown** returns all cameras that are **Busy** (the camera is preparing to download media to VideoManager and therefore cannot be used), **Unavailable** (the instance of VideoManager does not have the correct access control key to unlock the camera), or **Unknown** (the camera was undocked without being assigned to a user). • **Error** returns all cameras that are in an error state. The error usually occurs because the camera cannot download its recorded media (either because VideoManager has no more storage space, or because the camera is faulty). • **Unknown** returns all cameras whose status is **Unknown** (the camera was undocked without being assigned to a user). • **Allocated** returns all cameras that are assigned to a specific user but have not been tapped out with an RFID card. • **Service required** returns all cameras for whom **Service required** has been set to **On**.

Filter	Description
	For more information, see Editing Camera Properties on page 114.
Custom status	If there is a custom status assigned to the device, the filter returns the cameras that match the value entered here.
Family drop-down list	This drop-down list allows the user to select the specified camera type.
Firmware drop-down list	The options are as follows: • **Default firmware** returns all cameras running the default firmware, as specified from the **Device Images** section. For more information, see Importing, Deleting, and Editing Images on page 274. • **Non-default firmware** returns all cameras running firmware other than the default firmware. • **Other...** gives you the option to enter the name of a specific firmware image. This search is useful if you want to find specific cameras running out-of-date firmware. If you do not enter anything, all cameras are returned.
Touch assign	If **Touch assign** is set to **Yes**, all cameras with **Touch Assign** enabled are returned. If set to **No**, cameras with **Touch Assign** disabled are returned.
Auto-upgrade enabled	If **Auto-upgrade enabled** is set to **Yes**, all cameras with auto-upgrade enabled are returned. If set to **No**, cameras with auto-upgrade disabled are returned. For more information, see Configuring Firmware Settings on page 273.
Battery	This drop-down list allows the user to filter the cameras that are either **Charged** or **Charging**.
SIM Status	This drop-down list allows the user to filter the cameras depending on their SIM status. The options are as follows: • **No active SIM** • **SIM active** • **eSIM active**

If VideoManager has been configured as a Central VideoManager, you also have the option to include remote cameras in your search by selecting the ☑ **Include remote devices** check box. Selecting this check box shows the cameras associated with the connected sites of a Central VideoManager.

If you have forgotten cameras because they have been lost or are redundant, you also have the option to include these cameras in your search by selecting the **Include forgotten devices** check box.

4. After choosing relevant filters, click **Find devices**.

   You may see icons next to your cameras. Potential combinations are as follows:

Icon(s)	Description
No icon	The 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 camera is charging but has not met the minimum charge criteria for single-issue and RFID.
	The camera is charging and has met the minimum charge criteria for single issue and RFID, but RFID assignment has been disabled for this camera from the **Edit device properties** pane.
	The camera is charging, has met the minimum charge criteria for single issue and RFID, and RFID assignment is enabled for this camera. It is ready to be assigned with single issue and RFID.
	The camera is fully charged, but RFID assignment has been disabled for this camera from the **Edit device properties** pane.
	The camera is fully charged and RFID assignment is enabled for this camera. It is ready to be assigned with single issue and RFID.
	The camera is not charging. Service may be required. You should check the audit log from the **Status** tab.
	The camera is charging at a reduced charge current or not at all due to high or low ambient temperature. When using RFID assignment, fully charged cameras with no temperature warning are preferred over fully charged cameras with temperature warning.

5. Optional: To clear the search filters, click **Reset filter**.

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

Postrequisites: Once media files have been filtered, you can perform any of the following actions:

- Change viewing options.

For more information, see Changing Viewing Options on page 39.

- Click **Pause**.
  The action freezes the list, and no cameras can be added or removed until it is unpaused.
- Bulk edit cameras.
  For more information, see Bulk Editing Cameras on page 118.

6.5 Searching Docks

Users with appropriate permissions can utilise search functions on VideoManager to locate docks, such as DockControllers or Smart Docks, in the **Devices** tab, which can be necessary if you need to discover the status of various docks.

Procedure:

1. Navigate to the **Devices** tab.
2. Select the **Search Docks** pane.
3. Filter docks by any of the following criteria:

Filter	Description
Name	Returns the dock whose name matches the one entered.
Serial	Returns the dock whose serial number matches the one entered.
Version	Returns the dock whose version matches the one entered.
Configuration status drop-down list	The options are as follows: • **ALL** returns any docks, regardless of whether they are configured or not. • **Unconfigured** • **Configured**
Connection status drop-down list	The options are as follows: • **ALL** returns any docks, regardless of whether they are online or offline. • **Online** • **Offline**
Type drop-down list	The options are as follows: • **ALL** returns any docks, regardless of their type. • **DockController** • **Smart Dock**

4. After choosing relevant filters, click **Find docks**.
5. Optional: To clear the search filters, click **Reset filter**.

6.6

Searching Vehicles

Users with appropriate permissions can utilise search functions on VideoManager to locate vehicles in the **Devices** tab, which can be necessary if you need to discover the status of various vehicles.

Procedure:

1. Navigate to the **Devices** tab.
2. Select the **Search Vehicles** pane.
3. Filter vehicles by any of the following criteria:

Filter	Description
Vehicle	Returns the devices whose serial number matches the one specified. If you want to search for multiple devices, you should separate the values with commas.
Operator	Returns any devices assigned to the operator specified.
Location	Returns any devices that are available at a specified location.
Status drop-down list	The options are as follows: • **All** returns all devices on the system, regardless of the status they are in. • **Ready** returns all devices that are ready to be used. • **In use** returns all devices that are currently in use. • **New** returns all devices that have been created, but are yet to be connected to VideoManager.
Custom status	If there is a custom status assigned to the device, the filter returns the vehicles that match the value entered here.

If you have forgotten vehicles because they have been lost or are redundant, you also have the option to include these vehicles in your search by selecting the **Include forgotten vehicles** check box.

4. After choosing relevant filters, click **Find vehicles**.
5. Optional: To clear the search filters, click **Reset filter**.

6.7
Moving an M500 to a New Vehicle

If you need to move your M500 to a new vehicle, you must clear the serial number of the M500, and then create a new vehicle configuration for it. The old configuration should not be deleted, as it will be linked to historic footage.

Procedure:

1. Navigate to the **Devices** tab.
2. Select the **Search Vehicles** pane.
3. Next to the M500 to be moved, click > **View device info**.
4. In the top right-hand corner, click **Clear serial number**.

Postrequisites: Create a new vehicle profile and apply it to the M500.
For more information, see Adding Your M500 to VideoManager on page 106.

6.8
Pre-Assigning Cameras

It is possible to pre-assign a camera to a user before it has been docked, which is useful if a remote worker is receiving a brand-new camera straight to their home, but does not have access to the VideoManager interface. Once the pre-assigned camera has been docked, it is ready to record.

NOTE: Only administrators can pre-assign the camera to the user. An administrator does not need to physically dock the camera to the user's instance of VideoManager.

Procedure:

1. If the remote worker is using an EdgeController, navigate to the relevant site.

   For more information, see Viewing Sites on page 127.
2. Select the **Devices** tab.
3. In the top right-hand corner, click **Advanced**.
4. Click **Pre-assign device**.
5. When prompted, populate the following fields:
   a. In the **Operator name** field, enter the name of the operator to whom the camera will be pre-assigned.
   b. From the **Assignment mode** drop-down list, select how the camera will be pre-assigned to the operator.

      For more information, see Devices Assignment and Media Recording on page 100.
   c. From the **Network profile** drop-down list, select a previously created network profile.

      This action dictates which WiFi networks will be utilised by the VT-series camera next time it connects to VideoManager.
   d. In the **Device serial no.** field, enter the serial number of the camera that is being pre-assigned.
6. To save the changes, click **Pre-assign**.

   As soon as the camera is connected to VideoManager (for example, through a DockController), it will be assigned to the previously determined user.

6.9

Editing Camera Properties

Once a camera has been connected to VideoManager for the first time, you can edit its properties. This can be done while the camera is docked or while it is out in the field.

Procedure:

1. Navigate to the **Devices** tab.
2. Select the **Search Devices** pane.
3. Filter the cameras as necessary and click **Find devices**.

   For more information, see Searching Cameras on page 107.
4. Next to the camera to be edited, click **View device info**.
5. Click **Edit device properties**.
6. Configure any of the following settings:
   a. In the **Device name** field, change the name of the camera on VideoManager.

      By default, the name is the serial number of the camera. If the name is changed while the camera is disconnected from VideoManager, its name will be overwritten once the camera is redocked.
   b. In the **Custom status** field, record notes about the relevant camera.

      For example, if it has recently been upgraded.
      Users with only the **See devices** permission can see custom statuses for assigned cameras while users with both **See devices** and **See unassigned devices** permissions can see custom statuses for all cameras on VideoManager.
   c. Set **Service required**.

      If **Service required** is set to **Yes**, a docked camera cannot be allocated or assigned to an operator until **Service required** has been set to **No** again.
      An undocked camera will be unallocated or unassigned as soon as it is redocked.

      NOTE: If the camera is a VB400, its LEDs will glow yellow as well, which should happen either immediately (if it was already docked) or as soon as it is redocked (if it was out in the field).
   d. Set **Touch assign**.

      If **Touch assign** is set to **Yes**, the camera can be assigned or allocated with RFID.
      For more information, see Devices Assignment and Media Recording on page 100.

      NOTE: Depending on how the camera settings have been configured, it may only be possible to assign a camera using **Touch Assign** if the battery is full. For more information, see Configuring Device Settings on page 165.
   e. Set **Auto-upgrade**.

      If **Auto-upgrade** is set to **Yes**, the firmware of the camera 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 Configuring Firmware Settings on page 273.
   f. Set **Use static IP**.

      If **Use static IP** is set to **Yes**, you must enter the IP address that the camera will use. If set to **Off**, the camera will have a different IP address every time it starts recording.
7. Click **Save changes**.

6.10

Performing Camera Actions

After a camera has been connected to VideoManager, you can perform various actions on it, which include: upgrading the firmware to the latest version, factory resetting, viewing and downloading an audit log, forgetting the camera, and installing an eSIM card for V500.

Procedure:

1. Navigate to the **Devices** tab.
2. Select the **Search Devices** pane.
3. Filter the cameras as necessary and click **Find devices**.

   For more information, see Searching Cameras on page 107.
4. Next to the relevant camera, click **View device info**.

   The information pane on the camera opens.
   You can view all relevant information about your camera in the **Device details** section.

Upgrading the Firmware

Procedure:

1. Ensure that the 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 opens.
   The most recent firmware appears at the top of the list.
3. To upgrade the device, click **Upgrade Device**.

   NOTE: Downgrading firmware is not recommended. If you want to downgrade firmware, contact Motorola Solutions support first.

Factory Resetting

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

Procedure:

1. Ensure that the camera is docked and charging.
2. In the top right-hand corner, click **Factory Reset this Device**.
3. To factory reset the camera, click **Yes, Reset Device**.

   NOTE: Factory resetting a camera means that all media on it that has not already been downloaded to VideoManager will be deleted.

Recording and Live Streaming

You can prompt a VB400 to start recording remotely if the camera is connected to VideoManager either via the network profile or through the Mobile App.
You can watch a live stream of the camera if the camera is streaming to VideoManager over its network profile.

Procedure:

- To start recording, click **Start recording**.
- To stop recording, click **Stop recording**.
- To watch a live stream, click **View live stream**.

Viewing and Downloading Audit Logs

Viewing an audit log of the camera gives you insight into how the camera has been used, for example, who its operator is, when it was last undocked, and more.

Procedure:

1. In the top right-hand corner, click **View device audit log**.
2. Filter the audit log by any of the following criteria:

Name	Description
Event type	Returns specific actions performed on the camera. If you start entering an event, VideoManager will suggest various event options (for example, `DEVICE_DOCKED`.
User	Returns actions performed on the camera by the specified user. If you start entering a username, VideoManager will suggest various usernames to match it.
Message	Returns specific actions performed on the camera, whose details match the keywords entered here. For example, the `DEVICE_DOCKED` event comes with the message `Device docked`.
Signature	Returns actions performed on media files recorded by this camera in the specified incident. For example, when a media file recorded by this camera was added to the specified incident.
Location	Returns actions performed on the camera from a specific dock or EdgeController.
Client	Returns actions performed on the camera from a specific IP address.
Server	Returns actions performed on the camera from a specific server hosting VideoManager.

Name	Description
Date range drop-down list	You can select the date range for these actions.

3. Click **Filter audit log**.
4. Optional: To download an audit log, in the top right-hand corner, click **Download device audit log**.

   The audit log is downloaded to the default downloads location of your PC.

Forgetting Cameras

If a camera has been undocked from VideoManager, it can be forgotten. This action is useful if a camera has been lost or taken out of rotation, and you want to hide it from any search results for organisational purposes.

NOTE: If a camera has been forgotten, it will not appear on VideoManager until it is redocked.

Procedure:

1. In the top right-hand corner, click **Forget Device**.
2. To confirm, click **Yes**.

Installing an eSIM Card for V500

An eSIM is a virtual SIM card in the form of a QR code instead of a physical SIM. Installing an eSIM onto the V500 involves scanning the eSIM QR code with the camera. After the QR code is scanned, the V500 connects to the network provider over WiFi to download and activate the eSIM.

A valid Network Profile with WiFi internet access must be configured in VideoManager to complete eSIM provisioning. For more information on how to configure a Network Profile, see Performing Network Profile Actions on page 178.

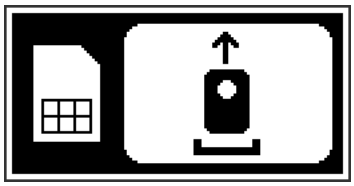
Prerequisites: Ensure that the V500 is docked and connected to VideoManager.

Procedure:

1. Select **Provision eSIM**.

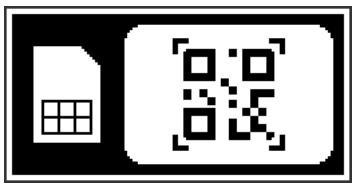
   VideoManager prompts you to specify the Network Profile to be used.
2. From the list, select a valid profile and click **Provision Device eSIM**.

   The V500 LCD displays that the device is in eSIM provisioning mode.



3. Undock the camera from the docking station.

   The camera is ready to scan your eSIM QR code when the V500 LCD display shows the following:

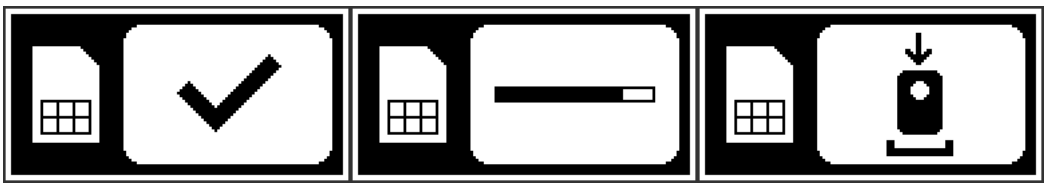


4. Scan your eSIM QR code.

   When the QR code is successfully scanned, the V500 beeps and the LCD display indicates the success.

   The V500 attempts to download and activate the eSIM, which can take several seconds. A progress bar is displayed on the LCD display.

   Once complete, the V500 beeps again and the LCD display indicates that the camera can be docked.



Postrequisites: If provisioning fails, the Dock Camera indication is displayed with a red backlight. For more information, see "eSIM Installation Troubleshooting" in the *V500 Body Camera User Guide*.

6.11 Bulk Editing Cameras

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

Procedure:

1. Navigate to the **Devices** tab.
2. Select the **Search Devices** pane.
3. Filter the cameras as necessary and click **Find devices**.

   For more information, see Searching Cameras on page 107.
4. Click **Bulk edit** and perform one of the following actions:
   - To select individual cameras, next to their rows, click .
   - To select all cameras on-screen, click **Toggle selection of ALL devices**.
5. Perform any of the following actions:
   - To assign all selected cameras, click **Assign**.
     Administrators must enter the name of the user to whom these cameras should be assigned.
   - To unassign all selected cameras, click **Return**.
   - To upgrade all selected cameras, if there is a firmware upgrade available, click **Upgrade**.
   - To reset all selected cameras, click **Factory reset**.
     The access control key and configuration of the camera will be reset.

- To update all selected cameras, click **Update**.

  You can change the following settings by clicking next to each one:

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

- To delete all selected cameras from the instance of VideoManager, click **Forget**.

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

6.12 Performing Dock Actions

After a dock has been associated with VideoManager, you can configure it from the **Docks** pane.

Prerequisites: Access any docks associated with your instance of VideoManager by performing the following actions:

1. Navigate to the **Devices** tab.
2. Select the **Docks** pane.
3. Next to the relevant dock, click **View details**.
   You can filter by **Name**, **Serial**, and **Version**.

If a dock is offline, you can view its serial number, mac address, device name, hardware revision, version, and status.

If a dock is online, you can view its serial number, mac address, device name, hardware revision, version, and status, as well as its **Bandwidth Rule** settings, and connected cameras.

Procedure:

- To change the dock's name, server settings, and IP settings, click **Configure Dock**.
- To transfer the dock from one instance of VideoManager to another, click **Configure Dock** and set **Configure for this VideoManager?** to **Off**.

  NOTE: To perform this action, you must know the API and the API secret for the other instance of VideoManager.

- To restart a dock, in the top right-hand corner, click **Restart Dock** and then, click **Yes**.
- To upgrade a dock, in the top right-hand corner, click **Upgrade Dock**, select the new dock image, and click **Upgrade Dock**.
- To download logs from a dock, in the top right-hand corner, click **Download logs from Dock**.

  The log is downloaded to your PC as a `.zip` file.

- To delete a dock from VideoManager, in the top right-hand corner, click **Delete Dock** and then, click **Yes**.
- To set the bandwidth rules and priority level for a dock, click the **Bandwidth Rule** drop-down list, and select the relevant bandwidth rule.

  For more information, see Performing Bandwidth Rules Actions on page 184.

If **High Priority Dock** is set to **On**, all media from this dock will be uploaded as quickly as possible, which means that if the dock is part of a bandwidth rule that has the **Shared bandwidth group** setting enabled, it halts the downloads of other docks in the group until all of its media has been uploaded.

- If you want multiple docks to share the same RFID reader, set **Allocate cameras from another touch assign reader** to **On** and in the **Available Dock** field, enter the name of the other dock whose RFID reader will be associated with this dock as well.

  Multiple docks can use the same RFID reader. If enabled, you can touch your RFID card to an RFID reader connected to one dock and receive a camera from either that dock or another one.

  For example, a dock A can use the RFID reader of a dock B, and a dock C can use the RFID reader of a dock A (which is actually the RFID reader of a dock B).

- To change which touch assign battery settings are used by a dock, in the **Device settings** pane, set **Device settings** to **Off**. Then, either set **Full battery required to touch assign** to **On**, or, in the **Minimum charge time** field, enter the number of minutes for which cameras must have been charging before they can be touch assigned.

  By default, a dock uses the system-wide settings configured from the **Admin** tab. Alternatively, administrators can configure a dock to have its own touch assign settings, which are different from the system-wide settings. This can be useful if, for example, users are docking their cameras at a dock temporarily, and should be able to touch assign cameras even if they are not fully charged.

- To change the time zone, from the **Time Zone** drop-down list, select the appropriate time zone.

  You can choose whether you want the cameras connected to a dock to use the time zone of the VideoManager's system or you can select a different time zone. For more information, see Setting the System Time Zone of VideoManager on page 287.

  This change can be necessary if VideoManager is hosted in a different country, or part of a country, from the dock itself. By changing the time zone of a dock, administrators can ensure video metadata from the cameras docked to the dock are displayed in local time.

  NOTE: If a non-default time zone has been selected in the device profile of the camera, the camera will use that time zone instead of the dock time zone. For more information, see Device Profiles on page 344.

6.13 Bulk Editing Docks

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

Procedure:

1. Navigate to the **Devices** tab.
2. Select the **Docks** pane.
3. Click **Bulk edit** and perform one of the following actions:
   - To select individual docks, next to their rows, click .
   - To select all docks, click **Toggle selection of ALL devices**.
4. Perform any of the following actions:
   - To upgrade all selected docks, if there is a firmware upgrade available, click **Upgrade**.
   - To restart all selected docks, click **Restart**.
     Restarting can be necessary if cameras are having difficulty connecting to VideoManager. Restarting a dock will disconnect and reconnect all cameras connected to it.

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

Chapter 7

Status

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

If you have sufficient permissions, you can perform the following actions:

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

  These messages could include system warnings, such as failed import jobs. You can click > **View system warning** to view more information about the warning.
- Manage exports and perform export actions, such as retrying failed exports, or viewing completed exports.
  For more information, see Managing Exports on page 122.
- View all scheduled and completed reports from the **Reports** pane.
  For more information, see Creating Reports and Performing Report Actions on page 124.
- Enable and configure a Central VideoManager and sites, including EdgeControllers.
  For more information, see Configuring Sites on page 297.
- Review the status of connected sites.
  For more information, see Viewing Sites on page 127.
- Review the uploads occurring at your sites from the **Site Uploads** pane.
  For more information, see Viewing Connected Site Uploads on page 128.
- Check online grids and their statuses from the **Grid** pane.
  For more information, see Viewing Grids on page 129.
- Review the comprehensive list of all actions taken on VideoManager from the **Audit Log** pane.
  For more information, see Filtering Audit Logs on page 129.
- Watch live statistics based on your infrastructure from the **Statistics** pane.
  For more information, see Viewing Statistics on page 131.
- If you have licenced *Asset Import*, you can view the status of imports that have been integrated into VideoManager.
  For more information, see Viewing Import Jobs on page 131.

7.1 Managing Exports

You can export previously created incidents. This action enables you 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 remain on VideoManager.

For more information, see Sharing Incidents Externally Using an Export on page 85.

If you have sufficient permissions, the **Manage Exports** pane enables you to view previously created exports. These exports can then be viewed or deleted to free up space on VideoManager.

Procedure:

1. Navigate to the **Status** tab.

2. Select the **Manage Exports** pane.
3. From the **Filter by State** drop-down list, select how exports are filtered.

   The options are as follows:

Name	Description
Failed exports	Shows all exports that have failed on VideoManager. For example, the export can fail if the **Exports** file space is full, and therefore no more exports can be sent there.
Pending exports	Shows all exports that are currently being processed by VideoManager. It also shows in real time what percentage of the export has been processed by VideoManager. **NOTE:** Incidents that contain multiple media files take longer for VideoManager to process than incidents with fewer media files.
Succeeded exports	Shows all succeeded exports on VideoManager. If an export has succeeded, it is ready to be shared.

Depending on the status of the export, you can perform different actions.

- If you select **Failed exports**, you can:
  - **Delete Export**.
  - **Retry all failed exports**
  - **Retry Export**

    NOTE: VideoManager does not automatically retry an export, even if more space is made available in the **Exports** file space which is why it is necessary to manually retry exports.
- If you select **Pending exports**, you can:
  - **Delete Export**

    As a result, VideoManager stops processing the export and the export is not created.

    This action does **not** delete the original incident from which the export was created.
- If you select **Succeeded exports**, you can:
  - **Delete Export**

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

    This action does **not** delete the original incident from which the export was created.
  - **Download Export**

    This action downloads an export to the default downloads location of your PC.

    This is one of two ways to share an export. The other way to share it is by using an export link. For more information, see Sharing Incidents Externally Using an Export on page 85.

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

- **View Export**
  This action allows you to see more information about an export, which includes creating a link, viewing an audit log of an export, and viewing details on an export.

  The details are as follows:

  - **Signature** is the unique signature of an export, which is automatically generated by VideoManager.
  - **Description** is the name of an export, which is not necessarily the same as the name of the original incident.
  - **Finished** is when an export finished being processed on VideoManager.

7.2
Creating Reports and Performing Report Actions

A report summarises information about how a certain aspect of VideoManager is being used. For example, administrators can check whether the system is being used correctly by other users, or review camera usage.

NOTE: Only administrators can create reports and perform report actions.

Creating Reports

Prerequisites:

- Configure report settings for VideoManager.
  These settings dictate when reports will be automatically deleted and run. For more information, see Configuring Report Settings on page 216.
- 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 Performing File Spaces Actions on page 278.

Procedure:

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** drop-down list, select the type of report to be generated.
   For more information, see Types of Reports on page 370.
6. Using the **Day starts at** field, select at what time the day should begin for this report.
   For example, an organization's work day might begin and end at 3 a.m.
   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 option can cause the report to finish the following day. For example, if **Day starts at** is set to 3 a.m., the report ends at 3 a.m. the following day.
7. From the **Schedule** drop-down list, select the relevant option.
   - **No** creates the report only once and you must choose the start and end dates that the report should cover.

- **Minutely** is only available if **Equipment** has been selected. From the **Interval** drop-down list, you can select how often the report should run.

  NOTE: VideoManager runs this report from :00 of the hour and continues regularly. For example, if you select **Every 30 minutes**, the report always runs at :00 and :30 minutes past.
- **Hourly** is only available if **Equipment** has been selected.
- **Daily** runs the report daily and you must choose how many previous days the report should cover.
- **Weekly** runs the report weekly and you must choose on which day of the week the report should run, and how many previous days the report should cover.
- **Monthly** runs the report monthly and you must choose on which day of the month the report should run, and how many previous days the report should cover.
- **Custom interval** – You must choose how often the report should run (days, weeks, or months), and how many previous days the report should cover.
- If you have already created a custom report schedule with a JSON file and imported it into VideoManager, you can select it here.

  For more information, see Configuring Report Settings on page 216.

If you have chosen to create a scheduled report, the **Number of reports retained** field appears.
In this field, you can configure how many versions of the report VideoManager should keep before the outdated ones are deleted automatically to free up space for new ones.

8. Optional: If you have created a **Report Auto Copy** file space, and have chosen a report that downloads to your PC as a CSV file, perform the following actions:
   a. Set **Auto Copy File Path** to **On**.

      For more information, see Performing File Spaces Actions on page 278.
   b. Using the **Add Field** drop-down list, choose the name of the subfolder where the report should be sent, within the file space.

      The options are as follows:

      - *<FILE_NAME>*
      - *<START_DATE>*
      - *<REPORT_TYPE>*

      You can also type in your own folders manually.
9. Click **Create**.

   The status of the report displays `Generating`. When the report is ready to be reviewed, the status changes to `Ready`.

   Non-recurring (one-off) reports can be downloaded from the **Reports** pane by clicking **Download report**.

   Recurring reports can be downloaded from the **Scheduled Reports** pane by clicking **Download latest report**.

   NOTE: If no reports have been automatically generated yet, the **Download latest report** control is not visible.

Editing Reports

Reports cannot be edited like other aspects of VideoManager, such as incidents. If you want to edit the parameters of a report, the report must be re-run.

Procedure:

1. To re-run the report, next to the relevant report, click **Re-run report**.

   The **Re-run an Existing Report** window opens.

2. Edit the parameters as necessary.

   All report parameters can be edited and there is no limit on how many can be changed.

3. Click **Create**.

   The report is re-run with the updated parameters.

Pausing Recurring Reports

Pausing a recurring report can be useful if a report should be temporarily stopped, but not deleted entirely.

Procedure:

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, which you can do by clicking **Resume Scheduled Report**.

Deleting Reports

Procedure:

Perform one of the following actions:

Option	Actions
Deleting a non-recurring report	a. Navigate to the **Status** tab. b. In the **Reports** pane, next to the report that you want to delete, click **Delete report** and confirm by clicking **Yes**.
Deleting a recurring report	a. Navigate to the **Status** tab. b. In the **Scheduled Reports** pane, next to the report that you want to delete, click **View schedule**. c. Click **Delete Scheduled Report** and confirm by clicking **Yes**.

7.3
Viewing Sites

Sites are instances of VideoManager that are connected to a Central VideoManager and enable administrators on the Central VideoManager to maintain oversight over these other instances of VideoManager, and monitor their activity. Media and incidents can also be automatically transferred from sites to a Central VideoManager.

Prerequisites: Configure your sites.

For more information, see Configuring Sites on page 297.

After you have configured your sites, you can view the status of these sites from the Central VideoManager. You can also access UI of your sites from the Central VideoManager.

Procedure:

1. Navigate to the **Status** tab.
2. Select the **Sites** pane.
3. Filter the sites by the following criteria:
   - In the **Filter by site** field, enter the name of the relevant site.
     As you type, VideoManager automatically filters the relevant results.
   - From the **Filter by status** drop-down list, filter your sites based on whether they are **Online**, **Offline**, or **Disabled**.
   - From the **Filter by upload status** drop-down list, select **All** or **Warning**.
     Selecting **Warning** returns sites which are experiencing congestion.
   - From the **Filter by last seen** drop-down list, filter your sites based on when they were last seen. The options are **Less than 4 hours ago** or **More than 4 hours ago**.

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

   You can clear the filters by clicking ✕ **Reset filter**.

   After you have filtered the sites, you can view the following columns:

Name	Description
Site	The name of the site, which can be configured when initially creating the site.
Status	The status of a site can be ⬆ `Online`, ⬇ `Offline`, or ✕ `Disabled`. **NOTE:** A site can be ⬇ `Offline` if the EdgeController hosting the site is turned off, or the network between the site and Central VideoManager is disconnected.
Version	The version of VideoManager running on the site.
Last seen	When the site was last connected to VideoManager.

Name	Description
	If the site is Online, this column reads as Connected.
Uploading	If the site is in the process of uploading media or incidents to the Central VideoManager, this column details the number of jobs running. For more information about the job(s), you can click .

7.4

Viewing Connected Site Uploads

After sites have been configured, the **Site Uploads** pane can be used to monitor all uploads from the sites to the Central VideoManager, and you can view the progress of site uploads.

Procedure:

1. Navigate to the **Status** tab.
2. Select the **Site Uploads** pane.
3. Filter the sites by the following criteria:
   - From the **Site** drop-down list, select from which site the uploads are filtered or you can leave it as **Any site**. This option returns uploads from all sites.
   - From the **Status** drop-down list, filter site uploads by their status. The options are as follows:
     - **Active uploads only** includes uploads that are currently in progress, as well as uploads that are queued.
     - **Include failed uploads** includes both active and failed uploads.
       The upload can fail if, for example, the media was deleted from the site before it had a chance to be uploaded.
     - **Include failed or completed** includes both active and failed uploads, as well as uploads that have been completed.

     TIP: If you select **Include failed uploads** or **Include failed or completed**, you can also filter the results by time frame, using the **Filter by Completion Time** drop-down list.

After you have filtered the sites, you can view the following columns:

Name	Description
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 the upload. **Description** includes Metadata upload (camera information and audit logs) and Media (the URN of the media file is included in the entry).

Name	Description
Status	The status of the upload can be `Upload Complete` or `Upload Cancelled`. If the status is `Upload Cancelled`, you can click **Retry this upload**.

7.5 Viewing Grids

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 media files.

NOTE: Only users with the **View grid status** permission can access the **Grid** pane.

Regular users cannot add, edit, or delete grids. The following procedure describes how to access worker statuses and logs which are the main aspects of grids, and can be accessed by regular users.

Procedure:

1. Navigate to the **Status** tab.
2. Select the **Grid** pane.
3. Click **View worker details** and perform any of the following actions:
   - To check the status of a grid, click **Worker settings check**.
     This action opens a window which displays the status of the grid's URLs.
   - To download grid logs, click **Download logs**.
     The `.zip` folder is downloaded to the PC running VideoManager. The folder contains a `.txt` file of the grid's logs.

   For more information about setting up grids with VideoManager, you can navigate to the Motorola Solutions Learning Experience Portal (registration is free) and search for *VideoManager and Grids Explained*.

7.6 Filtering Audit Logs

An audit log is a record of all actions that have been undertaken by the system, and who performed them, which enables administrators to keep tabs on which users, cameras, and sites are performing which actions. An audit log cannot be edited or deleted, only filtered.

Procedure:

1. Navigate to the **Status** tab.
2. Select the **Audit Log** pane.
3. Filter the audit logs by any of the following criteria:

Filter	Description
Source	Views all actions undertaken by the specified camera (to do that, you must enter the serial number) or import source.
Event type	Views all instances of the specified action taking place, such as creating an incident, or a report. By typing in the relevant action, various matches appear for you to select.
User	Views all actions undertaken by a specific user on VideoManager.
Message	Views all messages whose text matches what is entered here. A message could be any text entered when searching for an incident or media file, for example, by entering text into the **Title** field in the **Search Incidents** pane.
Signature	Views all actions performed on an incident with the same signature as the one specified here.
Media ID	Views all actions performed on a media file with the same URN as the one specified here.
Location	Views all actions performed in a location as the one specified here. For example, a dock or EdgeController
Search by file hash	Views all actions performed on a media file whose digest matches the file hash entered here. You can either enter the file hash manually or click **Read from file** and select the file from your PC
Date range drop-down list	You can select a specific time period. All actions undertaken within that time period are returned. The options are as follows: **None**, **In the last day**, **In the last 7 days**, **In the last 30 days**, or **Custom** where you can choose two dates to filter between.

4. Optional: Perform any of the following actions:

   - To clear the search filters, click **Reset filter**.
   - To view the audit log, click **Filter audit log**.

     The audit log is presented to you immediately and you can click **Download CSV** to download the audit log to your PC.
   - To create a report based on the filters you have selected, click **Create report**.

     If you choose this option, you must enter a title for the report, and decide if you want the report to be scheduled or not.

     For more information, see Creating Reports and Performing Report Actions on page 124.

7.7
Viewing Statistics

The **Statistics** pane is located in the **Status** tab and shows statistics relating to your VideoManager infrastructure in real time.

Procedure:

Hover your 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 cameras visible to VideoManager, and what state they are in.
- The **Docks** pane shows the number of DockControllers and Smart Docks visible to VideoManager, and whether they are connected or disconnected.
- The **Vehicles** pane shows the number of vehicles visible to VideoManager, and their current status.
- 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 media stored by VideoManager.
- The **Footage written today** pane shows the number of megabytes of media stored by VideoManager that day.
- The **Footage write rate** pane shows how much media has been written to disk by time.
- The **User activity** pane shows how many users are logged in by time.
- The **Media recording counts** pane shows the number of media files recorded in the past seven days.
- The **Total media in system** pane shows the total number of media files 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. You can click **Show file space breakdown** for more information.

7.8
Viewing Import Jobs

NOTE: Users with the *Media file Import* licence can import a variety of files into VideoManager, including still images and PDFs. However, only administrators can view the status of these import jobs.

Procedure:

1. Navigate to the **Status** tab.
2. Perform one of the following actions:
   - To view all import jobs, select the **Imports** pane.
   - To view only your own import jobs, select the **My Imports** pane.
3. Using the **Filter by state** drop-down list, filter the imports by any of the following criteria:
   - **Failed import jobs** shows any import jobs which failed on VideoManager.
   - **In-progress import jobs** shows any import jobs that are still in progress.

- **Completed import jobs** shows any import jobs that have been completed.
- **Earliest date** and **Latest date** fields filter import jobs by date.

4. Optional: Perform any of the following actions:
   - To view information about the **Signature** and **Status** of the import job, as well as when the job started and finished, click > **View details**.
   - To delete an import job, click **Delete**.
     If you have filtered import jobs using either the **Failed import jobs** filter or the **In-progress import jobs** filter, and clicked **Delete**, the media file will not be imported.

     If you have filtered import jobs using the **Completed import jobs** filter, and clicked **Delete**, only the import job is deleted. The media file will **not** be deleted from VideoManager.

Chapter 8

Tactical

The **Tactical** tab enables you to see the locations of your cameras represented on a live map.

NOTE: The **Tactical** tab is only visible if you have a *Tactical VideoManager* licence.

8.1 Performing Actions on the Tactical Tab

Prerequisites:

1. Configure a camera to live stream like normal.
   For more information, see Configuring Streaming on page 292.
2. Enable maps.
   For more information, see Enabling and Configuring Maps on page 270.

If cameras are GPS-enabled, they automatically appear on the **Tactical** tab.

Cameras only appear if they are live streaming. If they are recording but not live streaming, they do not appear on the **Tactical** tab.

After the cameras have appeared on the **Tactical** tab, you can perform the procedure.

Procedure:

Perform any of the following actions:

Option	Actions
Viewing the live stream of a camera	There are two ways of performing this action: • On the map, click the pin. • In the top right-hand corner list, click the name of the camera. The live stream appears in the bottom right-hand corner pane. **NOTE:** If you are viewing the live stream of an M500, you can change the camera angle or microphone from the drop-down list in the preview panel.

Option	Actions
Following a camera	**a.** Follow the relevant camera, either by clicking the pin on the map, or by clicking in the top right-hand corner list the name of the camera. **b.** In the leftmost column of the list, select the ■ check box. The map "follows" the camera until the check box is unselected. In this mode, the map automatically scales and moves to ensure that the followed cameras are never off-screen.
Viewing and performing actions on the Global or User Video Wall	**a.** Ensure that you have the relevant toggles enabled. For more information, see Configuring Tactical on page 272. **b.** Perform any of the following actions: • To open the Global Video Wall, in the top left-hand corner, click the **Open the Video Wall page** button. • To open the User Video Wall, in the top left-hand corner, click the **Open My Video Wall page** button. The wall opens in a new tab. **c.** Perform any of the following actions: • To change the number of live streams shown on the wall simultaneously, in the top right-hand corner, click the button. This action switches the wall between a 1-screen, 4-screen, and 9-screen view. • To change whether the wall is full-screen or not, in the top right-hand corner, click the button. • To remove a live stream from the wall, click **Clear panel**.

Option	Actions
Adding live streams to the Global or User Video Wall	This option gives you a fullscreen view of selected live streams. **a.** Focus on the relevant camera, either by clicking the pin on the map, or by clicking in the top right-hand corner list the name of the camera. **b.** In the bottom right-hand live stream pane, perform any of the following actions: • To add the live stream to the Global Video Wall, click **Add to Global Wall**. • To add the live stream to the User Video Wall, click **Add to User Wall**. **NOTE:** If you are streaming on an M500, you can change the camera angle or microphone by using the relevant buttons on the wall. The selected angle will appear on the wall.
Adjusting the map	perform any of the following actions: • To zoom in or out, in the top left-hand corner, click the + / − buttons. • To turn on the trail of the cameras, in the top left-hand corner, click the button. This action shows you a trail behind every camera, tracking their most recent movements. • To change whether the camera following is set to **On** or **Off**, in the top left-hand corner, click the button. If you follow a camera, this setting is turned on automatically. You can turn this feature off temporarily if you need to view an aspect of the map that is off-screen. When you change it back to **On**, the same cameras are followed as before.

Chapter 9

Admin

The **Admin** tab provides access to system administration functions.The tab is divided into panes, which are divided further into sections. You can find the relevant section by typing the name into the filter box at the top of the **Admin** tab.

The panes and sections are as follows:

- The **People** pane is divided into the following sections: **Users**, **Groups**, **Roles**, **Authentication**, **Two Factor Authentication**, **User Self Service**, and **User Import Settings**.
  For more information, see People on page 136.
- The **Devices** pane is divided into the following sections: **Device Profiles**, **Device Settings**, **Video metadata overlay settings**, **Access Control Key Management**, **Device Certificate Authorities**, and **Device security**.
  For more information, see Devices on page 162.
- The **Connectivity** pane is divided into the following sections: **ONStream**, **Network Profiles**, **Vehicle network profiles**, **LTE APNs Bandwidth Rules**, **Metadata/Footage Replication**, **Configuration Replication**, **Site Manager**, **Streaming Server**, and **Email Properties**.
  For more information, see Connectivity on page 174.
- The **Policies** pane is divided into the following sections: **Deletion Policy**, **Incident Exports**, **File Exports**, **Auto Incident Creation**, **Password Complexity**, **Reports**, **User-defined Incident Fields**, **User-defined Media Fields**, **User-defined Playback Reason Fields**, **User-defined Share Reason Fields**, **Import profiles**, **Antivirus Policy**, **Incident Sharing**, **Playback Policy**, **Playback Watermark**, **Mobile App Settings**, and **API Key Management**.
  For more information, see Policies on page 190.
- The **User Interface** pane is divided into the following sections: **Login Settings**, **Media List**, **Messages**, **Theme Resources**, **Player**, **Language**, **Maps**, **Thumbnails**, **Incidents**, and **Tactical**.
  For more information, see User Interface on page 261.
- The **Firmware** pane is divided into the following sections: **Firmware Settings**, **Device Images**, **Vehicle Images**, **LTE Images**, and **Dock Images**.
  For more information, see Firmware on page 273.
- The **System** pane is divided into the following sections: **Storage**, **Web Server**, **Backup Databases**, **Licences**, **Advanced Settings**, **System Time Zone**, **Import/Export System Config**, **Preview Features**, and **Server Controls**.
  For more information, see System on page 275.
- **Legal**
  For more information, see Viewing Legal Information on page 289.

9.1 People

In the **People** pane, you can edit aspects of VideoManager related to users and roles.

From the **People** pane, you can access the following sections:

- In the **Users** section, you can perform the following actions:
  - Create, edit, and delete users.
    For more information, see Creating, Editing, and Deleting Users on page 138.
  - Reassign users. This action transfers all media files and incidents from one user to another.
    For more information, see Reassigning Users on page 141.
  - Unlock users. If users cannot access VideoManager because they have entered their password incorrectly too many times, you can manually grant them access again.
    For more information, see Unlocking Users on page 141.
  - Export and import users and groups. You can download your entire database of users and groups to a CSV file, edit it, then reupload it, which makes it easy to bulk edit users and groups.
    For more information, see Exporting and Importing Users and Groups on page 142.
  - View a user's device affinities. If configured, this action shows a list of cameras that have been assigned to the user with single issue, undocked, and then redocked mid-shift.
    For more information, see Viewing and Clearing Device Affinities for Users on page 143.
- In the **Groups** section, you can perform the following actions:
  - Create, edit, and delete groups.
    For more information, see Creating, Editing, and Deleting Groups on page 144.
  - Create a group for use with the M500.
    For more information, see Creating a Group for Use with the M500 on page 147.
  - View the effective permissions for a user or group. This action details the aspects of VideoManager to which a user or group has access, and how they got their per-missions (for example, from a role, or because they belong to a group).
    For more information, see Viewing Effective Permissions for Users or Groups on page 148.
- In the **Roles** section, you can perform the following actions:
  - Create, edit, copy, import, export, and delete roles.
    For more information, see Performing Roles Actions on page 149.
- In the **Authentication** section, you can perform the following actions:
  - Configure how users can log on to VideoManager.
    For more information, see Configuring Authentication Settings on page 153.
  - Create Client Certificate Authentication realm for configuring the Client Certificate Authentication logon.
    For more information, see Creating Client Certificate Authentication Realm on page 153.
- In the **Two Factor Authentication** section, you can perform the following actions:
  - Enable and configure two factor authentication on VideoManager. This action prompts specific users to enter a code provided by their phone before they can log on to VideoManager, in addition to entering their password as normal.
    For more information, see Enabling Two Factor Authentication on page 154.
  - Enable and configure email login on VideoManager. This action prompts specific users to click a link sent to their email before they can log on to VideoManager, in addition to entering their password as normal.
    For more information, see Enabling and Configuring Login by Email on page 156.
- In the **User Self Service** section, you can perform the following actions:

- Configure user self-service. This action dictates whether users can reset their own passwords, and whether workers can create their own users on VideoManager.
  For more information, see Configuring User Self Service on page 158.

- In the **User Import Settings** section, you can perform the following actions:
  - Configure the built-in user import tool. This action enables you to import multiple users or groups simultaneously from a CSV or XLS/XLSX file.
    For more information, see Built-In User Import Tool Configuration on page 162.

9.1.1

Creating, Editing, and Deleting Users

A user is assigned to every person using VideoManager. Different users have varying levels of control over the system, depending on how they have been configured.

As well as creating users manually, it is also possible to configure VideoManager so that workers can create their own users. For more information, see Configuring User Self Service on page 158.

Creating Users

Procedure:

1. Navigate to the **Admin** tab.
2. Select the **People** pane.
3. Click the **Users** section.
4. In the top right-hand corner, click **Create user**.
5. In the **User name** field, enter a name for the user.

   NOTE:
   Each user must have a unique username. The username can be changed later but it cannot be changed to another user's username.

   If the user is assigned to a camera that is still in the field, the camera becomes associated with the "deleted" user, which is the old username, as well as any media that is still on the device.
6. In the **Password** field, enter a password for the user.

   NOTE: After you enter the password, the **User must change password** toggle is automatically set to **On** and the user is prompted to set their own password the first time they log on.

   You should configure when the password should expire from the **Password Complexity** section. For more information, see Configuring Password Complexity on page 215.
7. To confirm the password, in the **Confirm password** field, enter the same password.
8. In the **Display name** field, enter a display name for the user.

   The display name can be changed later.
9. Optional: In the **Email notifications** field, enter an email address for the user.

   Users can receive notifications via email when specific actions are performed on VideoManager. The exact actions that 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 on 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 on.

10. In the **Touch Assign ID** field, enter the touch assign ID to identify a user's RFID card with a camera.

    This field is only relevant if the user is assigned a camera with RFID. For more information, see Devices Assignment and Media Recording on page 100.

    If you want to find the RFID value of a card, you must touch the relevant card to the RFID reader and click in the **Touch Assign ID** field. This action shows a list of failed touch assign scans. The most recent entry is for that failed scan, which you can copy and paste into the **Touch Assign ID** field.

    NOTE: If a user should be associated with multiple RFID cards (for example, if they have a door card and a warrant card), you can repeat the procedure for as many cards as necessary, but you must separate the touch assign IDs with a comma in the **Touch Assign ID** field (for example, *<543642, 873924>*).

11. If you want to enable the user to log on to VideoManager, set **Enabled** to **On**. Otherwise, set the toggle to **Off**.

12. In the **Roles** pane, select the roles that the user should inhabit.

    This action determines which aspects of VideoManager the user can see and interact with.

    The user's roles can be changed later. For more information, see Performing Roles Actions on page 149.

13. In the **Group memberships** pane, select the groups to which the user should belong, enter the name of a previously created group, and click +.

    The groups can be changed later. For more information, see Creating, Editing, and Deleting Groups on page 144.

14. In the **Sharing** pane, select the sharing options required for the user.

    The options are as follows:

    - **Auto share with** – Any users or groups entered here have access to all media files, incidents, and exports created by the new user.

      NOTE: Users cannot see who their media files are auto-shared with, or if they are auto-shared at all.

    - **For new media, create shares for** – Any users or groups entered here are automatically entered into the **Shared:** field of new media files recorded by the new user.

      This option is useful if certain users or groups should have access to media files 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 are automatically entered into the **Shared:** field of new incidents created by the new user.

      This option 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 media files, which **Auto share with** would grant.

    - **Supervisor of** – Any users or groups entered here are supervised by the new user, which means that the user can view their media files, incidents, and exports from the **Supervised Media**, **Supervised Incidents**, and **Supervised Exports** panes.

15. To add the user or group, click +.

16. If required, from the **WiFi networks** pane, add user-specific WiFi networks by clicking **Add network**.

These networks only appear on the user's account, and are not viewable by other users on the system. For more information, see Creating User-Specific WiFi Networks on page 295.

17. Click **Create user**.

Editing Users

It can be necessary to edit a user if their password should be changed, or if they should be assigned to different roles.

Procedure:

1. Navigate to the **Admin** tab.
2. Select the **People** pane.
3. Click the **Users** section.
4. Locate the user to be edited by filtering users in one of the following ways:
   - In the **Name** field, enter the user's username or display name.
   - In the **Authentication ID** field, enter the user's authentication ID.
   - In the **In group** field, enter the group name of the user's group.
     If you enter a group name in the **In group** field, you have the option to change if **Only immediate members** is set to **On** or not. If set to **On**, only users that are assigned directly to the specified group are 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.
   - In the **Email** field, enter the user's email.
   - From the **Role** drop-down list, select the user's relevant role.

   You can click ✕ to reset the filter.
5. Click **Find**.
6. Next to the user to be edited, click > **Go to user**.
7. Make the necessary changes and click **Save user**.

Deleting Users

If a worker leaves an organisation, it can be necessary to delete their user from VideoManager. Deleting a user does not delete any of their media files or incidents.

Optionally, you can reassign the relevant user to another user on VideoManager. This action transfers all of their incidents, exports, and media files to the other user. For more information, see Reassigning Users on page 141. If the user is not reassigned, the **Operator** field for their media files reads as *<deleted user's name>* (DELETED). If a user is later recreated with the same username, all of the media files, exports, and incidents associated with that username are automatically associated with that user.

Procedure:

1. Navigate to the **Admin** tab.
2. Select the **People** pane.
3. Click the **Users** section.
4. Locate the user to be deleted by filtering users in one of the following ways:
   - In the **Name** field, enter the user's username or display name.

- In the **Authentication ID** field, enter the user's authentication ID.
- In the **In group** field, enter the group name of the user's group.
  If you enter a group name in the **In group** field, you have the option to change if **Only immediate members** is set to **On** or not. If set to **On**, only users that are assigned directly to the specified group are 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.
- In the **Email** field, enter the user's email.
- From the **Role** drop-down list, select the user's relevant role.

You can click ✕ to reset the filter.

5. Click **Find**.
6. Next to the user to be deleted, click > **Go to user**.
7. Click **Delete user**.
8. In the confirmation window, click **Yes**.

9.1.2
Reassigning Users

Reassigning a user transfers all of their media files and incidents to another user. This action is advised if a user has left an organisation and they should no longer have access to VideoManager, or if an organisation plans to reuse usernames on VideoManager. After a user is recreated with the same username as a previously deleted user, all media files and incidents associated with that username are 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.

Procedure:

1. Navigate to the **Admin** tab.
2. Select the **People** pane.
3. Click the **Users** section.
4. In the top right-hand corner, click **Reassign user**.
5. In the **Current owner** field, enter the name of the user whose media files and incidents will be transferred.

   If the user still exists on VideoManager, their name pops up when typed in. If the user has been deleted, their name does not pop up when typed in, but is available for reassignment.
6. In the **New owner** field, enter the name of the user who should receive the media files and incidents.
7. Click **Reassign**.

9.1.3
Unlocking Users

You 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. If a user's account is locked, they cannot log on to VideoManager until their account is either unlocked by VideoManager automatically, or by an administrator manually.

Procedure:

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 reads as `Locked` and it has an icon next to its username.
5. Set **Unlock now** to **Yes**.

   TIP: If the user made too many incorrect login attempts because they forgot their password, you can also reset their password from this pane by entering the new password in the **Password** and **Confirm password** fields.
6. Click **Save user**.

9.1.4

Exporting and Importing Users and Groups

You can download the database of users and groups to a CSV file, which enables you to edit the database in Excel, then reupload the same CSV file to VideoManager.

Exporting the Database from VideoManager

Procedure:

1. Navigate to the **Admin** tab.
2. Select the **People** pane.
3. Click the **Users** section.
4. Click **Export users and groups**.

   The CSV file is downloaded to your PC containing information about the users and groups. The file includes the users' roles and relationships, such as which users belong to which groups. You can edit the file in Excel.

Importing the Database into VideoManager

After editing the file, you can import the database back into VideoManager.

Procedure:

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 automatically performs a "dry run", allowing you to preview the changes before they come into effect. The following fields display:

   - **Users and groups added:** lists the number of users and groups which are in the CSV file but not on VideoManager.
   - **Users and groups updated:** lists the number of users and groups whose data in the CSV file does not match the data on VideoManager.
   - **Users and groups removed:** lists the number of users and groups which are on VideoManager but not in the CSV file.

6. Click **Import**.

   The following changes take place:

   - All users and groups which are in the CSV file but not on VideoManager are added.
   - All users and groups whose data in the CSV file does not match the data on VideoManager are updated.
   - All users and groups which are on VideoManager but not in the CSV file are deleted.

Postrequisites: You can import the CSV file into a **new** instance of VideoManager. This action copies the database at the time of export, and may be useful if you do not want to configure the built-in user import tool. To do so, follow the same procedure for importing users and groups but 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 fails.

To import a role:

1. Navigate to the **Admin** tab.
2. Select the **People** pane.
3. Click the **Roles** section.
4. Click **Export role**.
5. On the new instance of VideoManager, navigate to the same place, and click **Import role**.

9.1.5
Viewing and Clearing Device Affinities for Users

If **Enable shift-long field trips** has been set to **On** from the **Devices** section, all users who have been assigned a camera with single issue (either with RFID or through VideoManager) have an affinity with their camera. This means that if they dock their camera in the middle of their shift, VideoManager makes a note of the connection and allows them to undock the same camera later in the shift. You can view these affinities from the **Edit user** pane.

Procedure:

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 opens.

   The window shows all cameras that have been associated with the user via single issue (either with RFID or through VideoManager), undocked, and then redocked again.

   The window can be empty for one of the following reasons:

   - The camera has not been docked yet.

     The affinity is not created until the camera is docked within the user's shift for the first time
   - The camera was assigned to the user with permanent issue which does not create an affinity between the user and the camera, because the same camera is always associated with the user.
   - When the camera was redocked, it charged fully.
   - When the 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. To clear the affinity, click **Clear**.

   If the user docks the camera during their shift, the camera returns 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 camera assigned to them on VideoManager, before they can record more media during their shift.

   For more information, see Configuring Device Settings on page 165.

7. To return to the **Edit user** pane, click **Close**.

9.1.6

Creating, Editing, and Deleting Groups

You can create groups to associate certain users with each other. This action can be necessary if an organisation wants to share certain media files or incidents with lots of users at once, or if certain users should supervise other users. Groups can be members of groups themselves.

Creating Groups

Procedure:

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 field cannot be edited later.
6. In the **Display name** field, enter a display name for the group.

   NOTE: 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 that should apply to all users in this group.

   This action does not add all users that inhabit the role to the group.

8. In the **Group memberships** pane, enter the names of the groups to which this group should belong, and to add the user or group, click +.

   You can also add individual users to groups from the user's page. For more information, see Creating, Editing, and Deleting Users on page 138.

9. In the **Sharing** pane, configure any of the following fields.

   The options are as follows:

Option	Description
Auto share with	Any users or groups entered here have access to all media files, incidents, and exports created by the group. **NOTE:** Users in a group cannot see who their media files 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 media, create shares for	Any users or groups entered here are automatically entered into the **Shared:** field of new media files recorded or imported by the users within this group. This option is useful if certain users or groups should have access to media files recorded or imported 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 are automatically entered into the **Shared:** field of new incidents created by the users in this group. This option is useful if certain users or groups should have access to incidents created by the users in this group, but should not have access to all of their exports or media files, which **Auto share with** would grant.
Supervisor of	This option 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. **NOTE:** The supervision applies to incidents, exports, and cameras.

10. To add the group, click +.

11. Optional: In the **WiFi networks** pane, create user-specific WiFi networks that should only be available to all users in the group.

    This action can be necessary if all users in a group will be live streaming media with their cameras, over a specific hotspot.

12. Click **Create group**.

    After a group has been created, other users and groups can be added to it. For more information, see Creating, Editing, and Deleting Users on page 138.

Editing Groups

Procedure:

1. Navigate to the **Admin** tab.
2. Select the **People** pane.
3. Click the **Groups** section.
4. Locate the group to be edited by filtering groups in one of the following ways:
   - In the **Name** field, enter the group's username or display name.
   - In the **In group** field, enter the group name.
     If you enter a group name in the **In group** field, you have the option to change if **Only immediate members** is set to **On** or not. If set to **On**, only groups that are assigned directly to the specified group are 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.
   - From the **Role** drop-down list, select the group's relevant role.

   You can click ✕ to reset the filter.
5. Click **Find**.
6. Next to the group to be edited, click > **Go to group**.
7. Make the necessary changes and click **Save group**.

Deleting Groups

If a group becomes redundant, it can be deleted. Deleting a group does not delete any of the users within it. Instead, it immediately affects what those users can see on VideoManager, and to which media files/exports/incidents they have access.

Procedure:

1. Navigate to the **Admin** tab.
2. Select the **People** pane.
3. Click the **Groups** section.
4. Locate the group to be edited by filtering groups in one of the following ways:
   - In the **Name** field, enter the group's username or display name.
   - In the **In group** field, enter the group name.
     If you enter a group name in the **In group** field, you have the option to change if **Only immediate members** is set to **On** or not. If set to **On**, only groups that are assigned directly to the specified

group are 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.

- From the **Role** drop-down list, select the group's relevant role.

You can click ✕ to reset the filter.

5. Click **Find**.
6. Next to the group to be deleted, click > **Go to group**.
7. Click **Delete group**.
8. In the confirmation window, click **Yes**.

   If users belong to the deleted group, their permissions and abilities are 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' media files/exports/incidents.

9.1.7
Creating a Group for Use with the M500

Unlike body-worn cameras, where one user is assigned to one camera, the M500 should be assigned to a group of users. All users within this group will be then able to log on to using the control panel, and operate the M500 in the field. You must manually create this group on VideoManager.

Procedure:

1. Navigate to the **Admin** tab.
2. Select the **People** pane.
3. Click the **Groups** section.
4. In the top right-hand corner, click **Create group**.
5. Enter a name for the group.

   For example, `M500 Users`
6. Optional: In the **Display name** field, enter a display name for the group.

   The display name can be changed later.
7. In the right-hand **Roles** pane, ensure that **Vehicle Operator** is set to **On** for the group.
8. Click **Create group**.
9. Add all of the users to be operating M500s to this group by performing the following actions:
   a. Navigate to the **Admin** tab.
   b. Select the **People** pane.
   c. Click the **Users** section.
   d. Next to the relevant user, click > **Go to user**.
   e. In the **Group memberships** section, enter the previously created group name and click +.
   f. Click **Save user**.

9.1.8

Viewing Effective Permissions for Users or Groups

After a user or group has been created, their effective permissions can be viewed, which gives administrators insight into how the user or group's permissions and roles interact with each other.

Procedure:

1. Navigate to the **Admin** tab.
2. Select the **People** pane.
3. Click either the **Users** or **Groups** section.
4. Next to the relevant user or group, click **Go to user** or **Go to group**.
5. Click **View effective permissions**.

   The following information is viewable:

Name	Description
Assigned roles	• For a user, this pane shows the roles they inhabit, and how they got those roles, that is whether the user itself has the role, or whether it belongs to a group that has the role. • For a group, this pane shows the roles every user in the group inhabit, and how they got those roles, that is whether the group itself has the role, or whether it belongs to another group that has the role.
Assigned groups	For a user/group, this pane shows the groups they belong to, if any.
Assigned WiFi networks	For a user/group, this pane shows which user-specific WiFi networks they have been assigned, if any. If the user-specific WiFi networks are not included in the default network profile on VideoManager (because **User-specific networks** has been set to **Off**), a warning appears alerting the administrator to this fact. This is relevant because cameras assigned via single issue (with RFID) and permanent allocation automatically use the default network profile. If user-specific WiFi networks are not enabled for the default network profile, these cameras cannot use them to live stream media.
Device profiles	This pane shows the user/group's device profiles. The user/group could have these device profiles because:

Name	Description
	• The user/group has a role with which the device profiles are associated. • The user/group is assigned to a group that has the role with which the device profiles are associated. **NOTE:** Default device profiles are marked with ★. The default device profiles are automatically presented when the user is assigning a camera.
Permissions	For a user/group, this pane on the right-hand side shows their sum total of permissions. The user/group could have these permissions because: • The user/group has a role, which contains the permissions. • The user/group is assigned to a group that has the role, which contains the permissions. Users within this group have these permissions in addition to the permissions they would have from the roles they inhabit.

6. To return to the **Users** or **Groups** section, click **Back**.

9.1.9
Performing Roles Actions

A role is a collection of permissions within VideoManager, which can then be assigned to users. 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.

VideoManager provides the following default roles:

- **System Administrator** – Users assigned to this role can access all aspects of the VideoManager UI, such as deleting incidents, creating other users, and more.
- **Device Operator** – Users assigned to this role can record media files. They cannot perform any other actions on VideoManager, and cannot log on.
- **System User** – Users assigned to this role can view their own media files, and media files shared with them. They cannot operate cameras, or access the **Admin** tab.
- **System Supervisor** – Users assigned to this role can view their own media files and those recorded by users they are supervising. They cannot operate cameras, or access the **Admin** tab.
- **System Manager** – Users assigned to this role can view all media files on VideoManager, assign cameras, and perform actions on incidents.

Users may find it necessary to create their own roles, tailored to their workflow. Every default role except **System Administrator** can be edited manually.

Creating Roles

Procedure:

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 the role.
6. In the **Description** field, enter a description for the role.
7. Optional: From the **Default device profiles** drop-down list, select which previously created device profiles should apply to cameras that have been assigned to users in this role.

   Cameras assigned with RFID use this device profile automatically. If 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 camera family (VB400, VB100/VB200/VB300, and VT-series cameras). If they do not do so, the default device profile is used.

   If a user belongs to multiple roles, but all of the device profiles for roles are set to the system default except one, the one that is not the system default is used.

   If a user belongs to multiple roles, but some of the device profiles for roles are not set to the system default, the device profile that is highest in the device profile list, apart from the default profile, is used.

   NOTE: This list can be reordered from the **Device Settings** section of the **Devices** pane, in the **Admin** tab. From here, you can also change the system default device profile.
8. Set additional options for the new role using any of the following toggles.
   - If **Add new users to this role?** is set to **On**, any new users created on VideoManager from now on 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 Configuring Password Complexity on page 215.
   - From the **Role assignment tier** drop-down list, select which tier this role should belong to.
     By default, roles belong to tier 1. Users can only add other users to roles that are in the same tier or lower as their own roles.

     For example, if user A's role is in tier 2, 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.

     NOTE: Even users with the **Assign higher privileges** permission are not able to add other users to roles that 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 on to VideoManager.
     For more information, see Enabling Two Factor Authentication on page 154.
   - **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 Configuring Privilege Escalation on page 307.

9. Configure permissions for the role.

   This action determines what actions users in this role can perform. For more information, see Enable and Disable Permissions on page 152.

10. To save the role, click **Create role**.

Copying Roles

Copying a role duplicates the entire role except its name and is useful if you want to create many similar roles on your instance of VideoManager.

Procedure:

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 is copied and opened for editing, with the **Name** field left blank.

   NOTE: It is not possible to create two roles with the same name.

5. To save the changes, click **Create role**.

Editing Roles

It can be necessary to edit a role if the responsibilities of a user have changed.

Procedure:

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**.

   You can edit the properties, such as **Name**, **Description**, and **Default device profiles**, and permissions of a role.

5. Click **Save role**.

Deleting Roles

It can be necessary to delete a role if it has become obsolete.

Procedure:

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 opens to alert if there are users associated with the role.

5. Click **Yes**.

   NOTE: If users are associated with the role you want to delete, their ability to use VideoManager may be compromised once the role has been deleted. If the deleted role was the user's only role, they are unable to access VideoManager until they have been assigned a new role.

9.1.9.1

Enable and Disable Permissions

A permission is an individual rule, which determines the actions users can perform on VideoManager.

For a comprehensive list of all permissions, see Permissions on page 324.

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 that has it set to **Off**, that user will still be able to log on. There are no permissions that deny an action. Only the absence of permissions denies actions.

The groups of permissions are as follows:

- System permissions control users' abilities to log on to VideoManager, as well as their audit and export abilities.
- Media file permissions control users' abilities regarding media files. The permissions are sorted by the following criteria:
  - **Owned** – If enabled, users can perform actions on the media files recorded or imported by them.
  - **Shared** – If enabled, users can perform actions on the media files that have been shared with them by other users on the system.
  - **Supervised** – If enabled, users can perform actions on the media files that have been recorded or imported by other users on the system that they supervise.
  - **Any** – If enabled, users can perform actions on any media files on the system, regardless of who recorded them.
- Incident permissions control users' abilities regarding incidents. The permissions are 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 control users' abilities regarding cameras. The permissions are sorted by the following criteria:
  - **User** – If enabled, users can perform actions on the cameras assigned to them.
  - **Supervised** If enabled, users can perform actions on the cameras that are assigned to them or other users on the system that they supervise.
  - **Any** – If enabled, users can perform actions on any camera on the system.
- User permissions control users' abilities regarding other users. The permissions are 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 control how notifications work (if they have been licenced).
- Report permissions control users' abilities to create reports and view statistics.
- Field permissions dictate the access groups to which users belong, which affects which saved searches and user-defined incident fields they can see.
- Advanced permissions control users' abilities regarding advanced aspects of VideoManager. The permissions are 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.

9.1.10
Configuring Authentication Settings

By default, users must log on to VideoManager with a username and password. However, administrators can also configure the system so that users can log on with their Windows credentials, or other single sign-on credentials, for example, Azure. This action can be done from the **Authentication** section of the **People** pane, in the **Admin** tab.

Due to the complex nature of authentication configuration, the relevant information is contained in various technical papers.

Procedure:

- For more information about setting up Windows Active Directory authentication with a cloud instance of VideoManager, navigate to the Motorola Solutions Learning Experience Portal (registration is free) and search for *VideoManager (Cloud) and Win-dows Active Directory Explained*.
- For more information about setting up Windows Active Directory authentication with an on-premises instance of VideoManager, navigate to the Motorola Solutions Learning Experience Portal (registration is free) and search for *VideoManager (On-Premises) and Windows Active Directory Explained*.
- For more information about setting up Azure authentication with VideoManager, navigate to the Motorola Solutions Learning Experience Portal (registration is free) and search for *VideoManager and Azure Explained*.
- For more information about setting up any other OpenID OAuth2 with VideoManager, navigate to the Motorola Solutions Learning Experience Portal (registration is free) and search for *VideoManager and OpenID OAuth2 Providers Explained*.

9.1.11
Creating Client Certificate Authentication Realm

Procedure:

1. Navigate to the **Admin** tab.
2. Select the **People** pane.
3. Click the **Authentication** section.
4. Click **New realm**.
5. From the **Authentication type** drop-down list, select **Client Certificate Authentication**.
6. In the **Identifier** field, add an identifier.

For example, `cert-auth`

7. In the **Label** field, add a label.

   For example, `Certificate Authentication`

8. Ensure that **Enables** is set to **Yes**.
9. Optional: To map the user name, set **Use passthrough login matcher** to **Yes** and fill in the required fields.
10. In the **Client Certificate Authentication** section, click **Upload new certificate**.
11. Click **Choose File**.

    It is usually a .crt or .pem file.

12. Select the certificate and click **Open**.
13. Enter the password.
14. Click **OK**.
15. Click **Save**.

    The server restarts.

9.1.12 Enabling Two Factor Authentication

By default, users log on 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, which prompts users to scan a QR code with their phones, and enter the corresponding code into VideoManager.

Two factor authentication must be enabled on VideoManager before individual users can utilise it.

Procedure:

1. Navigate to the **Admin** tab.
2. Select the **People** pane.
3. Click the **Two Factor Authentication** section.
4. From the **Authentication settings** drop-down list, select how two factor authentication should behave 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.
     For more information, see Configuring Two Factor Authentication for Roles on page 155.
   - **Disabled** – Two factor authentication is disabled for this entire instance of VideoManager.

5. Click **Save settings**.

   Every user that is affected by the two factor authentication settings is prompted to associate their phone with VideoManager the next time they log on. For more information, see Setting Up Two Factor Authentication on page 155.

9.1.12.1

Configuring Two Factor Authentication for Roles

If two factor authentication has been set to **Per role** from the **Login Settings** section, you must now manually enable two factor authentication for individual roles.

Procedure:

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** drop-down list, configure the two factor authentication settings that should 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 on, and every login after that requires a 6-digit code to be entered as provided to the user via an app.
   - **Optional** – The user is not required to go through two factor authentication when initially logging on. However, they can enable it from their **Account Profile** page once they are logged on to VideoManager.
   - **Disabled** – Two factor authentication is not requested upon first login, and users cannot enable it from their **Account Profile** page.

   NOTE: 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 needs to utilise two factor authentication.
6. Click **Save role**.

9.1.12.2

Setting Up Two Factor Authentication

After 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 that has had **TOTP two-factor authentication** set to **Mandatory**, or if **Authentication** settings have been set to **Mandatory** for the entirety of VideoManager.

Procedure:

1. Download an authenticator app onto a phone.

   Motorola Solutions recommends **Google Authenticator**.
2. Log on to VideoManager as normal.

   You are asked to set up two factor authentication.
3. Click **Set up**.

   A QR code appears on the screen.
4. Using the authenticator app, either scan the QR code or manually type in the key.

   The authenticator app provides a 6-digit code.

5. In the field on VideoManager, enter the code provided by the authenticator app.
6. Click **Complete Set Up**.

   From now on, whenever you log on, you are asked to provide another 6-digit code from the authenticator app on your phone. You do not need to re-scan a QR code.

   If you get a new phone, you must repeat the process of associating it with VideoManager. You can do it by navigating to the **Account Profile** tab and clicking **Generate new authentication** in the **Two Factor Authentication** pane. You must scan the new QR code with the phone to be associated with VideoManager.

9.1.12.3
Resetting a Two Factor Authentication Key

If, for example, a user lost their phone and cannot use two factor authentication to log on to VideoManager, an administrator must reset their two factor authentication key for them.

Procedure:

1. Ensure that you are in a role where the **Clear Two Factor Authentication** permission has been set to **On**.

   For more information, see Enable and Disable Permissions on page 152.
2. Navigate to the **Admin** tab.
3. Select the **People** pane.
4. Click the **Users** section.
5. Next to the relevant user, click **Go to user**.
6. Click **Clear Two Factor Authentication key**.
7. Click **Save user**.

   Next time the user logs on, they are prompted to scan a new QR code.

9.1.13
Enabling and Configuring Login by Email

By default, users log on 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 after they have completed both of these actions.

Email logins must be enabled on VideoManager before individual users can utilise their email to log on.

Procedure:

1. Ensure that email settings have been enabled and configured from the **Email Properties** section of the **Connectivity** pane, in the **Admin** tab.

   For more information, see Configuring Email Properties on page 187.
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** drop-down list, select which users should 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, you must ensure that all users on VideoManager are associated with an email address, or they will be unable to log on.
- **Per role** – Login by email is determined on a role-by-role basis.
  If this setting is selected, you must enable email login for individual roles.
- **Disabled** – Login by email is disabled for this entire instance of VideoManager.

6. In the **Email subject template** and **Email content template** fields, configure the format of the email that users will receive when they try to log on.

   Possible variables are as follows:

   - *<siteName>* corresponds to Motorola Solutions VideoManager
   - *<siteUrl>* is the name of VideoManager. For example, `194.168.76.230`
   - *<siteHost>* is the public address of VideoManager. For example, `http://194.168.76.230:9080/`
   - *<loginUrl>* is the link which users must click to log on

     NOTE: If *<loginUrl>* is not included in the email, users will not be able to log on.

   - *<expirationTime>* 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, configure how long a login link is valid for.
8. Click **Save settings**.
9. Perform one of the following actions:

If...	Then...
If you have selected the **Mandatory** option from the drop-down list in step 5,	go to step 10.
If you have selected the **Per role** option from the drop-down list in step 5,	configure email login for individual roles by performing the following actions: a. Navigate to the **Admin** tab. b. Select the **People** pane. c. Click the **Roles** section. d. Next to the role to be edited, click **Go to role**. e. Set **Send a link by email to complete login** to **Yes**. f. Click **Save role**. g. Repeat for as many roles as necessary.

10. Add an email address to a user's profile by performing the following actions:
    a. Navigate to the **Admin** tab.
    b. Select the **People** pane.

c. Click the **Users** section.

d. Locate the user to be edited by filtering users in one of the following ways:

- In the **Name** field, enter the user's username or display name.
- In the **Authentication ID** field, enter the user's authentication ID.
- In the **In group** field, enter the group name of the user's group.
  If you enter a group name in the **In group** field, you have the option to change if **Only immediate members** is set to **On** or not. If set to **On**, only users that are assigned directly to the specified group are 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.
- In the **Email** field, enter the user's email.
- From the **Role** drop-down list, select the user's relevant role.

You can click ✕ to reset the filter.

You must ensure that all users that 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.

11. Click **Find**.
12. Next to the user to be edited, click > **Go to user**.
13. In the **Email notifications** field, enter the email address to which login links for the user should be sent.
14. Click **Save user**.

    From now on, whenever users try to log on to VideoManager, a link is sent to their email inbox. The users must click this link **in the same browser** that has VideoManager open. The link only works once. To request a new code, users must re-enter their password on VideoManager and try to log on again.

9.1.13.1 Disabling Login by Email

Procedure:

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** drop-down list, select **Disabled**.
5. Click **Save settings**.

   From now on, users only need to enter their password to log on.

9.1.14 Configuring User Self Service

It is possible to administer users manually from the **Users** section, which 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. Both password resetting and self-service registration are conducted through links sent via email. Administrators can configure for how many minutes these links are valid.

Procedure:

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 should expire and must be re-sent.
5. Click **Save settings**.

9.1.14.1

Enabling Users to Reset Their Own Passwords

All users on VideoManager must have a password to log on. If they forget their password, administrators can reset it for them. However, if configured, users can also reset their own passwords via email.

Prerequisites:

Users can 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, that is, 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 associate an email address with the user's account, perform the following actions:

  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**.

Procedure:

1. Ensure that emails are enabled.

   For more information, see Configuring Email Properties on page 187.
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 on the login pane and in the password reset email:
   a. In the **Password reset label** field, enter the text that users will see if they enter their password incorrectly.

      For example, `Forgotten password?`

b. In the **Link label** field, enter the text that users must click in order to send a password reset email.

   The text will be displayed on the login page alongside the **Password reset label** field.

   For example, `Reset here.` or `Click here.`

c. In the **Subject** field, enter the text to be set as the subject line for the password reset email.

d. In the **Content** field, enter the content of the password reset email.

   `${loginUrl}` and `${completionUrl}` can be utilised to direct users to the login pane and password reset pane, respectively.

7. Click **Save settings**.

9.1.14.2
Enabling Users to Complete Self-Registration

Every worker who is required to utilise VideoManager must have a unique user profile. Usually, administrators must create these users for them. However, if configured, workers can create their own users.

Prerequisites:

1. Ensure that emails are enabled.
   For more information, see Configuring Email Properties on page 187.
2. Ensure that at least one group to which new users can be added exists.
   For more information, see Creating, Editing, and Deleting Groups on page 144.

Procedure:

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, configure which email address patterns will be accepted by VideoManager when user creation is requested. To add an address pattern, perform the following actions:

   NOTE: Requests from email addresses with patterns not listed here will be ignored.

   a. Click **Add email pattern**.

   b. In the **Email pattern** field, enter an email address format.

   c. In the **Group assignment** field, enter a previously existing group to which all users with this specific email address format should be added.

   d. Click **Create**.

6. In the **Registration terms** section, configure what non-registered workers will see from the login pane:

   a. In the **Registration label** field, enter the text that will appear.

      For example, `Unregistered?` or `Don't have an account?`

   b. In the **Link label** field, enter the text for the link that workers must click in order to send a registration email.

      For example, `Register here.` or `Click here.`

   c. In the **Registration terms** field, enter the text to which non-registered workers must agree before they can create their new user profile.

d. Optional: Customize the text using any of the following settings:

TIP: Clicking the buttons again undoes the changes.

Name	Description
B Bold	Any text within the asterisks appears bold.
I Italic	Any text within the underscores appears italicised.
H Heading	Any text on the same line as ### appears as heading text.
URL/Link	You are prompted to enter a hyperlink. A link description can be entered in the square brackets.
Image	You can enter a URL for an image. An image description can be entered in the brackets.
Unordered List	Any text after the hyphen appears as part of a bullet point list. **Unordered List** must be clicked for each individual list entry.
Ordered List	Any text after the hyphen appears as part of a numbered list. **Ordered List** must be clicked for each individual list entry. The numbers appear in order once the message is previewed.
* Code	Any text within the single quotation marks appears as code.
Quote	Any text on the same line as > appears as a quote.

By clicking **Preview**, a previewable version becomes visible. You can edit the text by clicking **Preview** again.

7. In the **Welcome email** section, configure what workers will see when they open a welcome email from VideoManager:
   a. In the **Subject** field, enter the text to be set as the subject line for the welcome email.
   b. In the **Content** field, enter the content of the welcome email.

      <loginUrl> and *<completionUrl>* can be utilised to direct users to the 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:
   a. In the **Subject** field, enter the text to be set as the subject line for the email.
   b. In the **Content** field, enter the content of the email.

      <loginUrl> can be utilised to direct users to the login pane.

      <siteHost> can be utilised to insert the name of the specific VideoManager instance.

9. Click **Save settings**.

9.1.15
Built-In User Import Tool Configuration

You can import multiple users/groups simultaneously from another instance of VideoManager, which can be done from the **User Import Settings** section of the **People** pane, in the **Admin** tab.

For more information, see the document *Built-in User Import Tool Guide [ED-012-229]*, which can be found in the installation location of VideoManager, in the `userimporttool` folder.

Alternatively, you can manually export and import your entire user and group database via the **Users** section. For more information, see Exporting and Importing Users and Groups on page 142.

9.2
Devices

In the **Devices** pane, you can edit aspects of VideoManager related to camera configuration.

From the **Devices** pane, you can access the following sections:

- In the **Device Profiles** section, you can import, edit, and delete device profiles. The profiles control the way that individual cameras behave when assigned, depending on what type of a camera they are.
  For more information, see Performing Device Profiles Actions on page 163.
- In the **Device Settings** section, you can edit global camera settings. Unlike device profiles, settings configured here apply to all cameras connected to VideoManager, regardless of their type.
  For more information, see Configuring Device Settings on page 165.
- In the **Video metadata overlay settings** section, you can edit metadata display settings for all media on VideoManager, which affects which metadata is recorded alongside media files and subsequently displayed when users watch media that has been recorded on a camera.
  For more information, see Configuring Video Metadata Overlay Settings on page 167.
- In the **Access Control Key Management** section, you can import, edit, and delete access control keys. Access control keys determine which cameras can connect to VideoManager. By exporting and importing access control keys, users can access any media that was still on a camera when it was moved to a different instance of VideoManager.
  For more information, see Creating, Importing, and Deleting Access Control Keys on page 169.
- In the **Device Certificate Authorities** section, you can create, import, export, and delete certificate authorities. Certificate authorities validate media files from VB400s and ensure they have not been tampered with.
  For more information, see Performing Device Certificate Authorities Actions on page 170.
- In the **Device security** section, only users who know the in-vehicle administrator password can change administrative settings on their M500.
  For more information, see Setting an In-Vehicle Administrator Password on page 173.

9.2.1

Performing Device Profiles Actions

Device profiles are used to control the interface between cameras and VideoManager, as well as the recording behaviour and settings.

Searching for Device Profiles

Procedure:

1. Navigate to the **Admin** tab.
2. Select the **Devices** pane.
3. Click the **Device Profiles** section.
4. From the **Filter by** drop-down list, select one of the following options:
   - To show device profiles that are applicable to VB400s, select **VB400**.
   - To show device profiles that are applicable to VB100s/VB200s/VB300s, select **VB200/300**.
   - To show device profiles that are applicable to VT-series cameras, select **VT50/100**.

   NOTE: Camera families that are not present on your instance of VideoManager will still be presented as an option in the drop-down list.

Creating Device Profiles

Procedure:

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** drop-down list, select to which device family the device profile should apply.

   The options are as follows:
   - **VB400**
   - **VB200/300**
   - **VT50/100**

   NOTE: These details cannot be changed later.
7. Configure the device profile settings.

   For more information, see Device Profiles on page 344.
8. To save the device profile, click **Save settings**.

Postrequisites: After a device profile has been created, it can be applied to cameras. The options are as follows:

- If an operator is obtaining their camera through **Single Issue** or **Permanent Issue**, they can manually select the device profile when they assign their camera.

For more information, see Devices Assignment and Media Recording on page 100.

- If an operator is obtaining their camera through **Permanent Allocation**, VideoManager automatically selects the default device profile of the system, unless the operator is in a role that has a different device profile associated with it.
  For more information, see Performing Roles Actions on page 149.

Editing Device Profiles

Procedure:

1. Navigate to the **Admin** tab.
2. Select the **Devices** pane.
3. Click the **Device Profiles** section.
4. From the **Family** drop-down list, select a camera type.
5. Next to the profile to be edited, click **Go to profile**.
6. Make the relevant changes and click **Save settings**.

Reordering Device Profiles

Reordering device profiles can be necessary if users belong to multiple roles with different assigned device profiles. The device profile that is highest in the list is the one given to the camera. Furthermore, the device profile that is highest overall in the list is the system default.

Procedure:

1. Navigate to the **Admin** tab.
2. Select the **Devices** pane.
3. Click the **Device Profiles** section.
4. From the **Family** drop-down list, select a camera type.
5. Click **Reorder profiles**.
6. Make the necessary changes and click **Confirm new order**.

Deleting Device Profiles

Procedure:

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 that had this device profile as their default immediately switch back to the VideoManager-wide default.

Importing or Exporting Device Profiles

You can import/export all device profiles on VideoManager from the **Import/Export System Config** section of the **System** pane, in the **Admin** tab. For more information, see Exporting and Importing the Configuration of VideoManager on page 288.

9.2.2

Configuring Device Settings

You can configure settings which apply to all cameras on VideoManager, regardless of their type. Unlike device profiles, these settings do not need to be applied to cameras individually. They are automatically applied when a camera is connected to VideoManager.

Procedure:

1. Navigate to the **Admin** tab.
2. Select the **Devices** pane.
3. Click the **Device Settings** section.
4. Optional: In the **Touch assign** section, perform one of the following actions:
   - If only cameras with a full battery should be eligible for touch assign, set **Full battery required** to **On**.
   - If you set **Full battery required** to **Off**, enter a minimum charge time, before which the camera cannot be assigned by RFID.
     Cameras that have been permanently allocated to a user are the exception. In this case, the cameras can be tapped out by an RFID card even when they have not met the minimum charge time.
5. Optional: In the **Device discovery** section, perform one of the following actions:
   - If VideoManager should discover all cameras that are connected via USB, configured docks, or unconfigured docks, set **Enable device discovery** to **On**.
   - If VideoManager should only discover cameras that are connected to docks, set **Enable device discovery** to **Off**.
     Any cameras connected by USB do not appear on the **Devices** tab.
6. Optional: In the **Device setup** section, perform any of the following actions:
   - From the **Default device assignment mode** drop-down list, select which camera assignment mode should be the default.
     This action saves time when cameras are being assigned and one assignment mode is used consistently in an organisation. The options are as follows:
     - **Single issue** – The camera is assigned to a user and when it is redocked, it becomes unassigned and must be reassigned manually.
     - **Permanent issue** – The camera is assigned to the user and when it is redocked, it stays assigned to the same user.
     - **Permanent allocation** – The camera is allocated to a user, who must tap an RFID card before they can use it in the field. When the camera is redocked, it stays allocated to the same user.

       NOTE: In the **Device Field Trip**, **Operator Recorder Summary**, and **User Summary** reports, cameras in this mode are marked as `Unassigned` if they have been allocated but not tapped out with an RFID card.
   - Set **Show public QR code bootstrap screen** to either **On** or **Off**.

If set to **On**, users have the option to launch a public version of the QR config page when configuring a VT-series camera, which is useful if remote workers do not have access to VideoManager, but still need to assign their cameras. An administrator can send them the link to the public page, and the remote worker can use it to assign their 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 Connecting VT-Series Cameras to VideoManager Remotely on page 97.

- Set **Configure External Application account credentials** to **On**.

  NOTE: 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, set the range of MAC addresses with which cameras can pair.

  For more information about setting up radio integration with VB400s, you can navigate to the Motorola Solutions Learning Experience Portal (registration is free) and search for *VideoManager and Tetra Radio Integration Explained* or *VB400 and MOTOTRBO Radio Integration Explained*.

7. Optional: In the **Device offloads** section, perform any of the following actions:

   - To set the limit for the offload speed of simultaneous offloads performed by cameras, in the **Limit simultaneous offloads to** field, enter the desired number of megabits per second.

     This value is an approximation used to limit the number of offloads performed at once, and does not do any rate limiting.

     Increasing this value beyond the total available bandwidth of connected docks does not increase the offload throughput.

   - When a media download is interrupted and connection is then re-established, to resume downloading from the same point before connection was broken, set **Fast download recovery** to **On**.

     If set to **Off**, when a media download is interrupted and connection is then re-established, the download starts from the beginning.

   - If you want cameras to offload their oldest media to VideoManager first, set **Offload oldest media file first** to **On**.

     NOTE: The system default offloads most recent media first. This action is necessary if media are to be transferred to an Avigilon Control Center system.

8. Optional: In the **Device properties** section, perform any of the following actions:

   - Set **Battery life extender** to **On**.

     NOTE: 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 you want VB400s that are charging but cannot connect to VideoManager to restart periodically, set **Expect connectivity on charger** to **On**.

     This action improves the reliablility of USB connection to VideoManager, but should be set to **Off** if users are charging their VB400s in the field without connecting to VideoManager. For example, if users charge their cameras by connecting them via USB to a PC that does not have VideoManager installed.

9. Optional: In the **Shift-long field trips** section, set **Enable shift-long field trips** to **On**.

   If set to **On**, a camera assigned to a user has an affinity with that user once it is redocked in the middle of a shift.

   This means that if an operator redocks their camera mid-shift and then undocks it later in the shift, VideoManager automatically assigns the same camera to them, unless one of the following conditions is met:

- The camera is fully charged.
- The camera is manually unassigned on VideoManager.
- The shift ends, as determined by the number of hours entered into the **Maximum shift length** field.

NOTE: This function does not apply to cameras that have been assigned with permanent issue or permanent allocation because VideoManager associates the user to the camera permanently anyway.

10. Optional: In the **Footage signing** section, set **Enable footage signing** to **On**.

    You can enable footage signing if you have also created or imported a certificate authority from the **Device Certificate Authorities** section.

    If **Footage signing** is set to **On**, each VB400 is provided with a certificate that they will use to sign media files. When the media files are downloaded, VideoManager checks if the signatures of media files match the certificates of the cameras, and if the certificates can be trusted.

    NOTE: This action only works if a certificate authority has been created or imported into VideoManager. If you have not created or imported a certificate authority, this action does nothing.

    For more information, see Performing Device Certificate Authorities Actions on page 170.

11. Click **Save settings**.

9.2.3
Configuring Video Metadata Overlay Settings

VideoManager enables you to add metadata to recorded media. This metadata is stored in the media file and can be displayed in an overlay during playback and export. These settings apply to all media files recorded by cameras whose device profiles have been configured to include metadata.

Procedure:

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 media file overlay, scroll down to the bottom of the pane, and from the **Add element** drop-down list, select an element.

   NOTE: The order in which you choose the metadata elements determines the order in which the elements appear when a media file is played (left to right).

   The element options are as follows:

Name	Description
Device serial number	The serial number of the camera on which the media was recorded.
Operator name	The name of the operator who recorded the media. You can configure how many characters of the name should be visible over the media file, and how many spaces should be added to "pad" the name out to a minimum size.
Date and time	For media recorded on a VT-series camera or VB400, you can configure the following:

Name	Description

	• **Timezone**
	  ○ **UTC** – Greenwich Mean Time, but without adjustments for day-light savings time
	  ○ **Local Time** – taken from the server of VideoManager
	• **Time & date format** sets the format for date and time metadata. The options are as follows:
	  ○ **ISO Standard 8601** – If selected, the time and date is presented in an internationally standardised manner.
	  ○ **Custom** – If selected, more options are presented, as detailed below:
	  ■ **Time display** – **24-Hour Display** (for example, 19:00) or **12-Hour Display With AM/PM Markers** (for example, 12AM)
	  ■ **Timezone display** – **None**, **Show Timezone Offset In Hours:Minutes** (for example, +01:00), or **Show Timezone Name** (for example, 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** (for example, '19'), or **YYYY** (for example, '2019')

Frame counter	For media recorded on a VB400, VB300, VB200, or VB100, this option shows the user which frame is currently being shown in the playback viewer.
Recording time	For media recorded on a VB400, VB300, VB200, or VB100, this option shows the length of the recording. You can configure whether the recording time should start from when the operator pressed the record, or when the first frame was actually recorded. If you select the former option, any pre-recorded media appears as negative time in the metadata overlay, for example, -00:23:45.
Pre/Post-record marker	For media recorded on a VB400, VB300, VB200, or VB100, this option indicates which part of the media file has been pre-recorded or post-recorded, if any.
Text	You can enter text to give more information about the camera, operator, and more.

Name	Description
	Unlike other elements, you can add as many **Text** elements as necessary.
GPS	For media recorded on a VB400 or V700, this option displays the latitude and longitude of the camera. You can enable the following settings: • If you set **Include speed** to **On**, the speed of the camera is displayed in meters per second. • If you set **Include track** to **On**, the track of the camera is displayed in degrees.
Device name	The name of the camera, as configured from the **Edit device properties** pane.
Battery level	The level of battery of the VB400 when it recorded the media.

5. Optional: To delete a metadata element, click **Delete element**.

   The deleted element returns to the drop-down list, and can be reselected for use again.

6. To save the changes, click **Save settings**.

   These changes affect all cameras whose device profile has **Show video metadata overlay** set to **On**. The changes do not apply retroactively to media files that have already been recorded. For more information, see Performing Device Profiles Actions on page 163.

9.2.4

Creating, Importing, and Deleting Access Control Keys

Access control keys are the mechanism that VideoManager uses to encrypt media files. The keys prevent cameras from communicating with unauthorised instances of VideoManager.

Creating Access Control Keys

Procedure:

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**.

   After an access control key has been created, you can make it the default, by which all new or factory reset cameras are authenticated, by clicking **Set as default key**.

   NOTE: It is recommended that all access control keys are exported upon creation to somewhere secure. In event of a system failure, the export ensures that users can still access media on their cameras that has not been downloaded already.

Importing Access Control Keys

If you want to move a camera to another instance of VideoManager, you must import the corresponding access control key into that instance of VideoManager. Otherwise, the camera appears as `Locked` and you cannot access any media on the camera that has not already been downloaded to VideoManager.

Procedure:

1. In the original VideoManager instance, next to the access control key, click **Export key**.

   The access control key is downloaded to your PC.

2. In the new instance of VideoManager, click **Import key** and select the previously downloaded key.

Deleting Access Control Keys

You can delete an access control key if the cameras associated with it are no longer connected to the same instance of VideoManager.

Procedure:

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**.

   NOTE: If an access control key is deleted while cameras associated with it are still in the field, those cameras appear as `Locked` when redocked and all media that was not already downloaded to VideoManager is permanently inaccessible, unless you have 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
Performing Device Certificate Authorities Actions

VideoManager can verify media that has been downloaded from cameras, to check whether the media has been tampered with and whether it comes from a trusted source such as a genuine Motorola Solutions

camera. In order for this feature to function, you must first create or import a certificate authority into VideoManager, which signs the certificates issued to cameras. You must then enable media signing.

NOTE: If there is an existing certificate authority on VideoManager, the newly created or imported certificate authority replaces it as the signing certificate authority, that is VideoManager uses the new certificate authority to issue certificates to new cameras from now on. However, cameras that already have certificates created from the old certificate authority continue to sign files using their old certificates, and previously downloaded files contain signatures that refer to the old certificate authority. For this reason, the old certificate authority is retained so that VideoManager can use it to validate the media files from these cameras. If cameras should be issued new certificates based on the new certificate authority, the administrator must factory reset them.

Procedure:

1. Perform one of the following actions:

Option	Actions
Creating new certificate authorities	a. Navigate to the **Admin** tab. b. Select the **Devices** pane. c. Click the **Device Certificate Authorities** section. d. Click **Create new Certificate Authority**. VideoManager automatically populates the **Common Name** field with the public address + `root CA`. You can change the name, if you want. e. Optional: In the **Organisation** field, enter the name of your organisation. For example, `Motorola Solutions` f. Optional: In the **Organisational unit** field, enter the name of the department that the certificate authority is for. For example, `Research and Development` g. Click **Create**.

Option	Actions
Importing existing certificate authorities	a. Navigate to the **Admin** tab. b. Select the **Devices** pane. c. Click the **Device Certificate Authorities** section. d. Click **Import Certificate Authority**. e. Click **Choose File**. **NOTE:** Any imported certificate must be a certificate authority and must be accompanied by a private key. 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. Usually, if you want to use your own certificate authority, you must create it yourself. f. Select the certificate and click **Open**. g. Click **OK**.

2. From the **Device Settings** of the **Devices** pane, in the **Admin** tab, enable file signing.

   The setting is located in the **Footage signing** section.

   For more information, see Configuring Device Settings on page 165.

   From now on, all upgraded VB400s that are docked are issued with signing certificates. All media files downloaded from these VB400s are accompanied by a digital signature: VideoManager will check if the downloaded media files match their signatures and that the certificate associated with the signature is trusted by VideoManager. You can check whether the media files match this certificate from the **Media** tab.

   For more information, see Viewing and Editing Media File Properties on page 44.

Exporting Certificate Authorities

If cameras are moved from one instance of VideoManager to another, you should export the certificate authorities of those cameras from the original instance and import it into the new instance. This action ensures that media files from those cameras can have their signatures checked against the original certificate. Only the public part of the certificate authority is exported, so there is no security risk from importing these certificates into a less trusted system.

Procedure:

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 to be exported, click **View Certificate Authority**.

5. Click **Export Certificate Authority**.

   The certificate authority is downloaded to your 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**.

Deleting Certificate Authorities

If media files from a particular source should no longer be trusted, you can delete the corresponding certificate authority from VideoManager.

Procedure:

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, it means that the certificate authority is still actively signing certificates. Only certificate authorities that are being used for verification can be deleted.

5. Select the check box and click **Delete**.

   From now on, media files that would have been signed by the deleted certificate authority are not trusted by the system when downloaded, and media files that were already downloaded and signed by the deleted certificate are no longer trusted. In both cases, the **Signature** field of those media files reads as `Untrusted Certificate`.

9.2.6
Setting an In-Vehicle Administrator Password

Only users who know the in-vehicle administrator password can change administrative settings on their M500.

Procedure:

1. Navigate to the **Admin** tab.
2. Select the **Devices** pane.
3. Click the **Device Security** section.
4. In the **In-vehicle admin password** field, enter the password and make a note of it somewhere secure.
5. Click **Save settings**.

9.3
Connectivity

In the **Connectivity** pane, you can edit aspects of VideoManager related to WiFi and sites.

From the **Connectivity** pane, you can access the following sections:

- In the ONStream section, you can configure ONStream settings.
  For more information, see Configuring ONStream on page 175.
- In the **Network Profiles** section, you can create, edit, and delete network profiles, which is necessary if users want to send live streams from their cameras to VideoManager.
  For more information, see Performing Network Profile Actions on page 178.
- In the **Vehicle network profiles** section, you can create, edit, and delete vehicle network profiles, which is necessary if users want to send live streams from their M500 to VideoManager.
  For more information, see Performing Vehicle Network Profile Actions on page 181.
- In the **LTE APNs** section, you can create APNs.
  For more information, see Creating APNs on page 183.
- In the **Bandwidth Rules** section, you can configure bandwidth rules, which is necessary if you have sites uploading media, and you want to control when the media is uploaded.
  For more information, see Performing Bandwidth Rules Actions on page 184.
- If VideoManager has been configured as a Central VideoManager, **Metadata/Footage Replication** and **Configuration Replication** settings determine which aspects of its configuration, for example, users and roles, are automatically shared with its connected sites.
  For more information, see Configuring Sites on page 297.
- In the **Site Manager** section, you can configure sites. If VideoManager is not already acting as a Central VideoManager, this pane allows you to enable your instance of VideoManager to act as a site.

  NOTE: The **Site Manager** section is not available if VideoManager is acting as a Central VideoManager.

  For more information, see Configuring Sites on page 297.
- In the **Streaming Server** section, you can import and export a streaming server configuration. Network profiles can be configured so that devices live stream to a streaming server rather than streaming to this instance of VideoManager.
  For more information, see Importing and Exporting a Streaming Server Configuration on page 186.
- In the **Email Properties** section, you can:
  - Configure how emails are sent and received in VideoManager.
    For more information, see Configuring Email Properties on page 187.
  - Configure email notifications on VideoManager, including the email template and which actions prompt notifications to be sent to users.
    For more information, see Configuring Email Notifications on page 188.

9.3.1

Configuring ONStream

Before the system can be configured, ONStream must be configured and enabled from VideoManager.

Process:

1. Enable ONStream on VideoManager, with a licence.

   This step is only necessary if the user is running VideoManager version 14.2 or earlier.

   For more information, see Enabling ONStream on page 175.
2. Configure ONStream settings.

   These settings dictate how the system connects to VideoManager.

   For more information, see Configuring ONStream Settings on page 175.
3. Create outputs.

   These outputs determine how VideoManager users and cameras are mapped onto the system.

   For more information, see Creating and Resetting Outputs on page 177.

9.3.1.1

Enabling ONStream

From version 14.3 onwards, VideoManager enables ONStream by default as long as the user has at least one camera associated with VideoManager. For instances of VideoManager which are running version 14.2 or earlier, ONStream must be manually enabled by importing a licence into VideoManager.

Procedure:

1. Navigate to the **Admin** tab.
2. Select the **System** pane.
3. Click the **Licences** section.
4. Click **Import licence**.

   NOTE: You should select the ONStream licence provided to you by Motorola Solutions.
5. Click **Choose File**.
6. Select the certificate and click **Open**.
7. Enter the password.
8. Click **OK**.
9. Confirm again by clicking **Import**.

   If successful, the licence appears as `Valid` in the **Licences** section.

9.3.1.2

Configuring ONStream Settings

When enabled, ONStream presents an ONVIF-compatible interface with both Profile S (live streaming) and Profile G (recording retrieval) capability. ONStream presents live streams from cameras as channels in one

or more ONVIF compatible multi-channel encoders. The administrator must configure ONStream settings on VideoManager.

Procedure:

1. Navigate to the **Admin** tab.
2. Select the **Connectivity** pane.
3. Click the **ONStream** section.
4. Set **Enable ONStream** to **On**.
5. From the **Video codec** drop-down list, select the codec to be used to compress the live streams between devices and the system.

   The options are **MPEG4** or **H264**.
6. From the **Authentication mode** drop-down list, select whether users must enter additional credentials when connecting their instance of VideoManager to the system.
   - If no additional authentication is required, select **None**.
   - If users should be prompted to create a **Username** and **Password** on VideoManager, select **Basic**.

     These credentials must be entered in the system when it is being configured to connect to VideoManager.
7. From the **Multi device mode** drop-down list, select whether VideoManager presents as a single multi-channel encoder, or multiple encoders.
   - If the system will be used with 16 devices or fewer, select **Off**.
   - If the system will be used with more than 16 devices, select either **IP addresses** or **Domain names**.
8. In the **RTSP Port** field, configure the port that VideoManager should use to pass streams to the system.

   By default, the port is `554`.
   The administrator may need to change the default port if any software on the same machine as VideoManager is using port `554`.
9. Optional: Set **Allow historic footage fetch** to **On**.

   If set to **On**,the system has access to, and can copy, all media on VideoManager.
   This process does not start until the administrator has also configured the system to retrieve historic media.

   NOTE: Enabling **Allow historic footage fetch** permits the system to retrieve restricted media.
10. Click **Save settings**.

9.3.1.3

Creating and Resetting Outputs

Outputs determine how streams from individual users and cameras on VideoManager are mapped onto channels in an ONVIF compatible multi-channel encoder.

Creating Outputs

There must be one output for every user or camera that will be streaming to the system.

Procedure:

1. Navigate to the **Admin** tab.
2. Select the **Connectivity** pane.
3. Click the **ONStream** section.
4. Set **Enable ONStream** to **On**.
5. Scroll to the **Outputs** section.
6. Click **Create**.
   The **Create ONStream Outputs** window opens.
7. Enter the number of required outputs and click **Confirm**.
8. Select the type of output to be created.
   - If streams should correspond to the specified camera, regardless of the operator using the camera, select **Device** and enter the serial number of the camera.
     VideoManager will suggest serial numbers that match the one entered.
   - If streams should correspond to the specified operator, regardless of the camera used to stream media, select **Operator** and enter the username of an operator.
   - If streams should correspond to the specified number of panels, select **Tactical view panel** and enter the number.
9. Click **Save settings**.

Resetting Outputs

If the number of outputs should be raised or lowered after the outputs have been created, the outputs should be reset. Preexisting outputs will not be affected if the total number of outputs is raised. However, if the new number is lower than the previous number, a user's outputs will be deleted to match that number.

Procedure:

1. Navigate to the **Admin** tab.
2. Select the **Connectivity** pane.
3. Click the **ONStream** section.
4. Scroll to the **Outputs** section.
5. Click **Reset**.
6. Enter the new number of required outputs.
7. Click **Save settings**.

9.3.2

Performing Network Profile Actions

VideoManager uses network profiles to control the connectivity options available for a camera. A network profile is a collection of WiFi networks, which a camera can connect to when attempting to live stream media.

Creating Network Profiles

Procedure:

1. Navigate to the **Admin** tab.
2. Select the **Connectivity** pane.
3. Click the **Network Profiles** section.
4. Click **Create Network profile**.
5. In the **Name** field, enter a name for the network profile.
6. Optional: If you want the network profile to be the default, set **Default profile** to **On**.

   If set to **On**, cameras assigned with single issue via RFID and Permanent allocation will automatically use this network profile.
7. Optional: If you want a user's user-specific WiFi networks to be added to the network profile, set **User-specific networks** to **On**.

   User-specific WiFi networks are networks that only appear on a user's session of VideoManager. This action is useful if multiple users have their own individual mobile hotspots that should only be used by cameras assigned to them.

   For more information, see Creating User-Specific WiFi Networks on page 295.

   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 media 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 cameras first.
8. Add WiFi networks to the network profile by clicking **Add network**.

   Unlike user-specific WiFi networks, these WiFi networks can be used by all cameras that have this network profile assigned to them, regardless of their operator.
9. Configure any of the following settings:

   - In the **Network name (SSID)** field, enter the SSID of the WiFi network.
   - From the **Security type** drop-down list, select the security type of the WiFi network.
   - In the **Passphrase** field, enter the passphrase for the WiFi network.

   Usually, you can find these credentials on the bottom of the WiFi router.

   - From the **Band** drop-down list, select which frequencies the cameras should attempt to connect to.

     The options are as follows:

     - **Any** makes VB400s connect to both 2.4GHz and 5GHz frequencies.
     - **2.4GHz only** makes all cameras connect to 2.4GHz frequencies.
     - **5GHz only** makes VB400s connect to 5GHz frequencies.

- Set **Disconnect on low signal** to **On**.
  If set to **On**, cameras disconnect from the network if it has a low signal. The user can configure for how long the camera must be connected to the weak signal, after which the camera disconnects.
- If you want to enable cameras to connect to hidden networks, set **Hidden network** to **On**.

  NOTE: Hidden network should only be set to **On** if the networks within a network profile are hidden networks.

10. If VT-series cameras will be streaming, scroll down to the ★ **VT50/VT100** section and perform any of the following actions:
    - To enable users with appropriate permissions to live stream media over VideoManager from VT-series cameras in the field, set **Enable streaming** to **On**.
    - To enable users to assign and unassign VT-series cameras over WiFi, instead of having to manually dock the cameras first, set **Enable docking** to **On**.
11. If multiple networks should be contained within the network profile, repeat step 8 through step 10 until all the necessary networks have been added.

    NOTE: You can prioritise the networks by using **Move up** and **Move down**. Cameras will attempt to connect to the first network shown in the list, while the last network in the list will only be used if all the other networks are unavailable.
12. Optional: Set **Enable LTE** to **Yes**.

    NOTE: Assigning a network profile to a V500 that has both WiFi and LTE enabled will not send the WiFi configuration. The V500 can only use WiFi if it is assigned with a network profile that has LTE disabled.
13. Configure any of the following settings for VB-series or V500 cameras for the entire network profile:
    - If you want to enable cameras to be able to live stream media over the WiFi networks in this network profile, set **Enable streaming** to **On**.
    - If you want the media that has been recorded on the camera to be offloaded to VideoManager over the WiFi networks within this network profile, set **Offload video** to **On**.
      If you have configured device profiles so that VB400s or V500s can place bookmarks in a media file, then only bookmarked media files are downloaded over the WiFi networks.

      If you have not configured the device profiles, then all media files are downloaded over the WiFi networks when the camera is connected to power.

      For more information, see Performing Device Profiles Actions on page 163 and Device Profiles on page 344.
14. Click **Save profile**.

Postrequisites: After a network profile has been created, it can be applied to cameras. The options are as follows:

- If an operator is obtaining their camera through **Single Issue** or **Permanent Issue**, they can manually select the network profile when they assign their camera.
  For more information, see Devices Assignment and Media Recording on page 100.
- If an operator is obtaining their camera through **Permanent Allocation**, VideoManager automatically selects the default network profile of the system.

Editing Network Profiles

Procedure:

1. Navigate to the **Admin** tab.

2. Select the **Connectivity** pane.
3. Click the **Network Profiles** section.
4. Next to the profile to be edited, click **Go to profile**.
5. Make the relevant changes and click **Save profile**.

Deleting Network Profiles

Procedure:

1. Navigate to the **Admin** tab.
2. Select the **Connectivity** pane.
3. Click the **Network Profiles** section.
4. Next to the profile to be deleted, click **Delete profile**.

   NOTE: The default network profile **cannot** be deleted. You must first select another network profile to become the default instead. You can do so by clicking **Go to profile** next to the network profile, setting its **Default profile** to **On**, and clicking **Save profile**. The outdated network profile can now be deleted.

Duplicating Network Profiles

Duplicating network profiles can be useful if VideoManager should have multiple similar network profiles.

Procedure:

1. Navigate to the **Admin** tab.
2. Select the **Connectivity** pane.
3. Click the **Network Profiles** section.
4. Next to the profile to be duplicated, click **Duplicate Network profile**.

   The **Create Network profile** pane opens, with the original information of the network profile pre-set.
5. Optional: Edit the network profile like normal.

   By default, the **Name** of the network profile is set to *<name of the duplicated network profile>* `(copy)`.

   NOTE: Each network profile must have a unique name on VideoManager. You cannot save a network profile whose name is identical to an existing network profile.
6. Click **Save profile**.

Exporting Network Profiles

Exporting network profiles can be useful if sites should have the same network profiles as their Central VideoManager.

Procedure:

1. Navigate to the **Admin** tab.
2. Select the **Connectivity** pane.

3. Click the **Network Profiles** section.
4. Next to the profile to be exported, click **Export Network profile**.

   The network profile is exported to the default download location of your PC, and can be imported to other instances of VideoManager.

Importing Network Profiles

Importing network profiles can be useful if sites should have the same network profiles as their Central VideoManager.

Procedure:

1. Navigate to the **Admin** tab.
2. Select the **Connectivity** pane.
3. Click the **Network Profiles** section.
4. Next to the profile to be imported, click **Import Network profile**.
5. Select the relevant file from your PC.
6. Click **Import**.

   The network profile should appear on your instance of VideoManager.
   Alternatively, if you want to import/export all of your network profiles simultaneously, you can do so from the **Import/Export System Config** section of the **System** pane, in the **Admin** tab. For more information, see Exporting and Importing the Configuration of VideoManager on page 288.

9.3.3
Performing Vehicle Network Profile Actions

Creating Vehicle Network Profiles

You must create a vehicle network profile for your M500(s) to enable the M500 to connect to the router in the car, and by extension to VideoManager.

Procedure:

1. Navigate to the **Admin** tab.
2. Select the **Connectivity** pane.
3. Click the **Vehicle network profiles** section.
4. Click **Create vehicle network profile**.
5. In the **Name** field, enter a name for the network profile.
6. Optional: If you want the network profile to be the default, set **Default profile** to **On**.

   If set to **On**, devices assigned with single issue via RFID and Permanent allocation will automatically use this network profile.
7. From the **Wireless types** drop-down list, select the type of a router to which the M500 will connect in the car.

   If you are unsure, Motorola Solutions recommends choosing **Wired**.

8. If the network router should determine the IP, gateway, and subnet mask of the M500, set **DHCP client** to **On**.

   Alternatively, you can set **DHCP client** to **Off** if you wish to specify the network credentials of the M500 manually.

Editing Vehicle Network Profiles

Procedure:

1. Navigate to the **Admin** tab.
2. Select the **Connectivity** pane.
3. Click the **Vehicle network profiles** section.
4. Next to the profile to be edited, click **Go to profile**.
5. Make the relevant changes and click **Save profile**.

Deleting Vehicle Network Profiles

Procedure:

1. Navigate to the **Admin** tab.
2. Select the **Connectivity** pane.
3. Click the **Vehicle network profiles** section.
4. Next to the profile to be deleted, click **Delete profile**.

   NOTE: The default vehicle network profile **cannot** be deleted. You must first select another vehicle network profile to become the default instead. You can do so by clicking **Go to profile** next to the network profile, setting its **Default profile** to **On**, and clicking **Save profile**. The outdated vehicle network profile can now be deleted.

Duplicating Vehicle Network Profiles

Duplicating vehicle network profiles can be useful if VideoManager should have multiple similar vehicle network profiles.

Procedure:

1. Navigate to the **Admin** tab.
2. Select the **Connectivity** pane.
3. Click the **Vehicle network profiles** section.
4. Next to the profile to be duplicated, click **Duplicate vehicle network profile**.

   The **Create Vehicle network profile** pane opens, with the original information of the vehicle network profile pre-set.

5. Optional: Edit the vehicle network profile like normal.

By default, the **Name** of the vehicle network profile is set to *<name of the duplicated vehicle network profile>* (copy).

NOTE: Each vehicle network profile must have a unique name on VideoManager. You cannot save a vehicle network profile whose name is identical to an existing vehicle network profile.

6. Click **Save profile**.

Exporting Vehicle Network Profiles

Exporting vehicle network profiles can be useful if sites should have the same vehicle network profiles as their Central VideoManager.

Procedure:

1. Navigate to the **Admin** tab.
2. Select the **Connectivity** pane.
3. Click the **Vehicle network profiles** section.
4. Next to the profile to be exported, click **Export vehicle network profile**.

   The vehicle network profile is exported to the default download location of your PC, and can be imported to other instances of VideoManager.

Importing Vehicle Network Profiles

Importing vehicle network profiles can be useful if sites should have the same vehicle network profiles as their Central VideoManager.

Procedure:

1. Navigate to the **Admin** tab.
2. Select the **Connectivity** pane.
3. Click the **Vehicle network profiles** section.
4. Next to the profile to be imported, click **Import vehicle network profile**.
5. Select the relevant file from your PC.
6. Click **Import**.

   The vehicle network profile should appear on your instance of VideoManager.

   Alternatively, if you want to import/export all of your network profiles simultaneously, you can do so from the **Import/Export System Config** section of the **System** pane, in the **Admin** tab. For more information, see Exporting and Importing the Configuration of VideoManager on page 288.

9.3.4
Creating APNs

Procedure:

1. Navigate to the **Admin** tab.
2. Select the **Connectivity** pane.

3. Click the **LTE APNs** section.
4. Click **Create APN**.

   The **Create APN** window opens.
5. Fill in the following information:
   - **APN**
     This field is mandatory.
   - **Mobile country code**
   - **Mobile network code**
   - **User**
   - **Password**
6. Click **Save profile**.

9.3.5

Performing Bandwidth Rules Actions

You can configure bandwidth rules, which affect how much bandwidth is used when downloading data from both sites and docks.

Creating and Applying Bandwidth Rules

Procedure:

1. On the Central VideoManager (if creating a bandwidth rule for sites), or on VideoManager (if creating a bandwidth rule for docks), 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. Optional: If you want all docks that are added to this rule to be part of the same "group" and share the same bandwidth limit, set **Shared bandwidth group** to **On**.

   This action is useful if multiple docks are on the same network connection, and you want to stagger the downloads.
7. If you want all docks who are added to this rule to continuously download media to VideoManager, ignoring the overall download limit, set **Slow connection** to **On**.

   This action is useful if the docks have a slow network connection.
8. To create an individual rule, click **Add rule**.

   You can create multiple rules within one bandwidth rule, which is useful if there are certain "busy" times when media and other data should not be offloaded, and other "quiet" times when media and data should be offloaded.

   If there are multiple rules within one bandwidth rule, you should order them using the controls next to each rule. If there are two overlapping rules, for example, two rules apply on Saturday, the rule that is highest in the list takes priority.

You can delete an individual rule within a bandwidth rule by clicking **Delete bandwidth rule**.

9. Configure any of the following settings:
   - The day(s) of the week when the rule should occur.
   - In the **from** field, enter the time of day when the rule should begin.
   - In the **until** field, enter the time of day when the rule should finish.
   - In the **limit to** field, enter the number of kilobits per second to which uploads should be limited while the rule applies.
10. Click **Create bandwidth rule**.

    After a bandwidth rule is created, it must be manually applied in order to take effect.
11. Perform one of the following actions:

Option	Actions
Applying a bandwidth rule to a dock	a. Navigate to the **Devices** tab. b. Select the **docks** pane. c. Next to the relevant dock, click **View details**. You can filter docks by **Name**, **Serial**, and **Version**. d. In the **Bandwidth Rule** pane, click the drop-down menu, and select the relevant rule. e. Optional: If you want all media from the selected dock to be downloaded as quickly as possible, set **High Priority dock** to **On**. If the dock is part of a bandwidth rule that has the **Shared bandwidth group** setting enabled, it halts the downloads of other docks in the group until all of its media has been downloaded. f. Click **Save Bandwidth Rule**.
Applying a bandwidth rule to a site	The bandwidth rule can either be applied upon creation or the site can be edited afterward to include the rule. For more information, see Configuring Sites on page 297.

Copying Bandwidth Rules

Copying bandwidth rules enables to create multiple, similar bandwidth rules.

Procedure:

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 **Copy bandwidth rule**.

The name of the copied bandwidth rule is the name of the original bandwidth rule with _1 (if it is the first copy of the bandwidth rule) at the end.

NOTE: Unlike groups and users, it is possible to create two bandwidth rules with the same name, but it is not recommended.

5. Make any necessary changes to the copy of the bandwidth rule, and click **Save bandwidth rule**.

Editing Bandwidth Rules

Procedure:

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 automatically updates across all docks to which it has been applied.

Deleting Bandwidth Rules

Procedure:

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**.

   NOTE: If the deleted bandwidth rule was previously applied to a dock or site, the bandwidth setting for those docks and sites immediately changes to **No Restriction** until another bandwidth rule is manually reapplied.

9.3.6
Importing and Exporting a Streaming Server Configuration

Importing a Streaming Server Configuration

Procedure:

1. Navigate to the **Admin** tab.
2. Select the **Connectivity** pane.
3. Click the **Streaming Server** section.
4. Click **Import config for streaming to an external VideoManager**.
5. Select the relevant file from your PC.
6. Click **Import**.

Exporting a Streaming Server Configuration

Prerequisites: Configure a public web server address before generating a streaming server configuration.
For more information, see Configuring the Public Address of VideoManager on page 294.

Procedure:

1. Navigate to the **Admin** tab.
2. Select the **Connectivity** pane.
3. Click the **Streaming Server** section.
4. Click **Export new config for streaming to this VideoManager**.

   The streaming server configuration is exported to the default download location of your PC, and can be imported to other instances of VideoManager.

9.3.7

Configuring 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.

Prerequisites: Ensure that the *Notification* licence is enabled on VideoManager.
For more information, see Importing and Deleting Licences on page 286.

Procedure:

1. Navigate to the **Admin** tab.
2. Select the **Connectivity** pane.
3. Click the **Email Properties** section.
4. Set **Email notifications enabled** to **On**.
5. In the **Default properties** section, configure the following settings:
   a. In the **Sender email address** field, enter the email address from which all VideoManager emails should be sent.

      This includes email notifications, password reset emails, and user profile creation emails.
   b. In the **Host** field, enter the host from which emails should be sent.

      For Gmail, the host is `smtp.gmail.com`
   c. In the **Port** field, enter the port from which emails should be sent.

      For Gmail, the port is `587`
   d. If **Authentication** is set to **On**, enter the username and password belonging to the email address entered in the **Sender email address** field.

      NOTE: The password is not necessarily the same password that is utilised to log on to the email address's account.
6. **Gmail only:** Create an app password by performing the following actions:
   a. Open the account settings pane for the email address entered in the **Sender email address** field.
   b. Click the **Security** section.

c. Click **App passwords**.

d. From the **Select app** drop-down list, select **Other (Custom name)**.

e. Enter `VideoManager`

f. Click **Generate**.

g. Copy the password and paste it into the **Password** field.

If **STARTTLS enable** is set to **On**, all emails sent from VideoManager are protected with Transport Layer Security (TLS).

If **Trust server certificates** is set to **On**, VideoManager trusts the SMTP server.

If set to **Off**, VideoManager will check server certificates.

7. Optional: In the **Custom properties** section, add specific properties that dictate how VideoManager interacts with the SMTP server by performing the following actions:

a. Click **Add property**.

b. In the **Property** field, enter the name of the property.

This should be the name of a JavaMail SMTP property. For example, `mail.smtp.timeout` or `mail.smtp.reportsuccess`

c. In the **Value** field, enter the value of the property.

The format of the value (milliseconds, true/false, host name, and more) depends on the property name entered in the **Property** field.

8. Optional: In the **Custom templates** section, configure the notification email that is sent to users when specific actions are taken on VideoManager by performing any of the following actions:

- If you want to configure the email that users receive when another user on VideoManager logs on for the first time, set **First time login** to **On**.
- If you want to configure the email that users receive when a camera starts streaming, set **Device stream start** to **On**.

This could be the user's own camera, or a camera assigned to someone they supervise, depending on the way the user's permissions are configured.

9. Optional: In the **Test Properties** section, in the **Test recipient** field, enter the email address to which the test email should be sent, and click **Test**.

Postrequisites: You can also configure how password reset emails and user profile creation emails are sent. For more information, see Configuring User Self Service on page 158.

9.3.8 Configuring Email Notifications

After you have configured email settings on VideoManager, you can enable and configure email notifications. This action 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.

Procedure:

1. Optional: Configure the emails that users will receive when specific actions are taken on VideoManager by performing the following actions:

a. Navigate to the **Admin** tab.

b. Select the **Connectivity** pane.

c. Click the **Email Properties** section.

d. Scroll down to the **Custom templates** section.

The options are as follows:

- If **First time login** is set to **On**, you can configure the email that users receive when another user on VideoManager logs on 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**, you can configure the email that users receive when a camera starts streaming. This could be the user's own camera, or a 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**, you can configure the email that users receive when one of file spaces of VideoManager 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>.`

2. Configure which users should receive notifications on a role-by-role basis by performing the following actions:

a. Navigate to the **Admin** tab.

b. Select the **People** pane.

c. Click the **Roles** section.

d. Next to the role to be edited, click **Go to role**.

e. Enable the relevant permissions.

- **First time login** – Users receive a notification when other users first log on to VideoManager.
- **Personal device stream start** – Users receive a notification when a camera assigned to them starts streaming.
- **Supervised device stream start** – Users receive a notification when a camera assigned to users they supervise starts streaming.
- **File storage threshold warnings** – Users receive a notification when VideoManager is low on storage space.

f. Click **Save role**.

3. Ensure that all users in the notification-enabled roles have email addresses associated with them on VideoManager by performing the following actions:

a. Navigate to the **Admin** tab.

b. Select the **People** pane.

c. Click the **Users** section.

d. Locate the user to be edited by filtering users in one of the following ways:

- In the **Name** field, enter the user's username or display name, and click **Find**.
- In the **In group** field, enter the group name of the user's group, and click **Find**.
  If you enter a group name in the **In group** field, you have the option to change if **Only immediate members** is set to **On** or not. If set to **On**, only users that are assigned directly to the specified

group are 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.

- From the **Role** drop-down list, select the user's relevant role, and click **Find**.

You can click ✕ to reset the filter.

e. Next to the user to be edited, click > **Go to user**.

f. In the **Email notifications** field, enter an email address for the user.

g. Click **Save user**.

9.4

Policies

In the **Policies** pane, you can edit aspects of VideoManager relating to reoccurring rules and settings.

From the **Policies** pane, you can access the following sections:

- In the **Deletion Policy** section, you can configure when outdated media and incidents are automatically deleted.
  For more information, see Configuring Deletion Policies on page 193.
- In the **Incident Exports** section, you can configure incident export profiles. Incident export profiles determine how a user can export an already created incident from VideoManager that is DVD, MP4, or Evidence Export.
  For more information, see Configuring Incident Exports on page 197.
  You can also configure VideoManager for export confirmation.
  For more information, see Configuring VideoManager for Export Confirmation on page 211.
- In the **File Exports** section, you can configure whether recorded media should be sent straight from a camera to a predetermined location on a PC or server, in addition to being stored on VideoManager.
  For more information, see Configuring File Exports on page 214.
- In the **Auto Incident Creation** section, you can configure which user-defined media fields trigger automatic incident creation.
  For more information, see Enabling and Configuring Automatic Incident Creation on page 214.
- In the **Password Complexity** section, you can configure password complexity rules, to which all users on VideoManager must adhere.
  For more information, see Configuring Password Complexity on page 215.
- In the **Reports** section, you can configure when outdated reports are automatically deleted, and at what time of day scheduled reports are run.
  For more information, see Configuring Report Settings on page 216.
- In the **User-defined Incident Fields** section, you can perform the following actions:
  - Transfer copies of user-defined incident fields from one instance of VideoManager to another.
    For more information, see Exporting and Importing User-Defined Incident Fields on page 217.
  - Control the format of information entered into user-defined incident fields.
    For more information, see Creating and Applying Validators on page 218.
  - Reorder user-defined incident fields.
    For more information, see Reordering User-Defined Incident Fields on page 219.

- Create 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 Creating User-Defined Incident Fields on page 219.
- Edit default user-defined incident fields, which are built into VideoManager and can have various aspects of their configuration changed.
  For more information, see Editing Default User-Defined Incident Fields on page 230.
- Edit which incident clip properties can be viewed by different users, based on their permission groups.
  For more information, see Editing Incident Clip Field Visibility on page 232.
- Create an M500 event category incident field.
  For more information, see Creating an M500 Event Category Incident Field on page 233.
- Enable and configure automatic incident creation for M500.
  For more information, see Enabling and Configuring Automatic Incident Creation on page 234.
- Configure user-defined field layouts.
  For more information, see Configuring User-Defined Field Layouts on page 249.

- In the **User-defined Media Fields** section, you can perform the following actions:
  - Transfer copies of user-defined media fields from one instance of VideoManager to another.
    For more information, see Exporting and Importing User-Defined Media Fields on page 234.
  - Control the format of information entered into user-defined media fields.
    For more information, see Creating and Applying Validators on page 235.
  - Reorder user-defined media fields.
    For more information, see Reordering User-Defined Media Fields on page 236.
  - Create user-defined media fields. User-defined media fields enable users to categorise media files, using more complex fields than those which VideoManager provides by default.
    For more information, see Creating User-Defined Media Fields on page 236.
  - Edit default user-defined media fields, which are built into VideoManager and can have various aspects of their configuration changed.
    For more information, see Editing Default User-Defined Media Field Visibility on page 246.
  - Edit the M500 event category media field.
    For more information, see Editing the M500 Event Category Media Field on page 247.
  - Add M500 event tags to make other existing media fields compatible with the M500.
    For more information, see Adding Other M500 Event Tags on page 248.
  - Configure user-defined field layouts.
    For more information, see Configuring User-Defined Field Layouts on page 249.
- User-defined playback reason fields prompt users to enter a reason as to why they are watching an outdated media file. It is used in tandem with the playback policy configured in the **Playback Policy** section of the **Policies** pane, in the **Admin** tab. In the **User-defined Playback Reason Fields** section, you can perform the following actions:
  - Transfer copies of user-defined playback reason fields from one instance of VideoManager to another.
    For more information, see Exporting and Importing User-Defined Playback Reason Fields on page 249.
  - Control the format of information entered into user-defined playback reason fields.
    For more information, see Creating and Applying Validators on page 250.
  - Reorder user-defined playback reason fields.

For more information, see Reordering User-Defined Playback Reason Fields on page 251.

- Create user-defined playback reason fields. User-defined playback reason fields enable users to categorise media files, using more complex fields than those which VideoManager provides by default.
  For more information, see Creating User-Defined Playback Reason Fields on page 251.

- User-defined share reason fields prompt users to enter a reason as to why they are sharing an outdated media file. In the **User-defined Share Reason Fields** section, you can perform the following actions:
  - Transfer copies of user-defined share reason fields from one instance of VideoManager to another.
    For more information, see Exporting and Importing User-Defined Share Reason Fields on page 252.
  - Control the format of information entered into user-defined share reason fields.
    For more information, see Creating and Applying Validators on page 252.
  - Reorder user-defined share reason fields.
    For more information, see Reordering User-Defined Share Reason Fields on page 253.
  - Create user-defined share reason fields. User-defined share reason fields enable users to categorise media files, using more complex fields than those which VideoManager provides by default.
    For more information, see Creating User-Defined Share Reason Fields on page 253.

- In the **Import profiles** section, you can configure import profiles. These profiles dictate which user-defined media fields are automatically populated when a media file is imported into VideoManager.
  For more information, see Configuring Import Profiles on page 254.

  You can also test the export-import feedback mechanism.

  For more information, see Testing the Export-Import Feedback Mechanism on page 212.

- In the **Antivirus Policy** section, you can configure whether VideoManager scans imported media for viruses.
  For more information, see Enabling and Configuring the Antivirus Policy on page 255.

- In the **Incident Sharing** section, you can configure which email address should be the default, and which incident clip fields should be visible, when using incident links.
  For more information, see Configuring Incident Sharing on page 256.

- In the **Playback Policy** section, you can configure whether users must record their reason for watching a media file 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 Configuring the Playback Policy on page 257.

- In the **Playback Watermark** section, you can add and create watermarks to be displayed on media files when played back.
  For more information, see Configuring Playback Watermarks on page 257.

- In the **Mobile App Settings** section, you can configure Mobile App settings, if the Mobile App has been licenced from Motorola Solutions.
  For more information, see Configuring Mobile App Settings on page 258.

- In the **API Key Management** section, you can create API keys, which enable VideoManager to securely communicate with external software.
  For more information, see Creating, Viewing, and Deleting API Keys on page 259.

9.4.1

Configuring Deletion Policies

Deletion policies are used to control the way in which media files can be automatically deleted from the system to free storage space.

Procedure:

1. Navigate to the **Admin** tab.
2. Select the **Policies** pane.
3. Click the **Deletion Policy** section.
4. Configure any of the following categories.

Name	Description
Footage deletion policy	Controls the deletion policy regarding media on VideoManager. • If **Automatically delete old footage** is set to **On**, outdated media on VideoManager is automatically deleted. Enter the number of days for which recorded media should be kept before it is deleted. Enter the number of days for which downloaded media should be kept before it is deleted. **NOTE:** This differentiation is useful if media is not always downloaded on the same day as it is recorded, and users want more time to review media or add it to incidents. • If **Keep footage until auto file export complete** is set to **On**, the deletion policy is suspended for individual media files until they have been exported. After a media file has been exported, the original media file on VideoManager is subjected to the deletion policy like normal. **NOTE:** This option should **not** be enabled unless you 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 is kept if one media file within it has been added to an incident. If set to **Off**, only media files that have been added to incidents are preserved. The larg-

Name	Description
	er recording is subject to the deletion policy of VideoManager like normal. • A VB400 enables users to bookmark media in the field, drawing attention to certain portions of media. From the **Bookmarked footage policy** drop-down list, select how bookmarked media should be treated by the deletion policy of VideoManager. The options are as follows: ○ **Keep for same period as non-bookmarked media** – If this option is selected, the deletion policy treats bookmarked and non-bookmarked media identically. ○ **No automatic deletion** – If this option is selected, bookmarked media is entirely exempt from the deletion policy. ○ **Keep for specified amount of time** – If this option is selected, you have the option to configure for how long bookmarked media is kept. The default is 90 days. Enter the number of days for which media is kept after deletion is requested, in case a media file has been deleted accidentally. Enter the number of days for which media is protected after it has been removed from an incident. Media 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 media is subject to normal deletion policies. ○ **Enable forced delete** is set to **On**, as described in the next row.
Forced footage deletion	Controls the deletion policy regarding automatic media deletion. If **Enable forced delete** is set to **On**, media is deleted even if it is part of an incident. Normally, media is never deleted while it is part of an incident.
Export deletion policy	Controls the deletion policy regarding exports on VideoManager. If **Automatically delete old exports** is set to **On**, outdated exports on VideoManager are au-

Name	Description
	tomatically deleted, even if the export has not yet been downloaded to the user's PC. Enter the number of days for which exports are kept after being created. **NOTE:** The original incident is never deleted, only the export is.
Incidents deletion policy	Controls the deletion policy regarding incidents on VideoManager. If **Automatically delete old incidents** is set to **On**, the deletion policy automatically deletes outdated incidents from VideoManager. There is some configuration involved: **a.** From the **User-defined Incident Fields** section, create a new user-defined incident field like normal. For more information, see Creating User-Defined Incident Fields on page 219. **b.** From the **Type** drop-down list, select **Computed Auto-delete**. **NOTE:** There can only be one **Computed auto-delete** user-defined incident field per instance of VideoManager. If one already exists, this option is not visible in the drop-down list. **c.** In the **Delete incident if** field, enter the conditions under which this policy should 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 Custom Predicate Language on page 380. **d.** In the **Auto-deletion date** field, enter the relevant time period, which determines when an incident should be deleted, using the Motorola Solutions custom predicate language. The most simple input would be something similar to `dateAdd(<6, day, creation-time>)`, which would delete incidents that are six days old. For more information, see Custom Predicate Language on page 380. **e.** Click **Save settings**.

Name	Description
	f. Navigate back to the **Deletion Policy** section. g. Set **Automatically delete old incidents** to **On**. If there are incidents to be deleted within the next seven days due to the policy configured in the **Auto-deletion date** field, you can preview these incidents by clicking **<0> incidents will be scheduled for deletion over the next seven days**. If there are incidents to be deleted immediately due to the policy configured in the **Auto-deletion date** field, you can preview these incidents by clicking **<1> incident is scheduled for immediate deletion**. h. Click **Save settings**. i. Click **Yes, make these changes.** and then, **Yes** again to save the changes.
Dashboard	Controls whether a user's media files that are set to be deleted within a certain time frame are visible on their dashboard. In the **Show media scheduled to be deleted within <7> days** field, enter the number of days within which a media file should be deleted, before it will show up on a user's dashboard. This setting only applies to users that have the **View media scheduled to be deleted on dashboard** permission set to **Yes**.
Audit log deletion policy	Controls whether the audit log of VideoManager is automatically deleted after a certain period of time. If **Automatically delete old audit logs** is set to **On**, you must determine for how many days audit logs should be retained before they are automatically deleted by VideoManager.
Annual audit log deletion policy	Controls whether the audit log of VideoManager is automatically deleted after a certain number of years. If **Annually delete old audit logs** is set to **On**, you must determine for how many years an audit log entry should be retained before it is automatically deleted by VideoManager. The age of the audit log entry is calculated from midnight, January 1st. If a log entry is not the configured number of years old by that date, it is kept until the next year. For example,

Name	Description
	if the deletion policy is configured so that all entries are kept for one year, an audit log entry created on January 2nd 2020 will be deleted on January 1st 2022, because it was not one year old on January 1st 2021. **NOTE:** If both **Automatically delete old audit logs** and **Annually delete old audit logs** are set to **On**, audit logs are deleted in line with whichever policy sets the earlier deletion date.

5. Optional: Click **Download Change Summary**.

   This action downloads a CSV file directly to your PC. The file contains information about any changes to which media files and incidents should be deleted as a result of the new policy.

6. Click **Save settings**.

9.4.2
Configuring Incident Exports

You can configure export profiles, which determine how an incident is exported from VideoManager to the user's PC. Export profiles control how exports are handled on VideoManager. For example, how they are formatted, and more.

From the appropriate pane, you 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 action increases the rate at which export jobs are processed.

The types of export profile that you can create are as follows:

- DVD
  For more information, see Creating DVD Export Profiles on page 199.
- MP4
  For more information, see Creating MP4 Export Profiles on page 200.
- Evidence Export
  For more information, see Creating Evidence Export Profiles on page 202.

Enabling Automatic Incident Exports

You can change whether incidents are automatically exported upon creation, which is useful if, due to an organisation's workflow, every incident must be reviewed externally as soon as they have been saved. You can create an export profile first, which all automatically exported incidents will use.

Procedure:

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** drop-down list, select the previously created export profile that automatically exported incidents should inhabit.

   NOTE: You can set rules for export profiles to dictate whether the export profile can be applied to the relevant incident, based on the status of the user-defined incident fields of the incident. However, automatic export ignores any rules set by the selected export profile.
6. Click **Save settings**.

Changing the DVD Export Defaults

This action can be necessary if an organisation consistently uses a specific type of media.

Procedure:

1. Navigate to the **Admin** tab.
2. Select the **Policies** pane.
3. Click the **Incident Exports** section.
4. In the **DVD export defaults** section, from the drop-down list, choose a desired option.
5. Optional: If you want other users to be able to change the type of DVD media when they create an export, set **Can override defaults** to **On**.
6. Click **Save settings**.

Enabling Export Acceleration

Procedure:

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**.
5. Click **Save settings**.
6. From the **Server Controls** section, restart VideoManager.

   NOTE:
   If the PC running VideoManager has an nVidia GPU, it increases the rate at which export jobs are completed.

   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 does not function. You can find out more about the limit by navigating to https://developer.nvidia.com/video-encode-and-decode-gpu-support-matrix-new, expanding the **Encoding** table, and looking under the **Max # of concurrent sessions** column.

   If the PC running VideoManager does not have an nVidia GPU, this action does nothing.

9.4.2.1

Creating DVD Export Profiles

Procedure:

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 opens.
5. In the **Name** field, enter a name for the export profile.
6. From the **Type** drop-down list, select **DVD**.
7. Optional: If you want this export profile to be the default when creating an export from the **Incidents** tab, set **Default** to **Yes**.
8. Optional: If you want users to be able to manually select which incident clips should be included in the export when they export the incident, set **Select clips** to **Yes**.

   NOTE: Users cannot select individual clips if the incident they are exporting contains a composite clip.

   If set to **No**, all incident clips within the incident are included in the export.
9. Optional: In the **Ready to export rules** field, configure the conditions that 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 Creating User-Defined Incident Fields on page 219 and Custom Predicate Language on page 380.
10. Optional: If you want the `.zip` folder containing exports with this profile to be protected with AES 256 encryption, set **Encrypt downloads** to **Yes**.

    You must set a passphrase when you download the export to their PC. You must enter the same passphrase when you extract the `.zip` folder.

    NOTE: Windows cannot extract encrypted `.zip` folders. Instead, you must install 7-zip, which can be downloaded for free from www.7-zip.org, and extract the `.zip` with 7-zip.
11. Optional: If you have implemented a mechanism to automatically notify this system when the export has been processed by the destination system, set **Await export confirmation** to **Yes**.

    This option should only be enabled if exports from this system are automatically transferred to another system. For more information, see Configuring Incident Exports on page 197.

    The export will only appear complete when the destination system confirms the receipt of the export.

    NOTE: Enabling this setting without setting up a confirmation mechanism prevents exports from completing.
12. Optional: If you want to be able to choose the priority for this export when exporting an incident, set **Enable export priority** to **Yes**.

    You must ensure that you have enabled the **Change export priority** permission. For more information, see Incident Permissions on page 328.
13. Optional: If you set **Automatic retry of failed exports** to **Yes**, enter the maximum number of retries and the amount of time after which the failed exports should retry.
14. Optional: To preview title page, perform the following actions:

a. Click **Preview Title Page**.

   The **Preview Title Page** window opens.

b. Enter the Incident Signature.

c. Click **Test Title Page**.

d. To exit the window, click **Close**.

15. Optional: If you want only users or groups entered in the **Permitted users and groups** field to be able to select this export profile when exporting incidents, in the **Access Control** field, set **Restrict to specific users and groups** to **On**.

    You must click + after entering each name, or the user/group will not be added.

    NOTE: If no users are added to this list, then only users with the **Use any export profile** permission are able to access this export profile.

16. Optional: If you want to customise the title page of the export by using markdown, set **Use Template for Title Page** to **On**.

    For more information, see Custom Export Title Pages on page 392.

17. Optional: Set **Title pages**, **Watermark logo**, and **Watermark signature** to **Yes**.

    These settings are applied by default.

18. Optional: In the **Overridable?** column, set the toggles to **Yes**.

    You can change these settings on a per-export basis, as they are being created in the **Incidents** tab.

19. From the **Format** drop-down list, 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.

20. Click **Save settings**.

9.4.2.2
Creating MP4 Export Profiles

Procedure:

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 opens.

5. In the **Name** field, enter a name for the export profile.
6. From the **Type** drop-down list, select **MP4**.

   This export profile is the system default.

7. Optional: If you want this export profile to be the default when creating an export from the **Incidents** tab, set **Default** to **Yes**.

8. Optional: If you want users to be able to manually select which incident clips should be included in the export when they export the incident, set **Select clips** to **Yes**.

   NOTE: Users cannot select individual clips if the incident they are exporting contains a composite clip.

   If set to **No**, all incident clips within the incident are included in the export.

9. Optional: In the **Ready to export rules** field, configure the conditions that 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 Creating User-Defined Incident Fields on page 219 and Custom Predicate Language on page 380.

10. Optional: If you want the `.zip` folder containing exports with this profile to be protected with AES 256 encryption, set **Encrypt downloads** to **Yes**.

    You must set a passphrase when you download the export to their PC. You must enter the same passphrase when you extract the `.zip` folder.

    NOTE: Windows cannot extract encrypted `.zip` folders. Instead, you must install 7-zip, which can be downloaded for free from www.7-zip.org, and extract the `.zip` with 7-zip.

11. Optional: If you have implemented a mechanism to automatically notify this system when the export has been processed by the destination system, set **Await export confirmation** to **Yes**.

    This option should only be enabled if exports from this system are automatically transferred to another system. For more information, see Configuring Incident Exports on page 197.

    The export will only appear complete when the destination system confirms the receipt of the export.

    NOTE: Enabling this setting without setting up a confirmation mechanism prevents exports from completing.

12. Optional: If you want to be able to choose the priority for this export when exporting an incident, set **Enable export priority** to **Yes**.

    You must ensure that you have enabled the **Change export priority** permission. For more information, see Incident Permissions on page 328.

13. Optional: If you set **Automatic retry of failed exports** to **Yes**, enter the maximum number of retries and the amount of time after which the failed exports should retry.

14. Optional: To preview title page, perform the following actions:

    a. Click **Preview Title Page**.

       The **Preview Title Page** window opens.

    b. Enter the Incident Signature.

    c. Click **Test Title Page**.

    d. To exit the window, click **Close**.

15. Optional: If you want only users or groups entered in the **Permitted users and groups** field to be able to select this export profile when exporting incidents, in the **Access Control** field, set **Restrict to specific users and groups** to **On**.

    You must click **+** after entering each name, or the user/group will not be added.

    NOTE: If no users are added to this list, then only users with the **Use any export profile** permission are able to access this export profile.

16. Optional: If you want to customise the title page of the export by using markdown, set **Use Template for Title Page** to **On**.

    For more information, see Custom Export Title Pages on page 392.

17. Optional: Set **Title pages**, **Watermark logo**, and **Watermark signature** to **Yes**.

    These settings are applied by default.

18. Optional: In the **Overridable?** column, set the toggles to **Yes**.

    You can change these settings on a per-export basis, as they are being created in the **Incidents** tab.

19. Click **Save settings**.

9.4.2.3
Creating Evidence Export Profiles

Procedure:

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 opens.

5. In the **Name** field, enter a name for the export profile.
6. From the **Type** drop-down list, select **Evidence Export**.
7. Optional: If you want this export profile to be the default when creating an export from the **Incidents** tab, set **Default** to **Yes**.
8. Optional: If you want users to be able to manually select which incident clips should be included in the export when they export the incident, set **Select clips** to **Yes**.

   NOTE: Users cannot select individual clips if the incident they are exporting contains a composite clip.

   If set to **No**, all incident clips within the incident are included in the export.

9. Optional: In the **Ready to export rules** field, configure the conditions that 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 Creating User-Defined Incident Fields on page 219 and Custom Predicate Language on page 380.

10. From the **Export location** drop-down list, select where the export should be sent to. The options are as follows: **VideoManager filespace**, **Directory**, and **Box**.
    - If you choose **Directory**, configure the following settings:
      - If you want the export to replace another export that is in the same folder with the same name, set **Overwrite existing files** to **Yes**.
      - In the **Output directory** field, enter the output directory for the export.
        The output directory determines where the export is sent.
    - If you choose **Box**, configure VideoManager with the unique information of their Box. Contact the network administrator.
11. Optional: If you want the `.zip` folder containing exports with this profile to be protected with AES 256 encryption, set **Encrypt downloads** to **Yes**.

You must set a passphrase when you download the export to their PC. You must enter the same passphrase when you extract the `.zip` folder.

NOTE: Windows cannot extract encrypted `.zip` folders. Instead, you must install 7-zip, which can be downloaded for free from www.7-zip.org, and extract the `.zip` with 7-zip.

12. Optional: To simulate export, perform the following actions:
    a. Click **Simulate Export**.

       The **Simulate Export** window opens.

    b. Enter the Incident Signature.
    c. Click **Run Simulation**.
    d. To exit the window, click **Close**.
13. Optional: If you have implemented a mechanism to automatically notify this system when the export has been processed by the destination system, set **Await export confirmation** to **Yes**.

    This option should only be enabled if exports from this system are automatically transferred to another system. For more information, see Configuring Incident Exports on page 197.

    The export will only appear complete when the destination system confirms the receipt of the export.

    NOTE: Enabling this setting without setting up a confirmation mechanism prevents exports from completing.
14. Optional: If you want to be able to choose the priority for this export when exporting an incident, set **Enable export priority** to **Yes**.

    You must ensure that you have enabled the **Change export priority** permission. For more information, see Incident Permissions on page 328.
15. Optional: If you set **Automatic retry of failed exports** to **Yes**, enter the maximum number of retries and the amount of time after which the failed exports should retry.
16. Optional: If you want only users or groups entered in the **Permitted users and groups** field to be able to select this export profile when exporting incidents, in the **Access Control** field, set **Restrict to specific users and groups** to **On**.

    You must click **+** after entering each name, or the user/group will not be added.

    NOTE: If no users are added to this list, then only users with the **Use any export profile** permission are able to access this export profile.
17. Optional: Configure any of the following settings:

Name	Description
Export metadata	Controls what metadata is exported alongside the incident • If **Add metadata file** is set to **On**, a separate metadata file is exported alongside the incident file. • From the **Metadata file generation level** drop-down list, you can select which incidents should be exported. This is only relevant if you have licenced *Nested Incidents*. The options are as follows:

Name	Description
	○ **For all incident levels** – There are separate metadata files for the main incident and the nested incidents. ○ **Only the main incident** – There is only a metadata file for the main incident. ○ **Only nested incidents** – There is only 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 **Yes**, a file is created and exported that indicates the export has been completed.
Original footage	Controls what original media is exported alongside the incident. It is only visible if **Include original footage** is set to **Yes**. ● If **Use template for filename** is set to **On**, you must enter a filename template in the **Filename template** field. ● If **Add metadata file** is set to **On**, there are separate metadata files for each original piece of media. You must enter a metadata filename template and content template in the **Metadata filename template** and **Metadata content template** fields, respectively.
Clip footage	Controls what clipped media are exported alongside the incident It is only visible if **Include clip footage** is set to **Yes**. ● If **Use template for filename** is set to **On**, you must enter a filename template in the **Filename template** field. ● If **Add metadata file** is set to **On**, there are separate metadata files for each incident clip. You must enter a metadata filename template and content template in the **Metadata filename template** and **Metadata content template** fields, respectively. ● You can set **Include transcription PDF** to **On**.

You can configure other aspects of an evidence bundle. These aspects are controlled through toggles. The toggles in the left-hand column control whether the features are enabled, and the toggles in the

right-hand **Overridable?** column control whether users can override the predetermined configuration when exporting an incident.

- If **Watermark logo** is set to **Yes**, the export includes the previously configured watermark over the media in the incident.

  This option can be configured in the **Theme Resources** section.

  For more information, see Theme Resources on page 266.
- If **Watermark signature** is set to **Yes**, the automatically created signature of the export is shown over the media of the incident.

  This option corresponds with the information shown in the **Job** column in the **My Exports** pane.
- If **Include original footage** is set to **Yes**, the export includes the original, full-length media from which the incident clips were taken.
- If **Include clip footage** is set to **Yes**, the export includes the clips of the incident.
- If **Include confidential metadata** is set to **Yes**, the export includes the fields of the incident as a JSON file. This action is useful if the user is planning to upload the incident to another instance of VideoManager. This action allows VideoManager to automatically populate the incident fields when the incident is uploaded.
- If **Single file per incident clip** is set to **Yes**, the export includes every redacted incident clip as individual media files instead of one long media file.

18. Click **Save settings**.

9.4.3

Export-Import Feedback Mechanism

An export-import feedback mechanism manages the secure transfer of sensitive data from System A to System B, without compromising system access constraints.

Overview

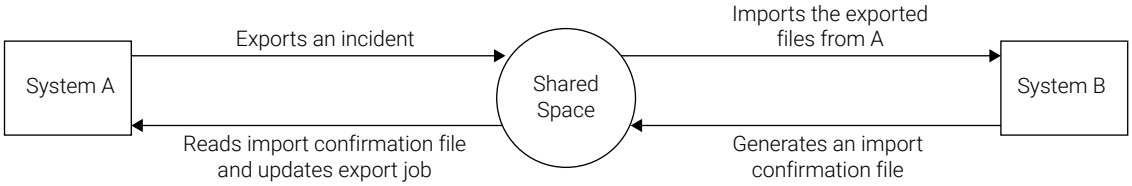
Consider a police officer who has collected crucial video evidence during an investigation. This evidence, stored in their VideoManager system (System A), needs to be accessed by a court official (System B). However, the court official does not have access to the police officer's system due to institutional restrictions or data protection concerns.

The process starts when the police officer creates an incident in System A, attaching the necessary video footage. This incident is then designated for export, leading to the data being transferred into a shared storage that both systems can access.

In parallel, System B has an automated import process that continuously scans the shared storage for new exports from System A. Upon detecting new data, System B initiates processing of the files. Once completed, System B generates a confirmation file that includes important information like the export job signature and a URL for direct access to the video. This file is written into another shared location accessible by System A.

Simultaneously, System A maintains an automated import process that monitors for "import confirmations" from System B. When such a confirmation is ingested, System A updates the associated original export job with the URL provided by System B, and notifies the user who initiated the export, completing the data exchange process.

Figure 1: Export-Import Feedback Mechanism



Configuration Requirements

There are three configuration elements required for System A to automatically export to System B:

1. System A requires an export profile to write the exported files to some mutually accessible location. The signature of the export job must be included in metadata.
2. System B requires an automatic import profile to monitor the location being used for System A's exports. This import profile must also define the location of the commit file and the location and contents of the confirm file used by System A. The confirm file must contain the export job signature to allow System A to confirm when the process completes. Both commit and confirm files must be written to a mutually accessible location, which does not have to be the same as for the System A exports. For more information, see Importing System Configuration for Automatic Imports on page 206.
3. System A must have an automatic import profile, which will be monitored and is used to import the confirmation files generated by System B. This profile does not create any commit/confirm files. System B will use the export job signature written into the confirm file by System A in order to complete the export-import process. For more information, see Exporting System Configuration for Import Confirmations on page 209.

9.4.3.1

Importing System Configuration for Automatic Imports

The importing VideoManager must be configured to automatically detect and import exported files from another exporting VideoManager. This requires configuring an import profile to detect when a new export is ready to be imported by the importing VideoManager, and creating the files used by the exporting VideoManager to verify when the import has completed. Once an automatic import profile is created, VideoManager uses it to automatically detect and import any files matching the given profile and at the specified, to be monitored, location.

To configure an import profile, see Configuring Import Profiles on page 254.

Field values

The key fields for configuring an automatic export are:

- **Profile** is a JSON file defining properties used for the import of files.

  It requires specification of a `monitorPath`. The importing VideoManager observes this location, and all subdirectories, to detect when the exporting VideoManager places new exports within it, which is indicated by a `*.exportcompletion` file being written.

  An `archivePath` must also be defined. When `cleanupMode` is `"MOVE"`, imported files are archived at that location.

The `filters` property is used to exclude any files not to be imported, including the `exportcompletion` file. For more information, see Exporting System Configuration for Import Confirmations on page 209.

- **Commit file path** is a FreeMarker template which, when rendered, defines the absolute path for writing the commit file.

  Both the commit and confirm file paths will be partially rewritten as part of creating the files, such that the commit/confirm files are placed in a subdirectory identified by the import signature. For example, if a path is configured at `c:\test\READY`, the actual file will be written to `c:\test\{exportSignature}\READY`.
- **Confirmation file path** is a FreeMarker template defining the absolute path for writing the confirmation file. The filename should end with the extension `exportcompletion`.
- **Confirmation file contents** is a FreeMarker template defining the contents of the confirmation file. The FreeMarker should resolve to JSON and include a mapping for the `exportSignature`, which is used to indicate completion of the import to the exporting system.
- **Automatic import** should be set to **On** to allow VideoManager to apply the new profile towards detecting and importing new files in the monitored location(s).

Example of the Import Profile

In the following example, the profile will monitor the path `c:\\test_auto_import\\export_to` for any new subdirectories to import. Completed imports, due to `"cleanupMode": "MOVE"`, will be moved into the `archivePath`.

```
{
  "owner":admin",
  "cleanupMode": "MOVE",
  "archivePath": "C:\\test_auto_import\\import_archive\\{name}",
  "moni torPath": "C:\\test_auto_import\\export_to",
  "maxRetries": 3,
  "filters": [
    {
      "pattern": "*.exportconfirmation"
    }
  ]
}
```

Example of the FreeMarker Template for Commit File Path

```
C:\\test_auto_import\\import_confirmation\\${exportJobSignature}_confirmation\\READY
```

Example of the Confirmation Path

```
C:\\test_auto_import\\import_confirmation\\${exportJobSignature}_confirmation\
\export.exportcompletion
```

Example of the Commit File Contents

```
{
  "exportSignature": "${exportJobSignature}"<#if (media[0])??>,
  "url": "${publicWebUri}/app/videos/${media[0].mediaId}/info"</#if>
}
```

NOTE: The above example uses FreeMarker conditionals to only render the URL if there is a media item in the import to link to. If so, the IRL is the first media file in the list.

Corresponding Exporting System Profile

For reference, the matching profile in the exporting system is as follows:

Profile

```
{
  "owner": "admin",
  "requires": "READY",
```

```
  "cleanupMode": "DELETE",
  "archivePath": "C:\\test_auto_import\\export_confirm_archive",
  "monitorPath": "C:\\test_auto_import\\import_confirmation",
  "monitorDetectionPattern": ".*confirmation",
  "maxRetries": 3,
  "filters": [
    {
      "pattern": ". *exportcompletion"
    }
  ]
}
```

The exporting system auto-import profile does not require values to be set for the commit path, confirm path or confirm contents.

Further References

FreeMarker Template Field Values

The import process creates a key:value map, subsequently used to populate variables within the FreeMarker templates defined in the import profile for commit file path, confirmation file path, and confirmation file contents.

When the import contains non-sidecar metadata files, the key:value entries within will also be extracted and exposed for use in rendering FreeMarker.

The import must provide an `*.exportconfirmation` file in the JSON format, used to determine the exportJobSignature. The import will fail if the file is not present, as the value is necessary to the file that notifies the exporting system when the import job has completed.

Table 2: Model Fields

Name	Type	Purpose/Meaning
`publicWebUri`	String	URI for VM public address
`importId`	String	ID of the import job
`importSignature`	String	Signature of the import job
`exportJobSignature`	String	Signature of the export job, provided by the `*.exportconfirmation` file used to trigger the import
`sourcePath`	String	Defines path to the source of the import
`jobCompletionTimeStamp`	Date	Time when the import job was completed
`importProfile`	Map<String, String>	Information on the profile used to perform the import The value is a map with keys `name` and `description`
`media`	List	List of maps, each with data for the imported media files
`metadata`	Map<String, Map> (filename to map)	Contents of any metadata files, that is `*.properties` or `*.json` files included in the import, and the key:value entries within

Name	Type	Purpose/Meaning
`incidents`	Map<String, IncidentTemplate-Model> (incident ID to Incident-TemplateModel)	Incidents associated with the import media, if created

Example

The following example is for FreeMarker to display a large number of the model fields.

```
{
  "importId": "${importId}",
  "publicWebUri": "${publicWebUri}",
  "importSignature": "${importSignature}",
  "exportJobSignature": "${exportJobSignature}",
  "jobCompletionTimeStamp": "${jobCompletionTimeStamp?date}"
  "sourcePath": ${sourcePath},
  "importProfile":
  {
    "name": "${importProfile.name}"
  },
  "metadata":
  [
    <#list metadata as name,entry>
    {
            "name": "${name}",
            <#list data?keys as key,value>
            "${key}": "${value}"
            </#list>
    }<#if name?has_next>,</#if>
    </#list>
    ],
    "firstIncident": "${incidents?values[0].id}"
    "allIncidents":
    [
        <#list incidents as name, entry>
        {
           "id": "${entry.id}",
           "signature": "${entry.signature}",
           "displaySignature": "${entry.display5ignature}",
            "basestationID": "${entry.basestationID}"
         }<#if name?has_next>,</#if>
         </#list>
    ]
}
```

9.4.3.2

Exporting System Configuration for Import Confirmations

To confirm that the export was successfully imported, the importing system creates a subfolder in a predetermined location, populating it with a special metadata file.

The auto-importer of the exporting system scans this location for new folders matching a pattern specified in the profile, ingests the metadata, and completes the export, while populating the `"url"` of the export job.

Generation of Import Confirmations

`exportcompletion` **File Naming**

The metadata file should have the file extension `.exportcompletion`. The rest of the filename is not important to the importer, but may usefully contain other information about the export or importing system.

`exportcompletion` **File Format**

The confirmation file is in the form of a JSON text file and must have the following properties:

- `exportSignature` is the signature of the export you want to confirm the import of.
- `url` is the URL in the destination system for this export.

An example of the file content:

```
{
"exportSignature": "abc123",
"url": "http://server.host:9080/link/to/media/12345"
}
```

Generation of Subfolders

The contents of the subfolder should also include a `"requires"` file that triggers the importer to begin processing the folder. The file should be created in the subfolder after the creation of the `.exportcompletion` file.

It is important that a separate file is used for this purpose, otherwise the importer could attempt to read the `.exportcompletion` file before it has been fully written to the subfolder.

The following example shows a possible layout of a generated subfolder:

```
export_abc123_20230713162000_confirmed/
abc123.exportcompletion
READY
```

Ingestion of Import Confirmations

The export system runs an `automatic` importer to scan for import confirmations from the other system, which requires the configuration of an automatic import profile.

Import Profile

On the export system, you must create an automatic import profile. The profile should include `"requires"`, `"monitorDetectionPattern"`, and `"filters"` properties.

The following is an example of such import profile:

```
{
  "owner": "USER",
  "requires": "READY",
  "cleanupMode": "MOVE",
  "archivePath": "/import_confirmation_archives/{name}-{sign}",
  "monitorPath": "/import_confirmations",
  "monitorDetectionPattern": ".*confirmed",
  "maxRetries": 3,
  "filters": [
    {
      "pattern": "*.exportcompletion"
    }
  ]
}
```

- `owner` is a valid system user.
- `requires` is the filename to detect in the subfolder, which triggers the import. In the example above, an appearance of a file called `READY` triggers the importer to process the subfolder.
- `monitorDetectionPattern` is an expression which matches the name of the subfolder containing the confirmation data. In the example above, the importer detects any subfolder with a suffix of "confirmed". For example, a subfolder named `export_abc123_20230713162000_confirmed` would be presumed to contain the relevant data, but a subfolder named `export_abc123_20230713162000` would not, and would be ignored.
- `filters` shoud be set to use the pattern `*.exportcompletion`, which will allow the importer to correctly identify and process the confirmation file.

As usual for automatic imports, other properties can be configured :

- `cleanupMode` specifies what should happen to the imported directory after completion of the import. For a standard direct mode import, the default is `NONE`, that is, tile directory is left where it is. For autoimports, the default is `RENAME`, which attempts to rename the directory and applies any formatting defined in `archivePath`. If the renamed directory already exists, the import job signature is usually applied as a suffix.

  Other options are `MOVE` and `DELETE`. `DELETE` attempts to completely remove the directory while `MOVE` attempts to move the directory to a location specified by `archivePath`.
- `archivePath` is a location and/or some filename formatting to be applied during the cleanup phase of an import. Tags include `{name}` for the original directory name, `{sign}` for the import job signature, `{year}` for the current year (`2018`), `{month}` for the current month (`05`), and `{day}` for the current day (`03`).
- `monitorPath` is the main directory the importer monitors for new import subfolders.

9.4.3.3
Configuring VideoManager for Export Confirmation

Procedure:

1. Navigate to the **Admin** tab.
2. Select the **Policies** pane.
3. Click the **Incident Exports** section.
4. Perform one of the following actions:
   - In the **Export Profiles** section, click **Create new export profile**.
     For more information, see Creating DVD Export Profiles on page 199, Creating MP4 Export Profiles on page 200, or Creating Evidence Export Profiles on page 202.
   - In the **Export Profiles** section, next to the relevant profile, click **Edit export profile**.
5. From the **Export location** drop-down list, select **Directory** and set a path.

   Ensure that the path has write access and is visible for both systems, including export/import grid workers.
6. Set **Await export confirmation** to **Yes**.

   NOTE: Enabling this setting without setting up a confirmation mechanism prevents exports from completing.
7. Optional: If you want the export to include an incident metadata file, in the **Export metadata** section, set **Add metadata file** to **On**.
8. To create an export, select the incident with some clips in it and select **Export Incident**.

   For more information, see Searching Incidents on page 77.

   The export begins. You can find your export in the **My Exports** pane in the **Incidents** tab. The export displays the `Awaiting Confirmation` status until the importing system acknowledges that the export was successfully imported.

   Once the importing system acknowledges a successful import, the export completes and the status changes to `Ready`.

   If available, you can copy the destination URL by clicking **Copy destination URL** next to the export.

   You can also access the URL from the **Destination URL** section in the **Export details** page.

9.4.3.4

Testing the Export-Import Feedback Mechanism

Prerequisites:

- Ensure that you have two VideoManager systems.
- Ensure that the shared storage is visible by the two instances.
  It can be a folder in the local machine.
- Create parent folders manually.

  NOTE: The path set in `monitorPath`, `archivePath`, `commit file path`, and `confirm file path` must exist. You must create the necessary folders to make the paths available to the systems.

Procedure:

1. Configure an Export Evidence export profile. For more information, see Configuring VideoManager for Export Confirmation on page 211.
2. Configure an import profile by performing the following actions:
   a. Navigate to the **Admin** tab.
   b. Select the **Policies** pane.
   c. Click the **Import profiles** section.
   d. Click **Create new profile**.
   e. Set the profile name and the profile details.
      For more information, see Configuring Import Profiles on page 254.
      For example:

```
{
    "owner": "{vmgr-user}",
    "requires": "READY",
    "cleanupMode": "MOVE",
    "archivePath": "D:\\SharedData\\confirmations_archive\\{name}-{sign}",
    "monitorPath": "D:\\SharedData\\confirmations\\",
    "maxRetries": 3,
    "filters": [
    {
        "pattern": "*.exportcompletion"
    }
  ]
}
```

   f. Set **Automatic import** to **On**.
   g. Click **Save Profile**.

   The export system (System A) scans any subfolders under `D:\\SharedData\\confirmations\\` for a commit file called `READY` and imports any file with extension `exportcompletion`.
3. Configure an import profile by performing the following actions:
   a. Navigate to the **Admin** tab.
   b. Select the **Policies** pane.
   c. Click the **Import profiles** section.
   d. Click **Create new profile**.

e. Set the profile name and the profile details.

For more information, see Configuring Import Profiles on page 254.
For example:

```
{
    "owner": "{vmgr-user}",
    "requires": "Commit.txt",
    "cleanupMode": "MOVE",
    "archivePath": "D:\\SharedData\\exports_archive\\{name}-{sign}",
    "monitorPath": "D:\\SharedData\\exports",
    "maxRetries": 3
}
```

f. Enter the commit file path and name.

For example:

`D:\\SharedData\\confirmations\\READY`

or

`D:/SharedData/confirmations/READY`

g. Enter the confirmation file name with `exportcompletion` as the extension.

For example:

`D:\\SharedData\\confirmations\\{filename}.exportcompletion`

or

`D:/SharedData/confirmations/{filename}.exportcompletion`

h. Set the confirmation file contents.

NOTE: It is important to have at least the export job signature. Otherwise, it will not work.

For example:

```
{
    "exportSignature": "${exportJobSignature}"
    <#if media??>
      ,
      "url": "${publicWebUri}/app/videos/${media[0].mediaId}/info"
    </#if>
}
```

i. Set **Automatic import** to **On**.

j. Click **Save Profile**.

The import system scans any subfolders under `D:\\SharedData\\exports` and imports any contents inside them. After the import is successful, it generates the commit and confirmation files to let the exporting system know that the import was successful.

The content of the confirmation file contains a `url` which is the URL of the importing system. The URL is visible in the exporting system. For more information, see Configuring VideoManager for Export Confirmation on page 211.

NOTE: In some scenarios, the shared space is located in the network. If this is the case, the absolute path will be in the form of either `\\\\vmware-host\\Shared Folders\\` or `//vmware-host/Shared Folders/SharedFolder`.

9.4.4

Configuring File Exports

You can configure VideoManager so that it automatically copies media files to an external location as soon as they have been downloaded from the corresponding cameras. The media files are still available on VideoManager like normal.

Procedure:

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 media files should automatically be sent.

   You can add fields to this path that correlate with the properties of the media files. You can do so by selecting the relevant fields from the **Add Field** drop-down list. You must separate each field with a slash.

   These fields send the media file to sub-folders based on, for example, the operator who recorded the media file, or the serial number of the camera.

   NOTE: If the specified folders do not already exist for this path, they are created as soon as the media files are automatically exported.
6. Optional: To reset the path, click **Reset to Default**.

   The path is reset to `C:\pss-file-exports\<DEV_SERIAL>\<REC_DATE_TIME>`.
7. In the **File name** field, enter the name for individual media files after they have been exported.

   You can add fields to this name that correlate with the properties of the media files, in addition to plaintext. You can do so by selecting the relevant fields from the **Add Field** drop-down list. You must separate each field with a slash.

   NOTE: VideoManager does not save the configuration of the **File name** field unless it generates a unique name for every exported media file. You can click for more information about how to guarantee unique names.
8. Optional: To reset the name, click **Reset to Default**.

   The path is reset to *<DEV_SERIAL>*-*<REC_DATE_TIME>*.*<FILE_INDEX>*.
9. Click **Save settings**.

9.4.5

Enabling and Configuring Automatic Incident Creation

You can configure VideoManager so that it automatically creates incidents, depending on how the user-defined media fields of a media file have been populated.

Prerequisites: Ensure that the *Media Properties* and *Incidents* features are enabled on VideoManager. Contact your account manager to obtain these features. For more information, see Importing and Deleting Licences on page 286.

Procedure:

1. Create user-defined media fields as necessary.

For more information, see Creating User-Defined Media Fields on page 236.

2. Navigate to the **Admin** tab.
3. Select the **Policies** pane.
4. Click the **Auto Incident Creation** section.
5. Set **Auto incident creation enabled** to **On**.
6. Optional: If you want an entire recording to be added to an automatically generated incident if one media file within it meets the requirements for automatic incident creation, set **Use whole recording** to **On**.

   If set to **Off**, a recording is not added to an incident if one of its media files meets the requirements for automatic incident creation. Instead, VideoManager only creates incidents for the individual media files that meet the requirements.
7. In the **Auto incident creation criteria** field, use Motorola Solutions custom predicate language to determine which user-defined media fields should prompt VideoManager to create an incident automatically.

   For more information, see Custom Predicate Language on page 380.
8. Click **Save settings**.

9.4.6
Configuring Password Complexity

You can customise the VideoManager password settings to meet existing security regulations, and make VideoManager more secure.

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.

Procedure:

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 action only affects a user's ability to change their own password from the **Update password** pane of their **Account Profile** tab. You can still update passwords from the **Users** section, even if doing so violates the rule configured here.

   For more information, see Creating, Editing, and Deleting Users on page 138.
6. Configure the password complexity by any of the following criteria:
   - If **Must contain lowercase** is set to **On**, a password must have at least one lowercase letter.
   - If **Must contain uppercase** is set to **On**, a password must have at least one uppercase letter.
   - If **Must contain number** is set to **On**, a password must have at least one number.
   - If **Must contain symbol** is set to **On**, a password must have at least one symbol.

- If **Disallow username in password** is set to **On**, a user cannot include their username in their password.
- If **Disallow repeated characters** is set to **On**, a password cannot have the same character multiple times in a row.
  You must set the maximum number of repeated characters allowed by VideoManager. For example, if the number is set to `1`, then the password `Bubble` would be deemed inadmissible because it has two bs in a row.
- If **Disallow password reuse** is set to **On**, a password cannot match the user's previous passwords.
  You must enter the number of previous passwords, which the new password cannot match.
- If **Require periodic password changes** is set to **On**, you must enter the number of days after which passwords on VideoManager must be reset.
- If **Prevent repeated login attempts** is set to **On**, you must enter the number of times someone can try to log on to VideoManager unsuccessfully, after which their account will be locked. You must also enter the number of minutes for which the profile will be locked, before users can try to log on again.
  Suitably privileged users can unlock other users from the **Users** section of the **People** pane, in the **Admin** tab. For more information, see Unlocking Users on page 141.
- If **Temporary password expire** is set to **On**, a temporary password given to a user if, for example, they forget their password, expires after a set number of hours. You must enter the number of hours for which the password is valid.
- If **Alternate** is set to **On**, the same password restrictions must be configured.
  Any roles that utilise the alternate password complexity must have **Alternate** set to **Yes**. For more information, see Performing Roles Actions on page 149.

7. 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.

9.4.7
Configuring Report Settings

VideoManager automatically deletes reports if the report file space is becoming full. You can configure when your reports should be deleted and when scheduled reports should be run. You can also import a custom report schedule.

Procedure:

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 affects all scheduled reports on VideoManager, and only dictates when reports are generated, not what times they cover.
6. Click **Save settings**.
   You can create a custom report schedule, which dictates what dates a scheduled report should cover, and is selectable by users when creating a scheduled report from the **Status** tab.

7. To create and import a custom schedule, perform the following actions:
   a. Create a JSON file with the desired schedule.

      You 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, so for example, 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
      ```

   b. Navigate to the **Admin** tab.
   c. Select the **Policies** pane.
   d. Click the **Reports** section.
   e. In the **Custom report schedule** pane, click **Import custom schedule**.
   f. Select the relevant JSON file and click **Import**.

      The imported schedule(s) immediately appear in the **Custom report schedule** pane. Users can now select the schedule from the **Schedule** drop-down list when they create a report.
      For more information, see Creating Reports and Performing Report Actions on page 124.

      NOTE: If you import a new JSON file to VideoManager, then all schedules with the same name are overwritten, and all schedules not mentioned in the new JSON file are deleted.

   g. Click **Save settings**.

9.4.8
Exporting and Importing User-Defined Incident Fields

If you have multiple instances of VideoManager, you can transfer a copy of your user-defined incident fields from one instance to another.

Procedure:

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 are saved to the default download location of your PC.

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**.
9. Select the previously downloaded user-defined incident fields.
10. Click **Import**.

    Alternatively, if you want to import all of your user-defined incident fields simultaneously, you can do so from the **Import/Export System Config** section of the **System** pane, in the **Admin** tab.
    For more information, seeExporting and Importing the Configuration of VideoManager on page 288 .

9.4.9

Creating and Applying Validators

You can control the format of information entered into user-defined incident fields. This action can be done through the creation of validators, which can be configured to accept certain patterns and reject others, for example, a UK postcode or a URL.

Procedure:

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 should see when populating a user-defined incident field.

   The description should detail the format to which the user-defined incident field should adhere.
8. In the **Pattern** field, enter the pattern of the validator.

   This action should be done utilising regular expressions.
9. Optional: If you want the validator to ignore the case of the text entered into the user-defined incident field, set **Case insensitive** to **On**.

   If set to **Off**, the case of the text entered into the user-defined incident field must match that of the **Pattern** field.
10. Optional: If you want to test the validator, in the **Test text** field, enter the example text.

    VideoManager determines whether the example text would be accepted by the validator or not.
11. Click **Confirm**.

Postrequisites: After validators have been created, they must be individually applied to user-defined incident fields to ensure that the user-defined incident fields obey the patterns detailed in the validators. This action 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 Creating User-Defined Incident Fields on page 219.

9.4.10
Reordering User-Defined Incident Fields

You can reorder user-defined incident fields, which changes the order in which they are presented during incident creation.

Procedure:

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 are presented in the same order that has been configured here.
   For more information, see Creating Incidents Manually and Performing Incident Actions on page 53.

9.4.11
Creating 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.

Prerequisites:

- Before you create new user-defined incident fields, you can create validators, which define how information entered into user-defined incident fields must be formatted, for example, as a UK postcode.
  For more information, see Creating and Applying Validators on page 218.
- If the new user-defined incident field should show users a different display name based on their session language, you should change the language for your own session before you create the field so that it does not match the server language of VideoManager. This action can be done from either the account menu or the **Language** section.
  For more information, see Configuring the Language on VideoManager on page 269.

Procedure:

1. Navigate to the **Admin** tab.
2. Select the **Policies** pane.
3. Click the **User-defined Incident Fields** section and perform one of the following actions:
   - If you are creating a user-defined incident field which users must populate while creating an incident, click **Create field**.

- If you are 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.

   The identifier should be all lowercase, and unique.

5. In the **Display name** field, enter a display name for the user-defined incident field.

   The display name is what the user-defined incident field is called in the VideoManager UI.

   NOTE: An optional second display name field appears if your session language does not currently match the server language of VideoManager. The field enables you to enter a display name for the field in both languages. If the display name should be set in more than two languages, you must complete the field, save it, then change your session to the third language and edit the field.

6. From the **Type** drop-down list, select the type of a user-defined incident field to be created:

Name	Description
Text	In this user-defined incident field, users can enter text related to the incident, which is useful if users need to search for a specific phrase or word, such as `Assault`, `Arrest`, and more.
Text List	In this user-defined incident field, users can select one or more texts related to the incident.
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 drop-down list related to the incident.
Check box	In this user-defined incident field, users can either select or unselect a check box 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 are populated.
Tag List	In this user-defined incident field, users can select one or more tags related to the incident.
Auto-delete	In this user-defined incident field, users can enter the conditions for auto-delete and the date when the incident should be automatically deleted.

NOTE: The type of user-defined incident field cannot be changed later.

7. Optional: If you do not want users to be able to save an incident unless they populate the field, set **Mandatory** to **On**.
8. From the **Permission group** drop-down list, select to which access group the user-defined incident field should apply.

   Any users in the selected access group are able to view and edit the user-defined incident field when creating and editing incidents.

   If all users should be able to utilise the user-defined incident field when creating and editing incidents, you can select **Public**.

   Computed fields do not need to have the same permission groups as the other user-defined incident fields that determine whether they appear or not. For example, if only some administrators should be able 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 **reviewed-already** could be set to **Public**.
9. From the **Column width** drop-down list, select how wide the column of the user-defined incident field should appear in incident search results.

   This action is only relevant if the user-defined incident field is configured to appear in the incident search results pane.

   For more information, see Configuring User-Defined Field Layouts on page 249.
10. Depending on the kind of user-defined incident field to be created, perform one of the following actions:
    - If you have selected **Text**, see Creating Text Fields on page 222.
    - If you have selected **Text List**, see Creating Text List Fields on page 223.
    - If you have selected **Date**, see Creating Date Fields on page 224.
    - If you have selected **Date & Time**, see Creating Date and Time Fields on page 225.
    - If you have selected **Drop down**, see Creating Drop Down Fields on page 225.
    - If you have selected **Check box**, see Creating Check Box Fields on page 226.
    - If you have selected **URL**, see Creating URL Fields on page 227.
    - If you have selected **Computed**, see Creating Computed Fields on page 228.
    - If you have selected **Tag List**, see Creating Tag List Fields on page 228.
    - If you have selected **Auto-delete**, see Creating Auto-Delete Fields on page 229.

Postrequisites: After you have 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. You can:

- Export user-defined incident fields from one instance of VideoManager, and import them into another instance.

  For more information, see Exporting and Importing User-Defined Incident Fields on page 217.
- Configure how user-defined incident fields are presented when viewing incidents in the **Search Incidents** pane.

  For more information, see Configuring User-Defined Field Layouts on page 249.
- Reorder user-defined incident fields, which affects how user-defined incident fields are presented when creating an incident.

  For more information, see Reordering User-Defined Incident Fields on page 219.

9.4.11.1

Creating Text Fields

After you have selected **Text** from the **Type** drop-down list, the following configuration options appear in the **Text** section.

Procedure:

1. In the **Number of lines** field, enter the number of lines (1-50) which should be displayed at once when viewing the text field in an incident.

   This action 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 four lines of text in the text field of an incident, a scroll bar appears on the right-hand side of the pane to show the last line.

2. In the **Maximum number of characters** field, enter the number.

   If the field is left empty, the field will be unrestricted. Some devices do not enforce this restriction.

3. From the **Validator** drop-down list, select a previously created validator or leave as **(None)**.

   This action dictates how the text field must be formatted, for example, as a UK postcode.
   For more information, see Creating and Applying Validators on page 218.

4. In the **Default value** field, enter a default value.

   This will be the value if nothing else is entered into the field.

   NOTE: If you have selected a validator from the **Validator** drop-down list, the default value in the **Default value** field must match this validator.

5. Optional: If you want incidents to be filtered by the text entered into this text field by using the **Match Text** field in the **Search Incidents** pane, set **Include in match text search** to **Yes**.

6. Optional: If a field should appear in the **Search Incidents** pane that enables users to filter incidents only by the text entered into the text field, set **Show search field** to **Yes**.

   For more information, see Searching Incidents on page 77.

7. Optional: If a field should appear in the transcript editor to provide more context during transcript creation and editing, set **Show in transcription editor** to **Yes**.

   For more information, see Creating and Importing Transcripts for Incident Clips on page 66.

8. Optional: In the **Conditions** section, configure whether the user-defined incident field only appears in the **New Incident** pane when another **Drop down** or **Check box** field has been populated in a specific manner by performing the following actions:

   a. Ensure there is at least one **Drop down** or **Check box** field on VideoManager already.

      Conditions can only be used on these fields.

   b. Click **New condition**.

   c. From the **Field** drop-down list, select which previously created user-defined incident field should dictate the appearance of the current user-defined incident field.

   d. From the **Value** drop-down list, select which values of the previously created user-defined incident field should dictate the appearance of the current user-defined incident field.

      This option is presented as a check box if a **Check box** field has been chosen, and a drop-down list if a **Drop down** field has been chosen.

   e. Click **Confirm**.

9. Click **Save settings**.

9.4.11.2

Creating Text List Fields

After you have selected **Text List** from the **Type** drop-down list, the following configuration options appear in the **Text List** section.

Procedure:

1. From the **Validator** drop-down list, select a previously created validator or leave as **(None)**.

   This action dictates how the text field must be formatted, for example, as a UK postcode.
   For more information, see Creating and Applying Validators on page 218.
2. In the **Maximum number of characters** field, enter the number.

   If the field is left empty, the field will be unrestricted. Some devices do not enforce this restriction.
3. In the **Maximum number of items** field, enter the number.

   If the field is left empty, the field will be unrestricted. Some devices do not enforce this restriction.
4. In the **Default value** field, enter a default value.

   This will be the value if nothing else is entered into the field.

   NOTE: If you have selected a validator from the **Validator** drop-down list, the default value in the **Default value** field must match this validator.

   You can add more default values by clicking **+**.
5. Optional: If a field should appear in the **Search Incidents** pane that enables users to filter incidents only by the text entered into the text field, set **Show search field** to **Yes**.

   For more information, see Searching Incidents on page 77.
6. Optional: If a field should appear in the transcript editor to provide more context during transcript creation and editing, set **Show in transcription editor** to **Yes**.

   For more information, see Creating and Importing Transcripts for Incident Clips on page 66.
7. Optional: In the **Conditions** section, configure whether the user-defined incident field only appears in the **New Incident** pane when another **Drop down** or **Check box** field has been populated in a specific manner by performing the following actions:
   a. Ensure there is at least one **Drop down** or **Check box** field on VideoManager already.

      Conditions can only be used on these fields.
   b. Click **+ New condition**.
   c. From the **Field** drop-down list, select which previously created user-defined incident field should dictate the appearance of the current user-defined incident field.
   d. From the **Value** drop-down list, select which values of the previously created user-defined incident field should dictate the appearance of the current user-defined incident field.

      This option is presented as a check box if a **Check box** field has been chosen, and a drop-down list if a **Drop down** field has been chosen.
   e. Click **Confirm**.
8. Click **Save settings**.

9.4.11.3

Creating Date Fields

After you have selected **Date** from the **Type** drop-down list, the following configuration options appear in the **Date** section.

Procedure:

1. In the **Default value** field, enter a default value.

   This will be the value if nothing else is entered into the field.

2. Optional: If a field should appear in the **Search Incidents** pane that enables users to filter incidents only by a range of dates entered into the date field, set **Search by range** to **Yes**.

   If set to **Off**, users can only filter by one date at a time.

   NOTE: This change does not come into effect unless **Show search field** is also set to **Yes**.

3. Optional: If you want incidents to be filtered by the date entered into this date field by using the **Earliest Date** and **Latest date** fields in the **Search Incidents** pane, set **Include in date search** to **Yes**.

4. Optional: If a field should appear in the **Search Incidents** pane that enables users to filter incidents only by the dates entered into the date field, set **Show search field** to **Yes**.

   For more information, see Searching Incidents on page 77.

5. Optional: If a field should appear in the transcript editor to provide more context during transcript creation and editing, set **Show in transcription editor** to **Yes**.

   For more information, see Creating and Importing Transcripts for Incident Clips on page 66.

6. Optional: In the **Conditions** section, configure whether the user-defined incident field only appears in the **New Incident** pane when another **Drop down** or **Check box** field has been populated in a specific manner by performing the following actions:

   a. Ensure there is at least one **Drop down** or **Check box** field on VideoManager already.

      Conditions can only be used on these fields.

   b. Click **New condition**.

   c. From the **Field** drop-down list, select which previously created user-defined incident field should dictate the appearance of the current user-defined incident field.

   d. From the **Value** drop-down list, select which values of the previously created user-defined incident field should dictate the appearance of the current user-defined incident field.

      This option is presented as a check box if a **Check box** field has been chosen, and a drop-down list if a **Drop down** field has been chosen.

   e. Click **Confirm**.

7. Click **Save settings**.

9.4.11.4

Creating Date and Time Fields

After you have selected **Date & Time** from the **Type** drop-down list, the following configuration options appear in the **Date & Time** section.

Procedure:

1. In the **Default value** field, enter a default value.

   This will be the value if nothing else is entered into the field.
   By clicking **Set to now**, users can set the default value to the current date and time of the server.

2. Optional: If you want incidents to be filtered by the date entered into the field by using the **Earliest Date** and **Latest date** fields in the **Search Incidents** pane, set **Include in date search** to **Yes**.

3. Optional: If a field should appear in the **Search Incidents** pane that enables users to filter incidents only by the date and time entered into the field, set **Show search field** to **Yes**.

   For more information, see Searching Incidents on page 77.

4. Optional: If a field should appear in the transcript editor to provide more context during transcript creation and editing, set **Show in transcription editor** to **Yes**.

   For more information, see Creating and Importing Transcripts for Incident Clips on page 66.

5. Optional: In the **Conditions** section, configure whether the user-defined incident field only appears in the **New Incident** pane when another **Drop down** or **Check box** field has been populated in a specific manner by performing the following actions:

   a. Ensure there is at least one **Drop down** or **Check box** field on VideoManager already.

      Conditions can only be used on these fields.

   b. Click **New condition**.

   c. From the **Field** drop-down list, select which previously created user-defined incident field should dictate the appearance of the current user-defined incident field.

   d. From the **Value** drop-down list, select which values of the previously created user-defined incident field should dictate the appearance of the current user-defined incident field.

      This option is presented as a check box if a **Check box** field has been chosen, and a drop-down list if a **Drop down** field has been chosen.

   e. Click **Confirm**.

6. Click **Save settings**.

9.4.11.5

Creating Drop Down Fields

After you have selected **Drop Down** from the **Type** drop-down list, the following configuration options appear in the **Drop Down** section.

Procedure:

1. Click **New Value**.

   This action adds an option to the **Drop Down** field, which the user can select when creating an incident.

2. In the **Value** field, enter the name of the drop-down option and click **Confirm**.

It is possible to create a **Drop Down** field with just one value.

3. From the **Default value** drop-down list, select a default value.

   This will be the value if nothing else is selected from the **Drop Down** field.

4. Optional: If you want incidents to be filtered by the value of the **Drop Down** field by using the **Match Text** field in the **Search Incidents** pane, set **Include in match text search** to **Yes**.

   For example, if the user selects a value from the **Drop Down** field called **Assault**, they should enter `Assault` into the `Match Text` field.

5. Optional: If a drop-down should appear in the **Search Incidents** pane that enables users to filter incidents only by the value chosen from the **Drop Down** field, set **Show search field** to **Yes**.

   For more information, see Searching Incidents on page 77.

6. Optional: If a field should appear in the transcript editor to provide more context during transcript creation and editing, set **Show in transcription editor** to **Yes**.

   For more information, see Creating and Importing Transcripts for Incident Clips on page 66.

7. Optional: In the **Conditions** section, configure whether the user-defined incident field only appears in the **New Incident** pane when another **Drop down** or **Check box** field has been populated in a specific manner by performing the following actions:

   a. Ensure there is at least one **Drop down** or **Check box** field on VideoManager already.

      Conditions can only be used on these fields.

   b. Click **New condition**.

   c. From the **Field** drop-down list, select which previously created user-defined incident field should dictate the appearance of the current user-defined incident field.

   d. From the **Value** drop-down list, select which values of the previously created user-defined incident field should dictate the appearance of the current user-defined incident field.

      This option is presented as a check box if a **Check box** field has been chosen, and a drop-down list if a **Drop down** field has been chosen.

   e. Click **Confirm**.

8. Click **Save settings**.

9.4.11.6
Creating Check Box Fields

After you have selected **Check box** from the **Type** drop-down list, the following configuration options appear in the **Check box** section.

Procedure:

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. The check box can either be selected or unselected.

2. Optional: If a check box should appear in the **Search Incidents** pane that enables users to filter incidents only by whether the check box field is selected or not, set **Show search field** to **Yes**.

   For more information, see Searching Incidents on page 77.

3. Optional: If a field should appear in the transcript editor to provide more context during transcript creation and editing, set **Show in transcription editor** to **Yes**.

   For more information, see Creating and Importing Transcripts for Incident Clips on page 66.

4. Optional: In the **Conditions** section, configure whether the user-defined incident field only appears in the **New Incident** pane when another **Drop down** or **Check box** field has been populated in a specific manner by performing the following actions:
   a. Ensure there is at least one **Drop down** or **Check box** field on VideoManager already.

      Conditions can only be used on these fields.

   b. Click **New condition**.
   c. From the **Field** drop-down list, select which previously created user-defined incident field should dictate the appearance of the current user-defined incident field.
   d. From the **Value** drop-down list, select which values of the previously created user-defined incident field should dictate the appearance of the current user-defined incident field.

      This option is presented as a check box if a **Check box** field has been chosen, and a drop-down list if a **Drop down** field has been chosen.

   e. Click **Confirm**.
5. Click **Save settings**.

9.4.11.7
Creating URL Fields

After you have selected **URL** from the **Type** drop-down list, the following configuration options appear in the **URL** section.

Procedure:

1. In the **Default value** field, enter a default value.

   This will be the value if nothing else is entered into the field.

   NOTE: The value must be in a URL format.
2. Optional: If you want incidents to be filtered by the URL entered into this text field by using the **Match text** field in the **Search Incidents** pane, set **Include in match text search** to **Yes**.
3. Optional: If a field should appear in the transcript editor to provide more context during transcript creation and editing, set **Show in transcription editor** to **Yes**.

   For more information, see Creating and Importing Transcripts for Incident Clips on page 66.
4. Optional: In the **Conditions** section, configure whether the user-defined incident field only appears in the **New Incident** pane when another **Drop down** or **Check box** field has been populated in a specific manner by performing the following actions:
   a. Ensure there is at least one **Drop down** or **Check box** field on VideoManager already.

      Conditions can only be used on these fields.

   b. Click **New condition**.
   c. From the **Field** drop-down list, select which previously created user-defined incident field should dictate the appearance of the current user-defined incident field.
   d. From the **Value** drop-down list, select which values of the previously created user-defined incident field should dictate the appearance of the current user-defined incident field.

      This option is presented as a check box if a **Check box** field has been chosen, and a drop-down list if a **Drop down** field has been chosen.

   e. Click **Confirm**.

5. Click **Save settings**.

9.4.11.8
Creating Computed Fields

After you have selected **Computed** from the **Type** drop-down list, the following configuration options appear in the **Computed** section.

Procedure:

1. In the **Expression** field, enter the relevant text using Motorola Solutions custom predicate language.

   For more information, see Custom Predicate Language on page 380.
2. Optional: If you want the field to be presented as a URL when creating an incident, set **As Url** to **Yes**.

   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. Optional: If a field should appear in the transcript editor to provide more context during transcript creation and editing, set **Show in transcription editor** to **Yes**.

   For more information, see Creating and Importing Transcripts for Incident Clips on page 66.
4. Optional: In the **Conditions** section, configure whether the user-defined incident field only appears in the **New Incident** pane when another **Drop down** or **Check box** field has been populated in a specific manner by performing the following actions:
   a. Ensure there is at least one **Drop down** or **Check box** field on VideoManager already.

      Conditions can only be used on these fields.
   b. Click **+ New condition**.
   c. From the **Field** drop-down list, select which previously created user-defined incident field should dictate the appearance of the current user-defined incident field.
   d. From the **Value** drop-down list, select which values of the previously created user-defined incident field should dictate the appearance of the current user-defined incident field.

      This option is presented as a check box if a **Check box** field has been chosen, and a drop-down list if a **Drop down** field has been chosen.
   e. Click **Confirm**.
5. Click **Save settings**.

9.4.11.9
Creating Tag List Fields

After you have selected **Tag List** from the **Type** drop-down list, the following configuration options appear in the **Tag List** section.

Procedure:

1. Click **+ New Value** and click **Confirm**.

   This action adds an option to the **Tag List** field, which the user can select when creating an incident. It is possible to create a **Tag List** field with just one value.
2. From the **Default value** drop-down list, select a default value.

   This will be the value if nothing else is selected from the **Tag List** field.

3. Optional: If a field should appear in the **Search Incidents** pane that enables users to filter incidents only by the value chosen from the **Tag List** field, set **Show search field** to **Yes**.

   For more information, see Searching Incidents on page 77.

4. Optional: If a field should appear in the transcript editor to provide more context during transcript creation and editing, set **Show in transcription editor** to **Yes**.

   For more information, see Creating and Importing Transcripts for Incident Clips on page 66.

5. Optional: In the **Conditions** section, configure whether the user-defined incident field only appears in the **New Incident** pane when another **Drop down** or **Check box** field has been populated in a specific manner by performing the following actions:

   a. Ensure there is at least one **Drop down** or **Check box** field on VideoManager already.

      Conditions can only be used on these fields.

   b. Click **New condition**.

   c. From the **Field** drop-down list, select which previously created user-defined incident field should dictate the appearance of the current user-defined incident field.

   d. From the **Value** drop-down list, select which values of the previously created user-defined incident field should dictate the appearance of the current user-defined incident field.

      This option is presented as a check box if a **Check box** field has been chosen, and a drop-down list if a **Drop down** field has been chosen.

   e. Click **Confirm**.

6. Click **Save settings**.

9.4.11.10
Creating Auto-Delete Fields

After you have selected **Auto-delete** from the **Type** drop-down list, the following configuration options appear in the **Auto-delete** section.

Procedure:

1. In the **Delete incident if** field, enter the relevant text using Motorola Solutions custom predicate language.

   For more information, see Custom Predicate Language on page 380.

2. In the **Auto-deletion date** field, enter the relevant text using Motorola Solutions custom predicate language.

   For more information, see Custom Predicate Language on page 380.

3. Optional: If a field should appear in the transcript editor to provide more context during transcript creation and editing, set **Show in transcription editor** to **Yes**.

   For more information, see Creating and Importing Transcripts for Incident Clips on page 66.

4. Optional: In the **Conditions** section, configure whether the user-defined incident field only appears in the **New Incident** pane when another **Drop down** or **Check box** field has been populated in a specific manner by performing the following actions:

   a. Ensure there is at least one **Drop down** or **Check box** field on VideoManager already.

      Conditions can only be used on these fields.

   b. Click **New condition**.

c. From the **Field** drop-down list, select which previously created user-defined incident field should dictate the appearance of the current user-defined incident field.

d. From the **Value** drop-down list, select which values of the previously created user-defined incident field should dictate the appearance of the current user-defined incident field.

   This option is presented as a check box if a **Check box** field has been chosen, and a drop-down list if a **Drop down** field has been chosen.

e. Click **Confirm**.

5. Click **Save settings**.

9.4.12

Editing Default User-Defined Incident Fields

You can create user-defined incident fields to meet unique needs of your organisation. However, VideoManager 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, which is similar to non-default user-defined incident fields. These aspects are the following fields: **Title**, **Incident time**, **Reference code**, and **Notes**.

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 aspects are the following fields: **Creation time**, **Update time**, **Clip count**, **Owner**, and **Signature**, and have an ⚙ icon next to their display names.

Procedure:

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**.
5. Perform one of the following actions:

You can edit any of the following criteria. They are not mandatory.

Option	Actions
Editing a user-defined incident field that is manually populated	• In the **Identifier** field, enter an updated identifier for the user-defined incident field. The identifier should be all lowercase, and unique. • In the **Display name** field, enter an updated display name for the user-defined incident field. • If you want users to be unable to save an incident unless they populate this field, set **Mandatory** to **On**. • From the **Permission group** drop-down list, select to which access group this user-defined incident field should apply. Any users in the selected access group will be able to view this user-defined incident field when creating and editing incidents. • From the **Column width** drop-down list, select how wide the column for the user-defined incident field should appear in incident search results. This action is only relevant if the user-defined incident field is configured to appear in the incident search results pane. For more information, see Configuring User-Defined Field Layouts on page 249. • Depending on the kind of user-defined incident field that is being edited, edit other settings: ○ If you are editing the **title**, **reference-code**, or **notes** field, you can change the configuration in the **Text** section. For more information, see Creating Text Fields on page 222. ○ If you are editing the incident-time field, you can change the configuration in the **Date & Time** section. For more information, see Creating Date and Time Fields on page 225.

Option	Actions
Editing a user-defined incident field which is automatically populated by VideoManager	• In the **Display name** field, enter an updated display name for the user-defined incident field. • From the **Permission group** drop-down list, select to which access group this user-defined incident field should apply. Any users in the selected access group will be able to view this user-defined incident field when creating and editing incidents. • From the **Column width** drop-down list, select how wide the column for the user-defined incident field should appear in incident search results. This action is only relevant if the user-defined incident field is configured to appear in the incident search results pane. For more information, see Configuring User-Defined Field Layouts on page 249. • If you do not want the user-defined incident field to be visible when users edit and view incidents, set **Show in summary** to **No**.

6. Click **Save settings**.

9.4.13
Editing Incident Clip Field Visibility

When a media file is added to an incident, it becomes an incident clip. Incident clips have four properties: **Operator**, **Origin**, **Duration**, and **Notes**. By default, all users on VideoManager can see these four fields. However, administrators can restrict which fields can be seen by users, based on the users' permission groups.

Procedure:

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 next to the field to be edited, click **View field**.

   There are four fields – one for each incident clip property.
5. From the **Permission group** drop-down list, select which users should be able to view the incident clip property.

   By default, the drop-down list 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 drop-down list, 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 340.

   NOTE: The administrator cannot edit the incident clip field further. Incident clip fields cannot be deleted, either.

6. Click **Save settings**.

Postrequisites: You can configure which of these fields are visible when viewing an incident link. For more information, see Configuring Incident Sharing on page 256.

9.4.14

Incident Fields and Rules Configuration for the M500

After you have configured media fields for the M500, you can dictate whether these fields are synchronized to corresponding incident fields, meaning they will be visible in an incident form containing the video, and whether VideoManager will automatically create incidents from videos tagged as critical.

9.4.14.1

Creating an M500 Event Category Incident Field

The M500 event category media field enables operators to categorise recordings on the M500 itself. However, by default, the value selected in this field only appears alongside the individual recording, and it does not appear in incidents the recording is added to. To synchronize this media field, so that its value appears in associated incidents, you must create a new incident field.

Procedure:

1. Navigate to the **Admin** tab.
2. Select the **Policies** pane.
3. Click the **User-defined Incident Fields** section.
4. In the top right-hand corner, click **Create field**.
5. In the **Identifier** field, enter `EventCategory`

   NOTE: The identifier must be set to `EventCategory`, or the two fields will not synchronize.
6. In the **Display name** field, enter a display name for the user-defined incident field.

   The display name is what the user-defined incident field is called in the VideoManager UI.

   NOTE: An optional second display name field appears if your session language does not currently match the server language of VideoManager. The field enables you to enter a display name for the field in both languages. If the display name should be set in more than two languages, you must complete the field, save it, then change your session to the third language and edit the field.
7. From the **Type** drop-down list, select **Drop down**.
8. If you want users to complete this field before they can proceed, set **Mandatory** to **Yes**.
9. From the **Permission group** drop-down list, select which access group should be able to see this field when viewing the video on VideoManager.
10. From the **Column width** drop-down list, select how much space this field should take up when displayed on VideoManager.
11. Scroll down to the **Drop down** section and recreate all of the values of the `EventCategory` media field by clicking **+** in the top right-hand corner, and adding each value one by one.

    NOTE: The incident field must have the exact same values as the media field, or the two fields will not synchronize.

    For more information, see step 10 in the Editing the M500 Event Category Media Field on page 247.

12. Optional: To configure whether the field only appears in the **Edit properties** pane of a video when another drop down field or check box field has been populated in a specific manner, scroll down to the **Conditions** section and perform the following actions:
    a. Ensure that there is at least one drop down field or check box field on VideoManager already.

       Conditions can only be used on these fields.

    b. In the top right-hand corner, click **New condition**.
    c. From the **Field** drop-down list, select which drop down field or check box field should dictate the appearance of this field.
    d. From the **Value** drop-down list, select which values of the drop down field or check box field should dictate the appearance of this field.

       This action is presented as a check box if a check box field has been chosen, and a drop-down list if a drop down field has been chosen.

    e. Click **Confirm**.
13. Click **Save settings**.

9.4.14.2
Enabling and Configuring Automatic Incident Creation

You can configure VideoManager to automatically create an incident for each video which has been tagged as critical on the M500, as soon as those videos have been imported.

Procedure:

1. Navigate to the **Admin** tab.
2. Select the **Policies** pane.
3. Click the **Auto Incident Creation** section.
4. Set **Auto incident creation enabled** to **On**.
5. Set **Use whole recording** to **On**.
6. In the **Auto incident creation criteria** field, enter:

   ```
   isCritical()
   ```
7. Click **Save settings**.

9.4.15
Exporting and Importing User-Defined Media Fields

If you have multiple instances of VideoManager, you can transfer a copy of your user-defined media fields from one instance to another.

Procedure:

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 are saved to the default download location of your PC.

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**.
9. Select the previously downloaded user-defined media fields.
10. Click **Import**.

    Alternatively, if you want to import all of your user-defined media fields simultaneously, you can do so from the **Import/Export System Config** section of the **System** pane, in the **Admin** tab.
    For more information, seeExporting and Importing the Configuration of VideoManager on page 288 .

9.4.16

Creating and Applying Validators

You can control the format of information entered into user-defined media fields. This action can be done through the creation of validators, which can be configured to accept certain patterns and reject others, for example, a UK postcode or a URL.

Procedure:

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 should see when populating a user-defined media field.

   The description should detail the format to which the user-defined media field should adhere.
8. In the **Pattern** field, enter the pattern of the validator.

   This action should be done utilising regular expressions.
9. Optional: If you want the validator to ignore the case of the text entered into the user-defined media field, set **Case insensitive** to **On**.

   If set to **Off**, the case of the text entered into the user-defined media field must match that of the **Pattern** field.
10. Optional: If you want to test the validator, in the **Test text** field, enter the example text.

    VideoManager determines whether the example text would be accepted by the validator or not.
11. Click **Confirm**.

Postrequisites: After validators have been created, they must be individually applied to user-defined media fields, which ensures that the user-defined media fields obey the patterns detailed in the validators. This action 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 Creating User-Defined Media Fields on page 236.

9.4.17

Reordering User-Defined Media Fields

You can reorder user-defined media fields, which changes the order in which they are presented during editing media files.

Procedure:

1. Navigate to the **Admin** tab.
2. Select the **Policies** pane.
3. Click the **User-defined Media Fields** section.
4. Click **Reorder fields**.
5. Grab the left-hand side of the relevant user-defined media field and drag it to the desired location in the list.
6. Click **Confirm**.

   When users edit a media file, the user-defined media fields to be populated are presented in the same order which has been configured here.

9.4.18

Creating User-Defined Media Fields

VideoManager comes with some built-in media fields, which enable users to categorise media files as they are being edited. Administrators can also create their own user-defined media fields to reflect the unique needs of their organisation.

Prerequisites:

- Before you create new user-defined media fields, you can create validators, which define how information entered into user-defined media fields must be formatted, for example, as a UK postcode.
  For more information, see Creating and Applying Validators on page 235.
- If the new user-defined media field should show users a different display name based on their session language, you should change the language for your own session before you create the field so that it does not match the server language of VideoManager. This action can be done from either the account menu or the **Language** section.
  For more information, see Configuring the Language on VideoManager on page 269.

Procedure:

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.

   The identifier should be all lowercase, and unique.
6. In the **Display name** field, enter a display name for the user-defined media field.

The display name is what the user-defined media field is called in the VideoManager UI.

NOTE: An optional second display name field appears if your session language does not currently match the server language of VideoManager. The field enables you to enter a display name for the field in both languages. If the display name should be set in more than two languages, you must complete the field, save it, then change your session to the third language and edit the field.

7. From the **Type** drop-down list, select the type of a user-defined media field to be created:

Name	Description
Text	In this user-defined media field, users can enter text related to the media file, which is useful if users need to search for a specific phrase or word, such as `Assault`, `Arrest`, and more.
Text List	In this user-defined media field, users can select one or more texts related to the media file.
Date	In this user-defined media field, users can select a date related to the media file.
Date & Time	In this user-defined media field, users can select a date and time related to the media file.
Drop down	In this user-defined media field, users can select an option from a drop-down list related to the media file.
Check box	In this user-defined media field, users can either select or unselect a check box related to the media file.
URL	In this user-defined media field, users can enter a URL related to the media file.
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 are populated.
Tag List	In this user-defined media field, users can select one or more tags related to the media file.

NOTE: The type of user-defined media field cannot be changed later.

8. Optional: If you do not want users to be able to save a media file unless they populate the field, set **Mandatory** to **Yes**.
9. Optional: From the **Display timeout** drop-down list, select how long this field should stay on the screen before it disappears.

NOTE: This option is only available on devices that support it and if the field is not mandatory.

10. From the **Permission group** drop-down list, select to which access group the user-defined media field should apply.

Any users in the selected access group are able to view and edit the user-defined media field when creating and editing media files.

If all users should be able to utilise the user-defined media field when creating and editing media files, you can select **Public**.

Computed fields do not need to have the same permission groups as the other user-defined media fields that determine whether they appear or not. For example, if only some administrators should be able 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 **reviewed-already** could be set to **Public**.

11. Optional: If you have selected **Text** from the drop-down type list, if you want in-vehicle devices to capture event information, set **Is Event Tag?** to **Yes**.
12. From the **Column width** drop-down list, select how wide the column of the user-defined media field should appear in media search results.

    This action is only relevant if the user-defined media field is configured to appear in the media search results pane.

    For more information, see Configuring User-Defined Field Layouts on page 249.
13. Depending on the kind of user-defined media field to be created, perform one of the following actions:
    - If you have selected **Text**, see Creating Text Fields on page 238.
    - If you have selected **Text List**, see Creating Text List Fields on page 240.
    - If you have selected **Date**, see Creating Date Fields on page 241.
    - If you have selected **Date & Time**, see Creating Date and Time Fields on page 241.
    - If you have selected **Drop down**, see Creating Drop Down Fields on page 242.
    - If you have selected **Check box**, see Creating Check Box Fields on page 243.
    - If you have selected **URL**, see Creating URL Fields on page 244.
    - If you have selected **Computed**, see Creating Computed Fields on page 245.
    - If you have selected **Tag List**, see Creating Tag List Fields on page 245.

Postrequisites: After you have 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. You can:

- Export user-defined media fields from one instance of VideoManager, and import them into another instance.

  For more information, see Exporting and Importing User-Defined Media Fields on page 234.
- Configure how user-defined media fields are presented when viewing media in the **Search Media** pane.

  For more information, see Configuring User-Defined Field Layouts on page 249.
- Reorder user-defined media fields, which affects how user-defined media fields are presented when editing a media file.

  For more information, see Reordering User-Defined Media Fields on page 236.

9.4.18.1
Creating Text Fields

After you have selected **Text** from the **Type** drop-down list, the following configuration options appear in the **Text** section.

Procedure:

1. In the **Number of lines** field, enter the number of lines (1-50) which should be displayed at once when viewing the text field in a media file.

This action 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 four lines of text in the text field of a media file, a scroll bar appears on the right-hand side of the pane to show the last line.

2. In the **Maximum number of characters** field, enter the number.

   If the field is left empty, the field will be unrestricted. Some devices do not enforce this restriction.

3. Optional: From the **Input type** drop-down list, select the type of input display to be used to enter the value on displays that support it, such as in-vehicle devices.

4. From the **Validator** drop-down list, select a previously created validator or leave as **(None)**.

   This action dictates how the text field must be formatted, for example, as a UK postcode.
   For more information, see Creating and Applying Validators on page 235.

5. In the **Default value** field, enter a default value.

   This will be the value if nothing else is entered into the field.

   NOTE: If you have selected a validator from the **Validator** drop-down list, the default value in the **Default value** field must match this validator.

6. Optional: If you want media files to be filtered by the text entered into the text field by using the **Match Text** field in the **Search Media** pane, set **Include in match text search** to **Yes**.

7. Optional: If a field should appear in the **Search Media** pane that enables users to filter media files only by the text entered into the text field, set **Show search field** to **Yes**.

   For more information, see Searching Media Files on page 36.

8. Optional: If the way the field is populated should be viewable in the **Incident clips** section of the incident editor after the media file has been added to an incident, set **Show in Incidents** to **Yes**.

9. Optional: If you want the field to be visible when users edit and view media, set **Show in summary** to **Yes**.

10. Optional: In the **Conditions** section, configure whether the user-defined media field only appears in the **Edit properties** pane when another **Drop down** or **Check box** field has been populated in a specific manner by performing the following actions:

    a. Ensure there is at least one **Drop down** or **Check box** field on VideoManager already.

       Conditions can only be used on these fields.

    b. Click **New condition**.

    c. From the **Field** drop-down list, select which previously created user-defined media field should dictate the appearance of the current user-defined media field.

    d. From the **Value** drop-down list, select which values of the previously created user-defined media field should dictate the appearance of the current user-defined media field.

       This option is presented as a check box if a **Check box** field has been chosen, and a drop-down list if a **Drop down** field has been chosen.

    e. Click **Confirm**.

11. Click **Save settings**.

9.4.18.2

Creating Text List Fields

After you have selected **Text List** from the **Type** drop-down list, the following configuration options appear in the **Text List** section.

Procedure:

1. From the **Validator** drop-down list, select a previously created validator or leave as **(None)**.

   This action dictates how the text field must be formatted, for example, as a UK postcode.
   For more information, see Creating and Applying Validators on page 235.
2. In the **Maximum number of characters** field, enter the number.

   If the field is left empty, the field will be unrestricted. Some devices do not enforce this restriction.
3. In the **Maximum number of items** field, enter the number.

   If the field is left empty, the field will be unrestricted. Some devices do not enforce this restriction.
4. In the **Default value** field, enter a default value.

   This will be the value if nothing else is entered into the field.

   NOTE: If you have selected a validator from the **Validator** drop-down list, the default value in the **Default value** field must match this validator.

   You can add more default values by clicking **+**.
5. Optional: If a field should appear in the **Search Media** pane that enables users to filter media files only by the text entered into the text field, set **Show search field** to **Yes**.

   For more information, see Searching Media Files on page 36.
6. Optional: If the way the field is populated should be viewable in the **Incident clips** section of the incident editor after the media file has been added to an incident, set **Show in Incidents** to **Yes**.
7. Optional: If you want the field to be visible when users edit and view media, set **Show in summary** to **Yes**.
8. Optional: In the **Conditions** section, configure whether the user-defined media field only appears in the **Edit properties** pane when another **Drop down** or **Check box** field has been populated in a specific manner by performing the following actions:
   a. Ensure there is at least one **Drop down** or **Check box** field on VideoManager already.

      Conditions can only be used on these fields.
   b. Click **+ New condition**.
   c. From the **Field** drop-down list, select which previously created user-defined media field should dictate the appearance of the current user-defined media field.
   d. From the **Value** drop-down list, select which values of the previously created user-defined media field should dictate the appearance of the current user-defined media field.

      This option is presented as a check box if a **Check box** field has been chosen, and a drop-down list if a **Drop down** field has been chosen.
   e. Click **Confirm**.
9. Click **Save settings**.

9.4.18.3

Creating Date Fields

After you have selected **Date** from the **Type** drop-down list, the following configuration options appear in the **Date** section.

Procedure:

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. Optional: If a field should appear in the **Search Media** pane that enables users to filter media files only by a range of dates entered into the date field, set **Search by range** to **Yes**.

   If set to **Off**, users can only filter by one date at a time.

   NOTE: This change does not come into effect unless **Show search field** is also set to **Yes**.

3. Optional: If a field should appear in the **Search Media** pane that enables users to filter media files only by the dates entered into the field, set **Show search field** to **Yes**.

   For more information, see Searching Media Files on page 36.

4. Optional: If the way the field is populated should be viewable in the **Incident clips** section of the incident editor after the media file has been added to an incident, set **Show in Incidents** to **Yes**.
5. Optional: If you want the field to be visible when users edit and view media, set **Show in summary** to **Yes**.
6. Optional: In the **Conditions** section, configure whether the user-defined media field only appears in the **Edit properties** pane when another **Drop down** or **Check box** field has been populated in a specific manner by performing the following actions:
   a. Ensure there is at least one **Drop down** or **Check box** field on VideoManager already.

      Conditions can only be used on these fields.

   b. Click **New condition**.
   c. From the **Field** drop-down list, select which previously created user-defined media field should dictate the appearance of the current user-defined media field.
   d. From the **Value** drop-down list, select which values of the previously created user-defined media field should dictate the appearance of the current user-defined media field.

      This option is presented as a check box if a **Check box** field has been chosen, and a drop-down list if a **Drop down** field has been chosen.

   e. Click **Confirm**.
7. Click **Save settings**.

9.4.18.4

Creating Date and Time Fields

After you have selected **Date & Time** from the **Type** drop-down list, the following configuration options appear in the **Date & Time** section.

Procedure:

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 current date and time of the server.

2. Optional: If a field should appear in the **Search Media** pane that enables users to filter media files only by the date and time entered into the field, set **Show search field** to **Yes**.

   For more information, see Searching Media Files on page 36.

3. Optional: If the way the field is populated should be viewable in the **Incident clips** section of the incident editor after the media file has been added to an incident, set **Show in Incidents** to **Yes**.
4. Optional: If you want the field to be visible when users edit and view media, set **Show in summary** to **Yes**.
5. Optional: In the **Conditions** section, configure whether the user-defined media field only appears in the **Edit properties** pane when another **Drop down** or **Check box** field has been populated in a specific manner by performing the following actions:
   a. Ensure there is at least one **Drop down** or **Check box** field on VideoManager already.

      Conditions can only be used on these fields.

   b. Click **New condition**.
   c. From the **Field** drop-down list, select which previously created user-defined media field should dictate the appearance of the current user-defined media field.
   d. From the **Value** drop-down list, select which values of the previously created user-defined media field should dictate the appearance of the current user-defined media field.

      This option is presented as a check box if a **Check box** field has been chosen, and a drop-down list if a **Drop down** field has been chosen.

   e. Click **Confirm**.
6. Click **Save settings**.

9.4.18.5
Creating Drop Down Fields

After you have selected **Drop Down** from the **Type** drop-down list, the following configuration options appear in the **Drop Down** section.

Procedure:

1. Click **New Value**.

   This action adds an option to the **Drop Down** field, which the user can select when editing a media file.
2. In the **Value** field, enter the name of the drop-down option and click **Confirm**.

   It is possible to create a **Drop Down** field with just one value.
3. From the **Default value** drop-down list, select a default value.

   This will be the value if nothing else is selected from the **Drop Down** field.
4. Optional: If you want media files to be filtered by the value of the **Drop Down** field by using the **Match Text** field in the **Search Media** pane, set **Include in match text search** to **Yes**.

   For example, if the user selects a value from the **Drop Down** field called **Assault**, they should enter `Assault` into the `Match Text` field.
5. Optional: If a drop-down should appear in the **Search Media** pane that enables users to filter media files only by the value chosen from the **Drop Down** field, set **Show search field** to **Yes**.

   For more information, see Searching Media Files on page 36.

6. Optional: If the way the field is populated should be viewable in the **Incident clips** section of the incident editor after the media file has been added to an incident, set **Show in Incidents** to **Yes**.
7. Optional: If you want the field to be visible when users edit and view media, set **Show in summary** to **Yes**.
8. Optional: In the **Conditions** section, configure whether the user-defined media field only appears in the **Edit properties** pane when another **Drop down** or **Check box** field has been populated in a specific manner by performing the following actions:
   a. Ensure there is at least one **Drop down** or **Check box** field on VideoManager already.

      Conditions can only be used on these fields.

   b. Click **New condition**.
   c. From the **Field** drop-down list, select which previously created user-defined media field should dictate the appearance of the current user-defined media field.
   d. From the **Value** drop-down list, select which values of the previously created user-defined media field should dictate the appearance of the current user-defined media field.

      This option is presented as a check box if a **Check box** field has been chosen, and a drop-down list if a **Drop down** field has been chosen.

   e. Click **Confirm**.
9. Click **Save settings**.

9.4.18.6
Creating Check Box Fields

After you have selected **Check box** from the **Type** drop-down list, the following configuration options appear in the **Check box** section.

Procedure:

1. From the **Default value** field, select a default value.

   This will be the value if the check box field is not edited. The check box can either be selected or unselected.

2. Optional: If a check box should appear in the **Search Media** pane that enables users to filter media files only by whether the check box field is selected or not, set **Show search field** to **Yes**.

   For more information, see Searching Media Files on page 36.
3. Optional: If the way the field is populated should be viewable in the **Incident clips** section of the incident editor after the media file has been added to an incident, set **Show in Incidents** to **Yes**.
4. Optional: If you want the field to be visible when users edit and view media, set **Show in summary** to **Yes**.
5. Optional: In the **Conditions** section, configure whether the user-defined media field only appears in the **Edit properties** pane when another **Drop down** or **Check box** field has been populated in a specific manner by performing the following actions:
   a. Ensure there is at least one **Drop down** or **Check box** field on VideoManager already.

      Conditions can only be used on these fields.

   b. Click **New condition**.
   c. From the **Field** drop-down list, select which previously created user-defined media field should dictate the appearance of the current user-defined media field.

d. From the **Value** drop-down list, select which values of the previously created user-defined media field should dictate the appearance of the current user-defined media field.

   This option is presented as a check box if a **Check box** field has been chosen, and a drop-down list if a **Drop down** field has been chosen.

e. Click **Confirm**.

6. Click **Save settings**.

9.4.18.7

Creating URL Fields

After you have selected **URL** from the **Type** drop-down list, the following configuration options appear in the **URL** section.

Procedure:

1. In the **Default value** field, enter a default value.

   This will be the value if nothing else is entered into the field.

   NOTE: The value must be in a URL format.

2. Optional: If you want media files to be filtered by the URL entered into this text field by using the **Match text** field in the **Search Media** pane, set **Include in match text search** to **Yes**.
3. Optional: If the way the field is populated should be viewable in the **Incident clips** section of the incident editor after the media file has been added to an incident, set **Show in Incidents** to **Yes**.
4. Optional: If you want the field to be visible when users edit and view media, set **Show in summary** to **Yes**.
5. Optional: In the **Conditions** section, configure whether the user-defined media field only appears in the **Edit properties** pane when another **Drop down** or **Check box** field has been populated in a specific manner by performing the following actions:

   a. Ensure there is at least one **Drop down** or **Check box** field on VideoManager already.

      Conditions can only be used on these fields.

   b. Click **New condition**.

   c. From the **Field** drop-down list, select which previously created user-defined media field should dictate the appearance of the current user-defined media field.

   d. From the **Value** drop-down list, select which values of the previously created user-defined media field should dictate the appearance of the current user-defined media field.

      This option is presented as a check box if a **Check box** field has been chosen, and a drop-down list if a **Drop down** field has been chosen.

   e. Click **Confirm**.

6. Click **Save settings**.

9.4.18.8

Creating Computed Fields

After you have selected **Computed** from the **Type** drop-down list, the following configuration options appear in the **Computed** section.

Procedure:

1. In the **Expression** field, enter the relevant text using Motorola Solutions custom predicate language.

   For more information, see Custom Predicate Language on page 380.
2. Optional: If you want the field to be presented as a URL when editing a media file, set **As Url** to **Yes**.

   The `encodeURIComponent()` function allows users to encode a string to make it suitable for use in a URL, even if the string contains characters that would normally not be allowed in a URL.
3. Optional: If you want the field to be visible when users edit and view media, set **Show in summary** to **Yes**.
4. Optional: In the **Conditions** section, configure whether the user-defined media field only appears in the **Edit properties** pane when another **Drop down** or **Check box** field has been populated in a specific manner by performing the following actions:
   a. Ensure there is at least one **Drop down** or **Check box** field on VideoManager already.

      Conditions can only be used on these fields.
   b. Click **+ New condition**.
   c. From the **Field** drop-down list, select which previously created user-defined media field should dictate the appearance of the current user-defined media field.
   d. From the **Value** drop-down list, select which values of the previously created user-defined media field should dictate the appearance of the current user-defined media field.

      This option is presented as a check box if a **Check box** field has been chosen, and a drop-down list if a **Drop down** field has been chosen.
   e. Click **Confirm**.
5. Click **Save settings**.

9.4.18.9

Creating Tag List Fields

After you have selected **Tag List** from the **Type** drop-down list, the following configuration options appear in the **Tag List** section.

Procedure:

1. Click **+ New Value** and click **Confirm**.

   This action adds an option to the **Tag List** field, which the user can select when editing a media file.
   It is possible to create a **Tag List** field with just one value.
2. From the **Default value** drop-down list, select a default value.

   This will be the value if nothing else is selected from the **Tag List** field.
3. Optional: If a field should appear in the **Search Media** pane that enables users to filter media files only by the value chosen from the **Tag List** field, set **Show search field** to **Yes**.

   For more information, see Searching Media Files on page 36.

4. Optional: If the way the field is populated should be viewable in the **Incident clips** section of the incident editor after the media file has been added to an incident, set **Show in Incidents** to **Yes**.
5. Optional: If you want the field to be visible when users edit and view media, set **Show in summary** to **Yes**.
6. Optional: In the **Conditions** section, configure whether the user-defined media field only appears in the **Edit properties** pane when another **Drop down** or **Check box** field has been populated in a specific manner by performing the following actions:
   a. Ensure there is at least one **Drop down** or **Check box** field on VideoManager already.

      Conditions can only be used on these fields.

   b. Click **New condition**.
   c. From the **Field** drop-down list, select which previously created user-defined media field should dictate the appearance of the current user-defined media field.
   d. From the **Value** drop-down list, select which values of the previously created user-defined media field should dictate the appearance of the current user-defined media field.

      This option is presented as a check box if a **Check box** field has been chosen, and a drop-down list if a **Drop down** field has been chosen.

   e. Click **Confirm**.
7. Click **Save settings**.

9.4.19

Editing Default User-Defined Media Field Visibility

VideoManager comes with built-in user-defined media fields. Some of these fields can be edited from the **Media** 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 can restrict which of these built-in fields can be seen by users, based on the users' permission groups.

Procedure:

1. Navigate to the **Admin** tab.
2. Select the **Policies** pane.
3. Click the **User-defined Media Fields** section.
4. Next to the relevant default field, click **Edit field**.

   TIP: Default user-defined media fields are marked with an icon.

5. From the **Permission group** drop-down list, select which users should be able to view the user-defined media field.

   By default, the drop-down list 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 drop-down list, so users can only view this property if one of their roles has this permission group enabled.

   NOTE: The administrator cannot edit the incident clip field further. Incident clip fields cannot be deleted, either.

6. Click **Save settings**.

   From now on, only users in a role that has the specified permission group enabled are able to see and edit the 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 Performing Roles Actions on page 149.

9.4.20
Media Fields Configuration for the M500

Media fields dictate how videos are categorised on the M500 after recording has stopped. In addition to a mandatory event category field, you can also optionally add up to five other media fields to the M500.

9.4.20.1
Editing the M500 Event Category Media Field

VideoManager comes with a built-in event category field, which enables users to categorise the videos they capture while still in the field on the M500 itself.

Procedure:

1. Navigate to the **Admin** tab.
2. Select the **Policies** pane.
3. Click the **User-defined Media Fields** section.
4. Next to the `EventCategory` field, click **Edit field**.
5. In the **Display name** field, enter the name which users will see when they are prompted to complete this field.
6. If you want users to complete this field before they can proceed, set **Mandatory** to **Yes**.
7. From the **Display timeout** drop-down list, select how long this field should stay on the screen of the M500 before it disappears.

   NOTE: This option is only available if the field is not mandatory.
8. From the **Permission group** drop-down list, select which access group should be able to see this field when viewing the video on VideoManager.
9. From the **Column width** drop-down list, select how much space this field should take up when displayed on VideoManager.
10. Optional: Scroll down to the **Drop down** section and perform any of the following actions:

    VideoManager comes with dropdown values for this field by default. You can choose to edit or delete these values, or create your own.

    - In the **Values** table, configure settings relating to the values of the field:
      - To create a new value, which users can choose to categorise their video with, in the top right-hand corner, click **+**.
        You can then configure:
        - The name of the value.
        - The display name of the value.

        - Whether the value is critical, that is, the recording will be prioritised during upload. Its resolution may be affected if you configure critical rules to determine image quality, and an incident will be created containing the recording upon import.
    - To edit an existing value, click **Edit value**.
      You can then change its name, display name, and critical status.
    - To delete an existing value, click **Delete value**.
- From the **Default value** drop-down list, select which value should be selected by default.
- If you want M500 videos to be filtered by the value selected from this drop-down list by using the **Match Text** field in the **Search Media** pane, set **Include in match text search** to **Yes**.
- If you want a field to appear in the **Search Media** pane that enables users to filter videos only by the value selected from this drop-down list, set **Show search field** to **On**.
- If you want the value of this drop-down list to be viewable in the **Incident clips** section of the incident editor after the video has been added to an incident, set **Show in Incidents** to **On**.
- If you want this field to be visible when users edit and view incidents, set **Show in summary** to **Yes**.

11. Optional: To configure whether the field only appears in the **Edit properties** pane of a video when another drop down field or check box field has been populated in a specific manner, scroll down to the **Conditions** section and perform the following actions:
    a. Ensure that there is at least one drop down field or check box field on VideoManager already.
       Conditions can only be used on these fields.
    b. In the top right-hand corner, click **New condition**.
    c. From the **Field** drop-down list, select which drop down field or check box field should dictate the appearance of this field.
    d. From the **Value** drop-down list, select which values of the drop down field or check box field should dictate the appearance of this field.
       This action is presented as a check box if a check box field has been chosen, and a drop-down list if a drop down field has been chosen.
    e. Click **Confirm**.
12. To save the event category field, click **Save settings**.

9.4.20.2
Adding Other M500 Event Tags

You can make other existing media fields compatible with the M500, so users can categorise the videos they capture while still in the field on the M500 itself. These are called event tags. Up to five media fields can be enabled as event tags, in addition to the event category.

Procedure:

1. Navigate to the **Admin** tab.
2. Select the **Policies** pane.
3. Click the **User-Defined Media Fields** section.
4. Next to the relevant field, click **Edit field**.
5. Set **Is Event Tag?** to **On**.
6. Click **Save settings**.

7. Optional: If you want operators to use the M500 control panel to specify the title of the incident which will be created automatically when a critical recording is saved, create a new user-defined media field with the following settings:
   a. Set **Identifier** to *<title>*.
   b. Set **Is Event Tag?** to **On**.

9.4.21
Configuring User-Defined Field Layouts

When a user searches for incidents or media files, they are presented with a table showing all relevant incidents or media files in the **Search Incidents** or **Search Media** pane. Administrators can configure which user-defined fields, if any, are shown in this table when the **List** view is selected.

Procedure:

1. Navigate to the **Admin** tab.
2. Select the **Policies** pane.
3. Click either the **User-defined Incident Fields** or **User-defined Media Fields** section.
4. Click **Field layouts**.
   You are presented with the following sections:
   - **Small tables** shows which user-defined fields are displayed in a small table, for example, on a mobile phone.
   - **Medium tables** shows which user-defined fields are displayed in a medium table, for example, on a tablet.
   - **Large tables** shows which user-defined fields are displayed in a large table, for example, on a computer.
5. In the relevant section, click **+**.
6. From the drop-down list, select which user-defined fields should be added to the table.
   The user-defined fields are added to the bottom of the list.
7. If necessary, rearrange the fields in the table by grabbing the left-hand side of the relevant field and dragging it to the desired location in the list.
8. Click **Save changes**.

9.4.22
Exporting and Importing User-Defined Playback Reason Fields

If you have multiple instances of VideoManager, you can transfer a copy of your user-defined playback reason fields from one instance to another.

Procedure:

1. In the original instance of VideoManager, 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 are saved to the default download location of your PC.
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**.
9. Select the previously downloaded user-defined playback reason fields.
10. Click **Import**.

    Alternatively, if you want to import all of your user-defined playback reason fields simultaneously, you can do so from the **Import/Export System Config** section of the **System** pane, in the **Admin** tab. For more information, see Exporting and Importing the Configuration of VideoManager on page 288.

9.4.23

Creating and Applying Validators

You can control the format of information entered into user-defined playback reason fields. This action can be done through the creation of validators, which can be configured to accept certain patterns and reject others, for example, a UK postcode or a URL.

Procedure:

1. Navigate to the **Admin** tab.
2. Select the **Policies** pane.
3. Click the **User-defined Playback Reason 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 should see when populating a user-defined playback reason field.

   The description should detail the format to which the user-defined playback reason field should adhere.
8. In the **Pattern** field, enter the pattern of the validator.

   This action should be done utilising regular expressions.
9. Optional: If you want the validator to ignore the case of the text entered into the user-defined playback reason field, set **Case insensitive** to **On**.

   If set to **Off**, the case of the text entered into the user-defined playback reason field must match that of the **Pattern** field.
10. Optional: If you want to test the validator, in the **Test text** field, enter the example text.

    VideoManager determines whether the example text would be accepted by the validator or not.
11. Click **Confirm**.

Postrequisites: After validators have been created, they must be individually applied to user-defined playback reason fields to ensure that the user-defined playback reason fields obey the patterns detailed in the validators. This action must be done during user-defined playback reason field creation. Validators cannot be edited after a user-defined playback reason field has been created.

For more information, see Creating User-Defined Playback Reason Fields on page 251.

9.4.24
Reordering User-Defined Playback Reason Fields

Procedure:

1. Navigate to the **Admin** tab.
2. Select the **Policies** pane.
3. Click the **User-defined Playback Reason Fields** section.
4. Click **Reorder fields**.
5. Grab the left-hand side of the relevant user-defined media field and drag it to the desired location in the list.
6. Click **Confirm**.

   When users edit a media file, the user-defined playback reason fields to be populated are presented in the same order which has been configured here.

9.4.25
Creating User-Defined Playback Reason Fields

User-defined playback reason fields are used in conjunction with the playback policy. When a user views a media file, which is a certain number of days old, VideoManager prompts 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.

Procedure:

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 creating user-defined incident fields, but with fewer options. Administrators can create as many user-defined playback reason fields as necessary.

   For more information, see Creating User-Defined Incident Fields on page 219.

Postrequisites:

After you have created user-defined playback reason fields, you must configure the playback policy to prompt users to complete these fields after a certain period of time.

For more information, see Configuring the Playback Policy on page 257.

You can perform actions on these user-defined playback reason fields from the **User-defined Playback Reason Fields** pane. You can:

- Export user-defined playback reason fields from one instance of VideoManager, and import them into another instance.

  For more information, see Exporting and Importing User-Defined Playback Reason Fields on page 249.

- Reorder user-defined playback reason fields, which affects how user-defined playback reason fields are presented.
  For more information, see Reordering User-Defined Playback Reason Fields on page 251.

9.4.26

Exporting and Importing User-Defined Share Reason Fields

If you have multiple instances of VideoManager, you can transfer a copy of your user-defined share reason fields from one instance to another.

Procedure:

1. In the original instance of VideoManager, navigate to the **Admin** tab.
2. Select the **Policies** pane.
3. Click the **User-defined Share Reason Fields** section.
4. Click **Export**.
   The user-defined share reason fields are saved to the default download location of your PC.
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 Share Reason Fields** section.
8. Click **Import**.
9. Select the previously downloaded user-defined share reason fields.
10. Click **Import**.
    Alternatively, if you want to import all of your user-defined share reason fields simultaneously, you can do so from the **Import/Export System Config** section of the **System** pane, in the **Admin** tab.
    For more information, see Exporting and Importing the Configuration of VideoManager on page 288.

9.4.27

Creating and Applying Validators

You can control the format of information entered into user-defined share reason fields. This action can be done through the creation of validators, which can be configured to accept certain patterns and reject others, for example, a UK postcode or a URL.

Procedure:

1. Navigate to the **Admin** tab.
2. Select the **Policies** pane.
3. Click the **User-defined Share Reason 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 should see when populating a user-defined share reason field.

   The description should detail the format to which the user-defined share reason field should adhere.

8. In the **Pattern** field, enter the pattern of the validator.

   This action should be done utilising regular expressions.

9. Optional: If you want the validator to ignore the case of the text entered into the user-defined share reason field, set **Case insensitive** to **On**.

   If set to **Off**, the case of the text entered into the user-defined share reason field must match that of the **Pattern** field.

10. Optional: If you want to test the validator, in the **Test text** field, enter the example text.

    VideoManager determines whether the example text would be accepted by the validator or not.

11. Click **Confirm**.

Postrequisites: After validators have been created, they must be individually applied to user-defined share reason fields to ensure that the user-defined share reason fields obey the patterns detailed in the validators. This action must be done during user-defined share reason field creation. Validators cannot be edited after a user-defined share reason field has been created.

For more information, see Creating User-Defined Share Reason Fields on page 253.

9.4.28
Reordering User-Defined Share Reason Fields

Procedure:

1. Navigate to the **Admin** tab.
2. Select the **Policies** pane.
3. Click the **User-defined Share Reason Fields** section.
4. Click **Reorder fields**.
5. Grab the left-hand side of the relevant user-defined media field and drag it to the desired location in the list.
6. Click **Confirm**.

   When users edit a media file, the user-defined share reason fields to be populated are presented in the same order which has been configured here.

9.4.29
Creating User-Defined Share Reason Fields

User-defined share reason fields are used in conjunction with the playback policy. When a user wants to share a media file, which is a certain number of days old, VideoManager prompts them to give a reason as to why they want to share it. The user must then enter their answer in the previously created user-defined share reason field.

Procedure:

1. Navigate to the **Admin** tab.
2. Select the **Policies** pane.

3. Click the **User-defined Share Reason Fields** section.

   The process for creating user-defined share reason fields is the same as the process for creating user-defined incident fields, but with fewer options. Administrators can create as many user-defined share reason fields as necessary.

   For more information, see Creating User-Defined Incident Fields on page 219.

Postrequisites: After you have created user-defined share reason fields, you can perform actions on these user-defined share reason fields from the **User-defined Playback Reason Fields** pane. You can:

- Export user-defined share reason fields from one instance of VideoManager, and import them into another instance.

  For more information, see Exporting and Importing User-Defined Share Reason Fields on page 252.
- Reorder user-defined share reason fields, which affects how user-defined share reason fields are presented.

  For more information, see Reordering User-Defined Share Reason Fields on page 253.

9.4.30

Configuring Import Profiles

Import profiles determine how media files can be imported into VideoManager. They can also be used in tandem with user-defined media fields to insert media file metadata into VideoManager as the media files are imported.

Prerequisites: Create at least one user-defined media field, which can be populated by users when they import media files.

For more information, see Creating User-Defined Media Fields on page 236.

Procedure:

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.

   The description tells other users on VideoManager what this profile controls. For example, which user-defined media fields are automatically populated.
7. In the **Profile** field, enter the profile.

   The most simple profile populates certain user-defined media fields for a media file automatically, when it is imported. This means that the user does not need to do it manually after the media file is imported. The JSON format is as follows:

   ```
   "properties": "<name of user-defined media field>": "<value of user-defined media field>"
   ```

   For example, if you created a user-defined media field called `vehicle-type`, any media files 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 as shown in the following example.

```
"properties": "vehicle-type": "car","category": "arrest"
```

Another simple profile enables users to populate the user-defined media fields for a media file, before the media file is imported. The JSON properties are as follows:

- `promptedFields` – The user importing the media file can optionally populate these user-defined media fields before the media file is imported.
- `promptedMandatory` – The user importing the media file must populate these user-defined media fields before the media file 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 media file.

```
"promptedFields": "import-reason"
```

In the following configuration, users would have to populate the `import-reason` user-defined media field before they could import their media file.

```
"promptedMandatory": "import-reason"
```

NOTE: For more complex import profile configurations, you should contact Motorola Solutions Support.

8. Verify that **Automatic import** it set to **Off**.

   Automatic import should be set to **Off** unless specified by Motorola Solutions Support.

   When set to **Off**, the user must choose the profile from the drop-down list when manually importing files from the **Media** tab.

   For more information, see Importing Media Files on page 41.

9.4.31
Enabling and Configuring the Antivirus Policy

Users can import media files from external sources into VideoManager. If administrators have an OPSWAT account, they can use it to automatically scan these media files for viruses as they are being imported into VideoManager.

Prerequisites: Configure the antivirus policy.

The antivirus policy dictates the type of files to be scanned for viruses.

Procedure:

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 you have an on-premise OPSWAT account, the URL will be different. For more information, you should contact the system administrator.

6. In the **API Key** field, enter the API key associated with your OPSWAT account.

   To find the API key, log on 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** and check the **Current connection status:** section.

   - If the status displays `Connection succeeded`, the API key is valid and working correctly.
   - If the status displays `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 to scan them for viruses.

   The file size upper limit depends on your 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.

   NOTE: The larger an imported file, the longer OPSWAT takes to scan it for viruses.

10. Optional: From the **Media files** and **Non media files** drop-down lists, 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, media files are scanned for viruses as they are imported into VideoManager. If a media file fails the antivirus scan, it cannot be imported.

9.4.32
Configuring Incident Sharing

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 becomes inaccessible to anyone who does not have an account on VideoManager, and configure which incident clip fields are visible in a link.

Procedure:

1. Navigate to the **Admin** tab.
2. Select the **Policies** pane.
3. Click the **Incident Sharing** section.
4. In the **Default email address** field, enter the email address, which should 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 should be active, before it expires.

   Users can override this expiry time when creating a link from the **Incidents** tab. For more information, see Sharing Incidents Externally Using a Link on page 85.

6. Optional: In the **Incident link visible fields** section, configure which incident clip fields are visible when an incident is shared via an incident link.

   This action 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 is configured so that only users in permission group one can view it, then you could enable **Access Group One** here. This means that the **Operator** property would be visible in the incident link.

   For more information, see Editing Incident Clip Field Visibility on page 232.

7. Click **Save settings**.

9.4.33

Configuring the Playback Policy

You can control whether, after a certain time, media files cannot be viewed on VideoManager without the user first recording their reason for viewing, and whether all media files on VideoManager have a watermark when played back.

Prerequisites: Create a user-defined playback reason field.

This action enables users to provide their reason for rewatching media files. If a user-defined playback reason field is not created after the playback policy is configured, then users must still acknowledge that they are rewatching a media file after a certain amount of time has elapsed, but VideoManager does not prompt them for a reason.

For more information, see Creating User-Defined Playback Reason Fields on page 251.

Procedure:

1. Navigate to the **Admin** tab.
2. Select the **Policies** pane.
3. Click the **Playback Policy** section.
4. If you want users to record their reason for watching a media file after a set number of days, set **Enable playback reason auditing** to **On**.
5. In the **Require media playback reason** section, enter the number of days since the media file was recorded, after which a user must give a reason for watching it.
6. From the **Protection mode** drop-down list, select one of the following options:
   - If you want to enable authenticated and authorised users to use download tools, select **Disabled**.
   - If you want to protect videos against download tools running on modern web browsers only, select **Default protection**.
   - If you want to protect videos against download tools running on modern web browsers and reject play attempts from older web browsers, select **Strict protection**.

     NOTE: If you select **Strict protection**, all users must be on modern web browsers in order to play videos.
7. Click **Save settings**.

9.4.34

Configuring Playback Watermarks

Procedure:

1. Navigate to the **Admin** tab.

2. Select the **Policies** pane.
3. Click the **Playback Watermark** section.
4. Set **Enable playback watermarking** to **On**.
5. In the **Text** box, enter the text to be displayed.
6. Next to the **Text** box, click + and from the drop-down list, select which live field you want to add to the text.

   The options are: **Playback signature**, **Username**, **Date**, and **Time**.
7. From the **Size** drop-down list, select the desired size of the watermark.
8. From the **Background opacity** drop-down list, select the background opacity of the watermark.
9. From the **Position** drop-down list, select where the watermark should be displayed.
10. Click + **Add watermark**.
11. To add a new watermark, repeat step 5 through step 10.
12. To delete the watermark, next to the watermark to be deleted, click .
13. Click **Save settings**.

9.4.35

Configuring Mobile App Settings

If the Mobile App has been licenced from Motorola Solutions, you can configure its settings from VideoManager. You should do this before you start operating your Mobile App.

For more information about setting up the Mobile Apps with VideoManager, you can navigate to https://www.motorolasolutions.com/en_xu.html and search for *VideoManager: VB SmartControl User Guide* or *VideoManager VB Companion Guide*.

Procedure:

1. Navigate to the **Admin** tab.
2. Select the **Policies** pane.
3. Click the **Mobile App Settings** section.
4. In the **VB Companion settings** section, perform the following actions:
   a. In the **Update app configuration after** field, enter the number of days after which VB Companion must receive an updated configuration from VideoManager.

      NOTE: For the action to be successful, the phone running VB Companion must be able to reach the instance of VideoManager from which it was provisioned, for example over a WiFi network or VPN, and the administrator must click **Refresh config** in VB Companion. If VB Companion cannot reach VideoManager within the number of days specified, it stops working.
   b. In the **Devices must be docked every** field, enter the number of days after which the body-worn cameras associated with individual instances of VB Companion must be redocked.

      Only one body-worn camera can be associated with an instance of VB Companion at any one time. However, multiple instances of VB Companion can be associated with one instance of VideoManager.
   c. Optional: If you want all communication between the VB400 and the user's phone to be encrypted with SSL, set **Use SSL** to **Yes**.

If enabled, you are presented with an SSL certificate which you must download and install onto the phone which is running VB Companion.

5. In the **VB SmartControl settings** section, perform any of the following actions:
   - If you want all communication between the VB400 and the user's phone to be encrypted with SSL, set **Use SSL** to **Yes**.
   - If you want watermarks to be displayed on video playback in the mobile app, set **Enable playback watermarks** to **Yes**.
6. From the **SmartControl default auth mode**, select which authentication method you will use during provisioning.

   The options are as follows: **Client certificate** or **Bluetooth**.

   NOTE:
   Depending on the Mobile App, VB400 supports different Authentication modes:
   - For VB Companion, VB400 supports only Client Certificate mode.
   - For VB SmartControl, VB400 supports only Bluetooth Authentication mode.
   - For SmartControl, VB400 supports both Client Certificate and Bluetooth modes, with Client Certificate as the default.

   V500 supports only Bluetooth Authentication mode.
7. Click **Save settings**.

9.4.36
Creating, Viewing, and Deleting API Keys

API keys dictate how VideoManager communicates with external software or cameras.

Creating API Keys

Procedure:

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 but it is strongly recommended.
6. If you want the API key to be automatically generated upon creation, set **Generate key** to **On**.

   NOTE: Setting to **On** is necessary if you are creating an entirely new API key.

   If set to **Off**, you can enter the key manually, which is necessary if you are adding a previously existing API key to VideoManager.
7. If you want the API secret to be automatically generated upon creation, set **Generate secret** to **On**.

   NOTE: Setting to **On** is necessary if you are creating an entirely new API key.

   If set to **Off**, you can enter the secret manually, which is necessary if you are adding a previously existing API key to VideoManager.

8. From the **API key roles** drop-down list, select which role is most appropriate for the API key.

   NOTE: If you will be integrating your own software with VideoManager, the **Use System Role** option is recommended.

9. If you selected the **Use System Role** option, from the **Roles** drop-down list, select which roles of VideoManager the API key should inhabit.
10. Verify that the information entered is correct.

    NOTE: API keys cannot be edited after creation.

11. To save the API key, click **Confirm**.

    The API key and API secret are presented.

    NOTE: You must make a note of the API secret because it cannot be viewed again.

Viewing API Keys

Procedure:

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**.

   You can enter the name of the API key in the **Name / Key** field, and select the role of an API key from the **API key roles** drop-down list.

   You can click **Reset filter** to clear the search filters.

5. Next to the API key to be edited, click **View API key**.

   You can view here the **Name**, **Key**, and **API key role**.

6. Click **Close**.

Deleting API Keys

Procedure:

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**.

   You can enter the name of the API key in the **Name / Key** field, and select the role of an API key from the **API key roles** drop-down list.

   You can 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

In the **User Interface** pane, you can edit aspects of VideoManager relating to the appearance and layout of the user interface.

From the **User Interface** pane, you can access the following sections:

- In the **Login Settings** section, you can create, edit, and delete login warnings, and configure user agreements.
  For more information, see Configuring Login Settings on page 261.
- In the **Media List** section, you can change how all users view media files on their homepage.
  For more information, see Configuring the Media List on page 264.
- In the **Messages** section, you can create messages that all users can view on their homepage.
  For more information, see Creating, Editing, and Deleting Messages on page 264.
- In the **Theme Resources** section, you can change the logos displayed on VideoManager and its colour scheme.
  For more information, see Theme Resources on page 266.
- In the **Player** section, you can change the default quality at which media files are played on VideoManager.
  For more information, see Configuring Player on page 268.
- In the **Language** section, you can change the default language in which the VideoManager user interface is displayed.
  For more information, see Configuring the Language on VideoManager on page 269.
- In the **Maps** section, you can change map settings. This action is necessary if administrators want to use Tactical VideoManager, view location data for recorded media, and filter recorded media by location.
  For more information, see Enabling and Configuring Maps on page 270.
- In the **Thumbnails** section, you can change the default thumbnail for media files that have been imported without a built-in thumbnail.
  For more information, see Configuring Thumbnails on page 271.
- In the **Incidents** section, you can configure how incident clips are presented in incidents.
  For more information, see Configuring Incident Settings on page 272.
- In the **Tactical** section, you can configure viewing options for the **Tactical** tab.
  For more information, see Configuring Tactical on page 272.

9.5.1
Configuring 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.

Procedure:

1. Navigate to the **Admin** tab.
2. Select the **User Interface** pane.

3. Click the **Login Settings** section.

   You can configure any of the following sections:

   - **Login warning** enables administrators to create a login warning on VideoManager. The login warning will be displayed at the bottom of the login pane of VideoManager, and will be visible to all users before they access VideoManager.
   - **User agreement** enables administrators to create a user agreement. All users on VideoManager must agree to this text when logging on for the first time.
   - **Session settings** controls how frequently users must log on to VideoManager if the system is inactive.
   - **Privilege elevation** controls privilege escalation settings. For more information, see Configuring Privilege Escalation on page 307.

4. Optional: If you want to configure the **Login warning** section, perform the following actions:

   a. In the **Warning text** field, enter the warning.

   b. Customize the text using any of the following settings:

Name	Description
B Bold	Any text within the asterisks appears bold.
I Italic	Any text within the underscores appears italicised.
H Heading	Any text on the same line as ### appears as heading text.
URL/Link	You are prompted to enter a hyperlink. A link description can be entered in the square brackets.
Image	You can enter a URL for an image. An image description can be entered in the brackets.
Unordered List	Any text after the hyphen appears as part of a bullet point list. **Unordered List** must be clicked for each individual list entry.
Ordered List	Any text after the hyphen appears as part of a numbered list. **Ordered List** must be clicked for each individual list entry. The numbers appear in order once the message is previewed.
Code	Any text within the single quotation marks appears as code.
Quote	Any text on the same line as > appears as a quote.

   Clicking the buttons again undoes the changes.

   By clicking **Preview**, a previewable version becomes visible. You can edit the text by clicking **Preview** again.

   c. Click **Save settings**.

5. Optional: If you want to configure the **User agreement** section, perform the following actions:
   a. Set **Users must accept agreement on login** to **On**.
   b. In the **Agreement title** field, enter a title for the user agreement.
   c. In the **Agreement text** field, enter the text for the user agreement.

      The text could be legal information, or terms and conditions.
   d. Customize the text using any of the following settings:

Name	Description
B Bold	Any text within the asterisks appears bold.
I Italic	Any text within the underscores appears italicised.
H Heading	Any text on the same line as ### appears as heading text.
URL/Link	You are prompted to enter a hyperlink. A link description can be entered in the square brackets.
Image	You can enter a URL for an image. An image description can be entered in the brackets.
Unordered List	Any text after the hyphen appears as part of a bullet point list. **Unordered List** must be clicked for each individual list entry.
Ordered List	Any text after the hyphen appears as part of a numbered list. **Ordered List** must be clicked for each individual list entry. The numbers appear in order once the message is previewed.
Code	Any text within the single quotation marks appears as code.
Quote	Any text on the same line as > appears as a quote.

      Clicking the buttons again undoes the changes.

      By clicking **Preview**, a previewable version becomes visible. You can edit the text by clicking **Preview** again.
   e. In the **Acceptance text** field, enter an agreement text.

      Users must agree to this text before logging on to VideoManager.

      NOTE: The default text is
      `I agree to the terms and have read the User Agreement.`
   f. Click **Save settings**.
6. Optional: If you want to configure the **Session settings** section, perform the following actions:
   a. In the **Session timeout** field, enter the number of minutes for which VideoManager must be inactive, after which the user must log on again.
   b. Click **Save settings**.

9.5.2
Configuring the Media List

You can customize how media files are presented by default, for both users' personal dashboards and the **Media** tab.

Procedure:

1. Navigate to the **Admin** tab.
2. Select the **User Interface** pane.
3. Click the **Media List** section.
4. From the **Media display mode** drop-down list, select how media files on users' dashboards are presented.

   The options are **List** or **Gallery**.
5. From the **Media sort order** drop-down list, select how media files in the **Media** tab are ordered.

   The options are **Recording date**, **Recording date (least recent)**, or **Date added**.
   This action sets the default in the **Media** tab for all users. However, users with the correct permissions can override the default for their individual session. For more information, see Changing Viewing Options on page 39.
6. Click **Save settings**.

9.5.3
Creating, Editing, and Deleting Messages

Messages are displayed on the dashboard when a user logs on. From the appropriate pane, you can create, edit, and delete messages.

Creating Messages

Procedure:

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.

   The title appears in bold at the top of the message.
6. From the **Type** drop-down list, select the type of message to be created.
   - **General** – appears next to the message.
   - **Warning** – appears next to the message.
   - **Tutorial** – appears next to the message.
7. In the **Text** field, enter the message.
8. Optional: Customize the text using any of the following settings:

Name	Description
Bold	Any text within the asterisks appears bold.
Italic	Any text within the underscores appears italicised.
Heading	Any text on the same line as ### appears as heading text.
URL/Link	You are prompted to enter a hyperlink. A link description can be entered in the square brackets.
Image	You can enter a URL for an image. An image description can be entered in the brackets.
Unordered List	Any text after the hyphen appears as part of a bullet point list. **Unordered List** must be clicked for each individual list entry.
Ordered List	Any text after the hyphen appears as part of a numbered list. **Ordered List** must be clicked for each individual list entry. The numbers appear in order once the message is previewed.
Code	Any text within the single quotation marks appears as code.
Quote	Any text on the same line as > appears as a quote.

Clicking the buttons again undoes the changes.

By clicking **Preview**, a previewable version becomes visible. You can edit the text by clicking **Preview** again.

9. Optional: In the **Link** field, enter the address of another website.

   The address appears at the bottom of the message, and users can click on it to learn more about the message.

10. Optional: If you want users to be able to hide the message on their own dashboard by clicking **Hide**, set **User can hide** to **On**.

    NOTE: This action only hides 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**.

Editing Messages

Editing messages can be necessary if the content or formatting of the message should be changed.

Procedure:

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**.

Deleting Messages

Procedure:

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**.
5. In the confirmation window, click **Yes**.

9.5.4
Theme Resources

You can specify certain aspects of images, colour scheme, and branding of VideoManager, which can be done from the **Theme Resources** section of the **User Interface** pane, in the **Admin** tab.

There are two aspects to configuring theme resources:

- Changing logos
  For more information, see Changing Logos of VideoManager on page 266.
- Changing colour scheme
  For more information, see Changing the Colour Scheme of VideoManager on page 267.

9.5.4.1
Changing Logos of VideoManager

Every instance of the Motorola Solutions logo can be replaced with still or animated images in .jpg, .jpeg, .png or .gif format. This action enables users to change logos of VideoManager to match the branding of their organisation.

Procedure:

1. Navigate to the **Admin** tab.
2. Select the **User Interface** pane.
3. Click the **Theme Resources** section.

   The options presented are as follows:

   - **Login background** – The image used as the background when users log on
   - **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.
     The image must be a PNG file with a transparent background.

- **Favicon** – The icon shown in the VideoManager tab
  The icon must be a file that is 16 x 16 pixels.

4. Next to the image to be edited, click **Replace theme resource**.
   The **Import theme resource** window opens.
5. Select **Choose File**.
6. Select the file to be used, and click **OK**.
   The new graphics are updated immediately.
7. Optional: To reset the logo, next to the icon to be reset, click **Reset to default**.

9.5.4.2

Changing the Colour Scheme of VideoManager

You can change the colour scheme of VideoManager to match the corporate branding of an organisation.

Procedure:

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**.
   You can enter a specific colour name as either a HTML/CSS colour name or a Hex code. For example, `orangered` and `#ff4500` would produce the same colour in the UI. Alternatively, you can click the box on the right-hand side to choose the colour manually.
5. Optional: In the **General colours** section, configure any of the following categories:
   - **Background colour** changes the background colour of VideoManager.
   - **Text colour** changes the colour of the text in body of VideoManager, as well as the colour of icons when the cursor is held over them.
   - **Link colour** changes the colour of UI controls that take the user to a different page. For example, **Find incidents**.
   - **Dark areas** changes the colour of pane headings.
   - **Light areas** changes the colour of unselected heading options.
6. Optional: In the **Navigation Bar colours** section, configure any of the following categories:
   - **Text colour** changes the colour of unselected text in the main navigation bar.
   - **Background colour** changes the colour of the background in the main navigation bar.
   - **Current section text colour** changes the colour of the selected text in the main navigation bar.
   - **Current section background colour** changes the colour of the selected background in the main navigation bar.
   - **Background colour (when mouse over)** changes the colour of the background in the main navigation bar when the mouse is hovering over it.
7. Optional: In the **Media panel colours** section, configure **Header background colour (in incidents)**.
   This option changes the colour of the headings for media files that are included in one or more incidents.

8. To save the colour scheme, click **OK**.
9. Optional: To reset the colour scheme, click **Reset to defaults**.

9.5.4.2.1
Transfering Copies of the Colour Scheme

Transfering a copy of a colour scheme from one instance of VideoManager to another can be 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.

Procedure:

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. Next to the colour scheme to be exported, click **Export**.

   The colour scheme is downloaded to your 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 and click **Import**.

9.5.5
Configuring Player

You can select the default quality at which media files are played in the VideoManager player.

Procedure:

1. Navigate to the **Admin** tab.
2. Select the **User Interface** pane.
3. Click the **Player** section.
4. From the **Default quality** drop-down list, select the default media file quality.

   The options are as follows: **Highest**, **Standard**, **Low**, **Lower**, **Very low**, and **Lowest**.
5. Click **Save settings**.

   Any changes come into effect only when you log on again or when you refresh the page.
   Users who have the **Control playback quality** permission enabled can override this default when they watch media files from the **Media** tab. Users without the permission must watch all media files from the **Media** tab in the selected quality.

   For more information, see Viewing Media Files on page 42.

9.5.6

Configuring the Language on VideoManager

You can perform a range of actions regarding the language of VideoManager. You can change the language in which the VideoManager interface is presented to all users, as well as import new language files, and disable languages.

Changing the Server Language of VideoManager

Server language is the default language in which all users navigate VideoManager.

Procedure:

1. Navigate to the **Admin** tab.
2. Select the **User Interface** pane.
3. Click the **Language** section.
4. In the top pane, from the **Server language** drop-down list, select a language.

   NOTE: 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.

Ignoring the Browser Language at Login

Ignoring the browser language at login can be useful if the browser running VideoManager is in one language, but users want to use it in another.

Procedure:

1. Navigate to the **Admin** tab.
2. Select the **User Interface** pane.
3. Click the **Language** section.
4. Set **Ignore browser language at login** to **Yes**.

   If set to **No**, VideoManager will try to use the browser language.

Changing the Language of the Current Session

Changing the language of your current session is useful if you want to navigate VideoManager in a different language for the duration of your personal session.

Procedure:

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 is changed only until you log out or your session expires.

   Users can 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 so must be configured

by an administrator. The relevant permission is **Select Language for login session**, under **Advanced** permissions.

Importing Language Files into VideoManager

Importing language files into VideoManager enables you to navigate VideoManager in that language.

Procedure:

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 opens.
5. Browse to the file to be imported and click **Import**.

Disabling Language Files

If a language has been disabled, users cannot select it from their drop-down list. However, a disabled language can still be set as the server language of VideoManager, or the language for an individual's session.

Procedure:

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

Enabling and Configuring Maps

You can enable or disable maps, select between map and location lookup providers, and set the default location for media recorded without a GPS track.

Prerequisites: If you will be using the private ArcGis service, you must first register VideoManager as an app on the service.

Procedure:

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** drop-down list, select the maps provider.

   This action enables you to perform actions such as utilising Tactical VideoManager, adding location data to videos, and filtering videos based on this location data. The options are as follows:

- If you selected **Google Places**, enter an API key in the **Google API key** field.
  An API key can be generated from the Google developers' page, which can be found at https://developers.google.com/maps/documentation/javascript/get-api-key.
- If you selected **OpenStreetMap**, enter a server URL in the **OSM tile server URL** field.
  A list of free tile providers can be found at https://wiki.openstreetmap.org/wiki/Raster_tile_providers.
- If you selected **ArcGIS**, enter a server URL in the **ArcGIS tile server URL** field.

  NOTE: If you are using a private ArcGis service, you must 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.

  If you are not using a private ArcGis service, Motorola Solutions recommends copying and pasting this server URL.

6. From the **Location lookup provider** drop-down list, select the location lookup provider.

   This action enables you to enter specific addresses and postcodes when filtering videos based on your location and editing video location data. The options are as follows:

   - If you selected **Google Places**, enter an API key.
     You can use the same API key as entered in step 5.
   - If you selected **Nominatim**, enter a server URL into the **Nominatim server URL** field.
     Nominatim providers can prompt you to enter an API key into the **Nominatim API key** field.
   - If you selected **ArcGIS**, enter a server URL from your ArcGis account into the **ArcGIS search server URL** field.
     If you are not using a private ArcGis service, Motorola Solutions recommends copying and pasting this server URL.
   - If you selected **–**, go to step 7.
     No further details must be entered.

     NOTE: If you select this option, you cannot enter specific addresses and postcodes when setting location data for videos. You will only be able to drag and drop a location pin.

7. From the **Distance units** drop-down list, select the unit of measurement that should be used by VideoManager when presenting maps.

   The options are: **Imperial (ft/mi)** and **Metric (m/km)**.

8. Optional: In the **Default location** field, set a default location for videos that do not have GPS data.

   For example, because the camera on which the videos were recorded is not GPS-enabled.

   - To confirm the choice, click **Set**.
   - To clear the field, click ✕.

9. Click **Save settings**.

9.5.8 Configuring Thumbnails

You can utilise markdown to create a phrase that will appear in the place of a thumbnail for media files that were imported without a built-in thumbnail.

The following procedure describes how to edit the custom thumbnails for imported media files.

Procedure:

1. Navigate to the **Admin** tab.

2. Select the **User Interface** pane.
3. Click the **Thumbnails** section.
4. Edit any of the following fields:
   - **Audio file expression** dictates the default thumbnail for audio media files.
   - **PDF file expression** dictates the default thumbnail for PDF media files.
   - **Other files expression** dictates the default thumbnail for other types of media files.

   There are some thumbnail-specific functions that you can input. The functions are as follows:
   - `\n` creates a line break.
   - `+` strings multiple values together.
   - `text()` returns a string representation of whatever input it is given. This could be a number, or dates.
   - `formatInterval()` rearranges a number of seconds into a more readable format.

   For example, `formatInterval(100)` would return `1m40s`.

   NOTE: The expression entered is formatted with markdown.
5. Click **Save settings**.

9.5.9
Configuring Incident Settings

- If VideoManager was upgraded to 17.0 or higher, media files, which have been added to an incident, that is incident clips, are presented by default as separate clips within that incident, regardless of which recording they came from. However, you can configure VideoManager to present incident clips as children of the original recording they came from. This action enables other users on the system to directly compare the original recording to the redacted and shortened incident clips.
- If VideoManager was installed with 17.0 or higher, incident clips are presented by default as children of the original recording they came from. However, you can configure VideoManager to present incident clips as separate clips within that incident, regardless of which recording they came from.

Procedure:

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** or **No**.
5. Click **Save settings**.

   NOTE: This change applies retroactively to all incidents on the system.

9.5.10
Configuring Tactical

Procedure:

1. Navigate to the **Admin** tab.

2. Select the **User Interface** pane.
3. Click the **Tactical** section.
4. Perform any of the following actions:
   - Set **Show events panel** to **On**.
     When enabled, the events panel displays at the bottom of the map in the **Tactical** tab, and lists device events.
   - Set **Show global video wall** to **On**.
     When enabled, you can open the Global Video Wall and add streams to it.
   - Set **Show user video wall** to **On**.
     When enabled, you can open the User Video Wall and add streams to it.
5. Click **Save settings**.

9.6 Firmware

In the **Firmware** pane, you can edit aspects of VideoManager relating to camera firmware.

From the **Firmware** pane, you can access the following sections:

- In the **Firmware Settings** section, you can change global firmware settings, regarding auto-upgrades.
  For more information, see Configuring Firmware Settings on page 273.
- In the **Device Images** section, you can import, delete, and edit body-worn camera images.
  For more information, see Importing, Deleting, and Editing Images on page 274.
- In the **Vehicle Images** section, you can import, delete, and edit images from an M500.
  For more information, see Importing, Deleting, and Editing Images on page 274.
- In the **LTE Images** section, you can import, delete, and edit LTE images.
  For more information, see Importing, Deleting, and Editing Images on page 274.
- In the **Dock Images** section, you can import, delete, and edit dock images.
  For more information, see Importing, Deleting, and Editing Images on page 274.

9.6.1 Configuring Firmware Settings

VideoManager can automatically upgrade cameras when new firmware is released, which eliminates the need for users to manually upgrade their cameras from the **Devices** tab.

Procedure:

1. Navigate to the **Admin** tab.
2. Select the **Firmware** pane.
3. Click the **Firmware Settings** section.
4. In the **Auto-upgrade** section, configure whether the cameras, vehicles, docks, and EdgeControllers should be automatically upgraded by VideoManager to whichever firmware is set as the default.

   If set to **Off**, you must manually upgrade cameras, vehicles, docks, and EdgeControllers from the **Devices** tab.

5. Optional: If you have selected **Auto-upgrade docks** to **On**, in the **From:** and **Until:** fields, enter the times between which docks will attempt to upgrade.

   This action minimises disruption to the system.

   NOTE: If a dock is upgrading, all cameras connected to it will be inaccessible until a dock has finished upgrading, which means that they cannot be assigned or allocated.

6. In the **Default firmware** section, configure which firmware on VideoManager is set as the default.

   If **Use latest firmware as default** is set to **On**, the default images for cameras, vehicles, docks, and EdgeControllers are automatically set to the most recent.

   The effect this action has depends on how the **Auto-upgrade** section is configured.

   - If auto-upgrade is enabled for devices, they are upgraded to the most recent firmware automatically.
   - If auto-upgrade is disabled for devices, the most recent firmware is presented as default when a user tries to upgrade them manually from the **Devices** pane. Users can override this default.

7. Click **Save settings**.

9.6.2

Importing, Deleting, and Editing Images

Importing Images

Procedure:

1. Navigate to the **Admin** tab.
2. Select the **Firmware** pane.
3. Perform one of the following actions:
   - Click **Device Images**.
   - Click **Vehicle Images**.
   - Click **LTE Images**.
   - Click **Dock Images**.
4. Click **Import image**.
5. Select a file to import as a new image.
6. Optional: If you want the image to become the default, set **Default Image** to **On**.

   When users upgrade a camera from the **Devices** tab, this image will be presented first. However, users can change which image is used.

   This setting is only available if **Use latest firmware as default** is set to **Off** in the **Firmware Settings** section. For more information, see Configuring Firmware Settings on page 273.

7. To confirm the choice, click **OK**.

Deleting Images

Procedure:

1. Navigate to the **Admin** tab.

2. Select the **Firmware** pane.
3. Perform one of the following actions:
   - Click **Device Images**.
   - Click **Vehicle Images**.
   - Click **LTE Images**.
   - Click **Dock Images**.
4. Next to the image to be deleted, click .

   NOTE: A default image cannot be deleted.
   Cameras retain their images, even if the image has been deleted.
5. To confirm deletion, click **OK**.

Editing Images

Procedure:

1. Navigate to the **Admin** tab.
2. Select the **Firmware** pane.
3. Perform one of the following actions:
   - Click **Device Images**.
   - Click **Vehicle Images**.
   - Click **LTE Images**.
   - Click **Dock Images**.
4. Next to the image to be edited, click .
5. Optional: In the **Name** field, change the name of the image.
6. Optional: If you want the image to become the default, set **Default Image** to **On**.

   When users upgrade a camera from the **Devices** tab, this image will be presented first. However, users can change which image is used.
   This setting is only available if **Use latest firmware as default** is set to **Off** in the **Firmware Settings** section. For more information, see Configuring Firmware Settings on page 273.
7. Optional: To learn more about the type of image and the hardware that the image can support, click **More details**.
8. To confirm the changes, click **Confirm**.

9.7 System

In the **System** pane, you can edit aspects of VideoManager relating to storage and server configuration.

NOTE: The **System** pane should not be accessed unless the administrator has working knowledge of their PC.

From the **System** pane, you can access the following sections:

- In the **Storage** section, you can:
  - Configure file containers, if you will be using S3 Object Storage or Azure Blob Storage instead of a filesystem.
    For more information, see Creating and Editing File Containers on page 276.
  - Configure file spaces and free up space on an instance of VideoManager.
    For more information, see Performing File Spaces Actions on page 278.
  - Configure file space warnings, which appear when one of the file spaces of VideoManager is almost full.
    For more information, see Configuring File Space Warnings on page 282.
- In the **Web Server** section, you can configure web server settings, and discover the public and listen addresses of the server.
  For more information, see Configuring Listen and Public Addresses of VideoManager on page 283, Configuring SSL Certificates for Device Authentication on page 284 or Using a Client Certificate Authentication for Login on page 284.
- In the **Backup Databases** section, you can configure how often backups are performed.
  For more information, see Creating and Configuring Backup Databases on page 285.
- In the **Licences** section, you can import or renew licences. Licences determine which actions users can perform on VideoManager. For example, Tactical VideoManager is a licenced feature.
  For more information, see Importing and Deleting Licences on page 286.
- In the **Advanced Settings** section, you can configure the advanced settings file.
  For more information, see Advanced Settings Configuration on page 287.
- In the **System Time Zone** section, you can configure the system time zone of VideoManager.
  For more information, see Setting the System Time Zone of VideoManager on page 287.
- In the **Import/Export System Config** section, you can import or export key aspects of the configuration of VideoManager.
  For more information, see Exporting and Importing the Configuration of VideoManager on page 288.
- In the **Preview Features** section, you can preview features that are suitable for demonstration and field trial.
- In the **Server Controls** section, you can restart the server. This action allows certain changes to come into effect. For example, if the administrator has changed the server listen address of VideoManager.

9.7.1
Creating and Editing File Containers

If media and other data are stored in object storage instead of a file system, administrators must create file containers on VideoManager, which contain information about the object store. This action enables file spaces on VideoManager to connect to the cloud.

NOTE: You can only perform this procedure if you are using Amazon S3 Object Storage or Azure Blob Storage. If you are using filesystem storage, you can skip this procedure.

Procedure:

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.

   The file container will be identified by that name on VideoManager.
6. From the **Type** drop-down list, select either **S3 Object Storage** or **Azure Blob Storage**.
7. Perform one of the following actions:

If...	Then...
If you are using S3 Object Storage,	perform the following actions: **a.** In the **Bucket name** field, enter the bucket name. Motorola Solutions suggests using a unique fully qualified domain name of VideoManager **b.** In the **Endpoint** field, enter the endpoint of the file container. To check this information, you must 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. Then, you must enter the region in the **Endpoint** field, with the following format: `s3.<region code>.amazonaws.com` where *<region code>* is the region. **NOTE:** The endpoint must match the region where the bucket was created. **c.** In the **Key** and **Secret** fields, enter the key and secret of the IAM user, respectively. You can only get this information immediately after creating an IAM user with S3 access. If you do not have the key and secret for the IAM user, you must create another user and make a note of the key and secret's information, which is presented when the user is saved.

If...	Then...
If you are using Azure Blob Storage,	perform the following actions: **a.** In the **Container name** field, enter the name of the container. You can either enter the name of a container that already exists in your Azure account, or enter the name for a new container. If a new container name is entered, Azure Blob Storage automatically creates the container. To check whether the action 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. **b.** In the **Endpoint** field, enter the endpoint of the file container. To check this information, in the **Endpoints** tab, you must click the **Blob service** pane, and copy and paste the value from the **Blob service** field. **c.** In the **Account** field, enter the name of the Azure Blob Storage account. **d.** In the **Secret** field, enter the secret of the container. To check this information, on Azure, you must navigate to the **Access Keys** tab, click **Show keys**, and copy and paste either of the keys.

8. Click **Confirm**.

9.7.2
Performing File Spaces Actions

File spaces determine where files from VideoManager are stored, how much space VideoManager can use, and whether the files are encrypted when they are stored. Files can be stored on the administrator's PC (if administrators have accepted the default file space configuration, file spaces are stored on the PC with the path `C:\ProgramData\Motorola Solutions\VideoManager.`), network-attached storage, or Amazon S3 Object Storage/Azure Blob Storage (if it has been purchased). It is important to note that some files, such as temporary files and config files, are always kept on the local hard drive, even if VideoManager has been configured to use a different kind of storage.

NOTE: VideoManager only supports Amazon S3 Object Storage or Azure Blob Storage. Other kinds of object storage are not compatible and cannot be used to store files from VideoManager.

Cameras generate large numbers of very large files. It is important to consider how much storage capacity will be required and how much bandwidth the storage system will require, which is why Motorola Solutions recommends dedicated network-attached storage. When file spaces are full, associated system functions will stop working. For example, cameras will be unable to download media files, and will enter an error state.

You can administer your file spaces, which includes creating new file spaces, moving files within them, increasing their sizes, and deleting them.

Creating File Spaces

You can create new file spaces alongside existing ones. This action can be necessary if files should be stored in a different location, or if a file space of one type is becoming full and more space should be added.

Procedure:

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.

   If you have purchased S3 Object Storage or Azure Blob Storage, you should enter the name of a folder within the bucket, which will then be created.

   NOTE: If you are using a grid configuration, you must ensure that the path can be accessed by all workers in the grid. For more information about setting up grids with VideoManager, you can navigate to the Motorola Solutions Learning Experience Portal (registration is free) and search for *VideoManager and Grids Explained*.
6. From the **Category** drop-down list, select a category for the file space.

   The options are as follows:

   - **Footage** is where media on VideoManager are stored. Additionally, imported media files are stored here, too.
   - **Exports** is where exports on VideoManager are stored.
   - **Reports** is where reports on VideoManager are stored.
   - **Backups** is where system backups on VideoManager are stored.
   - **Resources** is where theme resources, such as logos, colour schemes, and device firmware, are stored on VideoManager.
   - **Import Workspace** is where temporary files are stored. This option is only necessary if a grid system with import workers is being used with VideoManager.
7. From the **Container** field, select the type of container for the file space.

   The options are as follows:

   - **Filesystem** – The file space is contained in the filesystem.
   - If you have created a file container whose details correspond to either a S3 Object Storage or Azure Blob Storage container, you can select either of these storages.
8. In the **Max size** field, enter the maximum size that VideoManager should use in the file space.

   Motorola Solutions recommends that the maximum size is not set to the absolute upper limit of the disk/drive, as VideoManager will behave incorrectly when the disk/drive is completely full.

   NOTE: Because many object storage systems do not have a maximum capacity, this field ensures that storage costs are capped.
9. From the **State** drop-down list, select a state for the file space.

In most cases, the option is **Online**.

The other options are as follows:

- **OBSOLETE** – Files in an obsolete file space are still available, but no new files will be written to the file space.
- **OFFLINE** – Usually, if a file space is unexpectedly unavailable, VideoManager stops writing files to all file spaces. However, if a file space is marked as offline, VideoManager can continue using other file space. Files in the offline file space will be unplayable and inaccessible.
- **EVACUATE** – This option automatically moves all data in the file space to the other file space(s) of the same type, which is useful if an old file space should not have any new files written to it, but the existing files within it should be kept.

  NOTE: If another administrator on the system is viewing, editing, or exporting the data in a file space that is being evacuated, the evacuation is forced to wait until the other actions have finished.

10. If relevant, from the **Encryption** drop-down list, select an encryption type.

    The options are as follows: **None**, **AES-128**, **AES-192**, or **AES-256**.

    NOTE: If unsure, Motorola Solutions recommends choosing **AES-256**.

    The encryption type cannot be changed later. If an encryption mode is chosen, you must download the encryption key after creation, and store it offsite. This action ensures that the data can be recovered later in case of a disaster.

    To download the encryption key, you must click **Go to file space** next to the file space whose encryption key should be downloaded, and click **Download Key**.

    The key is downloaded to the default download location of your PC. It should be transferred to a secure location offsite.

11. Optional: If you want all information relevant to the file space to be sent to the file space until it is full, set **Preferred** to **Yes**.

    If multiple file spaces have **Preferred** set to **Yes**, VideoManager alternates between those file spaces when storing resources.

    If no file spaces have **Preferred** set to **Yes**, VideoManager alternates between all file spaces when storing resources.

12. To save the changes, click **Confirm**.

Relocating Files

If you want to relocate the files in a file space to a new location, Motorola Solutions recommends creating an entirely new file space with the new desired path, and evacuating all files in the old file space over to it.

Procedure:

1. Navigate to the **Admin** tab.
2. Select the **System** pane.
3. Click the **Storage** section.
4. If the new file space has not already been created, 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. Next to the old file space whose path must be changed, click > **Go to file space**.
9. From the **Category** drop-down list, select **Evacuate**.

   The data in the old file space is evacuated to the file space with the new path. The evacuation can take some time.

10. Optional: After the old file space has been fully evacuated, delete it by clicking **Delete file space**.

Changing the Path of File Spaces

Prerequisites:

1. Stop the VideoManager service from the services control panel on the PC running VideoManager.
2. Manually move the files to the new location, for example, by dragging and dropping the files into the new location on the PC.

Procedure:

1. Navigate to the **Admin** tab.
2. Select the **System** pane.
3. Click the **Storage** section.
4. Next to the file space whose path you want to change, click > **Go to file space**.
5. Click **Change**.
6. Enter the new path.
7. Click **Confirm**.

   NOTE: VideoManager will not save the changes if the data has not already been manually moved to the location specified in the new path.

Changing the Size of File Spaces

Changing the size of a file space can be necessary if more or less space has become available, or a space should be redistributed between file spaces.

Procedure:

1. Navigate to the **Admin** tab.
2. Select the **System** pane.
3. Click the **Storage** section.
4. Next to the file space whose size you want to change, click > **Go to file space**.
5. In the **Max size** field, make the relevant changes.

   NOTE: You cannot make the file space smaller than the size of the files which are already in the file space.

6. Click **Confirm**.

Deleting File Spaces

Deleting a file space involves evacuating all files in the file space to another suitable file space.

Procedure:

1. Ensure that there is at least one other file space on VideoManager whose **Category** matches that of the file space that is being deleted, and whose **State** is set to **Online**.
2. Next to the file space to be deleted, click > **Go to file space**.
3. From the **Category** drop-down list, select **Evacuate**.
4. Click **Confirm**.

   The data in the deleted file space is evacuated to the other file space(s). This process may take hours or days, depending on the amount of information in the file space.
5. Optional: After the evacuation has finished, to check that all of the files have been evacuated correctly, click **Evacuation report**.
6. Next to the now empty file space, click **Delete file space**.

   NOTE: File spaces should not be deleted until they have been evacuated. However, as a last resort, administrators can delete a file space whose status has been set to **OFFLINE**, if the files in the file space have been irretrievably lost.

9.7.3

Configuring File Space Warnings

You can configure file space warnings, which appear when file spaces reach a certain threshold. The warnings are useful because they ensure that administrators can take action before the file spaces are completely full.

Procedure:

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 and enter a percentage between 1 and 100% above which an alarm will be triggered.

   The options are as follows:

   - **Warn when footage storage is above threshold**
   - **Warn when export storage is above threshold**
   - **Warn when backup storage is above threshold**
5. Click **Save settings**.

   From now on, whenever the **Footage**, **Exports** or **Backups** file spaces grow larger than the specified percentage, a system warning appears in the **Notifications** pane on the administrator's homepage, and in the **System** pane of the **Status** tab.

9.7.4

Configuring Listen and Public Addresses of VideoManager

A public address determines how users, cameras, and docks access VideoManager on the network.

A listen address determines which connections VideoManager accepts from these users, cameras, and docks.

It is possible to assign different purposes to different public and listen addresses. For example, one listen address for cameras and one for users to access VideoManager via a browser.

It is important to configure a public address because otherwise users will only be able to access VideoManager on the PC where it is installed.

Configuring the Listen Address

By default, VideoManager will listen on port 9080 for all traffic. Before you add a new listen address, you should confirm that your organization's firewall settings will allow access before changing ports. Otherwise, your users, devices or sites may lose access to VideoManager.

Procedure:

1. Navigate to the **Admin** tab.
2. Select the **System** pane.
3. Click the **Web Server** section.
4. At the bottom of the **Listen Addresses** section, in the lower right-hand corner, click **New listen address**.
5. From the **Purpose** drop-down list, select all purposes of the new address.
6. Optional: If VideoManager should only listen on a certain address, specify this address in the **Server address** field.
7. In the **Server port** field, set the port that VideoManager will listen on.
8. Set **Use SSL?** to **On**.
9. Upload a valid SSL certificate by clicking **Configure**.

   The same SSL certificate can be used for multiple listen address configurations.
10. Click **Save settings**.

Configuring the Public Address

A public address is the address that web clients and devices use when not on the same network as the VideoManager instance. You must configure at least one public address.

Procedure:

1. Navigate to the **Admin** tab.
2. Select the **System** pane.
3. Click the **Web Server** section.
4. Scroll down to the **Public Addresses** section.
5. At the bottom of the section, in the lower right-hand corner, click **New public address**.
6. From the **Purpose** drop-down list, select all purposes of the new address.

7. In the **Public URL** field, enter the fully qualified public URL used to access the service.

   URL must include `http://` or `https://` at the beginning and the port number at the end, for example `9999`
8. Click **Save settings**.

9.7.5 Configuring SSL Certificates for Device Authentication

Procedure:

1. Navigate to the **Admin** tab.
2. Select the **System** pane.
3. Click the **Web Server** section.
4. In the **Listen Addresses** section, click **New listen address**.
5. From the **Purpose** drop-down list, select **Client certificate authenticated devices**.
6. Optional: In the **Server address** field, enter the server address.
7. In the **Server port** field, enter the server port.
8. Optional: Set **Use certificate forwarding?** to **On**.

   Enabling this option allows you to download certificate.
9. Ensure that **Use SSL?** is set to **On**.
10. In the **SSL certificate** field, click **Configure**.
11. Click **Choose File**.

    NOTE: Acceptable certificate formats are BASE64 and PEM.
12. Select the certificate and click **Open**.
13. Enter the password.
14. Click **OK**.
15. Click **Save settings**.

9.7.6 Using a Client Certificate Authentication for Login

It is possible to use a client certificate in order to log on to VideoManager. In order to do that, you need to configure a listen address with Client Certificate Authentication purposes, and a new authentication realm to upload the client certificate.

NOTE: The address that users use to access the login page must have the same hostname as the server address and must include `https`. You must ensure that the browser accepts the certificate and does not show any warnings.

Procedure:

1. Navigate to the **Admin** tab.
2. Select the **System** pane.
3. Click the **Web Server** section.

4. In the **Listen Addresses** section, click **New listen address**.
5. From the **Purpose** drop-down list, select **Client certificate authenticated users**.
6. Optional: In the **Server address** field, enter the server address.
7. In the **Server port** field, enter the server port.

   NOTE: The server port must be different for each one for the list of listen addresses.
8. Set **Use SSL?** to **On**.
9. In the **SSL certificate**, click **Configure**.
10. Click **Choose File**.

    The certificate format is usually .p12 or .pfx.
11. Select the certificate and click **Open**.
12. Enter the password.
13. Click **OK**.
14. Click **Save settings**.

    The server restarts.
15. Perform Creating Client Certificate Authentication Realm on page 153.

9.7.7

Creating and Configuring 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 media files, incidents, and exports. These backups can be used by Motorola Solutions to restore an administrator's instance of VideoManager.

The backup function only backs up the system state and does not back up the contents of the media, exports or reports filespaces.

NOTE: Backups should be regularly transferred to a secure location offsite.

Creating Backup Databases

You can initiate an immediate backup, which captures the state of VideoManager at the time when the immediate backup was created.

NOTE: Only users with the **Initiate immediate database backup** permission can initiate the backup of the database.

Procedure:

1. Navigate to the **Admin** tab.
2. Select the **System** pane.
3. Click the **Backup Databases** section.
4. Click **Backup now**.

   The backup is sent to the location that has been configured in the **Storage** section. For more information, see Performing File Spaces Actions on page 278.

Configuring Backup Databases

You can configure recurring backups, which run automatically every hour.

Procedure:

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 action enables you to configure more settings relating to automatic backups.
5. Enter the number of most recent daily and hourly backups that should 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. Optional: If you want backups to only occur when there is little or no activity occurring on VideoManager, in order to minimise system load, set **Avoid busy times** to **On**.
7. Click **Save settings**.

   The backup is sent to the location that has been configured in the **Storage** section. For more information, see Performing File Spaces Actions on page 278.

   The current backup status, as well as the start and end date of the backup, are displayed at the bottom of the pane.

9.7.8

Importing and Deleting Licences

The **Licences** pane enables you to licence features of VideoManager, which would otherwise be inaccessible. It also allows you to view the licences you have already bought, the expiry dates of the licences, and the number of VB-series cameras and VT-series cameras which your licences support.

Importing Licences

Procedure:

1. Navigate to the **Admin** tab.
2. Select the **System** pane.
3. Click the **Licences** section.
4. Click **Import licence**.
5. Click **Choose File**.

   NOTE:
   You should select the licence provided to you by Motorola Solutions. For more information, contact Motorola Solutions Support.

   The maximum size of the licence can be 1 MB.
6. In the **Activation key** field, enter the key provided by Motorola Solutions in the licence email.

   NOTE: 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 appears as `Valid`. All licences are on and enabled by default once imported.

Deleting Licences

An imported licence usually has an expiry date. A warning will appear on VideoManager when a licence is one week away from expiration. When the licence expires, VideoManager restarts. It can be necessary to delete a licence after it expired.

Procedure:

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 presents a list of all the features which will stop working when the licence is deleted.
5. Click **Tick to confirm**.
6. Click **Yes**.

   NOTE: If the licence was still valid at the time of deletion, all VideoManager features associated with it immediately stop working.

9.7.9
Advanced Settings Configuration

The advanced settings file allows you to configure specialised features, for a demonstration or tutorials. All edits to the file can be done from the **Advanced Settings** section of the **System** pane, in the **Admin** tab.

NOTE: The configuration should only be done if you have been given explicit permission from Motorola Solutions Support, and should not be attempted otherwise.

9.7.10
Setting the System Time Zone of VideoManager

For on-premises instances, by default, the **System Time Zone** is the time zone of the operating system on which users are accessing VideoManager. For cloud instances, by default, **System Time Zone** is the time zone of the server on which VideoManager is being hosted.

The system time zone of VideoManager affects a number of functions, including:

- The start and end times for reports.
- When scheduled reports run.
- The interpretation of bandwidth rules, which apply to specific times or days.

The system time zone of VideoManager does not necessarily dictate video metadata, which is determined by the time zone of the camera on which the video was recorded, which is itself determined by the following:

- The time zone of the device profile.

  For more information, see Device Profiles on page 344.
- If the time zone of the device profile is left as the default, the time zone of a video is determined by the time zone of the dock to which the camera is docked.

For more information, see Performing Dock Actions on page 119.

- If the time zone of the dock is left as the default, the time zone of a video is determined by the system time zone of VideoManager.

NOTE: The system time zone can be changed to be independent of the host server time zone by users with the permission to edit **System time zone**.

Procedure:

1. Navigate to the **Admin** tab.
2. Select the **System** pane.
3. Click the **System Time Zone** section.
4. From the **Time Zone** drop-down list, select the system time zone of VideoManager.
5. Click **Save settings**.

9.7.11

Exporting and Importing the Configuration of VideoManager

Exporting or importing the configuration of VideoManager can be necessary if, for example, VideoManager has been configured on a test server, and the results should be imported into a live, working version.

Exporting a System Configuration

Procedure:

1. Navigate to the **Admin** tab.
2. Select the **System** pane.
3. Click the **Import/Export System Config** section.
4. Optional: From the **Replace this configuration on target system** drop-down list, select which policies should be added to the system configuration file. To add a set of information to the exported configuration, click **+**.

   NOTE: Imported policies overwrite previously existing policies on VideoManager.

   The options are as follows:

   - By clicking **Password complexity**, the password complexity policy is exported.
   - By clicking **Deletion policy**, the deletion policy is exported.
5. Optional: From the **Merge this configuration with target system** drop-down list, select which roles, fields, and profiles should be added to the system configuration file. To add a set of information to the exported configuration, click **+**.

   NOTE: 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.

   The options are as follows:

   - By clicking **Shareable device keys**, the access control keys are exported.
   - By clicking **Roles**, roles are exported.
   - By clicking **Import profiles**, import profiles are exported.

- By clicking **Export profiles**, export profiles are exported.
- By clicking **User defined fields**, user-defined incident fields, user-defined media fields, user-defined playback reason fields, and user-defined share reason fields are exported.
- By clicking **Device profiles**, device profiles are exported.
- By clicking **Network profiles**, network profiles are exported.

6. Click **Save settings**.
7. Click **Export system config**.

   The exported configuration is downloaded to the default download location of your PC.

Importing a System Configuration

Procedure:

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 and click **Confirm**.

9.8
Viewing Legal Information

You can view information about VideoManager related to legality and the terms of service.

Procedure:

1. Navigate to the **Admin** tab.
2. Select the **Legal** pane.
3. Click **About**.

   You can view the following fields:

   - **Product name** is the name of the system.
   - **Product version** is the version number of the system.
   - **Copyright notice** describes who has copyrighted the system, and for how long.
   - **View licence agreement** – By clicking **View**, you can check the licence agreement, which will have already been agreed to when initially logging on to the system.

9.9
Creating a System Health Check

Normally, the IT department is able to monitor computers and ensure that they are working properly. However, in some deployment scenarios, it can 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, for example, check that the disk RAID array is working correctly, and if not, provide a suitable error message to show to the user.

Procedure:

1. Navigate to the `config` folder of VideoManager.

   By default, the folder is in the path `C:\ProgramData\Motorola Solutions\VideoManager`.

   NOTE: If ProgramData is not visible, you should navigate to the **View** tab at the top of the pane, and select the **Hidden Items** check box.

2. In the `config` folder, create a file called `health-check.bat`.

   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
   ```

3. Save the file, and from the **Server Controls** section, restart VideoManager.
4. Perform one of the following actions:

Option	Actions

Configuring when the health check is run automatically	a. Navigate to the **Admin** tab.
	b. Select the **System** pane.
	c. Click the **Advanced Settings File** section.
	d. In the file, enter the following:
	`health.check.period.secs=number of seconds`
	This action sets the period between health checks while healthy to the number of seconds specified.
	`health.check.error.period.secs=number of seconds`
	This action sets the period between health checks while in an error state to the number of seconds specified.
	NOTE: The default time period for a reccurring healthy system check is an hour. The default time period for a reoccurring error system check is three minutes.

Running the health check manually	a. Navigate to the **Admin** tab. b. Select the **System** pane. c. Click the **Web Server** section. d. Click **Run Health Check**.

Chapter 10

Account Profile

In the **Account Profile** pane, you can edit aspects of your VideoManager profile.

To access your account profile:

1. In the top right-hand corner of the screen, click the user icon.
2. From the drop-down list, select **Account Profile**.

From the **Account Profile** pane, you can:

- Edit your display name by entering the new display name in the **Display name** field, and clicking **Save Changes**.
- Update your password by entering your current password in the **Update password** pane, and then entering the new password. You must click **Save new password** to save.
- Create, edit, and delete user-specific WiFi networks, which is necessary if you want to stream media over a personal hotspot.
  For more information, see Creating User-Specific WiFi Networks on page 295.
- View two factor authentication settings.
  For more information, see Multi-Step Processes on page 292.

Chapter 11

Multi-Step Processes

Some processes on VideoManager span multiple sections of the user interface (UI), which is why they are compiled here.

11.1 Configuring Streaming

Cameras can be configured to send a live stream to VideoManager while recording. Administrators can then watch the live stream in real time.

NOTE: If the administrator has trouble configuring streaming, they should see FAQ on page 310.

Process:

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 Configuring Firewalls on page 293.
2. Configure the public address of VideoManager.

   For more information, see Configuring the Public Address of VideoManager on page 294.
3. If the user will be live streaming over a personal hotspot, create a user-specific WiFi network.

   For more information, see Creating User-Specific WiFi Networks on page 295.
4. Create a network profile that can be used for streaming.

   For more information, see Performing Network Profile Actions on page 178.
5. Assign the camera to a user, and begin streaming media.

   For more information, see Assigning Cameras for Streaming on page 296.
6. View the live stream.

   For more information, see Viewing Live Streams on page 297.

11.1.1

Configuring Firewalls

Sometimes, cameras cannot stream to VideoManager without prior firewall configuration. The firewall configuration can be necessary if the user has either changed the default port of VideoManager, or has connected VideoManager to a public network.

Procedure:

Perform one of the following actions:

If...	Then...
If the user has changed the default web server port of VideoManager,	create a new inbound rule by performing the following actions: **a.** In the Windows menu, navigate to **Control Panel**. **b.** Select **System and Security**. **c.** Click **Windows Defender Firewall**. **d.** In the left-hand menu pane, click **Advanced Settings**. **e.** In the left-hand menu pane, select **Inbound Rules**. **f.** In the right-hand menu pane, click **New Rule...** **g.** Set the rule type to **Port**, and click **Next**. **h.** In the **Specific local ports** field, enter the port of VideoManager, and click **Next**. The port can be found on VideoManager, in the **Web Server** section of the **System** pane, in the **Admin** tab. **i.** Ensure that **Allow the connection** is selected, and click **Next**. **j.** Check the relevant profiles for this rule. If in doubt, leave all selected, and click **Next**. **k.** Enter a name for the rule and click **Finish**. **NOTE:** If the user has other firewalls or NAT routers in the network between VideoManager and the WiFi network to which cameras will connect, they must also be configured to allow TCP connections between the camera and the VideoManager server.

If...	Then...
If the user has connected VideoManager to a public network,	perform the following actions: **a.** In the Windows menu, navigate to **Control Panel**. **b.** Select **System and Security**. **c.** Click **Windows Defender Firewall**. **d.** In the left-hand menu pane, click **Advanced Settings**. **e.** In the left-hand menu pane, select **Inbound Rules**, and scroll down until the **VideoManager Web** rule is visible. **f.** Double-click the rule and in the **Advanced** section, ensure that **Public** is selected. **g.** Click **OK**.

11.1.2

Configuring the Public Address of VideoManager

A camera connects to VideoManager by using the public address of VideoManager. If the cameras are connecting to the same IP network as VideoManager, users can utilise the same IP address as the VideoManager machine.

Procedure:

1. Navigate to the **Admin** tab.
2. Select the **System** pane.
3. Click the **Web Server** section.
4. Scroll down to the **Public Addresses** section.
5. At the bottom of the section, in the lower right-hand corner, click **New public address**.
6. From the **Purpose** drop-down list, select all purposes of the new address.
7. In the **Public URL** field, enter the fully qualified public URL used to access the service.

   URL must include `http://` or `https://` at the beginning and the port number at the end, for example `9999`
8. Click **Save settings**.

11.1.3

Creating User-Specific WiFi Networks

It is possible for users to create user-specific WiFi networks that only appear on their profile and cannot be viewed by other users on the system. The networks can be added to network profiles later, but they will still be kept private. This action is useful if the user has created a mobile phone hotspot for streaming.

Procedure:

1. Perform one of the following actions:

If...	Then...
If you are configuring a user-specific WiFi network for another user,	perform the following actions: a. Navigate to the **Admin** tab. b. Select the **People** pane. c. Click the **Users** section. d. Next to the user to be edited, click **Go to user**.
If you are creating the user-specific WiFi network for yourself,	perform the following actions: a. In the top right-hand corner of VideoManager, click the icon. b. From the drop-down list, select **Account Profile**.

2. In the **WiFi networks** pane, click **Add network**.
3. In the **Network name (SSID)** field, enter the name of the WiFi network or hotspot.

   NOTE: The name cannot be changed later.
4. From the **Security type** drop-down list, select which security configuration the user-specific WiFi network should use.
5. In the **Passphrase** field, enter the passphrase of the WiFi network or hotspot.
6. From the **Band** drop-down list, select which frequencies the cameras should attempt to connect to.

   The options are as follows:

   - **Any** – This option is suitable for all cameras.
   - **2.4GHz only** – This option is suitable for all cameras.
   - **5GHz only** – This option is only suitable for VB400s.
7. If **Use static IP** is set to **Yes**, enter the corresponding static IP details.
8. If you want cameras to disconnect from the network if the signal is weak, set **Disconnect on low signal** to **On**.

   You can define the "weak" signal as a percentage, and the time in seconds that the camera must be connected to the specified signal level, after which the camera will disconnect.
9. If you want to enable cameras to connect to hidden networks, set **Hidden network** to **On**.
10. To save the network, click **Add**.

11.1.4

Assigning Cameras for Streaming

Users can now operate a camera and live stream the media back to VideoManager.

To assign a VB400 to a user through single issue and RFID, the user should tap their RFID card against the RFID reader associated with VideoManager. In the pool, LEDs of a VB400 will light up and the camera will emit a beep. The user can undock and operate this camera.

Perform the following procedure to assign a VB400 to a user through **Single issue**, **Permanent issue**, or **Permanent allocation**.

Procedure:

1. Navigate to the **Devices** tab.
2. Select the **Search Devices** pane.
3. Filter the cameras as necessary, and click **Find devices**.

   For more information, see Searching Cameras on page 107.
4. Next to the relevant camera, click **Assign Device**.

   NOTE: The camera must be connected to VideoManager and unassigned. To unassign a camera, you must click **Return Device**.

   The **Assign Device** dialogue opens.
5. In the **Operator name** field, enter the name of the user who should be recording with this camera.

   This must be a valid username on VideoManager. For more information, see Performing Roles Actions on page 149.
6. Select which **Assignment mode** the camera should use.
   - **Single issue** – The camera is assigned to a user and when it is redocked, it becomes unassigned and must be reassigned manually.
   - **Permanent issue** – The camera is assigned to the user and when it is redocked, it stays assigned to the same user.
   - **Permanent allocation** – The camera is allocated to a user, who must then tap an RFID card before they can use it in the field. When it is redocked, it stays allocated to the same user.

     If you choose **Permanent allocation**, the user will not be able to select the relevant device profile and network profile. However, the default VideoManager device profile is suitable for streaming, and the network profile should have already been set as the default.

     If the network profile has not already been set as the default, you can navigate to the **Admin** tab, select the **Connectivity** pane, click the **Network Profiles** section, click **Go to profile** next to the newly created network profile, and set **Default profile** to **On**.

   For more information, see Devices Assignment and Media Recording on page 100.
7. If you have chosen either **Single issue** or **Permanent issue**, perform the following actions:
   a. From the **Device profile** drop-down list, select the default device profile.
   b. From the **Network profile** drop-down list, select the previously created network profile.
   c. Click **Assign Device**.

   When the status of the camera changes to `Ready`, the device can be undocked and a user can start streaming from their camera.

11.1.5
Viewing Live Streams

After a camera has been assigned to a user and has a network profile that allows streaming, the user can begin recording and view the live stream that is created at the same time. Live streams are only broadcasted while the camera is recording.

Procedure:

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

   Next to the streaming camera, there should be two alerts. One alert should say `Rec` and the other should say `Live`.

2. Click **View live**.

   You are taken to a page where you can view the live stream.

   NOTE: Only users with the permission to view cameras live can see live streams. However, even with this permission, they can only see live streams from cameras they have permission to view, which could be cameras they own, cameras they supervise, or all cameras.

   When a live stream stops, the screen goes blue and there is a message reading `Device not streaming`.

11.2
Configuring 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.

NOTE: It is highly recommended that these computers are running the same version of VideoManager. Otherwise, there may be problems with syncing the configuration. If the versions of VideoManager are not the same, the computer with the more recent version must act as the Central VideoManager. You should check the release notes to see which versions of VideoManager are compatible.

Process:

1. Enable and configure Central VideoManager.

   For more information, see Enabling and Configuring the Central VideoManager on page 298.

2. Configure how media on sites is treated, that is whether it is automatically uploaded to the Central VideoManager or not.

   For more information, see Configuring Metadata/Footage Replication on page 298.

3. Configure how other information on sites is treated, that is whether it is automatically replicated from the Central VideoManager to the sites or not.

   For more information, see Enabling Configuration Replication on page 299.

   After the Central VideoManager has been configured, you can connect sites to it. The steps for configuring a site differ, depending on the type of a site to be used.

4. Perform one of the following actions:

Option	Actions
Connecting another instance of VideoManager to the Central VideoManager	a. Create site profiles from the Central VideoManager. These profiles map the sites onto the Central VideoManager. For more information, see Creating Sites on the Central VideoManager on page 300. b. Enable and configure sites. For more information, see Enabling and Configuring Sites on page 302.
Connecting an EdgeController to the Central VideoManager	a. Enable and configure sites. For more information, see Configuring EdgeControllers on page 302. After an EdgeController has been configured to act as a site, it can be administered over WiFi. For more information, see Performing EdgeController Platform Change Requests on page 306.

Postrequisites: Some configurations require a Three-tier site setup. Motorola Solutions should be contacted first.
For more information, see Configuring Three-Tier Sites on page 306.

11.2.1
Enabling and Configuring the Central VideoManager

The Central VideoManager acts as a "hub", to which other sites can connect.

Procedure:

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
Configuring Metadata/Footage Replication

It is possible to automatically upload media files 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. 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 media files with a Central VideoManager because otherwise, every media file would have to be manually submitted or committed from the site or Central VideoManager, respectively.

Procedure:

1. Navigate to the **Admin** tab.
2. Select the **Connectivity** pane.
3. Click the **Metadata/Footage Replication** section.
4. Configure any of the following criteria:
   - **Metadata/Footage Replication** – These settings control whether media is automatically uploaded from a site to a Central VideoManager.
     - If **Auto-fetch media and audit metadata** is set to **On**, all metadata for site media is transferred to the Central VideoManager and is displayed in the the Central VideoManager.
     - From the **Auto-fetch footage** drop-down list, select how media is uploaded from a site to a Central VideoManager. The options are as follows:
       - **Don't auto-upload footage** – No media from a site is uploaded automatically. This option is useful if the user's Central VideoManager does not have a lot of storage.
       - **Auto-upload incident footage** – Only media that is part of an incident is uploaded automatically, which includes the entire media file if the media has been clipped for the incident, as soon as the incident has been created.
       - **Auto-upload footage from committed incidents** – Only media that is part of an incident that has been manually taken control of is uploaded automatically.
         For more information, see Committing Incidents on page 89.
       - **Auto-upload all footage** – All media on the site is uploaded automatically, regardless of whether it is in an incident or not. This option is only recommended if the user's Central VideoManager has a lot of storage.
         For more information, see Creating Sites on the Central VideoManager on page 300.
   - **Media distribution monitor settings** – These settings control how media is uploaded from sites to the Central VideoManager.
     - If **Congestion warning** is set to **On**, VideoManager displays a warning if a media file 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 is shown, can be configured after it has been set to **On**.
     - If **Auto-Cancel** is set to **On**, VideoManager automatically cancels 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 is canceled, can be configured after it has been set to **On**.
5. Click **Save settings**.

11.2.3
Enabling 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. The **Configuration Replication** section is only visible from a Central VideoManager. If VideoManager is configured as a site, it is not visible.

Users can share the configuration of a Central VideoManager with all of its connected sites because it allows 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.

Procedure:

1. Navigate to the **Admin** tab.
2. Select the **Connectivity** pane.
3. Click the **Configuration Replication** section.
4. Configure any of the following criteria.
   - If **Keys** is set to **On**, the Central VideoManager shares access control keys with its sites, enabling cameras assigned at one site to be docked at any other, if necessary.
     This option also replicates the filesigning configuration of VideoManager, including certificate authorities, which means that all media files that can be verified by the Central VideoManager can also be verified at the sites.

     NOTE: For security reasons, the private key is not replicated to sites.
   - If **Roles & password rules** is set to **On**, the Central VideoManager shares 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 are shared across sites, which means that if a user can log on to a Central VideoManager, they can also log on to the corresponding site.

     NOTE: It is best practice to share both **Roles & password rules** and **Users**, or neither.
   - If **Device profiles** is set to **On**, the Central VideoManager shares device profiles with its sites.
   - If **Deletion policies** is set to **On**, the Central VideoManager shares its deletion policy with its sites.
   - If **User-defined Fields** is set to **On**, the Central VideoManager shares user-defined incident fields with its sites.
   - If **Firmware and upgrade policy** is set to **On**, the Central VideoManager synchronises 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 are synchronised with the Central VideoManager clock.

   NOTE: Users with sufficient permissions can still make changes to these settings on their site, such as changing the default device profile. However, as soon as the relevant setting is changed in the Central VideoManager, any changes made on the site are overwritten.
5. Click **Save settings**.

11.2.4
Creating Sites on the Central VideoManager

Administrators should create site profiles from the Central VideoManager before connecting any sites. This action is only necessary if the sites are instances of VideoManager, not EdgeControllers.

Site profiles map the sites themselves onto the Central VideoManager.

Procedure:

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 Enabling and Configuring the Central VideoManager on page 298.

3. Click **Create site**.
4. In the **Name** field, enter the display name for the site.

   The display name helps administrators differentiate between different sites, and can be changed later.
5. In the **Identifier** field, enter a unique name for the site.

   NOTE: The identifier cannot be changed later.
   You should make a note of the **Identifier** because it will be needed for authentication when connecting the sites to the Central VideoManager.
6. In the **Password** field, enter a password for the site.

   NOTE: You should make a note of the password because it will be needed for authentication when connecting the sites to the Central VideoManager.
7. From the **State** drop-down list, select the state of the site.

   The options are as follows:

   - **Enabled** – If a site is enabled, it functions as normal. It can be configured from the Central VideoManager and automatically uploads media and incidents.
   - **Disabled** – If a site is disabled, it does not transfer media and incidents to the Central VideoManager. Any settings that have been configured from the Central VideoManager's **Metadata/Footage Replication** and **Configuration Replication** panes will not apply until the state for the site has been changed to **Enabled**.

     NOTE: A site whose state is 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 expire.
8. From the **Auto-fetch footage** drop-down list, select what should happen to media 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** – Media is not automatically sent from the site to the Central VideoManager.
   - **Auto-upload incident footage** – Media is only automatically sent to the Central VideoManager if it is part of an incident.
   - **Auto-upload all footage** – All media is automatically sent to the Central VideoManager, regardless of whether it is part of an incident or not.
   - **Default** *<0>* – This option is the default auto-fetch setting, as configured from the **Configuration Replication** section.

     For more information, see Enabling Configuration Replication on page 299.
   - **Auto-upload footage from committed incidents** – Media is only automatically sent to the Central VideoManager if it is part of an incident that has been committed, that is pulled from the site to the Central VideoManager.
9. From the **Bandwidth rule** drop-down list, select which previously created bandwidth rule should apply to the site. If no bandwidth rules have been created, select **No Restriction**.

   Bandwidth rules dictate when media is uploaded from sites to the Central VideoManager, and also how much is uploaded at once. A lower bandwidth means that media and metadata are transferred more slowly, but are also less disruptive to other users on the system.

   For more information, see Performing Bandwidth Rules Actions on page 184.

10. Click **Create site**.

    NOTE: This procedure should be repeated for every instance of VideoManager that will become a site.

11.2.5 Enabling and Configuring Sites

After site profiles have been created from the Central VideoManager, the administrator must convert the relevant instances of VideoManager into sites.

Procedure:

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 information can be found on the Central VideoManager, in the **Web Server** section of the **System** pane, in the **Admin** tab.
6. Enter the identifier and password of this site, which should have already been created from the Central VideoManager.

   For more information, see Creating Sites on the Central VideoManager on page 300.
7. Click **Save settings**.

   If successful, the site should appear in the **Sites** tab of the Central VideoManager.

11.2.6 Configuring 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. The configuration file should be generated from the Central VideoManager.

Prerequisites: Ensure that the EdgeController is connected to mains power.
You can connect it by performing the following actions:

1. Unpackage the power supply of the EdgeController.
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 by using the button on the top of the device.

After the EdgeController has been connected to mains power, its configuration file can be generated on VideoManager and delivered via USB.

Procedure:

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.

   The serial number can be found on the front right-hand corner of the EdgeController.
5. Set **Use static IP** to **On**.

   NOTE: This action is only necessary if an EdgeController cannot get its networking configuration by DHCP.
6. Set **Set WiFi config** to **On**.

   NOTE: It is recommended that EdgeControllers are connected to networks over ethernet. The **Set WiFi config** option is useful if the user's EdgeController will be connecting to VideoManager via WiFi. Users should enter the SSID and passphrase of the WiFi network.
7. To create the file, click **Download config**.

   The file is downloaded to the default downloads location of your PC.
8. Plug the USB drive into the same PC.

   NOTE: 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 USB ports of the EdgeController.

    If successful, the site should appear in the **Sites** tab of the Central VideoManager.

11.2.6.1
Editing the Network Configuration of EdgeControllers

Occasionally, it can 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.

Procedure:

1. On the Central VideoManager, navigate to the **Status** tab.
2. Select the **Sites** pane.
3. Next to the relevant EdgeController, click **> View site**.

4. Perform one of the following actions:

If...	Then...
If the EdgeController is online,	perform the following actions: a. Click **Edit Network Config**. b. Optional: If you want to configure whether the EdgeController should have a static IP address or not, set **Change wired network configuration** to **On**. c. Optional: Set **Change WiFi Configuration** to **On** and configure any of the following settings. • If **Set WiFi config** is set to **On**, you can change the details of the WiFi network to which the EdgeController is connected. **NOTE:** If the details entered here are incorrect, and the EdgeController is connected to the Central VideoManager over WiFi, instead of Ethernet, the EdgeController goes offline and must be reconfigured via USB. • If **Clear WiFi configuration** is set to **On**, the WiFi configuration of the EdgeController is cleared. **NOTE:** This setting should only be set to **On** if the administrator is transferring their EdgeController from a WiFi network to an Ethernet connection. d. Click **Apply Immediately**.

If...	Then...
If the EdgeController is offline,	perform the following actions: **a.** Click **Generate Offline Network Config**. **b.** Optional: If you want to configure whether the EdgeController should have a static IP address or not, set **Change wired network configuration** to **On**. **c.** Optional: Set **Change WiFi Configuration** to **On** and configure any of the following settings. • If **Set WiFi config** is set to **On**, you can change the details of the WiFi network to which the EdgeController is connected. **NOTE:** If the details entered here are incorrect, and the EdgeController is connected to the Central VideoManager over WiFi, instead of Ethernet, the EdgeController goes offline and must be reconfigured via USB. • If **Clear WiFi configuration** is set to **On**, the WiFi configuration of the EdgeController is cleared. **NOTE:** This setting should only be set to **On** if the administrator is transferring their EdgeController from a WiFi network to an Ethernet connection. **d.** Click **Download config**. The file is downloaded to the default downloads location of your PC. **e.** Plug the USB drive into the same PC. **NOTE:** The USB drive must have FAT32 format. **f.** Drag and drop the EdgeController configuration file into the root folder of the USB drive. **g.** Safely eject the USB drive. **h.** Plug the USB drive into one of the USB ports of the EdgeController.

11.2.6.2

Performing EdgeController Platform Change Requests

Occasionally, it can be necessary to upload a configuration file directly from the UI of the EdgeController, if instructed to do so by Motorola Solutions.

Procedure:

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**.
   You are taken to the UI of the EdgeController.
4. On the UI of the EdgeController, 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 you have 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

Configuring Three-Tier Sites

Administrators can create a three-tier site setup that is structured like a pyramid with:

- 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.

Prerequisites: Ensure that you 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.

Process:

1. Configure the VideoManager Mid-tier like a normal Central VideoManager.
   For more information, see Enabling and Configuring the Central VideoManager on page 298.
2. Configure the sites and add them to the Central VideoManager Mid-tier.
   For more information, see Creating Sites on the Central VideoManager on page 300 and Enabling and Configuring Sites on page 302.
3. Configure the top tier Central VideoManager like a normal Central VideoManager.
   For more information, see Enabling and Configuring the Central VideoManager on page 298.
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 Enabling and Configuring Sites on page 302.

   NOTE: A normal Central VideoManager cannot connect to another Central VideoManager, which 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 Configuring Privilege Escalation

Privilege escalation is the mechanism by which administrators can ensure that there is an extra step of responsibility before important actions, such as incident deletion, are taken on VideoManager.

Process:

1. Configure global settings related to privilege escalation.

   For more information, see Configuring Privilege Escalation for VideoManager on page 307.
2. Configure privilege escalation on a role-by-role basis.

   For more information, see Configuring Privilege Escalation for Roles on page 307.
3. Use privilege escalation.

   For more information, see Using Privilege Escalation on page 308.

11.3.1 Configuring 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.

Procedure:

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. Optional: If you want users to re-enter their password before they can escalate their privileges, set **Requires re-authentication** to **On**.

   If set to **Off**, users do not need to re-enter their password when escalating their privileges.
6. Optional: If you want users to be automatically returned to their non-escalated role after the specified number of minutes has elapsed, set **Timeout** to **On**.

   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 Configuring Privilege Escalation for Roles

After privilege escalation has been configured for the entirety of VideoManager, it can be configured on a per-role basis.

Procedure:

1. Navigate to the **Admin** tab.

2. Select the **People** pane.
3. Click the **Roles** section.
4. Perform one of the following actions:
   - If you want to create a new role, click **Create role**.
   - If you want to edit an already existing role, next to the relevant role, click **Go to role**.
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 Using Privilege Escalation on page 308.

   NOTE: If there are any users that only belong to this role, they are unable to perform any actions on VideoManager until they have elevated their privileges.
6. Click **Save role**.

   For any users who inhabit this role, the change comes into effect the next time they log on.

11.3.3
Using Privilege Escalation

After privilege escalation has been configured, users can escalate their privileges on VideoManager when they want to perform an action, which would usually be unavailable to them.

Procedure:

1. In the top right-hand corner of VideoManager, click the icon.
2. Click **Elevate Privilege**.

   The roles available to the user appear as a list. The user should choose the relevant role from the list.

   NOTE: If **Elevate Privilege** is not available, the user does not inhabit a role that requires privilege escalation.

   If **Requires re-authentication** is set to **On**, the **Validate password** window opens.
3. In the **Validate password** window, re-enter your password and click **Validate**.

   The user's privileges are escalated. An orange banner appears in VideoManager, which revokes the user's privileges immediately, if clicked.

11.4
Configuring Peer-Assisted Recording with Cameras

This mode requires two or more VB400s. When one camera starts recording, any cameras in its vicinity are prompted to start recording as well.

This section is intended as a cursory insight into how administrators can configure Peer-Assisted Recording (PAR) for immediate use. For more in-depth information about possible configuration options, such as how to

use PAR with groups, you should navigate to the Motorola Solutions Learning Experience Portal (registration is free) and search for *Peer-Assisted Recording Explained*.

Procedure:

1. Ensure that there are at least two users who have a role with the **Operate device** permission enabled by performing the following actions:
   a. Navigate to the **Admin** tab, select the **People** pane, and click the **Roles** section.
   b. Next to the relevant role, click **Go to role** and set **Operate device** to **On**.
   c. Navigate to the **Admin** tab, select the **People** pane, and click the **Users** section.
   d. Next to the relevant user, click **Go to user** and set the relevant role to **On**.
2. Ensure that there is a device profile on VideoManager that has **Peer-Assisted recording** set to **On** by performing the following actions:
   a. Navigate to the **Admin** tab, select the **Devices** pane, and click the **Device Profiles** section.
   b. Next to the relevant device profile, click **Go to profile**.
   c. In the **Bluetooth Settings** section, set **Peer-Assisted recording** to **On**.
   d. Perform one of the following actions:
      - If you want the users to be able to enter the number of seconds after assignment, during which a VB400 does not prompt other VB400s to start recording, set **Suppress PAR after undocking** to **On**.
      - If you want to enable VB400 to prompt other VB400s to start recording as soon as it has been assigned and undocked, set **Suppress PAR after undocking** to **Off**.
3. Assign the VB400s to the users by performing the following actions:
   a. Navigate to the **Devices** tab.
   b. Next to the relevant VB400, click **Assign Device**.
   c. In the **Operator name** field, enter the name of the user who will operate the VB400.
   d. From the **Device profile** drop-down list, select the previously created device profile.
   e. Repeat step 3 for the other VB400.

   Whenever one VB400 starts recording in the vicinity of another, the other VB400 is prompted to start recording as well. However, it is not possible to stop multiple cameras recording with Bluetooth. Users must stop recording individually and manually.

Chapter 12

FAQ

The following sections list a series of frequently asked questions (FAQ) by users relating to VideoManager.

12.1 Media File FAQ

The following table lists a series of frequently asked questions (FAQ) by users relating to media files.

Question	Answer
After recording, how do I download media files from my camera to VideoManager?	To download media files from your camera, perform the following actions: 1. Either dock your camera or plug it in to your PC using a USB cable. 2. Navigate to the **Devices** tab. 3. Next to the relevant camera, click > **View device info**. 4. In the **Status** window, click the **Downloading** sign. The media file should now be available to view under the **Media** tab.
Why are some of the headings on my media files blue?	If a media file is part of an incident, the heading becomes blue instead of grey and has a star ★ next to the name. You can click the **This video is in** *<0>* **incident** button, which takes you to the incident(s) it is part of.
Can I share media files with people who are not on VideoManager?	If you need to share a media file with someone outside of VideoManager, you can share it as part of an incident by using a link via email. For more information, see Sharing Incidents Externally Using a Link on page 85. You can also download the media file straight to your PC. For more information, see Performing Media File Actions on page 47.
What is the difference between the operator and the owner of a media file?	The operator of a media file is the one who physically recorded it on their camera. The owner has full administrative control over the media file. Usually, it is the same person. However, if the media is too sensitive for more junior users to retain control of, it can be necessary to reallocate who the owner is.

Question	Answer
	For more information, see Sharing Media Files on page 50.
Why can I not see some of the media files on VideoManager?	There are two possible reasons: • Permissions – VideoManager gives administrators lots of control over what actions can be performed by other users on the site through roles. Roles affect how much privilege a user has on the site. It is possible that when you were creating your admin user after logging on for the first time, you did not assign it the privileges, which would allow you to see the media files filmed by yourself and others on the system. To fix this, perform the following actions: 1. Navigate to the **Admin** tab. 2. Select the **People** pane. 3. Click the **Roles** section. 4. Next to your role, click the **Go to role** button. 5. Scroll down to the **Media permissions** window. 6. Next to the relevant permissions, set each button to **On**. Permissions apply to either your media files, media files that have been shared with you, media files that have been recorded by people you supervise, or all media files on the system. • Deletion Policies – You can check the configuration of your deletion policy, in case it is configured to delete media almost immediately by performing the following actions: 1. Navigate to the **Admin** tab. 2. Select the **Policies** pane. 3. Click the **Deletion Policy** section. 4. Change the number of days that media is kept for after it has been recorded and downloaded.
Why do some of my media files have a cloud symbol instead of a thumbnail?	A cloud symbol indicates that a media file is not available on your instance of VideoManager because: • You are on a Central VideoManager and the media file is on the site. You must fetch the media file from the site before you can watch it.

Question	Answer
	For more information, see Bulk Editing Media Files on page 49. • You are on a site and the media file was fetched from the Central VideoManager, which means that you can no longer watch the media file on the site.
I accidentally deleted a media file. Can I undo this action?	You can reinstate a deleted media file, as long as your deletion policy has been configured to keep deleted media files for a short period of time after deletion and you are in a role which has the **Undelete** permission set to **On**. To reinstate a media file, perform the following actions: 1. Navigate to the **Media** tab. 2. Select the **Search Media** pane. 3. Select the **Include deleted media** check box. The deleted media file appears with a red heading. 4. Click **Reinstate media**. 5. Click **Yes**.

12.2
Incident FAQ

The following table lists a series of frequently asked questions (FAQ) by users relating to incidents.

Question	Answer
What is the difference between an export link and an incident link?	An export link downloads the media directly to the recipient's PC. An incident link only provides the recipient with browser-based access to the media, which is disabled after a set period of time. For more information, see Sharing Incidents Externally Using a Link on page 85.
Why are my incident headings different colours?	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 have not 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.

Question	Answer
	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 are coloured red.
Why can I not export an incident from VideoManager?	You cannot export an incident that does not contain any media. After media is added to an incident, you should be able to export it. You can still create incident links for incidents without media. For more information, see Sharing Incidents Externally Using a Link on page 85. Alternatively, you may not be able to export an incident if it does not meet the configured export profile rules. For more information, see Configuring Incident Exports on page 197.
I have accidentally deleted an incident. Can I undo this action?	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 the **Reinstate** permission set to **On**. To reinstate an incident, perform the following actions: 1. Navigate to the **Incidents** tab. 2. Select the **Search Incidents** pane. 3. Click **Show recently deleted incidents**. The deleted incident appears with a red heading. 4. Click **Reinstate incident**. 5. Click **Yes**.

12.3 Device FAQ

The following table lists a series of frequently asked questions (FAQ) by users relating to devices.

Question	Answer
Why is my VB300 not docking?	To restart your VB300, perform the following actions: 1. Hold the camera so that it is facing you.

Question	Answer
	2. Simultaneously press and hold the two plastic buttons on the top-left and bottom-right corners of the camera for 5 to 10 seconds. All the lights on the camera should come on and start flashing. 3. Release the two buttons. 4. After the lights have stopped flashing, try re-docking the camera again. If the procedure still does not work, leave the camera off its charging base until the battery is completely flat. This could take over 24 hours. After the battery is flat, try re-docking the camera. If neither of the procedures work, the camera must be returned to Motorola Solutions for servicing or repair. Perform the following actions: 1. Navigate to http://motorolasolutions.com/en_xu/support.html and from the drop-down list, select **Service Returns**. 2. Fill in the form by entering your company name, email address, telephone number, and return address details. **NOTE:** Leave the reseller name blank. 3. From the drop-down list under "part", select the correct camera model. 4. Enter the serial number of your faulty camera. 5. In the **Fault Description** box, describe the fault. **NOTE:** Leave the rest of the fields blank. 6. If you are returning more than one camera, click **Add line for each additional return** and fill out the form as detailed above. 7. Click **Create**.
Why is my VB100/VB200 not docking?	To restart your VB100 or VB200, perform the following actions: 1. Turn the camera upside down. 2. Pull the rubber charging cover upwards gently and rotate it to the side, so that you can see the charging/docking port. 3. To the right of the charging/docking port, there is a small plastic switch. Press the switch down for 5 to 10 seconds. Keep looking at the top of the camera. The green power light should first go out. Then,

Question	Answer
	it should glow orange and red, and the other lights on the top of the camera should glow green. This indicates that the camera is rebooting. 4. After the lights have stopped flashing, try re-docking the camera again. If the procedure above does not work, leave the camera off its charging base until the battery is completely flat. This could take over 24 hours. After the battery is flat, try re-docking the camera. If neither of the procedures work, the camera must be returned to Motorola Solutions for servicing or repair. Perform the following actions: 1. Navigate to http://motorolasolutions.com/en_xu/support.html and from the drop-down list, select **Service Returns**. 2. Fill in the form by entering your company name, email address, telephone number, and return address details. **NOTE:** Leave the reseller name blank. 3. From the drop-down list under "part", select the correct camera model. 4. Enter the serial number of your faulty camera. 5. In the **Fault Description** box, describe the fault. **NOTE:** Leave the rest of the fields blank. 6. If you are returning more than one camera, click **Add line for each additional return** and fill out the form as detailed above. 7. Click **Create**.
Can I move my cameras from one VideoManager system to another one?	Yes. Before starting the process, ensure that either: • All media on the camera has been downloaded to the instance of VideoManager it was originally associated with. After the camera has been factory reset, all media that was not downloaded is lost. • You have imported the access control key of the camera from the old instance of VideoManager to the new instance. For more information, see Creating, Importing, and Deleting Access Control Keys on page 169. If you have enabled file signing, you should export your certificate authority. If your certificate authority is not exported, media files recorded by the

Question	Answer
	moved cameras cannot be verified on the new instance of VideoManager. For more information, see Performing Device Certificate Authorities Actions on page 170. To move a camera from one instance of VideoManager to another, perform the following actions: 1. Undock your camera from the PC or dock associated with the old version of VideoManager. 2. Dock the camera to the PC or dock associated with the VideoManager it should be moved to. 3. Navigate to the **Devices** tab, and next to the relevant camera, click > **View device info**. If you have not imported the access control key of the camera, it appears as locked. You must click **Factory Reset this Device** to associate the camera with the new instance of VideoManager.
Why does my camera appear as "locked" on VideoManager?	Your camera appears as locked if it has been undocked from one instance of VideoManager and redocked at a different VideoManager that does not have its access control key, which means that all media on the camera is inaccessible. The camera is unlocked immediately if you export its access control key from the original VideoManager to the VideoManager, which the camera is connected to now.
My VB400 is broken. How do I prevent other operators on VideoManager from accidentally using it?	You can change the status of your VB400 to `Service Required`. This action removes the VB400 from the pool, that is it cannot be assigned or allocated, and the LEDs A, B, and C glow yellow. Perform the following actions: 1. Navigate to the **Devices** tab. 2. Select the **Search Devices** pane. 3. Filter the cameras as necessary, and click **Find devices**. 4. Next to the camera to be edited, click > **View device info**. 5. Click **Edit device properties**. 6. Set **Service required** to **Yes**. 7. Click **Save changes**. The VB400 is unusable until you set **Service required** to **No**.
Can I return broken cameras?	Yes. Motorola Solutions has a self-service portal that allows you to return your cameras. Perform the following actions:

Question	Answer
	1. Navigate to http://motorolasolutions.com/en_xu/support.html and from the drop-down list, select **Service Returns**. 2. Fill in the form by entering your company name, email address, telephone number, and return address details. **NOTE:** Leave the reseller name blank. 3. From the drop-down list under "part", select the correct camera model. 4. Enter the serial number of your faulty camera. 5. In the **Fault Description** box, describe the fault. **NOTE:** Leave the rest of the fields blank. 6. If you are returning more than one camera, click **Add line for each additional return** and fill out the form as detailed above. 7. Click **Create**.
What do the icons next to my cameras mean?	You can configure VideoManager so that it is only possible to assign a camera with **Single issue** and RFID if the battery is charged to a certain level. VideoManager displays icons next to your cameras depending on the charging status, and whether they have met the configured level. Potential icon combinations are as follows: • No icon – The camera is not connected to VideoManager. For example, because it is assigned and in the field (**In use**) or unassigned and in the field (**Unknown**). • – The camera is charging but has not met the minimum charge criteria for single-issue and RFID. • – The camera is charging and has met the minimum charge criteria for single-issue and RFID, but RFID assignment is disabled for this camera from the **Edit device properties** pane. • – The camera is charging, has met the minimum charge criteria for single-issue and RFID, and RFID assignment is enabled for this camera. It is ready to be assigned with single-issue and RFID.

Question	Answer
	• – The camera is fully charged, but RFID assignment is disabled for this camera from the **Edit device properties** pane. • – The camera is fully charged and RFID assignment is enabled for this camera. It is ready to be assigned with single-issue and RFID. • – The camera is not charging. Service can be required. You should check the audit log from the **Status** tab.

12.4
Admin FAQ

The following table lists a series of frequently asked questions (FAQ) by users relating to Admin actions.

Question	Answer
Can I change my username after I have created my user?	You cannot change your username after you have created and saved your user. You can, however, change your **Display name**, which is what other users see on VideoManager. You can do so from the **Users** section of the **People** pane, in the **Admin** tab. For more information, see Creating, Editing, and Deleting Users on page 138.
Can I change my password after I have created my user?	Yes. You can change your password from the **Users** section of the **People** pane, in the **Admin** tab. In the **Password** section, delete your outdated password and enter a new one. Re-enter it in the **Confirm password** field and click **Save user** to 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 drop-down list. 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**.
If I delete a user, what happens to their media?	If you delete a user, none of their media, exports, or incidents are deleted from VideoManager. You can reassign a user's media, exports, and incidents before or after they are deleted. This action transfers their data to another user.

Question	Answer
	If their data is not reassigned and the username is later reused for a new user, the data is reassigned to that user automatically, even if the username does not belong to the same worker anymore. For more information, see Reassigning Users on page 141.
How can I reset my password on VideoManager?	Motorola Solutions cannot change your password for you, unless your server is hosted by Motorola Solutions. Another administrator user must reset your password by performing the following actions: 1. Navigate to the **Admin** tab. 2. Select the **People** pane. 3. Click the **Users** section. 4. Next to the relevant user, click the **Go to user** button. The administrator can now change your password for you. 5. Click **Save user**. **NOTE:** If you are the only administrator on your system, you must contact Technical Support. Alternatively, if *Email Notifications* are licenced, you can have a password reset URL sent to you. For more information, see Enabling Users to Reset Their Own Passwords on page 159.
What are licences?	Motorola Solutions sells licences, which can be used to enable functionality in VideoManager that is not otherwise available. The licences include: • Composite clips licence allows users to create composite clips in an incident. Composite clips show all media files in an incident simultaneously. • Object storage licence enables users to create S3 cloud file containers. • ONStream licence allows users to connect VideoManager to their VMS if ONStream is enabled. • Text and Email notifications licence allows users to be given the opportunity to enter their email addresses and phone numbers. Users can configure when the notifications are sent from the **Roles** section of the **Admin** tab.

Question	Answer
Is there a way to set messages that all users on VideoManager can see?	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 can see on their home dashboard. For more information, see Creating, Editing, and Deleting Messages on page 264.
How can I view legal information of VideoManager?	Navigate to the **Admin** tab and click the **Legal** pane. Click **About** and select **View** to view the licence agreement of VideoManager.
Why does two factor authentication not work when I try to log on?	Two factor authentication codes are time-dependent. They expire after a certain period of time, and a new one is re-issued, which 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.
Can I move an EdgeController from one VideoManager system to another one?	Due to security risks, you cannot transfer an EdgeController after it has been associated with a specific VideoManager system. Contact Technical Support for more assistance and guidance.

12.5
Streaming FAQ

The following table lists a series of frequently asked questions (FAQ) by users relating to streaming.

Question	Answer
Why is my audio not working with my live stream?	Due to technical limitations, Internet Explorer does not support audio with live streams. You should use another browser, like Google Chrome.
Why is my camera not streaming?	There are a variety of reasons as to why your camera might not be sending a live stream back to VideoManager: • Ensure that you have the correct network profile selected. The network profile must have streaming enabled. • Try temporarily disabling the firewall on the machine running VideoManager. If it fixes the problem, you must turn the firewall back on and configure a firewall rule. For more information, see Configuring Firewalls on page 293. • Check whether the device profile of the camera enables it to connect to WiFi automatically. The camera may have been configured so you need to press a button before it connects to WiFi.

Question	Answer
	For more information, see Device Profiles on page 344. • The camera does not have the most recent firmware. Perform the following actions: 1. Ensure that the camera is docked. 2. Navigate to the **Devices** tab. 3. Next to the camera, click > **View device info**. 4. Click ⌃⌃ **Upgrade this Device**. 5. Select the newest firmware and click **Upgrade Device**.

12.6
General FAQ

The following table lists a series of general frequently asked questions (FAQ) by users.

Question	Answer
Why can I not log on to VideoManager?	Users can be unable to log on to VideoManager for a variety of reasons: • Your user is not enabled. To enable the user, an administrator must perform the following actions: 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. Set **Enabled** to **On**. 6. Save the user. • You have entered your credentials wrong. VideoManager is case-sensitive, which means that usernames and passwords must be entered exactly as they were configured. • Your user does not have the correct permissions to log on. An administrator must perform the following actions: 1. Navigate to the **Admin** tab. 2. Select the **People** pane.

Question	Answer
	3. Click the **Users** section. 4. Next to the relevant user, click **Go to 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, ensure that all of the login permissions are set to **On**. 9. Click **Save role**.
Why can I not see some aspects of the VideoManager user interface?	There are two possible reasons: • Permissions – VideoManager gives administrators lots of control over what actions can be performed by other users on the site through roles. Roles affect what aspects of the UI can be viewed and edited by a user. It is possible that when you were creating your administrator user after logging on for the first time, you did not assign it the correct privileges. Perform the following actions: 1. Log out of VideoManager. 2. Log back on as an administrator. 3. Navigate to the **Admin** tab. 4. Select the **People** pane. 5. Click the **Users** section. 6. Next to the relevant user, click **Go to user**. 7. Set **System Administrator** to **On**. You should now be able to see all media files and incidents in VideoManager, along with various other panes. • Licensing – Some aspects of VideoManager, such as ONStream, are only available to view if they have been licensed by your organisation. For more information, contact Motorola Solutions Sales.
Can I change the logos that users see on VideoManager?	Yes. Navigate to the **Admin** tab, select the **User Interface** pane, and click the **Theme Resources** section. Here, you can download logos of your company and use them instead.

Question	Answer
	For more information, see Changing Logos of VideoManager on page 266.
Can I change the colour scheme of VideoManager?	Yes. Navigate to the **Admin** tab, select the **User Interface** pane, and click the **Theme Resources** section. Here, you can change the colour scheme to match your own corporate branding. For more information, see Changing the Colour Scheme of VideoManager on page 267.
Can other users see the passwords of WiFi networks I added to VideoManager?	No.

Appendix A

Permissions

A role is a collection of permissions within VideoManager, which can 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 are available accordingly.

A.1 System Permissions

The **System permissions** pane offers control over logging on to the VideoManager, audit logs, and export abilities.

Login

Login permissions affect the manner in which users log on to VideoManager.

- **Login to VideoManager website** permission enables users to log on to the VideoManager web interface.
- **Login to VideoManager application** permission enables users to log on to the desktop VideoManager administrator application. They can use the same credentials as they would use to log on to VideoManager normally.
- **Access VideoManager website with single sign-on** permission enables users to authenticate into VideoManager through their desktop account. If enabled, single sign on is available to users.

Audit

Audit permissions control whether users can view audit information and download the system logs.

- **View auditing information** permission enables users to view audit logs of VideoManager from the **Status** tab. An audit log is a list of all actions taken on VideoManager.

  The permission does not apply to individual media file audit logs. The ability to view media file audit logs is dictated by the **View audit log** permission in the **Media permissions** section.

  For more information, see Media Permissions on page 325.
- **Download system logs** permission enables users to download the system logs from the dashboard.

  The permission is useful for troubleshooting. If necessary, the system logs can be sent to Motorola Solutions support, who can diagnose the problem.

Export

Export permissions control whether users can view, delete, and share exports, and view the audit log entries for exports. There are toggles accompanying each permission that 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** permission enables users to view and delete finished exports.

  If enabled, users have access to the **My Exports** pane, (in accordance with the **Owned** toggle), **Supervised Exports** pane (in accordance with the **Supervised** toggle), and **Manage Exports** pane (in accordance with the **Any** toggle), in the **Incidents** tab.
- **View audit log** permission enables users to view the audit log of all exports. These audit logs only encompass one incident each.

If enabled, users have access to the **View Export audit log** control when viewing their exports.

- **Externally share** permission enables users to share incidents externally, which 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 have access to the **Links** pane when viewing their exports.

A.2
Media Permissions

The **Media permissions** pane offers control over the various operations that can be performed on media files.

There are toggles accompanying some permissions that determine which media files the permissions apply to: **Owned** (media files created by the user), **Shared** (media files that have been shared with a user by other users on the system), **Supervised** (media files that have been created by other users on the system that the user supervises), and **Any** (any media files on the system, regardless of who created them).

Media

- **Access** permission controls which media files users can see on the **Media** tab.
- **List** permission controls whether users are presented with the **My Media**, **Shared Media**, and **Supervised Media** panes in the **Media** tab.

  The permission also controls whether users can see recently imported media files and downloaded media files on their homepage.
- **Access deleted** permission enables users to search for deleted media files, by selecting the **Include deleted media** check box in the **Search Media** pane.
- **Play** permission enables users to play previously recorded media files on VideoManager.
- **Delete** permission enables users to delete media files from VideoManager.

  Deleted media files are retained in line with the deletion policy of VideoManager. Even if users have the permission, they cannot delete media files that have been added to an incident.
- **Delete forever** permission enables users to permanently delete media, which immediately removes it from the system, irrespective of the deletion policy.

  The action is unrecoverable.

  To permanently delete a media file, the user should have the **List**, **Access**, and **Access deleted** permissions enabled. After they have filtered incidents with the **Include deleted media** box in the **Search Media** pane, deleted media appear with a red banner. The user can click **Delete media forever** to permanently delete the media.
- **Undelete** permission enables the user to reinstate previously deleted media, as long as it has been retained in line with the deletion policy.

  To undelete a media file, the user should have the **List**, **Access**, and **Access deleted** permissions enabled. After they have filtered incidents with the **Include deleted media** box in the **Search Media** pane, deleted media appear with a red banner. The user can click **Reinstate media** to permanently reinstate the media.
- **Add to incident** permission enables users to add media files directly to already created incidents.

  In order to use the permission, the following permissions are required: **Create incident from footage**, **Use single media as evidence**, **Use whole recording as evidence**, and **Add footage to existing incident**.
- **View audit log** permission enables users to view the audit log of a specific media file. Logged actions include adding a media file to, and removing a media file from, an incident.

The permission 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 324.

- **Download** permission enables users to download a media file from VideoManager straight to their PC.
  The only way users can share media files with people who are not on VideoManager is by downloading a media file using the **Download** permission and either putting it on a USB stick or emailing it to the relevant people.

  NOTE: After a media file has been downloaded to a PC, VideoManager has no control over it.

- **Edit share list** permission enables users to edit the **Sharing** pane, which dictates whether the media file is shared with other users on VideoManager.
- **View share list** permission enables users to view the **Sharing** pane, which shows whether the media file is shared with other users on VideoManager.
- **Change owner** permission enables users to change the owner of a media file, from the **Sharing** pane.
  The permission is useful if, for example, media files of an event were captured on multiple cameras but one user is creating and administering the incident.
- **Restrict** permission enables users to restrict a media file, which makes it unviewable to other users unless they have the **List restricted media** and **Play restricted media** permissions enabled.
- **Upload from site** permission enables users to upload media files from a site to a Central VideoManager, if their instance of VideoManager is configured to act as a site.
- **Set location** permission enables users to set location data for media files which do not already have location data associated with them.

  The action is only possible if users have already enabled maps, from the **Maps** section.
- **Edit location** permission enables users to overwrite location data for media files. They can only overwrite data that was set after the media file was recorded. They cannot overwrite data that was recorded alongside a media file.

  The action is only possible if users have already enabled maps, from the **Maps** section.
- **Edit device** permission enables users to change the recorded name of the camera that a media file was recorded on.

  The action can be done from the **Edit properties** pane.
- **Edit operator** permission enables users to change the recorded name of the user who recorded a media file.

  The action can be done from the **Edit properties** pane.
- **Edit timestamps** permission enables users to change the recorded time of a media file.

  The action can be done from the **Edit properties** pane.
- **Edit properties** permission enables users to edit the user-defined media fields for a media file once it has been downloaded.

  The action can be done from the **Edit properties** pane.
- **View scheduled deletion date** permission enables users to view the deletion date for their media file from its **Properties** pane, depending on the deletion policy.
- **View location** permission enables the user to view location recording information associated with a media file they are viewing.
- **Rotate/Flip** permission enables users to rotate and flip media files in the redaction editor.

- **Verify** permission enables users to compare a media file to the database of VideoManager, to ensure that it has not been corrupted.
- **Prepare media** permission enables users to prepare a media file in the same way that they would redact media in an incident.
  Unlike media, media files can be prepared even if they are not part of an incident.
- **Import media** permission enables users to import media files captured on cameras other than VB-series cameras or VT-series cameras into VideoManager.
- **Allow large uploads from site** permission enables users on a Central VideoManager to upload more than one hour of media from a site at a time.
  The upload applies to both multiple media files whose total length is more than one hour, and individual media files whose length is more than one hour.
- **Bulk-edit media** permission enables users to bulk edit multiple media files at once. Actions that can be performed on multiple media files include **Create incident** and **Delete**.
  The action is useful because it allows users to perform actions across many media files immediately.
- **Search by location** permission enables users to filter media by the location recording data attached to it.
  The action is only possible if users have already enabled maps, from the **Maps** section.
- **Search using advanced filter** permission enables users to filter media files with the custom predicate language.
  For more information, see Custom Predicate Language on page 380.
- **Search by scheduled deletion date** permission enables users to filter media files based on when they are set to be deleted by the deletion policy.
- **Control playback quality** permission enables users to change the quality of the media files they watch from the **Media** tab. The permission enables them to override the default quality set from the **Player** section of the **User Interface** pane, in the **Admin** tab.
- **Take screenshot** permission enables users to screenshot a media file while it is being viewed.
  The screenshot is downloaded directly to the user's PC.
- **List restricted media** permission enables users to view restricted media files in the **My Media**, **Shared Media**, or **Supervised Media** panes.
- **Play restricted media** permission enables users to play media files which have been restricted by other users.
- **Full control of restricted media** permission enables a user to treat a restricted media file exactly as they would an unrestricted one.
- **Display audit log of restricted media** permission enables users to view the audit log entries for restricted media files.
- **Download restricted media** permission enables users to download a restricted media file, utilising the **Download original file** control.
  For more information, see Performing Media File Actions on page 47.
- **Add restricted media to incidents** permission enables users to add restricted media files to an incident.
- **Search Media** permission enables users to search for specific media files from the **Search Media** pane of the **Media** tab.
- **Search By Shared Media Only** permission enables users to search for media files that have been shared either by them or with them, from the **Search Media** pane of the **Media** tab.

- **Search by bookmarked media only** permission enables users to search for media files that have been bookmarked, either in the field using a predetermined VB400 gesture, or on VideoManager after the media file was downloaded.

  Users with the permission have access to the **Only bookmarked media** control.
- **Create incident from footage** permission enables users to create an incident from a media file they are currently viewing.
- **Create incident with bulk select** permission enables users to create an incident comprising of media files chosen through bulk select.

  The action is useful if users want to create an incident containing a large number of media files.
- **Use single media as evidence** permission enables users to add a single media file from a longer recording to an incident.

  Administrators can configure how a camera divides a long recording from its device profile. By default, if a recording is longer than 15 minutes, it is divided into 15-minute media files upon download.
- **Use whole recording as evidence** permission enables users to add an entire recording to an incident, instead of only individual media files.
- **Add footage to existing incident** permission enables users to add media files to already existing incidents, instead of only new incidents.
- **Add additional footage from same operator as evidence** permission enables users to add media from the same operator to an incident, if there is already media belonging to that operator in the incident.

  VideoManager only offers to add media from the same operator if the recording times of media files overlap.
- **Hide playback watermark when redacting** permission enables users to toggle the playback watermark when manually redacting the incident clip.
- **View media scheduled to be deleted on dashboard** permission enables users to view which of their media files are set to be deleted within a certain timeframe, via their personal **Home** tab.
- **View media in large view mode** permission enables users to view media files from the **Media** tab in large mode if it is set as the system default.

  With the permission, users can manually select **Large** from the **View options** menu, which changes the **Media** tab to large mode if it is not set as the default.
- **View media in gallery view mode** permission enables users to view media files from the **Media** tab in gallery mode if it is set as the system default.

  With the permission, users can manually select **Gallery** from the **View options** menu, which changes the **Media** tab to gallery mode if it is not set as the default.
- **View media in list view mode** permission enables users to view media files from the **Media** tab in list mode if it is set as the system default.

  With the permission, users can manually select **List** from the **View options** menu, which changes the **Media** tab to list mode if it is not set as the default.

A.3 Incident Permissions

The **Incident permissions** pane offers control over the various operations that can be performed on incidents.

Incident

There are toggles accompanying some permissions that 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** permission controls which incidents users can see on the **Incidents** tab.

  NOTE: If this permission is set to **Off**, any other incident permissions in the same column will also be set to **Off** because all of the following permissions require access to the incident.

- **List** permission controls whether users are presented with the **My Incidents**, **Shared Incidents**, and **Supervised Incidents** panes in the **Incidents** tab.

  The permission also controls whether users can see recently edited and created incidents on their homepage.

- **Access deleted** permission enables users to search for deleted incidents, by selecting the **Show recently deleted incidents** check box in the **Search Incidents** pane.
- **Play** permission enables users to play previously recorded media files on VideoManager, as long as they are part of an incident.
- **Duplicate** permission enables users to duplicate incidents. A new incident that is created contains the same media, location recording, and title.
- **Delete** permission enables users to delete incidents from VideoManager.

  Deleted incidents are retained in line with the deletion policy of VideoManager.

- **Reinstate** permission enables the user to reinstate previously deleted incidents, as long as they have been retained in line with the deletion policy.

  To reinstate an incident, the user should 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 appear with a red banner. The user can click **Reinstate incident** next to the relevant incident.

- **Add to incident collection** permission enables users to add an incident to an incident collection, as long as they have the *Nested Incidents* licence.

  The permission controls which incidents users can add to incident collections and must be used in tandem with the **Create incident collection** and **Add incident to existing incident collection** permissions to create incident collections.

- **Edit** permission enables users to edit the incidents they have access to.

  It is only possible to enable the permission if the corresponding **Access** permission is enabled as well.

- **Export** permission enables users to create exports. Exports, along with incident links, let users share incidents with people who are not on VideoManager.

  Even if a user does not have the permission, automatic exports are created if enabled.

  NOTE: After an incident is exported, VideoManager has no control over it.

- **View audit log** permission enables users to view the audit log of incidents they can already access.
- **Edit share list** permission enables users to edit the **Sharing** pane, which dictates whether the incident is shared with other users on VideoManager.
- **View share list** permission enables users to view the **Sharing** pane, which shows whether the incident is shared with other users on VideoManager.
- **Externally share** permission enables users to create incident links. Incident links, along with exports, let users share incidents with people who are not on VideoManager.

  Incident links only offer access to the incident for a limited time. After the link expires, people outside VideoManager lose access to the incident.

- **Change owner** permission enables users to change the owner of an incident, from the **Sharing** pane.

The permission is useful if the user who created an incident should not own it anymore.

- **Submit** 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.
  The permission is useful if, due to bandwidth limitations, users cannot automatically upload incidents to a Central VideoManager by using **Metadata/Footage Replication**. Instead, users can manually choose to upload incidents from their site.
- **Take control** 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.
  The permission is useful if, due to bandwidth limitations, users cannot automatically upload incidents to a Central VideoManager by using **Metadata/Footage Replication**. Instead, users can manually choose to upload incidents to their Central VideoManager.
- **Restrict** 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** permission enables users to add attachments to an incident, such as PDFs or JPGs.
- **View attachments** permission enables users to view any attachments that have been added to an incident.
- **Remove attachments** permission enables users to delete any attachments from an incident.
- **Edit location** permission enables users to edit the location data for a media file that belongs to the incident they are editing.
  The permission is only applicable for media files that were recorded without location data. Users cannot overwrite previously recorded location data. They can only edit location data that was added to the media file in VideoManager.
- **View location** permission enables users to view the location data for all media files within the incident they are viewing.
  If more than one media file with location data has been added to an incident, the location data is superimposed on top of each other.
- **Commit incident to CommandCentral Evidence** permission enables users to commit incidents from VideoManager to CommandCentral Evidence.
- **Derestrict** permission enables users to derestrict an incident. If an incident is derestricted, all users with the corresponding **Access** permissions can view it.
- **Search Incidents** permission enables users to search for any incidents from the **Search Incidents** pane of the **Incidents** tab.
- **Create incident with no footage** permission enables users to create an incident without any media files in it.
- **Create incident collection** permission enables users to create incident collections containing incidents.
  The permission is not visible unless the user has the *Nested Incidents* licence.
- **Add incident to existing incident collection** permission enables users to add incidents to existing incident collections.
  The permission is not visible unless the user has the *Nested Incidents* licence.
- **View any restricted incident** permission enables users to view restricted incidents.
- **Create incident custom link** permission enables users to create custom links. Custom links, along with exports, let users share incidents with people who are not on VideoManager.
  Incident links only offer access to the incident for a limited time. After the link expires, people outside VideoManager lose access to the incident. Unlike incident links, custom links cannot be emailed. They can only be copied.
- **Bulk-edit incidents** permission enables users to bulk edit incidents.

Users with the permission can delete a large number of incidents at once by using **Delete**.

- **Search by only shared incidents** permission enables users to search for incidents that have been shared either with, or by, them.
- **Search by only externally linked incidents** permission enables users to search for incidents that have been shared with either an incident link or custom link.

  For more information, see Sharing Incidents Externally Using a Link on page 85.
- **Search using advanced filter** permission enables users to search for incidents using the advanced search box and the custom predicate language of VideoManager.

  For more information, see Custom Predicate Language on page 380.
- **Can use saved incident search** permission enables users to search for incidents with a saved search.

  The permission is useful if there are a few repeated searches that are regularly performed.
- **Create saved incident search** permission enables users to create their own saved search.
- **Edit saved incident search** permission enables users to edit previously created saved searches.
- **Delete saved incident search** permission enables users to delete saved searches.
- **Use any export profile** permission enables users to use all export profiles when creating an export, not just export profiles they have been added to.

  Export profiles can be configured from the **Incident Exports** section of the **Policies** pane, in the **Admin** tab.
- **Change export priority** permission enables users to make exports high priority when exporting an incident.

  Export profiles can be configured from the **Incident Exports** section of the **Policies** pane, in the **Admin** tab.

  For more information, see Configuring Incident Exports on page 197.

Incident clips

After a media file is 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 some permissions that determine what incident clips the permissions apply to: **New**, **Existing**, and **Duplicate**.

- **Edit clip times** permission enables users to edit the start/end times of a clip by using **Edit clip start/end time**.

  For more information, see Clipping Videos in Incidents on page 58.
- **Manual redaction** permission enables users to perform redactions on their incident clips.

  The permission is useful if a face or number plate should be obscured due to GDPR reasons, or if a certain aspect of the media should be highlighted.

  For more information, see Manually Redacting Incident Clips on page 58.
- **Assisted redaction** permission enables users to access the Assisted Redaction editor to edit redactions of recorded events and cases, as well as other properties of the clip.

  For more information, see Assisted Redaction Editor on page 69.
- **Edit clip notes** permission enables users to edit the **Notes** section while editing an incident, where users can enter comments about the relevant incident clip.
- **Edit clip bookmarks** permission enables users to edit bookmarks of an incident clip.

  Bookmarks highlight particularly relevant parts of media, which is useful if an incident clip is too long to be watched in full.

  For more information, see Creating, Editing, and Deleting Bookmarks on page 82.

- **Delete clip** permission enables users to delete incident clips from an incident.
  The action does **not** delete the original media file.
- **Select video/audio channel for clip** permission enables users to choose which video or audio channel they want to use in an incident clip.
- **Create composite clip** permission enables users to create composite clips in an incident.
  Composite clips show all media files in an incident simultaneously.
- **Edit composite clip** permission enables users to edit composite clips.
- **Delete composite clip** permission enables users to delete composite clips.
- **View transcription** permission enables users to view transcription within an incident clip.
- **Edit transcription** permission enables users to edit transcription within the incident editor.
- **Import transcription** permission enables users to import transcription to an incident clip.
- **Export transcription** permission enables users to export transcription from an incident clip.
- **Can duplicate incident media clip** permission enables users to duplicate an incident clip in an incident, by clicking **Duplicate clip**. A duplicated incident clip retains the same redaction effects as the original incident clip.
- **Can add new clip for recording in incident editor** permission enables users to add a complete, unredacted recording to an incident by clicking **Add new clip for recording**, if **Group incident clips by recording** is set to **Yes**.

A.4 Device Permissions

The **Device permissions** pane offers control over assigning and operating different devices.

There are toggles accompanying some permissions that determine which devices the permissions apply to: **User** (devices assigned to the user), **Supervised** (devices assigned to users supervised by the user), and **Any** (all devices visible to VideoManager).

Device

- **See devices** permission enables users to see a list of devices detected by VideoManager, from the **Devices** tab.
- **View device on dashboard** permission enables users to see devices assigned to them on their personal **Home** tab.
- **Request device Record-After-The-Fact** permission enables users to request a BWC to generate an RATF event for the device.
- **Configure device for eSIM provisioning** permission enables users to set up their device for eSIM provisioning.
- **Operate device** permission enables users to operate devices. For example, have cameras assigned to them, undock cameras, and record media using the cameras.
- **See unassigned devices** permission enables users to see devices that have not yet been assigned to users, from the **Devices** tab.
- **See devices at sites** permission enables users whose instance of VideoManager is configured as a Central VideoManager to view devices that are connected to their sites.

The devices can be found by navigating to the **Devices** tab, selecting the **Search Devices** pane, and selecting **Include remote devices**. After clicking **Find devices**, devices associated with the sites of Central VideoManager are returned as well as devices directly associated with the Central VideoManager.

- **See forgotten devices** permission enables users to view devices that have been forgotten. Forgotten devices are devices that used to be connected to VideoManager, but have been manually removed by users because they are redundant.

  The devices can be found by navigating to the **Devices** tab, selecting the **Search Devices** pane, and selecting **Include forgotten devices**. After clicking **Find devices**, devices associated with the sites of Central VideoManager are returned as well as devices directly associated with the Central VideoManager.
- **Forget devices** permission enables users to "forget" devices that were once connected to VideoManager but are now disconnected, either because they are in use, or because they have been replaced or are no longer in circulation.

  A device can be forgotten by navigating to the **Devices** tab, clicking **View device info** next to the relevant device, clicking **Forget Device** in the top right-hand corner, and clicking **Yes** to confirm.
- **Bulk-edit devices** permission enables users to bulk edit devices.

  Users with the permission can perform a variety of issues on a large number of devices, including **Upgrade** and **Forget**.
- **Download device audit logs** permission enables users to download the audit logs of a specific device to their PC.

  An audit log of the device can be downloaded by navigating to the **Devices** tab, clicking **View device info** next to the relevant device, clicking **View device audit log** in the top right-hand corner, and clicking **Filter audit log**.
- **Request a device state capture** permission enables users to receive information about the current status of their device.
- **Download device configuration** permission enables users to download the configuration of their device after generating it.

Vehicle

- **View vehicles** permission enables users to see a list of vehicles detected by VideoManager.
- **Edit vehicle configuration** permission enables users to edit the configuration of a specific vehicle.
- **Download vehicle configuration** permission enables users to download the configuration of the vehicle after generating it.
- **Operate vehicles** permission enables users to operate vehicles.
- **Request a vehicle state capture** permission enables users to receive information about the current status of a specific vehicle.
- **Forget vehicles** permission enables users to "forget" vehicles that were once connected to VideoManager but are now disconnected, either because they are in use, or because they have been replaced or are no longer in circulation.
- **See vehicles at sites** permission enables users whose instance of VideoManager is configured as a Central VideoManager to view vehicles that are connected to their sites.
- **See forgotten vehicles** permission enables users to view vehicles that have been forgotten. Forgotten vehicles are vehicles that used to be connected to VideoManager, but have been manually removed by users because they are redundant.
- **Bulk-edit vehicles** permission enables users to bulk edit vehicles.

Users with the permission can perform a variety of issues on a large number of vehicles, such as "forgetting" the vehicle.

- **Download vehicle audit logs** permission enables users to download the audit logs of a specific vehicle to their PC.
- **Request vehicle Record-After-The-Fact** permission enables users to request a vehicle to generate an RATF event.

Management

Management permissions control device settings, factory resetting, and updating the firmware of devices as well as managing, viewing, and deleting docks.

- **Change custom status** permission enables users to change the custom status of a device from the **Custom status** field in the **Edit device properties** pane.
- **Factory reset devices** permission enables users to factory reset devices.
  When a device is factory reset, its access control key and any media that was not already downloaded to VideoManager are deleted.
- **Apply device firmware upgrades** permission enables users to upgrade devices, if new firmware is available.
- **Manage docks** permission enables users to configure, reboot, and upgrade connected docks.
- **View docks** permission enables users to view the list of docks currently visible to VideoManager from the **Status** pane, including their statuses (**Online**, **Offline**, or **Disabled**).
- **Delete docks** permission enables users to remove docks that are no longer connected to VideoManager from the **Docks** pane of the **Devices** tab.
- **Bulk-edit Docks** permission enables users to bulk edit docks from the **Docks** pane of the **Devices** tab.
- **Associate camera by QR code** permission enables users to assign a VT-series camera with a QR code, instead of needing to dock it first.
- **Change device name** permission enables users to change the name of a device from the **Device name** field in the **Edit device properties** pane.
- **Change auto upgrade** permission enables users to change an auto-upgrade status of a device by using the **Auto-upgrade** toggle in the **Edit device properties** pane.
- **Change static IP** permission enables users to change static IP settings of a device by using the **Use static IP** toggle in the **Edit device properties** pane.
- **Change touch assign** permission enables users to change touch assign settings of a device by using the **Touch assign** toggle in the **Edit device properties** pane.
- **Set service required** permission enables users to change status of a device to **Service Required** by using the **Service required** toggle in the **Edit device properties** pane.
- **Clear service required** permission enables users to change status of a device from **Service Required** to normal by using the **Service required** toggle in the **Edit device properties** pane.
- **Resilient Touch Assign configuration** permission enables users to configure RTA (Resilient Touch Assign). RTA allows the continued assigning of devices using a dock that is no longer connected to VideoManager, so that users can still assign devices during a network or service outage.

Mobile App

Mobile App permissions control what actions a user can perform when configuring or using the Mobile App.

- **Setup Mobile App for myself** permission enables users to configure the Mobile App for themselves.

- **Setup Mobile App for supervised user** permission enables users to configure the Mobile App for users they supervise.
- **Setup Mobile App for any user** permission enables users to configure the Mobile App for all users on VideoManager.
- **Use Mobile App** permission enables users to utilise the Mobile App on their mobile phones.
- **Use Mobile App view finder** permission enables users to utilise the viewfinder function of the Mobile App. The viewfinder function enables users to see what their device sees and check whether their device is mounted correctly.
- **Play video in Mobile App** permission enables users to watch the media files in the Mobile App.
- **View/Edit Mobile App metadata** permission enables users to view and edit the metadata of the media files they have recorded in the field.
- **View system page in Mobile App** permission enables users to access the **System** page of the Mobile App. The **System** page displays the status of the VB400, that is whether it is recording or not, and its serial number.
- **Allow streaming** permission enables users to stream in the Mobile App.

ONStream

ONStream permissions control what actions a user can perform during a device live stream.

- **Live view** permission enables the user to view a live stream of a device by using VideoManager.

Assignment

Assignment permissions control the user's ability to assign devices, both to themselves and other users on the system.

- **Return devices** permission enables users to unassign devices detected by VideoManager.
- **Assign device** permission enables users to assign devices visible to VideoManager. Devices must be assigned to users before they can record media.

  For more information, see Devices Assignment and Media Recording on page 100.

  NOTE: The permission must be combined with either **Manually assign a device for single use**, **Manually assign a device for permanent use**, or **Manually allocate a device**.
- **Assign device using RFID touch assign** permission enables users to assign devices visible to VideoManager by using touch assign.
- **Assign multiple devices using RFID touch assign** permission enables users to assign more than one device to a user by using touch assign.

  The permission can be necessary if there is one user to whom all devices should be assigned in case of an emergency, so that many operators can undock and use devices quickly. However, in that case, media cannot be traced back to one specific operator.
- **Assign all available devices using RFID touch assign** permission enables users to make all docked devices available for recording with touch assign.

  For more information, see Bulk Touch Assigning on page 105.
- **Select device profile when assigning** permission enables users to select the device profile for the device they are assigning. If users do not have the permission, VideoManager uses either the default device profile as set in the **Device Profiles** section of the **Devices** pane, in the **Admin** tab, or the device profile that is assigned to the user's role.
- **Pre-assign device** permission allows users to pre-assign a device before it has been docked to VideoManager.

The permission is useful if a remote worker is being sent a new device, but they do not have access to the UI of their site. Pre-assign allows the system administrator to assign the device from the UI of the site so that it is ready to use when it arrives at the remote worker's home.

- **Find and collect allocated device using RFID touch assign** permission enables users to collect a device assigned to them by using touch assign.
- **Allocate new device using RFID touch assign** permission enables users without an assigned device to permanently assign themselves a device from the pool by using touch assign.
- **Manually assign a device for single use** permission enables users to assign a device to a user for one trip.
  After the device is redocked, it becomes unassigned and is returned to the pool.
  If users want to enable the permission, they must also enable **Assign device**.
- **Manually assign a device for permanent use** permission enables users to assign a device to a user permanently, until it is manually unassigned.
  After the device is redocked, it remains assigned to the same user.
  If users want to enable the permission, they must also enable **Assign device**.
- **Manually allocate a device** permission enables users to assign a device to a user permanently, until it is manually unassigned. The user must undock the device by using touch assign.
  After the device is redocked, it remains assigned to the same user.
  If users want to enable the permission, they must also enable **Assign device**.
- **Force unassign** permission enables users to unassign a device while it is in the field from the **Edit device properties** pane.
  The permission does not unassign the device while the operator is still using it.
  As soon as the device is redocked, it becomes unassigned, even if it was originally assigned with permanent issue.

A.5 User Permissions

The **User permissions** pane offers control over what power a user has to change the information of other users and groups on the system.

There are toggles accompanying some permissions that determine which users the permissions apply to: **Supervised** (users supervised by the user), and **Any** (all users on VideoManager).

User

User permissions control the user's ability to create, edit, and delete other users on VideoManager.

- **View** permission enables users to view other user's profiles.
- **Delete** permission enables users to delete other users.
- **Change touch assign** permission enables users to edit the touch assign value for other users on the system. If the 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** permission enables users to enable other users. When a user is enabled, they can log on.
- **Disable** permission enables users to disable other users. When a user is disabled, they cannot log on.
- **Edit display name** permission enables users to change the display name of other users.
- **Force password change** permission enables users to force other users to change their password next time they log on to VideoManager via the **User must change password** toggle.

- **Undo force password change** permission enables users to undo the effects of the **Force password change** permission.
- **Add user-specific WiFi networks** permission enables users to create their own user-specific WiFi networks.
- **Edit user-specific WiFi networks** permission enables users to edit existing user-specific WiFi networks.
- **Remove user-specific WiFi networks** permission enables users to remove existing user-specific WiFi networks.
- **Change password** permission enables users to change the password of other users.
- **Set password for new user** permission enables a user to set the password for a new user before they log on for the first time.
- **Edit sharing** permission determines whether or not users can alter the sharing settings of other users, such as whether their media and incidents are automatically shared with other users on the system.
- **Edit roles** permission enables users to edit what roles other users inhabit.
- **Edit groups** permission enables users to edit which users are supervised by groups.
- **Edit external app config** permission enables users to configure how VB-series cameras interact with the VideoBadge View app.
- **Create** permission enables users to create other users.
- **Clear Two Factor Authentication** permission gives a user the ability to clear the two factor authentication key for another user from the **Edit Role** pane.
  The permission is useful if a user has lost the phone on which their two factor authentication code is configured. They are locked out of VideoManager until the key is reset.
- **Edit user email** permission enables a user to edit the email address of either users they supervise or all users on the system. The permission is only viewable if email notifications have been licenced from Motorola Solutions.
- **Edit user mobile** permission enables a user to edit the phone number of either users they supervise or all users on the system. The permission is only viewable if SMS notifications have been licenced from Motorola Solutions.
- **Test user email** permission enables a user to send a test email to either users they supervise or all users on the system. The permission is only viewable if email notifications have been licenced from Motorola Solutions.
- **Test user mobile** permission enables a user to send a test SMS to either users they supervise or all users on the system. The permission is only viewable if SMS notifications have been licenced from Motorola Solutions.
- **View permission report** permission enables users to view a user's effective permissions by utilising the **View effective permissions** control.
- **View Bluetooth pairing** permission enables users to view cameras that have been paired to a specific user by utilising the **View device Bluetooth pairings** control.
- **Remove Bluetooth pairing** permission enables users to remove Bluetooth Peripherals and other Bluetooth cameras from users by utilising the **Remove pairing** control.
- **View device affinity** permission enables users to view the device affinities for other users.
- **Clear user device affinity** permission enables users to clear the device affinities for other users.
  For more information, see Viewing and Clearing Device Affinities for Users on page 143.
- **Edit user authentication ID** permission enables users to edit the authentication ID of a specific user.
- **Edit user user property** permission enables users to edit properties of a specific user.

- **Reassign user** permission enables users to reassign a user, which transfers the ownership of all incidents, media files, and exports from one user to another. Incidents and media files shared with the first user are shared with the second user instead.
  The permission is useful if a user is going to be deleted, and another user should take ownership of their media and incidents. Users can be reassigned even after they have been deleted.
- **Assign higher privileges** permission enables users to add themselves and other users to a role which has permissions that the user does not have.
  If the permission is set to **Off**, the user cannot add other users to a role if the role has permissions that the user does not have.

  NOTE: Even users with the **Assign higher privileges** permission are not able to add other users to roles that are in a higher tier than their own role.
- **Export users** permission enables users to export an entire user database of VideoManager to a CSV file.
- **Import users** permission enables users to import an entire user database of VideoManager to a CSV file.
- **Edit user in same tier** permission enables users to edit the details of the users that are at the same tier level as them.
- **Edit user in higher tier** permission enables users to edit the details (including password and email addresses) of any user in the system, including the users that are in a higher tier than them.
- **Assign roles at same tier** permission enables users to assign roles of the same tier level as them.
  This action allows users to elevate users of a lower tier to the same tier as them.

Account

Account permissions control what actions from the **Account Profile** pane a user can take on themselves.

- **View user-specific WiFi networks** permission enables users to view their own user-specific WiFi networks.
- **Edit user-specific WiFi networks** permission enables users to edit their own user-specific WiFi networks.
- **Edit own display name** permission enables users to change their own display name.

User group

User group permissions control the user's ability to create, edit, and delete groups on VideoManager.

- **View** permission enables users to view the **Groups** section of the **People** pane, in the **Admin** tab.
- **Delete** permission enables users to delete groups.
- **Edit display name** permission enables users to change the display name of a group.
  The **Group name** cannot be changed after it is set, but the **Display name** can be changed as many times as necessary.
- **Add user-specific WiFi networks** permission enables users to add a user-specific WiFi network to a group.
- **Edit user-specific WiFi networks** permission enables users to edit a user-specific WiFi network that has been added to a group.
- **Remove user-specific WiFi networks** permission enables users to delete a user-specific WiFi network that has been added to a group.

  If enabled, users have access to the **WiFi networks** pane in the **Groups** section.
- **Edit sharing** permission enables users to configure which users or groups have access to the group's media files and incidents.

  If enabled, users have access to the **Sharing** pane in the **Groups** section.
- **Edit roles** permission enables users to edit the roles that a group inherits.

If enabled, users have access to the **Roles** pane in the **Groups** section.

- **Edit groups** permission enables users to edit which groups are supervised by other groups.

  If enabled, users have access to the **Group memberships** pane in the **Groups** section.
- **Create** permission enables users to create a new group.
- **View permission report** permission enables users to view the permissions report for a group by utilising the **View effective permissions** control.

A.6
Notification Permissions

If notifications are licenced, the **Notification** pane controls when users receive notifications. Users can typically receive notifications either through SMS or email. The action can be configured from the **Users** section of the **People** pane, in the **Admin** tab.

Receive notifications on

Receive notifications on permissions control which actions performed by users on VideoManager prompt a notification.

- **First time login** permission prompts a notification when other users first log on to VideoManager.
- **Personal device stream start** permission prompts a notification when a camera assigned to the user starts streaming.
- **Supervised device stream start** permission prompts a notification when a camera assigned to users that other users supervise starts streaming.
- **File storage threshold warnings** permission prompts a notification when VideoManager is low on storage space.

Dashboard notifications

Dashboard notifications permissions control which notifications users can see on their dashboard.

- **Media shares** permission enables users to see which media has been shared with them, via a notification on their homepage.
- **Media ownership changed** permission enables users to see which media now belongs to them, via a notification on their homepage.
- **Media downloaded** permission enables users to see which media files have been successfully downloaded from their cameras, via a notification on their homepage.
- **Incident shares** permission enables users to see which incidents have been shared with them, via a notification on their homepage.
- **Incident ownership changed** permission enables users to see which incidents now belong to them, via a notification on their homepage.
- **Completed exports** permission enables users to see which of their exports have finished processing, via a notification on their homepage.
- **Completed imports** permission enables users to see which of their imports have finished processing, via a notification on their homepage.
- **Licence warnings** permission enables users to see when licences expire, via a notification on their homepage.

  The notification cannot be cleared.

- **Application warnings** permission enables users to see system warnings, such as if a licence is expiring within a week, via a notification on their homepage.

  The notification cannot be cleared.

A.7 Report Permissions

The **Report permissions** pane controls whether users can view aspects of VideoManager relating to reports and live statistics.

Reports

Reports permissions control whether users can perform actions on reports.

- **View reports** permission enables users to view reports from the **Reports** pane of the **Status** tab.
- **Create reports** permission enables users to create new reports from the **Reports** pane of the **Status** tab.

  If enabled, users have access to the **Create New Report** control.

  If **Create scheduled reports** is not enabled, users do not have the ability to make their reports scheduled.
- **View scheduled reports** permission enables users to view scheduled reports from the **Reports** pane of the **Status** tab.

  If enabled, users have access to the **Scheduled Reports** pane.
- **Create scheduled reports** permission enables users to create scheduled reports from the **Reports** pane of the **Status** tab.

  If enabled, users have access to the **Create New Report** control.

  If **Create reports** is not enabled, users do not have the ability to make a one-off report. In the **Schedule** drop-down list, the **No** option will not be available.

Live stats

Live stats permission dictates whether users can view the **Statistics** pane in the **Status** tab.

- **View live stats** permission enables users to view statistics related to their instance of VideoManager, from the **Statistics** pane.

A.8 Field Permissions

The **Field permissions** pane 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.

A.9 Advanced Permissions

The **Advanced permissions** pane offers control over access control keys, viewing sites, and changing manager settings.

Settings

The first half of the 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 the permissions control advanced actions.

- **Change manager settings** 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** permission enables users to export access control keys from an instance of VideoManager.
- **Delete access control keys** permission enables users to delete access control keys.

  If cameras on VideoManager were using the access control key that is deleted, the cameras appear as `Locked` and any media on them which had not yet been downloaded to VideoManager at time of deletion is lost forever.
- **Export file space keys** permission enables users to export keys used for decrypting file spaces.
- **Select Language for login session** permission enables users to choose in which language their instance of VideoManager is presented. The language only applies to their personal session. When they log out, it is reset to the default specified from the **Language** section of the **User Interface** pane, in the **Admin** tab.
- **List sites connected to the Manager** permission enables users on a Central VideoManager to see a list of all sites connected to it.

  If enabled, users have access to the **Sites** and **Site Uploads** panes in the **Status** tab.
- **Visit sites connected to the Manager** permission enables users to access the UI of a site through the Central VideoManager.

  If enabled, users have access to the **View site** control in the **Sites** pane.
- **Edit EdgeController network configuration** permission enables users to edit a previously generated EdgeController configuration.
- **Generate EdgeController network configuration** permission enables users to create an EdgeController configuration.
- **Export device profile** permission enables users to export a device profile from their instance of VideoManager.

  The permission 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** is enabled, import the profiles into their sites.
- **Import device profile** permission enables users to import a device profile into their instance of VideoManager.

  The permission 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** is enabled, users can manually export the relevant profiles and import the profiles into their site.
- **Export Network profile** permission enables users to export a network profile from their instance of VideoManager.

  NOTE: The action also exports the passwords associated with the WiFi networks within the network profile.
- **Import Network profile** permission enables users to import a network profile from their instance of VideoManager.
- **Export vehicle network profile** permission enables users to export a network profile of a specific vehicle.
- **Import vehicle network profile** permission enables users to import a network profile of a specific vehicle.
- **Export self service settings** 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** 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** permission enables users to restart their VideoManager server.
  Restart can be necessary if, for example, a new licence has been downloaded or if the public address of VideoManager has changed, and more.
- **View system status** permission enables users to view the status of their system from the **Status** tab.
  If there are any system warnings, they are viewable here.
- **Export database** permission enables users to export and entire database of VideoManager.
- **Allow platform change requests** permission enables users to change EdgeController configurations from the EdgeController over WiFi, instead of needing to deliver the configuration physically by USB.
- **View grid status** permission enables users to view the status of their grids, if grids are being used.
  If enabled, users have access to the **Grid** pane in the **Status** tab.
- **View UI configuration tab** permission enables users to view the **UI Configuration** tab in the VideoManager administrator application.
- **View UI login mode tab** permission enables users to view the **UI Login Mode** tab in the VideoManager administrator application.
- **View about legal page** permission enables users to view the **Legal** pane in the **Admin** tab.
  The pane gives users insight into terms and conditions of VideoManager.
- **Initiate immediate database backup** permission enables users to initiate an immediate backup of the database that captures the state of VideoManager at the time when the immediate backup was created.
- **Export import profiles** permission enables users to export their import profile from an instance of VideoManager.
- **Import import profiles** permission enables users to import their import profile into their instance of VideoManager.
- **Import system config** 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** 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.
- **Edit Record-After-The-Fact settings** permission enables users to change system settings relating to RATF.

Accessibility

Accessibility permissions control printing and copying text from the web interface.

- **Print from website** permission allows users to print pages of VideoManager, if enabled.
  Although the user can use CTRL + P like normal if this permission is not enabled, the page will appear as blank.
- **Copy text from website** permission enables users to copy text from VideoManager.
  Although the user can use CTRL + C like normal and highlight text if this permission is not enabled, they will not be able to paste the results.

Tactical Video Manager

Tactical Video Manager permissions are only viewable if Tactical VideoManager has been licenced from Motorola Solutions.

- **Access tactical mode** permission enables users to view the **Tactical** tab.
- **View Tactical Video Wall** permission enables users to view the Tactical VideoManager wall.

- **Update Tactical Video Wall** permission enables users to add and remove live streams from the Tactical VideoManager wall.

Asset imports

Asset imports permissions dictate which users can import media files into VideoManager.

There are toggles accompanying some permissions that determine which asset imports the permissions apply to: **Owned** (asset imports created by the user), **Supervised** (asset imports that have been created by other users on the system that the user supervises), and **Any** (any asset imports on the system, regardless of who created them).

- **View/delete** permission enables users to view and delete media files.
- **View audit log** permission enables users to view the audit logs of relevant media files.
- **Use asset imports** permission enables users to import media files.
- **View/delete automated imports** permission enables users to view and delete automated imports from the **Media** tab.

API

- **Access OpenApi resources** permission enables users to access OpenAPI resources from the **API Key Management** section.
- **View anonymous live stream links** permission enables users to receive an anonymous live stream URL for a device via the devices API. When a device starts live streaming, the system can send a notification via SMS, email, or HTTP (to an external integration system) that contains an "anonymous" access URL for the live stream. Anyone with access to the URL can view the VideoManager live stream without any further authentication.

Appendix B

Device Profiles

A device profile determines the behaviour of a camera when it is recording. There is a different device profile for each type of camera.

B.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**, **Audio Settings**, **Bluetooth Settings**, **Mobile App Settings**, and **Controls**.

To view the relevant settings, perform the following actions:

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. In the **Details** pane, from the **Device family** drop-down list, select **VB400**.

The following settings are now available.

Notifications & Alarms

Notifications & Alarms section enables administrators to customise how the VB400 alerts its operator to various states and events.

- If **Sound alarm when storage nearly full** is set to **Yes**, the VB400 beeps periodically when the storage space is low.
- If **Sound alarm when battery level critical** is set to **Yes**, the VB400 beeps periodically when the battery level is critically low, that is less than 10 minutes of recording remains.
- If **Customise LED patterns** is set to **Yes**, the administrator can customise how LEDs behave when recording and pre-recording by using the **When recording** and **When pre-recording** drop-down lists, respectively. The options for both drop-down lists are as follows:
  - **Solid red**
  - **Solid green**
  - **Blinking red**
  - **Blinking red (top light only)**

  If set to **No**, the VB400 uses the default LEDs.
- The administrator can customise how a VB400 behaves when in normal mode and hush mode by 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 **Yes**, LEDs indicate when a camera starts and stops recording/pre-recording.

- If **Enable beeps** is set to **Yes**, sounds indicate when a camera starts and stops recording/pre-recording.
- If **Enable vibrate** is set to **Yes**, haptic feedback indicates when a camera starts and stops recording/pre-recording.
- If **Enable X-Series LEDs** is set to **Yes**, any X-series cameras connected to VB400s in the device profile have their LEDs enabled to indicate when they are recording.
- If **Enable X-Series vibrate** is set to **Yes**, any X-series cameras connected to VB400s in the device profile have haptic feedback enabled to indicate when they start recording.

- The administrator can customise whether a VB400 alerts the user periodically while it is recording or while its audio is muted by using the **Recording alarm** and **Alarm while muted** rows. The options for the rows are as follows:
  - If **Enable beeps** is set to **On**, the VB400 beeps while recording or muted.
  - If **Enable vibrate** is set to **On**, the VB400 buzzes while recording or muted.

  In the **Seconds** field, administrators can configure the interval at which the alarm should sound (between 5 and 600 seconds). The field applies to both beeps and haptic feedback, depending on what is enabled.

  NOTE: If **Enable beeps** and **Enable vibrate** have not also been set to **On** in either the **When in normal mode** or **When in hush mode** row, none of the configuration in the **Recording alarm** row takes effect.

Power Management

Power Management section enables administrators to configure advanced battery life management.

- From the **Behaviour when idle** drop-down list, the administrator must select how the VB400 behaves when idle, that is when it is assigned and undocked, but not recording. The options are as follows:
  - **Device enters standby mode** – The camera enters standby. The VB400 leaves standby as soon as it is prompted to record again.
  - **Device shuts down** – The camera shuts down. The VB400 turns on a few seconds after it is prompted to record.

    NOTE: If **Device shuts down** is selected, the battery lasts for longer between charges.

- If **Enter safety mode if idle after undocking** is set to **Yes**, the VB400 enters safety mode shortly after it is undocked, which means it cannot be used, and does not respond to any button presses, until the operator performs the preconfigured gesture that prompts it to leave safety mode.

  NOTE: A gesture to exit safety mode must be configured from the **Controls** section. Otherwise, VB400s in the device profile cannot be used.

Recording Behaviour

Recording Behaviour section controls how the VB400 acts when it is recording.

- If **Show video metadata overlay** is set to **Yes**, metadata is shown over all media files recorded on cameras which inhabit the 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 Configuring Video Metadata Overlay Settings on page 167.

- If **Overwrite oldest footage when full** is set to **Yes**, the camera overwrites the oldest media with newer media if it has run out of storage space.

  If set to **No**, the camera stops recording after it runs out of storage space.

- From the **Recording policy** drop-down list, the administrator must determine whether the VB400 starts recording automatically from undock, or it must be manually prompted to start recording. The options are as follows:

  - **Controlled by gesture** – The VB400 does not start recording automatically. The operator must prompt it to record by using the gesture determined in the **Controls** section. Alternatively, the VB400 can be prompted to start recording via peer-assisted recording or a Bluetooth Peripheral.
  - **While not docked** – The VB400 starts recording automatically, as soon as it is undocked. It continues to record until it runs out of battery, or is redocked again. The user cannot stop recording manually, even if gesture(s) have been configured in the **Controls** section.
  - **Start once on undocking, then gesture controlled** – The VB400 starts recording automatically, as soon as it is undocked. The operator can then stop and start recording manually by using the gesture(s) determined in the **Controls** section. Alternatively, the VB400 can be prompted to start recording via peer-assisted recording or a Bluetooth Peripheral.

- If **Allow recording in hush mode** is set to **Yes**, the camera can record media while in hush mode. The camera can also enter hush mode while recording.

  If set to **No**, if the camera is in hush mode and the operator performs the gesture that prompts their body-worn camera to start recording, the camera exits hush mode. If the camera is recording and the operator performs the gesture that prompts their camera to enter hush mode, the camera stops recording.

  NOTE: Pre-record still works in hush mode, even if **Allow recording in hush mode** is set to **No**.

- If **Pre-record** is set to **Yes**, pre-recording media is enabled.

  When pre-record is enabled, the following options are available:

  - In the **Seconds** field, the administrator must enter the number of seconds for which the VB400 pre-records. The default is 30 seconds, and the upper limit is 120 seconds.
  - From the drop-down list, the administrator must select when pre-record starts. The options are as follows:
    - **Always pre-record when not charging** – Pre-record is enabled as soon as the camera is undocked.
    - **Manually start/stop pre-record** – The administrator must manually configure an action that, when performed, starts pre-record. The action can be done from the **Controls** pane.
  - The administrator can set **Post-record** to **Yes**.

    In the **Seconds** field, the administrator must enter the number of seconds for which the VB400 post-records. The default is 30 seconds, and the upper limit is 120 seconds.

- From the **Record audio** drop-down list, the administrator can select whether their body-worn cameras record audio or not. The options are as follows:
  - **Yes** – Audio is recorded during both pre-record and normal recording.
  - **Yes (except during pre-record)** – Audio is only recorded during normal recording.

    NOTE: The option is only available if pre-record is enabled.

  - **No** – Audio is not recorded during pre-record or normal recording, and cannot be heard when viewing live streams.
- If **Record audio** is set to **Yes**, the administrator can configure whether audio is initially muted when the VB400 starts recording. The action can be controlled by using the **Audio initially muted** toggle.
- If **Enable GPS** is set to **Yes**, GPS location data is recorded alongside any media file.

  NOTE: GPS location data is captured by VB400s in one-second intervals.

  If set to **No**, the user can still add location data to the media files after they have been downloaded to VideoManager.

- If **Capture image on bookmark** is set to **Yes**, the VB400 takes a screenshot of the video it is recording at the same time as it captures a bookmark. The screenshot is downloaded to VideoManager as a JPEG after the VB400 is redocked.

  NOTE: A bookmark gesture must be selected from the **Controls** section, or else the configuration does not have any effect.

- In the **Video length** field, the administrator must enter the number of minutes for which a VB400 can record, after which the media is split into multiple media files.

  The administrator can select between 5 and 30 minutes.

- In the **Suppress recording on undock** field, the administrator must enter the number of seconds for which the camera is prevented from recording after it is undocked, which means that in the configured period of time, the camera ignores any gestures that would normally prompt it to record.

  NOTE: The action applies to recordings that would be started by Bluetooth Peripherals.

- From the **Time Zone** drop-down list, the administrator can select the time zone for VB400s in the device profile, which affects video metadata and filenames. If left as the default, video metadata and filenames either are dictated by the time zone of the associated dock or, if the time zone of the dock is not set, the system time zone of VideoManager.

  For more information, see Setting the System Time Zone of VideoManager on page 287.

Video Settings

Video Settings section controls video resolution and frame rate.

- From the **Video resolution** drop-down list, the administrator can select the video resolution of media files recorded on cameras that inhabit the 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** drop-down list, the administrator can select the frame rate in which a VB400 records. The options are as follows: **25** or **30**.

Audio Settings

Audio Settings section controls the audio options.

- From the **Audio profile** drop-down list, the administrator must select which audio profile should be used by VB400s in the device profile. The options are as follows:
  - **Mostly outdoor** profile is ideal if the majority of recording takes place outdoors.
  - **Mostly indoor** profile is ideal if the majority of recording takes place indoors.
- From the **Audio codec** drop-down list, the administrator must select the kind of audio to be recorded by VB400s with the device profile. The options are as follows:
  - **AAC** compresses the audio, and results in smaller file sizes.
  - **PCM** records high-quality audio, but results in larger file sizes.

Bluetooth Settings

Bluetooth Settings section controls whether Bluetooth can be used with a VB400.

- From the **Yardarm™ Holster Aware™ peripherals** drop-down list, the administrator can select how many Bluetooth Peripherals should be associated with cameras in the device profile. If a VB400 in the device profile cannot find the number of Bluetooth Peripherals specified here when it is out in the field, an alarm sounds.

  For more information about setting up Holster Aware sensors with VB400s, you can navigate to the Motorola Solutions Learning Experience Portal (registration is free) and search for *VideoManager and Personal-Issue Yardarm Holster Aware Sensors Explained.*
- If **Peer-Assisted recording** is set to **On**, an assigned or allocated VB400 automatically starts recording if another VB400 starts recording in its vicinity. When enabled, the following options are available:
  - If **Suppress PAR after undocking** is set to **Yes**, the administrator can set the number of seconds after undocking a camera before this camera starts advertising a recording start event to other cameras.
  - If **PAR beacon timeout** is set to **Yes**, the administrator can set the number of minutes after a camera starts recording for which it will trigger nearby cameras to start recording.
  - From the **PAR proximity** drop-down list, the administrator can select the approximate maximum distance between the cameras to trigger the PAR recording.

  For more information about setting up peer-assisted recording, you can navigate to the Motorola Solutions Learning Experience Portal (registration is free) and search for *Peer-Assisted Recording Explained*.
- From the **Motorola radio integration** drop-down list, the administrator can configure which radios should be compatible with cameras in the device profile.

  For more information about setting up radio integration with VB400s, you can navigate to the Motorola Solutions Learning Experience Portal (registration is free) and search for *VideoManager and Tetra Radio Integration Explained* or *VB400 and MOTOTRBO Radio Integration Explained*.

Mobile App Settings

From the **Enable mobile app** drop-down list, the administrator can select which Mobile App can be used with a VB400. The options are as follows: **None**, **VB SmartControl**, and **VB Companion**.

For more information about setting up the Mobile Apps with VideoManager, you can navigate to https://www.motorolasolutions.com/en_xu.html and search for *VideoManager: VB SmartControl User Guide* or *VideoManager VB Companion Guide*.

Controls

Controls section enables administrators to configure the buttons and gestures.

- From the **Hold timing** drop-down list, the administrator can select how long an operator must hold the button on a VB400 for the camera to register the gesture as a "hold". The options are: **Long**, **Normal**, or **Short**.
- From the **Double click timing** drop-down list, the administrator can select how quickly an operator must double-click the button on a VB400 for the camera to register the gesture as a "double-click". The options are: **Long**, **Normal**, or **Short**.

VB400

Administrators can map the following VB400 buttons: **Front button** to gestures, such as **Press**, and the actions that will be performed as a result, such as **No action**.

To map a button gesture onto an action, the administrator must identify the relevant button and gesture from the **Control** column. By using the corresponding **Action** drop-down list, the administrator must select the action to be performed when the button 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 recording, recording stops when the gesture is performed. If the VB400 is not recording when the gesture is pressed, recording starts.
- **Start recording** – The gesture starts recording. If recording is 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 stops recording and shuts down.
- **Show battery status** – The gesture causes the LED C to reflect the battery status. If the LED is green, the camera still has plenty of charge left. If the LED is yellow, the battery is running low and should be recharged as soon as possible. If the LED is red, the camera is about to shut down due to low battery.
- **Record bookmark** – The gesture places a bookmark in the media file. After the media file is 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 media file. Users can place bookmarks into media files on VideoManager, but they must be in an incident first.

  For more information, see Creating, Editing, and Deleting Bookmarks on page 82.

  NOTE: If **Capture image on bookmark** is set to **Yes** in the **Recording Behaviour** section, the gesture prompts the VB400 to take a screenshot of the video.
- **Enter hush mode** – The VB400 enters hush mode. While in hush mode, the VB400 obeys the settings configured in the **When in hush mode** row of the **Notifications & Alarms** pane.
- **Exit hush mode** – The VB400 exits hush mode. Without hush mode, the VB400 obeys 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.
- **Mute audio** – The gesture stops the VB400 from recording audio. If the VB400 is muted, the gesture does nothing.
- **Unmute audio** – The gesture stops the VB400 from recording audio. If the VB400 is unmuted, the gesture does nothing.
- **Toggle mute audio** – The gesture changes whether audio is recorded. If the VB400 is muted, it starts recording audio when the gesture is performed. If the VB400 is unmuted, it stops recording audio when the gesture is performed.
- **Pair Bluetooth peripheral** – The gesture prompts 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 allows 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** drop-down list.
- **Enter safety mode** – The gesture causes the VB400 to enter safety mode. While in safety mode, the VB400 is completely inert, that is it start/stop recording gestures do not work, and the camera does not connect to WiFi networks/Bluetooth, and does not make noise.
- **Exit safety mode** – The gesture causes the VB400 to exit safety mode. After the VB400 exits safety mode, it can record media, connect to WiFi networks/Bluetooth, and make noise.
- **Toggle safety mode** – If the VB400 is in safety mode, it exits safety mode. If the VB400 is not in safety mode, it enters safety mode.

The following drop-down options are only visible if **Pre-record** is set to **Yes** in the **Recording Behaviour** pane:

- **Start pre-record** – The gesture starts pre-recording. The length of the pre-record depends on the configuration in the **Recording Behaviour** pane.
- **Stop pre-record** – The gesture stops pre-recording and the pre-recorded media is discarded.
- **Toggle pre-record** – If the camera is pre-recording, the gesture stops pre-recording. If the camera is not pre-recording, the gesture starts pre-recording.

In the **Controls** section, there is an option to make the **WiFi connection** either **Automatic** or **Manual**. If set to **Automatic**, the VB400 searches for WiFi upon powering on. If set to **Manual**, the VB400 must be ordered to search for WiFi by using a button gesture, which is why more options appear in the drop-down list dictating what action the button performs.

- **Connect to WiFi** – The gesture prompts the VB400 to start searching for WiFi. If the VB400 is connected to WiFi, the gesture does nothing.
- **Disconnect from WiFi** – The gesture disconnects the VB400 from WiFi. If the VB400 is not connected to WiFi, the gesture does nothing.
- **Toggle WiFi connection** – The gesture changes the state of the WiFi connection. If the WiFi was turned off, it will be turned on, and vice versa.

X-100/X-200

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 to be performed as a result. To map the gesture to an action, the user must use the **Action** drop-down list. The options are the same as in the VB400 section.

B.2
VB200/300 Device Profile

The device profile section for a 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, perform the following actions:

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. In the **Details** pane, from the **Device family** drop-down list, select **VB200 / 300**.

The following settings are now available.

Notifications & Alarms

Notifications & Alarms section enables administrators to customise how 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 beeps periodically when the storage space is low.
- If **Sound alarm when battery level critical** is set to **Yes**, the VB-series camera beeps periodically when the battery level is critically low, that is less than 10 minutes of recording remains.
- If **Sound alarm when recording starts or stops** is set to **Yes**, the VB-series camera beeps when recording starts.
- If **Sound alarm regularly while recording** is set to **Yes**, the VB-series camera regularly beeps while recording video.

  Administrators can configure the interval at which the alarm sounds.
- If **Enable alarms in hush mode** is set to **Yes**, any alarms that have been configured in the previous settings still make a noise when the camera is in hush mode.

- If **Blink LED in standby** is set to **Yes**, a VB-series camera blinks when it is in standby mode. It enters standby mode when it has been idle, that is assigned and undocked, but not recording, for a period of time.
- If **Show front LEDs when recording VB300** is set to **Yes**, the LEDs of the VB-series camera are turned on during recording.
- If **Show LEDs when recording X-100/X-200** is set to **Yes**, the LEDs of the X-100/X-200 are turned on during recording.
- If **Enable X-100/X-200 buzzer** is set to **Yes**, X-100s and X-200s have haptic feedback.

Power Management

Power Management section enables administrators to configure advanced battery life management.

- If **Power off when idle** is set to **Yes**, the administrator can configure for how many hours the VB-series camera must be away from the charger, after which it powers off.

  The action preserves battery life. However, the camera must be manually powered on before it can record, which can be done by pressing any button on the body-worn camera.

Recording Behaviour

Recording Behaviour section controls how the VB-series camera acts when it is recording.

- If **Show video metadata overlay** is set to **Yes**, metadata is shown over all media files recorded on cameras which inhabit the 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 Configuring Video Metadata Overlay Settings on page 167.
- If **Overwrite oldest footage when full** is set to **Yes**, the camera overwrites the oldest media with newer media if it has run out of storage space.

  If set to **No**, the camera stops recording after it runs out of storage space.
- If **Pre-record** is set to **Yes**, pre-recording media is enabled.

  When pre-record is enabled, the following options are available:

  - In the **Seconds** field, the administrator must enter the number of seconds for which the VB300 pre-records. The default is 30 seconds, and the upper limit is 120 seconds.
  - From the drop-down list, the administrator must select when pre-record starts. The options are as follows:
    - **Always pre-record when not charging** – Pre-record is enabled as soon as the camera is undocked.
    - **Manually start/stop pre-record** – The administrator must manually configure an action which, when performed, starts pre-record. The action can be done from the **Controls** pane.
- From the **Record audio** drop-down list, the administrator can select whether their body-worn cameras record audio or not. The options are as follows:
  - **Yes** – Audio is recorded during both pre-record and normal recording.
  - **No** – No audio is recorded.
  - **Yes (except during pre-record)** – Audio is only recorded during normal recording.

    NOTE: The option is only available if pre-record is enabled.
  - **Require double consent** – The user must go through two steps before audio can be recorded. Firstly, they must start recording with their camera, and then they must perform another gesture, as defined in the **Controls** pane, before the audio can be recorded alongside a media file.

Video Settings

Video Settings section controls video resolution and frame rate.

- From the **Video resolution** drop-down list, the administrator can select the video resolution of media files recorded on cameras that inhabit the 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** drop-down list, the administrator can select the frame rate in which cameras inhabiting the device profile records. There are two options: **25FPS** or **30FPS**.
- If **Enhanced night vision** is set to **Yes**, the frame rate is cut in half and the exposure time is doubled, which produces more well-lit media but should only be used if the VB-series camera is mounted on a stable surface.

Controls

Controls section controls which gestures and actions are associated with the buttons of an X-100, X-200, and VB300.

To map a button gesture onto an action, the administrator must identify the relevant button and gesture from the **Control** column. By using the corresponding **Action** drop-downs list, the administrator must select the action to be performed when the button 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 recording, recording stops when the gesture is performed. If the VB300 is not recording when the gesture is pressed, recording starts.
- **Start recording** – The gesture starts recording. If recording is 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 places a bookmark in the media file. After the media file is downloaded to VideoManager, users can skip straight to the bookmark while viewing it.
  For more information, see Creating, Editing, and Deleting Bookmarks on page 82.
- **Enter hush mode** – The VB300 enters hush mode. LEDs turn off and alarms do not sound. If the VB300 is in hush mode, the gesture does nothing.
- **Exit hush mode** – The VB300 exits hush mode. LEDs turn on and alarms 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 exits hush mode. If the VB300 is not in hush mode when the gesture is performed, it enters hush mode.

The following drop-down options are only visible if **Pre-record** is set to **Yes** in the **Recording Behaviour** pane:

- **Start pre-record** – The gesture starts pre-recording. The length of the pre-record depends on the configuration in the **Recording Behaviour** pane.
- **Stop pre-record** – The gesture stops pre-recording and the pre-recorded media is discarded.
- **Toggle pre-record** – If the camera is pre-recording, the gesture stops pre-recording. If the camera is not pre-recording, the gesture starts pre-recording.

In the **Controls** section, there is an option to make the **WiFi connection** either **Automatic** or **Manual**. If set to **Automatic**, the VB300 searches for WiFi upon powering on. If set to **Manual**, the VB300 must be ordered to

search for WiFi by using a button gesture, which is why more options appear in the drop-down list dictating what action the button performs.

- **Connect to WiFi** – The gesture prompts the VB300 to start searching for WiFi. If the VB300 is connected to WiFi, the gesture does nothing.
- **Disconnect from WiFi** – The gesture disconnects the VB300 from WiFi. If the VB300 is not connected to WiFi, the gesture does nothing.
- **Toggle WiFi connection** – The gesture changes the state of the WiFi connection. If the WiFi was turned off, it will be turned on, and vice versa.

X-100/X-200

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 to be performed as a result, such as **No action**. To map the gesture to an action, the user must use the **Action** drop-down list. The options are the same as in the VB300 section.

B.3 Viewing the VT-Series Camera Device Profile

The device profile section for a VT-series camera has only one section: **Recording Behaviour**.

Procedure:

1. Navigate to the **Admin** tab.
2. Select the **Devices** pane.
3. Click the **Device Profiles** section.
4. Click **Create profile**.
5. In the **Details** pane, from the **Device family** drop-down list, select **VT50 / 100**.
6. Optional: If you want all VT-series cameras in the device profile to record media files with burned-in metadata, set **Show video metadata overlay** to **On**.

   Administrators can configure what information should be included in the metadata from the **Video metadata overlay settings** section of the **Devices** pane, in the **Admin** tab.
   For more information, see Configuring Video Metadata Overlay Settings on page 167.
7. Optional: From the **Time Zone** drop-down list, select the time zone for VB400s in the device profile.

   The action affects video metadata. If left as the default, video metadata is either dictated by the time zone of the associated dock or, if the time zone of the dock is not set, the system time zone of VideoManager.
   For more information, see Setting the System Time Zone of VideoManager on page 287.

B.4 M500 Device Profile

The device profile section for M500 is split into the following tabs: **General**, **Device**, **Recording**, and **Network**.

To view the relevant settings, perform the following actions:

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. In the **Details** pane, from the **Device family** drop-down list, select **M500**.

The tabs are now available.

B.4.1
General Tab

You can perform the following actions in the **General** tab:

- From the **Time Zone** drop-down list, you can specify the time zone in which your M500s are operating.
- From the **Temperature units** drop-down list, you can specify whether the ambient temperature of the car is reported in **Fahrenheit** or **Celcius**.
- From the **Distance units** drop-down list, you can specify whether the distance covered by the car is reported in **Kilometers** or **Miles**.
- From the **Locale** drop-down list, you can specify the language of a place where your agency is located. The selected locale determines the date format for the device and its events.
- From the **Login mode** drop-down list, you can select between **User interface** and **RFID**.
- If **Auto-logout on shutdown** is set to **On**, the officer is automatically logged out when the M500 shuts down, and must log on again at next boot. If set to **Off**, the last logged in officer remains logged, which can impact evidential chain of custody.

B.4.2
Device Tab

The actions that you can perform in the **Device** tab are divided into the following sections:

Artificial Intelligence (AI)

If you set **Enable AI** to **On**, you can perform the following actions:

- You can set **Enable Automatic License Plate Recognition (ALPR) feature** to **On**.
- From the **Show plate detections** drop-down list, you can select when boxes around the capture licence plates on the device should be displayed.
- If **Enable auto-record on backseat passenger detection** is set to **On**, if a human form is detected, the cabin camera will be included in an active recorded event.
- If **Prevent override of backseat passenger detection** is set to **On**, users cannot override the AI decision to include the cabin camera in an event.

On-Screen Text Management

You can select which information is presented to the M500 user as text on the screen.

GPS

- If **Include vehicle speed in metadata file** is set to **On**, speed information is stored in the metadata file of videos recorded on M500s with this device profile.

In-Car Officer Permissions

- If **Allow modification of date/time** is set to **On**, users are able to manually change the date and time of the M500.
- From the **Review video** drop-down list, you can select which videos can be reviewed on the M500 by users:
  - By selecting **No video review access**, users cannot review videos on the M500. They still may be able to do so on VideoManager, depending on their permissions.
  - By selecting **Only video since last login**, users can only review videos on the M500 which were recorded since they last logged on.
  - By selecting **Access to all videos**, users can review all videos stored on the HDD of the M500 (normally around 4–5 days).

Power Behavior

- If **Power DVR ON automatically with ignition** is set to **On**, the M500 turns on automatically when the vehicle ignition is started.
- If **Power DVR OFF automatically with ignition** is set to **On**, the M500 turns off automatically when the vehicle ignition is turned off. If a time has been set from the **Ignition shutdown timer** field, then the M500 shuts down after this timer expires.
- If **Allow DVR to power OFF while ignition is on** is set to **On**, the M500 can be turned off even if the ignition is on.
- If **Stop recording when Ignition Shutdown Timer expires** is set to **On**, the M500 stops recording when the ignition is stopped, and the shutdown timer has expired.
- In the **Ignition shutdown timer** field, you can enter the number of minutes for which the M500 stays on after the ignition is turned off.
- In the **Wireless transfer shutdown timer** field, you can enter the number of minutes for which the M500 continues to wirelessly offload footage to VideoManager after the ignition is turned off. The value entered here is added to the time already configured from the **Ignition shutdown timer** field.

  NOTE: If there is no footage to offload, the M500 powers down immediately.

Other

- If **Blank screen on movement** is set to **On**, the screen on M500 immediately shows a static M500 splash screen when it detects the car moving. No moving images are shown.
- If **Allow covert mode** is set to **On**, the M500 enters covert mode when the **On** button is held down for a few seconds. In this mode, the screen and button LEDs go off, but the M500 does not make any noise.

B.4.3
Recording Tab

The actions that you can perform in the **Recording** tab are divided into the following sections:

Recording Settings

- If **Require logged-in user for recording** is set to **On**, the M500 cannot record unless a user logs on first.
- If **Reminder alerts when active recording** is set to **On**, you can configure how often the M500 alerts the user to the fact that an event is being recorded, via a beep. The intention is to prompt an officer to stop the event recording when appropriate.

- From the **Pre-event record time** drop-down list, you can select how much footage the M500 retains from the period before recording was initiated.
- In the **USB events rewrite time** field, you can specify the period of time after which the M500 starts re-writing footage to a USB stick.

  NOTE: Normally, when a piece of M500 footage is exported to a USB stick, the M500 “marks” the footage so that it is not exported again. However, after the time period specified in this field, the M500 “unmarks” the footage and re-exports it to a USB stick, if the USB stick is inserted.

Camera

- If **Enable Record-After-The-Fact (RATF)** is set to **On**, the M500 continuously records and saves videos in a continuous loop until the hard drive is full, after which, it records over the oldest footage. But it does not record over event recordings that have not yet been uploaded.
  - If set to **On**, the **Configure RATF maximum retention period for non-event footage** toggle appears. If set to **On**, you can configure the number of days for which the non-event video files should be retained in the storage.
- If **Stop recording confirmation** is set to **On**, officers must press the stop button twice to stop a recorded event.
- If **Allow Priority Offload** is set to **On**, users can prioritize a chosen event for upload.
- If **Use critical rules to determine quality** is set to **On**:
  - Videos tagged with a critical event category are saved in the configured primary stream resolution.
  - Videos tagged with a non-critical event category are saved in the configured secondary stream resolution.
- If **Allow increased video quality** is set to **On**, the user can manually upgrade the resolution of a video tagged with a non-critical event category.
- If **Lens distortion correction** is set to **On**, the fisheye effect is reduced. If set to **Off**, the distortion correction is removed to provide a full available field of view.
- If **Keep background video** is set to **On**, M500 uploads media from background cameras by default. The device operator can override this setting at the point of stopping a recording.

Watermarks

- If **Motorola Solutions logo** is set to **On**, the Motorola Solutions logo appears over every frame of a video recorded on the M500.
- If **Time stamp watermark** is set to **On**, a time stamp appears over every frame of a video recorded on the M500.
- If **Device identifier watermark** is set to **On**, the serial number of the M500 appears over every frame of a video recorded on the M500.

Front Camera, Front Camera Wide, Cabin Camera, Rear Camera, Left Camera, and Right Camera

You can configure the resolution, quality, and frame rate for each camera and corresponding stream.

NOTE: Selecting a higher video quality results in larger storage space needs.

The following table lists the supported video quality options for the M500 system camera views with their storage space needs.

Table 3: Supported Video Quality Options for the M500 System Camera

Video Quality	Video Resolution	Frames per Second	Storage Space (GB per Hour)
HD high resolution	1920 x 1080	30	4.50
		15	2.25
		10	1.50
		5	0.75
	1280 x 720	30	2.25
		15	1.125
		10	0.75
		5	0.375
HD medium resolution	1920 x 1080	30	3.60
		15	1.80
		10	1.20
		5	0.60
	1280 x 720	30	1.80
		15	0.90
		10	0.60
		5	0.30
HD low resolution	1920 x 1080	30	2.70
		15	1.35
		10	0.90
		5	0.45
	1280 x 720	30	1.35
		15	0.675
		10	0.45
		5	0.225
SD high resolution	864 x 480	30	0.90
		15	0.45
		10	0.30
		5	0.15
SD medium resolution	864 x 480	30	0.675
		15	0.338
		10	0.225
		5	0.113
SD low resolution	864 x 480	30	0.45
		15	0.225
		10	0.15

Video Quality	Video Resolution	Frames per Second	Storage Space (GB per Hour)
		5	0.075

You can also configure whether users can turn off the front camera wide, cabin camera or rear camera by using the **User permissions** drop-down list. The options are as follows:

- By selecting **Camera on or off**, **Camera on or background** or **Camera on, off or background**, officers can turn off the camera from the control panel.
- By selecting **Force camera on**, users cannot change the camera state from the M500. The camera remains on if the M500 system is on. Users are not allowed to turn off the camera.

  NOTE: The front camera is always on and cannot be turned off.

Wired 1 Microphone, Wired 2 Microphone, and Cabin Camera Microphone

- If **Allow muting** is set to **On**, users can turn off the relevant microphone regardless of recording status.
- From the **Recording** drop-down list, you can select when the relevant microphone should capture audio. The options are as follows:
  - **Always on**
  - **During event recording**
  - **Never**
- If **Unmute at start of recording** is set to **On**, the relevant microphone unmutes itself upon recording, even if the user has manually turned it off.

Auto-Start Record

You can configure which in-car events trigger the M500 to start recording automatically.

- If **Patrol speed** is enabled, you can configure the speed in MPH/KPH which triggers recording.
- If **Use delay** is enabled for Lights/Siren/Auxiliary 1 input/Auxiliary 2 input, you can select from the **Delay** drop-down list how much of a delay there is between the event and the M500 initiating recording.

Auto-Stop Record

- From the **Prompt for stop** drop-down list, you can select how long the M500 waits after recording is automatically started, to prompt the user to stop recording.
- If **Maximum recorded event time** is set to **On**, you can configure the maximum length of the video recorded on an M500, before recording is stopped automatically.

Recording Groups

If **Group member start** is set to **On**, the M500 starts a recorded event when informed by another group member that the other group member has started an event.

Peer Assisted Recording

Peer Assisted Recording (PAR) automatically activates other M500 cameras when they come into range, which allows to capture multiple viewpoints of the same incident. If you enable PAR, the following fields appear:

- If **PAR beacon timeout** is set to **Yes**, you can specify the period of time after a camera starts recording for which it will trigger nearby cameras to start recording as well.

- From the **PAR proximity** drop-down list, you can specify the approximate maximum distance between a camera that is recording and other cameras to be triggered to start recording as well.

Event Tags

In the **Assigned event tags** table, you can optionally enable the previously created event tags.

B.4.4 Network Tab

The actions that you can perform in the **Network** tab are divided into the following sections:

Domain Name

By default, your M500 connects to VideoManager by using the public address of VideoManager.

- If you want your M500 to connect to VideoManager via another address, you can set **Use custom address** to **On**. By enabling this option, you must enter the following information:
  - Domain name
  - Port
- If **Secondary address** is set to **On**, you must enter the following information:
  - Domain name
  - Port

  Optionally, you can set **Treat as LTE** to **On** if you want the secondary address to be assumed to be an LTE upload address.

DNS Server

In this section, you can enter the IP addresses of the DNS server and secondary DNS server.

Streaming and Location Options

From the **Enable streaming** drop-down list, you can select between **None**, **Location only**, or **Location and live streaming**.

If you select **Location and live streaming**, the **Live stream configuration** section appears.

Live Stream Configuration

You can set **Enable stream outside of recording** to **On**.

B.5 V700 Device Profile

The device profile section for V700 is split into the following tabs: **General**, **Device**, **Recording**, and **Network**.

To view the relevant settings, perform the following actions:

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. In the **Details** pane, from the **Device family** drop-down list, select **V700**.

The tabs are now available.

B.5.1
General Tab

The actions that you can perform in the **General** tab are divided into the following sections:

General Settings

- From the **Time Zone** drop-down list, you can specify the time zone in which your V700s are operating.
- From the **Locale** drop-down list, you can specify the language of a place where your agency is located. The selected locale determines the date format for the device and its events.

Integrations

- If **APX radio integration** is set to **On**, the V700 starts a recorded event when a paired APX radio enters emergency mode.
- If **SmartControl Integration** is set to **On**, the V700 can integrate with SmartControl, on a smartphone and/or on a PC.
- If **SmartControl for PC Security** is set to **On**, you must enter the PC Administrator password. The password must have at least one lowercase letter, one uppercase letter, one number, and be between 8 and 63 characters. It cannot contain spaces.

  IMPORTANT: Disabling the **SmartControl for PC Security** feature allows unprotected review of events on a V700 camera connected to SmartControl on a PC.
- If **SmartControl for Mobile Security** is set to **On**, you must enter the Mobile Administrator password. The password must have at least one lowercase letter, one uppercase letter, one number, and be between 8 and 63 characters. It cannot contain spaces.

  IMPORTANT: Disabling the **SmartControl for Mobile Security** feature allows unprotected review of events on a V700 camera connected to SmartControl on a mobile.

B.5.2
Device Tab

The actions that you can perform in the **Device** tab are divided into the following sections:

GPS

You can enable or disable GPS by setting the **GPS Enabled** toggle to either **On** or **Off**.

Sensors

You can enable the use of sensors with the V700, such as holster trigger, by setting **Enable sensors** to **On**.

Other

If **Allow covert mode** is set to **On**, officers can enable or disable Covert Mode on the V700.

B.5.3
Recording Tab

The actions that you can perform in the **Recording** tab are divided into the following sections:

Camera

- If **Enable Record-After-The-Fact (RATF)** is set to **On**, the V700 continuously records and saves videos in a continuous loop until the hard drive is full, after which, it records over the oldest footage. But it does not record over event recordings that have not yet been uploaded.
  - If set to **On**, the **Clear non-event RATF footage on assignment** toggle appears. If set to **On**, buffered non-event video files are deleted from its storage at checkout.
- From the **Manual start recording** drop-down list, you can configure the **Record Start/Stop** button to manually start a recorded event. The options are as follows: **Short press**, **Long press**, or **Press twice (confirmation)**.
- From the **Manual stop recording** drop-down list, you can configure the **Record Start/Stop** button to manually stop a recorded event. The options are as follows: **Short press**, **Long press**, or **Press twice (confirmation)**.
- If **Lens distortion correction** is set to **On**, the fisheye effect is reduced. If set to **Off**, the distortion correction is removed to provide a full available field of view.
- If **Enable bookmark** is set to **On**, the user can place a bookmark in the media file.
  For more information, see Creating, Editing, and Deleting Bookmarks on page 82.
- If **Enable capture image** is set to **On**, the user can take a screenshot of the video that the V700 is recording.

Microphone Settings

- If **Allow muting** is set to **On**, users can turn off the relevant microphone regardless of recording status.
- From the **Recording** drop-down list, you can select when the relevant microphone should capture audio. The options are as follows:
  - **Always on**
  - **During event recording**
  - **Never**
- If **Allow primary microphone continuous mute** is set to **On**, officers can continuously mute the V700 audio recording.
- If **Enable maximum continuous mute time limit** is set to **On**, you can set the continuous mute duration limit.
  The continuous mute duration limit can be 1 to 480 minutes.
- If **Enable mute periodic alert** is set to **On**, you can set the reminder interval for the V700 to remind officers that the audio recording is muted.
  The reminder interval can be from 6 seconds to 60 minutes.

Watermarks

- If **Motorola Solutions logo** is set to **On**, the Motorola Solutions logo appears over every frame of a video recorded on the V700.
- If **Time stamp watermark** is set to **On**, a time stamp appears over every frame of a video recorded on the V700.

- If **Device identifier watermark** is set to **On**, the serial number of the V700 appears over every frame of a video recorded on the V700.

Front Camera

You can configure the resolution, quality, and frame rate for the front camera and corresponding stream.

NOTE: Selecting a higher video quality results in larger storage space needs.

The following table lists the supported video quality options for the V700 system camera views with their storage space needs.

Table 4: Supported Video Quality Options for the V700 System Camera

Video Quality	Video Resolution	Frames per Second	Storage Space (GB per Hour)
HD high resolution	1920 x 1080	30	4.50
		15	2.25
		10	1.50
		5	0.75
	1280 x 720	30	2.25
		15	1.125
		10	0.75
		5	0.375
HD medium resolution	1920 x 1080	30	3.60
		15	1.80
		10	1.20
		5	0.60
	1280 x 720	30	1.80
		15	0.90
		10	0.60
		5	0.30
HD low resolution	1920 x 1080	30	2.70
		15	1.35
		10	0.90
		5	0.45
	1280 x 720	30	1.35
		15	0.675
		10	0.45
		5	0.225
SD high resolution	864 x 480	30	0.90
		15	0.45
		10	0.30

Video Quality	Video Resolution	Frames per Second	Storage Space (GB per Hour)
		5	0.15
SD medium resolution	864 x 480	30	0.675
		15	0.338
		10	0.225
		5	0.113
SD low resolution	864 x 480	30	0.45
		15	0.225
		10	0.15
		5	0.075

Recording Reminder Alerts

If **Active recording** is set to **On**, you can configure how often the V700 alerts the user to the fact that an event is being recorded, via a beep. The intention is to prompt an officer to stop the event recording when appropriate.

Additional Record Time

From the **Pre-event time** drop-down list, you can select how much footage the V700 retains from the period before recording was initiated.

Recording Groups

- If **Group member start** is set to **On**, the V700 starts a recorded event when informed by another group member that the other group member has started an event.
- If **Group member stop** is set to **On**, the V700 stops a recorded event when informed by another group member that the other group member has stopped an event.
- If **Allow manual stop** is set to **On**, the V700 can manually stop the recorded event while other group members continue to record the event.

Event Tags

In the **Assigned event tags** table, you can optionally enable the previously created event tags.

B.5.4
Network Tab

The actions that you can perform in the **Network** tab are divided into the following sections:

Domain Name

By default, your V700 connects to VideoManager by using the public address of VideoManager.

- If you want your V700 to connect to VideoManager via another address, you can set **Use custom address** to **On**. By enabling this option, you must enter the following information:
  - Domain name
  - Port

DNS Server

In this section, you can enter the IP address of the DNS server.

WiFi

- From the **Enable streaming** drop-down list, you can select between **None**, **Location only**, or **Location and live streaming**.
  If you select **Location and live streaming**, the **Live stream configuration** section appears.
- From the **Enable offload** drop-down list, you can select between **Auto**, **Manual**, or **None**.
  If you select **Auto** or **Manual**, the **Offload event types** drop-down list appears where you can select between **Critical** or **All**.

LTE

- If **Enable roaming** is set to **On**, the V700 can use the LTE connection to stream or upload the footage.
- From the **Enable streaming** drop-down list, you can select between **None**, **Location only**, or **Location and live streaming**
- From the **Enable offload** drop-down list, you can select between **Auto**, **Manual**, or **None**.
  If you select **Auto** or **Manual**, the **Offload event types** drop-down list appears where you can select between **Critical** or **All**.
- If **Set custom APN settings** is set to **On**, the following fields appear that you should fill in to provide all the details that your V700 needs to connect to mobile data:
  - **Access point name**
  - From the **Authentication type** drop-down list, you can select between **CHAP** (Challenge Handshake Authentication) or **PAP** (Password Authentication Protocol).
  - **Username**
  - **Password**

Live Stream Configuration

You can set **Enable stream outside of recording** to **On**.

B.6
V500 Device Profile

The device profile section for a V500 is split into the following sections: **Details**, **Notifications & Alarms**, **Recording Behaviour**, **Video Settings**, **Audio Settings**, **Live-streaming**, and **Controls**.

To view the relevant settings, perform the following actions:

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. In the **Details** pane, from the **Device family** drop-down list, select **V500**.

The following settings are now available.

Notifications & Alarms

Notifications & Alarms section enables administrators to customise how the V500 alerts its operator to various states and events.

- If **Sound alarm when storage nearly full** is set to **Yes**, the V500 beeps periodically when the storage space is low.
- If **Sound alarm when battery level critical** is set to **Yes**, the V500 beeps periodically when the battery level is critically low, that is less than 10 minutes of recording remains.
- If **Shoulder LED enabled while recording** is set to **No**, the shoulder LED is turned off while recording.
  By default, the shoulder LED is turned on while recording.
- The administrator can customise how a V500 behaves when in normal mode and hush mode by 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 **Yes**, LEDs indicate when a camera starts and stops recording/pre-recording.
  - If **Enable beeps** is set to **Yes**, sounds indicate when a camera starts and stops recording/pre-recording.
  - If **Enable vibrate** is set to **Yes**, haptic feedback indicates when a camera starts and stops recording/pre-recording.
  - If **Enable X-Series LEDs** is set to **Yes**, any X-series cameras connected to V500s in the device profile have their LEDs enabled to indicate when they are recording.
  - If **Enable X-Series vibrate** is set to **Yes**, any X-series cameras connected to V500s in the device profile have haptic feedback enabled to indicate when they start recording.
- If **Recording alarm** is set to **Yes**, a V500 alerts the user periodically while it is recording.
  In the **Seconds** field, administrators can configure the interval at which the alarm should sound (between 5 and 600 seconds).

Recording Behaviour

Recording Behaviour section controls how the V500 acts when it is recording.

- If **Show video metadata overlay** is set to **Yes**, metadata is shown over all media files recorded on cameras which inhabit the 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 Configuring Video Metadata Overlay Settings on page 167.
- If **Overwrite oldest footage when full** is set to **Yes**, the camera overwrites the oldest media with newer media if it has run out of storage space.
  If set to **No**, the camera stops recording after it runs out of storage space.
- From the **Recording policy** drop-down list, the administrator must determine whether the V500 starts recording automatically from undock, or it must be manually prompted to start recording. The options are as follows:
  - **Controlled by gesture** – The V500 does not start recording automatically. The operator must prompt it to record by using the gesture determined in the **Controls** section. Alternatively, the V500 can be prompted to start recording via peer-assisted recording or a Bluetooth Peripheral.
  - **While not docked** – The V500 starts recording automatically, as soon as it is undocked. It continues to record until it runs out of battery, or is redocked again. The user cannot stop recording manually, even if gesture(s) have been configured in the **Controls** section.

- **Start once on undocking, then gesture controlled** – The V500 starts recording automatically, as soon as it is undocked. The operator can then stop and start recording manually by using the gesture(s) determined in the **Controls** section. Alternatively, the V500 can be prompted to start recording via peer-assisted recording or a Bluetooth Peripheral.

- If **Allow recording in hush mode** is set to **Yes**, the camera can record media while in hush mode. The camera can also enter hush mode while recording.

  If set to **No**, if the camera is in hush mode and the operator performs the gesture that prompts their body-worn camera to start recording, the camera exits hush mode. If the camera is recording and the operator performs the gesture that prompts their camera to enter hush mode, the camera stops recording.

  NOTE: Pre-record still works in hush mode, even if **Allow recording in hush mode** is set to **No**.

- If **Pre-record** is set to **Yes**, pre-recording media is enabled.

  When pre-record is enabled, the following options are available:

  - In the **Seconds** field, the administrator must enter the number of seconds for which the V500 pre-records. The default is 30 seconds, and the upper limit is 120 seconds.
  - From the drop-down list, the administrator must select when pre-record starts. The options are as follows:
    - **Always pre-record when not charging** – Pre-record is enabled as soon as the camera is undocked.
    - **Manually start/stop pre-record** – The administrator must manually configure an action that, when performed, starts pre-record. The action can be done from the **Controls** pane.
  - The administrator can set **Post-record** to **Yes**.

    In the **Seconds** field, the administrator must enter the number of seconds for which the V500 post-records. The default is 30 seconds, and the upper limit is 120 seconds.

- From the **Record audio** drop-down list, the administrator can select whether their body-worn cameras record audio or not. The options are as follows:
  - **Yes** – Audio is recorded during both pre-record and normal recording.
  - **Yes (except during pre-record)** – Audio is not recorded during pre-precord.
  - **No** – Audio is not recorded during pre-record or normal recording, and cannot be heard when viewing live streams.

- If **Enable GPS** is set to **Yes**, GPS location data is recorded alongside any media file.

  NOTE: GPS location data is captured by V500s in one-second intervals.

  If set to **No**, the user can still add location data to the media files after they have been downloaded to VideoManager.

- If **Capture image on bookmark** is set to **Yes**, the V500 takes a screenshot of the video it is recording at the same time as it captures a bookmark. The screenshot is downloaded to VideoManager as a JPEG after the V500 is redocked.

  NOTE: A bookmark gesture must be selected from the **Controls** section, or else the configuration does not have any effect.

- In the **Video length** field, the administrator must enter the number of minutes for which a V500 can record, after which the media is split into multiple media files.

  The administrator can select between 5 and 30 minutes.

- In the **Suppress recording on undock** field, the administrator must enter the number of seconds for which the camera is prevented from recording after it is undocked, which means that in the configured period of time, the camera ignores any gestures that would normally prompt it to record.

  NOTE: The action applies to recordings that would be started by Bluetooth Peripherals.

- From the **Time Zone** drop-down list, the administrator can select the time zone for V500s in the device profile, which affects video metadata and filenames. If left as the default, video metadata and filenames either are dictated by the time zone of the associated dock or, if the time zone of the dock is not set, the system time zone of VideoManager.

  For more information, see Setting the System Time Zone of VideoManager on page 287.

Video Settings

Video Settings section controls video resolution and frame rate.

- From the **Video resolution** drop-down list, the administrator can select the video resolution of media files recorded on cameras that inhabit the 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** drop-down list, the administrator can select the frame rate in which a V500 records. The options are as follows: **25** or **30**.

Audio Settings

Audio Settings section controls the audio options.

- From the **Audio profile** drop-down list, the administrator must select which audio profile should be used by V500s in the device profile. The options are as follows:
  - **Mostly outdoor** profile is ideal if the majority of recording takes place outdoors.
  - **Mostly indoor** profile is ideal if the majority of recording takes place indoors.

Live-streaming

Setting **Enable Two-way Audio** to **Yes** enables two-way audio communication with a live-streaming device.

Mobile App Settings

Mobile App Settings section controls whether the Mobile App can be used with a V500.

- From the **Enable mobile app** drop-down list, the administrator can either select **None** or **VB SmartControl**.

  If you select **VB SmartControl**, the **Connection** drop-down list appears with **WiFi Access Point** as the default.

For more information about setting up the Mobile App with VideoManager, you can navigate to https://www.motorolasolutions.com/en_xu.html and search for *VideoManager: VB SmartControl User Guide*.

Controls

Controls section enables administrators to configure the buttons and gestures.

- From the **Hold timing** drop-down list, the administrator can select how long an operator must hold the button on a V500 for the camera to register the gesture as a "hold". The options are: **Long**, **Normal**, or **Short**.
- From the **Double click timing** drop-down list, the administrator can select how quickly an operator must double-click the button on a V500 for the camera to register the gesture as a "double-click". The options are: **Slow**, **Normal**, or **Fast**.

V500

Administrators can map the following V500 buttons: **Front**, **Programmable 0 (P0)**, **Programmable 1 (P1)**, and **Programmable 2 (P2)** to gestures such as: **Press**, **Hold**, and **Double click**.

To map a button gesture onto an action, the administrator must identify the relevant button and gesture from the **Control** column. By using the corresponding **Action** drop-down list, the administrator must select the action to be performed when the button gesture is performed. The options are as follows:

- **No action** – The gesture does nothing.
- **Start recording** – The gesture starts recording. If recording is in progress, the gesture does nothing.
- **Stop recording** – The gesture stops recording. If recording is not in progress, the gesture does nothing.
- **Start/stop recording** – The gesture changes recording mode. If the V500 is recording, recording stops when the gesture is performed. If the V500 is not recording when the gesture is pressed, recording starts.
- **Record bookmark** – The gesture places a bookmark in the media file. After the media file is 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 media file. Users can place bookmarks into media files on VideoManager, but they must be in an incident first.

  For more information, see Creating, Editing, and Deleting Bookmarks on page 82.

  NOTE: If **Capture image on bookmark** is set to **Yes** in the **Recording Behaviour** section, the gesture prompts the V500 to take a screenshot of the video.
- **Enter hush mode** – The V500 enters hush mode. While in hush mode, the V500 obeys the settings configured in the **When in hush mode** row of the **Notifications & Alarms** pane.
- **Exit hush mode** – The V500 exits hush mode. Without hush mode, the V500 obeys 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.
- **Show backlight** – The gesture causes the V500 to display backlight.
  For more information, see "LEDs and Display Backlight Overview" in the *V500 Body Camera User Guide*.
- **Mute alarms** – The gesture mutes all audio notifications.
  If selected, the administrator must also select **Unmute alarms** for a different button.
- **Unmute alarms** – The gesture unmutes all audio notifications.
  If selected, the administrator must also select **Mute alarms** for a different button.
- **Toggle mute alarms** – The gesture allows to toggle all audio notifications.

The following drop-down options are only visible if **Pre-record** is set to **Yes** in the **Recording Behaviour** pane:

- **Start pre-record** – The gesture starts pre-recording. The length of the pre-record depends on the configuration in the **Recording Behaviour** pane.
- **Stop pre-record** – The gesture stops pre-recording and the pre-recorded media is discarded.
- **Toggle pre-record** – If the camera is pre-recording, the gesture stops pre-recording. If the camera is not pre-recording, the gesture starts pre-recording.

Administrators can also map the **Power button** to a **Hold** gesture to which they can map one of the following actions:

- **No action** – The gesture does nothing.
- **Shutdown** – The V500 stops recording and shuts down.

In the **Controls** section, there is an option to make the **WiFi connection** and **Mobile network connection** either **Automatic** or **Manual**. If set to **Automatic**, the V500 searches for WiFi/mobile network upon powering on. If set to **Manual**, the V500 must be ordered to search for WiFi/mobile network by using a button gesture, which is why more options appear in the drop-down list dictating what action the button performs.

- **Connect to WiFi**/**Connect to mobile network** – The gesture prompts the V500 to start searching for WiFi/mobile network. If the V500 is connected to WiFi/mobile network, the gesture does nothing.
- **Disconnect from WiFi**/**Disconnect from mobile network** – The gesture disconnects the V500 from WiFi/mobile network. If the V500 is not connected to WiFi/mobile network, the gesture does nothing.
- **Toggle WiFi connection**/**Toggle mobile network connection** – The gesture changes the state of the WiFi/mobile network connection. If the WiFi/mobile network was turned off, it will be turned on, and vice versa.

X-100/X-200

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 to be performed as a result. To map the gesture to an action, the administrator must use the **Action** drop-down list. The options are the same as in the V500 section, except for the **Mute alarms**, **Unmute alarms**, and **Toggle mute alarms** gestures which are not available.

Appendix C

Types of Reports

VideoManager offers many types of reports. The following appendix covers every type of report that can be created, and the corresponding columns and values they contain.

To download reports as CSV files instead of ZIP, you can navigate to the **Advanced Settings** section of the **System** pane, in the **Admin** tab. In the text box, you must enter `web.reports.filetype=CSV` and click **Save settings**. Now, if you go to the **Reports** pane in the **Status** tab and download a report, it is saved as a CSV file.

Sites

If VideoManager is configured to act as a Central VideoManager, the report returns a list of all sites connected to it, detailing how long in hours the sites have been online/offline.

- **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 the site to the Central VideoManager, including media and metadata

Management

The report returns a high-level overview of key system parameters, including the total hours of media 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 in minutes of recordings captured in the period covered by the report
- **Recordings (MB)** – The total size in MB of recordings captured in the period covered by the report
- **Average recording (length)** – The average length in minutes of recording captured in the period covered by the report
- **Average recording (MB)** – The average size in MB of recording captured in the period covered by the report
- **Media items (total)** – The total number of media. The report includes media files recorded on cameras, and imported media files within the period covered by the report.
- **Media items (length)** – The total length in minutes of media recorded or imported in the period covered by the report
- **Media items (MB)** – The total size in MB of media recorded or imported in the period covered by the report
- **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 that 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 that have cameras assigned to them within the period covered by the report
- **Active Devices** – The number of cameras that have been assigned within the period covered by the report
- **Video Test Failures** – The number of media files 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, it counts as different events in the report.

User Summary

The report returns 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 on/not logged on. If no username is entered, the report presents the information for all users on the system. If scheduled, the 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 the database of VideoManager
- **State** – Whether the user is enabled, that is can log on to VideoManager, or disabled, that is cannot log on to VideoManager
- **Date Assigned with Recording** – The number of days that the user was assigned a camera and recorded media within the period covered by the report
- **Date Assigned without Recording** – The number of days that the user was assigned a camera but did not record media within the period covered by the report
- **Days Not Assigned** – The number of days that the user was not assigned a camera within the period covered by the report
- **Days Logged In** – The number of days that the user logged on to VideoManager within the period covered by the report
- **Days Not Logged In** – The number of days that the user did not log on to VideoManager within the period covered by the report

Incidents

The report returns a list of all incidents that have been created in the period covered by the report. The reports also returns the details for the 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, the report can be copied to the `Report auto-copy` file space.

The columns which users can see depend on how user-defined incident fields are configured. By default, if the administrator has not edited the built-in incident fields, that is has not renamed, deleted, or reordered them, the columns are as follows:

- **ID** – The internal ID for the incident in the database of VideoManager
- **Incident Created** – When the incident was created
- **Last Edited** – When the incident was last edited
- **Title** – The title of the incident
- **Incident time** – The time of the incident, as configured in the **Incident time** field
- **Reference code** – The reference code of the incident, as configured in the **Reference code** field
- **Notes** – The notes of the incident, as configured in the **Notes** field

- Any other user-defined incident fields that the administrator has created appear as separate columns, regardless of whether the fields have been populated in the incidents.

  NOTE: Computed fields are 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 the incident, the column shows the name of the deleted user-defined incident field(s) and the corresponding value(s).
- **Recorded by** – If the incident includes media, the column lists the operator(s) that recorded the media.

Media

The report returns a list of all media files that were recorded on cameras or imported into VideoManager in the period covered by the report. The report also returns the details for the media files, including who recorded them, when the recording started and stopped, the duration of media files, and the serial numbers of the cameras that recorded them. If scheduled, the report can be copied to the `Report auto-copy` file space.

- **URN** – The unique ID of the media file
- **Recording identifier** – The unique recording ID of the media file
- **Recording index** – If the media file is part of a longer recording, the column shows its position in the recording, that is the first media file will be 0, the second media file will be 1, etc.
- **Username** – The user who recorded or imported the media file
- **Badge ID** – The camera that recorded the media file. If the media file was imported, the field reads as `import`.
- **Start time** – When the media file started
- **End time** – When the media file ended
- **Duration** – How long the media file is
- **Quality** – The resolution and FPS of the media file
- **Data size (MB)** – The size in MB of the media file
- **Bookmarked?** – Whether the media file was bookmarked in the field
- **In incident?** – Whether the media file is in an incident
- **Deleted?** – Whether the media file has been deleted from VideoManager
- **SHA-256** – The SHA-256 hash of the media file

User Export

The report returns a list of all users on VideoManager at the time the report was created. The report also returns the details for the users, including their usernames, display names, RFID IDs, and the roles they inhabit. If scheduled, the 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, that is can log on to VideoManager, disabled, that is cannot log on to VideoManager, or deleted
- **RFID** – The Touch Assign ID of the user, if the user has been associated with an RFID card
- **BLE MAC Address** – The BLE MAC Address of the user, if enabled for the report. Users are automatically issued an Address by VideoManager the first time they use Bluetooth, either with the Mobile App, peer-assisted recording, or Bluetooth Peripherals.
- **Roles** – The roles that the user inhabits

Operator Recorder Summary

The report returns a summary of operator activity, that is how many media files have been recorded in the period covered by the report, broken down by operator and date. The report also returns the details for each field trip, including the serial numbers of the cameras, and how many media files were recorded. If scheduled, the report can be copied to the `Report auto-copy` file space.

- **Operator Name** – The name of the operator who recorded the media
- **Device Number** – The serial number of the camera that was used by the operator on the specified date
- **Date** – The date(s) when the operator recorded media
- **Number Of Videos** – The number of media files that 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 media files on the specified date that are shorter than 20 seconds
- **% of videos < 20 secs** – The percentage of media files on the specified date that are shorter than 20 seconds

Equipment

The report returns a list of all equipment associated with the currently used instance of VideoManager, that is cameras, docks, EdgeControllers, Central VideoManager, sites, grid cores, and grid workers. The report also returns the details for the pieces of equipment, including their type, such as VB400, when they were last "seen" by VideoManager, and the software they are running. If scheduled, the report can be copied to the `Report auto-copy` file space.

- **Serial Number** – The serial number of the relevant equipment
- **Type** – The type of equipment, for example, VB400, DC-200, grid
- **Identity or custom status** – The information presented depends on the type of equipment:
  - If the equipment is a camera, the information includes the custom status, as configured from the **Custom status** field.
  - If the equipment is not a camera, the information includes the 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, the timestamp is when the report was run
- **Last connected from** – When the equipment was last connected from VideoManager.
- **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, the field reads as `Central`.
- **Last sub-location** – The dock where the equipment was last detected by VideoManager. If cameras are directly connected to VideoManager via USB, the field reads as `USB`. If cameras are connected to VideoManager via WiFi, the field reads 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 depends on the state of the equipment:
  - If the camera is assigned, the field reads as the operator it is assigned to.
  - If the camera has been forgotten from VideoManager, the field reads as the date when it was forgotten.

  - If equipment was moved from the currently used instance of VideoManager, the field reads as `Moved to another location`.
  - If the site was deleted from VideoManager, the field reads as the date when it was deleted.
- **Hardware Status** – If the equipment is a camera, the information includes the status of the hardware. The column reads as `OK` if the camera has not detected a fault.
- **Name** – The information presented depends on the type of equipment:
  - If the equipment is a camera, the information includes the serial number, unless an administrator has set a name from the **Edit device properties** pane.
    For more information, see Editing Camera Properties on page 114.
  - If the equipment is a dock or site, it is the same value as the one reported in the **Identity or custom status** column.
- **Latitude** – The latitude of the location of a device.
- **Longitude** – The longitude of the location of a device.
- **Last geolocation** – The last geolocation reported by a device while connected remotely to VideoManger. If the device is still connected, it is the current geolocation of the device.
- **ICCID** – The Integrated Circuit Card Identification number of the SIM card.
- **IMEI 1** and **IMEI 2** – The International Mobile Equipment Identity numbers of a dual-SIM device.
- **EID** – The Embedded Identity Document of the eSIM. This only applies to V500s that have had the eSIM provisioned.

Battery Audit

The report details whether the batteries of cameras have degraded. The battery could degrade if the 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, the report can be copied to the `Report auto-copy` file space.

- **Device Name** – The unique device ID of the camera that is experiencing battery issues
- **Event Date** – When VideoManager first registered the battery issue. If the camera powered down unexpectedly in the field, the information includes when it was redocked.
- **Event Type** – The specific kind of battery issue that the camera is experiencing:
  - `battery status` – The camera has detected an issue with charging the battery.
  - `high self discharge` or `self discharge` – The battery charged down quickly while docked after being fully charged. It only applies to VB100, VB200, and VB300 cameras.
  - `limited battery capacity` – The camera was fully charged when undocked, but ran out of charge unexpectedly while in the field. It only applies to VB100, VB200, and VB300 cameras.
- **Summary** gives more detail about the battery issue:
  - If the issue is `battery status`, it provides information about the specific problem with the battery, such as whether it is refusing to charge, charging too slowly, or could not be detected.
  - If the issue is `high self discharge` or `self discharge`, it provides information about when and how much voltage was discharged from the battery while charging, as measured from when the battery was fully charged. For example, `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 issue is `limited battery capacity`, it provides information about when the camera shut down unexpectedly, compared to the expected battery life.

Device Availability

The report returns a list of cameras at each location, such as a dock, in five-minute intervals for the duration of the period covered by the report. The report also returns the number of cameras that are busy, charging, or assigned, and the number of cameras that are available, that is ready to be assigned, at each location. If scheduled, the report can be copied to the `Report auto-copy` file space.

- **Location** – The DC-200 that is being audited. If cameras are directly connected to VideoManager via USB, the field reads as `USB`. If sites have been configured, the field reads as *<site name / Dock name >*, or `USB`.
- **Timestamp** – When VideoManager checked the location, in five-minute intervals
- **Busy** – The number of cameras at the location that are upgrading firmware or downloading media
- **Charging** – The number of cameras at the location that are charging
- **MinimumAvailable** – The minimum number of cameras available for assignment over the course of the five-minute interval
- **Assigned** – The number of cameras at the location that are assigned to users

Device Field Trip

The report returns a list of trips made by cameras within the period covered by the report. The report also returns the details for the trips, including where the cameras were initially docked, where they were redocked after recording, for example, if a camera was redocked to a different dock, and the start/end times of the trips. If scheduled, the 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 camera was undocked. If sites have not been configured, or if the camera was undocked at the Central VideoManager, the field reads as `Central`.
- **End Site** – The site where the camera was redocked. If sites have not been configured, or if the camera was undocked at the Central VideoManager, the field reads as `Central`.
- **Start Location** – The dock where the camera was undocked. If cameras are directly connected to VideoManager via USB, the field reads as `USB`. If cameras are connected to VideoManager via WiFi, the field reads as `Network:` *<WiFi Network Name>*.
- **End Location** – The dock where the camera was redocked. If cameras are directly connected to VideoManager via USB, the field reads as `USB`. If cameras are connected to VideoManager via WiFi, the field reads as `Network:` *<WiFi Network Name>*.
- **Badge ID** – The serial number of the camera that was operated by the user
- **Start time** – When the camera was undocked
- **End time** – When the camera was redocked. If the camera is still in the field, the field reads as `In Field`.
- **Duration** – The length of the field trip, from the camera being undocked to redocked

Operator Activity

The report returns a list of every user on VideoManager who has recorded at least one media file in the period covered by the report. The report also returns the length of the media files from 30 seconds up to over 40 minutes, whether those media files are in incidents or not, the total number of media files recorded by a user, and the combined length of a user's media files. If scheduled, the 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 media files recorded by the operator that 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 media files recorded by the operator that 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 media files recorded by the operator that 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 media files recorded by the operator that 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 media files recorded by the operator that 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 media files recorded by the operator that 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 media files recorded by the operator that 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 media files recorded by the operator that 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 media files recorded by the operator that 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 media files recorded by the operator that 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 that were recorded in the period covered by the report have been added to an incident
- **Total length of recordings** – The total length in seconds of the operator's recordings that were recorded in the period covered by the report
- **Count of cameras booked out** – The number of times that a camera assigned to the user was undocked within the period covered by the report

Full User Export

The report returns information about all users on the system, including their roles, groups, and, optionally, user-specific WiFi networks. The report can be used with the user import tool to import all users from one VideoManager system into another. If scheduled, the 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, that is can log on to VideoManager, or disabled, that is cannot log on to 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** – The Touch Assign ID of the user, if the user has been associated with an RFID card

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 that apply to the exported users/groups.

- **UserOrGroup** – The name of the user/group
- **Role name** – The name of the role on VideoManager that 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 that has some form of oversight over another user/group
- **Relationship** – The kind of oversight that **UserOrGroup1** has, which could be either **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, which could be either **WPA2-PSK**, **WPA-PSK**, **WEP**, **Open**, or **WPA2-PEAP-MSCHAPV2**
- **Identity** – The column is 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** – The columns correspond to the **Band** drop-down list of the WiFi network. The columns are mutually exclusive.
- **Use Static IP**, **IP**, **Network Mask**, **Gateway**, **DNS Server 1**, **DNS Server 2** – The information is only relevant to the network administrator.
- **Signal Threshold** – Corresponds to the **Disconnect on low signal** toggle and is either `true` or `false`
- **Signal Percent** – If the **Signal Threshold** column is populated with `true`, it is the corresponding signal level below which the WiFi network is disconnected from the camera.
- **Signal Threshold Time** – If the **Signal Threshold** column is populated with `true`, it is the corresponding time in seconds that the signal must be weak for after which the WiFi network is disconnected.
- **Hidden Network** – Corresponds with the **Hidden network** toggle and is either `true` or `false`

For more information, see the *Built-in User Import Tool Guide* [ED-012-229], which can be found in the installation location of VideoManager, in the `userimporttool` folder.

Fleet Battery Health Indicator

The report returns the list of cameras that turned off abnormally at least once within 8 hours of being assigned and used by the user, and were fully charged prior to assignment. In most cases, this applies to cameras whose battery has failed and requires replacement.

- **Device Serial no** – The serial number of the device
- **Device Name** – The name of the camera that recorded the media file
- **Device ID** – The unique device ID
- **Last Location** – The site where the device was last detected by VideoManager
- **Last sub-location** – The dock where the device was last detected by VideoManager
- **Shutdown count** – The number of times the camera shut down within 8 hours of receiving a full charge during normal use

Appendix D

Keyboard Shortcuts

Users can utilise keyboard shortcuts to locate the relevant section in a media file.

The following shortcuts can be used when viewing a media file that is part of an incident:

- A – Cycles between on-screen annotations
- E – Edits selected annotation
- K – Navigates to next annotation
- J – Navigates to previous annotation

The following shortcuts can be used either when viewing a media file that is part of an incident, or when viewing a media file from the **Media** pane:

- SPACE, PLAY/PAUSE – Plays/pauses the media player
- R – Plays the media player
- P – Pauses the media player
- LEFT ARROW – Steps forwards
- RIGHT ARROW – Steps backwards
- X – Jumps forward 5 seconds in the clip
- Z – Jumps backward 5 seconds in the clip
- V – Jumps forward 60 seconds in the clip
- C – Jumps backward 60 seconds in the clip
- M – Mutes the media
- F – Toggles fullscreen for player
- T – Toggles theater mode for player
- D – Toggles date time overlay
- S – Downloads a screenshot of the current frame in the player
- 0 – Jumps to start of clip
- 1 – Jumps 10% into clip
- 2 – Jumps 20% into clip
- 3 – Jumps 30% into clip
- 4 – Jumps 40% into clip
- 5 – Jumps 50% into clip
- 6 – Jumps 60% into clip
- 7 – Jumps 70% into clip
- 8 – Jumps 80% into clip
- 9 – Jumps 90% into clip

Appendix E

Custom Predicate Language

The Motorola Solutions custom predicate language is used for a variety of advanced features on VideoManager. The following appendix covers 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 Media** pane,
- Creating incidents automatically based on how user-defined media fields of a media file are populated,
- Deleting incidents automatically based on how user-defined incident fields of an incident are populated,
- Creating rules for an export profile based on how user-defined incident fields of an incident are populated,
- Creating computed fields, which appear and change based on how other user-defined incident fields in an incident are populated.

E.1 Custom Predicate Language and Incident and Media Fields

Motorola Solutions custom predicate language is based around incident and media fields, and how they are populated.

For advanced incident searches, VideoManager can return incidents based on how their built-in and user-defined incident fields are populated.

For advanced media searches, VideoManager can return media files based on how their built-in and user-defined media fields are populated.

For automatic incident creation, incidents can be created based on how their built-in and user-defined incident fields are populated.

For automatic incident deletion, incidents can be deleted based on how their fields have been populated, and how outdated 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 built-in and user-defined incident fields of an incident are populated. Export profile rules are usually formatted as CASE functions. All examples of export profile rules in this documentation are formatted as CASE functions. For more information, see CASE Functions on page 387.

For computed fields, administrators can determine whether the field appears based on how other built-in and user-defined incident fields are populated. They can either be formatted as a boolean function, which presents the computed field as a check box; selected if true, unselected if false, or as a CASE function. This documentation gives examples for both. For more information, see CASE Functions on page 387.

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 media files. 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 the fields manually. The fields enable users to categorise their incidents and media in a more advanced manner that suits the unique needs of their organisation.

E.2 Match Text Operators and Values

Users can match text fields to a specific value, for example, `owner = test`, by using the following operators:

- `=`
  The text field matches the value. For example, `title = 'Incident 0001'`
- `< >` or `!=`
  The text field does not match the value. For example, `title != 'Incident 0001'`
- `like`
  The text field matches the case-sensitive value.
- `ilike`
  The text field matches the case-insensitive value.
- `contains()`
  Only used for tag list fields. Users must enter the tag list field identifier and the name of the specific tag(s). For example, `contains (`*`<priority-level>`*`, 'high priority')`

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`.

Users should use the identifier of the text field, instead of the display name. If the identifier is more than one word, either wrap it in square brackets, for example, `[ready-to-export]`, or use camel case, for example, `readyToExport`.

Users should 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 Examples

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 starts with `t` would be returned:

```
title like 't%'
```

In the following example, any incident whose title starts with `t` or `T` would be returned:

```
title ilike 't%'
```

Advanced Media Search Examples

In the following example, any media file whose `vehicle` tag list field includes `car` would be returned:

```
contains(vehicle, 'car')
```

In the following example, any media file whose `vehicle` tag list field includes `car` and `bus` would be returned:

```
contains(vehicle, 'car, bus')
```

In the following example, any media file whose title starts with `t` would be returned:

```
title like 't%'
```

In the following example, any media file whose title starts with `t` or `T` would be returned:

```
title ilike 't%'
```

Auto-Incident Creation Examples

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 is set to `true` would be added to an incident:

```
owner = admin and [auto-incident] = true
```

In the following example, any media whose title starts with `t` would be added to an incident:

```
title like 't%'
```

In the following example, any media whose title starts with `t` or `T` would be added to an incident:

```
title ilike 't%'
```

Auto-Incident Deletion Examples

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 eligible for deletion:

```
[reviewed-already] = yes and [ready-to-delete] = yes
```

In the following example, any incident whose title starts 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 Examples

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 Examples

In the following example, the computed field `[reviewed]` would appear as a selected check box 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 selected check box in any incidents whose `[review-notes]` user-defined incident field is 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 is 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 selected check box in any incidents whose `[reviewer]` user-defined incident field is 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 is 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
```

E.3
Match Date Operators and Values

Users can match values to a built-in date field or user-defined date field by utilising the following operators:

- `=`
  The date field matches the value. For example, `[creation-time] = 2019/12/11`, the **Creation Time** field has a value of December 11th, 2019.
- `<`
  The date field is less than the value. For example, `[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. For example, `[creation-time] <= 2019/12/11`, the **Creation Time** field has a value that is either December 11th, 2019 or earlier.
- `>`
  The date field is greater than the value. For example, `[creation-time] > 2019/12/11`, the **Creation Time** field has a value that is later than December 11th, 2019.
- `>=`
  The date field is equal to, or greater than, the value. For example, `[creation-time] >= 2019/12/11`, the **Creation Time** field has a value which is either December 11th, 2019 or later.

Users can also utilise wildcard values that match date fields to dates that are relative to today. The wildcard values are as follows:

- `now()` is today's date and time.
- `today()` is today's date.

- `dateAdd()`

  Users can add intervals using three formats: number, interval, and dates. For example, `> dateAdd(-7, day, now())` would set the time to a week before now.

  The number can be positive or negative, such as `7` or `-7`, and the intervals can be the following: `day`, `month`, `year`, `hour`, `minute`, and `second`.

Users should use the identifier of the date field, instead of the display name. If the identifier is more than one word, either wrap it in square brackets, for example, `[creation-time]`, or use camel case, for example, `creationTime`. The date format is YYYY/MM/DD and should be wrapped in single quotation marks, for example, `'2007/11/30'`.

Advanced Incident Search Examples

In the following example, any incidents that were created before 04/06/2020 would be returned:

```
[creation-time] < '2020-06-04'
```

In the following example, any incidents that were created before today would be returned:

```
[creation-time] < today()
```

In the following example, any incidents that were created within the week before today would be returned:

```
[creation-time] > dateAdd(-7, day, today())
```

Advanced Media Search Examples

In the following example, any media files whose `[upload-date]` user-defined media field is populated with a date earlier than 04/06/2020 would be returned:

```
[upload-date] < '2020-06-04'
```

In the following example, any media files whose `[upload-date]` user-defined media field has a value before today would be returned:

```
[upload-date] < today()
```

In the following example, any media files whose `[upload-date]` user-defined media field has a value within the week before today would be returned:

```
[upload-date] > dateAdd(-7, day, today())
```

Auto-Incident Creation Examples

In the following example, media files whose `[upload-date]` user-defined media field is populated with 24/07/2020 would be added to an incident:

```
[upload-date] = '2020-07-24'
```

In the following example, any media files whose `[upload-date]` user-defined media field has a value within the week before today would 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, which ensures that the field is always valid, no matter when it was created. In the following example, any incident that is one week old and meets the deletion requirements would be deleted:

```
dateAdd(7, day, creationTime)
```

In the following example, if the system has an incident with two clips, both of which were recorded more than seven days ago, then that incident is tagged for immediate deletion and displays the start time of the clip plus seven days as deletion date.

```
dateAdd(7, day, mediaLatestStartTime())
```

However, if the system has an incident with two clips, one recorded more than seven days ago and one within the last seven days, then that incident is not shown for immediate deletion.

Export Profile Examples

In the following example, only incidents that 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 Examples

In the following example, the computed field `[review-reminder]` would appear with different text, depending on how the `[date-reviewed]` user-defined incident field is 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 is 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
```

E.4
CASE Functions

A CASE function evaluates conditions and returns a value when the first condition is met. The function 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 that belong to the logged-in user would be returned if the `[priority-level]` field was set to `high`. Incidents that do not belong to the logged-in user would be returned if the `[priority-level]` field was 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 media files that belong to the logged-in user would be returned if their `[priority-level]` field was set to `high`. Media files which do not belong to the logged-in user would be returned if their `[priority-level]` field was 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 media file would be added to an incident if their `title` field started with `t` and their `[ready-for-incident]` field was selected:

```
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 starts with `t` would be eligible for deletion:

```
case
when title = 't%' then true
end
```

Export Profile Examples

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 starts 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 `fallbackValue` to determine what happens to incidents whose user-defined incident fields are not populated in the expected manner. In the following example, only incidents whose `title` field starts with `b` could use the export profile:

```
case
when title = 'b%' then ''
else 'You cannot use this export profile.'
end
```

Computed Field Examples

In the following example, the computed field `[send-email-to-reviewer]` would only appear if the `[reviewer-email]` user-defined incident field was populated in incidents:

```
case
when [email] != '' then "mailto:" + encodeURIcomponent([reviewer-email])
end
```

The administrator would also need to set **As Url** to **On**, which enables them to set the URL text which users can 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 was 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**, which enables them to set the URL text which users can see:

```
case
when [postcode] != '' then 'Search for this postcode'
else 'No postcode selected'
end
```

E.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()` refers to the logged-in user performing the search.
- `ownedByMe()` returns incidents or media files that are owned by the logged-in user.
- `supervisedByMe()` returns incidents or media files that have been created by users supervised by the logged-in user.

- `isShared()` returns incidents or media files that have been explicitly shared with other users on the system, through the **Sharing** section.

  NOTE: The search does not return incidents that have been automatically shared with other users.

- `isSharedWith('user')` returns incidents or media files that have been explicitly shared with the specified user, through the **Sharing** section.
- `isOwnedBy()` returns incidents or media files that 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()` returns incidents that have external access links, including expired links.
- `hasActiveExternalLink()` returns incidents that have live external access links.

The following functions only apply to advanced media searches:

- `operator` returns media whose operator matches the user entered.
  By default, the operator is whoever recorded or imported the media file.
- `mediaType` returns media with the same media type as the one specified.
  Possible media types are as follows: `video`, `audio`, `image`, `pdf`, and `other`.
  In the following example, only media files would be returned:

  ```
  mediaType = 'media file'
  ```

- `audioCodec` returns media files with the same audio codec as the one specified.
  Possible audio codecs are as follows: `MP2`, `ULAW`, `ACC`, `MP3`, `PCM_S16LE`, and `VORBIS`.
  In the following example, only media files that have an MP3 audio codec would be returned:

  ```
  audioCodec = 'MP3'
  ```

- `media fileCodec` returns media files with the same media file codec as the one specified.
  Possible media file codecs are as follows: `H264`, `MPEG4`, `H265`, and `JPEG`.
  In the following example, only media files that have an H624 media file codec would be returned:

  ```
  media fileCodec = 'H624'
  ```

  NOTE: All audio codec and media file codec properties are case-sensitive.

- `width` returns media files whose width in pixels matches the one specified, if applicable.
  In the following example, only media files that have a width between 320 pixels and 768 pixels would be returned:

  ```
  width >= 320 and width < 768
  ```

- `height` returns media files whose height in pixels matches the one specified, if applicable.
  In the following example, only media files that have a height greater than 740 pixels would be returned:

  ```
  height > 740
  ```

- `startTime` returns media files whose start time matches the one specified.

In the following example, only media files whose start time matches today's date would be returned:

```
startTime = today()
```

NOTE: If the start time is not applicable, the search would return media files that were added to VideoManager on the specified date.

- `duration` returns media files whose duration, in seconds, matches the one specified, if applicable.
  In the following example, only media files whose duration is longer than 120 seconds would be returned:

  ```
  duration › 120
  ```

- `deviceId` returns media files that were recorded on the device specified.
  In the following example, only media files recorded on the device with an ID `00:c0:d0:00:00:00` would be returned:

  ```
  deviceId = '00:c0:d0:00:00:00'
  ```

  NOTE: Users can find the unique ID of a camera 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 ID.

- `deviceName` returns media files that were recorded on the camera specified. The search uses the serial number of a camera, instead of its ID. If the relevant media file was imported, users can specify the name of the source of the file.
  In the following example, only media files recorded on the camera with the serial number `467632` would be returned:

  ```
  deviceName = '467632'
  ```

  In the following example, only media files imported from the source with the name `LAPTOP-458823` would be returned:

  ```
  deviceName = 'LAPTOP-458823'
  ```

  NOTE: Users can edit the camera name for a media file from the **More details** pane. For more information, see Viewing and Editing Media File Properties on page 44.

- `urn` returns media files whose URN matches the one specified.
  In the following example, only media files with the URN `8e31d1f305792c6d7d68705cee864ae4` would be returned:

  ```
  urn = '8e31d1f305792c6d7d68705cee864ae4'
  ```

- `filename` returns media files whose original filename, as it was imported, matches the one specified.
  In the following example, only media files with the filename `example.pdf` would be returned:

  ```
  filename = 'example.pdf'
  ```

- `actualFilename` returns media files whose filename in the media file space of VideoManager matches the one specified.
  In the following example, only media files with the filename `example_wGzoSjCWxA_2.pdf` in the media file space of VideoManager would be returned:

  ```
  actualFilename = 'example_wGzoSjCWxA_2.pdf'
  ```

  NOTE: The filename can be found by navigating to the media file space of VideoManager.

- `fileExtension` returns media files whose file extension matches the one specified.
  In the following example, only media files with the file extension `jpg` would be returned:

  ```
  fileExtension = 'jpg'
  ```

- `importsignature` returns media files whose import signature matches the one entered.
  In the following example, only media files with the import signature `ystKH9cssC` would be returned:

  ```
  importsignature = 'ystKH9cssC'
  ```

  NOTE: The import signature can be found by navigating to the **Status** tab.

- `bookmarked` returns media files which have been bookmarked via a pre-determined gesture performed on a VB400.

  ```
  bookmarked = true
  ```

  ```
  bookmarked = false
  ```

- `fetched` returns media files on a Central VideoManager, which have been pulled from a site, that are editable on the Central VideoManager.

  ```
  fetched = true
  ```

  ```
  fetched = false
  ```

- `mediaEarliestStartTime()` returns a timestamp matching the start time of the earliest clip in the incident. If the start time of the earliest clip was moved forward, `mediaEarliestStartTime()` returns a timestamp matching the start time of the original clip before editing.
- `mediaLatestStartTime()` returns a timestamp matching the start time of the latest clip in the incident. If the start time of the latest clip was moved forward, `mediaLatestStartTime()` returns a timestamp matching the start time of the original clip before editing.

Appendix F

Custom 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.

The model consists of a hierarchy of properties and functions. Each level of the hierarchy is separated by a full stop. For example, `export.incident.signature` refers to the signature property of the incident model within the export.

To customise the title page, the administrator must ensure that **Use Template for Title Page** is set to **On**.

The syntax to be used with the customisable export title page is as follows:

- `#list` is necessary if a field can have multiple values, for example, 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, for example, an incident may not have any bookmarks.
- `#if` is necessary if a field can have a null value, for example, an incident may not have bookmarks.
- `?string` is necessary if a field has a yes/no value.
- `?datetime` formats a value as a datetime value, for example, 20/03/21, 11:02:01.
- By default, VideoManager presents timestamp fields with both a date and time value. Alternatively, administrators can specify whether only one value is presented by using the following syntax:
  - `?date` presents a date value, for example, 20/03/21.
  - `?time` presents a time value, for example, 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 value of the row.

The models which can be used with the syntax are as follows:

- Export model provides information about the export.
  For more information, see Export Model on page 393.
- Incident model provides information about incidents in the export.
  For more information, see Incident Model on page 393.
- Export job model provides information about the export job.
  For more information, see Export Job Model on page 395.
- Incident field set model provides a set of functions indicating which information may be available from the model.
  For more information, see Incident Field Set Model on page 396.
- Incident clip model provides information about incident clips in the incident which is being exported.
  For more information, see Incident Video Clip Model on page 397.
- Video file model provides information about the video files which are being exported.
  For more information, see Video File Model on page 398.
- User-defined incident fields and user-defined media fields model provide 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 400.

- Bookmark model provides information about the bookmarks in the incident clips and incidents which are being exported.
  For more information, see Bookmark Model on page 403.

F.1
Export Model

The export model contains information about the export.

The values must be wrapped in curly brackets preceded by `$`, and the field must be preceded by `export.` within the brackets. For example, `${export.videoFile}`

Potential fields are as follows:

- `incident` provides information about the incident model, including access to clips and custom fields.
  For more information, see Incident Model on page 393.
- `exportJob` provides information about the export job.
  For more information, see Export Job Model on page 395.
- `fieldSet` provides information about what metadata may be available from the model.
  For more information, see Incident Field Set Model on page 396.
- `outputFilename` provides information about the metadata output filename, if available. This is dependent on template filename generation. The default is `metadata.json`.
- `url` provides a URL to the incident page in VideoManager.
- `clip` provides information about an incident video clip.

  NOTE: This information is only available for converted footage metadata.

  For more information, see Incident Video Clip Model on page 397.
- `videoFile` provides information about a video file.

  NOTE: This information is only available for original footage metadata.

  For more information, see Video File Model on page 398.

The model also provides functions that can be used to process a value, for example by transforming it in a certain way.

- `sanitized(text)` – Passing some text into `sanitized` makes the text suitable for use in a path or filename, by converting any questionable characters into underscores. For example, if the input text is `abc/\/def`, the resulting text is sanitised to `abc___def`.

F.2
Incident Model

The incident model contains information about the incident that is being exported.

The values must be wrapped in curly brackets preceded by `$`, and the field must be preceded by `export.incident.` within the brackets. For example, `${export.incident.basestationID}`

Potential fields are as follows:

- `id` is the internal incident ID.
- `creationTimeStamp` is when the incident was created.

The field can optionally use the `?date` or `?time` syntax.

```
${export.incident.creationTimeStamp?date}
```

```
${export.incident.creationTimeStamp?time}
```

- `editTimeStamp` is when the incident was last edited.
  The field can optionally use the `?date` or `?time` syntax.

  ```
  ${export.incident.editTimeStamp?date}
  ```

  ```
  ${export.incident.editTimeStamp?time}
  ```

- `deletionTimeStamp` is when the incident was deleted, if applicable.
  The field can optionally use the `?date` or `?time` syntax.

  ```
  ${export.incident.deletionTimeStamp?date}
  ```

  ```
  ${export.incident.deletionTimeStamp?time}
  ```

- `clipCount` is the number of clips in the incident.
- `signature` is the signature of an incident, which is automatically generated by VideoManager upon creation.
- `displaySignature` is the display signature of an incident, which can be different from `signature` if it is a child incident in an incident collection.
- `basestationID` is the basestation ID associated with the incident.
- `owner` is the owner of an incident. By default, the owner is the user who created an incident, but administrators can also manually change the owner of an incident.
  Additional potential fields in the Owner Model are as follows:
  - `username`
  - `displayName` is the name of a user that is presented to others on the VideoManager system, which is not necessarily the same as a username.
    The field must use the `#if` syntax.
    Example

    ```
    <#if (export.incident.owner.displayName)?has_content>$
    {export.exportJob.owner.displayName}<#else><No displayName></#if>
    ```

  - `rfidId` is the RFID ID for the user, if applicable.
    The field must use the `#if` syntax.
    Example

    ```
    <#if (export.incident.owner.rfidId)?has_content>$
    {export.exportJob.owner.rfidId}<#else><No rfidId></#if>
    ```

  - `state` is the current state of the user.
- `location` is the geolocation of an incident, if a location has been set.
  Additional potential fields in the Location Model are as follows:
  - `lat` is the latitude of the location.
  - `lng` is the longitude of the location.

- `speed`
  The field must use the `#if` syntax.
  Example

```
<#if export.incident.location.speed??>${video.location.speed}<#else><No speed></
#if>
```

- `bearing`
  The field must use the `#if` syntax.
  Example

```
<#if export.incident.location.bearing??>${video.location.bearing}<#else><No
bearing></#if>
```

- `customFields` is the set of custom fields, if applicable.
  For more information, see User-Defined Incident Fields and User-Defined Media Fields Model on page 400.
- `isIncidentCollection()` displays whether an incident is an incident collection, that is a parent incident containing other incidents.
  The field must use the `?string` syntax.

```
${export.incident.isIncidentCollection()?string('yes','no')}
```

- `isWithinIncidentCollection()` displays whether an incident is part of an incident collection, that is a child incident.
  The field must use the `?string` syntax.

```
${export.incident.isWithinIncidentCollection()?string('yes','no')}
```

- `parent` is the parent incident, if applicable.
- `children` is a list of child incidents, if applicable.
- `clips` is a list of incident video clips.
- `compositeConfig`
- `path` applies to child incidents only and is the generated, templated or otherwise, path for this child incident in the export.
- `childIndex` is the index of this child incident within the collection.
- `bookmarks` is a list of bookmarks.

F.3 Export Job Model

The export job model corresponds to information about the export.

The values must be wrapped in curly brackets preceded by `$`, and the field must be preceded by `export.exportJob.` within the brackets. For example, `${export.exportJob.signature}`

Potential fields are as follows:

- `description` is the description of the export.
- `signature` is the unique signature of the export, automatically generated by VideoManager upon creation.
- `jobCreationTimeStamp` is when the export job started.

The field must use the `?datetime`, `?date` or `?time` syntax.

Example

```
${export.exportJob.jobCreationTimeStamp?datetime}
```

- `owner` is who created the export.
  Additional potential fields in the Owner Model are as follows:
  - `username`
  - `displayName` is the name of a user that is presented to others on the VideoManager system, which is not necessarily the same as a username.
    The field must use the `#if` syntax.
    Example

    ```
    <#if (export.exportJob.owner.displayName)?has_content>$
    {export.exportJob.owner.displayName}<#else><No displayName></#if>
    ```

  - `rfidId` is the RFID ID for the user, if applicable.
    The field must use the `#if` syntax.
    Example

    ```
    <#if (export.exportJob.owner.rfidId)?has_content>$
    {export.exportJob.owner.rfidId}<#else><No rfidId></#if>
    ```

  - `state` is the current state of the user.

If the administrator previews a template featuring the fields, the values are all presented as `example`.

F.4 Incident Field Set Model

The field set model provides a set of functions indicating which information may be available from the model. This model is usually determined by permissions.

The values must be wrapped in curly brackets preceded by `$`. The field must be preceded by `export.fieldSet.` within the brackets and must use the `?string` syntax.

For example, `${export.fieldSet.containsCreatedTime()?string('yes','no')}`

Potential fields are as follows:

- `containsCreatedTime()` displays whether the time when an incident was created is available.
- `containsEditedTime()` displays whether the time when an incident was last edited is available.
- `containsOwner()` displays whether the owner information is available.
- `containsLocation()` displays whether the location information is available.
- `containsClipTimes()` displays whether the clip times are available.
- `containsClipNotes()` displays whether clip notes are available.
- `containsClipVideos()` displays whether clip vidoes are available.
- `containsBookmarks()` displays whether the bookmark information is available.
- `containsDevice()` displays whether the device information is available.
- `containsOperator()` displays whether the operator information is available.
- `containsCompositeClipInfo()` displays whether the composite clip information is available.

- `containsFileName()` displays whether the filename information is available.

F.5 Incident Video Clip Model

The incident video clip model corresponds to information about the incident video clips that are being exported.

The values must be wrapped in curly brackets preceded by `$`, and the field must be preceded by `export.clip.` within the brackets. For example, `${clip.mediaType}`

Potential fields are as follows:

- `index` is the clip index.
- `device` is the device that was used to record an incident clip.
  Additional potential fields in the Device Model are as follows:
  - `longId`
  - `shortId`
  - `serialNumber`
  - `displayId`
  - `isSource()`
- `startTimeStamp` is the start time of an incident clip.
  The field can optionally use the `?date` or `?time` syntax.

```
${export.clip.startTimeStamp?date}
```

```
${export.clip.startTimeStamp?time}
```

- `endTimeStamp` is the end time of an incident clip.
  The field can optionally use the `?date` or `?time` syntax.

```
${export.clip.endTimeStamp?date}
```

```
${export.clip.endTimeStamp?time}
```

- `notes` are any notes about an incident clip, if applicable.
- `creationTimeStamp` is when the incident clip was created.
  The field can optionally use the `?date` or `?time` syntax.

```
${export.clip.creationTimeStamp?date}
```

```
${export.clip.creationTimeStamp?time}
```

- `editTimeStamp` is when the incident clip was last edited, for example, redacted, or clipped further.
  The field can optionally use the `?date` or `?time` syntax.

```
${export.clip.editTimeStamp?date}
```

```
${export.clip.editTimeStamp?time}
```

- `videoFiles` is a list of video files.

- `mediaType` displays whether the incident clip is an MP4, PDF, JPG, and more.
- `convertedClipName` is the name of the converted clip.
- `bookmarks` is a list of bookmarks, if applicable.
- `videoStreamIndex` is the index of a video stream.
- `videoStreamName` is the name of a video stream.
- `audioStreamIndex` is the index of an audio stream.
- `audioStreamName` is the name of an audio stream.

F.6
Video File Model

The video file model corresponds to information about the video files that are being exported, that is the properties of video files on VideoManager, separate from the properties of incident clips.

The values must be wrapped in curly brackets preceded by `$`.

Video File Syntax

To present information about video files, administrators must use the `#list` syntax:

```
<#list export.clip.videoFiles as video>
| EXAMPLE COLUMN NAME | EXAMPLE COLUMN VALUE |
</#list >
```

Example

```
<#list export.clip.videoFiles as video>
| name : | ${video.name} |
</#list >
```

Video File Values

Potential fields are as follows:

- `device` is the device used to record the video file.
  Additional potential fields in the Device Model are as follows:
  - `longId`
  - `shortId`
  - `serialNumber`
  - `displayId`
  - `isSource()`

  Example

  ```
  ${video.device.shortId}
  ```
- `name` is the name of the file as stored on the server of VideoManager.
- `originalName` is the original file name. The original file name is different from `name` if the video file was imported from an external source.
- `recordingStartTimeStamp` is when the recording that the video file belongs to started.
  The field can optionally use the `?date` or `?time` syntax.

- `startTimeStamp` is the start time of the video file. The start time can be different from `recordingStartTimeStamp` if the recording was split into multiple video files.
  The field can optionally use the `?date` or `?time` syntax.
- `endTimeStamp` is the end time of the video file.
  The field can optionally use the `?date` or `?time` syntax.
- `isPreRecording()` displays whether prerecording was enabled for the video file.
  The field must use the `?string` syntax.
- `duration` is the duration in seconds of the video file.
- `operator` is the operator of the video file. By default, the operator is the user who recorded the video file.
- `deletionTimeStamp` is when the video file was deleted, if applicable.
  The field can optionally use the `?date` or `?time` syntax.
- `deletionRequestTimeStamp` is the requested time of deletion, if the deletion policy has been configured to keep video files after a user has requested them to be deleted.
  The field can optionally use the `?date` or `?time` syntax.
- `recordingIdentifier` is the recording identifier.
- `indexInRecording` is the index of the video file within the recording.
  If the recording only consists of the video file, the value is `0`.
- `downloadTimeStamp` is when the video file was downloaded to VideoManager from a camera, or imported as external media.
  The field can optionally use the `?date` or `?time` syntax.
- `editTimeStamp` is when the video file was last edited.
  The field can optionally use the `?date` or `?time` syntax.
- `frameWidth` is the frame width of the video file.
- `frameHeight` is the frame height of the video file.
- `videoCodec` is the video codec of the video file.
- `audioCodec` is the audio codec of the video file.
- `urn` is the unique resource identifier of the video file.
- `owner` is the owner of the video file.
  Additional potential fields in the Owner Model are as follows:
  - `username`
  - `displayName` is the name of a user that is presented to others on the VideoManager system, which is not necessarily the same as a username.
    The field must use the `#if` syntax.

    Example

    ```
    <#if (video.owner.displayName)?has_content>${video.owner.displayName}<#else><No
    displayName></#if>
    ```
  - `rfidId` is the RFID ID for the user, if applicable.
    The field must use the `#if` syntax.

    Example

    ```
    <#if (video.owner.rfidId)?has_content>${video.owner.rfidId}<#else><No rfidId></
    #if>
    ```

- `state` is the current state of the user.

  Example

  ```
  ${video.owner.username}
  ```

- `restricted` displays whether the video file is restricted.
  The field must use the `?string` syntax.

  ```
  <#list export.clip.videoFiles as video>
  | Was this pre-recorded? : | ${video.restricted?string
  ('yes','no')} |
  </#list >
  ```

- `size` is the size in bytes of the video file.
- `customFields` is the set of user-defined media fields, if applicable.
  For more information, see User-Defined Incident Fields and User-Defined Media Fields Model on page 400.
- `location` is the geolocation of the video file, if the camera that recorded it had GPS enabled.
  Additional potential fields in the Location Model are as follows:
  - `lat` is the latitude of the location.
  - `lng` is the longitude of the location.
  - `speed`
    The field must use the `#if` syntax.

    Example

    ```
    <#if video.location.speed??>${video.location.speed}<#else><No speed></#if>
    ```

  - `bearing`
    The field must use the `#if` syntax.

    Example

    ```
    <#if video.location.bearing??>${video.location.bearing}<#else><No bearing></#if>
    ```

- `exportOriginalFileName` is the original file name of the video file that is being exported.
- `exportConvertedFileName` is the converted file name of the video file that is being exported.

F.7

User-Defined Incident Fields and User-Defined Media Fields Model

Using the `customFields` function, administrators can display information about the user-defined incident fields of the exported incident, and the user-defined media fields of exported media files. The action requires using 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 should be included in the template.

To include all user-defined incident fields in the template, regardless of whether they are populated in the incident:

```
<#list export.incident.customFields?keys as key>
<#assign field = export.incident.customFields[key]>
| EXAMPLE COLUMN NAME : | EXAMPLE COLUMN VALUE |
</#list>
```

To include only user-defined incident fields that are populated in the template:

```
<#if export.incident.customFields["custom-field-name"]??>
<#assign field = export.incident.customFields["custom-field-name"]>
| EXAMPLE COLUMN NAME : | EXAMPLE COLUMN VALUE |
</#if>
```

The syntax is the same for user-defined media fields, but requires using an additional `#list` function:

```
<#list export.clip.videoFiles as video>|
<#list video.customFields?keys as key> <#assign field = video.customFields[key]>>
| EXAMPLE COLUMN NAME : | EXAMPLE COLUMN VALUE |
</#list>
</#list>
```

```
<#list export.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

After 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` is the value of the custom field.

  ```
  <#if export.incident.customFields["custom-field-name"]??> <#assign field =
  export.incident.customFields["custom-field-name"]>
  | ${field.name} : | ${field.value.text} |
  </#if>
  ```

- `name` is the identifier of the custom field.

  ```
  <#if export.incident.customFields["custom-field-name"]??> <#assign field =
  export.incident.customFields["custom-field-name"]>
  | Name : | ${field.name} |
  </#if>
  ```

- `displayName` is the display name of the custom field.

  ```
  <#if export.incident.customFields["custom-field-name"]??> <#assign field =
  export.incident.customFields["custom-field-name"]>
  | Name | ${field.displayName} |
  </#if>
  ```

- `isText` is whether the custom field is a text field or not.

  The field must use the `?string` syntax.

  ```
  <#if export.incident.customFields["custom-field-name"]??> <#assign field =
  export.incident.customFields["custom-field-name"]>
  | ${field.name} : | ${field.isText?string('yes','no')} |
  </#if >
  ```

- `isDate` is whether the custom field is a date field or not.
  The field must use the `?string` syntax.

```
<#if export.incident.customFields["custom-field-name"]??> <#assign field =
export.incident.customFields["custom-field-name"]>
| ${field.name} : | ${field.isDate?string('yes','no')} |
</#if>
```

- `isTimestamp` is whether the custom field is a timestamp or not.
  The field must use the `?string` syntax.

```
<#if export.incident.customFields["custom-field-name"]??> <#assign field =
export.incident.customFields["custom-field-name"]>
| ${field.name} : | ${field.isTimestamp?string('yes','no')} |
</#if>
```

- `isBool` is whether the custom field is a check box field or not.
  The field must use the `?string` syntax.

```
<#if export.incident.customFields["custom-field-name"]??> <#assign field =
export.incident.customFields["custom-field-name"]>
| ${field.name} : | ${field.isBool?string('yes','no')} |
</#if >
```

- `mandatory` is whether the custom field is mandatory, that is the user cannot save the incident unless they have populated the field.
  The field must use the `?string` syntax.

```
<#if export.incident.customFields["custom-field-name"]??> <#assign field =
export.incident.customFields["custom-field-name"]>
| ${field.name} | ${field.mandatory?string('yes','no')} |
</#if>
```

- `fieldType` is the type of the user-defined incident field. The options are as follows: `USER_DEFINED`, `OWNER`, `CREATION_TIME`, `UPDATE_TIME`, `SIGNATURE`, or `CLIP_COUNT`.

```
<#list export.incident.customFields?keys as key>
<#assign field = export.incident.customFields[key]>
| ${field.name} : | ${fieldType} |
</#list>
```

- `purpose` is the purpose of the custom field. The options are as follows: `INCIDENT`, `INCIDENT_ DELETE`, `MEDIA`, `CC_VAULT`, or `PLAYBACK_REASON`.

```
<#list export.incident.customFields?keys as key>
<#assign field = export.incident.customFields[key]>
| ${field.name} : | ${purpose} |
</#list>
```

- `derived` is whether the custom field value is dynamically calculated from other information, such as a computed field.
  The field must use the `?string` syntax.

```
<#if export.incident.customFields["custom-field-name"]??>
<#assign field = export.incident.customFields["custom-field-name"]>
| ${field.name} : | ${field.derived?string('yes','no')} |
</#if >
```

- `defaultValue` is the default value of the custom field, if nothing else is entered.

```
<#list export.incident.customFields?keys as key>
<#assign field = export.incident.customFields[key]>
```

```
| ${field.name} : | ${defaultValue} |
</#list>
```

- `deleted` is whether the custom field has been deleted from VideoManager or not.
  The field must use the `?string` syntax.

```
<#if export.incident.customFields["custom-field-name"]??> <#assign
field = export.incident.customFields["custom-field-name"]>
| Has ${field.name} been deleted? : | ${field.deleted?string
('yes','no')} |
</#if >
```

- `permissionGroup` is the access group that users must belong to in order to view and edit the user-defined incident field. The options are as follows: `0`, that is public, `ONE`, `TWO`, and more.

```
<#list export.incident.customFields?keys as key><#assign field =
export.incident.customFields[key]>
| What is the permission group for ${field.name}? : |
${permission} |
</#list>
```

- `orderIndexSmall`
- `orderIndexMedium`
- `orderIndexWide`

F.8
Bookmark Model

The bookmark model contains information about bookmarks included in either the incident, which have been manually added on VideoManager, or individual video files within the incident, which were added in the field by the camera that recorded it.

Bookmark Syntax

Firstly, the administrator must decide which bookmarks should be included in the template.

To present information about bookmarks of an incident, the administrator must use the `#list` syntax, and optionally `![]` if not all incidents have bookmarks.

```
<#list export.incident.bookmarks![] as bookmark>
| EXAMPLE COLUMN NAME : | EXAMPLE COLUMN VALUE |
</#list>
```

To present information about bookmarks of an individual video file, the administrator must first use the `#list` syntax to list the video files. They must then use the `#list` syntax to list the bookmarks, and optionally `![]` if not all video files have bookmarks.

```
<#list export.clip.videoFiles as video >
<#list export.video.bookmarks![] as bookmark >
| EXAMPLE COLUMN NAME : | EXAMPLE COLUMN VALUE |
</#list>
</#list>
```

Bookmark Values

After the administrator has configured the template, they can use the following values to present information about the bookmarks:

- `name` is 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 in the field by a camera:

- If the bookmark was created after the video file was 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 camera, the default bookmark name is the time it refers to in the video file.

- `startTime` is when the bookmark was placed in the video file or incident clip.
  The field must use the `?datetime`, `?date` or `?time` syntax.

  Example

  ```
  ${bookmark.startTime?date}
  ```

Appendix G

Profiles Hierarchy

When a camera is assigned, the device profiles and network profiles it takes are defined by parallel hierarchies.

One hierarchy defines which network profile is chosen for the camera to use, and which networks within that profile are used for streaming. For more information, see Network Profiles Hierarchy on page 405.

One hierarchy defines which device profile is chosen for the camera to use. For more information, see Device Profiles Hierarchy on page 407.

G.1 Network Profiles Hierarchy

Figure 2: Network Profiles Hierarchy

The following flowchart demonstrates how VideoManager determines which network profile is chosen when a user assigns a VB-series camera or VT-series camera.

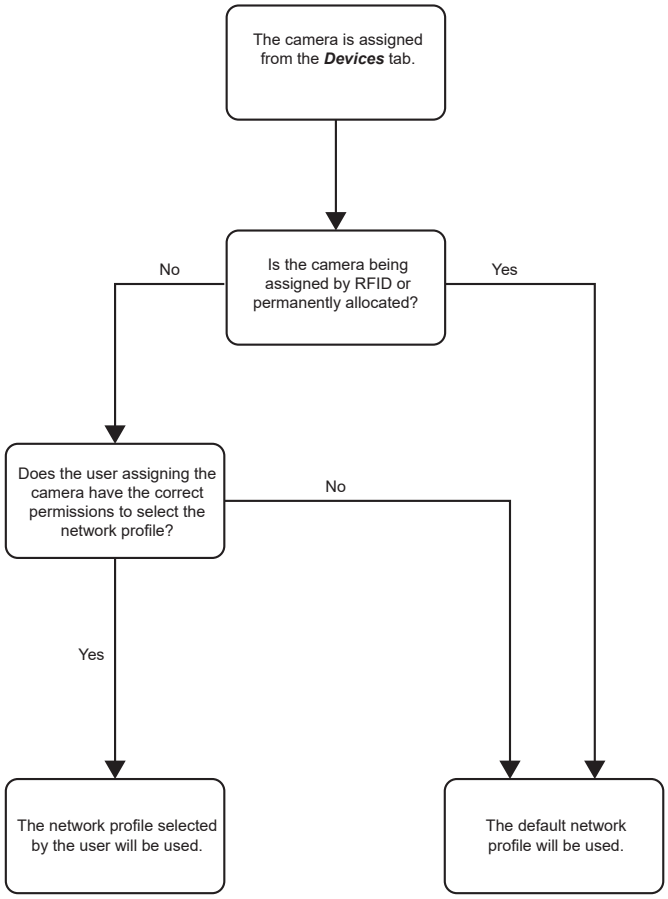
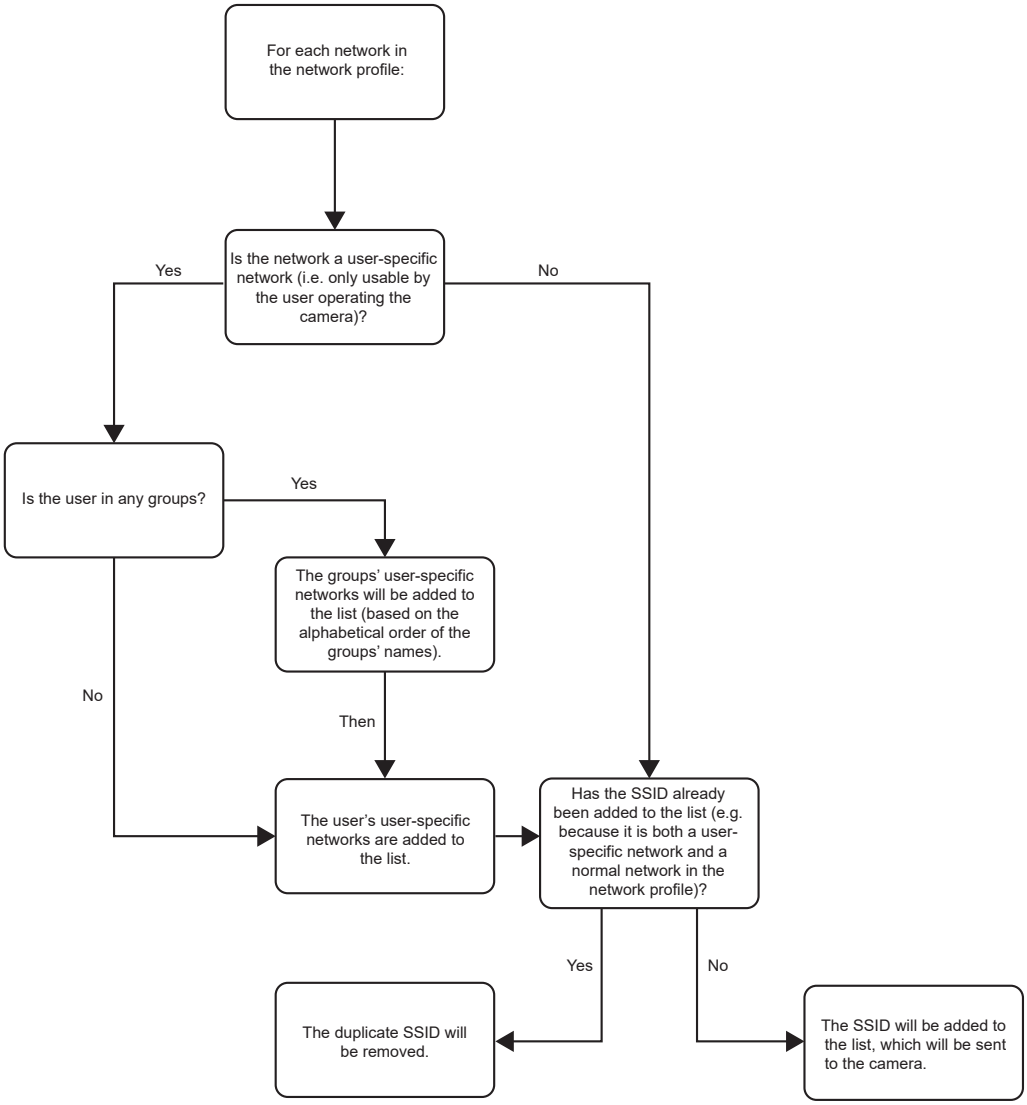


Figure 3: Networks Hierarchy

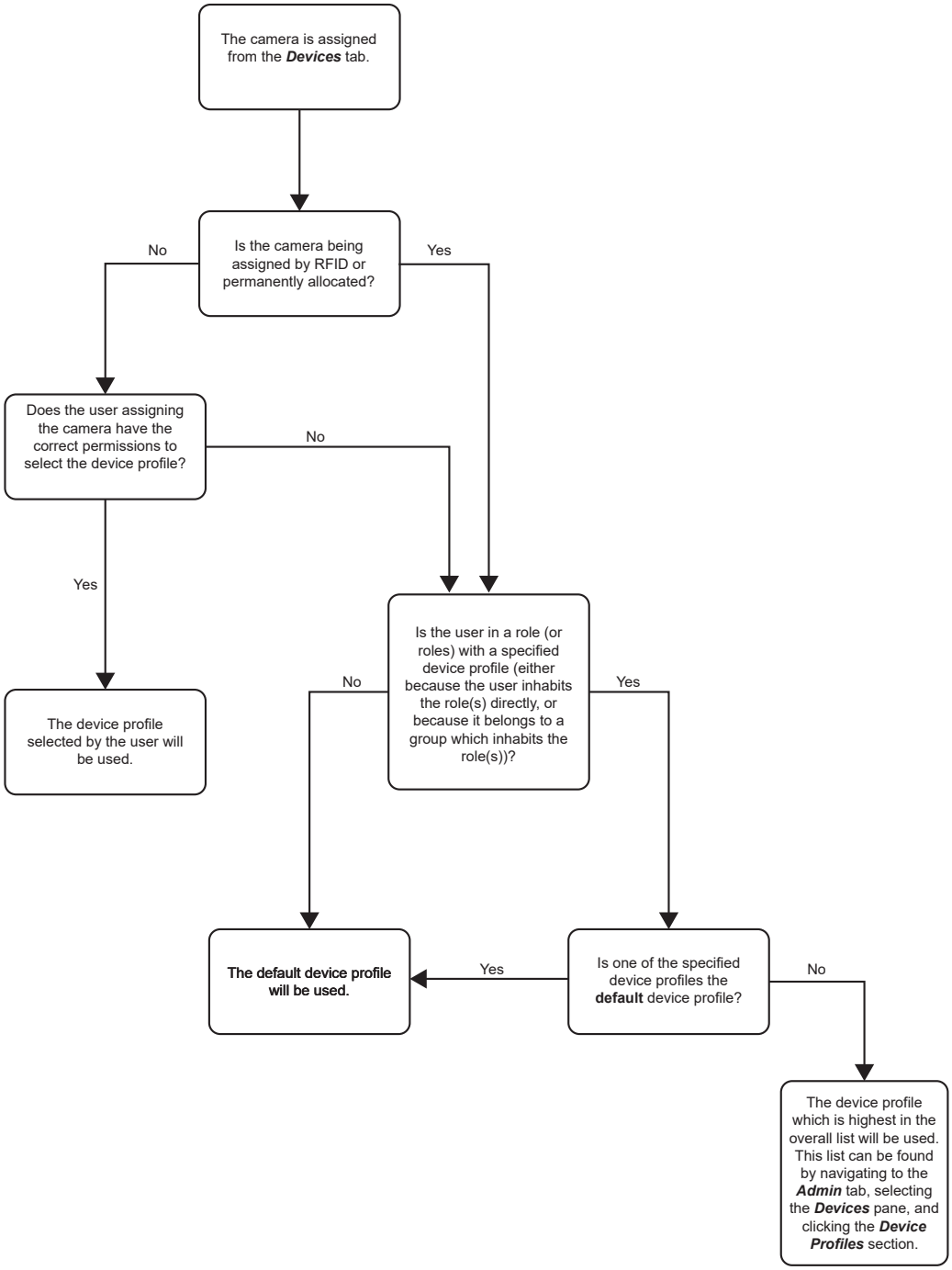
The following flowchart demonstrates how VideoManager determines which individual networks the VB-series camera or VT-series camera has access to.



G.2
Device Profiles Hierarchy

Figure 4: Device Profiles Hierarchy

The following flowchart demonstrates how VideoManager determines which device profile is chosen when a user assigns a camera.



Appendix H

Glossary

Access control key
The security mechanism that prevents unauthorised cameras from connecting to VideoManager. In addition, if a camera is lost or stolen, its recorded footage cannot be recovered unless the person who has possession of the 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 that 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 regular users on the system.

Assigned/Unassigned
If a camera has been assigned, it has been paired with a user and can record footage. An unassigned 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 cameras, deleted media files, and more. This trail is not deletable.

Bandwidth rule
A configurable rule that determines when footage is uploaded from sites to the Central VideoManager. This is useful if remote workers do not want to put strain on their home WiFi during high-traffic hours.

Bluetooth peripheral
A device that sends a notification to cameras when a change in state is detected (e.g. a gun is unholstered). Administrators can configure 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 media file. It can be created by the camera that is recording the media file in the field, if the operator presses a configured button. Alternatively, users can add bookmarks to a media file in an incident, once the media file has been downloaded to VideoManager.

Central VideoManager
An instance of VideoManager that acts as a "hub", to which other instances of VideoManager (known as sites) can connect, in order to pass on their footage and metadata.

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 that 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 that has been associated with VideoManager, such as cameras, docks.

Device affinity
This is created when a camera is assigned to a user with a single issue (either with RFID or through VideoManager), and the user then redocks the camera mid-way through their shift. VideoManager will remember the connection, allowing the user to undock the same camera later in the shift.

Display name
The name of a user that will be presented to others on the VideoManager system, which is not necessarily the same as a username.

DockController
A device that converts the media files from cameras into data that can be sent over a network or the internet. This allows up to 84 cameras to be used with just one DockController, and enables these cameras to be installed away from the physical VideoManager server.

EdgeController
A small embedded computer with inbuilt storage, which provides remote or home-based workers with a docking location for their cameras. They are used exclusively as a site, connected to a Central VideoManager.

Export
Incidents that have been exported from VideoManager to the user's PC. A version of the incident will remain on VideoManager.

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 media file that has been added to an incident.

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.

Media
Any media files or assets, which can be added to an incident for evidential purposes.

Media file
Any media that has been imported or downloaded to VideoManager. This could be a PDF, a still image, a video, or an audio file.

Media file ID
A unique ID that identifies a specific media file. It is used in the audit log to record which media file/asset an entry refers to, and can be used to locate media files/assets.

Network profile
A collection of individual WiFi networks that is then applied to a camera. The camera in question will stream to VideoManager over these networks.

ONStream
A licenced feature from Motorola Solutions that enables cameras to send a live stream to VideoManager over WiFi.

Operator
By default, this is the user who recorded the media file on a camera, or imported the asset into VideoManager (either manually, or as configured in an automatic import profile).

Owner of a media file
This is the user who has administrative control over a media file. By default, this is the user who recorded the media file on a camera, or imported it 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.

Peer-Assisted Recording (PAR)
The mechanism that, when one camera starts recording, will notify other cameras in the vicinity that a recording has started, via Bluetooth Low Energy (BLE). This allows the receiving camera to also start recording, if applicable.

Permanent allocation
If a 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 camera with RFID touch assign.

Permanent issue
If a camera has been assigned to a user with a 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 that determines the actions users can perform on VideoManager.

Post-record
The media file immediately following an event that is captured automatically, once the operator stops recording. This could be between 1 and 120 seconds.

Pre-record
The media file preceding an event that is automatically captured as soon as an operator starts recording. This could be between 1 and 120 seconds.

Recording
This is the complete footage recorded by a camera, from the moment it is prompted to start recording until the moment it is prompted to stop (including any pre- and post-record periods). A recording will be split into multiple media files if it reaches a certain length, as defined in the camera's device profile.

Recording ID
A unique ID that identifies a specific recording. If a recording has been split up into multiple media files (due to the device profile of the camera that recorded it), these media files will all have the same recording ID.

Remote devices
Cameras that are connected to a site, and can still be configured like normal from the Central VideoManager.

Role
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 that 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.

Safety mode
While a 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 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 camera has been assigned to a user with single issue, it will only be assigned to the user for one trip. Once the camera is redocked, it will return to the pool and can be assigned to a different user.

Site
An instance of VideoManager that connects to another instance of VideoManager (known as a "Central VideoManager"), in order to pass on its footage and metadata.

System administrator
A role that cannot be edited or deleted. Any users with this role will be able to access any aspect of VideoManager.

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 on.

User
Every individual on an instance of VideoManager must have their own user.

User-defined field
A manually-created field that 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 should not be able to access.

VB SmartControl
Motorola Solutions VB SmartControl enables users who are still in the field to use their phone to view and categorise footage they have recently recorded.

VB200
A robust camera designed and sold by Motorola Solutions. It can record for up to 8 hours and has 16GB of recording storage.

VB300
A robust 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 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 camera's device profile.

VT100
A VT100 is a lightweight, discreet 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 camera in Motorola Solutions' VT-series camera range to have haptic feedback.

VT50
A lightweight, discreet 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.