



MOTOROLA SOLUTIONS

VideoManager 14.6.4 Getting Started Guide

This document is intended to serve as a reference to administrators when installing and configuring VideoManager for the first time.

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

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

Intended purpose This document is intended to serve as a reference to administrators when installing and configuring VideoManager for the first time.

Document ID ED-012-213-06

Conventions This document uses the following conventions:

Convention	Description
► For more information...	A cross-reference to a related or more detailed topic.
[]	Text enclosed in square brackets indicates optional qualifiers, arguments or data.
< >	Text enclosed in angle brackets indicates mandatory arguments or data.

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

Safety notices



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



Additional information relating to the current section.

Contents

1 Welcome to VideoManager	4
2 Initial Configuration	5
2.1 Download VideoManager	6
2.2 Re-Download VideoManager	8
3 System Configuration	9
3.1 Configure the Web Server	10
3.2 Configure Storage	11
3.2.1 Create, Edit and Delete File Containers	12
3.2.2 Create, Edit and Delete File Spaces	13
3.3 Create, Import, and Export Access Control Keys	17
3.4 Configure Deletion Policies	19
3.5 Create Backup Databases	21
4 Connect Body-Worn Cameras to VideoManager	22
4.1 Configure and Connect a DockController to VideoManager	23
4.2 Connect Docks and Body-Worn Cameras to DockControllers	25
4.3 Connect VT-Series Cameras to VideoManager Remotely	27
5 Add Users and Roles	29
5.1 Add Users	30
5.2 Add Roles	31
5.3 Associate Roles With Users	33
6 Assign Body-Worn Cameras and Record Footage	34
6.1 Assign Body-Worn Cameras with Single Issue on VideoManager	35
6.2 Assign Body-Worn Cameras with Single Issue and RFID	36
6.3 Assign Body-Worn Cameras with Permanent Issue	37
6.4 Assign Body-Worn Cameras with Permanent Allocation	38
7 Glossary	40

1 Welcome to VideoManager

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

This documentation is designed to walk you through installing VideoManager, configuring the necessary security measures, adding users to the system, and assigning devices to those users.

For more complex procedures, please consult the VideoManager user guide.

2 Initial Configuration

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

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

- Download VideoManager for the first time.

>> For more information, see Download VideoManager on page 6

- Re-download VideoManager.

>> For more information, see Re-Download VideoManager on page 8

2.1 Download VideoManager

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

1. Ensure that Software Assurance has been obtained from Motorola Solutions. Please contact edesixsales@motorolasolutions.com to obtain Software Assurance.
2. Double-click the downloaded **VideoManager-setup-14.6.4.exe** file.
3. Confirm that the installer can make changes to the PC.
4. The VideoManager installer will open. Click **Next**.
5. The administrator will be given the option to change where VideoManager is installed on their PC - once the destination has been chosen, click **Install**.
VideoManager will be downloaded.
6. Click **Finish**.
7. Multiple installers will open. Click through every one by clicking **Next** and **Finish**.
8. Navigate to VideoManager's installation location, and click **pss.exe**.
9. The web UI will be opened. Click **Set Up**.
10. Read the licence agreement, and click **Accept**.
11. Choose where users, groups, and incidents will be stored. The options are as follows:
 - **Use built-in database server (recommended)** - if this is selected, all users, groups, incidents, and other VideoManager data will be stored in VideoManager's default database.
 - **Use external SQL Server database (advanced)** - if there is an existing SQL Server, the administrator can connect it to VideoManager now.If this option is selected, the administrator must enter the following information:

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

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


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

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

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

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

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

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

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

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



For more information, please see the technical paper "VideoManager and SQL Server Explained [ED-009-032]".

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

>> For more information, see Configure Storage on page 11

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

2.2 Re-Download VideoManager

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

1. Ensure that Software Assurance has been obtained from Motorola Solutions.
Please contact edesixsales@motorolasolutions.com to obtain Software Assurance.
2. Double-click the downloaded **VideoManager-setup-14.6.4.exe** file.
3. Confirm that the installer can make changes to the PC.
4. The administrator will be asked to uninstall the old version of VideoManager. This will **not** delete the administrator's database, as long as the administrator is upgrading to a newer version. Click **Yes**, then **Uninstall**.
5. The VideoManager installer will open. Click **Next**.
6. The administrator will be given the option to change where VideoManager is installed on their PC - once the destination has been chosen, click **Install**.
VideoManager will be re-installed.
7. Click **Finish**.
8. Multiple installers will open. Click through every one by clicking **Next** and **Finish**.
9. Launch the web UI interface like normal.



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

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

3 System Configuration

There are a few important VideoManager settings that must be configured before users start utilizing the system.

1. Configure the webserver.

>> For more information, see [Configure the Web Server](#) on page 10

2. Configure storage settings. This dictates how footage is stored in VideoManager.

>> For more information, see [Configure Storage](#) on page 11

3. Create an access control key. This ensures that only specific body-worn cameras can connect to VideoManager.

>> For more information, see [Create, Import, and Export Access Control Keys](#) on page 17

4. Configure the deletion policy. This dictates how old footage is automatically deleted.

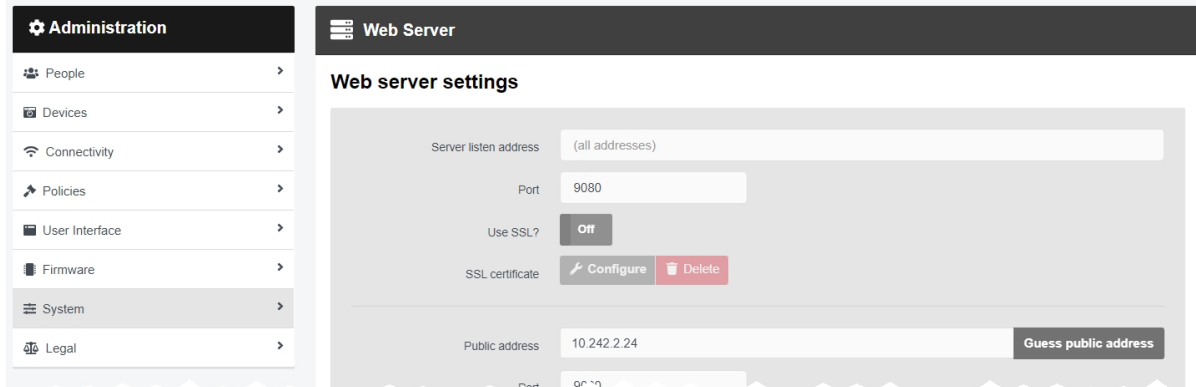
>> For more information, see [Configure Deletion Policies](#) on page 19

5. Configure backups. This dictates where VideoManager's database backups - **not** footage - are sent.

>> For more information, see [Create Backup Databases](#) on page 21

3.1 Configure the Web Server

The **Web Server** pane is used to control how VideoManager offers the browser-based user interface to users. This is done from the **Web Server** section of the **System** pane, in the **Admin** tab.



To configure the browser-based interface:

1. Navigate to the **Admin** tab.
2. Select the **System** pane.
3. Click the **Web Server** section.
4. Enter the following information:
 - **Server listen address** - the address which users should enter to get to VideoManager. This should ordinarily be the local IP address of the server running VideoManager. If the user does not know this address, they should click **Guess public address**
 - **Port** - the port which VideoManager will listen on. By default, this is 9080.
 - **Public address** - this is the address which users can use to access VideoManager if they are not on the same network as the server. **Guess public address** will try to guess what this address should be.
 - **Port** - the port which users using the **Public address** to connect to VideoManager.
 - **Use SSL?** - if enabled, then SSL will be used to secure connections to the **Public address**.



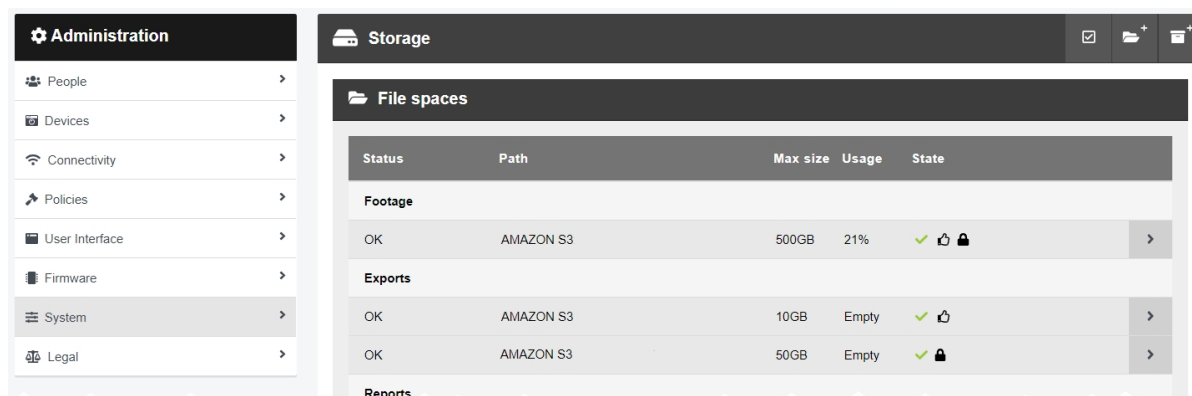
The server's listen address and public address are shown at the bottom of the pane.

5. Click **Save settings**.

3.2 Configure Storage

VideoManager organises file resources into file spaces. These can either reside in file systems (e.g. network file storage, local file storage on a PC, or storage area networks), or they can be organised through file containers (e.g. Amazon S3 Object Storage). The user can configure file spaces for backups, exports, reports, and footage.

Over time, it may become necessary to increase the size of file spaces, or add new ones. This is done from the **Storage** section of the **System** pane, in the **Admin** tab.



The aspects to configuring storage are as follows:

- Create, edit and delete file containers (if they have been licensed).

>> For more information, see [Create, Edit and Delete File Containers](#) on page 12

- Create, edit and delete file spaces.

>> For more information, see [Create, Edit and Delete File Spaces](#) on page 13




3.2.1 Create, Edit and Delete File Containers

If they have purchased Amazon S3 Object Storage from Amazon AWS, users should create file containers before they create any file spaces. These "buckets" allow VideoManager to store a user's Amazon S3 Object Storage information so that their file spaces can connect to the cloud. This is useful if a user is processing more information than could reasonably be stored locally.



These steps can be ignored by users who haven't bought Amazon S3 Object Storage, and will be using filesystem storage instead.

To create a file container:

1. Navigate to the **Admin** tab.
2. Select the  **System** pane.
3. Click the  **Storage** section.
4. Click  **Create file container**.
5. Enter a name in the **Name** field. This will be how the file container is identified in the UI.
6. From the **Type** dropdown, select **S3 Object Storage**.
7. Fill out the **Bucket name**. This should be VideoManager's unique fully qualified domain name.
8. Enter the **Endpoint** of the file container.
This can be discovered by navigating to the S3 Management Console and checking what the bucket's region is (this will have been set by the user when they originally created the bucket), then inserting this region into the format `s3.region.code.amazonaws.com`.






*The endpoint **must** match the region where the bucket was created.*

9. Enter the **Key** of the file container.
This can be discovered by copying the Access Key ID from Amazon AWS console, and pasting it into VideoManager.
10. Enter the **Secret** of the file container.
This can be discovered by clicking **Show** under the secret access key in Amazon AWS console, and pasting the key into VideoManager.
11. Click **confirm**.

3.2.2 Create, Edit and Delete File Spaces

File spaces determine where information from VideoManager is stored - this could be on the user's PC, a network database, or Amazon S3 Object Storage (if it has been purchased).

To create a file space:

1. Navigate to the **Admin** tab.
2. Select the  **System** pane.
3. Click the  **Storage** section.
4. Click  **Create file space**. The **Create file space** window opens.
5. Enter the path for the new file space.

A network database with a backup system is encouraged if users have this instead. If the user has purchased Amazon S3 Object Storage, they should enter the name of a folder within the bucket, which will then be created.

6. From the **Category** dropdown, select a category for the file space.

The categories are as follows:

- **Footage** - this is where all downloaded footage will be stored.
- **Exports** - this is where all incident exports will be stored.
- **Backups** - this is where the VideoManager database information from backups will be stored.

>> For more information, see Create Backup Databases on page 21

- **Reports** - this is where all reports will be stored.
 - **Report Auto Copy** - this is where all scheduled reports will be automatically copied to. If this option is selected, no more configuration is necessary from this pane, and the user can click **confirm**.
7. In the **Max size** field, enter the maximum size of the file space. From the dropdown, choose a unit in which the data will be counted - this could be **Bytes**, **Kilobytes**, **Megabytes**, **Gigabytes**, **Terabytes**, or **Petabytes**.

Motorola Solutions recommends that the maximum size is **not** set to the absolute upper limit of the disk/drive.



*If every file space of one type is full, system functions will stop working (e.g. if all **Footage** file spaces are full, body-worn cameras will not be able to download footage to VideoManager when docked, and will instead enter an error state).*



8. From the **State** dropdown, select a state for the file space. In most cases, this will be **Online**. However, users can also select:

- **Obsolete** - this is useful if users wish to keep a file space on VideoManager, but do not want footage or other data to be sent there.
- **Offline** - this is useful if the network database or local storage is down for maintenance. However, if the file space is marked as **Offline**, all information that was in the file space will be unavailable until it comes back online again.
- **Evacuate** - this will automatically move all data in the file space to the other file space(s) of the same type. This is useful if an old file space should be deleted, but the data within it should be kept.

If another user on the system is viewing, editing, or exporting the data in a file space which is being evacuated, the evacuation will be forced to wait until the other actions have finished.

9. From the **Encryption** dropdown, select an encryption type (if relevant). The options are **NONE**, **AES-128**, **AES-192**, and **AES-256**.

This cannot be changed later. If an encryption mode is chosen, users **must** download the encryption key after creation, and store it offsite. This ensures that the data can be recovered later in case of a disaster. To do so:

- Click  **Go to file space** next to the file space whose encryption key should be downloaded.
- Click  **Download Key**.

The key will be downloaded to the PC's default download location. It should be transferred to a secure location offsite.



*If unsure, Motorola Solutions recommends that users choose **AES-256**.*




10. If **Preferred** is set to **Yes**, all footage/exports/reports/backups will be sent to this file space until it is full.



If multiple file spaces have **Preferred** set to **Yes**, VideoManager will alternate between those file spaces when storing resources.

If no file spaces have **Preferred** set to **Yes**, VideoManager will alternate between all file spaces when storing resources.




11. Click **confirm** to save the changes.

Once file spaces have been created, their paths can be changed. Motorola Solutions recommends creating an entirely new file space with the updated path, and migrating all files in the old file space over to it. To do so:




1. Navigate to the **Admin** tab.
2. Select the  **System** pane.
3. Click the  **Storage** section.
4. Click  **Create file space**. The **Create file space** window opens.

5. Enter the path for the new file space.
6. Configure the rest of the settings as desired, and ensure that **Preferred** is set to **Yes**.
7. Click **confirm**.
8. Click  **Go to file space** next to the old file space whose path must be changed.
9. From the **Category** dropdown, select **Evacuate**.
The data in the old file space will be evacuated to the file space with the new path. The old file space can now be deleted, by clicking  **Delete file space**.


Alternatively, administrators can change the path of the original file space itself. Before doing so, they must stop the VideoManager service, and manually move the files to the new location. Then, on VideoManager:

1. Navigate to the **Admin** tab.
2. Select the  **System** pane.
3. Click the  **Storage** section.
4. Click  **Go to file space**,
5. Click **Change**.
6. Make the required edits, and click **confirm**.

If the user wishes to change the size of the file space because it is becoming full, the steps they must take are as follows:

1. Navigate to the **Admin** tab.
2. Select the  **System** pane.
3. Click the  **Storage** section.
4. Click  **Go to file space** next to the file space whose size should be changed.
5. In the **Max size** field, make the relevant changes.
6. Click **confirm**.

It may become necessary to delete a file space altogether. To do so users must first ensure that **all** data in the file space has been evacuated to another suitable file space. To do so:

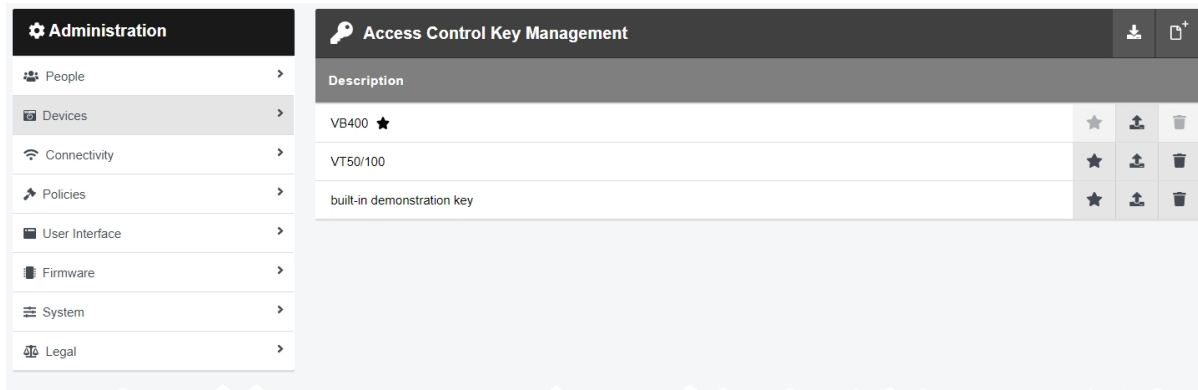
1. Ensure that there is at least one other file space on VideoManager whose **Category** matches that of the file space which is being deleted, and whose **State** is set to **Online**.
2. Click  **Go to file space** next to the file space to be deleted.
3. From the **Category** dropdown, select **Evacuate**.
4. Click **confirm**.

The data in the deleted file space will be evacuated to the other file space(s).

5. Next to the now-empty file space, click  **Delete file space.**

3.3 Create, Import, and Export Access Control Keys

Access control keys are the mechanism that VideoManager uses to encrypt videos. They also prevent body-worn cameras from communicating with unauthorised instances of VideoManager. This is done from the **Access Control Key Management** section of the **Devices** pane, in the **Admin** tab.



To create an access control key:

1. Navigate to the **Admin** tab.
2. Select the **Devices** pane.
3. Click the **Access Control Key Management** section.
4. Click **Create key**.
5. In the **Description** field, enter a name for the access control key.
6. Click **Create key**.
7. Once an access control key has been created, the administrator can make it the default, by which all new or factory reset body-worn cameras are authenticated, by clicking **Set as default key**.




It is recommended that all access control keys are exported upon creation to somewhere secure - in event of a system failure, this will ensure that users can still access footage on their body-worn cameras that has not been downloaded already.

If an administrator wishes to move a body-worn camera to another instance of VideoManager, they **must** import the corresponding access control key into that instance of VideoManager as well - otherwise, the body-worn camera will appear as **locked** and the user will not be able to access any footage on the body-worn camera which has not already been downloaded to VideoManager. To do so:

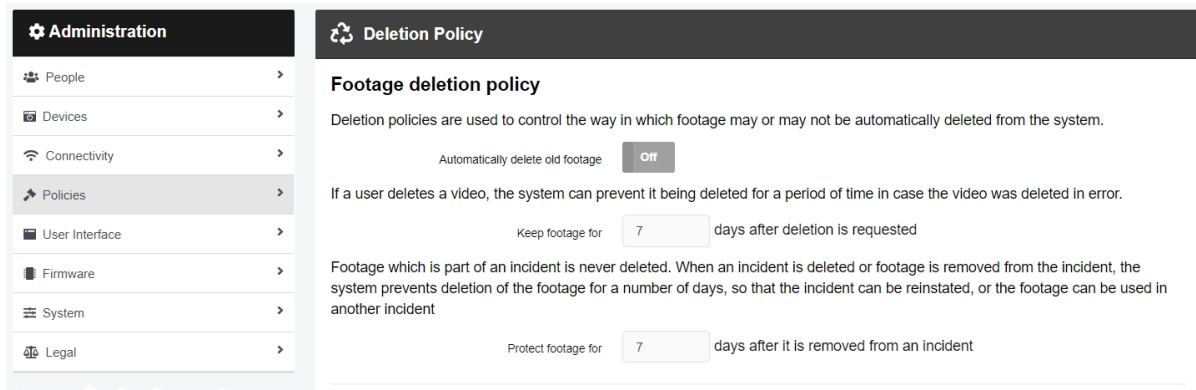
1. In the original VideoManager instance, next to the access control key, click **Export key**.

The access control key will be downloaded to the administrator's PC.

2. In the new instance of VideoManager, click  **Import key**.
Select the previously downloaded key.

3.4 Configure Deletion Policies

Deletion policies are used to control the way in which videos may or may not be automatically deleted from the system to free storage space. This is done from the **Deletion Policy** section of the **Policies** pane, in the **Admin** tab.



To reach the **Deletion Policy** section:

1. Navigate to the **Admin** tab.
2. Select the **Policies** pane.
3. Click the **Deletion Policy** section.

There are multiple categories that administrators can configure:

Footage deletion policy - this section controls the deletion policy regarding footage on VideoManager.

- If **Automatically delete old footage** is set to **On**, old footage on VideoManager will be automatically deleted.

Enter the number of days for which recorded footage should be kept before it is deleted.

Enter the number of days for which downloaded footage should be kept before it is deleted.



This differentiation is useful if footage isn't always downloaded on the same day as it is recorded, and users want more time to review footage or add it to incidents.

- If **Keep footage until auto file export complete** is set to **On**, the deletion policy will be suspended for individual videos until they have been exported. Once a video has been exported, the original video on VideoManager will be subjected to the deletion policy like normal.



*This should **not** be enabled unless users have also enabled automatic incident exports, as determined from the **Incident Exports** section of the **Policies** pane, in the **Admin** tab.*

- If **Keep all recording footage** is set to **On**, an entire recording will be kept if **one** video within it has been added to an incident.


If set to **Off**, only videos which have been added to incidents will be preserved. The larger recording will be subject to VideoManager's deletion policy like normal.

- A VB400 enables users to bookmark footage in the field, drawing attention to certain portions of footage. From the **Bookmarked footage policy** dropdown, select how bookmarked footage will be treated by VideoManager's deletion policy. The options are as follows:
 - **Keep for same period as non-bookmarked footage** - if this option is selected, the deletion policy will treat bookmarked and non-bookmarked footage identically.
 - **No automatic deletion** - if this option is selected, bookmarked footage will be entirely exempt from the deletion policy.
 - **Keep for specified amount of time** - if this option is selected, users will have the option to configure for how long bookmarked footage is kept. The default is 90 days.
- Enter the number of days for which footage is kept after deletion is requested, in case a video has been deleted accidentally.
- Enter the number of days for which footage is protected after it has been removed from an incident. Footage in an incident is never deleted unless:
 - It has been manually removed from the incident.
 - The incident it is a part of has been deleted, in which case the footage will be subject to normal deletion policies.
 - **Enable forced delete** is set to **On**, as described below.

Forced footage deletion - this section controls the deletion policy regarding automatic footage deletion.

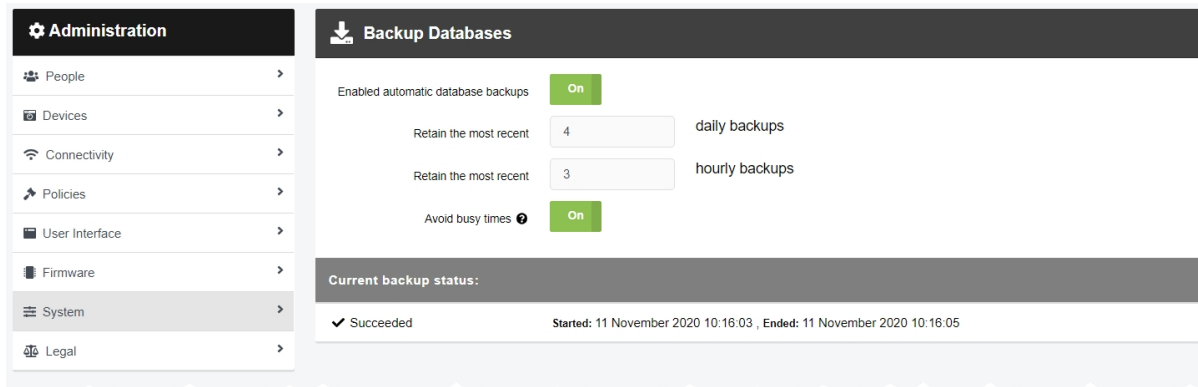
- If **Enable forced delete** is set to **On**, footage will be deleted even if it is part of an incident.

Normally, footage will never be deleted while it is part of an incident.

Optionally click  **Download Change Summary**. This will download a CSV file directly to the administrator's PC which contains information about any changes to which videos and incidents will be deleted as a result of the new policy. Click **Save settings**.

3.5 Create Backup Databases

VideoManager offers a backup database service to help prevent the loss of crucial files in the event of an IT failure. A backup contains database metadata, such as the audit log, custom configurations, and descriptions of videos, incidents, and exports. These backups will be used by Motorola Solutions to restore a user's instance of VideoManager. Backups are configured from the **Backup Databases** section of the **System** pane, in the **Admin** tab.



To create a backup database:

1. Navigate to the **Admin** tab.
2. Select the **System** pane.
3. Click the **Backup Databases** section.
4. Set **Enabled automatic database backups** to **On**.
This will enable the user to configure more settings in relation to automatic backups.
5. Enter the number of most recent **daily** and **hourly** backups that will be retained.
A **daily** backup is the last **hourly** backup within a 24-hour window. It is recommended to configure both of these settings
6. If **Avoid busy times** is set to **On**, backups will only occur when there is little or no activity occurring on VideoManager, in order to minimise system load.



*The backup function only backs up the system state - it does not back up the contents of the footage, exports or reports filespace. **Backups should be regularly transferred to a secure location offsite.***

The current backup status will be displayed at the bottom of the pane, as well as the start and end date of the backup.

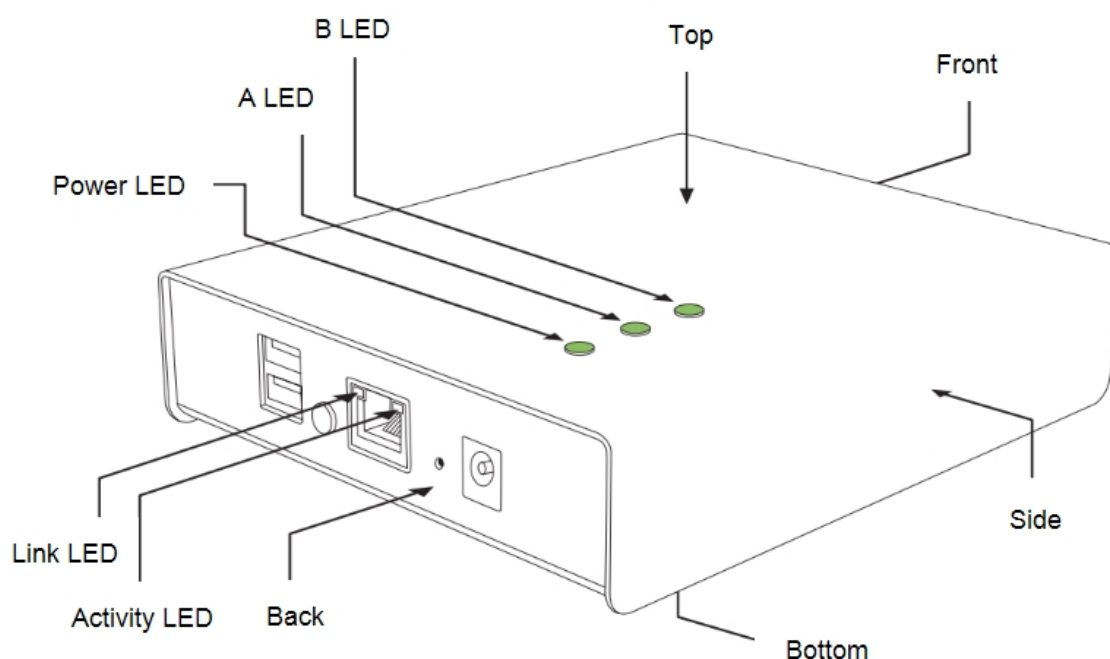
7. Click **Save settings**.

Backups will be sent to wherever has been configured from the **Storage** section.

>> For more information, see Create, Edit and Delete File Spaces on page 13

4 Connect Body-Worn Cameras to VideoManager

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



Administrators must first configure their DockController.

>> For more information, see [Configure and Connect a DockController to VideoManager](#) on page 23

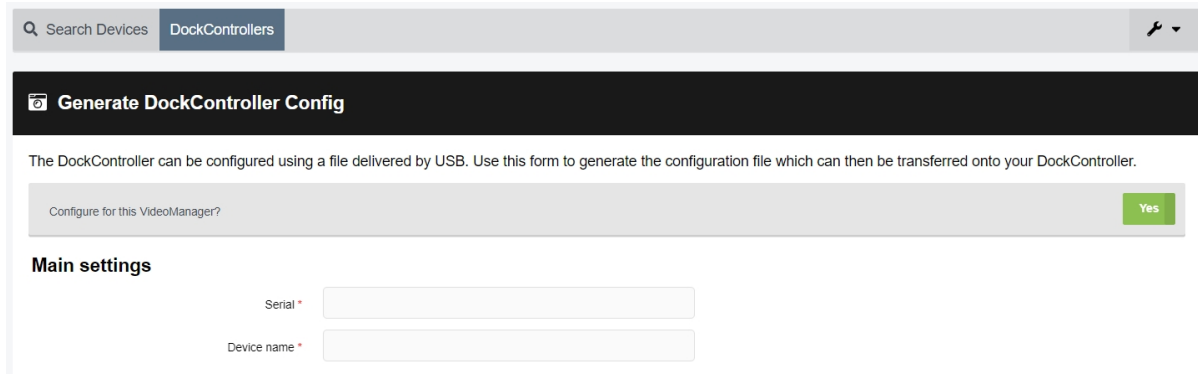
Once the DockControllers have been configured, the body-worn cameras should be connected to them. Through this, the body-worn cameras will be connected to VideoManager automatically.

>> For more information, see [Connect Docks and Body-Worn Cameras to DockControllers](#) on page 25

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



4.1 Configure and Connect a DockController to VideoManager

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



The screenshot shows the 'Generate DockController Config' form in the VideoManager interface. At the top, there is a search bar and a 'DockControllers' tab. Below the tab, a dark header bar contains the title 'Generate DockController Config'. The main content area has a sub-header 'The DockController can be configured using a file delivered by USB. Use this form to generate the configuration file which can then be transferred onto your DockController.' Below this is a checkbox labeled 'Configure for this VideoManager?' with a green 'Yes' button. Under the 'Main settings' section, there are two input fields: 'Serial *' and 'Device name *', both with red asterisks indicating required fields.

To configure a DockController:

1. Plug one end of the DockController's power cable into its power socket, and the other end into mains power.
2. Plug the Ethernet cable into the DockController's Ethernet port.
3. Plug the other end of the Ethernet cable into any available port on the Network Switch.
4. Turn the power on at the mains.
5. On VideoManager, navigate to the **Devices** tab.
6. Select the **DockControllers** pane.
7. Click  **Advanced** in the top right-hand corner.
8. Click  **Generate DockController Config**.
9. In the **Serial** field, enter the DockController's unique serial number.
This can be found on the bottom of the DockController.
10. In the **Device name** field, enter the name by which this DockController will be known on VideoManager.
11. The **Host** field should be pre-populated with VideoManager's webserver.
12. If **SSL** is set to **On**, all footage passed through this DockController will have an extra layer of encryption.
13. If **Use static IP** is set to **On**, the user must enter an IP address for the DockController.
14. From the **Security** dropdown, select what kind of whether the DockController will be protected with **WPA2-PEAP-MSCHAPV2** or not.
15. Click **Generate**.

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

16. Plug the USB drive into the same PC.

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

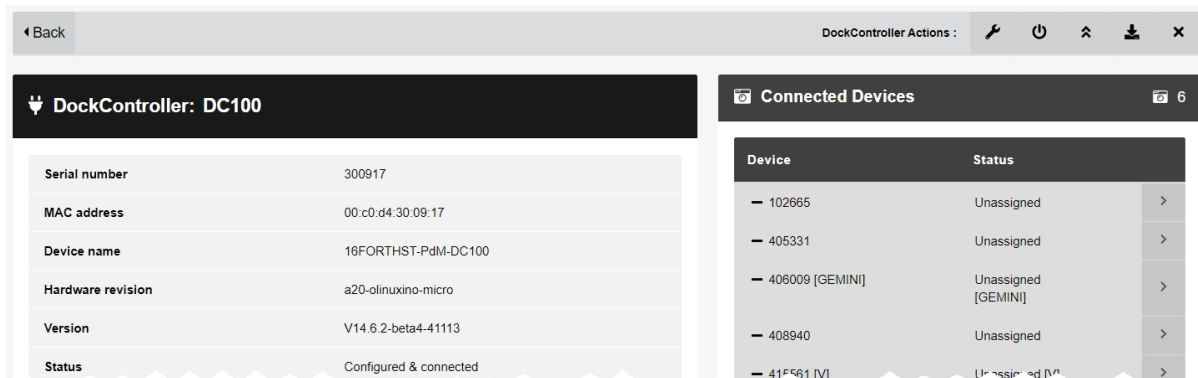
17. Drag and drop the DockController configuration file into the root folder of the USB drive.
18. Safely eject the USB drive.
19. Plug the USB drive into one of the two DockController USB ports next to the function button.



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

4.2 Connect Docks and Body-Worn Cameras to DockControllers

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



To connect docks to DockControllers:

1. Plug one end of the dock's USB into its USB port, and the other end into one of the six USB ports on the front side of the DockController.
The dock's USB indication LED will go green. This indicates that the dock is connected to the DockController.
 2. Plug one end of the dock's power cable into its power port, and the other end into mains power.
 3. Turn the power on at the mains.
The dock's power LED will go green. This indicates that the dock is receiving power.
- Repeat these steps for as many docks as necessary.

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

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

1. On VideoManager, navigate to the **Devices** tab.
2. Select the **DockControllers** pane.
3. The DockController should appear in the pane, and its status should read as **Open & Connected**.
4. Click **> View details**.
5. In the **Connected Devices** section, users can see how many body-worn cameras are connected to the DockController in question. The user can also view:

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

4.3 Connect VT-Series Cameras to VideoManager Remotely

It is possible to configure a VT-series cameras using a QR code. This is important if a user cannot configure their VT-series cameras using the VideoManager UI. There are two reasons for this: firstly, if the user will not have access to VideoManager but they need to configure their body-worn camera, and secondly, if an administrator does not have physical access to VideoManager (e.g. because it is a cloud service). By creating a QR code, they can configure the VT-series camera to connect to VideoManager via their local WiFi. The VT-series camera can then be assigned like normal.

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

1. Navigate to the **Devices** tab.
2. Click **Advanced** in the top right-hand corner.
3. Choose **Generate device config code** from the dropdown.
The **Generate Device Config Code** pane will open.
4. In the **Serial number** field, enter the VT-series camera's serial number.
5. From the **SSID** dropdown, the administrator must select the WiFi profile which will be used by the VT-series camera to connect to VideoManager. The options are as follows:





- **Enter SSID manually** - configure the WiFi network, using the **SSID** and **Password** fields, and the **Security type** dropdown.

This does **not** need to be the same network that VideoManager is operating on.

- Select a previously-created WiFi profile.
6. Click **Generate code**.
 7. The VT-series camera can now be connected to VideoManager by following the instructions onscreen.
- Once the VT-series camera has been connected to VideoManager, it can be assigned to operators like normal.

>> For more information, see Assign Body-Worn Cameras and Record Footage on page 34

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

1. The administrator must navigate to the **Devices** tab.
2. Click  **Advanced** in the top right-hand corner.
3. Choose  **Generate device config code** from the dropdown.
The **Generate Device Config Code** pane will open.
4. In the  **Info** pane, click  **Launch the public version of this page**.
5. Copy the URL, and share it with the operator. The operator can access this URL and configure the following settings:
 - In the **Serial number** field, enter the VT-series camera's serial number.
 - From the **SSID** dropdown, select the WiFi profile which will be used by the VT-series camera to connect to VideoManager. The options are as follows:
 - **Enter SSID manually** - configure the WiFi network, using the **SSID** and **Password** fields, and the **Security type** dropdown.
This does **not** need to be the same network that VideoManager is operating on.
 - Select a previously-created WiFi profile.
 - Click **Generate code**.
 - The VT-series camera can now be connected to VideoManager by following the instructions onscreen.

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

>> For more information, see Assign Body-Worn Cameras and Record Footage on page 34

5 Add Users and Roles

Every worker who will be utilising VideoManager **must** have a user created for them.

Every user **must** belong to at least one role. Roles dictate what actions a user can perform on VideoManager, what parts of the UI they can see, etc.

- Create one user for each worker who will be accessing VideoManager.

>> For more information, see Add Users on page 30

- Create roles for users on VideoManager.

>> For more information, see Add Roles on page 31

- Associate roles with previously-created users.

>> For more information, see Associate Roles With Users on page 33

5.1 Add Users

Every worker who will be utilising VideoManager must have a corresponding user. This will enable them to log in, operate devices, and perform other actions on VideoManager.

The screenshot shows the 'New User' form on the left and the 'Roles' table on the right.

New User Form:

- USER NAME ***: Enter a user name for this user
- PASSWORD**: Enter a password for the user (with an eye icon to toggle visibility)
- CONFIRM PASSWORD**: Confirm password (with an eye icon to toggle visibility)
- DISPLAY NAME**: Enter a display name for this user
- EMAIL NOTIFICATIONS**: Enter email address, with **TEST** and **OFF** buttons
- MOBILE NOTIFICATIONS**: Enter mobile number, with **TEST** and **OFF** buttons

Roles Table:

Role	Status
SYSTEM ADMINISTRATOR	OFF
ADMINISTRATOR	ON
COMPANION APP USER	OFF
DEVICE OPERATOR	OFF
INCIDENT REVIEWER	OFF
SYSTEM MANAGER	OFF
SYSTEM SUPERVISOR	OFF
SYSTEM USER	ON
SYSTEM USER [OWN ONLY]	ON

To create a user:

1. Navigate to the **Admin** tab.
2. Select the **People** pane.
3. Click the **Users** section.
4. Click **Create user**.
5. Enter the following information for the new user:
 - **User name** - enter a name for this user. No two users can have the same name on one VideoManager system. This cannot be changed later.
 - **Password** - enter a password for the user.



Once a value is entered here, the **User must change password** toggle will automatically switch to **On**.

- **Confirm password** - enter the password again to confirm it.
 - **Display name** - enter a display name for this user. This can be changed later.
 - Set **Enabled** to **On**.
6. Click **Create user**.

5.2 Add Roles

Roles are associated with users. They affect what actions a user can perform and what aspects of the UI they can see. Because roles are separate from users, one role can be associated with multiple users.

To add a role to VideoManager:




1. Navigate to the **Admin** tab.
2. Select the **People** pane.
3. Click the **Roles** section.
4. Click **Create role**.
5. Enter the following information for the new role:
 - **Name** - enter a name for this role.
 - **Description** - enter a description for this role.
 - **Default device profiles** - devices controlled by users in this role will use the device profile selected here.
6. Enable or disable permissions as necessary.
The groups of permissions are as follows:
 - **System permissions** - these permissions control users' abilities to log in to VideoManager, as well as their audit and export abilities.
 - **Video permissions** - these permissions control users' abilities regarding videos. The permissions are also sorted by four criteria:
 - **Owned** - if enabled, users can perform actions on the videos created by them.
 - **Shared** - if enabled, users can perform actions on the videos that have been shared with them by other users on the system.

- **Supervised** - if enabled, users can perform actions on the videos that have been created by other users on the system that they supervise.
- **Any** - if enabled, users can perform actions on any videos on the system, regardless of who created them.
- Incident permissions - these permissions control users' abilities regarding incidents. The permissions are also sorted by four criteria:
 - **Owned** - if enabled, users can perform actions on the incidents created by them.
 - **Shared** - if enabled, users can perform actions on the incidents that have been shared with them by other users on the system.
 - **Supervised** - if enabled, users can perform actions on the incidents that have been created by other users on the system that they supervise.
 - **Any** - if enabled, users can perform actions on any incidents on the system, regardless of who created them.
- Device permissions - these permissions control users' abilities regarding devices. The permissions are also sorted by four criteria:
 - **User** - if enabled, users can perform actions on the devices assigned to them.
 - **Supervised** - if enabled, users can perform actions on the devices that are assigned to them or other users on the system that they supervise.
 - **Any** - if enabled, users can perform actions on any device on the system.
- User permissions - these permissions control users' abilities regarding users. The permissions are also sorted by two criteria:
 - **Supervised** - if enabled, users can perform actions on the users on the system that they supervise.
 - **Any** - if enabled, users can perform actions on any user on the system.
- Notification permissions - these permissions control how notifications work (if they have been licensed).
- Report permissions - these permissions control users' abilities to create reports and view statistics.
- Advanced permissions - these permissions control users' abilities regarding advanced aspects of VideoManager. The permissions are also sorted by the following criteria:
 - **View** - if enabled, users can view certain aspects of VideoManager which would otherwise be inaccessible.
 - **Edit** - if enabled, users can edit certain aspects of VideoManager.

5.3 Associate Roles With Users

Once both users and roles have been created, roles can be associated with users. This determines the level of control users have over VideoManager.

To associate roles with users:

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 **Roles** panel, select the roles which the user will inhabit, by setting the relevant roles to **On**. The user's roles can be altered later.
If the user will be operating body-worn cameras (i.e. recording footage), the **Device Operator** role should be set to **On**.
6. Click **Save user**.

6 Assign Body-Worn Cameras and Record Footage

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

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

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

>> For more information, see Assign Body-Worn Cameras with Single Issue on VideoManager on page 35

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

>> For more information, see Assign Body-Worn Cameras with Single Issue and RFID on page 36

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

>> For more information, see Assign Body-Worn Cameras with Permanent Issue on page 37



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

>> For more information, see Assign Body-Worn Cameras with Permanent Allocation on page 38

6.1 Assign Body-Worn Cameras with Single Issue on VideoManager

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

To assign a body-worn camera with single issue:

1. Navigate to the **Devices** tab.
2. Select the  **Search Devices** pane.
3. Filter the body-worn cameras as necessary, and click **Find devices**.
4. Find a suitable body-worn camera, and click  **Assign Device** next to it.



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

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

5. In the **Operator name** field, enter the name of the user who will be recording with this body-worn camera. This must be a valid username on VideoManager.
If the user's name does not appear in the dropdown menu, they do not have the ability to operate body-worn cameras. This is due to their roles. Their roles must be changed before they can use a body-worn camera.
6. From the **Assignment mode** dropdown, select **Single issue**.
7. Select a suitable device profile from the **Device Profile** dropdown. This determines how the body-worn camera will behave - which buttons perform which actions, etc.
8. Select a previously-created WiFi profile, if necessary. This determines which WiFi profile the body-worn camera will use, and is only relevant if the body-worn camera will be streaming in the field, uploading footage over WiFi, or connecting to the Companion App.
9. Click **Assign Device**.

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





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

6.2 Assign Body-Worn Cameras with Single Issue and RFID

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

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

A user must be associated with an RFID card on VideoManager. It is only necessary to do this once. To do so:

1. Tap the relevant RFID card against the reader, and wait until it emits three low beeps.
2. Navigate to the **Admin** tab.
3. Select the  **People** pane.
4. Click the  **Users** section.
5. Next to the user which will be associated with the RFID card in question, click  **Go to user**.
6. In the **Touch Assign ID** field, click  .
The user will be taken to VideoManager's audit log, where the recent RFID scan will be visible.
7. Copy the touch assign ID from the audit log, and paste it into the **Touch Assign ID** field.
8. Click **Save user**.

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



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

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

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

6.3 Assign Body-Worn Cameras with Permanent Issue

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

1. Navigate to the **Devices** tab.
2. Select the  **Search Devices** pane.
3. Filter the body-worn cameras as necessary, and click **Find devices**.
4. Find the relevant body-worn camera, and click  **Assign Device** next to it.



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

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

5. In the **Operator name** field, enter the name of the user who will be recording with this body-worn camera. This must be a valid username on VideoManager.
If the user's name does not appear in the dropdown menu, they do not have the ability to operate body-worn cameras. This is due to the roles they inhabit. Their roles must be changed before they can use a body-worn camera.
6. From the **Assignment mode** dropdown, select **Permanent issue**.
7. Select the relevant device profile from the **Device Profile** dropdown. This determines how the body-worn camera will behave - which buttons perform which actions, etc.
8. Select a previously-created WiFi profile, if necessary. This determines which WiFi profile the body-worn camera will use, and is only relevant if the body-worn camera will be streaming in the field, uploading footage over WiFi, or connecting to the Companion App.
9. Click **Assign Device**.

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





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

6.4 Assign Body-Worn Cameras with Permanent Allocation



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

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

A user must be associated with an RFID card on VideoManager. It is only necessary to do this once. To do so:

1. Tap the relevant RFID card against the reader, and wait until it emits three low beeps.
 2. Navigate to the **Admin** tab.
 3. Select the  **People** pane.
 4. Click the  **Users** section.
 5. Next to the user which will be associated with the RFID card in question, click  **Go to user**.
 6. In the **Touch Assign ID** field, click  .
The user will be taken to VideoManager's audit log, where the recent RFID scan will be visible.
 7. Copy the touch assign ID from the audit log, and paste it into the **Touch Assign ID** field.
 8. Click **Save user**.
- From now on, the RFID card will be associated with the relevant user.

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

1. Navigate to the **Devices** tab.
2. Select the  **Search Devices** pane.
3. Filter the body-worn cameras as necessary, and click **Find devices**.
4. Find the relevant body-worn camera, and click  **Assign Device** next to it.



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

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

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

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

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

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

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

7 Glossary

A

Access Control Key

The security mechanism that prevents unauthorised body-worn cameras from connecting to VideoManager - in addition, if a body-worn camera is lost or stolen, its recorded footage cannot be recovered unless the person who has possession of the body-worn camera also has its access control key.

Asset

Any non-video import to VideoManager. This could be a PDF, a still image, or an audio file.

Assigned/Unassigned

If a body-worn camera has been assigned, it has been paired with a user and can record footage. An unassigned body-worn camera has not been paired with a user, and cannot record footage until it has been assigned.

Audit Log

The trail of information that records every action on the system. This includes when people logged on, logged off, whether they docked or undocked body-worn cameras, deleted videos, etc. This trail is not deletable.

B

Bandwidth Rule

A configurable rule that determines when footage is uploaded from sites to the Central VideoManager. This is useful if remote workers don't want to put strain on their home WiFi during high-traffic hours.

C

Companion App

Motorola Solutions' Companion App enables users who are still in the field to view, and categorise, footage they have recently recorded.

D

Dashboard

VideoManager's homepage, to which all users are automatically directed upon logging in. If an administrator has created a message for users, they will see it here.

Device

Motorola Solutions equipment which has been associated with VideoManager (e.g. body-worn cameras, DockControllers).

Display Name

The name of a user that will be presented to others on the VideoManager system - this is not necessarily the same as a username.

DockController

A device which converts the videos from body-worn cameras into data that can be sent over a network or the internet - this allows up to 84 body-worn cameras to be used with just one DockController, and enables these body-worn cameras to be installed away from the physical VideoManager server.

E

EdgeController

A small embedded computer with inbuilt storage, which provides remote or home-based workers with a docking location for their body-worn cameras. They are used exclusively as a site, connected to a Central VideoManager.

Export

Incidents which have been exported from VideoManager to the user's PC. A version of the incident will remain on VideoManager.

I

Incident

A collection of evidence - such as footage, notes, and users - which can be exported or shared with people outside of VideoManager. In some lines of work, this is known as an exhibit.

Incident Clip

Any video which has been added to an incident.

L

Licence

Some features on VideoManager are not available unless a licence has been obtained from Motorola Solutions. Such features include assisted redaction, Tactical VideoManager, and ONStream.

M

Media

Any videos or assets which can be added to an incident for evidential purposes.

O

ONStream

A licensed feature from Motorola Solutions which enables body-worn cameras to send a live stream to VideoManager over WiFi.

Operator

By default, this is the user who recorded the video on a body-worn camera, or imported the asset into VideoManager (either manually, or as configured in an automatic import profile).

Owner of a Video/Asset

This is the user who has administrative control over a video/asset. By default, this is the user who recorded the video on a body-worn camera, or imported the asset into VideoManager (either manually, or as configured in an automatic import profile). However, this can be changed to a senior user with more permissions.

Owner of an Incident

This is the user who has administrative control over the incident. By default, this is the user who created the incident. However, this can be changed to a senior user with more permissions.

P

Permanent allocation

If a body-worn camera has been assigned to a user with permanent allocation, it will be assigned to the user permanently, even when it is redocked. It does not need to be reassigned every time the user wishes to use it. Unlike permanent issue, the user can only undock the body-worn camera with RFID touch assign.

Permanent issue

If a body-worn camera has been assigned to a user with permanent issue, it will be assigned to the user permanently, even when it is redocked. It does not need to be reassigned every time the user wishes to use it.

Permission

An individual rule which determines the actions users can perform on VideoManager.

Post-record

The video immediately following an event which is captured automatically, once the operator stops recording. This could be between 1 and 120 seconds.

Pre-record

The video preceding an event which is automatically captured as soon as an operator starts recording. This could be between 1 and 120 seconds.

R

Recording

This is the complete footage recorded by a body-worn camera, from the moment it is prompted to start recording until the moment it is prompted to stop (including any pre- and post-record periods). A recording will be split into multiple videos if it reaches a certain length, as defined in the body-worn camera's device profile.

Recording ID

A unique ID that identifies a specific recording. If a recording has been split up into multiple videos (due to the device profile of the body-worn camera that recorded it), these videos will all have the same recording ID.

Report

Instead of applying permissions directly to users, they are applied to a role, which is then applied to a user. This means that multiple users can belong to the same role.

S

Saved Search

VideoManager allows incident searches to be saved and re-searched by other users on the system as many times as necessary.

Single issue

If a body-worn camera has been assigned to a user with single issue, it will only be assigned to the user for one trip. Once the body-worn camera is redocked, it will return to the pool and can be assigned to a different user.

System Administrator

A role which cannot be edited or deleted. Any users with this role will be able to access any aspect of VideoManager.

U**User**

Every individual on an instance of VideoManager must have their own user.

User-Specific WiFi Network

A WiFi network that only appears on the dashboard of the user who configured it - for instance, a mobile phone hotspot for streaming that other users shouldn't be able to access.

V**VB200**

A robust body-worn camera designed and sold by Motorola Solutions. It can record for up to 8 hours and has 16GB of recording storage.

VB300

A robust body-worn camera designed and sold by Motorola Solutions. It can record for up to 8 hours in HD and has 32GB of recording storage. It also has the ability to livestream footage to VideoManager over a WiFi network.

VB400

A robust body-worn camera designed and sold by Motorola Solutions. It can record for up to 8 hours in full HD and has 32GB of recording storage. It also has GPS-tracking, Bluetooth functionality, and can livestream footage to VideoManager over a WiFi network.

Video

A section of a recording, the length of which is determined by the body-worn camera's device profile.

Video ID

A unique ID that identifies a specific video/asset. It is used in the audit log to record which video/asset an entry refers to, and can be used to locate videos/assets.

VT100

A VT100 is a lightweight, discreet body-worn camera designed and sold by Motorola Solutions. It can record for up to 4 hours, and has the capacity to livestream footage to VideoManager if connected to WiFi. It is the first body-worn camera in Motorola Solutions' VT-series camera range to have haptic feedback.

VT50

A lightweight, discreet body-worn camera designed and sold by Motorola Solutions. It can record for up to 2 hours, and has the capacity to livestream footage to VideoManager if connected to WiFi.

W

WiFi Profile

A collection of individual WiFi networks that is then applied to a body-worn camera. The body-worn camera in question will stream to VideoManager over these networks.

For more information, please visit: www.motorolasolutions.com.

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

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

© 2015 - 2021 Motorola Solutions, Inc. All rights reserved. (ED-012-213-06)