VideoManager EX 16.0 Getting Started Guide

This document is intended to serve as a reference to administrators when installing and configuring an on-premises instance of VideoManager EX for the first time.

Copyright

Intended purpose

This document is intended to serve as a reference to administrators when installing and configuring an on-premises instance of VideoManager EX for the first time.

Document ID

ED-012-254-01-NA

Conventions

This document uses the following conventions:

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

Contact address

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

Safety notices

Caution

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

Additional information relating to the current section.

Contents

1 Welcome to VideoManager EX

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

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

For more complex procedures, please consult the VideoManager EX admin guide.

2 Initial Configuration

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

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depending on whether VideoManager EX is being downloaded for the first time, or being re-downloaded (i.e. to obtain a newer version of the software).

- Download VideoManager EX for the first time.

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

- Re-download VideoManager EX.

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

2.1 Download VideoManager EX

If this is the first time that VideoManager EX is being installed on this PC:

1. Ensure that you have valid Software Assurance from Motorola Solutions.

Please contact your account manager to obtain Software Assurance.

2. Double-click the downloaded **VideoManager EX-setup-16.0.exe** file.
3. Confirm that the installer can make changes to the PC.
4. The VideoManager EX installer will open. Click ***Next***.
5. The administrator will be given the option to change where VideoManager EX is installed on their PC - once the destination has been chosen, click ***Install***.

VideoManager EX will be downloaded.

6. Click ***Finish***.
7. Multiple installers will open. Click through every one by clicking ***Next*** and ***Finish***.
8. Navigate to VideoManager EX'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 EX data will be stored in VideoManager EX's default database.
    - ***Use external SQL Server database (advanced)*** - if there is an existing SQL Server, the administrator can connect it to VideoManager EX 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 EX 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 about setting up Azure authentication with VideoManager EX, please navigate to the Motorola Solutions Learning Experience Portal (registration is free) and search for VideoManager EX and SQL Server Explained.

12. The administrator will be prompted to create a VideoManager EX 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 media is sent initially:
    - If ***Encrypt Media*** is set to ***On***, all media will automatically be encrypted when sent between body-worn cameras and VideoManager EX.
    - In the ***Storage Location*** field, enter the path to which all media will be sent.

    This can be changed later.

>> For more information, see Create, Edit and Delete File Spaces on page 14

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

2.2 Re-Download VideoManager EX

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

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

Please contact your account manager to obtain Software Assurance.

2. Double-click the downloaded **VideoManager EX-setup-16.0.exe** file.
3. Confirm that the installer can make changes to the PC.
4. The administrator will be asked to uninstall the old version of VideoManager EX. 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 EX installer will open. Click ***Next***.
6. The administrator will be given the option to change where VideoManager EX is installed on their PC - once the destination has been chosen, click ***Install***.

VideoManager EX 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 EX to load after being updated - the administrator should refresh their browser if VideoManager EX 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 EX settings that must be configured before any users can start utilizing the system.

1. Configure the webserver. This enables users to access VideoManager EX from their browsers, instead of needing access to the PC running VideoManager EX.

>> For more information, see Configure the Web Server on page 10

2. Optionally configure storage settings. Although VideoManager EX prompts the administrator to configure storage when the licence agreement is first accepted, it is also possible to change these settings post-installation.

>> 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 your instance of VideoManager EX.

>> For more information, see Create, Import, and Export Access Control Keys on page 19

4. Configure the deletion policy. This dictates when old media will be automatically deleted.

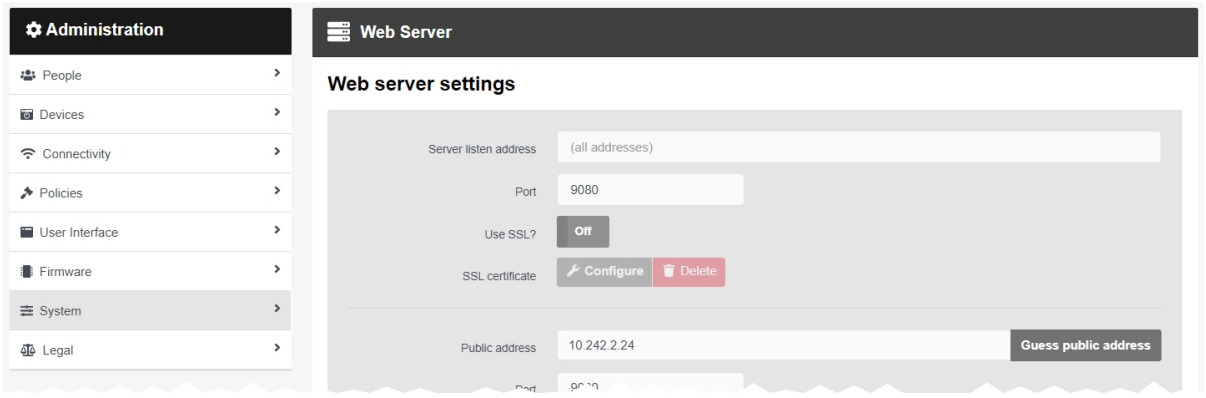
>> For more information, see Configure Deletion Policies on page 21

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

>> For more information, see Create Backup Databases on page 23

3.1 Configure the Web Server

The ***Web Server*** pane is used to control how VideoManager EX 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 EX. This should ordinarily be the local IP address of the server running VideoManager EX. If the administrator does not know this address, they should click ***Guess public address***
    - ***Port*** - the port which VideoManager EX will listen on. By default, this is 9080.
    - ***Public address*** - this is the address which users can use to access VideoManager EX if they are not on the same network as the server. ***Guess public address*** will try to guess what this address should be.
    - ***Port*** - the port which VideoManager EX uses to listen to traffic, including Dock-Controller and body-worn camera information.
    - ***Use SSL?*** - if enabled, then SSL will be used to secure connections to the ***Public address***.

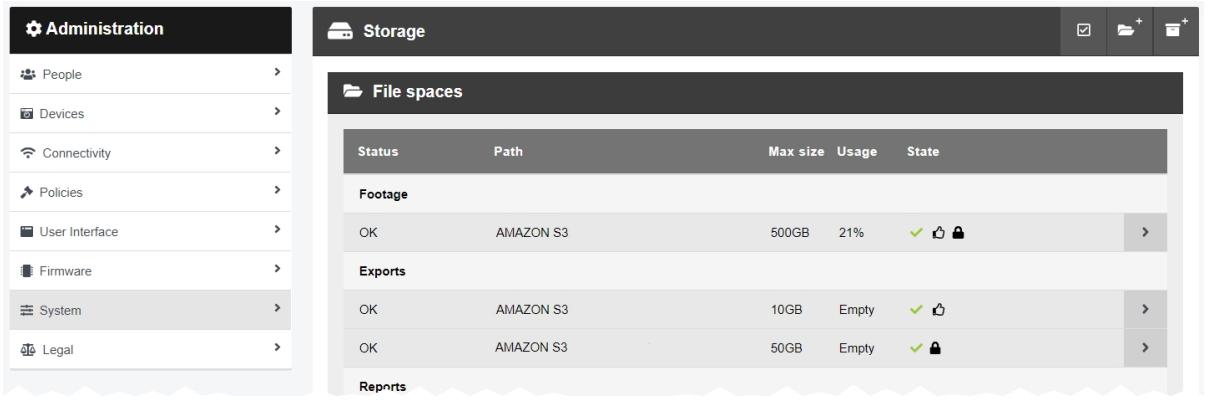
    The server's listen address and public address are shown at the bottom of the pane.

5. Click ***Save settings***.

3.2 Configure Storage

VideoManager EX 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 administrator can configure file spaces for backups, exports, reports, and media.

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).

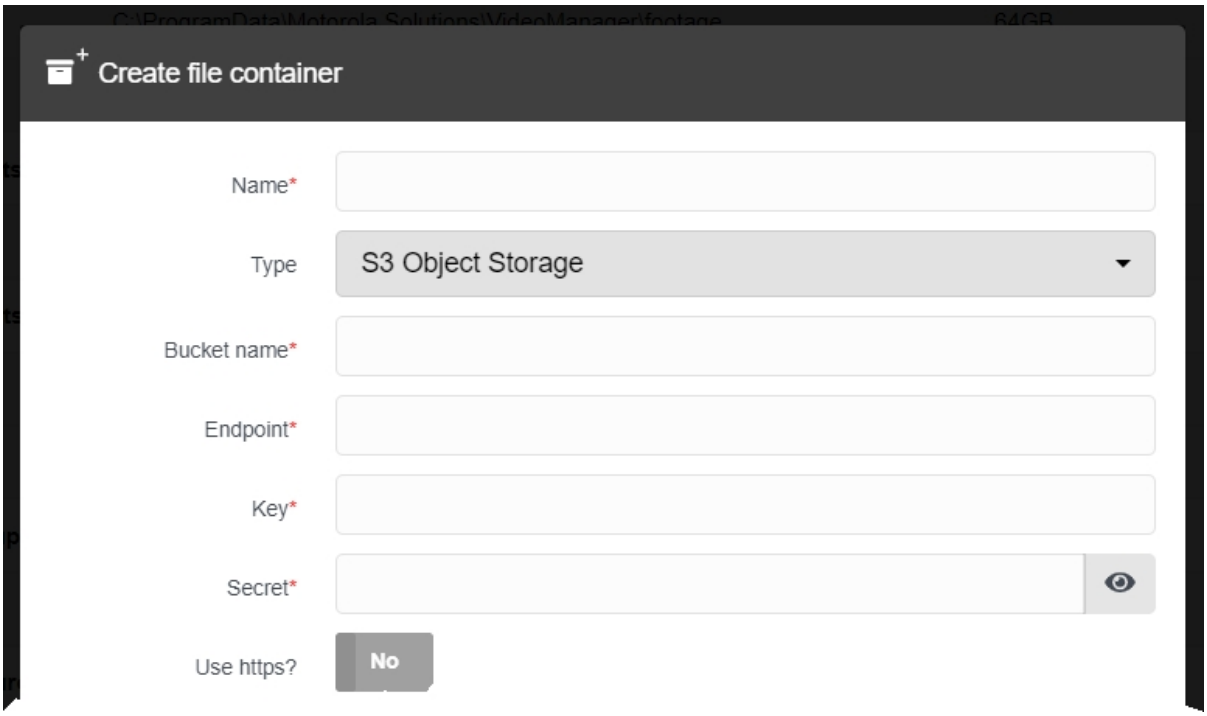
>> For more information, see Create, Edit and Delete File Containers on page 12

- Create, edit and delete file spaces.

>> For more information, see Create, Edit and Delete File Spaces on page 14

3.2.1 Create, Edit and Delete File Containers

If media and other data will be stored in object storage instead of a file system, administrators must create file containers on VideoManager EX which contain information about the object store. This enables file spaces on VideoManager EX to connect to the cloud. This configuration is completed from the ***Storage*** section of the ***System*** pane, in the ***Admin*** tab.



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

To create a file container for use with file spaces:

1. Navigate to the ***Admin*** tab.
2. Select the ***System*** pane.
3. Click the ***Storage*** section.
4. Click ***Create file container***.
5. In the ***Name*** field, enter a name for the file container. This will be how the file container is identified on VideoManager EX.
6. From the ***Type*** dropdown, select either **S3 Object Storage** or **Azure Blob Storage**.

The following steps differ, depending on the kind of storage purchased by the administrator.

If the administrator is using S3 Object Storage:

1. In the ***Bucket name*** field, enter the bucket name. Motorola Solutions suggests using VideoManager EX's unique fully qualified domain name.
2. In the ***Endpoint*** field, enter the endpoint of the file container.

To check this information, open the AWS console, navigate to the ***Properties*** tab, and select the ***Bucket overview*** pane. In the ***Region*** section, make a note of the region. Enter it in the ***Endpoint*** field, with the format `s3.region code.amazonaws.com` (where `region code` is replaced with the region).

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

3. In the ***Key*** and ***Secret*** fields, enter the IAM user's key and secret, respectively.

The administrator can only get this information immediately after creating an IAM user with S3 access. If the administrator does not have the key and secret for the IAM user, they must create another user and make a note of the key and secret's information which is presented when the user is saved.

If the administrator is using Azure Blob Storage:

1. In the ***Container name*** field, enter the name of the container.

The administrator can either enter the name of a container that already exists in their Azure account, or enter the name for a new container. If a new container name is entered, Azure Blob Storage will automatically create the container - to check whether this has been successful, on Azure, navigate to the ***Storage accounts*** tab, select the ***Storage account*** pane, and click the ***Containers*** section. The new container should be visible.

2. In the ***Endpoint*** field, enter the endpoint of the file container.

To check this information, in the ***Endpoints*** tab, click the ***Blob service*** pane, and copy and paste the value from the ***Blob service field***.

3. In the ***Account*** field, enter the name of the Azure Blob Storage account.
4. In the ***Secret*** field, enter the container's secret.

To check this information, on Azure, navigate to the ***Access Keys*** tab, click ***Show keys***, and copy and paste either of the keys.

Click ***confirm***.

3.2.2 Create, Edit and Delete File Spaces

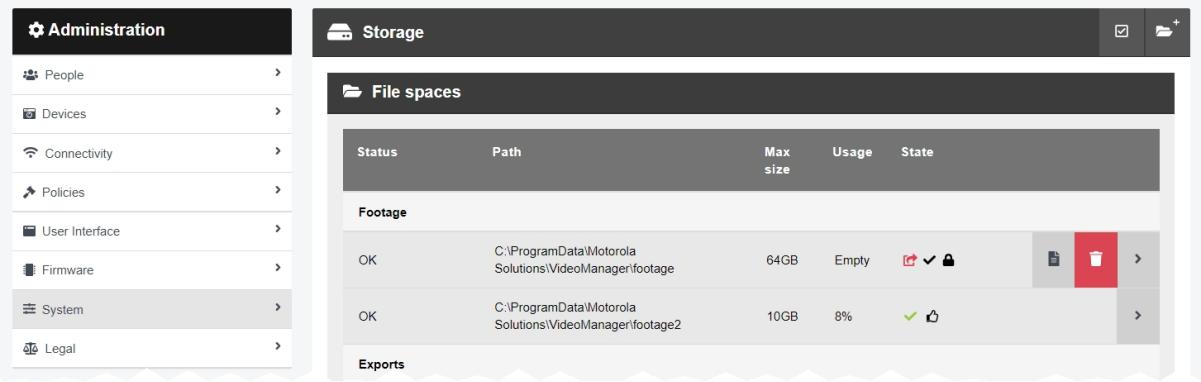
File spaces determine where files from VideoManager EX are stored, how much space VideoManager EX can use, and whether the files are encrypted when they are stored. Files can be stored on the administrator's PC (if administrators have accepted the default file space configuration, file spaces will be 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 EX has been configured to use a different kind of storage.

Caution

*VideoManager EX **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 EX.*

Body-worn 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. Motorola Solutions recommends dedicated network attached storage for this reason. When file spaces are full, associated system functions will stop working - for example, body-worn cameras will be unable to download media files, and will enter an error state.

Administrators can administer their file spaces, which includes creating new file spaces, moving files within them, increasing their sizes, and deleting them. This is done from the ***Storage*** section of the ***System*** pane, in the ***Admin*** tab.



It is possible to create new file spaces alongside existing ones. This may 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. To create a new 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.

If the administrator has purchased S3 Object Storage or Azure Blob Storage, they should enter the name of a folder within the bucket, which will then be created.

Administrators using a grid configuration must ensure that this path can be accessed by all Workers in the grid. For more information about setting up Azure authentication with VideoManager EX, please navigate to the Motorola Solutions Learning Experience Portal (registration is free) and search for VideoManager EX and Grids Explained.

6. From the ***Category*** dropdown, select a category for the file space. The options are as follows:
    - ***Footage*** - this is where media on VideoManager EX will be stored. Additionally, imported media files will be stored here, too.
    - ***Exports*** - this is where exports on VideoManager EX will be stored.
    - ***Reports*** - this is where reports on VideoManager EX will be stored.
    - ***Backups*** - this is where system backups on VideoManager EX will be stored.
    - ***Resources*** - this is where theme resources on VideoManager EX (such as logos, colour schemes, and device firmware) will be stored.
    - ***Import Workspace*** - this is where temporary files are stored. This is only necessary if a grid system with import workers is being used with VideoManager EX.
7. From the ***Container*** field, select the type of container for this file space. The options are as follows:
    - **Filesystem** - the file space will be contained in the filesystem.
    - If the administrator has created a file container whose details correspond to either a S3 Object Storage or Azure Blob Storage container, this can be selected instead.
8. In the ***Max size*** field, enter the maximum size that VideoManager EX will 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 EX will behave incorrectly when the disk/drive is completely full.

Because many object storage systems don't have a maximum capacity, this field ensures that storage costs are capped.

9. From the ***State*** dropdown, select a state for the file space. In most cases, this will be **Online**. However, administrators can also select:
    - **OBSOLETE** - files in an obsolete file space are still available, but no new files will be written to the file space.

- **Offline** - normally, if a file space is unexpectedly unavailable, then VideoManager EX will stop writing files to **all** file spaces. However, if a file space is marked as offline, then VideoManager EX can continue using other file space. Files in the offline file space will be unplayable and inaccesible.
- **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 not have any new files written to it, but the existing files within it should be kept.

If another administrator 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.

10. From the ***Encryption*** dropdown, select an encryption type (if relevant). The options are **None**, **AES-128**, **AES-192**, or **AES-256**.

This cannot be changed later. If an encryption mode is chosen, administrators **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 administrators choose **AES-256***.*

11. If ***Preferred*** is set to ***Yes***, all information relevant to this file space will be sent to this file space until it is full.

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

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

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

Administrators may wish 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. To do so:

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. 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. This may take some time.
10. Once the old file space has been fully evacuated, it can be deleted, by clicking ***Delete file space***.

Alternatively, administrators can change the path of **the original file space itself**. Before doing so, the VideoManager EX service must be stopped from the services control panel on the PC running VideoManager EX. The administrators can then manually move the files to the new location (e.g. by dragging and dropping the files into the new location on the PC). Finally, on VideoManager EX, they must create the new file space:

1. Navigate to the ***Admin*** tab.
2. Select the ***System*** pane.
3. Click the ***Storage*** section.
4. Next to the file space whose path will be changed, click ***Go to file space***.
5. Click ***Change***.
6. Enter the new path.
7. Click ***confirm***.

Caution *VideoManager EX will not save the changes if the data has not already been manually moved to the location specified in the new path.*

Administrators can change the size of a file space once it has been created. This may be necessary if **more space** has become available (e.g. because the size of the disk has increased), **less space** has become available (e.g. because the disk is being used for another function), or space should be redistributed between file spaces. To change the size of a file space:

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.

Caution *The administrator cannot make the file space smaller than the size of the files which are already in the file space.*

6. Click ***confirm***.

It may become necessary to delete a file space altogether. This process involves evacuating all files in the file space to another suitable file space. To delete a file space:

1. Ensure that there is at least one other file space on VideoManager EX 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***.

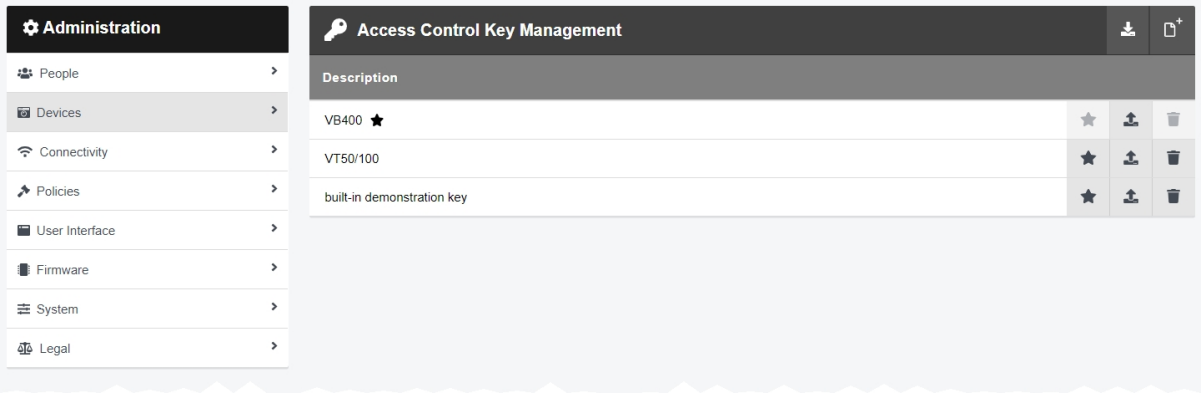
The data in the deleted file space will be evacuated to the other file space(s). This may take hours or days, depending on the amount of information in the file space.

5. Once the evacuation has finished, the administrator can optionally click ***Evacuation report*** to check that all of the files have been evacuated correctly.
6. Next to the now-empty file space, click ***Delete file space***.

Caution *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.*

3.3 Create, Import, and Export Access Control Keys

Access control keys are the mechanism that VideoManager EX uses to encrypt media files. They also prevent body-worn cameras from communicating with unauthorised instances of VideoManager EX. 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 media 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 EX, they **must** import the corresponding access control key into that instance of VideoManager EX as well - otherwise, the body-worn camera will appear as **locked** and the administrator will not be able to access any media on the body-worn camera which has not already been downloaded to VideoManager EX. To do so:

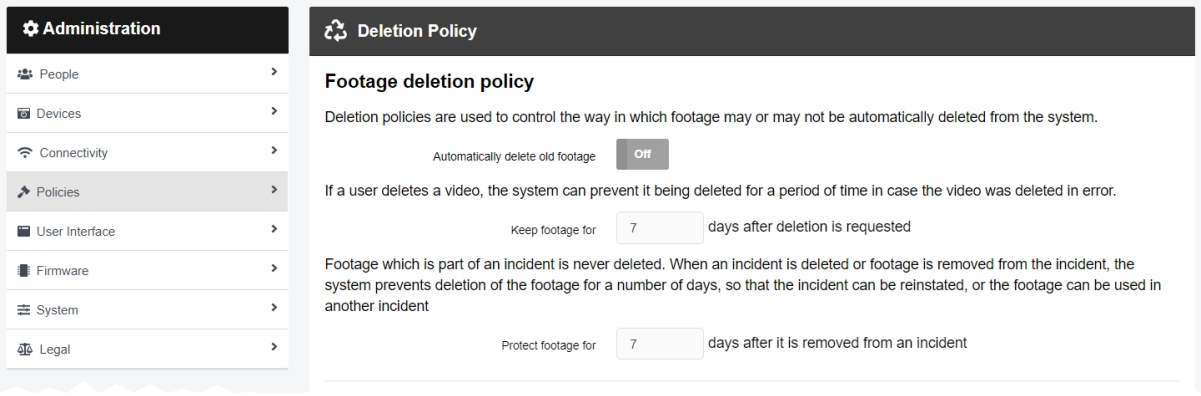
1. In the original VideoManager EX instance, next to the access control key, click ***Export key***.

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

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

3.4 Configure Deletion Policies

Deletion policies are used to control the way in which media files 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 media on VideoManager EX.

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

This differentiation is useful if media isn't 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 will be suspended for individual media files until they have been exported. Once a media file has been exported, the original media file on VideoManager EX will be subjected to the deletion policy like normal.

Caution

*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** media file within it has been added to an incident.

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

- The ***Bookmarked footage policy*** dropdown is not relevant to the VideoManager EX user interface.

- A VB400 enables users to bookmark media in the field, drawing attention to certain portions of media. From the ***Bookmarked footage policy*** dropdown, select how bookmarked media will be treated by VideoManager EX's deletion policy. The options are as follows:

  - **Keep for same period as non-bookmarked media** - if this option is selected, the deletion policy will treat bookmarked and non-bookmarked media identically.
  - **No automatic deletion** - if this option is selected, bookmarked media 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 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 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 media deletion.

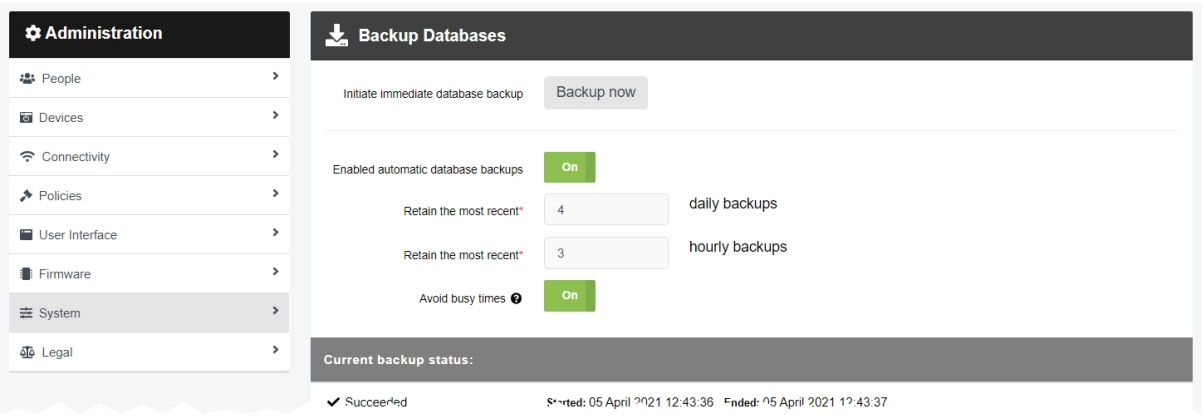
- If ***Enable forced delete*** is set to ***On***, media will be deleted even if it is part of an incident.

Normally, media 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 media files and incidents will be deleted as a result of the new policy. Click ***Save settings***.

3.5 Create Backup Databases

VideoManager EX 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 will be used by Motorola Solutions to restore an administrator's instance of VideoManager EX. Backups are configured from the ***Backup Databases*** section of the ***System*** pane, in the ***Admin*** tab.



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

Administrators can initiate an immediate backup. This will capture VideoManager EX's state at the time when the immediate backup was created. To do so:

1. Navigate to the ***Admin*** tab.
2. Select the ***System*** pane.
3. Click the ***Backup Databases*** section.
4. Click ***Backup now***.

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

>> For more information, see Create, Edit and Delete File Spaces on page 14

Administrators can also configure recurring backups, which run automatically every hour. To do so:

1. Navigate to the ***Admin*** tab.
2. Select the ***System*** pane.
3. Click the ***Backup Databases*** section.
4. Set ***Enabled automatic database backups*** to ***On***.

This will enable the administrator to configure more settings in relation to automatic backups.

5. Enter the number of most recent **daily** and **hourly** backups that will be retained.

A **daily** backup is the last **hourly** backup within a 24-hour window. It is recommended to configure both of these settings

6. If ***Avoid busy times*** is set to ***On***, backups will only occur when there is little or no activity occurring on VideoManager EX, in order to minimise system load.
7. Click ***Save settings***.

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

>> For more information, see Create, Edit and Delete File Spaces on page 14

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

4 Connect Body-Worn Cameras to VideoManager EX

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

To configure both docks and a DockController:

1. Configure the DockController.

>> For more information, see Connect a DockController to VideoManager EX on page 26

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

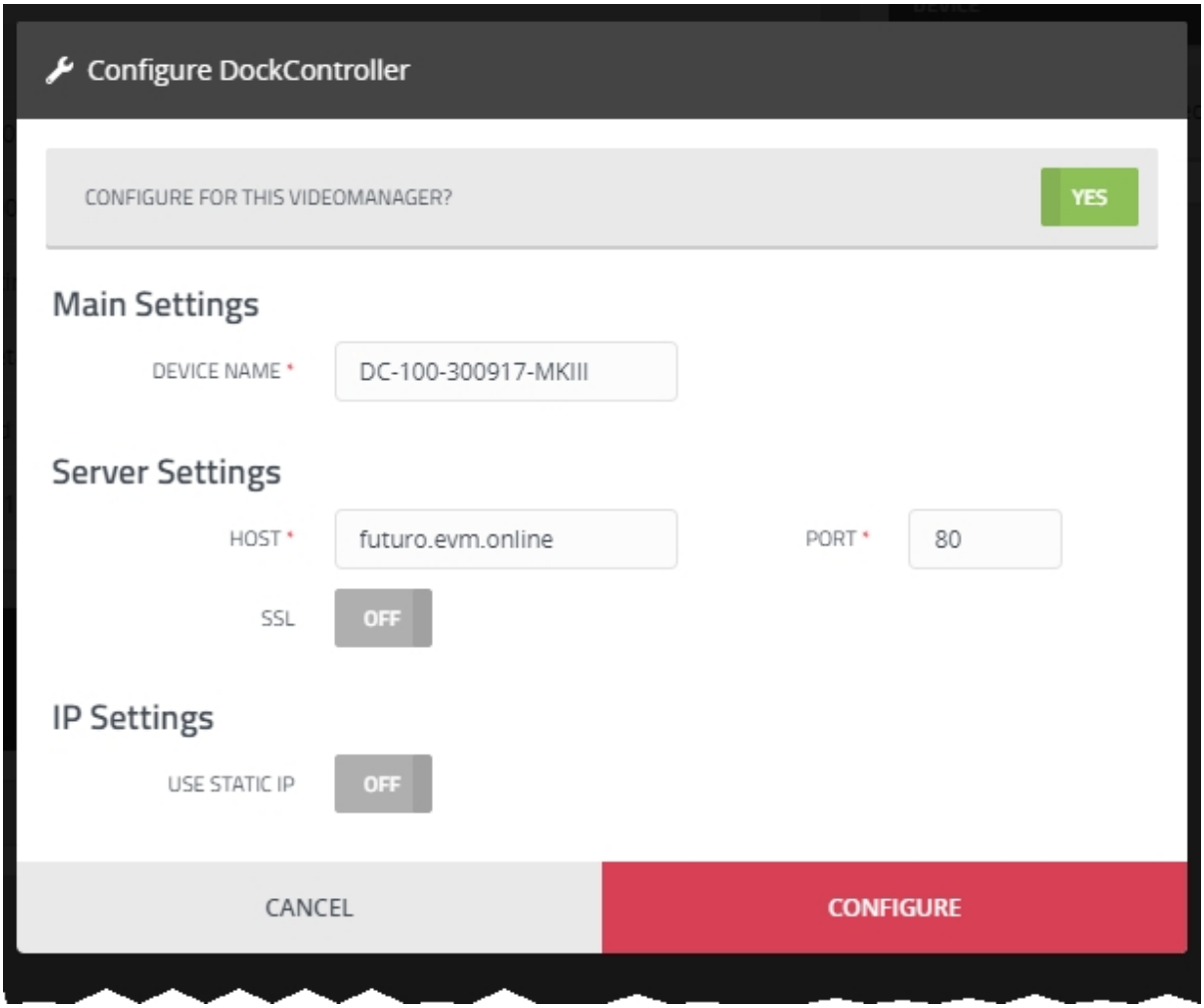
>> For more information, see Connect Docks and Body-Worn Cameras to DockControllers on page 28

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

>> For more information, see Connect a Solo Dock to VideoManager EX on page 30

4.1 Connect a DockController to VideoManager EX

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



To configure a DockController:

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

For more information about DockControllers, please see the DockController Quickstart Guide. This can be downloaded here.

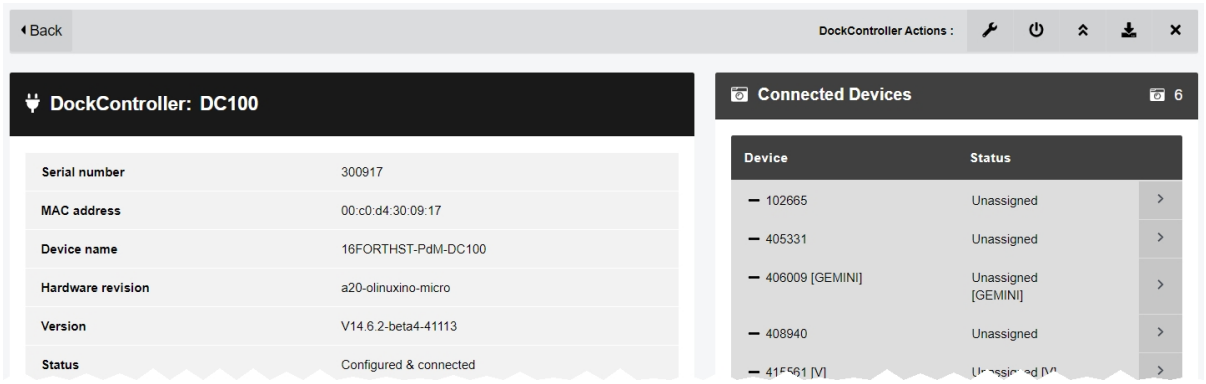
5. On VideoManager EX, navigate to the ***Devices*** tab.
6. Select the ***DockControllers*** pane.

7. Click ***Advanced*** in the top right-hand corner.
8. Click ***Generate DockController Config***.
9. In the ***Serial*** field, enter the DockController's unique serial number.
   This can be found on the bottom of the DockController.
10. In the ***Device name*** field, enter the name by which this DockController will be known on VideoManager EX.
11. The ***Host*** field should be pre-populated with VideoManager EX's webserver.
12. If ***SSL*** is set to ***On***, all media passed through this DockController will have an extra layer of encryption.
13. If ***Use static IP*** is set to ***On***, enter an IP address for the DockController.
14. From the ***Security*** dropdown, select whether the DockController will be protected with **802.1x (WPA2-PEAP-MSCHAPV2)** or not.
15. Click ***Generate***.
    The file will be saved to the PC's default downloads location.
16. Plug the USB drive into the same PC.
    The USB drive must have **FAT32 format**.
17. Drag and drop the DockController configuration file into the root folder of the USB drive.
18. Safely eject the USB drive.
19. Plug the USB drive into one of the two DockController USB ports next to the function button.

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

4.2 Connect Docks and Body-Worn Cameras to DockControllers

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



To connect a 14-slot dock to a DockController:

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

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

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

3. Turn the power on at the mains.

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

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

To connect a solo dock to a DockController:

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

   Repeat these steps for up to four solo docks.

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

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

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

2. Select the ***DockControllers*** pane.

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

4. Click > ***View details***.

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

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

4.3 Connect a Solo Dock to VideoManager EX

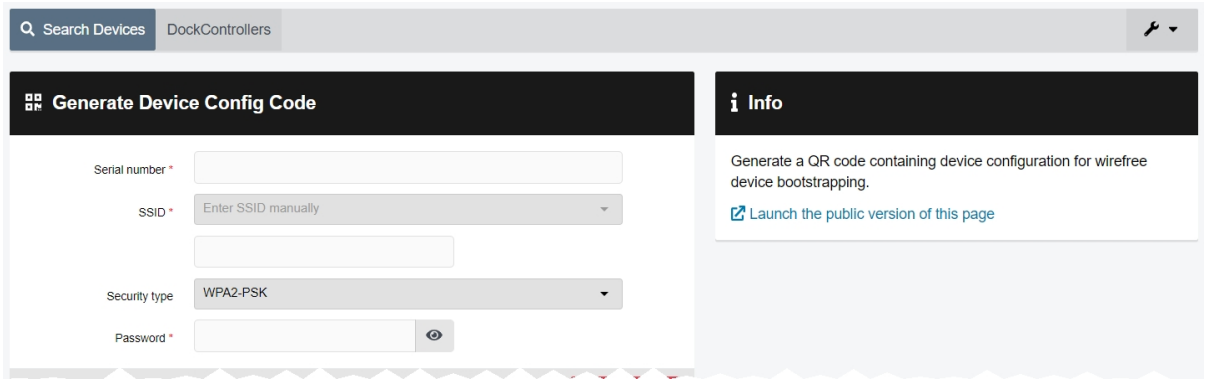
If the administrator has not purchased a DockController, it is possible to connect a solo dock directly to the PC running VideoManager EX. To do so:

1. Plug the dock's USB into the PC running VideoManager EX.
2. Insert the body-worn camera into the dock.
3. On VideoManager EX, navigate to the ***Devices*** tab.
4. Click ***Find devices***.
5. The body-worn camera should be visible, and its status should read as ***Unassigned***.

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

4.4 Connect VT-Series Cameras to VideoManager EX Remotely

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



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

1. Navigate to the ***Devices*** tab.
2. Click ***Advanced*** in the top right-hand corner.
3. Choose ***Generate device config code*** from the dropdown.

The ***Generate Device Config Code*** pane will open.

4. In the ***Serial number*** field, enter the VT-series camera's serial number.
5. From the ***Network name (SSID)*** dropdown, the administrator must select the WiFi profile which will be used by the VT-series camera to connect to VideoManager EX. The options are as follows:

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

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

   - Select a previously-created WiFi profile.

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

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

>> For more information, see Assign Body-Worn Cameras and Record Media on page 37

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

1. The administrator must navigate to the ***Devices*** tab.
2. Click ***Advanced*** in the top right-hand corner.
3. Choose ***Generate device config code*** from the dropdown.

The ***Generate Device Config Code*** pane will open.

4. In the ***Info*** pane, click ***Launch the public version of this page***.
5. Copy the URL, and share it with the operator. The operator can access this URL and configure the following settings:
    - In the ***Serial number*** field, enter the VT-series camera's serial number.
    - From the ***Network name (SSID)*** dropdown, select the WiFi profile which will be used by the VT-series camera to connect to VideoManager EX. The options are as follows:
        - **Enter Network name (SSID) manually** - configure the WiFi network, using the ***Network name (SSID)*** and ***Password*** fields, and the ***Security type*** dropdown.

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

        - Select a previously-created WiFi profile.
    - Click ***Generate code***.
    - The VT-series camera can now be connected to VideoManager EX by following the instructions onscreen.

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

>> For more information, see Assign Body-Worn Cameras and Record Media on page 37

5 Add Users and Roles

Every worker who will be utilising VideoManager EX **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 EX, what parts of the UI they can see, etc.

By default, VideoManager EX comes with the following roles pre-configured:

- Optionally create new roles for users on VideoManager EX.

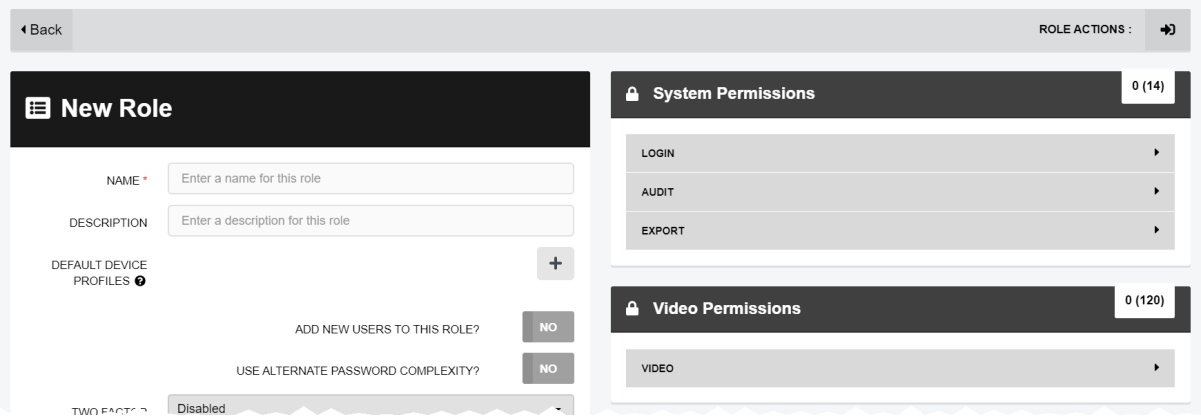
>> For more information, see Add Roles on page 34

- Create one user for each worker who will be accessing VideoManager EX, and associate the previously-created roles with them.

>> For more information, see Add Users on page 36

5.1 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 EX:

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:

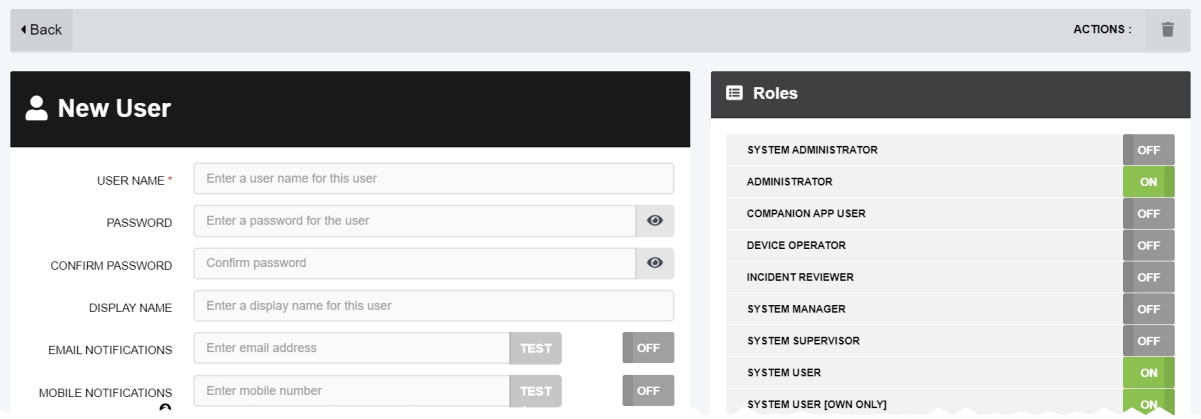
- System permissions - these permissions control users' abilities to log in to VideoManager EX, as well as their audit and export abilities.
- Media file permissions - these permissions control users' abilities regarding media files. The permissions are also sorted by four criteria:
  - **Owned** - if enabled, users can perform actions on the media files created 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 created 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 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 EX. The permissions are also sorted by the following criteria:
  - **View** - if enabled, users can view certain aspects of VideoManager EX which would otherwise be inaccessible.
  - **Edit** - if enabled, users can edit certain aspects of VideoManager EX.

5.2 Add Users

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



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 EX 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***.
   - 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 media), the ***Device Operator*** role should be set to ***On***.
6. Click ***Create user***.

6 Assign Body-Worn Cameras and Record Media

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

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

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

>> For more information, see Assign Body-Worn Cameras with Single Issue on VideoManager EX on page 38

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

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

>> For more information, see Assign Body-Worn Cameras with Single Issue and RFID on page 39

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

>> For more information, see Assign Body-Worn Cameras with Permanent Issue on page 40

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

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

>> For more information, see Assign Body-Worn Cameras with Permanent Allocation on page 41

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

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

To assign a body-worn camera with single issue:

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

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

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

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

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

6. From the ***Assignment mode*** dropdown, select **Single issue**.
7. Select a suitable device profile from the ***Device profile*** dropdown. This determines how the body-worn camera will behave - which buttons perform which actions, etc.
8. Select a previously-created WiFi profile, if necessary. This determines which WiFi profile the body-worn camera will use, and is only relevant if the body-worn camera will be streaming in the field, uploading media over WiFi, or connecting to VB Companion.
9. Click ***Assign Device***.

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

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

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

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

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

1. Tap the relevant RFID card against the reader, and wait until it emits three low beeps.
2. Navigate to the ***Admin*** tab.
3. Select the ***People*** pane.
4. Click the ***Users*** section.
5. Next to the user which will be associated with the RFID card in question, click ***Go to user***.
6. In the ***Touch Assign ID*** field, click .

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

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

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

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

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

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

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

6.3 Assign Body-Worn Cameras with Permanent Issue

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

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

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

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

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

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

6. From the ***Assignment mode*** dropdown, select **Permanent issue**.
7. Select the relevant device profile from the ***Device profile*** dropdown. This determines how the body-worn camera will behave - which buttons perform which actions, etc.
8. Select a previously-created WiFi profile, if necessary. This determines which WiFi profile the body-worn camera will use, and is only relevant if the body-worn camera will be streaming in the field, uploading media over WiFi, or connecting to VB Companion.
9. Click ***Assign Device***.

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

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

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 EX, and one RFID card for every user which will be operating their body-worn cameras with **Permanent allocation**.

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

1. Tap the relevant RFID card against the reader, and wait until it emits three low beeps.
2. Navigate to the ***Admin*** tab.
3. Select the ***People*** pane.
4. Click the ***Users*** section.
5. Next to the user which will be associated with the RFID card in question, click ***Go to user***.
6. In the ***Touch Assign ID*** field, click .

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

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

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

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

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

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

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

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

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

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

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

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

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

7 Glossary

A

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

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

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

B

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

Bookmark
This draws attention to a specific part of a media file. It can be created by the body-worn camera which is recording the media file in the field, if the operator presses a configured button. Alternatively, users can add bookmarks to a media file in an incident, once the media file has been downloaded to VideoManager EX.

D

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

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

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

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

E

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

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

I

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

Incident Clip
Any media file which has been added to an incident.

L

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

M

Media
Any media files or assets which can be added to an incident for evidential purposes.

Media File
Any media which has been imported or downloaded to VideoManager EX. This could be a PDF, a still image, a video or an audio file.

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

O

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

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

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

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

P

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

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

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

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

Pre-record
The media file preceding an event which is automatically captured as soon as an operator starts recording. This could be between 1 and 120 seconds.

R

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

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

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

Role Assignment Tier
Every role on VideoManager EX belongs to a role assignment tier. Users can only add other users to roles which are in a tier equal to or lower than the highest assignment tier of their own roles. This includes any roles that they get through their groups.

S

Safety Mode
While a body-worn camera is in safety mode, all functionality (LEDs, beeps, haptic feedback, recording, Bluetooth connection, etc.) will be disabled. To restore functionality, the operator must either perform the gesture associated with leaving safety mode, or connect the body-worn camera to power.

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

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

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

U

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

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

V

VB Companion
Motorola Solutions VB Companion enables users who are still in the field to use their phone to view, and categorise, footage they have recently recorded.

VB200
A robust body-worn camera designed and sold by Motorola Solutions. It can record for up to 8 hours and has 16GB of recording storage.

VB300
A robust body-worn camera designed and sold by Motorola Solutions. It can record for up to 8 hours in HD and has 32GB of recording storage. It also has the ability to livestream footage to VideoManager

EX over a WiFi network.

VB400
A robust body-worn camera designed and sold by Motorola Solutions. It can record for up to 8 hours in full HD and has 32GB of recording storage. It also has GPS-tracking, Bluetooth functionality, and can livestream footage to VideoManager EX over a WiFi network.

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

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

VT50
A lightweight, discreet body-worn camera designed and sold by Motorola Solutions. It can record for up to 2 hours, and has the capacity to livestream footage to VideoManager EX if connected to WiFi.

W

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

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

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

MOTOROLA SOLUTIONS