MOTOROLA SOLUTIONS

VideoManager 15.2 Getting Started with ONStream and Genetec Security Center Guide

This document is intended to serve as a guide for enabling live streams, and configuring VideoManager to work with ONStream and the Genetec Security Center system.

Copyright

Intended purpose

This document is intended to serve as a guide for enabling live streams, and configuring VideoManager to work with ONStream and the Genetec Security Center system.

Document ID

ED-009-051-01

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

⚠ 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

Thank you for choosing Motorola Solutions VideoManager as your aggregator of evidential-ready media. VideoManager is designed as an intuitive browser-based system, requiring minimal training. This document assumes administrative familiarity with VideoManager already. For more information, please see the Administrator Guide.

The administrator can connect Security Center to VideoManager, using VideoManager's ONVIF-compliant interface. This enables VideoManager to pass live streams and recordings from body-worn cameras straight to Security Center. To do so, the administrator must configure live streaming and ONStream on VideoManager, and then configure Security Center to accept the streams. This document will cover all three steps.

2 Configure Streaming

Body-worn cameras on VideoManager should be configured to live stream before users configure ONStream and the Security Center system. These live streams will be automatically passed on to the Security Center system once it has been connected to VideoManager. To configure live streams:

1. Configure firewalls.

   This step is only necessary if VideoManager is configured to use anything other than its default port **or** if VideoManager is set up on a public network.

   >> For more information, see Configure Firewalls on page 6

2. Configure VideoManager's public address.

   >> For more information, see Configure VideoManager's Public Address on page 7

3. Create a user-specific WiFi network, if the user will be live streaming over a personal hotspot.

   >> For more information, see Create User-Specific WiFi Networks on page 8

4. Create a WiFi profile which can be used for streaming.

   >> For more information, see Create a WiFi Profile on page 10

5. Assign the body-worn camera to a user, and begin streaming media.

   >> For more information, see Assign a Body-Worn Camera for Streaming on page 12

6. View the live stream.

   Here, the administrator can check that their live streams are working before they enable and configure ONStream.

   >> For more information, see View Live Streams on page 14

2.1 Configure Firewalls

Sometimes, body-worn cameras will be unable to stream to VideoManager without prior firewall configuration. There are two reasons that firewall configuration might be necessary: the user has either changed VideoManager's default port, or has connected it to a public network. The steps below differ, depending on which situation applies to the user's instance of VideoManager.

If the user has changed VideoManager's default web server port, they must create a new inbound rule. This may also be necessary for the ONStream port that the Security Center system will connect to. To do so:

1. In the Windows menu, navigate to the ***Control Panel*** tab.
2. Select the ***System and Security*** pane.
3. Click the ***Windows Defender Firewall*** section.
4. In the left-hand menu pane, click ***Advanced Settings***.
5. Select ***Inbound Rules***.
6. In the right-hand menu pane, click ***New Rule...***.
7. Set the rule type to **Port**, and click ***Next***.
8. In the ***Specific Local Ports*** section, enter VideoManager's port, and click ***Next***.

   This can be found on VideoManager, in the ***Web Server*** section of the ***System*** pane, in the ***Admin*** tab.
9. Ensure that **Allow the connection** is checked, and click ***Next***.
10. Check the relevant profiles for this rule. If in doubt, leave all checked, and click ***Next***.
11. Enter a name for the rule and click ***Finish***.

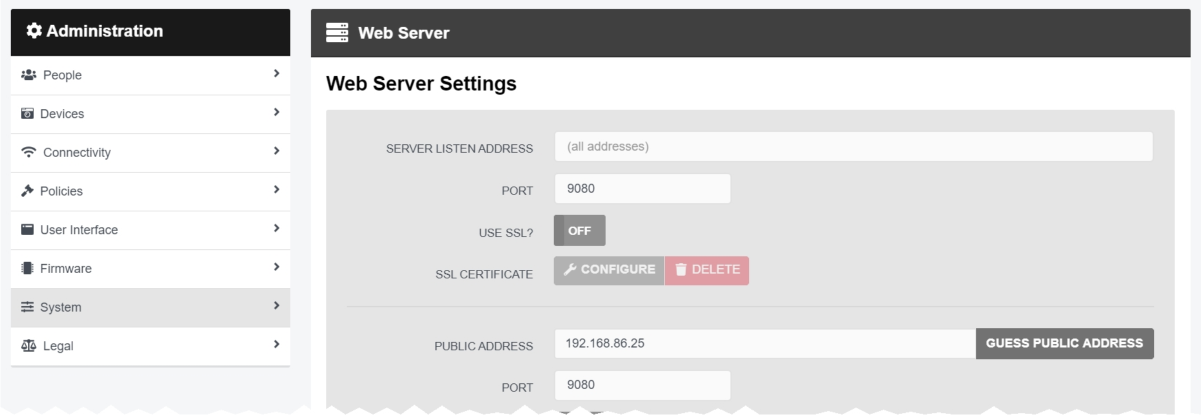
⚠ Caution *If the user has other firewalls or NAT routers in the network between VideoManager and the WiFi network to which body-worn cameras will connect, they must also be configured to allow TCP connections between the body-worn camera and the VideoManager server.*

If the user has connected VideoManager to a public network:

1. In the Windows menu, navigate to the ***Control Panel*** tab.
2. Select the ***System and Security*** pane.
3. Click the ***Windows Defender Firewall*** section.
4. In the left-hand menu pane, click ***Advanced Settings***.
5. Select ***Inbound Rules***, and scroll down until the *VideoManager Web* rule is visible.
6. Double-click on the rule and in the ***Advanced*** section, ensure that **Public** is checked.
7. Click ***OK***.

2.2 Configure VideoManager's Public Address

When a body-worn camera connects to VideoManager, it does so using VideoManager's public address. If the body-worn cameras are connecting to the same IP network as VideoManager, users can utilise the same IP address as the VideoManager machine.



Web Server Settings

SERVER LISTEN ADDRESS (all addresses)
PORT 9080
USE SSL? OFF
SSL CERTIFICATE
PUBLIC ADDRESS 192.168.86.25
PORT 9080

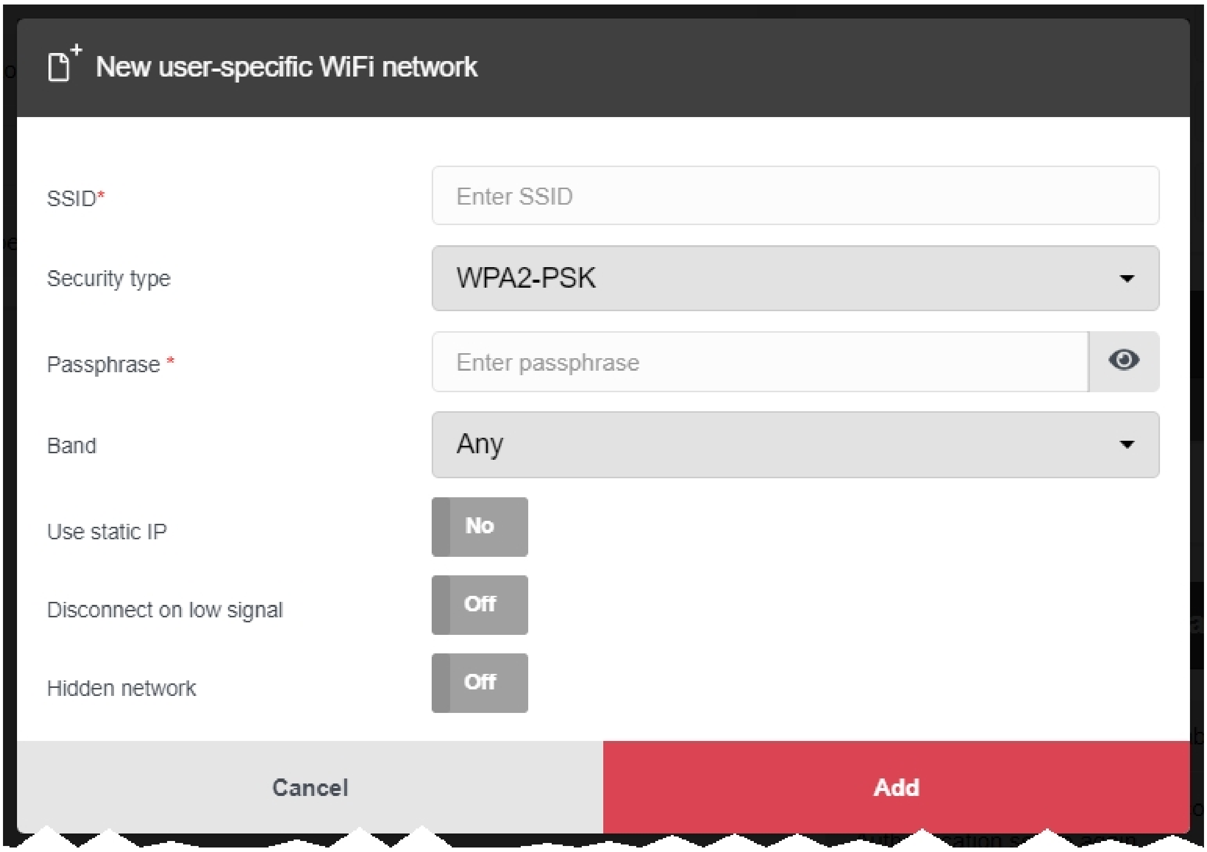
To configure a public address:

1. On VideoManager, navigate to the ***Admin*** tab.
2. Select the ***System*** pane.
3. Click the ***Web Server*** section.
4. In the ***Public address*** field, either enter the public address or click ***Guess public address*** to guess what this address should be.
5. Ensure that ***Use SSL?*** is set to ***Off***.
6. Click ***Save settings***.

VideoManager should be configured to use fixed address LAN infrastucture, and operate on a **Private** or **Domain** network, wherever possible.

2.3 Create User-Specific WiFi Networks

It is possible for users to create user-specific WiFi networks which will only appear on their profile and cannot be viewed by other users on the system. These can be added to WiFi profiles later, but they will still be kept private. This is useful if the user has created a mobile phone hotspot for streaming.



New user-specific WiFi network

SSID*: Enter SSID

Security type: WPA2-PSK

Passphrase *: Enter passphrase

Band: Any

Use static IP: No

Disconnect on low signal: Off

Hidden network: Off

The steps for creating a user-specific WiFi network differ, depending on whether the user is creating the network for **another user on VideoManager or for themselves**.

If the user is configuring a user-specific WiFi network for another user, the steps are as follows:

1. Navigate to the ***Admin*** tab.
2. Select the ***People*** pane.
3. Click the ***Users*** section.
4. Next to the user to be edited, click > ***Go to user***.
5. In the ***WiFi networks*** pane, click ***Add network***.
6. In the ***Network name (SSID)*** field, enter the name of the WiFi network or hotspot.

   This cannot be changed later.
7. From the ***Security type*** dropdown, select which security configuration the user-specific WiFi network will use. The options are **WPA2-PSK**, **WPA-PSK**, **WEP**, or **Open**.

8. In the ***Passphrase*** field, enter the passphrase of the WiFi network or hotspot.

9. From the ***Band*** dropdown, select which frequencies the body-worn cameras will attempt to connect to. The options are as follows:

   - **Any** - this option is suitable for all body-worn cameras.
   - **2.4GHz only** - this option is suitable for all body-worn cameras.
   - **5GHz only** - this option is only suitable for VB400s.

10. If ***Use static IP*** is set to ***On***, the user must enter the corresponding static IP details.

11. If ***Disconnect on low signal*** is set to ***On***, body-worn cameras trying to stream over this network will disconnect from it if its signal is weak.

Users will have the option to define the "weak" signal as a percentage, and the time in seconds that the body-worn camera must be connected to the specified signal level, after which the body-worn camera will disconnect.

12. Click ***Add*** to save the network.

If the user is creating the user-specific WiFi network for themselves:

1. In the top right-hand corner of VideoManager, click the 👤 icon.

2. Select **Account Profile** from the dropdown.

3. In the ***User-specific WiFi networks*** pane, click ***Add network***.

4. In the ***Network name (SSID)*** field, enter the name of the WiFi network or hotspot.

This cannot be changed later.

5. From the ***Security type*** dropdown, select which security configuration the user-specific WiFi network will use. The options are **WPA2-PSK**, **WPA-PSK**, **WEP**, or **Open**.

6. In the ***Passphrase*** field, enter the passphrase of the WiFi network or hotspot.

7. From the ***Band*** dropdown, select which frequencies the body-worn cameras will attempt to connect to. The options are as follows:

   - **Any** - this option is suitable for all body-worn cameras.
   - **2.4GHz only** - this option is suitable for all body-worn cameras.
   - **5GHz only** - this option is only suitable for VB400s.

8. If ***Use static IP*** is set to ***On***, the user must enter the corresponding static IP details.

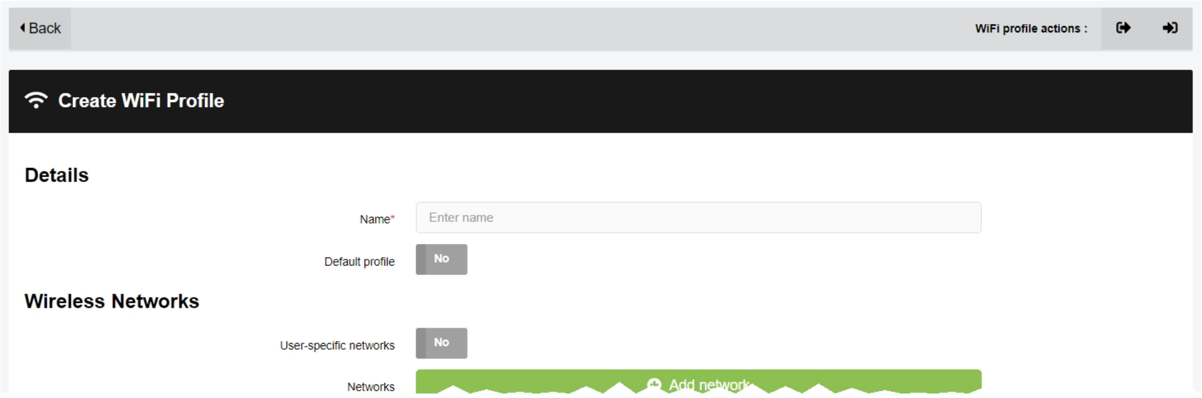
9. If ***Disconnect on low signal*** is set to ***On***, body-worn cameras trying to stream over this network will disconnect from it if its signal is weak.

Users will have the option to define the "weak" signal as a percentage, and the time in seconds that the body-worn camera must be connected to the specified signal level, after which the body-worn camera will disconnect.

10. Click ***Add*** to save the network.

2.4 Create a WiFi Profile

Administrators must create a WiFi profile which is suitable for live streams. A WiFi profile is a collection of WiFi networks, one of which a body-worn camera must connect to before it can live stream.



◂ Back

WiFi profile actions :

Create WiFi Profile

Details

Name* Enter name

Default profile No

Wireless Networks

User-specific networks No

Networks Add network

To create a WiFi profile:

1. Navigate to the ***Admin*** tab.
2. Select the ***Connectivity*** pane.
3. Click the ***WiFi Profiles*** section.
4. Click ***Create wifi profile*** in the top right-hand corner.
5. Enter the following information for the WiFi profile (this will apply to all body-worn cameras which use the profile in question):
   - In the ***Name*** field, enter a name for the WiFi profile.
   - Ensure that ***Default profile*** is set to ***On***.

   This ensures that, regardless of how body-worn cameras are assigned, they will always have access to this WiFi profile.

   - If the administrator has already created user-specific WiFi networks, they can be added to the WiFi profile by setting ***User-specific networks*** to ***On***.

   >> For more information, see Create User-Specific WiFi Networks on page 8

   - To add a new network to the WiFi profile, click ***Add network***.

   The administrator should enter the WiFi network's information. Unlike user-specific WiFi networks, this WiFi network will be used by all body-worn cameras in this WiFi profile, regardless of the users to which they have been assigned.

   - If VB100s, VB200s, VB300s, or VB400s will be streaming, scroll down to the ***VB300/VB400*** section set ***Enable streaming*** to ***On***.

- If VT-series cameras will be streaming, scroll down to the ★ ***VT50/VT100*** section and set ***Enable streaming*** to ***On***.

> 💡 *VT-series camera streaming settings must be configured for* ***every network*** *within a WiFi profile.*

6. Click ***Save settings***.

2.5 Assign a Body-Worn Camera for Streaming

Users can now operate a body-worn camera and live stream the media back to VideoManager. The steps differ, depending on how the body-worn camera will be assigned.

To assign a VB400 to a user through **single issue and RFID**, the user should tap their RFID card against the RFID reader associated with VideoManager. In the pool, a VB400's LEDs will light up and it will emit a beep. The user can undock and operate this body-worn camera. For more information, please see the Administrator Guide.

To assign a VB400 to a user through **Single issue**, **Permanent issue**, or **Permanent allocation**:

1. Navigate to the ***Devices*** tab.
2. Select the 🔍 ***Search Devices*** pane.
3. Filter the body-worn cameras as necessary, and click ***Find devices***.
4. Find the relevant VT100 or VB400, and click ***Assign Device*** next to it.

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

The ***Assign Device*** dialogue opens.

5. In the ***Operator name*** field, enter the name of the user who will be recording with this body-worn camera. This must be a valid username on VideoManager.
6. Select which ***Assignment mode*** the body-worn camera will use.
   - **Single issue** - the body-worn camera will be assigned to a user and when it is redocked, it will become unassigned and must be reassigned manually.
   - **Permanent issue** - the body-worn camera will be assigned to the user and when it is redocked, it will stay assigned to the same user.
   - **Permanent allocation** - the body-worn camera will be allocated to a user, who must then tap an RFID card before they can use it in the field. When it is redocked, it will stay allocated to the same user.

If **Permanent allocation** has been chosen, the user will **not** be able to select the relevant device profile and WiFi profile. However, this is not an issue - the default VideoManager device profile is suitable for streaming, and the WiFi profile should have already been set as the default.

*If the WiFi profile has not already been set as the default, navigate to the **Admin** tab, select the **Connectivity** pane, click the **WiFi Profiles** section, click > **Go to profile** next to the newly created WiFi profile, and set **Default profile** to **On**.*

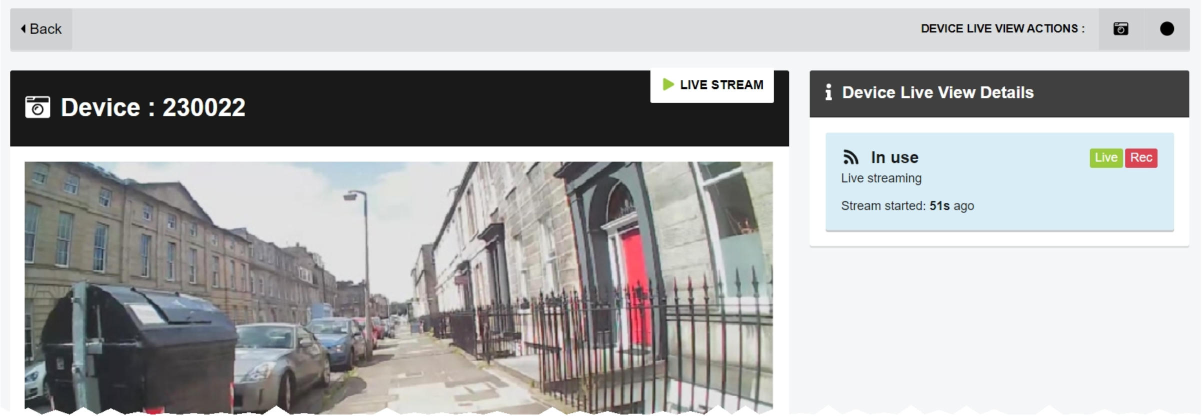
If **Single issue** or **Permanent issue** have been chosen, the user must do the following:

1. From the ***Device profile*** dropdown, select the default device profile.
2. From the ***WiFi profile*** dropdown, select the previously-created WiFi profile.
3. Click ***Assign Device***.

Wait until the body-worn camera's status changes to ***Ready***. At this point, the body-worn camera can be undocked and users can start streaming from their body-worn camera.

2.6 View Live Streams

Once streaming has been configured, a suitable body-worn camera has been assigned to a user, and the body-worn camera has started recording, the administrator should check that the live stream is working properly before enabling ONStream and connecting the Security Center system to VideoManager.



Live streaming

Stream started: **51s** ago

To view a body-worn camera's live stream:

1. Navigate to the ***Devices*** tab.
2. Next to the streaming body-worn camera, there will be two alerts - one will say ***Rec*** and one will say ***Live***. Click ***View live***.
3. This will take the user to a page where they can view the live stream.

> Caution
>
> *Only users with the permission to view body-worn cameras live can see live streams. However, even with this permission, they can only see live streams from body-worn cameras they have permission to view (this could be body-worn cameras they own, body-worn cameras they supervise, or all body-worn cameras).*

4. Once a live stream has stopped, the screen will go blue and there will be a message reading ***Device not streaming***.

3 Configure ONStream on VideoManager

Before the Security Center system can be configured, ONStream must be configured and enabled from VideoManager. To do so:

1. Enable ONStream on VideoManager, with a licence.

   This step is only necessary if the user is running VideoManager version 14.2 or earlier.

   >> For more information, see Enable ONStream on page 16

2. Configure ONStream settings - these dictate how the Security Center system will connect to VideoManager.

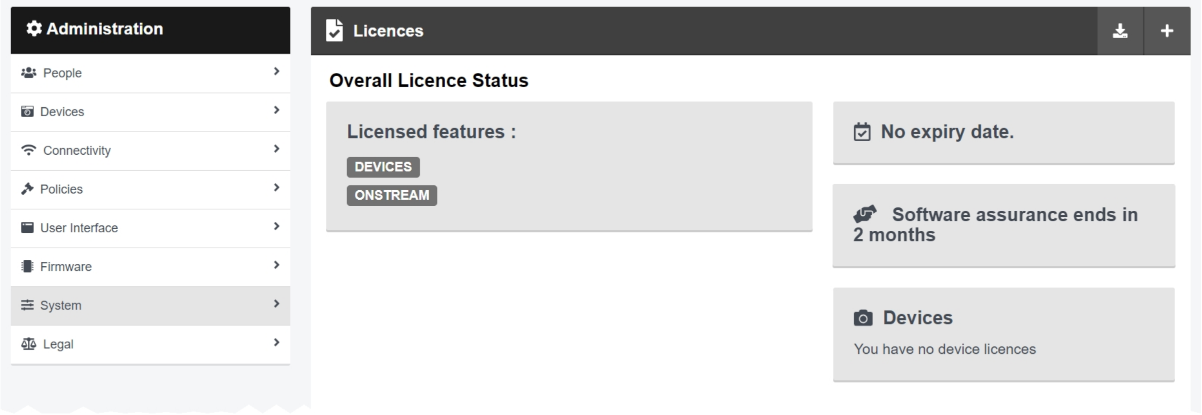
   >> For more information, see Configure ONStream Settings on page 17

3. Create outputs. These outputs determine how VideoManager users and body-worn cameras will be mapped onto the Security Center system.

   >> For more information, see Create and Reset Outputs on page 19

3.1 Enable ONStream

From version 14.3 onwards, VideoManager enables ONStream by default as long as the user has at least one body-worn camera associated with VideoManager. For instances of VideoManager which are running version 14.2 or earlier, ONStream must be manually enabled. Users can do this by importing a licence into VideoManager. This is done from the ***Licences*** section of the ***System*** pane, in the ***Admin*** tab.



Overall Licence Status

Licensed features :

DEVICES

ONSTREAM

No expiry date.

Software assurance ends in 2 months

Devices

You have no device licences

To import an ONStream licence into VideoManager:

1. Navigate to the ***Admin*** tab.
2. Select the ☰ ***System*** pane.
3. Click the ✓ ***Licences*** section.
4. Click + ***Import licence***.

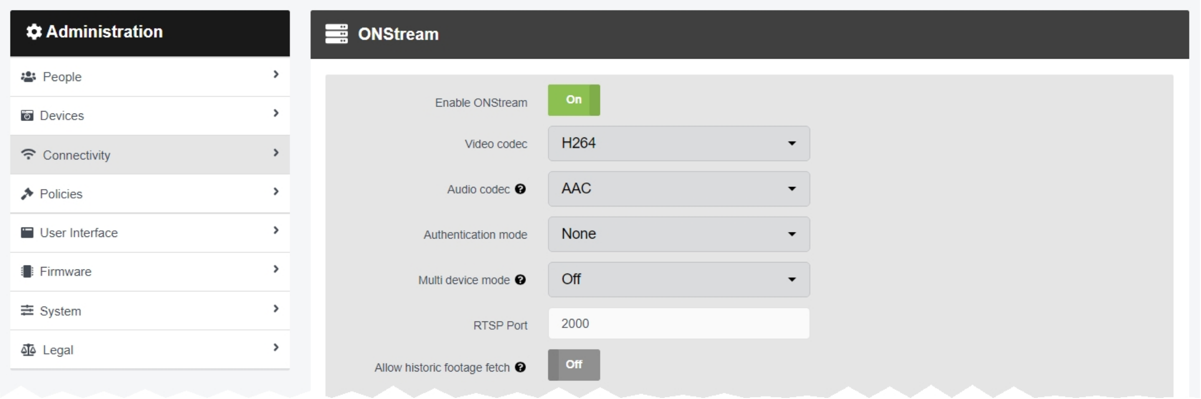
   Users should select the ONStream licence provided to them by Motorola Solutions.
5. Click ***upload***.
6. In the ***Licensee name*** field, enter the name provided by Motorola Solutions.

   ⚠ Caution *If the name entered here does not match the name set by Motorola Solutions, the licence **will not work**.*
7. Click ***confirm***.
8. Users will be asked to confirm again, by clicking ***import***.

   If successful, the licence should appear in the ✓ ***Licences*** section as ***Valid***.

3.2 Configure ONStream Settings

When enabled, ONStream presents an ONVIF-compatible interface with both Profile S (live streaming) and Profile G (recording retrieval) capability. ONStream presents live streams from body-worn cameras as channels in one or more ONVIF compatible multi-channel encoders. The administrator must configure ONStream settings on VideoManager. This is done from the ***ONStream*** section of the ***Connectivity*** pane, in the ***Admin*** tab.



Enable ONStream: On

Video codec: H264

Audio codec: AAC

Authentication mode: None

Multi device mode: Off

RTSP Port: 2000

Allow historic footage fetch: Off

To configure ONStream:

1. Navigate to the ***Admin*** tab.
2. Select the ***Connectivity*** pane.
3. Click the ***ONStream*** section.
4. Set ***Enable ONStream*** to ***On***.
5. From the ***Video codec*** dropdown, select which codec will be used to compress the live streams between devices and the Security Center system. The options are **MPEG4** or **H264**.
6. From the ***Audio codec*** dropdown, select **AAC**.
7. From the ***Authentication mode*** dropdown, select whether users must enter additional credentials when connecting their instance of VideoManager to the Security Center system. The options are as follows:
   - **None** - if selected, no additional authentication will be required.
   - **Basic** - if selected, users will be prompted to create a ***Username*** and ***Password*** on VideoManager.

   These credentials must be entered in the Security Center system when it is being configured to connect to VideoManager.
8. From the ***Multi device mode*** dropdown, the administrator can select whether VideoManager presents itself as a single multi-channel encoder to their VMS, or multiple encoders. Please see the relevant VMS's documentation for more information.

9. In the ***RTSP Port*** field, the administrator can configure the port that VideoManager will use to pass streams to the Security Center system.

By default, this is 554. The administrator may need to change the default port if any software on the same machine as VideoManager is using port 554.

⚠ Caution *This will be the case if the administrator is running the Security Center system on the same machine as VideoManager. Motorola Solutions recommends choosing a port above 2000.*

10. If ***Allow historic footage fetch*** is set to ***On***, the Security Center system will be given access to **all** media on VideoManager and the ability to copy it.

This process will not start until the administrator has also configured the Security Center system to retrieve historic media.

>> For more information, see Configure Archive Transfer on page 31

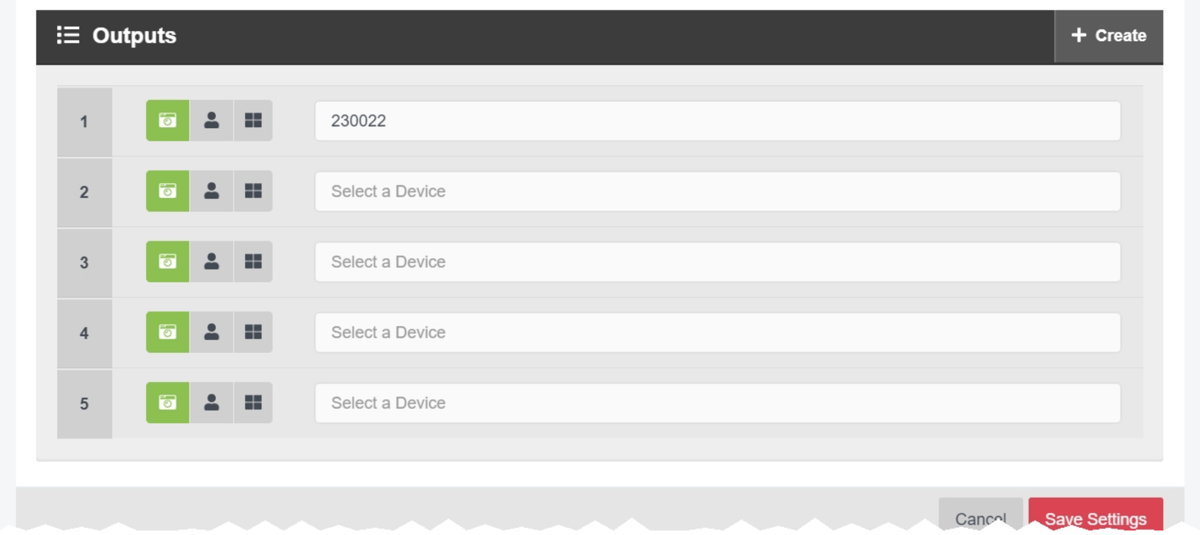
⚠ Caution *Enabling **Allow historic footage fetch** will permit the Security Center system to retrieve restricted media.*

11. Set ***Use Automatic Output Assignment*** to ***Off***.

12. Click ***Save settings***.

3.3 Create and Reset Outputs

Outputs determine how streams from individual users and body-worn cameras on VideoManager are mapped onto channels in an ONVIF compatible multi-channel encoder. This is done from the ***ONStream*** section of the ***Connectivity*** pane, in the ***Admin*** tab.



There must be **one** output for every user OR body-worn camera which will be streaming to the Security Center system. To create an output:

1. Navigate to the ***Admin*** tab.
2. Select the ***Connectivity*** pane.
3. Click the ***ONStream*** section.
4. Scroll to the ***Outputs*** section.
5. To create outputs, click + ***Create***.
   The ***Create ONStream outputs*** window opens.
6. Enter the number of required outputs, and click ***confirm***.
7. Select the type of output to be created. The options are as follows:
   - ***Device*** - if selected, streams will correspond to the body-worn camera specified, regardless of the operator using the body-worn camera.

   The user should enter the body-worn camera's serial number. VideoManager will suggest serial numbers which match the one entered.

   - ***Operator*** - if selected, streams will correspond to the operator specified, regardless of the body-worn camera used to stream media.

   The user should enter the username of an operator on VideoManager.
8. Click ***Save settings***.

If the number of outputs should be raised or lowered after the outputs have been created, the outputs should be reset. Preexisting outputs will not be affected if the total number of outputs is raised. However, if the new number is lower than the previous number, a user's outputs will be deleted to match that number. To do so:

1. Navigate to the ***Admin*** tab.
2. Select the ***Connectivity*** pane.
3. Click the ***ONStream*** section.
4. Scroll to the ☰ ***Outputs*** section.
5. Click ✕ ***Reset***.
6. Enter the new number of required outputs.
7. Click ***confirm***.

4 Configure Security Desk

VideoManager 15.2 is capable of streaming footage live from body-worn cameras to Genetec's Security Desk system. To support this streaming, VideoManager functions as an RTSP server, capable of forwarding these streams to Security Center.

VideoManager is configured to form connections with Security Center. These connections exist even when they are not actively streaming, and as such, Motorola Solutions recommends that a suitable number are created, even if not all of these streams will be used immediately. This is because adding or deleting streams requires Security Desk to be reconfigured.

The steps for configuring Security Desk are as follows:

1. Configure the firewall to let Security Desk through.

   >> For more information, see Open Firewall Ports for Security Desk on page 23

2. Add VideoManager to Security Desk. This will enable administrators to view live streams from Motorola Solutions body-worn cameras on Security Desk.

   >> For more information, see Add VideoManager to Security Desk on page 24

3. **Optionally** configure media file offload or Clearance, to pass media files or incidents from VideoManager to Security Desk or Clearance, respectively.

   >> For more information, see Configure Media file Offload or Clearance on page 25

4. If historic media fetch has been enabled on VideoManager, configure Security Desk to pull historic media.

   >> For more information, see Configure Archive Transfer on page 31

5. **Optionally** configure Security Desk to automatically record incoming live streams from body-worn cameras.

   >> For more information, see Configure Security Desk Recording on page 33

6. **Optionally** rename live streams on Security Desk.

   >> For more information, see Rename Body-Worn Camera Live Streams on Security Desk on page 35

7. View live streams on the Security Desk system.

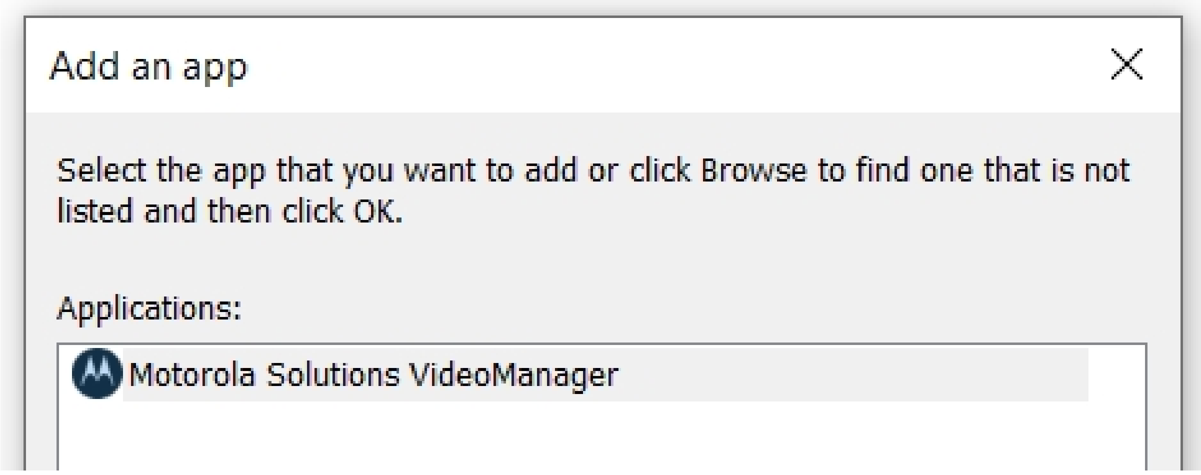
   >> For more information, see View Live Streams on Security Desk on page 36

8. Watch recorded media on the Security Desk system.

   >> For more information, see Watch Recorded Media on page 37

4.1 Open Firewall Ports for Security Desk

In order to communicate with Genetec Security Desk, VideoManager requires that certain ports be opened in the firewall of the computer running it.



Add an app

Select the app that you want to add or click Browse to find one that is not listed and then click OK.

Applications:

Motorola Solutions VideoManager

To open the relevant firewall ports:

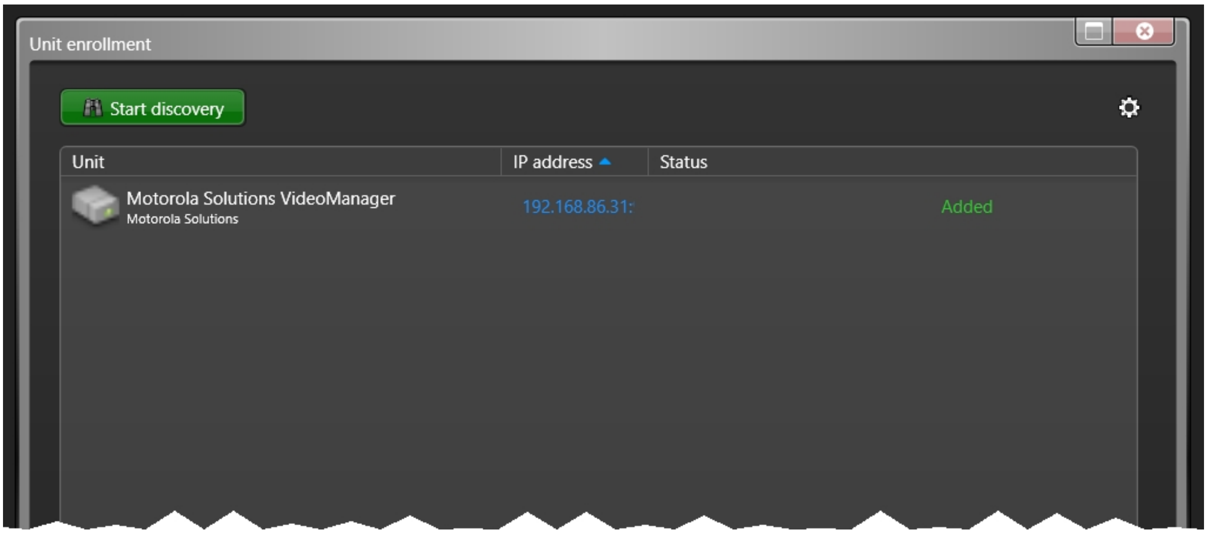
1. Open the Windows Control Panel.
2. Select ***System and Security***.
3. In the ***Windows Defender Firewall*** section, click ***Allow an app through Windows Firewall***.
4. Authenticate as an administrator if necessary.
5. If the list of apps is greyed out, click ***Change Settings*** and click ***Allow another app...***.
6. In the ***Path*** field, browse to VideoManager's installation location and select ***pss_service.exe***.

   By default, VideoManager's installation location is ***C:\Program Files (x86)\Motorola SolutionsVideoManager\pss_service.exe***.

7. Click ***Network Types...*** and select the appropriate type of network (Domain, Public or Private).
8. Click ***OK***, then ***Add*** and then ***OK***.
9. Navigate back to the ***Windows Defender Firewall*** section.
10. Click ***Advanced Settings*** in the left-hand menu pane.
11. Select ***Inbound Rules*** in the left-hand menu pane.
12. From the list, select ***File and Printer Sharing (Echo Request - ICMPv4-In)*** and enable it from the right-hand menu pane.

4.2 Add VideoManager to Security Desk

Once the firewall is configured to allow live streams from VideoManager through to Security Center, VideoManager must be added to Security Desk.



Unit	IP address	Status
Motorola Solutions VideoManager Motorola Solutions	192.168.86.31:	Added

To add VideoManager to Security Desk:

1. Open the Security Desk application.
2. In the left-hand menu pane, navigate to the ***Tools*** tab.
3. Click ***Config Tool***.

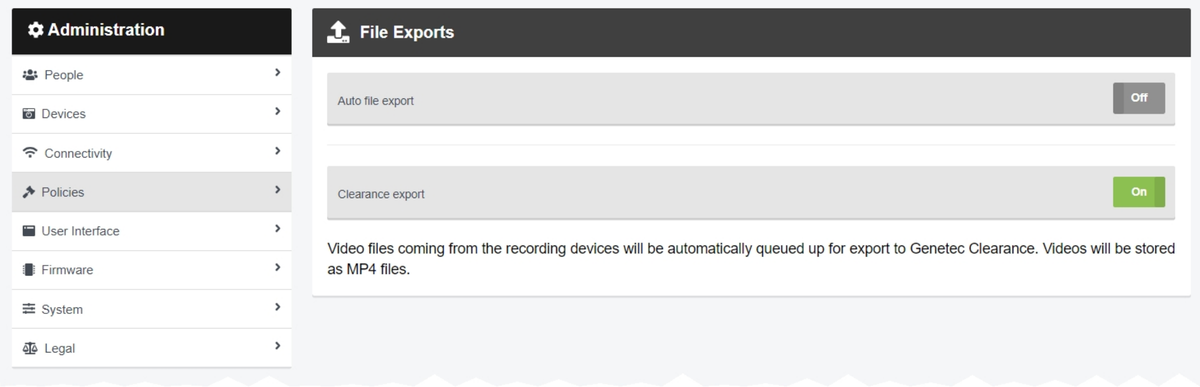
   The tool will open in a separate window.
4. In the left-hand menu pane, navigate to the ***Tools*** tab.
5. Click ***Unit Enrollment***.
6. Click ✎ ***Manual Add...*** in the bottom right-hand corner.
7. Select ***Video***.
8. From the ***Manufacturer*** dropdown, select **Genetec Protocol**.
9. From the ***Product Type*** dropdown, select **All**.
10. In the ***IP Address*** field, enter the IP address of VideoManager.

    This corresponds to the ***Public address*** field in the ***Web Server*** section on VideoManager.
11. In the ***HTTP port*** field, enter VideoManager's port.

    This corresponds to the ***Port*** field in the ***Web Server*** section on VideoManager.
12. If authentication has been enabled from the ***ONStream*** section on VideoManager, set ***Authentication*** to *Specific*. Enter the username and password which was created.
13. Click ***Add and Close***.

4.3 Configure Media file Offload or Clearance

VideoManager can transfer media files or incidents to Security Desk or Clearance automatically, if the feature has been licensed.



Auto file export: Off

Clearance export: On

Video files coming from the recording devices will be automatically queued up for export to Genetec Clearance. Videos will be stored as MP4 files.

The steps for configuring Clearance differ, depending on the type of software the administrator has.

- **If the administrator has Security Desk on their PC**, they must complete the steps for media file offload.

  >> For more information, see Configure Media file Offload on page 26

- **If the administrator has Clearance as a cloud service**, they must complete the steps for Clearance.

  >> For more information, see Configure Clearance on page 28

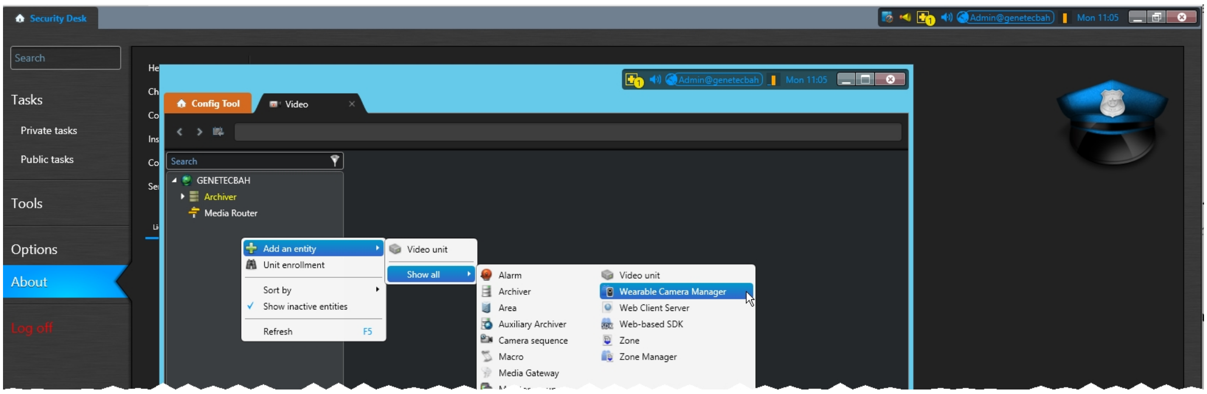
Once the Security Desk system has been configured, the administrator must import the configuration into VideoManager.

>> For more information, see Configure VideoManager for Media file Offload or Clearance on page 29

Clearance must have been licenced from Motorola Solutions first.

4.3.1 Configure Media file Offload

VideoManager can automatically transfer media files to Security Desk, if the feature has been licenced.



To configure media file offload:

1. Open the Security Desk application.
2. In the left-hand menu pane, navigate to the ***Tools*** tab.
3. Click ***Config Tool***.

   The tool will open in a separate window.
4. In the left-hand menu pane, navigate to the ***Tasks*** tab.
5. Select the ***Video*** task. If there is already a role in the left-hand pane called *Wearable Camera Manager*, go straight to the next step. If not, perform the following steps:
   1. In the left-hand pane, right-click and select ***Add an Entity***.
   2. Click ***Show All***, and select ***Wearable Camera Manager***.
   3. Give the new role a name, click ***Next*** through the default values, and click ***Create***.
6. Double-click the ***Wearable Camera Manager*** role.
7. In the top navigation bar, navgiate to the ***Hardware*** tab.
8. Under the ***Camera Stations*** pane, click the **+** button.

   This will create a configuration file which will be imported to VideoManager later.
9. Enter a name and click ***Apply***.

   A configuration file will be created.
10. Next to the new configuration file under the ***Actions*** pane, click *Go to file location*. This will download it to the administrator's PC.

The administrator can also optionally configure whether media files are only sent from body-worn cameras to Security Desk at certain times of day. To do so:

1. On Security Desk, in the left-hand menu pane, navigate to the ***Tools*** tab.
2. Click ***Config Tool***.
3. In the left-hand menu pane, navigate to the ***Tasks*** tab.
4. Click ***Video***.
5. Expand the ***Archiver*** section.
6. Navigate to the ***Resources*** tab.
7. Click ***Advanced Settings...*** in the bottom right-hand corner.
8. Set ***Enable Edge Playback Results*** to ***On***.
9. Click ***OK***.
10. In the top navigation bar, click ***Archive transfer***.
11. Click + .
12. Select ***Retrieve from edge***.
13. In the ***Name*** field, enter a name for the transfer group.
14. Below the ***Sources*** section, click + , and select the body-worn cameras whose media should be transferred.
15. Click ***Add***.
16. From the ***Recurrance*** dropdown, select the desired interval.

> *All media files must be downloaded to VideoManager before this transfer occurs. For this reason, it is recommended that the Security Desk transfer time is set to a few hours after body-worn cameras are initially docked to VideoManager.*

17. Click ***Save***.

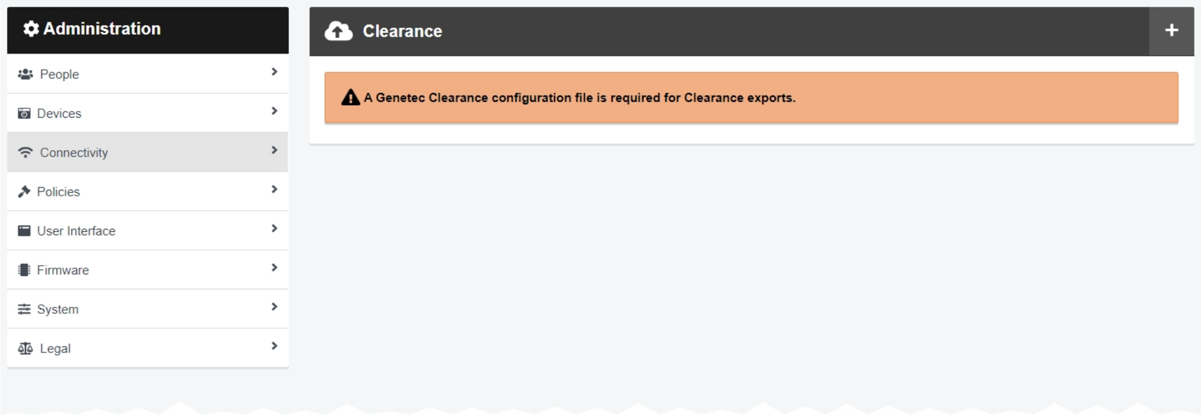
4.3.2 Configure Clearance

If it has been licenced, Clearance allows incidents created on VideoManager to be manually exported to the Clearance cloud service. To do so:

1. Log in to Clearance in an internet browser.
2. Click ***Configurations***.
3. Click **+** in the top right-hand corner.
4. Select ***Service***.
5. Click ***Save***.
6. In the top right-hand corner, click ***Download Configuration***. This will create a configuration file which will be imported to VideoManager later. The file will be downloaded to the administrator's PC.

4.3.3 Configure VideoManager for Media file Offload or Clearance

Once a configuration has been created, either from Security Desk or the Clearance cloud service, it must be imported into VideoManager. After this, it is possible to configure VideoManager to pass media file and incidents to Security Desk or the Clearance cloud service, respectively.



A Genetec Clearance configuration file is required for Clearance exports.

To import the previously downloaded configuration to VideoManager:

1. Navigate to the ***Admin*** tab.
2. Select the ***Connectivity*** pane.
3. Click the ***Clearance*** section.
4. Click + ***Import configuration***, and select the config file downloaded from Security Desk/Clearance.
5. Click ***import***.

Once the configuration has been imported, exports should be configured so the correct information is passed onto Security Desk/Clearance. These steps differ, depending on whether the administrator has VideoManager on their PC or as a cloud service.

If the administrator has Security Desk on their PC:

1. On VideoManager, navigate to the ***Admin*** tab.
2. Select the ***Policies*** pane.
3. Click the ***File Exports*** section.
4. Set ***Clearance export*** to ***On***. This means that all media files downloaded to VideoManager will be automatically transferred to Security Desk.

   *This is mutually exclusive with **File Exports** - media files can either be sent to the path determined by **File Exports**, or to Security Desk, but not both.*

5. If the administrator has configured the deletion policy so that old media is automatically deleted, they must also configure it to ensure that media is not deleted from

> VideoManager until it has been sent to Security Desk. To do so, navigate to the ***Admin*** tab, select the ***Policies*** pane, and click the ***Deletion Policy*** section. Set ***Keep footage until auto file export complete*** to ***On***.

This is useful because, if VideoManager cannot connect to Security Desk in order to transfer media, non-exported media will be kept despite the deletion policy until it can be exported.

If the administrator has Clearance as a cloud service:

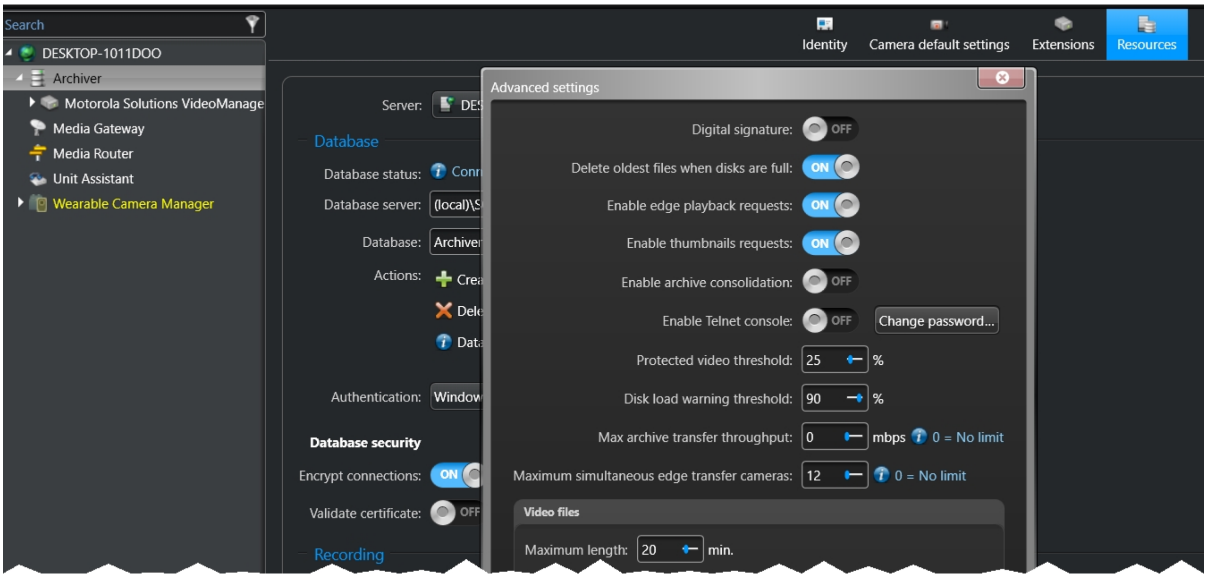
1. On VideoManager, navigate to the ***Admin*** tab.
2. Select the ***Policies*** pane.
3. Click the ***Incident Exports*** section.
4. Click ***Create new export profile***.
5. From the ***Type*** dropdown, select **Clearance**.

   Now, whenever an incident is being exported, the administrator can choose the ***Clearance*** export profile - instead of downloading the incident to the PC, it will be sent straight to the cloud.

6. Optionally, set ***Export incident on create*** to ***On***. This means that whenever an incident is created on VideoManager, a copy is automatically exported to Clearance.

4.4 Configure Archive Transfer

It is necessary to configure archive transfer if ***Allow historic footage fetch*** has been set to ***On*** on VideoManager. The administrator must configure which body-worn cameras will have their historic media pulled to Security Desk.



Server: DES
Database status: Conn
Database server: (local)\S
Database: Archiver
Authentication: Window
Encrypt connections: ON
Validate certificate: OFF

Advanced settings

Digital signature: OFF
Delete oldest files when disks are full: ON
Enable edge playback requests: ON
Enable thumbnails requests: ON
Enable archive consolidation: OFF
Enable Telnet console: OFF Change password...
Protected video threshold: 25 %
Disk load warning threshold: 90 %
Max archive transfer throughput: 0 mbps 0 = No limit
Maximum simultaneous edge transfer cameras: 12 0 = No limit

Video files

Maximum length: 20 min.

To configure archive transfer:

1. Open the Security Desk application.
2. In the left-hand menu pane, navigate to the ***Tools*** tab.
3. Click ***Config Tool***.
4. In the left-hand menu pane, navigate to the ***Tasks*** tab.
5. Click ***Video***.
6. Expand the ***Archiver*** section.
7. Navigate to the ***Resources*** tab.
8. Click ***Advanced Settings...*** in the bottom right-hand corner.
9. Set ***Enable Edge Playback Results*** to ***On***.
10. Click ***OK***.

Next, the administrator can immediately transfer their historic media to Security Desk. To do so:

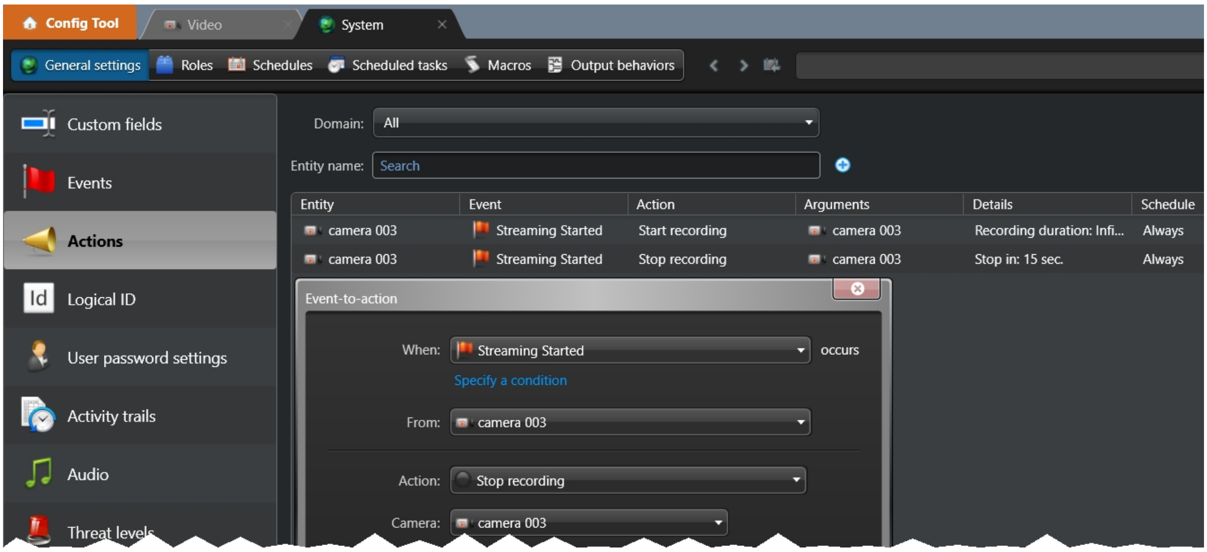
1. In Security Desk, in the left-hand menu pane, navigate to the ***Tools*** tab.
2. Click ***Config Tool***.
3. In the left-hand menu pane, navigate to the ***Tasks*** tab.
4. Click ***Video***.

5. In the top navigation bar, click ***Archive transfer***.
6. In the bottom right-hand corner, click ***Transfer now***.
7. Below the ***Sources*** section, click +, and select the body-worn cameras whose historic media should be transferred.
8. In the ***Time range*** field, configure which media files will be transferred, determined by when they were recorded.
9. Click ***Start***.

The transfer will start immediately. Because media files are copied to Security Desk, not moved, the original media files on VideoManager will still be subject to VideoManager's deletion policies, and the copied media files will be subject to Security Desk's deletion policies.

4.5 Configure Security Desk Recording

It is possible to configure Security Desk to record the live streams from body-worn cameras automatically.



Domain: All

Entity name: Search

Entity	Event	Action	Arguments	Details	Schedule
camera 003	Streaming Started	Start recording	camera 003	Recording duration: Infi...	Always
camera 003	Streaming Started	Stop recording	camera 003	Stop in: 15 sec.	Always

When: Streaming Started occurs

From: camera 003

Action: Stop recording

Camera: camera 003

To configure Security Desk to record live streams, the administrator must create two actions: one which prompts Security Desk to start recording the live stream, and one which prompts it to stop. To do so:

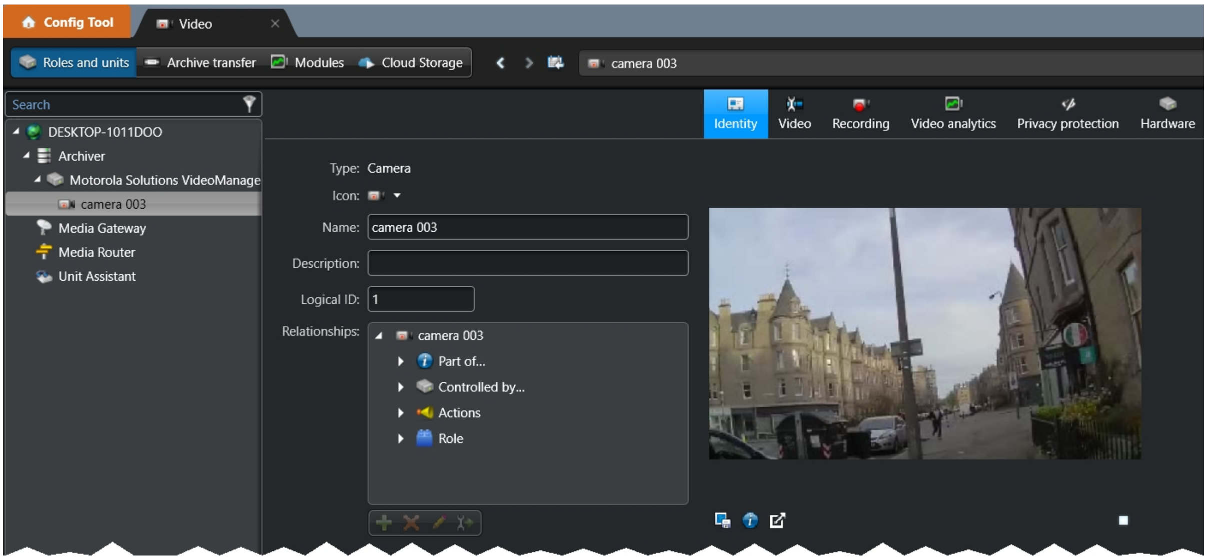
1. Open the Security Desk Config Tool.
2. In the left-hand menu pane, navigate to the ***Tasks*** tab.
3. Click ***System***, then ***General Settings***.
4. Select ***Actions***, and click + .
5. From the ***When: ... occurs*** dropdown, select **Streaming Started**.
6. From the ***From:*** dropdown, select a body-worn camera connected to VideoManager.
7. From the ***Action:*** drodpown, select **Start recording**.
8. From the ***Camera:*** dropdown, select the same body-worn camera.
9. From the ***Recording duration:*** drodpown, select **Infinite**.
10. Click ***Save***.
11. In the same pane, click + again.
12. From the ***When: ... occurs*** dropdown, select **Streaming Stopped**.
13. From the ***From:*** dropdown, select the same body-worn camera as in the previous action.
14. From the ***Action:*** drodpown, select **Stop recording**.
15. From the ***Camera:*** dropdown, select the same body-worn camera.

16. From the ***Stop in:*** drodpown, select **Specific**. Enter *15 seconds* to ensure no media is lost.

17. Click ***Save***.

4.6 Rename Body-Worn Camera Live Streams on Security Desk

By default, the live streams added to Security Desk will have the naming convention *Motorola Solutions VideoManager Camera (number)*, where *(number)* is the output number on VideoManager associated with this live stream. The administrator can optionally change this, in the Config Tool.



Type: Camera

Icon:

Name: camera 003

Description:

Logical ID: 1

To rename a body-worn camera live stream on Security Desk:

1. Open the Security Desk Config Tool.
2. In the left-hand menu pane, navigate to the ***Tasks*** tab.
3. Click ***Video***.
4. Expand the ***Archiver*** section.
5. Expand the ***Motorola Solutions VideoManager*** input.

   This will show a list of the outputs configured on VideoManager.

6. Double click the relevant live stream name in the left-hand menu pane.

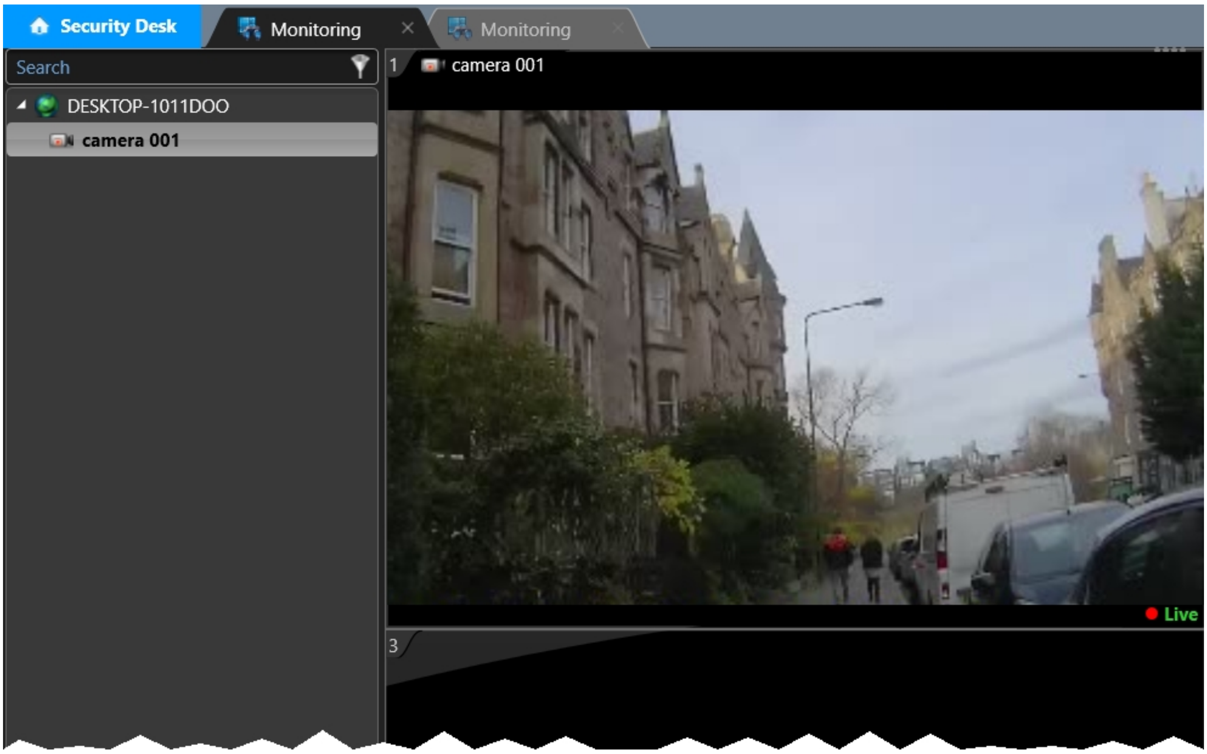
   The live stream's information will open in the main pane.

7. In the ***Name*** field, rename the live stream.
8. Click ✓ ***Apply***.

Repeat this process for as many live streams as necessary.

4.7 View Live Streams on Security Desk

Once the previous configuration has been completed, administrators can view live streams from body-worn cameras in Security Desk.



To view live streams:

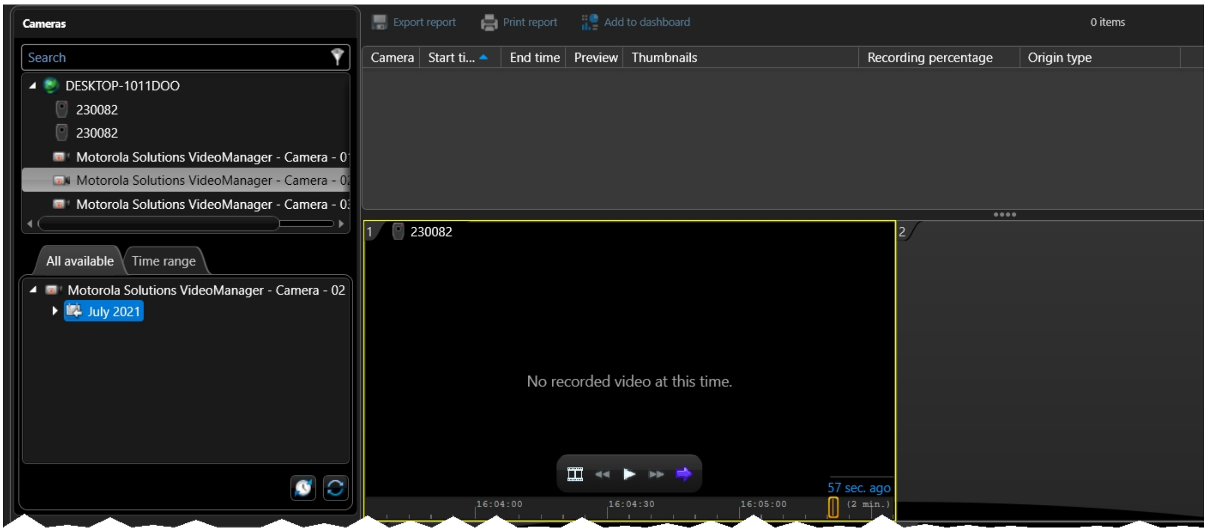
1. Open the Security Desk application.
2. In the left-hand menu pane, navigate to the ***Tasks*** tab.
3. Click the ***Monitoring*** task.
4. Either drag an output (body-worn camera) from the left-hand menu pane into a free tile, or double-click the output. This will open it in the next free tile.

To change the number of live streams presented simultaneously, click ***Change tile pattern***. Here, the administrator can select one, four, nine, or sixteen tiles.

To remove a live stream, right-click on its tile and select ***Clear***.

4.8 Watch Recorded Media

If the administrator has enabled **media file offload**, **live stream recording**, or **historic footage fetch**, all recorded media from body-worn cameras can be viewed from the ***Archive*** tab on Security Desk.



To watch recorded media on Security Desk:

1. Open the Security Desk application.
2. In the left-hand menu pane, navigate to the ***Tasks*** tab.
3. Click ***Archives***.
4. In the left-hand menu pane, select the camera whose media should be accessed.
   - **If the administrator has configured video offload or historic footage fetch**, select a camera which has a body-worn camera icon.
   - **If the administrator has configured live stream recording**, select a camera which has a CCTV icon. This corresponds to an output on VideoManager.
5. Select the ***All available*** tab (to show all available records from the selected camera, broken down by date) or the ***Time range*** tab (to choose a specific time period).
   - If ***All available*** has been selected, choose a date.
   - If ***Time range*** has been selected, optionally add more cameras to the report, and choose a time period to cover.
6. Click ***Generate report***.

This will return a list of all recorded media corresponding to the camera(s) and time(s) specified.

5 Glossary

A

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.

D

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.

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.

O

ONStream

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

ONVIF

ONVIF is an open industry forum that provides and promotes standardized interfaces for effective interoperability of IP-based physical security products.

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 use 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.

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.

Role

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

S

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

VB400

A VB400 is 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.

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' VideoTag range to have haptic feedback.

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.