MOTOROLA *SOLUTIONS*

VideoManager 14.4
Getting Started with ONStream
and ACC™ System Guide

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

Intended purpose

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

Document ID

ED-009-035-05

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 footage. 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.

Users can connect the Avigilon Control Center ™ (ACC) system to VideoManager, using VideoManager's ONVIF-compliant interface. This enables VideoManager to pass live streams and recordings from body-worn cameras straight to the ACC system. To do so, users must configure both ONStream and live streams, as well as the ACC system.

2 Configure Streaming

Devices on VideoManager should be configured to live stream before users configure ONStream and the ACC system. These live streams will be automatically passed on to the ACC 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 8

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 9

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

    >> For more information, see Create a WiFi Profile on page 11

5. Assign the device to a user, and begin streaming footage.

    >> For more information, see Assign a Device for Streaming on page 12

6. View the live stream.

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

    >> For more information, see View Live Streams on page 13

2.1 Configure Firewalls

Sometimes, devices 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 ACC 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 devices will connect, they must also be configured to allow TCP connections between the device 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 VideoBadge or VideoTag connects to VideoManager, it does so using VideoManager's public address. If the devices are connecting to the same IP network as VideoManager, users can utilise the same IP address as the VideoManager machine.
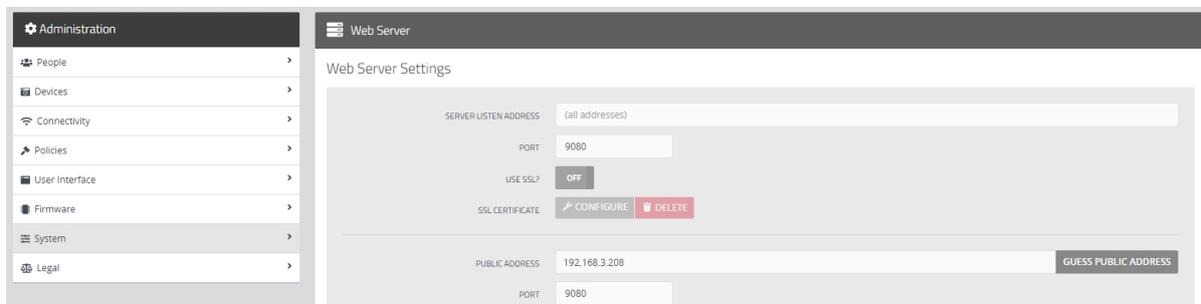
To configure a public address:

1. On VideoManager, navigate to the *Admin* tab.

2. Select the ⇌ *System* pane.

3. Click the ▤ *Web Server* section.

4. In the *Public Address* field, either enter the public address or click *Guess Public Address* to guess what this address should be.

5. Click *Save Settings*.

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

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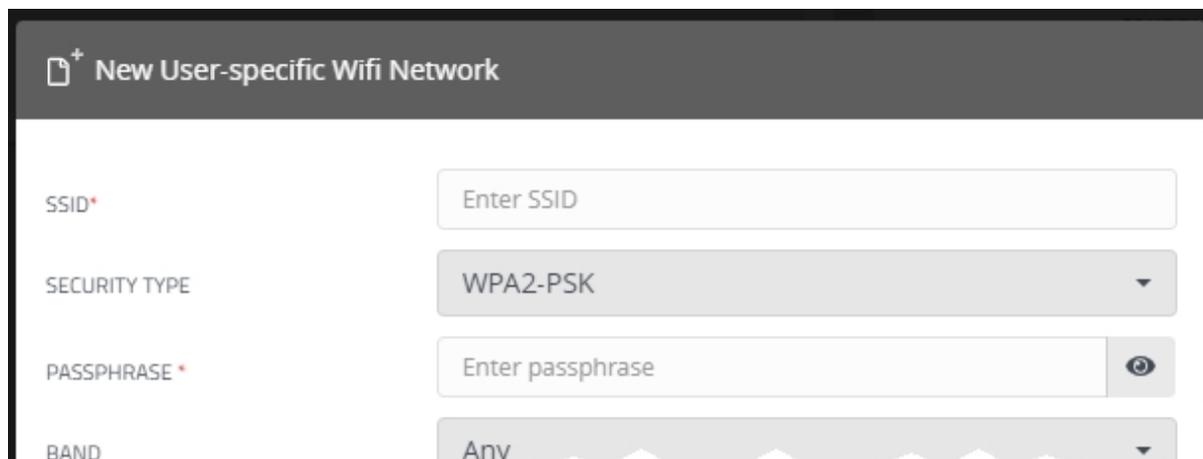
The steps for creating a user-specific WiFi network differ, depending on whether the user is creating the network for **another user on VideoManager or for themselves**.

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 *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 devices will attempt to connect to. The options are as follows:

   - **Any** - this option will make VB-400s connect to both 2.4GHz and 5GHz frequencies.

   - **2.4GHz only** - this option will make all devices connect to 2.4GHz fre-

quencies.

- **5GHz only** - this option will make VB-400s connect to 5GHz frequencies.

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*, devices 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 device must be connected to the specified signal level, after which the device 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 *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 devices will attempt to connect to. The options are as follows:

- **Any** - this option will make VB-400s connect to both 2.4GHz and 5GHz frequencies.

- **2.4GHz only** - this option will make all devices connect to 2.4GHz frequencies.

- **5GHz only** - this option will make VB-400s connect to 5GHz frequencies.

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*, devices 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 device must be connected to the specified signal level, after which the device will disconnect.

10. Click *Add* to save the network.

2.4 Create a WiFi Profile

Users must create a WiFi profile which is suitable for live streams. A WiFi profile is a collection of WiFi networks, one of which a device must connect to before it can live stream.

To do so:

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 devices which use the profile in question):

   - In the *Name* field, enter a name for the WiFi profile.

   - Ensure that *Default profile* is set to *On*.

   - If the user 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 9

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

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

   - If VideoBadges will be streaming, scroll down to the *VideoBadge* section set *Enable Streaming* to *On*.

   - If VideoTags will be streaming, scroll down to the ⭐ *VideoTag* section and set *Enable streaming* to *On*.

     *VideoTag streaming settings must be configured for **every network** within a WiFi profile.*

6. Click *Save Settings*.

2.5 Assign a Device for Streaming

Users can now operate a device and live stream the footage back to VideoManager.

To do so:

1. Navigate to the *Devices* tab.

2. Select the 🔍 *Search Devices* pane.

3. Filter the devices as necessary, and click *Find Devices*.

4. Find the relevant VT-100 or VB-400, and click 👤⁺ *Assign Device* next to it.

This device must be connected to VideoManager and unassigned. To unassign a device, 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 device. This must be a valid username on VideoManager.

6. Select which *Assignment Mode* the device will use.

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.

⚠ Caution   *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 device's status changes to *Ready*. At this point, the device can be undocked and users can start streaming from their device.

2.6 View Live Streams

Once streaming has been configured, a suitable device has been assigned to a user, and the device has started recording, users should check that the live stream is working properly before enabling ONStream and connecting the ACC system to VideoManager.
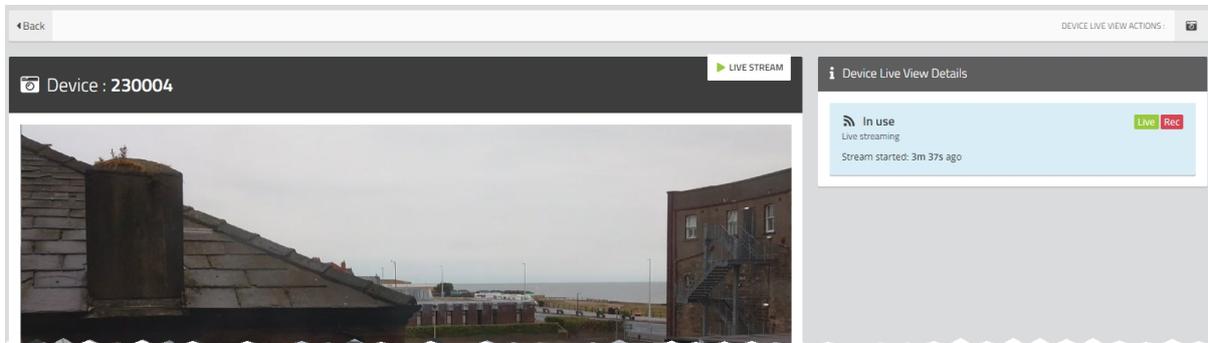
To view a device's live stream:

1. Navigate to the *Devices* tab.

2. Next to the streaming device, 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 devices live can see live streams. However, even with this permission, they can only see live streams from devices they have permission to view (this could be devices they own, devices they supervise, or all devices).*

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 ACC 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 15

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

   >> For more information, see Configure ONStream Settings on page 16

3. Create outputs. These outputs determine how VideoManager users and devices will be mapped onto the ACC system.

   >> For more information, see Create and Reset Outputs on page 18

3.1 Enable ONStream

From version 14.3 onwards, VideoManager enables ONStream by default as long as the user has at least one device 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.
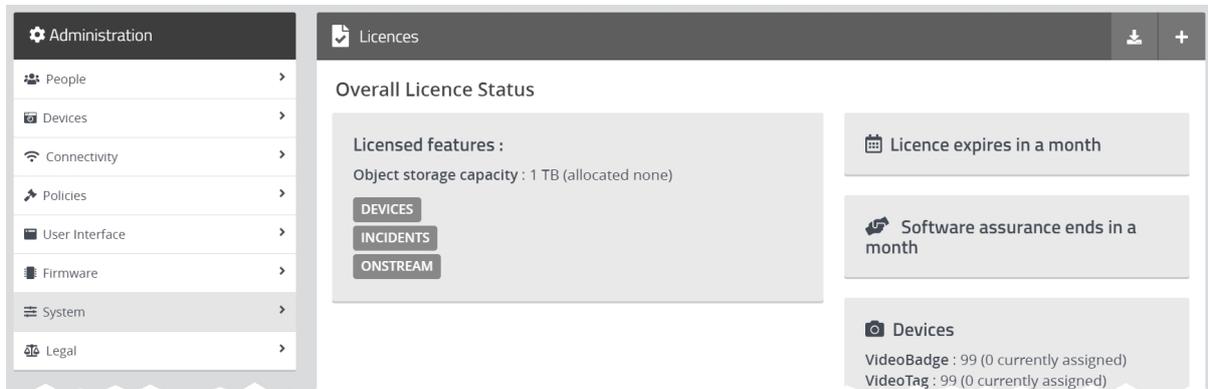
To import an ONStream licence into VideoManager:

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 Avigilon.

5. Click *Upload*.

6. In the *Licensee Name* field, enter the name provided by Avigilon.

⚠ Caution   *If the name entered here does not match the name set by Avigilon, 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. Users must configure ONStream settings on VideoManager. This is done from the *ONStream* section of the *Connectivity* pane, in the *Admin* tab.
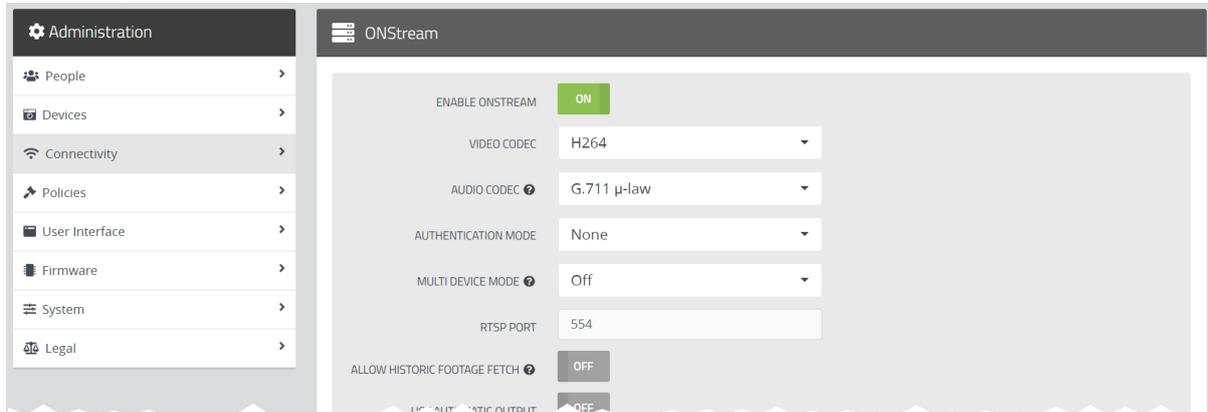
To configure ONStream:

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 ACC 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 ACC 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 ACC system when it is being configured to connect to VideoManager.

8. From the *Multi device mode* dropdown, users can select whether VideoManager presents itself as a single multi-channel encoder, or multiple encoders.

9. In the *RTSP port* field, users can configure the port that VideoManager will use to pass streams to the ACC system.

By default, this is 554. Users 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 user is running the ACC system on the same machine as VideoManager.*

10. If *Allow historic footage fetch* is set to *On*, VideoManager's ONVIF Profile G interface will be enabled. This gives the ACC system access to **all** footage on VideoManager and the ability to copy it.

This process will not start until the user has also configured the ACC system to retrieve historic footage.

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

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 devices 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.
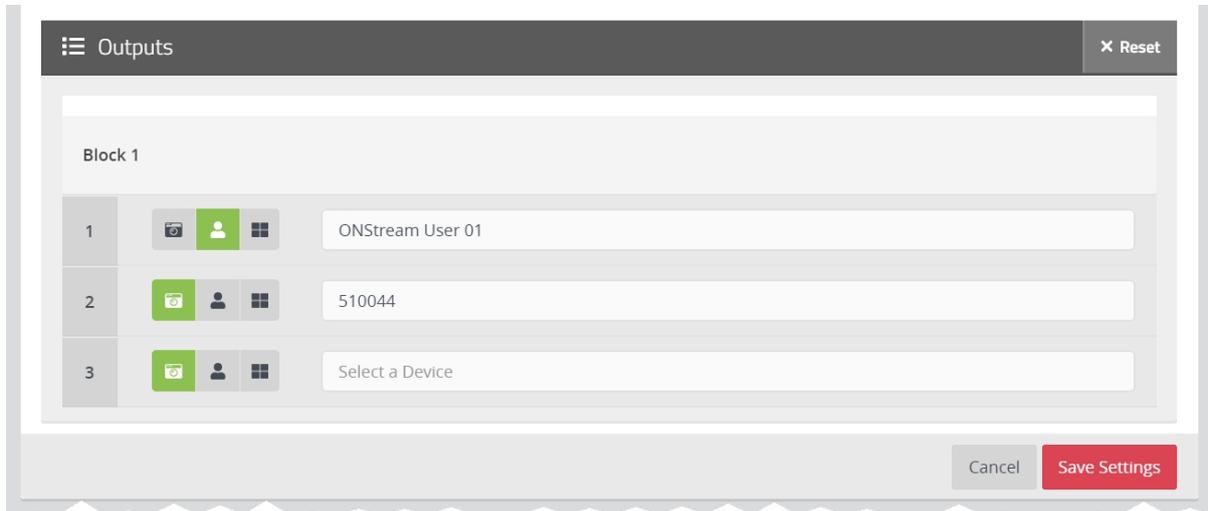
There must be **one** output for every user OR device which will be streaming to the ACC system. To create an output:

1. Navigate to the *Admin* tab.

2. Select the 🛜 *Connectivity* pane.

3. Click the 🖳 *ONStream* section.

4. Scroll to the ☰ *Outputs* section.

5. By default, VideoManager provides **five** outputs. If more outputs are needed, click ✖ *Reset*, enter the number of required outputs, and click *confirm*.

💡   *Only 16 outputs are supported on the ACC system.*

---

6. Select the type of output to be created. The options are as follows:

   - 📷 *Device* - if selected, streams will correspond to the device specified, regardless of the operator using the device.

   The user should enter the device'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 device used to stream footage.

The user should enter the username of an operator on VideoManager.

7. 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 the ACC System

Once ONStream has been configured, users can enable the ACC system to connect to VideoManager. This will require one camera channel from Avigilon, for up to 16 VideoManager outputs.

To do so:

1. In the ACC system, in the ☰ *New Task* menu, click *Site setup*.

2. In the left-hand menu pane, select the site to which the VideoManager devices will be added.

3. In the *Other* section, click *Connect/Disconnect Devices*.

   A new tab will open.

4. If the ACC system has automatically detected VideoManager, it will appear in the *Discovered Devices* pane. If not, VideoManager must be added to the ACC system manually. To do so:

   1. Click *Find Devices*.

   2. From the *Device Type* dropdown, select **ONVIF**.

   3. In the *IP Address* field, enter VideoManager's public address or domain name.

      This is located on VideoManager, in the *Web Server* section of the *System* pane, in the *Admin* tab.

   4. In the *Control Port* field, change the port to 8101.

      This is the same for all instances of VideoManager.

   5. If a username and password has been configured from the *ONStream* section on VideoManager, they must be entered here.

   6. Click *OK*.

      The instance of VideoManager should appear in the *Discovered Devices* pane.

5. In the *Discovered Devices* pane, select the VideoManager entry, and click *Connect*.

   If successful, VideoManager will appear in the *Connected Devices* pane.

6. Navigate back to the original tab.

7. In the left-hand menu pane, select the VideoManager entry.

   The outputs which have been configured on VideoManager already should be viewable.

> *Even if outputs have been assigned to users on VideoManager, they will be presented as cameras here.*

There are two ways to view a live stream on the ACC system.

Users can create alarms in the ACC system. These alarms will alert users when a body-worn camera starts live streaming, and will prompt the live streams to appear **automatically** in the ACC system viewing pane.

>> For more information, see Create Alarms on page 22

Alternatively, instead of creating alarms for individual body-worn cameras, users can drag and drop the relevant output from the left-hand menu pane into the ACC system viewing pane **manually**. If the ACC application has been configured, users can view live streams on their phone as well.

4.1 Create Alarms

To have a live stream appear on the ACC system when a body-worn camera starts live streaming, the user must configure an alarm. To create an alarm on the ACC system:

1. In the ☰ *New Task* menu, click *Site setup*.

2. In the left-hand menu pane, select the site which contains the devices connected to VideoManager.

3. In the *General* section, click *Alarms*.

4. Click *Add Alarm*.

5. From the *Alarm Trigger Source* dropdown, select **Motion Detection**.

6. Click *Next*.

7. Select the device which will be the source of the alarm.

8. Select the same device to link to the alarm, and check the *View linked devices when alarm is triggered* field.

9. Complete the alarm configuration, and as a last step check the *Enable alarm box* field.

When the specified device starts to live stream, an alarm will be raised in the ACC system and the live stream will appear.

🔅 *As with any other ACC Alarm, the alarm can be received and managed through the ACC Mobile 3 app.*

---

5 Glossary

A

Assigned/Unassigned

If a VideoBadge/VideoTag is assigned, it has been paired with a user and can record footage. An unassigned VideoBadge/VideoTag has not been paired with a user, and cannot record footage until it has been assigned.

D

Dashboard

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

Device

Any Motorola Solutions body-worn camera which has been associated with VideoManager.

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 devices 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 device 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 device with RFID touch assign.

Permanent issue

If a device 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

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 device has been assigned to a user with single issue, it will only be assigned to the user for one trip. Once the device 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

VB-400

A VB-400 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.

VT-100

A VT-100 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 assigned to a VideoBadge or VideoTag. The device in question will stream to VideoManager over these networks.

Warranty service and technical support can be obtained by contacting Avigilon Technical Support: avigilon.com/contact-us/.

MOTOROLA *SOLUTIONS*