MOTOROLA SOLUTIONS

Camera Configuration Tool User Guide

Copyright

MOTOROLA, MOTO, MOTOROLA SOLUTIONS, and the Stylized M Logo are trademarks or registered trademarks of Motorola Trademark Holdings, LLC and are used under license. All other trademarks are the property of their respective owners. © 2016 - 2020 Motorola Solutions, Inc. All rights reserved.

PDF-CCT-C

Revision: 1 - EN

20201218

Table of Contents

Introduction 1
- Logging In to Cameras 1
- Navigating the Camera Configuration Tool 1
- Camera Status 2
- Changing the Factory Default Credentials 3
- Changing the Connection Credentials 3
- Adding a Secondary Admin User 4

Finding Cameras 5
- Sending a Discovery Broadcast 5

Filtering and Sorting Cameras 6
- Filtering Cameras 6
- Clearing a Filter 6
- Sorting Cameras 6

Editing Cameras 7
- Editing a Single Camera 7
- Editing Multiple Cameras 7
- Applying Changes 7

Setting Tabs 9

Assigning IP Addresses 12
- Assigning Static IP Addresses 12
- Assigning an IP by MAC Address 13

Setting the NTP Server 14

Managing Certificates 15
- Downloading a Certificate Signing Request 15
- Uploading Signed Certificates 15
- Applying Certificates 16
- Deleting Certificates 16

Network Security 17
- Disabling HTTP Connections in the Camera Configuration Tool 17
- Disabling HTTP Connections for a Camera 17
- Changing the HTTP or HTTPS Port 17

Configuring Analytics 19
- Analytics Setting Description 19

Setting Up Classified Object Motion Detection 21
Configuring Analytic Events 22
Analytic Event Descriptions 23
Updating Firmware 26
Downloading Firmware 26
Applying Firmware 26
Exporting and Importing Settings 27
Exporting Settings 27
Editing the Export File 27
Importing Settings 27
Device Logs 29

Introduction

The Camera Configuration Tool allows you to configure all cameras that are discovered on your network. You can apply common settings to multiple cameras at the same time, or adjust individual cameras to fit your site requirements.

To use this tool, make sure the following requirements are met:

- All the cameras you are configuring have been installed and are physically connected to the network.
- The Camera Configuration Tool is installed on a computer that has access to the same network as the cameras.
- You know the password for all the cameras.

Logging In to Cameras

By default, all the cameras on your network are auto-discovered by the Camera Configuration Tool. The discovered cameras are connected to your immediate subnet or subnets configured for multicast messages.

Before you can edit the cameras in the system, you must first log in to the cameras.

1. When you launch the Camera Configuration Tool, you are immediately prompted to log in to all discovered devices.
    - In the **User Name** and **Password** fields, enter the camera credentials. The tool assumes that all connected devices are using the same credentials.
    - If the cameras use the credentials admin/admin or administrator/<blank>, select the **Use the factory default credentials if the above credentials fail.** checkbox.
    - The tool will not log in to new cameras that do not have any credentials.
2. Click **Connect to Devices**.

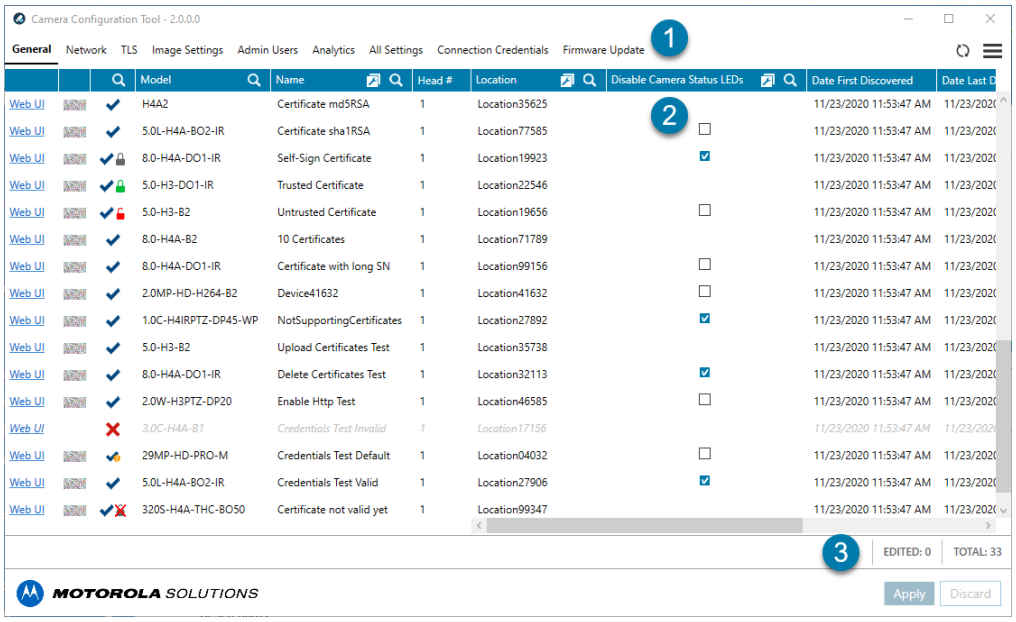
    You are logged into the discovered cameras using the selected credentials.

If the tool failed to log in to some cameras, select the **Connection Credentials** tab and manually enter the correct credentials for those cameras. For more information, see *Changing the Connection Credentials* on page 3.

If you notice that one or more cameras that you want to configure are missing from the list, you can manually search and add the cameras to the list. For more information, see *Finding Cameras* on page 5.

Navigating the Camera Configuration Tool

After you login to all the cameras, the application window presents you with a list of all the cameras that were automatically detected in the system.



1. **Menu bar** — the camera settings tabs are displayed on the left, and the additional task menu ☰ is available on the right. For more information, see *Setting Tabs* on page 9.
2. **Camera list** — the list of discovered cameras and their related settings.
3. **Implementation area** — the area at the bottom-right corner of the application window. This displays the total number of discovered cameras, and the number of cameras with pending setting changes. Changes are not implemented until you click **Apply**.

Camera Status

The camera status column displays the following details about each camera.

- ✔ — successfully logged into the camera.
- ✔ — successfully logged into the camera using admin/admin or administrator/<blank> credentials. It is recommended that you change the camera credentials. For more information, see *Changing the Factory Default Credentials* on the next page.
- ! — camera is in factory default state and has no credentials. Change the camera credentials in order to use the camera. For more information, see *Changing the Factory Default Credentials* on the next page.
- ? — trying to log into the camera.
- ✖ — failed to log into the camera. Change the login credentials on the **Connection Credentials** tab. For more information, see *Changing the Connection Credentials* on the next page.
- ⊗ — no longer able to communicate with the camera. This may appear if the camera is offline or if there has been an error retrieving the camera settings.
- 🔒 — securely connected over HTTPS using a trusted certificate.

- — securely connected over HTTPS using a self-signed certificate.
- — securely connected over HTTPS using not trusted certificate.
- — connected over HTTPS using invalid certificate.

Changing the Factory Default Credentials

If cameras are in the factory default state or are using the admin/admin or administrator/<blank> credentials , change the camera credentials.

1. Select the **Admin Users** tab.
2. Click and select either or .
3. In the **Admin User Name** column, enter a new username for one or all cameras.
4. In the **Admin Password** column, enter a new password for one or all cameras.

   > **Tip:** Select the checkbox next to the password field to see your entry.

5. Click **Apply**.

Changing the Connection Credentials

If the Camera Configuration Tool failed to log in to a camera, the camera displays this status: .

To change the credentials used to access the camera, complete the following steps:

1. Select the **Connection Credentials** tab.
2. Click in the camera status column and select the checkbox.
3. Double-click the **User Name** or **Password** field to enter different camera credentials.

   The settings you changed are highlighted in yellow.

   > **Tip:** Select the checkbox next to the password field to see your entry.

4. In the bottom-right corner, click **Apply**.

The tool will try to log in to the cameras using the new credentials. The camera status updates to show the cameras you have access to.

Adding a Secondary Admin User

Note: If the default administrator credentials are lost, you may need to restore the camera to the factory default settings. Depending on how the camera is configured, this option may not be possible.

To protect the default administrator user account on the camera, you may want to create a secondary admin user.

You can choose to use the secondary account for daily operations instead of the default administrator account. Or, you can use it as a backup in case the default administrator password is lost.

1. Select the **Admin Users** tab.
2. In the Secondary Admin User Name column, enter a new username.

   If you want to use the same username for all cameras, click then enter the username.
3. In the Secondary Admin Password column, enter a password for the new username.

   If you want to use the same password for all cameras, click then enter the password.

   Tip: Select the checkbox next to the password field to see your entry.
4. Click **Apply**.

You can add more admin users through the camera web browser interface, however the Camera Configuration Tool will only display the default administrator user and one other admin user on this tab.

Finding Cameras

If a camera is not auto-discovered by the Camera Configuration Tool, it may be on a different subnet that is not configured to allow multicast messaging. You can manually discover cameras and add them to the tool for configuration.

1. In the top-right corner, select ☰ > **Add Devices by IP**.
2. To find one camera:
   - Enter the IP address of the camera in the **Start IP Address** field. Leave the **End IP Address (Optional)** field empty.
3. To find multiple cameras:
   - Enter the IP address range. Enter the first IP address in the **Start IP Address** field, and the last IP address in the **End IP Address (Optional)** field.

     The Number of IP Addresses area displays the total number of IP addresses included in the IP range. The tool will search for no more than 65,536 addresses at a time.
4. Enter the **User Name** and **Password** for the cameras.
5. Update the **HTTP Port #** and **HTTPS Port #** if needed.
6. Click **Add Devices**.

The tool searches through all the addresses in the IP address range, and does not stop until all the IP addresses have been checked or you click **Cancel**. The search occurs in the background so you can continue to use the tool during the search. If a camera is discovered, it is automatically added to the camera list.

> **Tip:** New cameras may not be displayed if the camera list is filtered. For more information, see *Filtering and Sorting Cameras* on the next page.

Sending a Discovery Broadcast

If you are in the process of configuring a large system, there may be new cameras added to the network over an extended period of time. The Camera Configuration Tool sends out a discovery broadcast every minute, but you can force the software to send a discovery broadcast as well.

The discovery broadcast looks for new cameras that are connected to the network. Each time it discovers a new camera, it is added to the camera list.

- In the top-right corner, click ↻.

Filtering and Sorting Cameras

Depending on the size of your site, you may need to edit over 100 cameras. To help you focus on the cameras that need your attention, you can filter or sort the listed cameras.

Filtering Cameras

1. At the top of a column, click .
2. Select or enter your filter values.

   A list of the active filters is displayed at the bottom of the page.

Clearing a Filter

- At the bottom of the page, click **X** for the filter that you want to remove.

Sorting Cameras

- Click the column name to sort the column in ascending alphanumeric order.
- Click the same column again to sort the column in descending order.

  You can sort any column that is displayed.

Editing Cameras

In the Camera Configuration Tool, you can edit all the cameras that you have successfully logged into.

Move between different tabs to see and edit the categorized camera settings. For more information, see *Setting Tabs* on page 9.

You can only edit the cameras that are displayed. To edit specific cameras, you can filter the camera list. For more information, see *Filtering and Sorting Cameras* on the previous page.

> **Tip:** As you edit the camera settings, you can disable camera filters but you cannot add new filters until after the setting changes have been either applied or discarded.

You can edit any column that displays .

Editing a Single Camera

To edit a setting for a single camera, do one of the following:

- Select a setting from the options available.
- Double-click the camera setting, then enter a new value.

The edited setting is highlighted in yellow but is not yet applied. See *Applying Changes* below.

> **Note:** Changes made to the HD Multisensor Dome camera are automatically applied to all camera heads.

Editing Multiple Cameras

To edit the same setting for all cameras in the camera list:

1. In the column heading, click .
2. Select or enter the new setting.
3. Press Enter or click **Apply** to change the setting.

The edited settings are highlighted in yellow but are not yet applied. See *Applying Changes* below.

Applying Changes

Edited settings are highlighted in yellow.

To apply all changes:

- Click **Apply** to validate the changes.

  If the camera rejects a setting, the camera row is highlighted in red and the rejected setting is highlighted in yellow.

  In the bottom-right implementation area, click next to **FAILED** to display only cameras with rejected settings.

To clear all changes:

- Click **Discard**.

Setting Tabs

The tabs in the menu bar provide you with a filtered list of settings and information about each camera.

The first 6 columns are the same in every tab:

1. **Web UI** — a direct link to the camera's full web browser interface for advanced configuration.
2. **Live video** — a low quality live stream from the camera to help you identify where the camera is installed.
3. **Camera status** — identifies if the camera is online and if you were able to successfully log in to the camera.
4. **Model** — the specific camera model.
5. **Name** — the name of the camera. By default, the camera name is the same as its model number.
6. **Head #** — identifies the camera head for multisensor cameras.

The tabs show the following details:

Note: Some settings are not displayed if they are not supported by the camera.

Tab	Settings
General	• Location • Disable Camera Status LEDs • Date First Discovered • Date Last Discovered • Serial Number • Manufacturer • Firmware Version • Date — the date and time of the camera

Tab	Settings
Network	• Enable DHCP • IP Address • Subnet Mask • Default Gateway • Hostname • NTP Server Mode • NTP Server • MAC Address • Enable HTTP • HTTP Port # • HTTPS Port #
TLS	• Download CSR • TLS Certificate Subject • TLS Certificate Issuer • Expiry Date • Certificate Type • Signature Algorithm • Manage Certificates • Certificates
Image Settings	• Encoding • Flicker Control • Enable WDR • Image Rate • Quality • Max Bitrate • Resolution • Keyframe Interval • Camera Heads • Camera Mode
Admin Users	• Admin User Name • Admin Password • Secondary Admin User Name • Secondary Admin Password

Tab	Settings
Analytics	• Camera Type • Analytics Scene Mode • Enable Noise Filter • Tamper Sensitivity • Tamper Trigger Delay • Enable Self Learning • Reset Self Learning • Video Analytics Mode • Analytic Events
All Settings	All available camera settings. Scroll right to see any settings that may be hidden.
Connection Credentials	• User Name • Password
Firmware Update	• Firmware Version • Available Firmware Version • Upgrade • Downgrade

Assigning IP Addresses

Note: Do not assign static IP addresses unless you are highly familiar with IP network addressing. The Camera Configuration Tool is not designed to calculate or validate IP address ranges, subnet masks, default gateways or other IP parameters.

Assigning Static IP Addresses

If you need to assign static IP addresses to the cameras in your system, you can do so from the Network tab. This tab allows you to apply an IP address range to the listed cameras, or apply a specific IP address to a camera.

Tip: Only assign IP addresses from subnets that you can access, or you will lose access to the cameras after the new IP addresses have been applied. You may be able to recover the camera by assigning a new IP address by the camera's MAC address. For more information, see *Assigning an IP by MAC Address* on the next page.

1. Select the **Network** tab.
2. To assign a static IP address range to the listed cameras:
   a. Filter the camera list to only display the cameras you want to change.
   b. At the top of the IP Address column, click .
   c. Enter the first IP address in the range in the **Start IP Address** field.
   d. Enter the **Subnet Mask** and **Default Gateway** for the IP addresses.
   e. Click **Apply**.

      DHCP is automatically disabled for the cameras, and the new network settings are highlighted in yellow.
3. To assign a static IP address to one camera:
   a. Locate the camera you want to change from the list.
   b. Double-click the **IP Address** field and enter the static IP address.

      DHCP is automatically disabled for the camera.

   c. Double-click the **Subnet Mask** field and the **Default Gateway** field to enter the required values.
4. At the bottom-right corner of the window, click **Apply**.

The new IP addresses are implemented on the cameras.

Assigning an IP by MAC Address

If you lose connection to a camera after it is assigned an IP address that you don't have access to, you can attempt to locate the camera by its MAC address then assign it a new IP address. After the Camera Configuration Tool connects to the camera once, it remembers the camera's MAC address.

If you know a camera's MAC address, you can also use this method to add a new camera to the Camera Configuration Tool.

> **Note:** You may need to reboot the camera to implement the new IP address.

1. If you've lost connection to a camera, locate the camera in the list and select one of its settings.

   The tool automatically copies the camera's MAC address and current IP address.

2. In the top-right corner, select ☰ > **Reset IP by MAC**.
3. Enter the camera's MAC address in the **MAC Address** field.
4. In the **IP Address** field, enter a new IP address for the camera.
5. Click **Set Device IP Address**.

The tool attempts to discover the camera and apply the new IP address. When the tool succeeds, the camera receives the new IP address and is added to the camera list.

If the tool is unable to apply the new IP address, you may be prompted to manually reboot the camera.

Setting the NTP Server

You can update the Network Time Protocol (NTP) server used for each camera.

1. Select the **Network** tab.
2. In the NTP Server Mode column, select **DHCP** or **Manual**.
3. If you select Manual, in the NTP Server column, enter the NTP server address.
4. Click **Apply**.

Managing Certificates

For increased security and efficiency, you can manage camera certificates and configure secure network connections in bulk using the Camera Configuration Tool.

Downloading a Certificate Signing Request

Download a Certificate Signing Request (CSR) for each camera. The CSR must be signed by a certificate authority (CA) to apply it to a camera.

1. Select the **TLS** tab.
2. In the Download CSR column, select the checkbox.
3. Click **Apply**.
4. Enter a **Common Name**. Maximum 64 characters, including the appended camera identifier. A preview is displayed.
    - Select the camera identifiers to append to the common name: **Hostname**, **IP Address**, **Serial Number**, or **MAC Address**. You can append multiple camera identifiers, but you must append at least the Serial Number or MAC Address.
5. Enter the following optional fields:
    - **Organizational Unit** — The division of an organization.
    - **Organization** — The organization name.
    - **Locality** — The city where the organization is located.
    - **State Or Province** — The state or province where the organization is located.
    - **Country** — The 2-letter country code.
    - **Subject Alternative Name** — The DNS hostname. Currently, you can only enter 1 hostname.
6. Click **Download CSR** and select where to save the CSR.

The CSR will be downloaded as a zip file. Submit this to a CA to be signed.

Uploading Signed Certificates

Once the CSRs have been signed by a CA, zip up all certificates to upload into the Camera Configuration Tool.

1. In the top-right corner, select ☰ > **Upload Certificates**.
2. Select the zip file containing the signed certificates.
3. Review the summary of the signed certificates.
4. Click **Upload**. Only certificates for connected devices will be uploaded.
5. Click **OK**.

The uploaded certificates can now be applied to their respective devices.

Applying Certificates

After you upload signed certificates, you can select which certificate to use for each device.

1. Select the **TLS** tab.
2. In the TLS Certificate Subject column, select a certificate.
3. Click **Apply**.

> **Tip:** Click **Manage** to view details about all available uploaded certificates before applying one to a camera.

Deleting Certificates

You can remove invalid, expired, self-signed or unwanted certificates from the Camera Configuration Tool.

> **Note:** You cannot delete a certificate that is Currently Active. Apply a different certificate, and then delete the unused certificate.

1. Select the **TLS** tab.
2. In the Manage Certificates column, click **Manage**.
3. Click **Delete** next to the certificate you want to delete.
4. Click **Yes** to confirm.

Network Security

By default, the Camera Configuration Tool will try to connect to cameras using secure HTTPS. If a secure connection is unavailable, the tool will use HTTP. You can manage these network settings.

Securely connected cameras will display one of the icons , , or next to their camera status.

Disabling HTTP Connections in the Camera Configuration Tool

For increased security, you can prevent the Camera Configuration Tool from connecting over HTTP if secure connections are unavailable. Cameras that cannot connect over HTTPS will appear offline.

1. Close the Camera Configuration Tool application.
2. In Windows Explorer, navigate to the installation folder. By default, this is `C:\Program Files (x86)\Motorola Solutions\Camera Configuration Tool`.
3. Double-click `CCT_DisableHttp.reg` to prevent the application from using HTTP.
4. Click **Yes**, then **OK**.
5. Open the Camera Configuration Tool application.

To re-enable connections over HTTP:

1. Close the Camera Configuration Tool application.
2. In Windows Explorer, navigate to the installation folder. By default, this is `C:\Program Files (x86)\Motorola Solutions\Camera Configuration Tool`.
3. Double-click `CCT_EnableHttp.reg`.
4. Click **Yes**, then **OK**.
5. Open the Camera Configuration Tool application.

Disabling HTTP Connections for a Camera

You can configure cameras to enable secure connections over HTTPS only.

1. Select the **Network** tab.
2. In the Enable HTTP column, clear the checkbox to use HTTPS only.
3. *Optional.* In the HTTPS Port # column, enter the HTTPS port number.
4. Click **Apply**.

Changing the HTTP or HTTPS Port

You can select which ports the cameras should use to connect to the network over HTTP and HTTPS.

1. Select the **Network** tab.
2. In the HTTP Port # column, enter the HTTP port number
3. In the HTTPS Port # column, enter the HTTPS port number.
4. Click **Apply**.

Configuring Analytics

If you have a video analytics camera, you can configure analytics settings in bulk in the Analytics tab.

Analytics Setting Description

The following table describes each setting. To configure the same setting for multiple cameras, click .

Column	Description
Camera Type	Select the type of camera that has been connected. • **Day and Night** — select this option if the camera can stream video in color or black and white. This type of camera typically displays color video during the day and black and white video at night to capture as much detail as it can of the scene. • **Color** — select this option if the camera can only stream video in color. • **Black and White** — select this option if the camera can only stream video in black and white. • **Thermal** — select this option if the camera can stream forward looking infrared (FLIR) video.

Column	Description
Analytics Scene Mode	Select the location that best describes where the camera is installed. • **Outdoor** — suitable for most outdoor environments. This setting optimizes the camera to identify vehicles and people. • **Large Indoor Area** — only detects people and is optimized to detect people around obstructions, like chairs and desks, if the head and torso are visible. • **Indoor Overhead*** — optimized for cameras mounted directly overhead and should only be used when a torso cannot be seen in the camera field of view. Any movement is assumed to be human. Use in areas with limited space but with high ceilings, or to monitor doors. Do not use with the Avigilon Appearance Search feature, Face Recognition, the Self-Learning feature, or to detect people traveling against the crowd. • **Outdoor High Sensitivity*** — optimized to run with higher sensitivity for detecting people and vehicles in challenging outdoor scenes. This option may generate more false positives. Only use this option if you require the system to be more sensitive than the Outdoor setting. • **Long Range Night*** — prioritizes outdoor long-range object detection at night over object classification and tracking during the day. Uses external IR illumination rather than built-in IR illumination from the camera. Object classification and tracking accuracy during the day is reduced compared to other outdoor modes. Available for H4A cameras only. * These modes are not available for H5A cameras.
Enable Noise Filter	Select the checkbox if the camera is too sensitive and falsely detects motion as classified objects.
Tamper Sensitivity	Enter a value between 1-10 to select how sensitive a camera is to tampering events. Tampering is a sudden change in the camera field of view, usually caused by someone unexpectedly moving the camera. Lower the setting if small changes in the scene, like moving shadows, cause tampering events. If the camera is installed indoors and the scene is unlikely to change, you can increase the setting to capture more unusual events.
Tamper Trigger Delay	Enter a value between 2-30 to define how many seconds the camera will wait before sending tampering events. The default value is 8. If the tampering ends before the trigger delay time has elapsed, no tampering events will be sent. If the time elapses but the tampering has not stopped, the events will be sent by the camera.
Enable Self Learning	Select the checkbox to enable self-learning.

Column	Description
Reset Self Learning	Click **Reset** after the camera is stable after initial configuration. Always reset self-learning after a camera is physically moved or adjusted, or if the focus or zoom level is changed. The change in the camera's FoV affects the video analytic results.
Video Analytics Mode	Select which analytics mode you want to enable. You can only configure Analytic Events for cameras using Classified Object mode. • **Classified Object** — detects and classifies objects such as a person or a vehicle. • **Unusual Motion Detection** — detects motion and compares the speed, direction, and location of movement with what is typical for a scene. • **Tamper Only** — detects sudden changes in the scene.
Analytic Events	Click **Configure** to manage analytic events for the selected camera in Classified Object mode. For more information, see *Configuring Analytic Events* on the next page.

Setting Up Classified Object Motion Detection

Use the Classified Object Motion Detection settings to configure object motion detection. This allows you to define when the system detects a person or vehicle in the scene.

The camera must be configured to use the Classified Object Video Analytics Mode.

1. Select the **Analytics** tab.
2. In the Analytic Events column, click **Configure**.
3. Select **Classified Object Motion Detection**, then click **Edit**.
4. Define the region of interest (ROI) where motion is detected. Motion events are only triggered if the bottom center of the detected object's bounding box is in the ROI.
   - Click and drag the yellow markers on the border. Extra markers are automatically added to help you fine tune the shape of the overlay.
   - Click and drag to move the green overlay.
   - Click to add an exclusion area. The exclusion area is added inside the green overlay.

     Classified object motion is *not* detected in exclusion areas.
   - To delete an exclusion area, select an exclusion area and then click .
   - Click to restore the default green overlay.

5. Define the objects that are detected by the system.
    a. Check the **Person** box to detect people in the area.
    b. Check the **Vehicle** boxes to detect vehicles in the area.
    c. Move the **Sensitivity:** slider to adjust how sensitive the system is to the detection of classified objects.

       If you set the slider to **Low**, the video analytics device will detect fewer objects because the system must be highly confident that it has detected a person or vehicle before you are notified of an event.

       If you set the slider to **High**, the video analytics device will detect more objects because the system does not need to be as certain of the object classification before you are notified of a motion event.

       If the slider is set too low, the system may miss classified object motion. If the slider is set too high, the system may generate a higher number of false classified object motion detections.
    d. In the **Threshold Time:** field, set how long an object must be moving before an classified object motion detection event is triggered.
6. Click **OK** to save your settings.

Configuring Analytic Events

You can add, edit, and delete analytic events for individual cameras from the Camera Configuration Tool.

- In the Analytic Events column, click **Configure**. The Analytic Events dialog box is displayed.

To add an analytic event:

1. Click .
2. Enter a name for the event.
3. Select the **Enabled** checkbox. If the checkbox is clear, the video analytics event will not detect or trigger any events.
4. Select an **Activity:**. For a description of each option, see *Analytic Event Descriptions* on the next page.
5. Configure the green video overlay to specify the region of interest (ROI).

   Note: Analytic events are only triggered if the bottom center of the detected object's bounding box is in the ROI or crosses the beam.

6. Select the **Object Types:** the event applies to.

7. Click **Show Advanced Options** and configure the available settings:
    - **Sensitivity:** — the likeliness of an object to trigger the event. The greater the sensitivity, the more likely an event will be triggered for objects detected with low confidence. The default value is 8.
    - **Number of Objects:** — the number of objects required to trigger the event.
    - **Threshold Time:** — the minimum duration of the event before the system triggers an event. The default value is 0-30 seconds depending on the activity.
    - **Timeout:** — the maximum duration of the event. Events that are still active after this time will trigger a new event. The default value is 60 minutes.
    - **Prohibited Direction:** — the arrow in the circle defines the direction that objects should not be traveling.
8. Click **OK** to save your settings.

To edit an analytic event:

1. Select an event and click .
2. In the following dialog box, make the required changes.

> **Note:** If you change the name of the event, any rules or alarms linked to the event may no longer function.

To delete an analytic event:

- Select an event and click .

Analytic Event Descriptions

The following table shows the Activity: options that can be used when configuring analytic events. For more information and advanced options, see *Configuring Analytic Events* on the previous page.

> **Note:** The region of interest (ROI) is like a rug or tripwire. Events are only triggered if the bottom center of the detected object's bounding box is in the ROI or crosses the beam.

Activity:	Description
Objects in area	The event is triggered when the selected number of objects are present in the ROI for longer than the threshold time. The object can appear from within the ROI or enter from outside. Only one event is activated when the specified number of objects are detected in the area. Additional objects in the area will not trigger additional events.

Activity:	Description
Object loitering	The event is triggered for each object that stays within the ROI longer than the threshold time. Each object triggers a separate event. The event resets when the object leaves the ROI or the event times out.
Objects crossing beam	The event is triggered when the specified number of objects have crossed the beam in the specified direction within the threshold time. If the number of objects is 1, the event is triggered after the threshold time elapses. ◦ To change the direction of the beam, click . ◦ To detect objects traveling in either direction of the beam, click .
Object appears or enters area	The event is triggered once for each object in the ROI for longer than the threshold time. The object can appear from within the ROI or enter from outside the ROI. This video analytic event causes many alarms. For example, if 20 objects are detected within the ROI, 20 events are triggered – one for each object.
Object not present in area	The event is triggered when no objects are present in the ROI for longer than the threshold time.
Objects enter area	The event is triggered when the specified number of objects are detected in the field of view (FoV) then enter the ROI within the threshold time. If the number of objects is 1, the event is triggered after the threshold time elapses. The ROI must be smaller than the camera FoV to detect the object before it enters the ROI. Objects that appear within the ROI will not trigger an event. Only one event is activated when the specified number of objects are detected in the area. Additional objects in the area will not trigger additional events.
Objects leave area	The event is triggered when the specified number of objects are detected inside the ROI then leave the ROI within the threshold time. If the number of objects is 1, the event is triggered after the threshold time elapses. The ROI must be smaller than the FoV of the camera.
Object stops in area	The event is triggered if a classified object is detected moving within the ROI then stops moving for longer than the threshold time. One event is activated for each object that stops. An object can only be tracked for up to 15 minutes.

Activity:	Description
Direction violated	The event is triggered for each object that moves within 22 degrees of the prohibited direction for longer than the threshold time. One event is activated for each classified object that moves in the prohibited direction.

Updating Firmware

The Camera Configuration Tool lets you apply firmware updates to all the cameras in your camera list. Download and apply the firmware to connected cameras.

Downloading Firmware

1. Go to your camera website and download the camera firmware `.fp` file for your model.
2. Save the firmware `.fp` files to the Firmware directory in the installation folder. The default path is: `C:\Program Files (x86)\Motorola Solutions\Camera Configuration Tool\firmware`

To remove firmware files that are no longer used, delete the `.fp` file from the directory.

Applying Firmware

> **Tip:** To view available downloaded firmware, in the top-right corner select ☰ > **View Local Firmware Repository**.

1. Select the **Firmware Update** tab and filter the displayed cameras as required.
2. In the Available Firmware Version column, click .
3. Select the firmware, then click **Apply**. The selected firmware will only be applied to the related camera models.
4. Select the checkbox in the **Upgrade** or **Downgrade** columns. You must select a checkbox to install the firmware to the camera.

   The checkboxes are only displayed if the selected firmware is different from the version on the camera.
5. Click **Apply**.

The firmware is sent to the cameras and installed. The cameras may reboot and go offline to complete the update.

Depending on the number of cameras and the network speed, the update process can take a long time.

Exporting and Importing Settings

You can export the cameras list into a comma separated values (.csv) file. The .csv file includes all the camera's available settings.

You can import the settings back into the Camera Configuration Tool and apply the settings to the cameras list.

Exporting Settings

You can export camera settings to edit and re-import. The exported file can also act as a backup of the current camera settings.

1. (Optional) Filter the cameras list.

   Only the listed cameras are included in the export. For more information, see *Filtering and Sorting Cameras* on page 6.

2. In the top-right corner, select ☰ > **Export Device Settings**.
3. In the Save As dialog box, name and save the export file.

Editing the Export File

You can edit an exported file then import the changes back into the Camera Configuration Tool.

If you edit the export file, keep the following in mind:

- Do not delete or re-order the columns.
  Deleting or changing the order of the columns corrupts the file and prevents the exported file from being imported again.
- Do not change the camera MAC Address.
  The Camera Configuration Tool uses the camera MAC Address to identify the cameras that are changed.
- If you apply a static IP address to a camera, change the **DHCPEnabled** column setting to *False*.
  If the **DHCPEnabled** column setting is *True*, the new static IP address will not be applied.

Importing Settings

You can import an updated .csv file into the Camera Configuration Tool to make bulk changes to the camera list.

1. In the top-right corner, select ☰ > **Import Device Settings**.
2. In the Open dialog box, select and open the camera settings .csv file.

   A confirmation message is displayed. The message includes the number of devices listed in the import file, and the number of devices that the Camera Configuration Tool can edit.

   If the settings file contains any errors, an error message is displayed. The error message includes a list of the issues that need to be corrected in the settings file. Correct the settings file then try again.

3. Click **Edit Devices**.

   The settings are imported into the Camera Configuration Tool. Modified settings are highlighted in yellow.

4. Click **Apply** to implement the changes.

Device Logs

To help you review and investigate issues, you can download a copy of the camera logs and track a live stream of the log messages.

1. Filter the camera list to only display the cameras you want to log.
2. In the top-right corner, select ☰ > **Device Logs**.
3. In the Device Logs window, click **Write Logs to File**.
4. Select a location to save the log file.

   The existing camera logs are automatically downloaded. The system continues to stream and record the live camera logs until you click **Stop** or close the Device Logs window. While the logs are streaming, you can continue to edit cameras in the Camera Configuration Tool.

In the Device Logs window, the left Devices list are the cameras included in the log file. On the right Logs list are the log messages in chronological order.

The log stream auto-scrolls to the latest message until you click a message in the stream. At this point, the auto-scrolling stops so you can read the message while the log stream continues. To have the application resume auto-scrolling, drag the scroll bar to the end.

You can identify what device is referenced in the log message by the Serial Number. If a camera goes offline, the camera will stop logging until it returns online - the other cameras in the Devices list will continue to stream their logs.

The log file you saved is in .txt format. You can also review the saved log in a text reader.

Each time you open the Device Logs window, the previous log is displayed. When you click Write Logs to File, the Devices list refreshes to include the latest filtered cameras and saves a new log file.